In the Name of God

Journal of
Information Systems & Telecommunication
Vol. 13, No.1, January-March 2025, Serial Number 49

Research Institute for Information and Communication Technology
Iranian Association of Information and Communication Technology
Affiliated to: Academic Center for Education, Culture and Research (ACECR)

Print ISSN: 2322-1437
Online ISSN: 2345-2773
Publication License: 91/13216
Editorial Office Address: No.5, Saeedi Alley, Kalej Intersection., Enghelab Ave., Tehran, Iran,
P.O.Box: 13145-799 Tel: (+9821) 88930150 Fax: (+9821) 88930157
E-mail: info@jist.ir , infojist@gmail.com
URL: jist.acecr.org

Indexed by:
- SCOPUS www. Scopus.com
- Islamic World Science Citation Center (ISC) www.isc.gov.ir
- Directory of open Access Journals (DOAJ) www.Doaj.org
- Scientific Information Database (SID) www.sid.ir
- Regional Information Center for Science and Technology (RICeST) www.ricest.ac.ir
- Magiran www.magiran.com

Publisher:
Iranian Academic Center for Education, Culture and Research **(ACECR)**

This Journal is published under scientific support of
Advanced Information Systems (AIS) Research Group and
Telecommunication Research Group, ICTRC

Acknowledgement

JIST Editorial-Board would like to gratefully appreciate the following distinguished referees for spending their valuable time and expertise in reviewing the manuscripts and their constructive suggestions, which had a great impact on the enhancement of this issue of the JIST Journal.

(A-Z)

- Alaeiyan, Mohammad Hadi, K.N. Toosi University of Technology, Tehran, Iran
- Al-Musawi, Bahaa, kufa university, kufa, Iraq
- Azarkasb, Seyed Omid, K.N. Toosi University of Technology, Tehran, Iran
- Aidi, Mohammad, Ilam University, Ilam,Iran
- Agahi, Hamed, Islamic Azad University ,Shiraz, Iran
- Anam, Syaiful, Brawijaya University, Malang, Indonesia
- Chenthur Pandian, Ram Kumar, Sri Krishna College if Technology Coimbatore, India
- Ebadati, Omid Mahdi, Kharazmi University,Tehran, Iran
- Fathi, Amir, Urmia University, Urmia, Iran
- Farsi, Hassan, University of Birjand, South Khorasan, Iran
- Farsijani, Hassan, Shahid Beheshti University, Tehran, Iran
- Fadaeieslam, Mohammad Javad, Semnan University, Iran
- Kheirkhah, Fatemeh, ACECR, Tehran, Iran
- Khorshidi, Mohammadreza, University of Birjand, South Khorasan, Iran
- Kolahkaj, Maral, Islamic Azad University, Karaj Branch, Iran
- Kamel Tabakh, Seyed Reza, Islamic Azad University, Mashhad Branch, Iran
- Kazerouni, Morteza, Malek-Ashtar University of Technology, Tehran, Iran
- Khamseh, Abbas, Islamic Azad University, Karaj Branch, Iran
- Moradi, Gholamreza, Amirkabir University,Tehran, Iran
- Mohammadzadeh, Sajjad, University of Birjand, South Khorasan, Iran
- Masoudifar, Mina, Hakim Sabzevari University, Sabzevar, Iran
- Marvi, Hossein, Shahrood University of Technology, Semnan Province, Iran
- Maghdid, Halgurd Sarhang, Koya University, Kurdistan Region, Iraq
- Obied, Ali, University of Al-Qadisiyah, Qadisiyyah, Iraq
- Patange , Abhishek, ABB Group, Zurich, Switzerlan
- Patel, Arpita, Charotar University of Science and Technology, Gujarat, India
- Rashno, Armin, Lorestan University, Iran
- Srivastava, Ashutosh, siddharth university, Kapilvastu, India
- Shaddiq, Syahrial, Lambung Mangkurat University, South Kalimantan, Indonesia
- Soleimanian Gharehchopogh, Farhad, Islamic Azad University Urmia, Iran
- Tourani, Mahdi, University of Birjand, South Khorasan, Iran
- Tashtarian, Farzad, Islamic Azad Mashad University, Mashad, Iran
- Uddin Talukdar, Muhammad Borhan, Daffodil International University, Bangladesh
- Zahedi, Mohammad Hadi, K. N. Toosi University of Technology, Tehran, Iran
- Zakeri, Bijan , Babol Noshirvani University of Technology, Mazandaran, Iran

Table of Contents

- **Outage Performance of Cooperative Underlay Cognitive Radio Relay Based NOMA Networks with Energy Harvesting Capability** 1

Maryam Najimi

- **Numerical Study of a Switchable Polarization for Reflect-array Unit-cell for Satellite Communications** 12

Mohammad Mansourinia and Ramezan Ali Sadeghzadeh

- **A Turkish Dataset and BERTurk-Contrastive Model for Semantic Textual Similarity** 24

Somaiyeh Dehghan and Mehmet Fatih Amasyali

- **Review on Architecture and Challenges in Smart Cities** 33

Mehdi Azadimotlagh, Narges Jafari and Reza Sharafdini

- **A Novel Hybrid Convolutional-Attention Recurrent Network (HCARN) for Enhanced Cybersecurity Threat Detection** 50

Archana R. Laddhad and Gurveen Vaseer

- **Enhancing IoT Device Behavior Prediction through Machine Learning Models** 63

Shubham Minhass, Ritu Chauhan and Harleen Kaur

Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 1-11
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Outage Performance of Cooperative Underlay Cognitive Radio Relay Based NOMA Networks with Energy Harvesting Capability

Maryam Najimi[1*]

[1].Department of Electrical and Computer Engineering, University of Science and Technology of Mazandaran, Behshahr, Iran

Received: 05 Nov 2023/ Revised: 04 Apr 2025/ Accepted: 04 May 2025

Abstract

In this work, Non-orthogonal multiple access (NOMA) technology is considered in cognitive radio (CR) networks in which the secondary users can only access the utilized spectrum of the primary user such that the primary user can tolerate the interference created by the secondary network. On the other words, the combination of CR and NOMA (CR-NOMA) is a novel concept to enhance the spectrum efficiency and the reliability of the network communication. The relaying technology with capability of energy harvesting is also considered which can improve the outage performance. In this scheme, the proper relay harvests energy from the secondary transmitter while it transmits the data of the secondary transmitter to the corresponding receiver. With this regard, the network throughput is improved in outage behavior and imperfect successive interference cancellation (SIC) condition at two users. Hence, the proposed problem is maximizing the performance of the network by proper selection of the relay for data transmission, setting the transmission power of the selected relay and optimal power allocation coefficients to each user with constraints on the outage probability and the interference in the primary user communication. For solving the problem, an iterative low complexity algorithm is proposed using the convex optimization scheme and Karush–Kuhn–Tucker conditions to select the best relay for transmission and users' power allocation coefficients and also set the transmission power of the selected relay. Simulation results verify the effectiveness of the proposed algorithm for increasing almost 30 percent of the network performance in comparison to the bench mark algorithms in different conditions.

Keywords: NOMA-Cognitive Network; SIC Technique; Network Throughput; Convex Optimization Method; Probability of Outage.

1- Introduction

Non orthogonal multiple access (NOMA) is a technique for the fifth generation (5G) wireless communication in comparison with OMA approach. On the other words, NOMA-enabled user utilizes the available resources such as frequency/time/code which results in spectral efficiency, user fairness and low latency in spectrum access [1]. In the NOMA networks, the transmitter sends its signals to all receivers by allocating different fractions of its power to nodes with respect to the estimated channel conditions. On the other hand, more transmission power is assigned to the users with weaker channels while the users with strong channels have less transmission power coefficients. Therefore, the users with stronger channels perform a successive interference cancellation (SIC) technique to decode signals of the other users and obtain their own signals [2], [3]. In [4], the performance of NOMA is studied in partial channel state information (CSI). They also state the outage probability in a closed form expression and the average two users' sum rate is calculated. To improve the network performance, NOMA scheme with relay is considered especially when the users are far from the transmitter or the channel condition is weak [5]. In [6], [7] and [8], a cooperative NOMA network with relay is studied. It is shown that the performance of both non-cooperative NOMA and cooperative OMA are worse than the cooperative NOMA. On the other hand, the cooperative communication can enhance the reliability of the users especially cell-edge users [9].

Due to the development of the high data rate services, the fixed spectrum allocation is not useful and spectral efficient communication networks are required. In cognitive radio (CR) networks, the primary users have the exclusive rights

✉ **Maryam Najimi**
Email Address: M.najimi@mazust.ac.ir

to use the spectrum. However, in these networks, the primary network allows the frequency band is utilized by the secondary network with respect to the interference created by the secondary users on the primary user communications [10]. In [11], combination of NOMA and CR networks is utilized to ensure a reliable transmission from primary users and secondary users while the spectral efficiency is improved. This enhancement can be obtained by using cognitive radio networks based on NOMA technique when the secondary transmitter sends its NOMA messages to its secondary receivers on the licensed spectrum if the primary user can stand the inter- network interference created by the secondary users' communications. However, in NOMA technology, intra-network interference can also happen when several users access the same spectrum with different power levels. Therefore, a proper combination of NOMA and CR networks is required to decrease the interference and improve the spectrum utilization.

Energy efficiency is another important issue in these networks due to the energy constraints of devices [12]. Energy harvesting (EH) is a technique where the radio frequency (RF) signals are used as the sources for harvesting the energy of wireless devices [13]. In this case, the energy efficiency of cognitive radio networks can be enhanced by utilizing the energy harvesting techniques [14]. In [15], the energy efficiency is maximized by power transmission allocation in unmanned aerial vehicles based NOMA networks.

1-1- Related Works

In [9], outage probabilities of primary user and secondary users are derived under imperfect CSI and imperfect SIC in cooperative cognitive radio networks based NOMA. In [16], underlay CR- NOMA network is considered and the probability of outage is evaluated to show the performance of secondary NOMA users. In [17], the error rate performance of a NOMA based CR network is considered by relay selection with imperfect SIC. In [18], a NOMA network is proposed with capability of energy harvesting. In this paper, multiple groups are considered with two users in each group where the NOMA technique is applied in each group and OMA technique is applied for inter- group. In this paper the performance of the system is analyzed and a closed form expression is derived for outage probability with imperfect channel state information (ICSI) consideration. In [19], a cooperative CR network is studied and outage probability is derived with ICSI consideration. Optimal power allocation for two users is also obtained such that the fairness of outage probability is maintained for two users. In [20], a cooperative NOMA network underlay cognitive radio network is studied with imperfect SIC and the probability of outage is obtained for each secondary user. In [21], the problem of maximizing the minimum secrecy energy efficiency is proposed by time slot and secondary transmission power allocation under transmission security and reliability constraints in a CR-NOMA network with the capability of non-linear energy harvesting of the secondary users. In [22], the reliability and security performance of a cooperative NOMA cognitive radio network is studied in the existence of eavesdroppers. The connection outage secrecy outage probabilities of each primary user are derived with cooperative NOMA and non-cooperative NOMA. In [23], a distributed sequential coalition formation algorithm is proposed for user grouping and power allocation such that the minimum rate requirement of the primary user is satisfied. In [24], a cooperative underlay cognitive radio NOMA is considered and the outage probability for two secondary NOMA user is calculated under Nakagami-m fading channel. In [25], A CR-NOMA network is proposed for spectrum efficiency and an energy harvesting relay scheme is considered to forward the secondary transmitter messages to the secondary receivers. In this paper, the outage probability and the throughput network are obtained on imperfect SIC. In [26], the outage probability and the system throughput are derived while the effect of the power allocation coefficient of NOMA and energy harvesting parameters on outage with imperfection SIC are investigated. In [27], ergodic sum rate and outage probability of the network are investigated in full duplex and half duplex modes at secondary user. In [28], the outage probability is expressed while the network throughput is improved in imperfect SIC condition.

To the best of our knowledge, the above works have made efforts to solve a variety of problems in CR-NOMA networks while the outage probability is obtained. However, maximization of the network throughput and improvement of the outage probability and the interference created for the primary user communication are not considered simultaneously in these works. Therefore, this motivates us to explore the efficiency of the cognitive radio relay based NOMA networks by selecting the suitable relay, setting its transmission power and allocating power coefficients of the secondary users. A summary of the works is provided in table 1.

1-2- Motivation and Contributions

In this work, a CR-NOMA network is considered with the energy harvesting capability of the relays. On the other hand, the secondary transmitter is allowed to forward its messages to its secondary users via the proper relays such that the primary user can stand the interference created by the secondary user communications. We also note that the CR-NOMA network works with imperfect SIC over Rayleigh fading channel. Therefore, our proposed problem is maximizing the overall throughput of network by selecting the suitable relay, setting its transmission power and allocating power coefficients of the secondary users so that

the outage probability of the secondary users and interference created for the primary user are improved. The main contributions of the paper are stated as

- A cognitive radio network is investigated, where the secondary source can use the licensed spectrum of the primary user and employs NOMA to forward its messages through the proper relay with energy harvesting capability to two secondary destinations through the Rayleigh fading channel.
- We formulate the problem of maximizing the network throughput by selecting the suitable relay, setting its transmission power and power allocation coefficients of the secondary users under the outage probability of the secondary users and interference created for the primary user communication constraints.
- The problem is solved using the convex optimization method and KKT conditions are applied to determine the optimal conditions. Then, an algorithm based on ellipsoid method is proposed to search the optimal solution for the problem which has polynomial complexity.
- Simulation results verify the efficiency of the proposed algorithm for improving the network throughput and outage probability of the secondary users and also interference created for the primary user communication.

This paper is stated as follows. In section 2, the system model is stated. The motivation and problem statement and its solution are stated in section 3. The proposed algorithm for solving the problem is stated in section 4. In Section 5, Simulation results are presented. Analysis of results are presented in section 6 while the conclusions are stated in section 7.

Table 1. Summary of the Works

Proposed Works(Ref.)	***Year***	***Contributions***
[9],[18],[19] ,[20],[24]	2024,2018,2019 ,2019,2018	Outage probability is derived under imperfect SIC or imperfect CSI
[17]	2020	Error rate performance is considered by relay selection with imperfect SIC
[21]	2018	Minimum secrecy energy efficiency is maximized by time slot and secondary transmission power allocation under transmission security and reliability constraints with the capability energy harvesting of the secondary users
[22]	2019	Reliability and security performance of a cooperative NOMA-CR network is studied
[23]	2019	Power allocation is done such that the minimum rate requirement of the primary user is satisfied
[25], [26], [28]	2020,2024,2025	Outage probability and the throughput network are obtained on imperfect SIC
[27]	2023	Ergodic sum rate and outage probability of the network are investigated in FD/HD modes

2- System Model

A cooperative cognitive radio (CR)-NOMA network is considered with the capability of energy harvesting of the relays (Fig.1). Primary network includes one primary transmitter and one primary receiver while in secondary network, the secondary source selects a suitable relay from the N relay and forwards its messages to two NOMA users (U_1 and U_2). It should be noted that due to the poor channel condition or the long distances between the secondary transmitter and secondary receiver, the proper relay can receive the information and harvest the energy to forward the signal to the secondary users by decode-and-forward (DF) technique utilization.

The wireless channel model is the Rayleigh fading model. We also assume that all nodes (primary or secondary users) have one antenna with available CSI. However, SIC is done in the secondary user. According to the cognitive radio network scenario, transmission of the secondary network is only allowed if the primary user can tolerate the interference created by the secondary transmission on the primary user communication. Therefore, the restriction on the transmission power of the nth relay is stated as follows

$$P_{R_n} \leq \min\left(\frac{I_{th}}{|h_{R_nP}|^2}, {P_{R_n}}^H\right) \quad (1)$$

Where I_{th} is the interference temperature constraint on primary user while h_{R_nP} is the channel coefficient between the n th relay and primary receiver [29]. In NOMA transmission, the secondary source sends its signal $X_s(t) = \sqrt{\alpha_i P_s}\, x_i + n_R$ to the suitable relay. In this scheme, α_i is the portion of the transmission power P_s for the ith user with $\sum_{i=1}^{2} \alpha_i = 1$. x_i is the unit messages of the i th user and n_R is the additive white Gaussian noise (AWGN) between the secondary source and the proper relay with variance N_0.

We assume three time slots with the duration T. The first time slot with duration δT is considered for energy harvesting the selected relay and the second time slot with duration $(1-\delta)\frac{T}{2}$ is for transmitting data from the secondary source to the suitable relay. In the third duration, the signal to the corresponding users are transmitted using the selected relay [25]. In this case, the harvested energy at the suitable relay in the allocated time duration is obtained as [30]

$$E_s = \eta P_s \left|h_{R_n P}\right|^2 \delta T \tag{2}$$

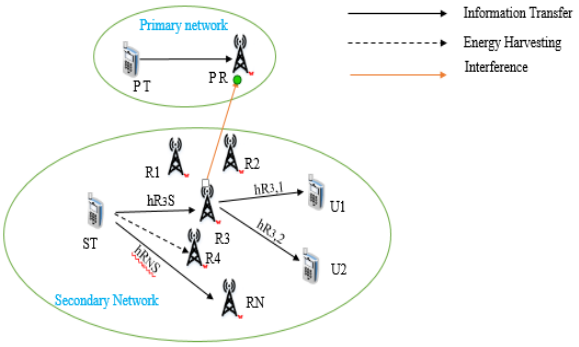


Fig.1 System Model

Where η is the energy conversion efficiency of the energy harvesting circuitry. Therefore, ${P_R}^H$ which is the maximum transmit power from the energy harvesting for the nth relay is given by

$${P_{R_n}}^H = \frac{E_s}{(1-\delta)\frac{T}{2}} \tag{3}$$

By assuming that $\alpha_1 < \alpha_2$ it is meant that more transmission power is allocated to U_2 while the channel coefficient of U_1 is stronger than U_2. Using the received signal via the selected relay, the signal-to-interference plus noise ratio (SINR) after considering x_1 as an interference is obtained as follows

$$\gamma_{R,2} = \frac{\alpha_2 P_s \left|h_{R_n S}\right|^2}{\alpha_1 P_s \left|h_{R_n P}\right|^2 + N_0(\varepsilon+1)} \tag{4}$$

And using imperfect SIC, the SINR after detection of x_2 is

$$\gamma_{R,1} = \frac{\alpha_1 P_s \left|h_{R_n S}\right|^2}{\alpha_2 P_s \left|g_{R_n S}\right|^2 + N_0(\varepsilon+1)} \tag{5}$$

Where $g_{RS} \sim CN(0, \xi\lambda_{R_n S})$ with $0 < \xi < 1$ where this metric indicates the residual interference level due to the imperfect SIC. In the second timeslot, the received signal at U_i $i = 1,2$ is obtained as

$$y_i = h_{R_n,i}\sqrt{P_{R_n}}(\sqrt{\alpha_1}x_1 + \sqrt{\alpha_2}x_2) + I_P + n_i \tag{6}$$

Where $h_{R_n,i}$ is the channel model between the suitable relay and ith user while x_i is the message of the ith user and n_i is the additive white Gaussian noise (AWGN) of the ith user. $I_P \sim CN(0, N_0\epsilon)$ is the interference created from the primary user communication on the users and the relay communications [19]. In this case, using SIC implementation in U_1 , x_2 detection and considering x_1 as a noise, the SINR is stated as

$$\gamma_{1,2} = \frac{\alpha_2 P_{R_n} \left|h_{R_n 1}\right|^2}{\alpha_1 P_{R_n} \left|h_{R_n 1}\right|^2 + N_0(\varepsilon+1)} \tag{7}$$

We also note SINR using imperfect SIC as follows

$$\gamma_1 = \frac{\alpha_1 P_{R_n} \left|h_{R1}\right|^2}{\alpha_2 P_{R_n} \left|g_{R_n 1}\right|^2 + N_0(\varepsilon+1)} \tag{8}$$

Where $g_{R_n 1}$ is defined similar to $g_{R_n S}$. SINR at U_2 is also obtained as

$$\gamma_2 = \frac{\alpha_2 P_{R_n} \left|h_{R_n 2}\right|^2}{\alpha_1 P_{R_n} \left|h_{R_n 2}\right|^2 + N_0(\varepsilon+1)} \tag{9}$$

In Raleigh fading channel, for obtaining the outage probability, cumulative distributed function (CDF) and the probability density function (PDF) of the wireless channel h with mean λ are defined as

$$F_h(x) = 1 - e^{-\frac{x}{\lambda}} \tag{10}$$

And

$$f_h(x) = \frac{1}{\lambda} e^{-\frac{x}{\lambda}} \tag{11}$$

As we know, the probability of outage is very important metric to evaluate the performance; Therefore, the outage probability with imperfect SIC for x_1 is formulated as follows

$$Ou\_P_1 = 1 - P(\gamma_{R_n,2} > \gamma_{2,th}, \gamma_{R_n,1} > \gamma_{1,th}, \gamma_{1,2} > \gamma_{1,th}, \gamma_1 > \gamma_{1,th}) \tag{12}$$

Where $\gamma_{i,th}$ $i = 1,2$ is the threshold corresponding to the target rate $R_{i,th}$ for two users. According to [25], we have

$$Ou\_P_1 = 1 - \mathrm{Z}_1 \times \mathrm{Z}_2 \tag{13}$$

Where Z_1 is expressed as follows

$$\mathrm{Z}_1 = \Upsilon_1 - \frac{\Upsilon_2 - \lambda_{R_n S}}{\Upsilon_3 \lambda_{PS} + \lambda_{R_n S}} \tag{14}$$

Where $\Upsilon_1 = \frac{\lambda_{R_n S}}{\Theta_1 \lambda_{PS} + \lambda_{R_n S}}$, $\Upsilon_2 = \frac{\zeta_P}{\zeta_P + 1}$ and $\Upsilon_3 = \frac{(\zeta_P + 1)\Theta - \Theta_1}{\zeta}$.

We also have [25]

$$\Theta_1 = \frac{\gamma_{1,th}(\epsilon+1)}{\rho_I \alpha_1}, \Theta_2 = \frac{\gamma_{2,th}(\epsilon+1)}{\rho_I \alpha_2}, \Theta = \max(\Theta_1, \Theta_2) \quad (15)$$

And

$$\zeta_P = \gamma_{1,th}\, \zeta \bar{\alpha} \ , \ \bar{\alpha} = \frac{\alpha_2}{\alpha_1} \quad (16)$$

Where $\rho_I = \frac{I_{th}}{N_0}$. Z_2 is also expressed as follows

$$\mathrm{Z}_2 = \mathrm{A}_1 + \mathrm{A}_2 \quad (17)$$

Where A_1 is stated as[22],[25]

$$\mathrm{A}_1 = \varrho_1 \Psi(\Theta \chi_1 + C) - \frac{\Upsilon_2 \lambda_1 \Psi(\Upsilon_3 \chi_1 + C)}{\Upsilon_3 \lambda_{PR} + \lambda_1} \quad (18)$$

And

$$\mathrm{A}_2 = \Psi(\Theta \chi_1) - \Psi(\Theta \chi_1 + C) - \Upsilon_2\, \Psi(\Upsilon_3 \chi_1) + \Upsilon_2\, \Psi(\Upsilon_3 \chi_1 + C) \quad (19)$$

Where $\chi_i = \frac{\lambda_{SP}}{\kappa \lambda_i \lambda_{R_n S}}$, $C = \frac{\lambda_{SP}}{\kappa \lambda_{PR_n} \lambda_{R_n S}}$, $\Psi(\mathrm{x}) = e^x(xE_1(-x) + e^{-x})$, $\varrho_i = \frac{\lambda_I}{\lambda_{PR}\Theta_i + \lambda_i}$ and $\kappa = \frac{2\eta\delta}{(1-\delta)}$. We also note the outage probability for x_2 which is calculated as follows [25]

$$Ou\_P_2 = 1 - P\big(\gamma_{R_n,2} > \gamma_{2,th}, \gamma_{R_n,1} > \gamma_{1,th}, \gamma_2 > \gamma_{2,th}\big) = 1 - \mathrm{Z}_1 \times \mathrm{Z}_3 \quad (20)$$

Where Z_3 is calculated as follows [22],[25]

$$\mathrm{Z}_3 = \varrho_2 \Psi(\Theta_2 \chi_2 + C) + \Psi(\Theta_2 \chi_2) - \Psi(\Theta_2 \chi_2 + C) \quad (21)$$

As shown in (13) and (20) formulas, important parameters which impress on the probability of outage implementation are SINR threshold, power allocation coefficients and the channel gain parameters. Therefore, for evaluation of the network performance, the overall throughput is expressed as follows [25]

$$T_{total} = \big(1 - Ou_{P_1}\big) R_{th_1} + \big(1 - Ou_{P_2}\big) R_{th_2} \quad (22)$$

Where R_{th_1} and R_{th_2} are the fixed target rates in delay-limited mode.

3- Problem Formulation and Its Solution

In this section, our goal is maximizing the network throughput while the constraints on the outage probability of the secondary users and interference created for the primary user communication are satisfied such that suitable relay is selected to transmit the secondary source messages to the NOMA users, its transmission power is adjusted and the optimal power allocation coefficients of the secondary users are obtained. Therefore, our proposed problem is formulated as follows

$$maximize_{R_n, P_{R_n}, \alpha_i}\, T_{total} \quad (23)$$

$$S.t. \ \ Ou_{P_i} \le \beta \ \ \forall i = 1,2 \quad (23\text{-}1)$$

$$PUinterf = P_{R_n} |h_{R_n P}|^2 \le I_{th} \quad (23\text{-}2)$$

$$\sum_{i=1}^{2} \alpha_i \le 1 \quad (23\text{-}3)$$

The first constraint (23-1) shows the constraint on the probability of outage of each user while (23-2) states the constraint on the interference which the primary user can tolerate due to the secondary network communications. (23-3) represents that the sum of the power allocation coefficients of the secondary users is equal to one. Exhaustive search algorithm is optimum solution for the problem in which all possible states of the answer is tested and the best answer which maximizes T_{total} and satisfies the constraints of the problem is selected as the optimal solution. However, due to the complexity of this method, we consider an iterative algorithm based on convex optimization to find the local solution for the problem. According to KKT conditions, Lagrangian function is given by [31]

$$L(\mu_i, \upsilon, \eta) = -T_{total} + \mu_i\big(Ou_{P_i} - \beta\big) + \upsilon(PUinterf - I_{th}) + \eta\big(\sum_{i=1}^{2} \alpha_i - 1\big) \quad (24)$$

Where μ_i, υ and η are the Lagrangian multipliers which have non-negative values. In fact, by applying Lagrangian function, the problem is converted to an unconstraint problem. On the other hand, for minimizing $L(\mu_i, \upsilon, \eta)$ and maintaining the problem constraints, the optimal value of the Lagrangian multipliers should be determined. In this case, we propose an iterative algorithm with low complexity to obtain the optimal values of the multipliers, optimal relay, its transmission power and power allocation coefficients of the secondary users. For this purpose, we use the ellipsoid method to solve convex functions. In fact, by applying this method, the optimal solution for the problem is obtained in finite iterations which is polynomial in the

input size. The parameters are updated in $i+1$ th iteration as

$$A_{i+1} = \frac{n^2}{n^2-1}\left(A_i - \frac{2}{n+1} A_i \tilde{g}_i \tilde{g}_i{}^T A_i\right) \quad (25)$$

And

$$x_{i+1} = x_i - \frac{1}{n+1} A_i \tilde{g}_i \quad (26)$$

Where $\tilde{g}_i = \frac{g_i}{\sqrt{g_i{}^T A_i g_i}}$ and g_i is the subgradient of $L(\mu_i, \upsilon, \eta)$ at the ellipsoid center x_i. The ellipsoid is halved in each iteration and one ellipsoid half is removed based on A_i. n is the unknown parameters' number [32]. Hence, the ellipsoid method can be candidate for multi-dimensional search methods.

4- Proposed Algorithm for Problem Solution

For solving the problem in (23), we consider an iterative algorithm. The proposed algorithm consists of the following steps in each iteration

- For each relay, the probability of outage for each user according to (13) and (20), the interference created by the secondary network to the primary user communication and therefore, the overall throughput are calculated.
- Lagrangian multipliers, $\alpha_i, i = 1,2$ and also transmission power of each relay(P_{R_n}) are updated using the ellipsoid method in (25) and (26).
- According to the previous step, the new values of T_{total}, probability of outage for each user and $PUinterf$ are calculated.
- The proposed algorithm terminates if the number of iterations reaches to the certain value or the convergence value of the algorithm is satisfied, Otherwise the algorithms goes to the first step and the algorithm is repeated again. We note that the result of increasing the number of iterations is more accuracy of the iterative algorithm.
- After stopping the algorithm, the relay which leads to more T_{total}, less probability of outage for each user and less interference for the primary user communication, is selected as the best relay. Pseudo code for our proposed algorithm which is named Power Allocation Coefficient Adjustment and Relay Selection (PACARS) is presented in Fig.2.

PACARS Algorithm

iter =500;
Initialization:
$\mu_i \epsilon [\mu_{i_{min}}, \mu_{i_{max}}]$
$\upsilon \epsilon [\upsilon_{min}, \upsilon_{max}]$
$\eta \epsilon [\eta_{min}, \eta_{max}]$
$\alpha_i \epsilon [0,1]$
ξ is the small number
it = 1 %%number of iterations
While(($|\upsilon^{t+1} - \upsilon^t| > \xi$)|| (it < iter))
Calculate T_{total}, Ou_P for each user and $PUinterf$ for the primary user
Update μ_i, υ, $\eta$and α_i multipliers by applying the ellipsoid method
Recalculate T_{total} , Ou_P for each user and $PUinterf$ for the primary user.
it = it + 1
End While
According to T_{total} and constraints of the problem, the best relay is selected

Fig.2. Pseudo Code for the Proposed Algorithm

5- Results and Discussion

We utilize MATLAB software for simulation. We consider a square field with the length of 500 m in which the secondary users, secondary base station, primary user and relays are distributed randomly. Number of relays is set to 5. Rayleigh fading channel is assumed as the channel model which is presented as follows [33], [34]

$$h = 10^{\frac{-L}{20}}.\mathrm{g} \quad (27)$$

Where g is considered as a Gaussian random process with zero mean and unit variance for Raleigh fast fading. L states the path loss according to the free- space path loss (FPL) model . Another part is a real Gaussian random variable with zero mean and standard deviation 3 for large scale log-normal shadowing. Therefore, we have [35]

$$L = 20\log\left(\frac{\mathrm{d}4\pi f_c}{c}\right) + n \quad (28)$$

Where f_c is the carrier frequency, d states the distance between two corresponding users while c is the speed light. Simulation results are evaluated by averaging over 1000 independent simulation runs. The other required parameters are stated in Table 2.

Table 2. The Value of the Simulation Parameters

Parameter	Value
R_{th_1}, R_{th_2}	0.5 BPCU
$\lambda_{SP}, \lambda_{PR_n}$	0.1
$\lambda_{SR_n}, \lambda_2$	1
λ_1	2
ζ	0.01
δ	0.1
η	0.9
ρ_I	0.5

To compare the results of the proposed algorithm, we propose other algorithms as the bench mark algorithms as follows

- Fixed Transmission Power of the Relays Algorithm: This algorithms is proposed to show the effectiveness of the selected relay transmission power in the network performance such as overall throughput, probability of outage of each user and interference created on the primary user communication.
- Random Relay Selection Algorithm: This algorithm is considered to show that the proper selection of the relay has an important role in improvement on the problem metrics in (23). This algorithm is selected due to its low complexity in implementation.
- Fixed Power Allocation Coefficients Algorithm: This algorithm is selected to show NOMA technology effectiveness, in improving the overall throughput, probability of outage of each user and interference created on the primary user communication.

Fig.3 shows the overall throughput versus different values of η. As we know, η is the energy conversion efficiency of the energy harvesting circuitry. Clearly, the proposed algorithm duo the proper selection the relay, setting its transmission power and power allocation coefficients of the secondary users, has the maximum value of this metric. However, the proposed algorithm with random relay selection has the minimum value. This algorithm presents the importance of the suitable relay selection for improving the network performance.

Fig.4 illustrates the outage probability versus different values of η. We note that all of the algorithms satisfy the constraint on the outage probability. However, the algorithm with the fixed power allocation coefficients for the users has the maximum value of this metric. In fact, this issue shows the importance of NOMA technology utilization in the performance improvement of the network.

Fig.5 presents the overall throughput for different values of ρ_I. Clearly by increasing ρ_I, the overall throughput is decreased due to the increasing the interference. Proposed algorithm with the power allocation factors setting has the maximum value of this parameter while the random relay selection algorithm has the minimum value. This shows the importance of the suitable relay selection in improving the performance of the network.

According to Fig.6, all algorithms satisfy the probability of outage constraint; however, the algorithm with fixed α, has the worst value of the outage probability. On the other words, NOMA technology has an important role for improving this metric.

Fig. 7 presents the overall throughput of the network for different values of δ. The algorithm with random relay selection has the worst value of this parameter. In fact, this figure shows the effect of the suitable relay selection in improving the throughput of the network. By increasing δ, the relays harvest more energy, therefore the selected relay has more transmission power. In this case, the overall throughput of the network also increases.

Fig.8 presents the outage probability for different values of δ. In fact, δ exhibits the balancing between the energy harvesting and information processing. Increasing δ leads to more time for energy harvesting. According to this figure, the algorithm with fixed α has more probability of outage since NOMA technology is not used in their network.

Fig.9 plots the overall throughput of the network for different values of ζ. In fact, ζ is the residual interference level due to the imperfect SIC. Therefore, by increasing ζ, the overall throughput is decreased. On the other hand, the highest value of the overall throughput is obtained in lowest value of ζ.

Fig.10 presents the convergence analysis for the proposed algorithm to find the optimal value of the Lagrangian parameter versus different iterations. In fact, this figure presents the steps of reaching the optimal values of the Lagrangian parameters. In figure, the convergence is evaluated according to overall network throughput for the steps that reach the optimal value of the Lagrangian parameters. In the 9th iteration, the optimal value of the Lagrangian parameter is obtained.

6- Analysis of Results

As it is clear in the previous section, the goal of the problem is maximizing the network throughput by selecting the suitable relay, setting its transmission power and allocating power coefficients of the secondary users while the outage probability and the interference created for the primary user communication are improved. Fig.3, Fig.5 , Fig.7 and Fig.9 illustrate the overall throughput enhancement in

comparison to the bench marked algorithms by varying the energy conversion efficiency of the energy harvesting circuitry(η), interference effects(ρ_I) , balancing between the energy harvesting and information processing(δ) and the residual interference level due to the imperfect SIC(ζ) parameters. In similar way, in Fig.4, Fig.6 and Fig.8, the proposed algorithm decreases the outage probability and improves this network metric. Fig.10 presents convergence analysis of the proposed algorithm to find the optimal value of the Lagrangian parameter in ellipsoid method. This figure states the iteration in which the optimal values of the Lagrangian parameters are obtained.

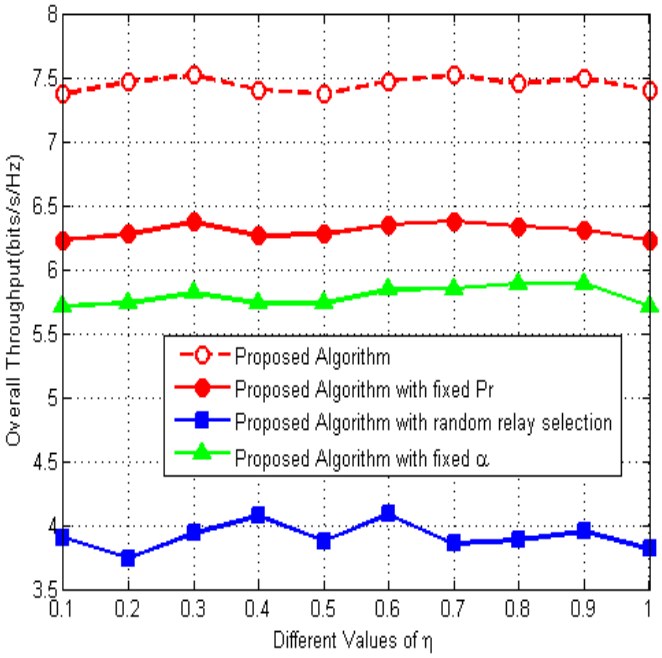


Fig.3. Overall Throughput Versus Different Values of η

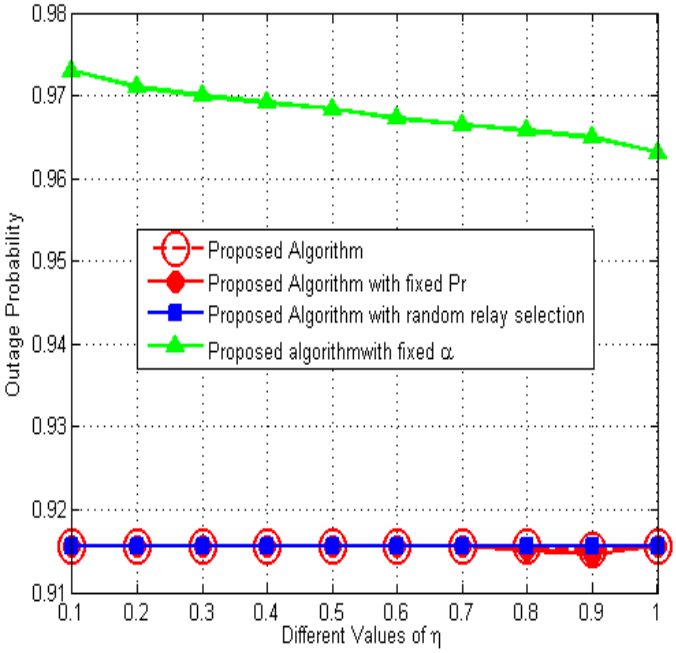


Fig.4. Outage Probability for Different Values of η

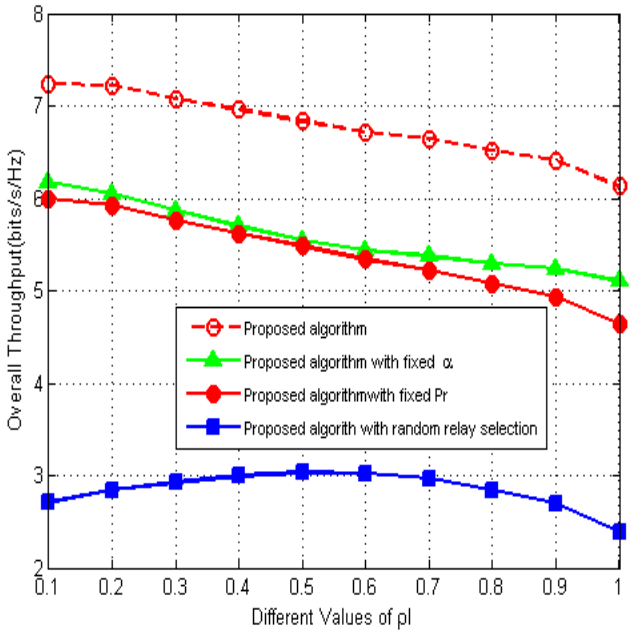


Fig.5. Overall Throughput Versus Different Values of ρ_I

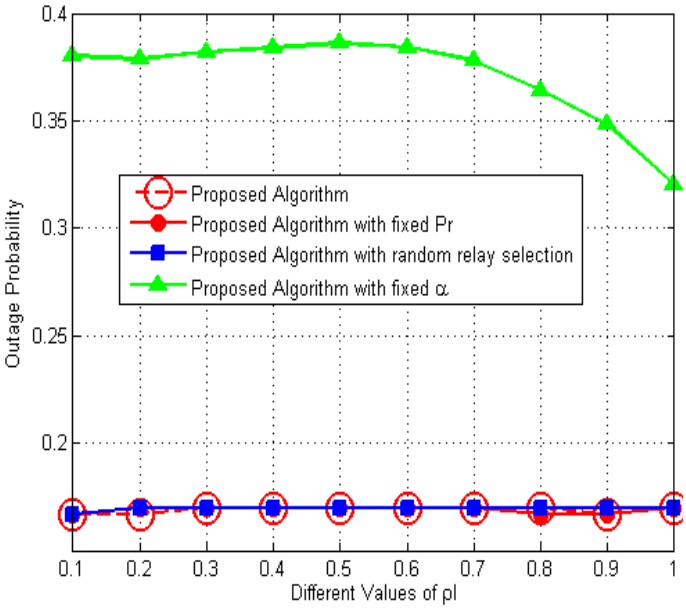


Fig.6. Outage Probability for Different Values of ρ_I

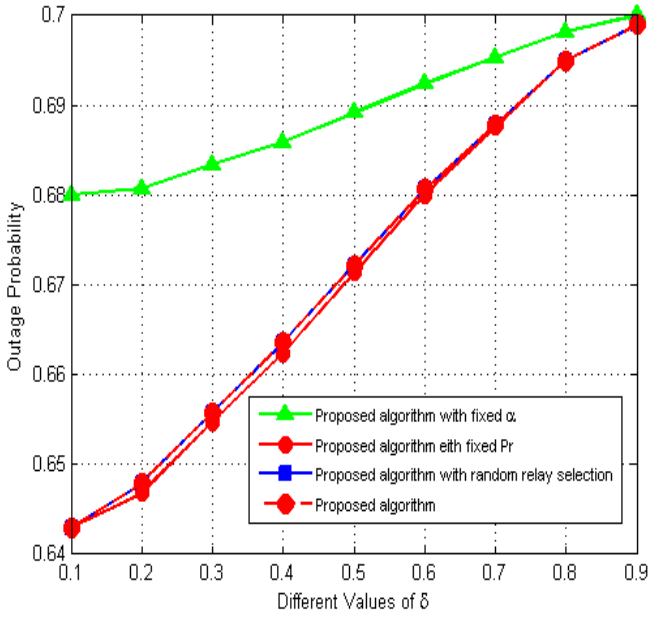


Fig.8. Outage Probability Versus Different Values of δ

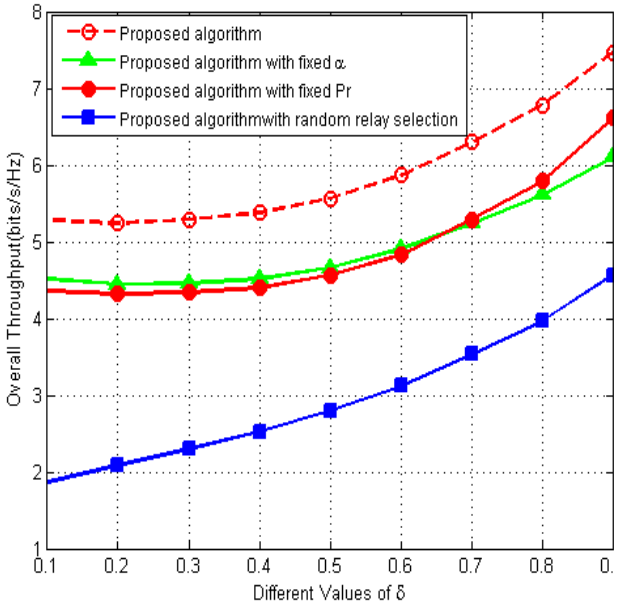


Fig.7. Overall Throughput Versus Different Values of δ

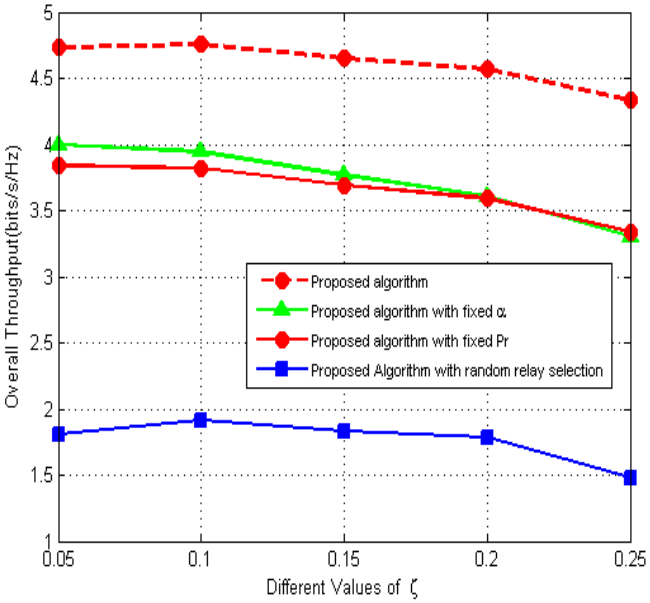


Fig.9. Overall Throughput Versus Different Values of ζ

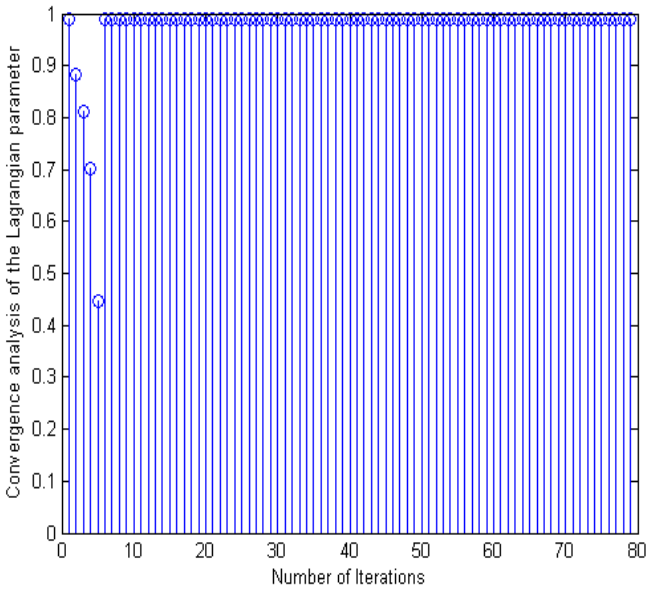


Fig.10. Convergence Analysis of the Lagrangian Parameter Versus Different Iterations

7- Conclusions

In this work, performance of a cooperative CR-relay based NOMA network is investigated in term of the throughput, outage probability and interference tolerated by primary user in Rayleigh fading channels. The problem of maximizing the network throughput is proposed to select the proper relay with the energy harvesting capability, set the transmission power of the selected relay and optimize the power allocation coefficients to each user with constraints on the outage probability and the interference created for the primary user communication. The problem is solved based on convex optimization method and KKT conditions. Numerical results validate the efficiency of the proposed iterative algorithm in comparison to the bench mark algorithms for different values of energy conversion efficiency of the energy harvesting circuitry (η) , interference effects (ρ_I) , balancing between the energy harvesting and information processing (δ) and the residual interference level due to the imperfect SIC(ζ). The problem investigation for Nakagami-m fading channel and multiple users can be considered for the future work of this paper.

References

[1] S. M. R. Islam, N. Avazov, O. A. Dobre and K. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and Challenges," IEEE Communications Surveys & Tutorials, Vol.9, No.2,2017,pp. 721-742.

[2] S. Zhang, B. Di, L. Song, and Y. Li, "Radio resource allocation for nonorthogonal multiple access (NOMA) relay network using matching game, " IEEE Int. Conf. Commun. (IEEE ICC), Kuala Lumpur, Malaysia, 2016, pp. 1-6.

[3] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System level performance evaluation of downlink non-orthogonal multiple access (NOMA), " IEEE Annu. Symp. Pers. Indoor Mobile Radio Commun. (IEEEPIMRC), Japan,2015.

[4] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information , " IEEE Trans. Commun., Vol.64,No.2,2016, pp.654-667.

[5] T. Do, DB. de Costa, TQ. Doung, B. An B, "Improving the performance of cell-edge users in NOMA systems using cooperative relaying," IEEE Trans. Commun., Vol.66, No.5,2018, pp. 1883–1901.

[6] Z. Ding, M. Peng and H. V. Poor, "Cooperative Non-Orthogonal Multiple Access in 5G Systems, " IEEE Commun. Lett., Vol.19,No.8,2015, pp. 1462- 1465.

[7] M. Ghamari Adian, "A novel resource allocation algorithm for heterogeneous cooperative cognitive radio networks, " Journal of Information Systems and Telecommunication (JIST) ,Vol.5, No.2, 2017, pp.138-145.

[8] M. Ghamari Adian, " Joint relay selection and power allocation in MIMO cooperative cognitive radio networks, " Journal of Information Systems and Telecommunication(JIST),Vol.3, No.1,2015, pp.29-40.

[9] Z.Doorbash, A. Jamshidi, G. Javidi and A. Sheybani , "Cooperative NOMA in cognitive radio networks: A study on imperfevt CSI, SIC and hardware imparements over Nakagami-m- fading channel, " Physical Commun. Vol.64, 2024.

[10] Q. Nhat Le, D.-Th. Do, B. An, "Secure wireless powered relaying networks: Energy harvesting policies and performance analysis, " International Journal of Commun. Sys., Vol.30, No.18,2017, pp. 1936 – 1947.

[11] H. Bany Salameh, Sh. Abdel-Razeq and H. l-Obiedollah, " Integration of cognitive radio technology in NOMA-based 5BG networks: State of art, challenges and enabling technologies, "IEEE Access, Vol.11,2023, pp. 12949 – 12962.

[12] F. Zhou, Z. Li, N. C. Norman, J. Cheng, and Y.Wang, "Resource allocation in wideband cognitive radio with SWIPT: Max-min fairness guarantees, " Proc. IEEE GLOBECOM, USA, 2016.

[13] H. Zhang, S. Huang, C. Jiang, K. Long, V.C.M. Leung, H. V. Poor "Energy efficient user association and power allocation in millimeter wave- based ultra dense networks with energy harvesting base stations, " IEEE J. Sel. Areas Commun., Vol.35, No.9,2017, pp. 1936–1947.

[14] Y. Chen, N. Zhao, and M.-S. Alouini, "Wireless energy harvesting using signals from multiple fading channels, " IEEE Trans. Commun., Vo.65,No.11, 2017,pp. 5027–5039.

[15] S.H. Mostafavi-Amjad , V. Solouk and H. Kalbkhani , "Energy-efficient user pairing and power allocation for granted uplink-NOMA in UAV communication systems, " Journal of Information Systems and Telecommunication (JIST) , Vol.10, No. 4, 2022, pp.312-323.

[16] S. Arzykulov, G. Nauryzbayev, T. A. Tsiftsis and B. Maham, "Performance analysis of underlay cognitive radio

nonorthogonal multiple access networks, " IEEE Trans. on Vehi. Tech., Vol.68, No.9, 2019,pp.9318-9322.

[17] L. Bariah, S. Muhaidat and A. Al-Dweik, "Error performance of NOMA based cognitive radio networks with partial relay selection and interferencep constraints, " IEEE Trans. on Communications, Vol.68, No.2,2020, pp.765-777.

[18] Y. Zhang, and J. Ge. "Impact analysis for user pairing on NOMA based energy harvesting relaying networks with imperfect CSI, " IET Commun., Vol. 12, No. 13, 2018, pp. 1609-1614.

[19] S. Arzykulov, T. A. Tsiftsis, G. Nauryzbayev and M. Abdallah, "Outage Performance of Cooperative Underlay CR-NOMA With Imperfect CSI, " IEEE Commun. Letters, Vol.23, No.1, 2019,pp. 176 – 179.

[20] G. Im and Jae Hong Lee, "Outage probability for cooperative NOMA systems with imperfect SIC in cognitive radio networks, " IEEE Commun. Letters, Vol.23,No.4,2019,pp. 692 – 695.

[21] D. Wang and S. Men, "Secure energy efficiency for NOMA based cognitive radio networks with nonlinear energy harvesting," IEEE Access, Vol. 6, 2018,pp. 62707 – 62716.

[22] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, R.Q.Hu, "Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks, " IEEE Trans. Commun., Vol.67, No.1,2019, pp. 83-96.

[23] W. Liang, K. D.Wang, J. Shi , L. Li and G. K. Karagiannidis, "Distributed sequential coalition formation algorithm for spectrum allocation in underlay cognitive radio networks, "IEEE Access, Vol.7, 2019,pp.56803 – 56816.

[24] G. Nauryzbayev, S. Arzykulov, T. A. Tsiftsis and M. Abdallah, "Performance of cooperative underlay CR-NOMA networks over nakagami-m channels, " IEEE International Conference on Communications Work-shops (ICC Workshops), USA, 2018,pp.1-6.

[25] D. THUAN Do, A. Tu Le and B. Moo Lee, "NOMA in cooperative underlay cognitive radio networks under imperfect SIC, " IEEE Access, Vol.8, 2020, pp. 86180 – 86195.

[26] P. Gosh, S. Dhar Roy and S.Kundu, "Outage of cooperative NOMA with an energy harvesting relay in an underlay cognitive radio network, "International journal of Commun. Sys., Vol.37, No.8, 2024.

[27] X. Li, X.Gao, Sh. Ahmed Shaikh, M. Zeng, G. Huang, N. Muhammad Faseeh Qureshi and D. Qiao, " NOMA-based cogtive radio network with hybrid FD/HD rlay in industry 5.0, "Journal of King Saud University- Comp. and Infor. Sciences, Vol.35, No.6, 2023.

[28] D. Samanta, Ch. Kumar De and A. Chandra , "Performance analysis of NOMA based hybrid cognitive radio network assist by full- duplex relay, " Telecommun. Sys. Journal, Vol.88, No.37, 2025.

[29] S. Arzykulov, G. Nauryzbayev and T. A. Tsiftsis, "Underlay Cognitive Relaying System Over α - μ Fading Channels, " IEEE Commun. Lett., Vol.21,No.1, 2017,pp 216–219.

[30] Dinh-Thuan Do, H.-S. Nguyen, "A tractable approach to analyze the energy-aware two-way relaying networks in presence of co-channel interference, " EURASIP Journal on Wirel. Commun. and Netw., 2016.

[31] S. Boyd, L. Vandenberghe Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[32] W. Yu, R. Lui , "Dual methods for nonconvex spectrum optimization of multicarrier systems, " IEEE Trans. Commun, Vol.54,No.7,2006, pp. 1310-1322.

[33] B. Sklar, "Rayleigh fading channels in mobile digital communication systems part1: Characterization, " IEEE Commun. Mag., Vo.35,No.9, 1997,pp.136-146.

[34] Y. Ma, D. I. Kim, Zh. Wu, "Optimization of ofdma-based cellular cognitive radio networks, " IEEE Trans. on Commun., Vol.58, No.8, 2010,pp.2265 - 2276 .

[35] M.Najimi, A.Ebrahimzadeh, S.M.Hosseini Andargoli and A. Fallahi, " A novel sensing nodes and decision node selection method for energy efficiency of cooperative sepectrum sensing in cognitive sensor networks, " IEEE Sens. Jour., Vol.13, No.5, 2013,pp. 1610-1621.

Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 12-23
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Numerical Study of a Switchable Polarization for Reflect-array Unit-cell for Satellite Communications

Mohammad Mansourinia[1*], Ramezan Ali Sadeghzadeh[1]

[1].Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran

Received: 02 Apr 2024/ Revised: 24 Feb 2024/ Accepted: 17 Mar 2025

Abstract
The purpose of this paper is to design and simulate a unit cell that is wideband and multi-polarized for a reflect-array antenna. Bandwidth of structure is greater than 70% of X and Ku bands for satellite applications that reached from two printed dipoles and asymmetric arrow head shape in structure for multi electric and magnetic resonances and used thicker substrate for enhancement of BW by stack up of substrate with different layers. Depending on the antenna usage, the proposed structure can provide dual or triple polarization switching through the use of one or two control bits. Among the innovations of this structure compared to other activities, it can be said that the switching capability to support multiple polarizations occurs in a common wide bandwidth, or in other words, each of the switching modes is not in different single frequency or a bandwidth of frequencies. Comparing the switching modes of the proposed design with other existing control structures, the feature of maintaining the polarization of the feeding antenna or converting it to orthogonal polarization in different bits distinguishes the proposed structure. The proposed design has a new geometrical structure and considering that it can have the main polarization of the feeding antenna, its orthogonal polarization and even circular polarization in any switching mode, it has a relatively simple geometry, which reduces the complexity of the construction mechanism.

Keywords: Reflect-Array; Wideband unit Cell; Multi-Polarized unit Cell; Configurable Structure.

1- Introduction

When it comes to array antennas, one of the most common array structures are phased array antennas whose most important application is to rotate the radiation pattern electrically. In phased array antennas, the technique of rotating the main beam of the radiation pattern creates a suitable phase difference between the elements of the array. Reflect-array antennas were suggested by some researchers to be a combination of phased array antennas and plate reflector antennas, but in new studies, the reflect-array is defined by the properties of the unit cell. In modern commercial applications, subscribers expect better quality and speed for telecommunication services, such as video calls and internet, so wide bandwidth and maximum utilization are necessary.

The capability of sending and receiving multiple polarizations of waves is a significant feature of antennas. If the reflect-array antenna has a unit cell that is capable of supporting multiple polarizations, a simple single-polarization feed antenna can receive any wave that has an unexpected change in polarization along its propagation path. The structures investigated in Refs. [1] - [6] can achieve a wide bandwidth in the X or Ku bands; their methods include increasing the dielectric thickness, using multiple resonance elements, layering the structure and so on. For example, in [1], the bandwidth increased by using multiple resonance elements, which were printed dipoles. However, increasing the number of resonators made the structure look like a high-pass filter for rotating the incident wave polarization. The broadband characteristic was achieved in [3] by combining the use of a multi-resonant element and a slotted rectangular patch element. Reference [4] investigated a novel bandwidth improvement method, which combined the multilayer approach with the sub wavelength element technique. A taper resonator and a thick substrate were utilized for the design and construction of an ultra-wideband polarization conversion meta-surface, which was made using a double-head arrow structure [6].

✉ **Mohammad Mansourinia**
m.mansorinia@email.kntu.ac.ir

Wave polarization conversion may occur unintentionally due to scattering or reflection from objects on the wave propagation path, so the antenna should support all types of polarizations, especially circular polarization, to receive the wave. The designs in Refs. [6] - [10] were proposed particularly for the conversion of polarization types. In [6], an ultra-wideband linear polarization rotator was designed by combining two typical symmetry-broken structures, i.e., oblique V-shaped and cut-wire resonators, which were capable of rotating a linear polarization to orthogonal one. In [7] coupled split ring resonators (SRRs) functioning as meta-atoms or unit cells comprise two concentric rings. Each of the rings has a slit positioned at the corner and rotated by 180° with respect to the other ring. The polarization transforming capability is stable for wide oblique incidence angles up to 60° for both transverse-electric and transverse-magnetic polarizations. Moreover, this capability acts as a meta-mirror, which preserves handiness of the circular polarization upon reflection. The structure in [9] consists of a square with two curves on the top right and lower left corners and a square SRR responsible for linear-to-linear and linear-to-circular polarization conversions in two frequency bands. A single layer mirror-symmetric anisotropic meta-surface is proposed in [10] using a novel unit cell having fish-like structure. The polarization conversion of the fish-like structure is achieved by different geometries along the x and y axes, as a result of different phase responses along the two orthogonal axes.

In this article, the proposed structure has reached a wide bandwidth in the X and Ku bands from the combination of multi frequency resonators that include two printed dipoles and asymmetric arrow head along with increasing the thickness of the substrate. The proposed simple structure can support multiple polarizations in ultra wide bandwidth compared to the other unit cells. The multiple polarizations are achieved by changing the impedance in a part of the structure, so it is adjustable. Maintaining feed antenna polarization, converting linear to orthogonal polarization and linear to circular polarization conversion in a simple structure distinguishes it from the other investigated unit cells. In addition, the ability to support multiple polarizations occurs in a same bandwidth. Another advantages of this structure is that the number of control bits can be reduced according to the application. In other words, if the types of conversion polarization are limited, the structure can be controlled with fewer control bits. In the following, we have theory, design, simulation, performance analysis sections. In the theory section, the concept of microstrip reflect array and polarization and its conversion and the introduction of important parameters of polarization converter structures are explained, in the next section, we will focus on the design and simulation and how it works and solve the challenges of its construction with alternative designs.

2- Theory

2-1- Microstrip Reflect-Array Structures

The first subject that needs to be mentioned is whether the microstrip reflect-array can be a suitable alternative to parabolic reflectors, which is supposed to work specifically on the design of a unit cell with specific characteristics for the reflect-array? To compare these two types of reflectors, the first one is the ability of the structure to focus and reflect the reflected wave when the feed antenna is not in front. As can be seen from the fig. 1, for the parabolic reflector, the reflected field is non-resonant, and due to the curvature of the geometry of the structure, the reflection of the waves will be in the direction in front of the reflector, while in the microstrip reflection array, there are two types of reflected fields: resonant and non-resonant fields. The noteworthy point is that such structures reflect the non-resonant field structure in the opposite direction of the incident wave but with the same incident angle due to the substrate space and the flatness of the ground plane. Resonant fields that are caused by the layer of resonant elements, despite being flat, naturally radiate in the direction perpendicular to the normal vector of the structure plane, so the resonant fields are reflected in the direction in front of the reflector likes parabolic reflectors [11].

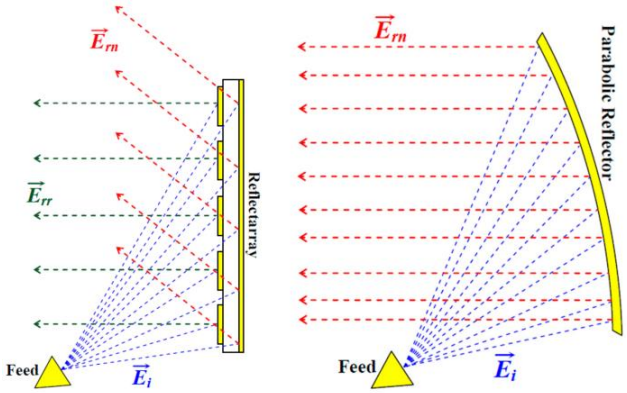


Fig. 1 Reflection of the Incident Signals from the Surface of the Reflect-Array and Parabolic Reflector [11]

Another important point is the incident and reflection phase of the wave in the reflect-array antenna. In parabolic reflector antennas, according to the geometry of the structure, if the feeding antenna is in front of the reflector, the phase difference caused by different locations of the reflector structure is geometrically compensated to a great extent, but this case for the reflect-array that has a flat geometry cannot be compensated in this way but several techniques have been proposed for microstrip reflect-array structures that solve this problem. One method is to use microstrip patches of the same size with stubs of variable length to control the reflection phase but a better approach is to use patches of variable size

to control the phase. The concept of using variable size rectangular patch elements to vary the reflection phase can be extended to other types of elements, such as circular patches, annular ring elements, and crossed dipole elements. These elements will respond to both vertical and horizontal polarizations, which is an advantage for dual linear or circularly polarized antennas. Another method is to use multiple layers of the structure in such a way that the phase compensating elements are placed in another layer compared to the layer containing resonance elements. Finally, it should be said that with such methods, the incident phase can be compensated in different feeding locations and also the reflected phase can be controlled, and this issue should be taken into account if the proposed unit cell were to be designed as an array [12].

2-2- Wave Polarization

The theory behind the subject needs to be explained first. In this section, it is necessary to define the polarization of the propagation wave that will be supposed the desired unit cell of the reflect-array has capable of conversion polarization. The property of an electromagnetic wave that identifies the time-varying direction and relative magnitude of the electric field vector is what defines polarization of a radiated wave [13]. In order to increase the conceptualization of this sentence, we must focus on an example to continue the explanation. If the relationship between the electric field of an arbitrary wave at the time and the phase domain from [14] is as follows:

$$\overrightarrow{E(z)} = \overrightarrow{a_x}E_1(z) + \overrightarrow{a_y}E_2(z) = \overrightarrow{a_x}E_{x0}e^{-jkz} + \overrightarrow{a_y}E_{y0}e^{-jkz}e^{j\varphi} \quad (1)$$

$$\overrightarrow{e(z,t)} = \overrightarrow{a_x}E_{x0}\,cos(\omega t - kz) + \overrightarrow{a_y}E_{y0}\,cos(\omega t - kz + \varphi) \quad (2)$$

By knowing the relationship between the time domain of the electric field, it is possible to plot the pattern of polarization of the electric field of the wave, or in better words, its type of polarization will be achieved. First step, in relation to the time domain of the electric field, a fixed plane in the direction of propagation should be considered, which is usually considered to be the z = 0 plane for simplicity, so the above relation is simplified as follows:

$$z = 0 \rightarrow \overrightarrow{e(t)} = \overrightarrow{a_x}E_{x0}\,cos(\omega t) + \overrightarrow{a_y}E_{y0}\,cos(\omega t + \varphi) \quad (3)$$

We are now required to examine the field's relationship during a time cycle and then connect the ends of the electric field vector at various times in the right-handed Coordinate axis system. As it can be seen from the relation (3) obtained, the parameters E_{x0},E_{y0} show the amplitude of the electric field components and the parameter φ which represents the phase difference between the two components of the electric field. The difference in the kind of wave's polarization originates from the different values of these parameters. So the question arises as to what kind of problem the polarization difference between the waves create which can be answered that the difference in polarization of the fields will directly affect the amplitude of the field received by the receiving antenna which has a different polarization compared to the transmitting antenna, so in the communication links, it is necessary to use co-polarization antennas or suitable structures that convert polarization with maximum efficiency.

2-3- Kind of Polarization Conversion

The wave amplitude and phase parameters determine the polarization of the wave. In general, the types of polarization are divided into linear, elliptical and circular polarization. Linear polarization is formed when there is no phase difference between the components of the electric field, and the type of linear polarization is different for different conditions between the amplitude of the components. For example, in equation (3) if E_{y0}=0, the linear polarization will be horizontal and if E_{x0}=0, it will be vertical. Another condition of linear polarization is oblique when $E_{x0}\neq0$,$E_{y0}\neq0$ will be reached. Circular polarization is formed when their amplitude is the same, the phase difference between the components is 90 degrees. Also, for elliptical polarization, a phase difference of 90 degrees between the components is necessary, with the difference that the amplitude of the components will be unequal.

By knowing the important parameters in determining the polarization, the type of polarization can be easily recognized. Now are going to discuss about conversion of polarization into each other. Polarization conversion is usually done with the help of elements that transmit or reflect electromagnetic waves with a specific polarization that are radiated to them with another type of polarization. Considering that our research in this article is based on reflector structures, parameters should be defined for polarization conversion, which are obtained from the parameters extracted from the simulation or measurement of reflector structures. In reflector structures, the reflection coefficient is the most important parameter that can be reported.

To show the degree of polarization change, reflection coefficient can be used in such a way that is checked separately for two specific types of polarization. For example, the reflection coefficient can be defined as, in the first case, Co-polarization reflection coefficient is the ratio of the reflected wave with horizontal polarization to the incident wave with horizontal polarization (R_{xx}), and in the next case, Cross-polarization reflection coefficient is the ratio of the reflected wave with the polarization Vertical to the incident wave with horizontal polarization (R_{yx}). Therefore, for polarization conversion, the parameter of polarization conversion ratio (PCR) and polarization maintenance ratio (PMR) are defined from [7] with the help of reflection coefficients concept as follows:

$$PCR = \frac{|R_{yx}|^2}{|R_{yx}|^2 + |R_{xx}|^2} \quad (4)$$

$$PMR = \frac{|R_{xx}|^2}{|R_{yx}|^2 + |R_{xx}|^2} \quad (5)$$

The axis ratio is another important parameter that actually shows the degree of circular polarization, and this parameter is reported in the research because of investigate circular polarization. When we change the polarization from a horizontal or vertical linear state to a 45 degree inclined linear polarization or to a circular polarization, we go to the axis ratio to distinguish between the two states, because the reflection coefficients alone do not show the difference between the said two states. According to the contents of the polarization theory section, the amplitude of both components is equal, but the phase difference between the components determines whether it is linear at 45 degrees or circular, and both amplitude parameters and phase difference exist in relation to the ratio of the axes taken from [8]. The axial ratio (AR) relation is given by:

$$AR = \left\{ \frac{|R_{xx}|^2 + |R_{yx}|^2 + \left(|R_{xx}|^4 + |R_{yx}|^4 + 2|R_{xx}|^2|R_{yx}|^2\cos(2\Delta\varphi)\right)^{\frac{1}{2}}}{|R_{xx}|^2 + |R_{yx}|^2 - \left(|R_{xx}|^4 + |R_{yx}|^4 + 2|R_{xx}|^2|R_{yx}|^2\cos(2\Delta\varphi)\right)^{\frac{1}{2}}} \right\}^{\frac{1}{2}} \quad (6)$$

$\Delta\varphi$ refers to phase difference between co- and cross-polarized reflection coefficients. If this ratio is below 3 dB on the logarithmic scale or below 1.41 on the linear scale, the polarization can be considered circular and above it elliptical or linear.

3- Design and Simulation

In the structure design section, the subjects such as geometry of the structure, converting polarizations, widening the bandwidth with a high percentage polarization conversion energy, controlling multiple polarization states, and the effects of the design parameters are investigated. The proposed structure is simulated in the CST software. Including the unit cell boundaries and Floquet port, the final dimensions of the unit cell are $5.5\ mm \times 5.5\ mm \times 3\ mm$, with the substrate consisting of two layers of RO4003 and one layer of PTFE.

3-1- Analysis of Structure Geometry

Fig. 2 shows the proposed structure that the main resonances elements can be placed at different angles to the coordinate system, but what angle can create the optimal and suitable state for polarization conversion? In general, α determines the degree of polarization conversion with horizontal or vertical polarization of the incident wave. According to the determination of this angle, the reflection components of the wave are affected and change the amount of conversion. For example, if we are looking for a linear conversion of the polarization of the structure, the created dominant surface current should be perpendicular to the incident wave component.

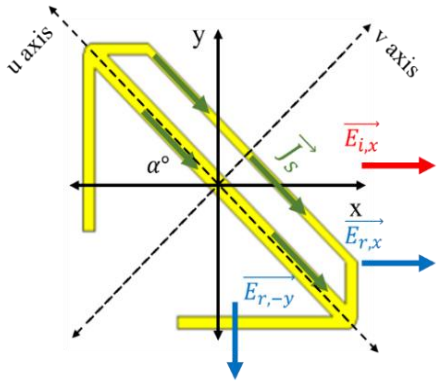


Fig. 2 Placement of Proposed Geometry in Unit Cell

For the fig. 2 that shows the placement of a resonant element such as a printed dipole with an arbitrary angle $0<\alpha<90$, if it is assumed that the incident field emitted in the z direction has a horizontal polarization, according to the previous sections, the electric field from the relation (2) with the assumption $\varphi = 0, E_{y0}=0$ can be rewritten as follows:

$$\vec{e}_i = \overrightarrow{a_x} E_{ix0} \cos(\omega t - kz) \quad (7)$$

According to the boundary conditions, a surface current will be created on the surface of the structure, which can be extracted according to the electromagnetic relations. In general, according to the geometry of the surface current structure, surface current will have both x and y components:

$$\vec{J_s} = \overrightarrow{a_x} J_{sx} \cos(\omega t + kz) + \overrightarrow{a_y} J_{sy} \cos(\omega t + kz + \varphi_j) \quad (8)$$

Also, we have the following relationship between electric field and surface current:

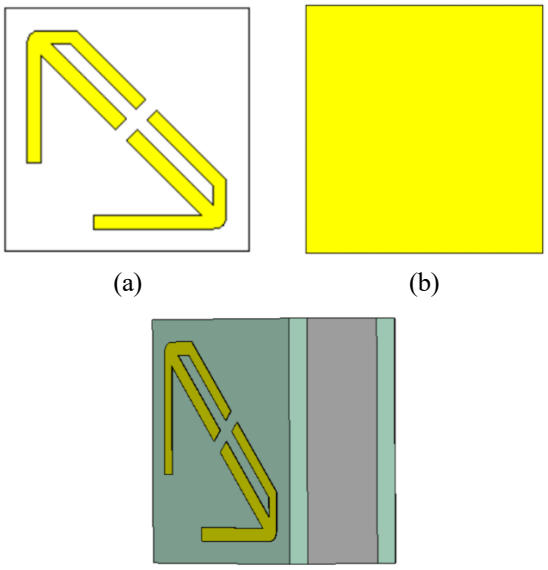
$$\vec{J} = \sigma \vec{E} \quad (9)$$

$$\vec{E_r} = \overrightarrow{a_x} \frac{J_{sx}}{\sigma} \cos(\omega t + kz) + \overrightarrow{a_y} \frac{J_{sy}}{\sigma} \cos(\omega t + kz + \varphi_j) \quad (10)$$

The reflected electric field created by the structure has the ability to remove the x or y component of the incident field. If we pay attention to the arbitrary angle α, we will realize that according to its value, the range of the x, y component of the surface current and then the reflected electric field can be controlled. Considering that this design is supposed to be controllable for multi-polarization, it is better that this angle is such that both x and y components are created, so for the design of such a unit cell, the optimal value is α=45°. It should be mentioned that the control points of the structure will be determined in such a way that the change of the impedance of the structure makes various coefficients of the surface current components in different states.

3-2- Electric and Magnetic Resonances

In [6], an arrowhead structure is proposed to achieve a wide bandwidth and converting linear to orthogonal polarization. The capability of control the rotated structure was added in the unit cell presented in [2]. Our proposed unit cell with changes in the arrowhead structure and adding another printed dipole creates the bandwidth required for satellite applications. The proposed unit cell has also some more advantages compared to [6] and other researches. These are supporting multi-polarization such as maintaining polarization of feed antenna, conversion of the feed antenna`s linear to orthogonal and circular polarizations. The Fig. 3 shows the final structure as a 3D model.

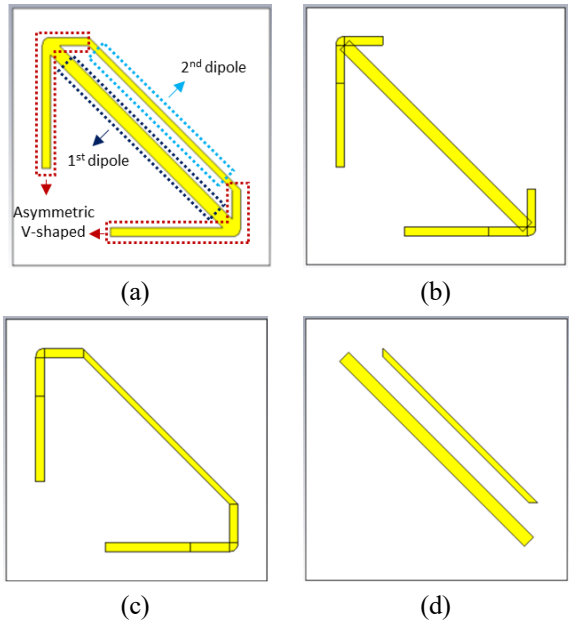


(a) (b) (c)

Fig. 3 Schematic of Proposed Structure a) Top View b) Bottom View c) 3D View

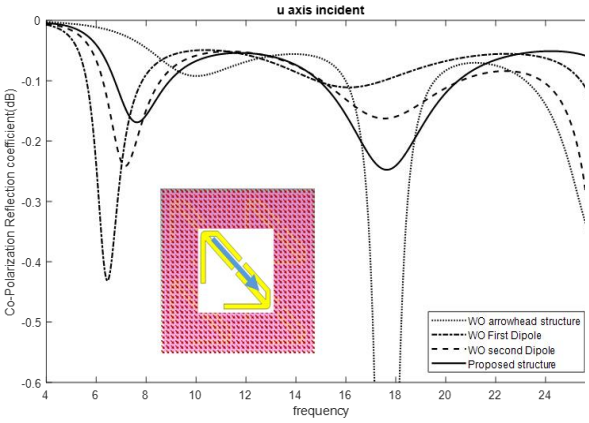
First, simulation investigates the number of natural electric and magnetic resonances of the structure with the presence or absence of the considered resonator in the structure, as shown in Fig. 3. It should be noted that if the structure creates more resonances with closer frequencies in the spectrum, a wider bandwidth can be achieved; how these natural resonances are identified? It is evident that the plasmon resonance Eigen-modes of the structure can be excited when electric components are along the v and u axes [6]. In other words, to extract the Eigen-modes of a structure, the field radiation should be in the direction of the structure geometry axes. The proposed structure uses an asymmetric V-shaped and two dipoles. The fields excitation should be in the direction of u and v axes. Different electrical length of each excitation is seen for the V-shaped structure, so the desired frequency spectrum is investigated for creating resonance in different modes. To judge whether a resonance is electric or magnetic, it is better to determine the resonance type through surface current distribution.

The investigation of natural resonances is done as in the schematics given in Fig. 4 for the cases where one of the resonators does not exist, and a comparison is made with the proposed final state. Fig. 5 shows the reflection coefficient of the structure when incident wave is in the direction of the u and v axes, so the final structure produces resonances with appropriate number and value (solid line) compared to other states for the desired bandwidth. It should be pointed out that this investigation was done only for one of the switching states with the primary dimensions.

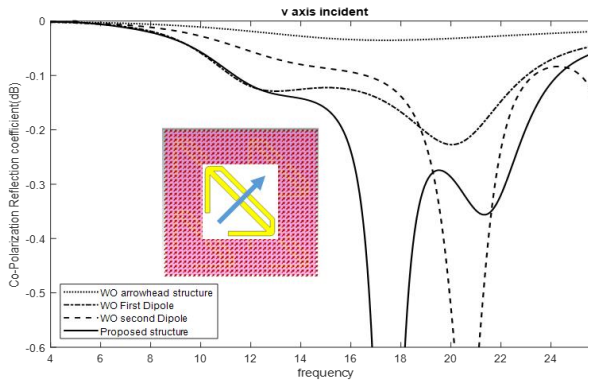


(a) (b) (c) (d)

Fig. 4 Different Cases of Structure for Investigation of Natural Resonances a) Proposed Structure b) Without Second Dipole c) Without First Dipole d) Without Arrowhead Structure



(a)



(b)

Fig. 5 Co-Polarization Reflection Coefficient for Different Cases fig.3 in a) u Axis incident b) v Axis Incident

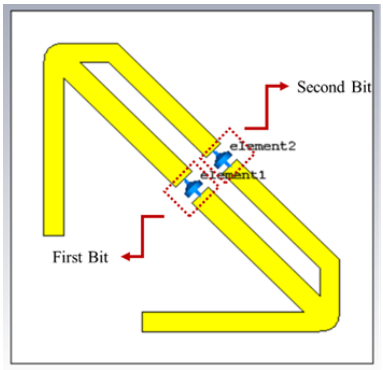


Fig. 6 control point of unit cell in schematic

3-3- Control Bits for Polarization Conversion

As shown in Fig. 6, the structure has two control points, which can reduce the number of command bits according to the usage. Table 1 shows different switching states and polarization conversion. According to this table, by controlling the impedance of these points (with different operating devices such as PIN diodes) in different states, it is possible to change the linear polarization from vertical to horizontal and vice versa or reflect the same polarization of the incident wave (polarization of feed antenna). Moreover, for this purpose, both control points are commanded with the same bit, so one command bit is enough. Another mode of control adds the ability to convert linear polarization to circular polarization based on the difference between the command bits, so we have to use two control bits. If actual control devices are placed in the structure, the inductive and capacitive effects of the control devices can be neutralized by several techniques. For instance, using a radial stub structure achieves the above goal. The radial stub structure is only visible in terms of direct current and is eliminated at high frequencies by the inductive and capacitive effects of the control device.

It should be noted that conversion is defined for a unit cell, and if the unit cell has to be used in the design of a reflect-array, the unit cell rotation technique can be used to create a 180-degree phase difference. Therefore, this structure has no weakness compared to the design in Ref. [2] in terms of creating a phase difference in the array by the unit cell rotation technique. Furthermore, in this structure, for the rotation of the main beam of the radiation pattern with the mentioned states, we have several phase differences between the unit cells. This creates smaller phase differences and increases the accuracy of rotation.

Table 1: States of switching unit cell

Bits	Impedance of Bits	Polarization of Incident Wave	Polarization of Reflected Wave
00	LL[1]	Vertical/Horizontal	Horizontal/Vertical
11	HH[2]	Vertical/Horizontal	Vertical/Horizontal
10	HL	Vertical/Horizontal	Circular Polarization
01	LH	Vertical/Horizontal	Circular Polarization

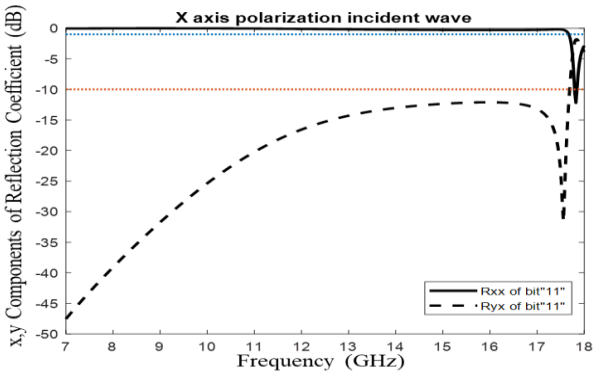
As mentioned, this structure can be used for the conversion of several polarizations. In the first state, when bits are "1", according to Fig. 7-a, the response of R_{xx} is higher than -1 dB and that of R_{yx} is lower than -10 dB in the bandwidth of 8-17 GHz. Therefore, the wave polarization does not change from horizontal to vertical because the reflected wave also has a good amount of horizontal polarization, and the linear polarization of the feed antenna is reflected. In the second state, when bits are "0", according to Fig. 7-b, the response of R_{xx} with a lower value of -10 dB and that of R_{yx} with a higher value of -1 dB indicate the conversion of the polarization from horizontal to vertical. The degree of linearity is determined by the axial ratio (AR), the results of which are given below. For the third and fourth states of the bits, i.e. "10" and "01", Figs. 7-c and 7-d show the response amplitudes of R_{xx} and R_{yx} in both states around -3 dB, with the difference that the third state has better response. Accordingly, we have relatively equal values of both x and y components in the reflected wave. However, to prove polarization conversion from linear to circular, it is better to obtain the AR parameter value as well.

After obtaining the reflection coefficients response, we extract the polarization conversion ratio (PCR) and polarization maintaining ratio (PMR) for different bits from the simulation. Therefore, we can determine the appropriate limits in the optimization of the structure parameters with the percentage of energy conversion to compare the structure with previous designs. Fig. 8 shows the polarization conversion ratio and polarization maintaining ratio of the structure for different command bits. Further analysis of this parameter reminds us that if the limit of the polarization

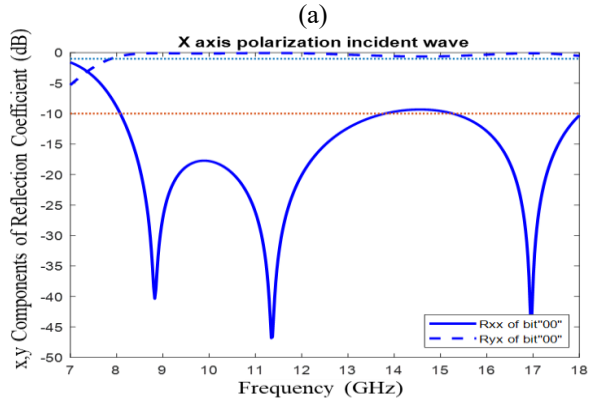
[1]. First bit and Second bit should be low impedance
[2]. First bit and Second bit should be high impedance

conversion ratio is considered to be higher than 70%, it can be claimed that regardless of the AR parameter, the polarization conversion cannot be circular, and the polarization is converted from a linear state to another type of linear state. In some studies, the limit of the conversion ratio is set to 50%. However, a higher limit for the conversion ratio is considered to achieve a higher efficiency of the structure for linear to linear polarization conversion. Therefore, the conversion ratio limit is 80-85% for bits "00", and the same limit is considered for the maintaining ratio of bits "11". With this limit value, a wide bandwidth is obtained for the structure. Of course, for bits "10" and "01", the limit values should be considered around 0.5. This is because the structure converts the polarization from linear to circular, and the first condition of circular polarization is that the x and y components of the wave are equal, so the polarization conversion or polarization maintaining for these bits should be around 0.5.

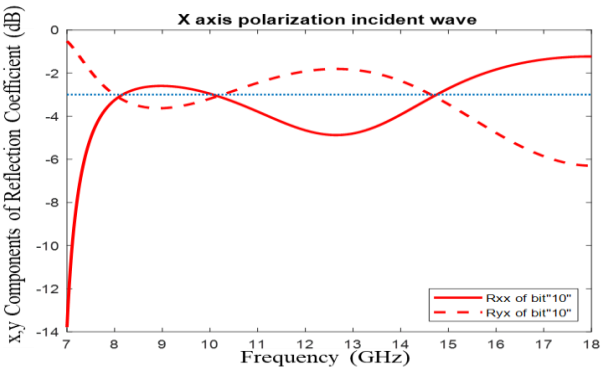
In addition to obtaining the previously mentioned parameters, AR should also be obtained. This parameter can determine the circularity of the wave polarization, and it is extracted from the relations in Ref. [8]. Fig. 9 shows that bits "10" and "01", which have the same component amplitudes and 90-degree phase difference between the components, have circular polarization. Moreover, the AR diagram of these states is below 1.41 on the linear scale in the desired bandwidth, so circular polarization is confirmed.



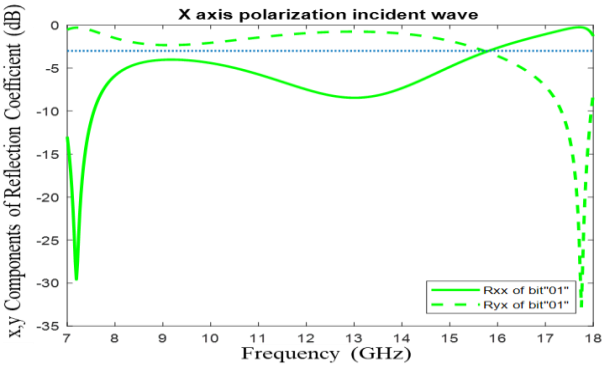
(a)



(b)



(c)



(d)

Fig. 7 Response of R_{xx}, R_{yx} Simulation for Different Bits in x Axis Incident Wave a) Bits “11” b) Bits “00” c) Bits “10” d) Bits “01”

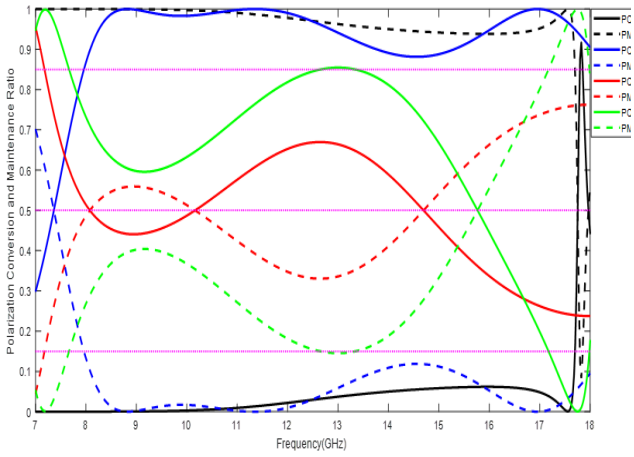


Fig. 8 Polarization Conversion and Maintenance ratio of Different Bit Control

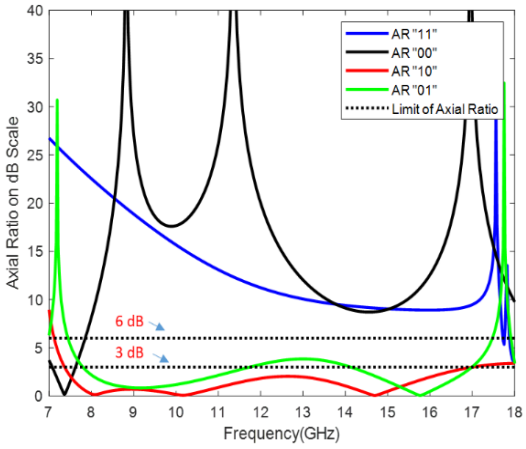


Fig. 9 Axial Ratio on Linear Scale of Different Bit Control

3-4- Surface Current

In this section, we simulate the surface current generated on the structure. According to Eq. (9), the electric field is produced by the surface current, so it is in the same direction as the surface current. The surface current and the reflected electric field vectors related to different bits of the structure can be shown by simulation and assuming that the incident wave has linear polarization in the x-direction. Fig. 10-a shows the surface current generated in state "11". In this figure, the concentration and intensity of the surface current vectors Js_n are shown in different parts of the structure. According to the current intensity, the final result is dominantly in the x-direction. Fig. 10-b shows the surface current generated in the state "00", where the components of the surface current and the reflected field have larger values in the y-direction. The components of the electric field along x and y in state "10" have almost equal values as shown in Fig. 10-c. States "11" and "10" have similar field concentration, with the difference that in state "11", the current intensity attributed to Js_2 is greater than that in state "10". Therefore, in state "11" current intensity has a greater effect on the x component, and in state "10", it has a slight effect on the x component for the surface current Js_1. Accordingly, in the case of "10", it can be claimed that the x and y components have the same values. Due to the similarity of "01" and "10" bits, one of them was checked. It should be noted that the surface current pattern gives a qualitative indication on the state of the electric field. To determine the exact type of polarization, one should assess the PCR or AR parameters, which report the type of polarization with a number and some criteria, as examined in the previous sections.

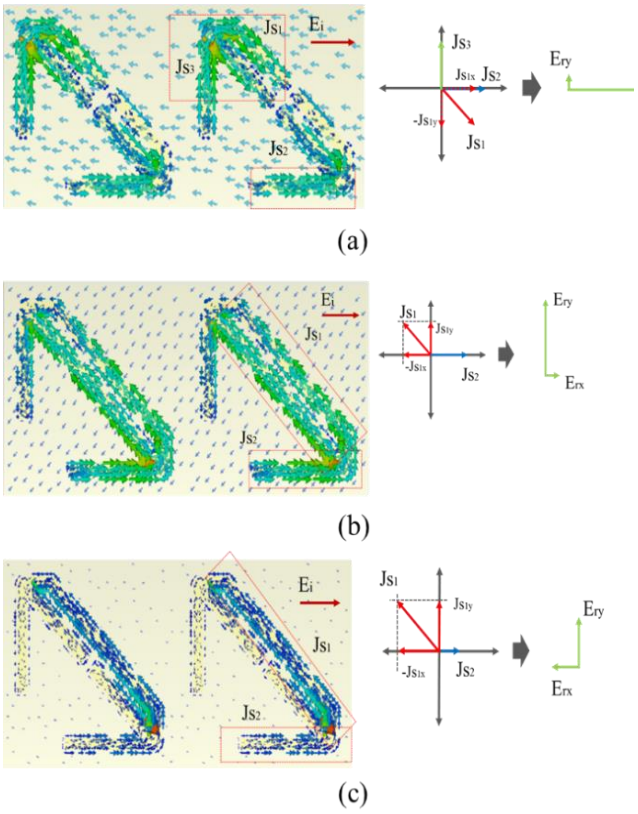


Fig. 10 Surface Currents and Analysis of Js_n Vectors Have Created by X-Direction Incident Wave a) Bit "11" b) Bit "00" c) Bit "10"

3-5- Parameters Study

The design parameters of the structure play an important role in its response and the length/width of dipoles and tentacles. Moreover, the thickness and dielectric constant (ε_r) of the substrate are investigated in the frequency response of the structure in this section. Fig. 11 shows different parameters in the design of the proposed structure. It should be mentioned that the investigations were made only for the reflection coefficient of the polarization conversion of bits "00". Additionally, checking the unfavourable changes of the frequency response is sufficient for only one of the switching modes.

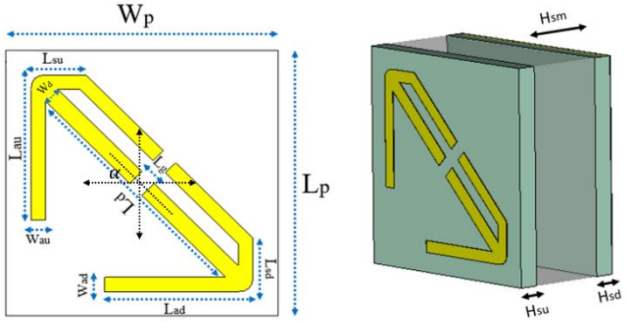
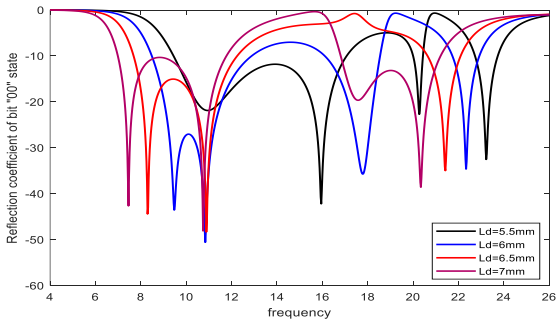


Fig. 11 Designed Parameters of Structure

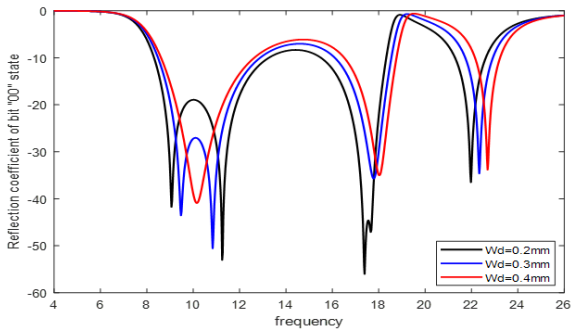
The first parameter, L_d, is the length of the dipoles. If L_d increases, the inductance effect increases in one of the resonant circuits of the structure. In addition, the capacitive effects created between printed dipoles and the ground plane and between two printed dipoles increase, and according to the relation $f=\frac{1}{\sqrt{LC}}$, the frequency of the resonant circuit of the modified element is reduced, and the circuit operates like a filter with a lower high cut-off frequency. Moreover, since the rest of the parameters are fixed, the other resonance frequencies remain constant. Then, according to the change in the resonance frequency of the printed dipole element, multiple resonance frequencies move away from each other. Therefore, this parameter plays an important role in shifting the desired frequency band, as can be seen in Fig. 12-a. It should be noted that because the dipoles are parallel and connected at the corners of the structure, it is not possible to extension only one of them.

The next parameter, W_d, is the width of the first dipole, which creates capacitive effect with the second dipole and the ground plane. W_d did not effect on all created resonances. Increasing W_d lead to both of the aforementioned capacitive effects increase. Because the capacitance between the dipoles increases according to the relation ($C = k\frac{A}{d}$) with the decrease of the distance between the two strips. The capacitance with the ground plane increases due to the increasing surface of the strip, resulting the dependent resonances shift to lower frequencies. Fig. 12-b shows adjacent resonances of structure close to each other, because of the depended resonances shifting due to the increase in W_d.

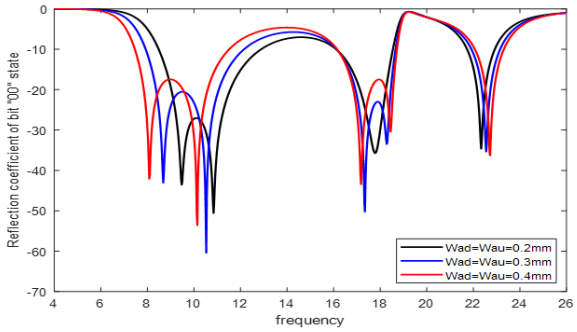
The parameter W_{au} shows the strip width of the entire structure except for the first dipole. Increasing W_{au} shifts the bandwidth towards lower frequencies because of capacitance enhancement of most resonant circuits of the structure. Fig. 12-c shows the effect of changes in W_{au} on the frequency response. Natural resonances change with the length of arrows. Fig. 12-d and 12-e show the effect of changes of L_{sd} (or L_{su}) and L_{ad} (or L_{au}).



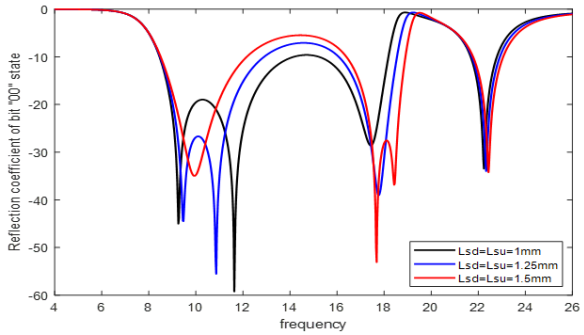
(a)



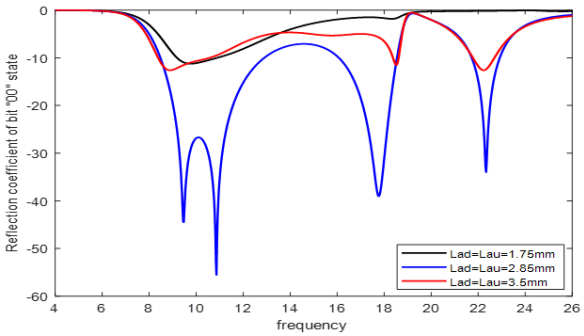
(c)



(d)



(e)

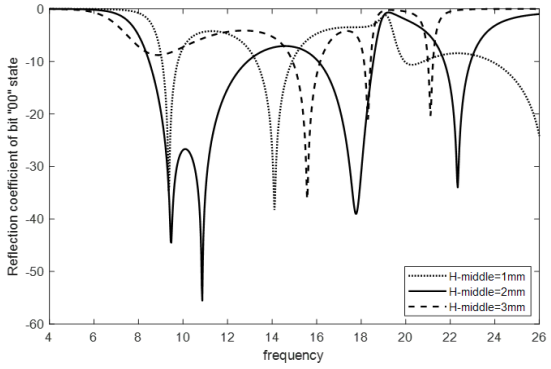


(f)

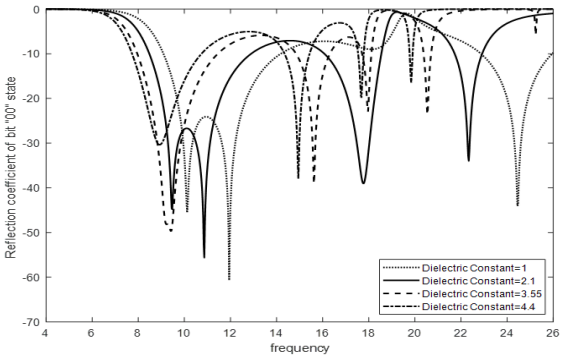
Fig. 12 Investigation on Effects of Changing Parameter Value a) Constant Parameter: W_d = 0.3 mm, W_{ad} = W_{au} = 0.2 mm, L_{ad} = L_{au} = 2.85 mm, L_{sd} = L_{su} = 1.25 mm b) Constant Parameter: L_d = 6 mm, W_{ad} = W_{au} = 0.2 mm, L_{ad} = L_{au} = 2.85 mm, L_{sd} = L_{su} = 1.25 mm c) Constant Parameter: L_d = 6 mm, W_d = 0.3 mm, L_{ad} = L_{au} = 2.85 mm, L_{sd} = L_{su} = 1.25 mm d) Constant Parameter: L_d = 6 mm, W_d = 0.3 mm, W_{ad} = W_{au} = 0.2 mm, L_{au} = L_{ad} = 2.85 mm e) L_d = 6 mm, W_d = 0.3 mm, W_{ad} = W_{au} = 0.2 mm, L_{su} = L_{sd} = 1.25 mm

After investigating the parameters of the dipoles and arrowhead structure, we study the substrate of the structure. The substrate thickness has the greatest impact on the capacitance between the structure elements and ground plane. The stack up of different substrate layers defines the effective dielectric constant (ε_{eff}). Changing the thickness of the middle layer of substrate in addition to increasing the distance between the capacitor plates also affects the effective dielectric constant, so we do not have a specific frequency shift in the frequency response. Furthermore, a change in the middle layer material shifts the multiple resonances, but the collective effect of these shifts can be such that they do not broaden the bandwidth. Fig. 13-a shows the simulation results for a thickness of 1 mm. A careful look at this figure reveals that both the distance between resonances and the reflection coefficient in the frequency spectrum increase. Moreover, for a thickness of 3 mm, in addition to these increases, an upward frequency shift occurs. The thickness of 2 mm leads to the most optimal results in terms of the previously mentioned parameters and the desired bandwidth range.

Besides thickness, another very important factor is the substrate material, so to choose an appropriate substrate, ε_r of different layers has to be studied. The changes of the dielectric constant of the middle layer directly affect the capacitive effects. By increasing ε_r of the middle layer, the lower frequency limit of the band shifts towards smaller values. As can be seen from Fig. 13-b, air as substrate with $\varepsilon_r = 1$ has a little more bandwidth and increases the efficiency of the structure. Substrates such as RT5880 and PTFE with dielectric constants of respectively 2.2 and 2.1 can be used to achieve the desired frequency response, with the difference that the rest of the parameters need to be adjusted for a better result. To further investigate the effect of other substrates, we simulate the structure with substrates that have greater dielectric constants. After examining the effects of various parameter values of the proposed structure to achieve the desired bandwidth for the four switching modes, these values are adjusted and chosen as given in Table 2. It should be noted that the simulation study results presented in the previous sections are reported with the final optimal parameters.



(a)



(b)

Fig. 13 Investigation on Effects of Changing Parameter Value of Substrate's Middle Layer a) Thickness b) Dielectric Constant

Table 2: Final Values of Proposed Structure's Parameter

Parameters	L_p	W_p	L_d	W_d	L_g	L_{ad}	L_{au}
Value(mm)	5.5	5.5	5.5	0.35	0.35	2.7	2.7
Parameters	L_{sd}	L_{su}	W_{au}	W_{ad}	H_{sm}	H_{su}	H_{sd}
Value(mm)	0.81	0.81	0.3	0.3	2	0.5	0.5

3-6- Radiation Pattern

The basic parameters of a proposed unit-cell have been investigated. The radiation pattern was examined. The unit-cell structure is independent of the linear polarization of the incident wave in the x or y direction, and the defined function is valid for both of these directions. In this section, it is also claimed that the radiation pattern will be the same when excited with either of these polarizations, so only one of these radiation modes is considered. Since the radiation pattern is the same in all bits, only bit 00 is shown. Fig. 14-a and 14-b show the two-dimensional radiation pattern in the φ=0 and 90degrees planes of the unit cell at frequencies of 10 and 14 GHz, respectively. Fig. 14-c shows the gain versus frequency.

Since the gain of the unit-cell is low, a significant amount of reflected power is not anticipated. Therefore, it is necessary to investigate that how many cells can be used to achieve a suitable gain. According to other research and rough estimates, a 30 cm× 30 cm physical surface would have a significant gain. Fig. 15-a and 15-b show the two-dimensional radiation pattern in the φ=0 and 90 degrees planes of 52×52 elements at frequencies of 10 and 14 GHz, respectively. Fig. 15-c shows the gain versus frequency.

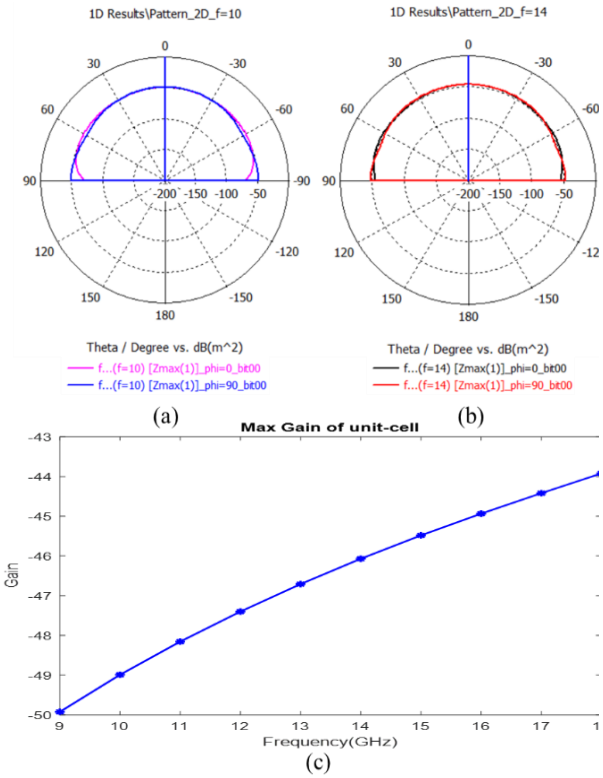


Fig. 14 a) 2-D Radiation Pattern of $\varphi = 0.90$ Plane in f=10GHz b) 2-D Radiation Pattern of $\varphi = 0.90$ Plane in f=14GHz c) Gain vs Frequency of Unit-Cell

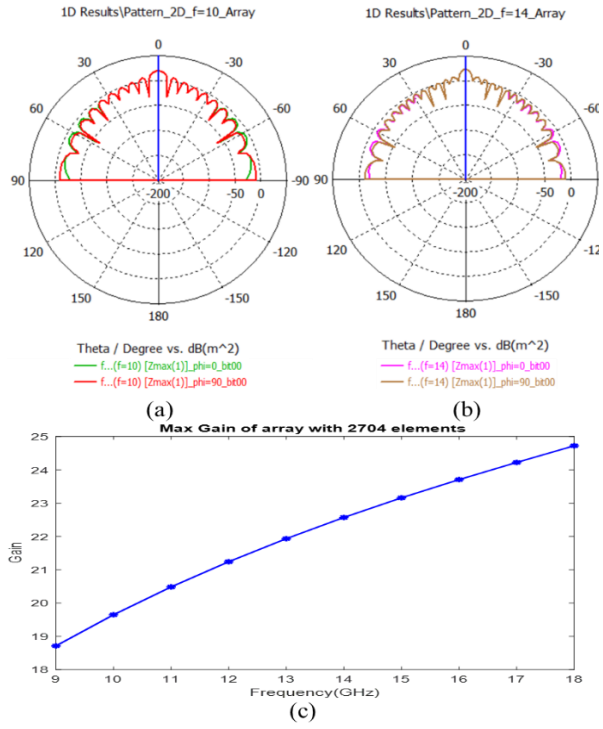


Fig. 15 a) 2-D Radiation Pattern of $\varphi = 0.90$ Plane in f=10GHz b) 2-D Radiation Pattern of $\varphi = 0.90$ Plane in f=14GHz c) Gain vs Frequency of 52×52 Elements

4- Performance Analysis

To analyse the performance of the proposed structure, its capabilities can be compared with other structures. The table 3 shows this comparison. As can be seen in the table 3, the proposed structure has smaller dimensions in a unit cell compared to other structures, and this can be achieved by proper analysis of the structure and geometry parameters to cover the desired bandwidth. The next point is that the ability to convert linear to linear and linear to circular polarization occurs separately in a common bandwidth, which means that each of the states of linear to linear and linear to circular conversion does not occur at different frequencies. In addition, this structure compared to the rest have a larger bandwidth. Another of its most important points is that the Impedance Switching mode supports wave reflection with the polarization of the feeding antenna, which means that it can play both the role of normal reflectors and the role of polarization convertor.

Table 3: Comparison Proposed Unit cell with other works

Ref.	f_1-f_2 , BW%	No. resonance layer	Size (mm^2)	Polarization
[2]	8-12,40%	One layer	6×6	LL,LR,CR
[5]	10-15,40%	Two layer	12×12	LR,CR
[15]	10.4-15.7,41%	One layer	12×12	LR,CR
[16]	11.5-14.5,23%	Multi-layer	13×13	LL
Proposed	8-17,72%	One layer	5.5×5.5	NLL,LL,LC

Note: The criterion for BW is the reflection coefficient of -10±1 dB, **LR**: Linear Rotation conversion (x incident wave convert –x reflected wave or y incident wave convert –y reflected wave), **CR**: Circular Rotation conversion (RHCP convert LHCP or vice versa), **LL**: Linear to Linear conversion (x incident wave convert y reflected wave...), **LC**: Linear to Circular conversion, NLL: No Linear to Linear conversion (x incident wave convert x reflected wave...)

5- Conclusions

In this research, we designed and simulated a unit cell of a reflect-array antenna with wide bandwidth capabilities and the ability to reflect the polarization of the feeding antenna or convert it to another polarization. The designed structure using the appropriate geometry of the upper layer (taper shape of tentacles and the use of two dipoles) and its relatively large thickness, we reached a simple design with a high degree of freedom to shift the frequency spectrum of its response. The ability to DC control and use of unit cell in the arrangement of the array can be future activities. By designing an array of this unit cell, its radiation pattern can be examined and the unit cell rotation technique can be used in its array arrangement to achieve a 180-degree phase difference. It should be noted that for connecting or not connecting control points, metal wire can be used instead of using control devices such as pin diodes for first construction, so that the cost does not increase, because the issue of cost

and assembly of control devices in the construction of the array will have more important. Finally, it should be said that the design of the unit cell is the first step of research in this field, and the construction of the unit cell and its application in the array structure can be the next steps of future activity.

References

[1] H. Luyen, Z. Yang, M. Gao, J. H. Booske and N. Behdad, "A Wideband, Single-Layer Reflectarray Exploiting a Polarization Rotating Unit Cell," in IEEE Transactions on Antennas and Propagation, vol. 67, no. 2, pp. 872-883, Feb. 2019.

[2] H. Luyen, Z. Zhang, J. H. Booske and N. Behdad, "Wideband, Beam-Steerable Reflectarrays Based on Minimum-Switch Topology, Polarization-Rotating Unit Cells," in IEEE Access, vol. 7, pp. 36568-36578, 2019.

[3] M. Min and L. Guo, "Design of a Wideband Single-Layer Reflectarray Antenna Using Slotted Rectangular Patch With Concave Arms," in IEEE Access, vol. 7, pp. 176197-176203, 2019.

[4] P. Nayeri, F. Yang and A. Z. Elsherbeni, "Broadband Reflectarray Antennas Using Double-Layer Subwavelength Patch Elements," in IEEE Antennas and Wireless Propagation Letters, vol. 9, pp. 1139-1142, 2010.

[5] B. Xi, Y. Xiao, K. Zhu, Y. Liu, H. Sun and Z. Chen, "1-Bit Wideband Reconfigurable Reflectarray Design in Ku-Band," in IEEE Access, vol. 10, pp. 4340-4348, 2022.

[6] Hongya Chen et al, "Ultra-wideband polarization conversion metasurfaces based on multiple plasmon resonances," in Journal of Applied Physics,2014.

[7] Muhammad Khan, Yixiao Chen, Bin Hu, Naeem Ullah, Syed Bukhari, Shahid Iqbal, "Multiband linear and circular polarization rotating metasurface based on multiple plasmonic resonances for C, X and K band applications," in Scientific Reports,2020.

[8] Majeed, A.; Zhang, J.; Ashraf, M.A.; Memon, S.; Mohammadani, K.H.; Ishfaq, M.; Sun, M. An Ultra-Wideband Linear-to-Circular Polarization Converter Based on a Circular, Pie-Shaped Reflective Metasurface. *Electronics* 2022.

[9] N. Pouyanfar, J. Nourinia, C. Ghobadi, "Multiband and multifunctional polarization converter using an asymmetric metasurface," in Sci Rep, 2021.

[10] Muhammad Khan, Zobaria Khalid, Farooq Tahir, "Linear and circular-polarization conversion in X-band using anisotropic metasurface," in Scientific Reports, 2019.

[11] M.H. Dahri, M.H. Jamaluddin, F.C. Seman, M.I. Abbasi, N.F. Sallehuddin, A.Y. I. Ashyap, M.R. Kamarudin, "Aspects of Efficiency Enhancement in Reflectarrays with Analytical Investigation and Accurate Measurement," in Electronics, vol. 9, 2020.

[12] D. M. Pozar, S. D. Targonski and R. Pokuls, "A shaped-beam microstrip patch reflectarray," in IEEE Transactions on Antennas and Propagation, vol. 47, no. 7, pp. 1167-1173, July 1999.

[13] Constantine A. Balanis, "*Antenna Theory: Analysis and Design*," Third Edition, John Wiley & Sons, Inc., Hoboken, 1136 pages, April 4, 2005.

[14] D. K. Cheng, "*Field and Wave Electromagnetics*," 2nd Edition, Addison Wesley, Inc., Boston, pp. 547- 557, 1989.

[15] Hoang Dang Cuong, Minh Thuy Le, Trong Toan Do and Nguyen Quoc Dinh, "Broadband Multipolarized Reconfigurable Unit Cell for Reflectarray Antennas with One Bit Control," in International Journal of Antennas and Propagation, 2022.

[1] M. -T. Zhang et al., "Design of Novel Reconfigurable Reflectarrays With Single-Bit Phase Resolution for Ku-Band Satellite Antenna Applications," in IEEE Transactions on Antennas and Propagation, vol. 64, no. 5, pp. 1634-1641, May 2016.

Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 24-32
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

A Turkish Dataset and BERTurk-Contrastive Model for Semantic Textual Similarity

Somaiyeh Dehghan[1*], Mehmet Fatih Amasyali[1]

[1].Department of Computer Engineering, Yildiz Technical University, Istanbul, Turkey

Received: 27 Sep 2024/ Revised: 04 Apr 2025/ Accepted: 04 May 2025

Abstract

Semantic Textual Similarity (STS) is an important NLP task that measures the degree of semantic equivalence between two texts, even if the sentence pairs contain different words. While extensively studied in English, STS has received limited attention in Turkish. This study introduces BERTurk-contrastive, a novel BERT-based model leveraging contrastive learning to enhance the STS task in Turkish. Our model aims to learn representations by bringing similar sentences closer together in the embedding space while pushing dissimilar ones farther apart. To support this task, we release SICK-tr, a new STS dataset in Turkish, created by translating the English SICK dataset. We evaluate our model on STSb-tr and SICK-tr, achieving a significant improvement of 5.92 points over previous models. These results establish BERTurk-contrastive as a robust solution for STS in Turkish and provide a new benchmark for future research.

Keywords: Semantic Textual Similarity; Contrastive Learning; Deep Learning; BERT; BERTurk; Turkish Language.

1- Introduction

Semantic Textual Similarity (STS) is a fundamental task in NLP that aims to measure the similarity of the semantic meaning of given texts. STS has a crucial role in various NLP downstream tasks, including information retrieval, text summarization, text classification, sentiment analysis, question answering, machine translation, automatic essay scoring, named entity recognition, plagiarism check, and many more. Many methods have been proposed for measuring STS including traditional methods (e.g., BOW and TF-IDF), neural embedding models (e.g., Word2Vec [1] and GloVe [2]), and deep contextualized language models (e.g., BERT [3]).

Traditional STS measurement methods only focus on a lexical level and do not consider the semantic information of words [4, 5]. For example, the two sentences “How old are you?” and “What is your age?” are completely similar in terms of meaning, but they do not have a word in common. Neural embedding-based STS measurement methods produce context-independent embeddings [6, 7]. While the meaning of words can change according to their context. For example, in these two sentences “I open a bank account.” and “The Ahilya fort on the banks of the river Narmada is amazing to see.”, the word *bank* has completely different meanings.

Recent methods of measuring STS have been able to overcome these weaknesses using deep contextualized embedding models. BERT [3] is a language model whose main technical innovation is the use of Transformers. The Transformer-based architecture of BERT uses the amazing attention mechanism that learns contextual relationships between words in a sequence of text. Moreover, BERT supports transfer learning and fine-tuning for specific tasks like STS. BERT has proven to be highly successful in a variety of NLP tasks, such as sentiment analysis [8], text classification [9], text chunking [10], and hate speech detection [11, 12, 13], demonstrating its versatility and effectiveness across different domains.

In this study, we propose a BERTurk model using contrastive learning for Semantic Textual Similarity. Our model seeks to learn a embedding space in which pairs of similar sentences remain close to each other while dissimilar sentence pairs are pushed apart. In addition, we also prepare an STS dataset for Turkish, namely SICK-tr. We evaluate our model on two Turkish STS benchmarks, STSb-tr [14] and our SICK-tr dataset. The evaluation findings show that our model performs noticeably better than previous models, demonstrating superior accuracy in capturing semantic similarities in Turkish texts, and setting a new standard for STS tasks in this language.

The proposed model and released dataset are available in our GitHub repository[1].

The current study provides significant contributions by attempting to fill several gaps as follows:

- First, the study extends the limited research on the STS task in the Turkish language, addressing a critical need in NLP for low resource languages.
- Second, the study is the first to consider contrastive learning for the STS task in Turkish, so that this method not only improves the precision of semantic similarity assessments but also sets a precedent for future research to use contrastive learning techniques in other low resource languages.
- Third, the study significantly expands the limited STS benchmarks in Turkish by releasing the SICK-tr dataset. This new dataset serves as a valuable resource for the NLP community, providing a robust foundation for future research and development in STS tasks for the Turkish language.

The remainder of the paper is structured as follows: A brief overview of related work is given in Section 2. The methodology for preparing SICK-tr dataset and our proposed model, BERTurk-contrastive, is provided in Section 3. The experiments are described in Section 4. The final portion includes conclusions and information about future work.

2- Related Work

There are many studies focusing on STS in other languages. However, to the best of our knowledge, there have been few studies in the literature for measuring semantic similarity of Turkish texts. In addition, there are seven standard benchmarks for evaluating STS in English, including STS12-STS16 [15-19], STSb [20], and SICK [21], while the only Turkish STS dataset is STSb-tr [14], which was created in 2021 by translating STSb using Google Cloud Translation API.

Ref. [14] proposed a BERT-based model for semantic textual similarity. They fine-tuned BERTurk using Cross-Entropy (CE) and Mean Squared Error (MSE) objectives on the NLI-tr [22] and STSb-tr [14] datasets, respectively. They achieved a Spearman's rank correlation of 83.31% on the STSb-tr test set for the S-BERTurk model. Ref. [23] proposed a statistical method for semantic textual similarity in Turkish news using Probabilistic Latent Semantic Analysis (PLSA) and Latent Dirichlet Allocation (LDA). They were able to predict the similarity between two news articles. However, the news articles they used in the experiments were few and had many words in common.

In recent years, there has been an increasing amount of literature on contrastive learning for fine-tuning BERT on semantic similarity in the English language. Contrastive learning is a deep metric learning method that encourages a model to learn an embedded space in which similar (positive) data samples (x_i, x_i^+) remain close to each other, while dissimilar (negative) data samples (x_i, x_i^-) are further apart.

Ref. [24] proposed $\text{SimCSE}_{\text{unsup}}$ and $\text{SimCSE}_{\text{sup}}$ models using self-supervised and supervised contrastive learning, respectively, to fine-tune BERT. They achieved the best results in the supervised setting with an average Spearman's rank correlation of 81.57% on seven standard STS benchmarks in English.

Ref. [25] proposed a supervised multiple positives and negatives contrastive learning model, SupMPN, to fine-tune BERT. Their idea was that by using multiple positives (similar sentences), the model would generalize in such a way that it could simultaneously bring together similar sentences in the embedding space, and by using multiple negatives (dissimilar sentences), the model would generalize to improve the distinction between similar and dissimilar sentences. They achieved an average Spearman's rank correlation of 82.07% on seven standard STS benchmarks in English.

Ref. [26] proposed a curriculum contrastive learning model (SelfCCL) by transferring self-taught knowledge for fine-tuning BERT, which mimics the human learning process. Their model learns by contrasting similar and dissimilar sentences, starting from the simplest to the hardest triplets(x_i, x_i^+, x_i^-). They achieved an average Spearman's rank correlation of 81.80% on seven standard STS benchmarks in English.

3- Methodology

This section first describes the preparation process of the SICK-tr dataset, followed by an introduction to our proposed model, BERTurk-contrastive.

3-1- Providing SICK-tr Dataset

SICK [21], an acronym for Sentences Involving Compositional Knowledge, contains about 10,000 sentence pairs with a wealth of lexical, syntactic, and semantic phenomena. Each pair of sentences has two types of annotations: relatedness and entailment. The human

[1] Our pre-trained model and released dataset are publicly available at: https://github.com/SoDehghan/BERTurk-contrastive
https://github.com/SoDehghan/SICK-TR

relatedness score ranges from 1 to 5, and there are three categories of entailment relations: entailment, contradiction, and neutral.

Table 1. Some Translation Examples by Google Translation API in SICK-tr Dataset

Sentence 1	Sentence 2	Relatedness Score	Relationship
Bir kadın bir makineyle dikiyor. (A woman is sewing with a machine.)	Bir kadın dikiş için yapılmış bir makine kullanıyor. (A woman is using a machine made for sewing.)	4.8	Gereklilik (Entailment)
Genç çocuklar bir parkta yeşil bir futbol topu ile poz veriyor. (The young boys are posing with a green soccer ball in a park.)	Bir topun önünde dört erkek yan yana diz çöküyor. (Four boys are kneeling next to each other in front of a ball.)	3.5	Nötr (Neutral)
Kameralı bir adam konuyu inceliyor. (A man with a camera is studying the subject.)	Konuyu inceleyen kameralı bir insan yok. (There is no man with a camera studying the subject.)	3.6	Çelişki (Contradiction)

Table 2. SICK and SICK-tr Statistics

Dataset	Size of Vocabulary	Average Word Length	Average Sentence Length
SICK [21]	2,551	6.38	9.65
SICK-tr (ours)	4,484	7.31	6.79

Table 3. Example of Some Translation Errors from English to Turkish for SICK-tr (ours)

	Error Type	English Sentence	Turkish Translation Using Google Translation API	Corrected Turkish Translation
1	Sentiment	A skilled person is riding a bicycle on one wheel.	Yetenekli bir kişi bir tekerleğe bisiklet sürüyor.	Yetenekli bir kişi tek tekerlek üzerinde bisiklet sürüyor.
2	Syntax	A brown dog is attacking another animal in front of the man in pants.	Kahverengi bir köpek, pantolondaki adamın önünde başka bir hayvana saldırıyor.	Kahverengi bir köpek, pantolonlu adamın önünde başka bir hayvana saldırıyor.

We use a variant of SICK that is located in the SentEval GitHub repository [27]. The train-split has 4,500 pairs, the development-split has 500 pairs, and the test-split has 4,927 pairs.

We translated the English SICK dataset using Google Cloud Translation API[2], creating a variant called SICK-tr, and released it in our GitHub repository. The translation quality and adherence to the original labels have not been verified by human experts. Table 1 shows some sentence pairs from SICK-tr translated by Google Translation API, and Table 2 shows some statistics on word and sentence lengths in both SICK and SICK-tr datasets.

3-1-1- Error Types in Translation from English to Turkish

According to a study conducted on translation from Turkish to English using Google Translation [28], there are five major types of errors, including lexical errors, syntactic errors, semantic errors, morphological errors, and pragmatic errors in machine translation. Although their study focused on Turkish to English translation, we also observed the same errors in the translation from English to Turkish. However, we have not changed them, as they are few in number, and generally, such translation errors are not considered to be a major problem in STS [14]. Table 3 shows some examples of these errors. As shown in Table 3, in example 2, the preposition “in” in “man in pants” means “with” in English. However, it was translated as if it meant “içinde” (inside) in Turkish.

[2] https://cloud.google.com/translate

Table 4: Training Setting for our Models. CE: Cross Entropy, SCL: Supervised Contrastive Loss, MSE: Mean Squared Error

Model	Training Dataset	Objective Function	Batch Size	Training Epochs
S-BERTurk-nli-ce [14] (reproduced)	NLI-tr	CE	512	6
S-BERTurk-nli-contrastive (ours)	NLI-tr	SCL	512	6
S-BERTurk-nli-stsb-contrastive-mse (ours)	NLI-tr, STSb (train-split)	SCL, MSE	512, 256	6, 8

3-2- BERTurk-Contrastive Model

Contrastive learning is a type of self-supervised learning approach used to learn representations of data by contrasting positive pairs (anchor-positive: similar or related data points) against negative pairs (anchor-negative: dissimilar or unrelated data points). Figure 1 shows contrastive learning idea.

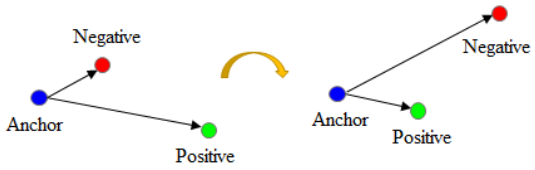


Fig 1. Contrastive Learning Idea [30]

We employ the supervised contrastive loss from [26], which incorporates a hard negative to develop a version of the NT-Xent loss [29]. In a mini-batch, the Supervised Contrastive Loss (SCL) for a triplet in the form anchor-positive-negative (x_i, x_i^+, x_i^-) is given as follows:

$$L_{SCL} = -log \frac{e^{(sim(x_i, x_i^+)/\tau)}}{\sum_{j=1}^{N}\left(e^{(sim(x_i, x_j^+)/\tau)} + e^{(sim(x_i, x_j^-)/\tau)}\right)} \qquad (1)$$

where $sim(\cdot)$ is the standard cosine similarity, and τ is a temperature parameter to scale the cosine similarity.

4- Experiments

4-1- Training Dataset

To train our model, we employ the Natural Language Inference (NLI) dataset in Turkish (NLI-tr) [22]. NLI is the process of determining, given a premise, whether a hypothesis is true (entailment), false (contradiction), or indeterminate (neutral). NLI-tr is a collection of two large datasets that were created by translating the SNLI [31] and MultiNLI [32] fundamental NLI corpora using Amazon Translate.

Our model's inputs are triplets in the form of (x_i, x_i^+, x_i^-), where entailment hypotheses are treated as positives and contradiction hypotheses are as negatives for the premise sentence (anchor). That is, we use only the entailment and contradiction labels, ignoring the neutral labels. Our training dataset contains roughly 300K input triplets in total.

4-2- Training Setup

The Hugging Face Model Hub hosts a pre-trained BERTurk model as our starting point. We employ the Sentence-BERT bi-encoder architecture of Sentence Transformers as described by [33]. We reproduced the S-BERTurk-nli-ce model based on [14], which was trained on the NLI-tr dataset as a three-way classification problem (entailment, contradiction, and neutral) using cross-entropy (CE) loss.

We trained two models, S-BERTurk-nli-contrastive and S-BERTurk-nli-stsb-contrastive-mse models. For S-BERTurk-nli-contrastive model, we trained BERTurk on NLI-tr using SCL. For the S-BERTurk-nli-stsb-contrastive-mse model, we first trained BERTurk on NLI-tr using SCL and then fine-tuned it on STSb-tr (train-split) using MSE (Mean Squared Error) loss.

The STSb-tr dataset, like the SICK-tr dataset, contains pairs of sentences whose degree of similarity is annotated in the range between 0 and 5. So in this case (a regression problem), MSE loss is used to compute the cosine similarity score between sentence pairs as follows:

$$L_{MSE} = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \qquad (2)$$

where y_i and $\hat{y}_i$ are the desired values and predicted values, respectively. We have summarized the information about the training settings for our reproduced and proposed models in Table 4.

Table 5. Results of the two Turkish STS Benchmark Evaluations. For each Benchmark, a Spearman's Rank Correlation as $\boldsymbol{\rho \times 100}$ is Provided in the Columns. The Best Results are in Bold for Each Column.

Model	Objective Function	STSb (test-split)	SICK-tr (test-split)	Average
No fine-tuned has been done				
BERTurk (baseline model)	-	55.23	55.67	55.45
Only trained on NLI-tr				
S-BERTurk-nli-ce [14] (reproduced)	CE	72.74	70.21	71.47
S-BERTurk-nli-contrastive (ours)	SCL	**78.43**	**76.35**	**77.39**
First trained on NLI-tr and then fined-tuned on STSb-tr (train-split)				
S-BERTurk-nli-stsb-ce-mse [14] (reproduced)	CE, MSE	83.31	-	-
S-BERTurk-nli-stsb-contrastive-mse (ours)	SCL, MSE	**84.38**	**76.71**	**80.51**

4-3- Evaluation on Turkish STS Benchmarks

In this experiment, we evaluate our models on the STSb-tr (test-split) and SICK-tr (test-split) datasets. We compare our proposed models to BERTurk (the baseline model), S-BERTurk-nli-ce [14] (our reproduced model), and S-BERTurk-nli-stsb-ce-mse model [14]. Table 5 shows the results.

Results: As seen in Table 5, our models outperform the previous models, demonstrating significant advancements in accuracy and in efficiency. S-BERTurk-nli-contrastive model achieved an average improvement of 5.92 points (71.47% vs. 77.39%) compared to S-BERTurk-nli-ce (our reproduced model). Moreover, S-BERTurk-nli-stsb-contrastive-mse model achieved an improvement of 1.07 points (83.31% vs. 84.38%) on the STSb-tr dataset compared to S-BERTurk-nli-stsb-ce-mse [14]. Our findings indicate that first replacing cross-entropy loss with contrastive loss improves accuracy, as demonstrated by the S-BERTurk-nli-contrastive model's 5.92-point improvement over the S-BERTurk-nli-ce model. Additionally, using contrastive loss followed by MSE loss further enhances performance, with the S-BERTurk-nli-stsb-contrastive-mse model achieving a 1.07-point improvement (83.31% vs. 84.38%) on the STSb-tr dataset compared to the S-BERTurk-nli-stsb-ce-mse model [14].

4-4- Visualizing Sentence Embedding Space

In this experiment, we visualize the embeddings of nine sentences from SICK-tr to demonstrate the ability of our proposed model, S-BERTurk-nli-contrastive, to create a better embedding space for similar and dissimilar sentences. As explained in Section 3.1, each pair of sentences in the SICK dataset is labeled in two ways: relatedness and entailment. Therefore, we chose three anchor sentences on three different topics and their entailment and contradiction sentences as similar and dissimilar sentences, respectively, which makes nine sentences.

We use t-SNE [34], short for t-student Distributed Stochastic Neighbor Embedding, which is an unsupervised machine learning tool for visualizing high-dimensional data. t-SNE converts similarities between data points using a normal distribution in a high-dimensional space and a t-distribution in a low-dimensional space, respectively. Then, it tries to optimize the difference between the probability distributions of these two spaces using a cost function called Kullback-Leibler divergence (KL).

Figures 2, 3, and 4 show the embedding space for BERTurk (baseline model), S-BERTurk-nli-ce [14] (our reproduced model), and S-BERTurk-nli-contrastive (our proposed model), respectively.

Results: Figure 2 illustrates that BERTurk (baseline) fails to accurately differentiate between semantically distinct sentences, as evident from the close embeddings of sentences with vastly different meanings. For instance, sentences about a child playing and a brown dog playing with a toy are incorrectly grouped. This highlights the limitations of the baseline model in capturing semantic nuances. Figure 3 demonstrates that the S-BERTurk-nli-ce [14] model improves upon BERTurk (baseline) by grouping sentences with similar sentiment polarity (positive or negative).

Fig. 2. Visualizing Embedding Space for Nine Sentences from SICK-tr Dataset by BERTurk (Baseline Model)

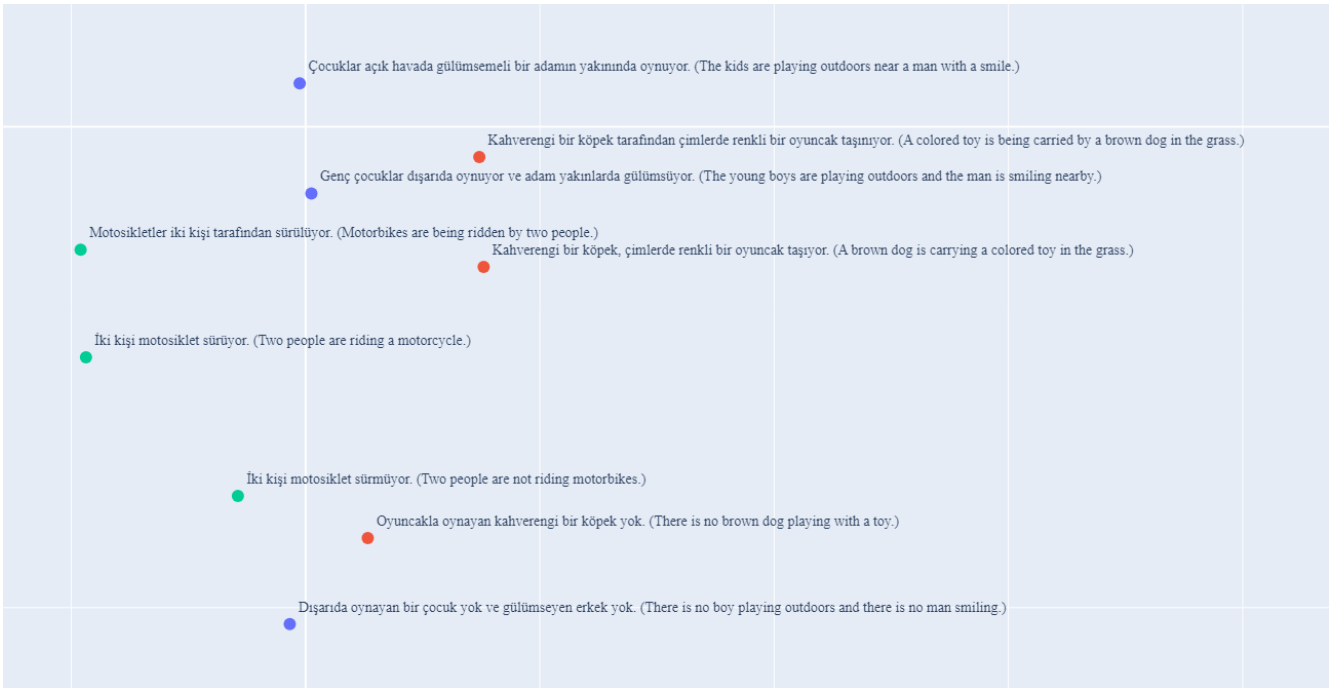


Fig. 3. Visualizing Embedding Space for Nine Sentences from SICK-tr Dataset by BERTurk-nli-ce (our Reproduced Model) [14]

Fig. 4. Visualizing Embedding Space for Nine Sentences from SICK-tr Dataset by BERTurk-nli-Contrastive (our Proposed Model)

However, it fails to capture semantic differences within the same sentiment category. For example, sentences such as "Dışarıda oynayan bir çocuk yok ve gülümseyen erkek yok. (There is no boy playing outdoors and there is no man smiling)", "Oyuncakla oynayan kahverengi bir köpek yok. (There is no brown dog playing with a toy)", and "İki kişi motosiklet sürmüyor. (Two people are not riding motorbikes)", are all embedded closely due to their shared negative polarity, despite their different semantics.

Figure 4 showcases the strength of our proposed S-BERTurk-nli-contrastive model, which organizes embeddings based on both sentiment and semantics. As can be seen in figure 4, our proposed model, S-BERTurk-nli-contrastive, is able to correctly embed the sentences in the embedding space based on their concepts (topics). In addition, our proposed model is better able to distinguish between positive (similar) and negative (dissimilar) sentences for each topic. For instance, for the sentences: "Kahverengi bir köpek, çimlerde renkli bir oyuncak taşıyor. (A brown dog is carrying a colored toy in the grass.)", "Kahverengi bir köpek tarafından çimlerde renkli bir oyuncak taşınıyor. (A colored toy is being carried by a brown dog in the grass.)", and "Oyuncakla oynayan kahverengi bir köpek yok. (There is no brown dog playing with a toy.)", our model successfully groups the first two sentences together due to their similar semantic meanings, both describing the action of a brown dog interacting with a toy. Meanwhile, it places the third sentence, which negates the presence of a brown dog playing with a toy, in a distinct position in the embedding space, reflecting its dissimilar semantic meaning. This demonstrates that our proposed model excels in accurately capturing both the concepts and the relationships between sentences, resulting in embeddings that align closely with their true semantic meanings.

5- Conclusion and Future Work

In this study, we proposed a BERTurk-contrastive model that used contrastive learning for the STS task in the Turkish language. This approach represents a significant advancement in the application of contrastive learning to the Turkish language, a relatively underexplored area in NLP research. Our primary contribution includes the creation of the SICK-tr dataset using the Google Translation API, which we have released publicly via GitHub for public use, providing a valuable resource and benchmark for future research on STS in Turkish.

Our evaluation results on two STS datasets, STSb-tr and SICK-tr, demonstrate that replacing cross-entropy loss with contrastive loss leads to a substantial improvement of 5.92 points (71.47% to 77.39%). This highlights the effectiveness of contrastive learning in capturing semantic similarities more accurately, particularly for low-resource languages. Additionally, visualizing the embedding space for nine sentences on three different topics shows that our model can better distinguish between similar and dissimilar

sentences within each topic. This capability is crucial for enhancing the performance of various downstream NLP applications, such as text clustering, information retrieval, and question answering.

The creation of the SICK-tr dataset, coupled with the improved performance of our contrastive model, establishes a foundation for further advancements in Turkish STS tasks. Future work will extend this research by exploring state-of-the-art large language models, such as GPT, and T5, and XLM-R, alongside novel contrastive learning strategies. These efforts aim to further advance the performance and applicability of STS systems in Turkish and other low-resource languages.

Limitations

The main limitations of our work include the reliance on a translation-based dataset (SICK-tr), which may not fully capture the nuances of Turkish language structure and idiomatic expressions, potentially introducing bias. Additionally, our model is evaluated only on two datasets (STSb-tr and SICK-tr), limiting its generalizability to other domains or real-world applications. Lastly, the computational requirements of training the model may pose challenges for broader accessibility.

References

[1] T. Mikolov, K. Chen, G. S. Corrado, J. Dean, “Efficient estimation of word representations in vector space,” In Proceedings of the 2013 International Conference on Learning Representations, 2013.

[2] J. Pennington, R. Socher, C. Manning, “Glove: Global vectors for word representation,” In Proceedings of the 2014 Conference on Empirical Methods in NLP (EMNLP), pp. 1532–1543. 2014.

[3] J. Devlin, JM.-W. Chang, K. Lee, K. Toutanova, “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding”, In Proceedings of the 2019 Conference of the American Chapter of the Association for Computational Linguistics, Vol. 1, pp. 4171—4186, 2019.

[4] H. Cheng, S. Yat, "A Text Similarity Measurement Combining Word Semantic Information with TF-IDF Method", Chinese Journal of Computers, 2011.

[5] S. Albitar, S. Fournier, B. Espinasse, "An Effective TF/IDF-based Text-to-Text Semantic Similarity Measure for Text Classification", Web Information Systems Engineering, pp. 105-114, 2014.

[6] J. Chandra, A. Santhanam, A. Joseph, "Artificial Intelligence based Semantic Text Similarity for RAP Lyrics," 2020 International Conference on Emerging Trends in Information Technology and Engineering, pp. 1-5, 2020.

[7] E. Hindocha, V. Yazhiny, A. Arunkumar, P. Boobalan, "Short-text Semantic Similarity using GloVe word embedding", International Research Journal of Engineering and Technology (IRJET), Volume: 06, Issue: 04, Apr 2019.

[8] S. Chakraborty, “An Efficient Sentiment Analysis Model for Crime Articles’ Comments using a Fine-tuned BERT Deep Architecture and Pre-Processing Techniques”, Journal of Information Systems and Telecommunication (JIST), Vol. 45, pp. 1-11, 2024.

[9] J. Nagesh, “Hierarchical Weighted Framework for Emotional Distress Detection using Personalized Affective Cues,” Journal of Information Systems and Telecommunication (JIST), Vol. 38, pp. 89-101, 2022

[10] P. Kavehzadeh, “Deep Transformer-based Representation for Text Chunking”, Journal of Information Systems and Telecommunication (JIST), Vol. 43, pp. 176-184, 2023.

[11] S. Dehghan, B. Yanıkoğlu, “Evaluating ChatGPT’s Ability to Detect Hate Speech in Turkish Tweets,” In Proceedings of the 7th Workshop on Challenges and Applications of Automated Extraction of Socio-political Events from Text (CASE 2024), pages 54–59, St. Julians, Malta. Association for Computational Linguistics, 2024.

[12] S. Dehghan, B. Yanıkoğlu, “Multi-domain Hate Speech Detection Using Dual Contrastive Learning and Paralinguistic Features,” In Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024), pages 11745–11755, Torino, Italia. ELRA and ICCL, 2024.

[13] S. Dehghan, M. U. Şen, B. Yanıkoğlu, “Dealing with annotator disagreement in hate speech classification,” Preprint, arXiv:2502.08266, 2025.

[14] F. B. Fikri, K. Oflazer, B. Yanıkoğlu, “Anlamsal Benzerlik için Türkçe Veri Kümesi (Turkish Dataset for Semantic Similarity)”, In Proceedings of the 29th IEEE Conference on Signal Processing and Communications Applications, Istanbul, Turkey, 2021.

[15] E. Agirre, D. Cer, M. Diab, A. Gonzalez-Agirre, “Semeval-2012 task 6: A pilot on semantic textual similarity,” In *SEM 2012: The First Joint Conference on Lexical and Computational Semantics (SemEval 2012), Association for Computational Linguistics, pp. 385–393, 2012.

[16] E. Agirre, D. Cer, M. Diab, A. Gonzalez-Agirre, W. Guo, “*sem 2013 shared task: Semantic textual similarity,” in In Second Joint Conference on Lexical and Computational Semantics (*SEM), Vol. 1, pp. 32–43, 2013.

[17] E. Agirre, C. Banea, C. Cardie, D. Cer, M. Diab, A. Gonzalez-Agirre, W. Guo, R. Mihalcea, G. Rigau, J. Wiebe, “Semeval-2014 task 10: Multilingual semantic textual similarity,” Association for Computational Linguistics, pp. 81–91, 2014.

[18] E. Agirre, C. Banea, C. Cardie, D. Cer, M. Diab, A. Gonzalez-Agirre, W. Guo, I. Lopez-Gazpio, M. Maritxalar, R. Mihalcea, G. Rigau, L. Uria, J. Wiebe, “Semeval-2015 task 2: Semantic textual similarity, english, spanish and pilot on interpretability,” Association for Computational Linguistics, pp. 252–263, 2015.

[19] E. Agirre, C. Banea, D. Cer, M. Diab,A. Gonzalez-Agirre, R. Mihalcea, G. Rigau, J. Wiebe, “Semeval-2016 task 1: Semantic textual similarity, monolingual and cross-lingual

evaluation," Association for Computational Linguistics, pp. 497–511, 2016.

[20] D. Cer, M. Diab, E. Agirre, I. Lopez-Gazpio, L. Specia, "Semeval-2017 task 1: Semantic textual similarity multilingual and crosslingual focused evaluation," In Proceedings of the 11th International Workshop on Semantic Evaluation, pp. 1–14, 2017.

[21] M. Marelli, S. Menini, M. Baroni, L. Bentivogli, R. Bernardi, R. Zamparelli, "A sick cure for the evaluation of compositional distributional semantic models," in In Proceedings of the International Conference on Language Resources and Evaluation (LREC), pp. 216–223, 2014.

[22] E. Budur, R. Özçelik, T. Güngör, "Data and Representation for Turkish Natural Language Inference", Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing, Nov. 2020.

[23] E. Yıldıztepe, V. Uzun, "Olasılıksal Yöntemler ile Türkçe Metinlerin Anlamsal Benzerliğinin Belirlenmesi", Sinop Üniversitesi Fen Bilimleri Dergisi, Sinop Uni J Nat Sci 3 (2): 66-78, 2018.

[24] T. Gao, X. Yao, D. Chen, "SimCSE: Simple Contrastive Learning of Sentence Embeddings", In Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing, 2021.

[25] S. Dehghan, M.F. Amasyali, "SupMPN: Supervised Multiple Positives and Negatives Contrastive Learning Model for Semantic Textual Similarity", Applied Sciences, 12:9659, 2022.

[26] S. Dehghan, M.F. Amasyali, "SelfCCL: Curriculum Contrastive Learning by Transferring Self-Taught Knowledge for Fine-Tuning BERT", Applied Sciences, Vol. 13(3):1913, 2023.

[27] A. Conneau, D. Kiela, "SentEval: An evaluation toolkit for universal sentence representations" In Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC), Miyazaki, Japan, 7--12 May, 2018.

[28] B. Koçer Güldalı, K. U. İşisağ, "A comparative study on google translate: An error analysis of Turkish-to English translations in terms of the text typology of Katherina Reiss", RumeliDE Dil ve Edebiyat Araştırmaları Dergisi, 2019.

[29] T. Chen, S. Kornblith, M. Norouzi, G. Hinton, "A simple framework for contrastive learning of visual representations," arXiv: 2002.05709, 2020.

[30] F. Schroff, D. Kalenichenko, J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering", arXiv:1503.03832, 2015

[31] S.R. Bowman, G. Angeli, C. Potts, C.D. Manning, "A large annotated corpus for learning natural language inference", In Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing, Portugal, 2015.

[32] A. Williams, N. Nangia, S. Bowman, "A broad-coverage challenge corpus for sentence understanding through inference", In Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics, Vol. 1, 2018.

[33] N. Reimers, I. Gurevych, "Sentence-bert: Sentence embeddings using siamese bert networks", In Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), pp. 3982–3992, 2019.

[34] L.V.D. Maaten, G.E. Hinton, "Visualizing Data Using t-SNE", Journal of Machine Learning Research, 9, pp. 2579–2605, 2008.

Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 33-49
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Review on Architecture and Challenges in Smart Cities

Mehdi Azadimotlagh [1*], Narges Jafari [2], Reza Sharafdini [3]

[1]. Department of Computer Engineering of Jam, Persian Gulf University, Jam, Iran
[2]. Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran
[3]. Department of Mathematics, Department of Mathematics, Persian Gulf University, Bushehr, Iran

Received: 25 Oct 2024/ Revised: 04 Mar 2025/ Accepted: 05 Apr 2025

Abstract

Due to rapid urbanization, a balance between resources and urban growth is required. For the achievement of this equilibrium, the use of information technologies is essential. Smart cities are the answer to this requirement, as a result, they improve various aspects of urban life and address related challenges and/or mitigate them. Modern technologies, including a wide range of Internet of Things (IoT) sensors, are used in smart cities for collecting and analyzing data on different aspects of urban life to enhance their inhabitants' lives. Smart cities improve the sustainability and efficiency of urban dynamics. Today, smart cities can enhance services and citizens' lives in various fields such as governance, education, healthcare, transportation, and energy. Smart city applications require collaboration among individuals from various disciplines, including engineering, architecture, urban design, and economics, to plan, design, implement, and deploy a smart solution for a specific task. Therefore, a proper understanding of the applications and architecture of smart cities and the challenges they face is crucial. In this paper, we will provide background information about the applications of smart cities, describe the architecture of applications in smart cities, present security and privacy challenges to examine robustness and flexibility in smart city applications, and examine new trends in this field.

Keywords: Urban Growth; Internet of Things; Smart Utilities; Infrastructure Implementation; Security.

1- Introduction

A set of economic, environmental, and social factors has a significant impact on rapid urbanization. Therefore, economic, environmental, and social sustainability are essential to balance rapid urbanization with cities' resources. Modern technologies can improve the financial, environmental, and social aspects of urban life simultaneously, helping to overcome related challenges or mitigate them. As a result, rapid urbanization is one of the most important factors in the development of intelligent infrastructure, accelerating the need for smart cities and smart spaces [1-6].

Smart cities combine information, connectivity, and sophisticated sensors to manage municipal assets, allowing information to be sent in real time by using Internet of Things (IoT) sensors and network infrastructures. Smart city systems aim for a seamless and secure interconnection of sensors, actuators, and data processing resources to ensure efficient and reliable digital services [7-9].

Technological advances like cloud computing systems, digital devices, networks, sensor systems, and artificial intelligence (AI) capabilities are used by smart city architects to allow the elements of smart cities to coordinate and communicate with the routing protocol. In the coming years, smart cities will experience significant development, particularly in consumer, industry, and public services fields. The key goal of most of these fields is to focus on human comfort in smart homes and buildings, along with smart transportation, healthcare, education, etc. It is crucial to pay attention to security and privacy issues to achieve robustness and resilience in smart city infrastructures [5, 9-11].

This paper is organized as follows:

Section 2 provides background information on various applications of smart cities, offering in-depth insights into the technology's user-centric aspects.

Section 3 describes the architecture and implementation of smart city technology. The four-plane and five-plane

✉ **Mehdi Azadimotlagh**
m.azadim@pgu.ac.ir

architectures are introduced, followed by a detailed discussion of the latest architectural model: the six-plane architecture. Key implementation standards for each plane of this model are also outlined.
Section 4 explores the challenges of implementing smart city applications. These challenges are examined in detail across four categories: security, data management, infrastructure, and cyberattacks. At the end of this section, the role of artificial intelligence in addressing cyberattacks in smart cities is analyzed.
In the final section, an indicator for assessing the progress and comparison of smart cities is presented. An economic analysis of the necessity of transitioning toward smart cities is provided, and the section concludes by introducing the most important emerging trends for future research in the field..

2- Applications and Advantages

Intelligent cities improve the sustainability and efficiency of urban dynamics. Smart city services encompass a wide range of applications, from smart utilities to smart health, smart transportation, smart governance, and smart environment, utilizing real-time sensing, knowledge engineering, and presentation of analyzed data in an understandable format [2,7].
In the following, we review some key smart city applications like governance [12-16], home and building [8,17-20], public services [21-25], education [9,11,26-31], healthcare [32-38], business management [39-42], transportation [43-51], electricity and energy [8,17,33], clean and sustainable environment [52-55], surveillance [56-59], defense [60-63], agriculture [64-67], water management [68-69], crime tracking and detection [70-73], tourism [74-77], entertainment [1,78,79], etc.

2-1- Smart governance

For cities to become smart, we need standard frameworks and procedures for integrating technology, citizens, and governments. Smart governance, as the intelligent use of ICT to improve decision-making through better collaboration among different stakeholders, including government and citizens, can be strongly related to government approaches. Smart governance requires complex interactions between governments, citizens, and other stakeholders. Transparency, collaboration, participation, partnership, communication, and accountability are important smart governance factors that impact the quality of life in the context of smart cities. ICT-based tools, such as social media, and openness can be factors that increase citizen engagement and support smart government [14-16].

2-2- Smart Home and Smart Building

A smart environment can acquire and apply knowledge about its occupants and their surroundings for adaption to the occupants and meet comfort and efficiency goals. Smart homes and smart buildings are two representative applications within the smart environment that use an ensemble of sensors and actuators installed in homes to improve energy consumption, promote healthy lifestyles, ensure security, etc., which inevitably ties smart homes with other smart city applications such as smart grid and smart healthcare. Aside from their many advantages, smart homes are sometimes perceived by citizens as an invasion of their privacy and security [17-20,80].

2-3- Smart Public Services

The fundamental organizational framework of the intelligent city includes advances in communications, data analytics, IoT development, and a range of physical infrastructures for smart operations management. Smart cities provide many advantages to enhance the safety of the public, such as linked surveillance systems, smart roads and transportation, public safety monitoring, education, healthcare, crime tracking and detection, etc. [4,25].

2-4- Smart Education

Smart education utilizing AI has numerous potential applications, such as grading and evaluating students, predicting student retention and dropout rates, conducting sentiment analysis, providing intelligent tutoring, and monitoring and recommending systems for classrooms. Smart education in a smart city has education-hard problems and education-soft problems and ways to resolve them. The hard problems are the management of education with technology to optimize or monitor in real-time by the IoT technology the physical infrastructure, aspects related to the institutions of higher education as strategies for teaching and learning, high-tech services, the interaction between student-professor, and the design and development of multimedia contents for learning. The soft problems are the educational problems that handle information inaccurate or incomplete, with uncertainty and ambiguity, being ambiguous, volatile, poorly understood, and dynamic (education public policy, administration, decision-making, educational reforms) [11,26,29].

2-5- Smart Healthcare

In response to challenges such as population aging and the widespread outbreak of chronic diseases such as diabetes and obesity, a wide variety of smart healthcare applications employ sensing technologies with different characteristics

suitable to provide personalized and continuous monitoring. Recent technological advancements have made medical sensing possible for patients in their homes and offices. Smart healthcare systems can automatically monitor and track patients, personnel, and biomedical devices within hospitals and improve workflow efficiency in hospitals. Also, they can monitor the spread of diseases by healthcare institutions and people's reactions to environmental factors, such as pollution [9,33,34]. The conceptual system for real-time remote cardiac health monitoring proposed in [36] has reduced healthcare costs while increasing diagnostic accuracy.

2-6- Smart Business Management

Organizations across industries are increasingly utilizing AI systems to enhance their innovation processes, supply chains, marketing and sales, and other business functions. Through the implementation of AI, firms have reported efficiency gains from automation and improved decision-making due to more relevant, accurate, and timely predictions. Alibaba, one of the largest retail commerce companies in the world, provides the fundamental technology infrastructure and marketing reach to engage with its users, customers, and business partners [39-42].

2-7- Smart Transportation

By developing cities and increasing population, smart transportation has become an essential component of modern societies. Smart transportation establishes connectivity among vehicles, citizens, and infrastructure to improve road safety, reduce traffic, and increase fuel efficiency. The main motivation for developing smart transportation is to help improve the traffic flow of cities for people who want a shorter time for their daily trips. Also, smart transportation can protect pedestrians while walking in the streets or crossing the roads. For this purpose, traffic sensors are also used to detect and track pedestrian behavior [44-46, 49-51].

2-8- Smart Electricity and Energy

Given the urgent need for energy development in cities and the challenges of energy supply sources, it is crucial to address these issues. Monitoring and control programs, energy harvesting, and innovative measurement methods through smart devices are becoming increasingly important. Smart grids are revolutionizing existing electricity distribution systems due to the growing demand for energy and the expansion of new and innovative information and communication technologies (ICT), especially from an economic perspective [17] [81].

2-9- Clean and Sustainable Environment

Humanity is currently facing immense challenges related to Air pollution mitigating environmental impacts and also reduction of CO2 emissions. Traditional methods to monitor air quality are complex and costly. IoT-based pollution control systems are real-time and more precise, using faster, more cost-effective, and modern technology devices. The processing of images and AI-based systems of the IoT could lead to a major evolution in the clean energy production sector [53-55].

2-10- Smart Surveillance

The purpose of smart surveillance is to monitor people, homes, industries, offices, etc. in the absence of the user using IoT-based security surveillance systems. A great example of smart surveillance is the NATO big project namely WITNESS, which includes wide integration of sensor networks [56,57,59,82,83].

2-11- Smart Defense

Smart defense is all about creating security at a lower cost through collaboration and increased flexibility. In this approach, countries form smaller groups to pool their resources and develop capabilities that can benefit the entire alliance. Smart defense systems incorporate cutting-edge sensors, weapon systems, command and control elements, and decision-making tools to safeguard a nation against a wide range of threats. Additionally, smart cyber defense is centered on protecting against cyberattacks originating in cyberspace and enhancing defense strategies [60,62,84].

2-12- Smart Crime Tracking and Detection

Recently, information and communication technologies have been used to track and monitor crime and criminal activities in real-time online to reduce the crime rate. An IoT-based detection and tracking of criminals system aims to enable communication and collaboration between citizens and police forces in the criminal investigation process by using IoT technologies and local data computation; and distribution, along with information sharing. Using new sensors to detect criminal behavior and identify individual perpetrators; leads to deterrence and crime prevention [70,72,73].

2-13- Smart Water Management

Water quality management has gained utmost importance due to increasing pollution levels caused by industrial growth. Hence, it is essential to address the smart utilization of water resources, both from the quantity and quality perspectives [68,69].

2-14- Smart Agriculture

By utilizing the IoT and big data solutions, agricultural lands can be automatically managed, tracked, and improved in terms of operational efficiency and productivity with minimal human intervention. Generally, IoT applications for smart agriculture can be classified into seven categories; including smart monitoring, smart water management, agrochemical applications, disease management, smart harvesting, supply chain management, and smart agricultural practices [65-67].

2-15- Smart Tourism and Entertainment

Smart tourism involves the integration of innovation and information technology with tourism applications and urban infrastructure to provide solutions to tourists to meet specific travel-related needs. For example, Dubai has implemented a smart city and smart tourism platforms to interact with various stakeholders. Also, new technologies provide a framework for creating entertainment and augmented reality systems, using cloud-based technologies and real-time mobile technology interaction in various contexts [74,75,77,79].

2-16- AI-Based Smart City Applications

In a smart city application, AI techniques aim to process and identify patterns in data obtained from individual sensors or collective data generated by several sensors and provide useful insights on how to optimize underlying services. Explainable AI is particularly important in some key applications of smart cities, such as healthcare, transportation, banking, and other financial services. For instance, in transportation, AI could be used to analyze data collected from different parts of a city for future planning or deploying different transportation schemes in the city. The basic motivation of ML applications in healthcare lies in their ability to automatically analyze, identify hidden patterns, and extract meaningful clinical insights from large volumes of data, which is beyond the scope of human capabilities [85-88].

3- Smart City Applications Architecture and Implementation

The first architectural model for smart cities is a 4-layer framework comprising the sensor, transmission, data management, and application layers. In this model, security is not treated as a standalone layer but is instead integrated into each of the existing layers to ensure comprehensive protection [89]. To address the limitations of this approach, a more advanced and widely recognized architectural model has been developed. This model incorporates five key planes: sensing, communication, data, security, privacy, and the application plane, as illustrated in Figure 1. This framework builds upon the 4-layer model by introducing a dedicated security plane, enhancing the overall robustness of the architecture [9]. To improve interaction between different applications and create a unified smart city ecosystem, new definitions of smart city architecture have introduced a new abstraction layer called the business logic or management plane. This plane acts as an additional management layer placed above multiple applications within a smart city and provides support for functions like device management, local network topology management, and traffic and congestion management. Its main goal is to enhance communication between these applications and ensure efficient management of the smart city, which includes monitoring system performance and addressing any issues that may arise [90].

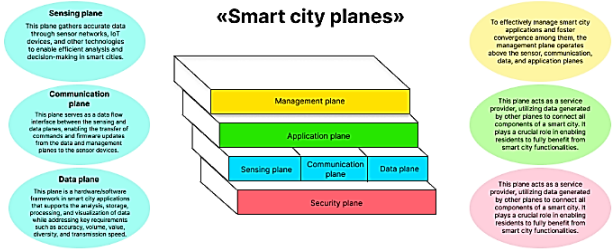


Fig 1. A High-Level Representation of the Smart City Six Planes Architecture

Although each plane has its standards for implementation in smart cities, the most crucial frameworks for developing and implementing smart cities are ITU-T Y.4000, ISO 37120, IEEE P1950.1, IEEE P2413.1, and the IES-City Framework from NIST.
The following subsections will delve into the architecture and significance of the sixth plane.

3-1- Sensing Plane

Collecting the correct data necessary for efficient analysis and decision-making in smart cities is a challenging and intricate task. This typically involves utilizing various components such as sensor networks, IoT devices, and more. Sensors can gather data from different smart city devices in various formats and can be applied in diverse scenarios. At the implementation level of this plane, sensors are generally divided into two categories. The first category includes dedicated sensors, such as humidity, temperature, and imaging sensors, which are designed to collect data for specific parameters. The second category comprises non-dedicated sensors, such as infrared, FID, and GPS sensors, which are capable of collecting and transmitting a variety of data types. In the field of sensors, we encounter three generations of these devices. The initial generation consisted of a limited number of sensor devices per application. The second generation was mainly influenced by the introduction of data fusion, enabling valuable insights to be derived by merging data from a wide array of sensors. The most recent (third) generation now integrates

information from external sources like databases, research, and external applications [9,89].
However, sensing in smart cities encounters several challenges, with the inadequate power supply being the primary cause of many of these obstacles. While energy harvesting techniques can alleviate this issue, their effectiveness in meeting other requirements such as cost, portability, and size is still limited. Additionally, the sensor plane is plagued by high fragmentation and heterogeneity, which complicates ensuring interoperability and scalability. The maturation of population sensing solutions can address many of these needs. Despite advancements in data processing and communication techniques contributing to this progress, the sensor plane itself has seen significant enhancements. Particularly, improvements in VLSI design have consistently decreased the power consumption and cost of sensors while enhancing their on-node computing capabilities [9].

3-2- Communication Plane

In the sensor plane, a network of connected devices collects data. After the data collection, it needs to be sent to the destination. Besides, the connected devices also need to communicate with others. The communication plane acts as a data flow interface between the sensing and data planes, facilitating the flow of commands and firmware updates from the data and management planes to the sensor devices. At the implementation level, the communication plane's functionality is divided into two components: the front-end and the back-end. The front-end establishes connections between sensor devices and focal points, such as access points or gateways. It encompasses local wireless networks, local wired networks, and backhaul networks. The back-end, on the other hand, provides communication links between these focal points and a centralized cloud-based or distributed edge-based data plane. This component handles the adoption, aggregation, and preprocessing of data.
The functionality of this plane can also be divided into three fields: (1) The first functional field is in-field communication, which involves resource-constrained sensor nodes to collect raw data and send it to in-field gateways or access points via wireless or wired connections. (2) The second functional field is the aggregation and adaptation capability, which involves cluster heads, gateways, and access points that have relatively more computational power than field sensors. The adaptation capability bridges the heterogeneous network technologies that exist in a typical smart city implementation. It ensures interoperability with the Internet, through which access to the cloud and its various services is provided. Finally, the third functional field is the network application component, which standardizes the message exchange between centralized or distributed cloud-based or edge-based servers and field devices, regardless of their vendor, topology, and functionality. The sending/receiving of data takes place at the transport layer, and the communication technology for communication can be divided into two primary modes. The first mode is short-range communication, which is suitable for various low-power sensor networks. The second mode is long-range communication, which is suitable for communication between ordinary smart devices such as mobile devices and various smart wired and wireless devices [9,89,91]. The most important IoT communication standards and protocols are MQTT, CoAP, LoRaWAN, Sigfox, Thread, Bluetooth, and BLE. Also, the most important IoT Networking Standards and protocols are 6LoWPAN, IPv6, and Thread.

3-3- Data Plane

Various smart city infrastructures continuously generate data. Data analysis is one of the most important features and functions of sustainable smart cities. The data plane is a hardware/software framework in smart city applications that enables the analysis, storage, processing, and visualization of data by observing data requirements such as accuracy, volume, value, diversity, and speed of transmission. Ultimately, it provides machine intelligence for smart city managers and residents, helping them make informed decisions in program implementation. Data collected from various sources must be cleaned and processed before use. Given the large volume of data generated in a smart city and the increasing amount of data, processing, storing, and maintaining them is a significant challenge; therefore, smart city infrastructures must be scalable. Data visualization can help smart city users and administrators understand the information extracted from the smart city. Machine learning and deep learning algorithms can be used to extract useful information from raw data. In an integrated smart city, effective and coherent visualization of data is crucial and challenging due to the wide range and differentiation of applications [9,92,93].
Two common approaches to data plane implementation are centralized cloud-based and distributed edge-based implementations. The former often offers superior management, usability, and reliability, while the latter usually excels in scalability and latency by reducing the physical distance between field devices and the data plane [89,94]. For example, the infrastructure monitoring system proposed in [95]. adopts a cloud-based architecture to meet core requirements such as large-scale data, real-time processing, and reliability, using replication techniques to enhance system robustness against occasional failures [96]. also proposes an edge-based platform with embedded scheduling techniques that reduce energy demand and provide quality service assurance. This solution allows participants to share their storage and processing resources through a Peer-to-Peer (P2P) network. The most important

IoT data and semantic standards and protocols are JSON, XML, RDF, and OWL.

3-4- Application Plane

The design of smart city services begins with defining applications. Other planes are then deployed to meet the needs of this application plane, from data collection to analysis. The application plane, as a service provider based on data generated by other planes, is crucial for users. This plane connects all components of a smart city so residents can enjoy the benefits of a smart city. The analyzed data from other planes is presented here as decisions. While people may not be aware of how applications work or the algorithms used for data collection and analysis, they can interact with the application plane to view final results and benefit from smart city services. These results include smart health services, smart energy, smart waste management, smart agriculture, smart education, and more. It's important to note that the efficiency of many smart city applications can be evaluated through this plane. If a program cannot effectively communicate with smart city users, even if it presents accurate results, it won't be utilized effectively. Therefore, a proper and user-friendly design of this plane is crucial [9,89]. Also, the most important IoT application layer standards and protocols are AMQP, LwM2M, XMPP, SSI, CoAP, MQTT, DDS, SMS/SMPP, USSD, and HTTP.

3-5- Management Plane

To optimally manage smart city applications and create convergence between different applications, the management plane sits on top of other sensor, communication, data, and application planes. In addition to device management, this plane also supports local network topology management, traffic, and congestion management. Its main goal is to increase communication between these applications and ensure efficient smart city management, including monitoring system performance and addressing any arising issues. The tasks of this plane are generally divided into two categories: Information Technology Service Management (ITSM) and Enterprise Business Service Management (ESM).

ITSM at three macro levels includes the strategy for delivering smart city services, reporting and dashboarding, and continuous service development. At a more granular level, tasks such as change management, service requests, project management, service asset management, asset management, service portfolio management, and service knowledge and catalog management constitute its components. ESM involves collaboration, follow-up, and improvement. Although at a more granular level, these components are similar to the IT service management level, issues are addressed from the perspective and framework of the organization and business rather than from an IT perspective [90,97]. The most important IoT device management standards and protocols are OMA-DM, OMA LWM2M, and AMQP.

3-6- Security Plane

The security plane of smart cities is situated alongside all the other smart city planes to ensure security. Each plane shown in Figure 1 requires mechanisms to guarantee security and privacy. The challenging task of meeting these requirements falls to the security plane. Many of these challenges stem from the security issues present in traditional information and communication systems used in other planes. Each smart city plane is made up of a variety of embedded cyber-physical systems, shared communication and computing infrastructures, and distributed systems. This diversity is a major factor contributing to the security challenges faced by smart cities. As a result, smart cities are increasingly vulnerable to cyber attacks, which can originate from both internal and external sources, underscoring the importance of security and privacy considerations. Designing an effective security plane necessitates comprehensive solutions that address the unique challenges faced by each plane. Some of these challenges include the susceptibility of the application plane to spoofing attacks due to its role in data collection and usage. The sensing plane is often vulnerable to attacks on the limited power capacity of sensors, given the challenges of power and energy provision. The communication plane requires security solutions that take into account the interoperability and coexistence of different communication technologies. The data plane manages a vast amount of heterogeneous, unstructured data stored in the cloud or at the mobile edge, inheriting security issues from cloud-based systems. Additionally, the management plane encounters authentication challenges [9,84,98-105]. In general, implementing services such as authentication, identification, access control, privacy, and data integrity are all related to this plane. The most important IoT Security Standards and protocols are TLS/SSL, DTLS, ECC, OAuth, and X.509.

4- Challenges

Smart city applications typically include a wide variety of sensing devices, leading to heterogeneity in sensing, communication, data, and security planes. Ensuring interoperability among these components and integrating them with existing infrastructure are major challenges in these applications [34]. Generally, challenges in the field of smart city applications can be classified into four categories:

1) Security challenges
2) Data-related challenges
3) Infrastructure challenges
4) Attacks

In the following section, these categories will be reviewed.

4-1- Security Challenges

Security challenges include integrity, availability, privacy, confidentiality, authentication, responsibility, and reliability which we must pay attention to in smart city applications [106-109]. In the following, the security challenges are reviewed.

4-1-1- Integrity

Data must be accurate and not easily accessible. This also includes protecting against external tampering [4].

4-1-2- Availability

Reliable real-time access is needed to monitor the different elements of the smart city infrastructure [4].

4-1-3- Privacy

The biggest challenge in human-centric smart city applications is ensuring the privacy of citizens, which is their fundamental right [1,107].

4-1-4- Confidentiality

Sensitive information must be kept private and secure against unauthorized access. This may include the deployment of firewalls or data anonymization [4].

4-1-5- Authentication

Continuous authentication and verification are essential for participating devices in smart city applications. Hybrid solutions combine behavioral pattern recognition with conventional biometrics-based hard authentication techniques to address this challenge [110].

4-1-6- Responsibility

System users must be responsible for their activities and interactions with sensitive data systems. User logs should document who accesses the information to provide accountability if issues arise [4].

4-1-7- Reliability

Reliability is defined as the probability that a product, system, or service will perform its intended function adequately for a specified period or operate in a defined environment without failure.

4-2- 4-2- Data-Related Challenges

Several challenges are associated with the collection, storage, sharing, ensuring, and maintaining the quality of data [1]. In the following, data-related challenges are reviewed.

4-2-1- Data ownership

people discuss data ownership, they really mean this key role in the data governance framework. They are not the only roles in a data governance framework, but they are the senior people who will make the data governance framework work.

4-2-2- Quality of Data

The quality of data in smart city applications largely depends on the accuracy of the IoT devices and sensors used for collecting data. Therefore, it should be ensured that the data infrastructure is accurate and error-free [111].

4-2-3- Diversity/Characteristics of the Data

In smart city applications, data is collected through several devices, making it challenging to understand the characteristics of the data for removing outliers [112].

4-2-4- Data Auditing

Data auditing involves assessing data to analyze whether the available data is suitable for a specific application, and the risks associated with poor data [1,113].

4-2-5- Informed Consent

Informed consent, which is the process of informing and obtaining participants's consent for data collection, is a key element of data ethics [1].

4-2-6- Data Biases

Datasets generally contain different types of hidden biases, either due to the collector or the respondent, in the collection phase, which are challenging to undo and have a direct impact on the analysis [106]. Various data biases can result in detrimental AI predictions in sensitive human-centric applications. For instance, algorithmic predictions may be biased against certain races and genders, as reported in [114,115]. Intentional and unintentional bias in AI decisions is even more dangerous, which might endanger citizens' lives in healthcare or law enforcement applications. For example, AI-based software used for future criminal predictions was found biased against blacks [1,115].

4-2-7- Interpretation

A key challenge to deploying AI in smart city applications is the lack of interpretability, which results in humans being unable to understand the causes of an AI model's decision [116]. Interpretability is a set of features fed to an AI algorithm, which learns from data by identifying hidden patterns and producing predictions. It is a key characteristic

of AI models deployed in smart city applications [116,117]. For better results, the data used for training an AI model should be interpretable [1].

4-2-8- Open Data

For transparency and developing trust, the data and insights obtained from the data should be openly accessible [1,118].

4-3- Infrastructure Challenges

Infrastructure challenges and security challenges include items such as a constrained environment, robustness to noise and interference, low-delay connectivity, and processing and battery efficiency of smart mobile devices. In the following, the security challenges are reviewed.

4-3-1- Constrained Environment:

Devices, in smart city applications, including data collection sensors and data transfer networks generally have limited resources (i.e., storage, bandwidth, and processing power) [111,119].

4-3-2- Robustness to Noise and Interference

Noise robustness is the capability of an application to maintain its performance despite noise and interference during activity.

4-3-3- Low-Delay Connectivity and Processing,

In user experience, delays of even a fraction of a second can determine success or failure, especially in the IoT as connected devices become more common. Users expect near-zero lag between user input and onscreen output. This requirement is more about humans than modern computers. While the device and its connection determine how quickly user input is reflected on the screen, humans are highly sensitive to response delays [120].

4-3-4- Battery Efficiency of Smart Mobile

Modern mobile devices that connect people consume a lot of battery for sensing and communication capabilities. Various sensors, high-resolution LCDs, wireless interfaces, GPS, and other advanced features drain batteries quickly, reducing operational time. Managing battery life in mobile devices is crucial and requires addressing ways to efficiently utilize battery life at hardware and software levels [121,122].

4-4- Attacks

The increased use of Smart Cities creates new attack opportunities for adversaries to gain access to or carry out disruptive attacks against local government and critical infrastructure networks. Security is one of the main concerns in smart city applications. AI has its unique security issues where a small modification in inputs or data consumed by AI algorithms might change the decision of AI models and cause serious consequences [1]. Intelligent city technology depends heavily on wireless IP networks that are increasingly susceptible to hackers [4]. AI models can be vulnerable to different kinds of attacks, such as adversarial examples, model extraction attacks, backdooring attacks, Trojan attacks, membership inference, and model inversion [123].

For instance, attackers can launch different types of adversarial attacks on AI models to affect their predictive capabilities and bias the decisions [124,125]. Attacks in sensitive application domains such as connected autonomous vehicles can lead to significant loss in terms of human lives and infrastructure [124]. For example, an adversarial attacker could potentially take control of an autonomous car on a highway and demand money to restart it. They could also halt a train on the platform just before the next train is scheduled to arrive [125]. In the following, some of the most important attacks are introduced:

1) Man-in-the-middle attacks
2) Data poisoning
3) Evasion attacks
4) Adversarial attacks
5) Trojan attacks
6) Model stealing (model extraction)
7) Membership inference attacks

4-4-1- Man-in-the-Middle Attacks

Manipulation of messages from a sender to a receiver, with the action being unnoticed by neither end, is termed a man-in-the-middle attack that has also been called manipulation attacks with the advent of the IoT concept. The most effective type of manipulation attack aims at manipulating the network layer immediately at the time when a new device is introduced to the network. As IoT is implemented in a distributed mobile environment, this makes IoT networks especially vulnerable [126-129].

In smart city applications, the session key establishment procedure is an open target for man-in-the-middle attacks. To address this vulnerability, a secure access control method with the objective of session key establishment based on a mutual authentication between a sender and a receiver and ECC encryption at the lower layer is proposed [130]. Network encryption, authentication and key management, identity verification, symmetric or asymmetric data encryption, and digest algorithms are the most effective solutions to answer smart city network layer security issues [131].

4-4-2- Data Poisoning Attack

In these attacks, adversaries intentionally manipulate training data, e.g., incorrect labels, to degrade model performance have control over the training data, or can contribute to it. They inject malicious perturbations into datasets, potentially leading to inaccurate results in offline learning and real-time decision-making processes. These attacks are an emerging threat as machine learning becomes widely deployed in AI applications [132-135].

4-4-3- Evasion Attacks

Compared to data poisoning, evasion attacks can take place after model training. In typical evasion attacks, an adversary perturbs a legitimate input to craft an adversarial sample that tricks a victim model into making an incorrect prediction. An evasion attack happens when the network is fed an “adversarial example” —a carefully perturbed input that looks and feels the same as its untampered copy to a human— but that completely throws off the classifier. Evasion attacks alter model behavior, usually to benefit the attacker [1,136].

4-4-4- Adversarial Attacks

This challenge has been recognized and discussed for crafting fake data that could belong to different domains: text [137], images [138], audio [139], and network signals [140], known as adversarial examples, or evaluating and developing solutions against this security threat [141]. Adversarial attacks are considered severe security threats in learner-based models due to their possible consequences. In smart cities and collaborations of data-driven applications and devices, the impact of misleading a model, e.g., a classifier, could result in harsh situations and a costly mess [1,142].

4-4-5- Trojan Attacks

Trojan attacks on AI algorithms are also very common in cloud and edge deployments of AI [143,144]. A Trojan Horse virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software. Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable file should be implemented and the program installed for the Trojan to attack a device’s system [145,146].

4-4-6- Model Stealing (Model Extraction)

The goal of model stealing (extraction) attacks is to steal the parameters or functionality of a confidential model. Model extraction is typically achieved by querying the confidential model and learning from its responses [147,148]. This occurs when an attacker gains access to the model's parameters. The ultimate objective of the adversary is to clone or reconstruct the target model, reverse engineer a black-box model, or compromise the nature and properties of the training data [149,150].

4-4-7- Membership Inference Attacks

In such attacks, the attackers do not necessarily need knowledge about the parameters of an AI model. Instead, knowledge of the type and architecture of the model and/or the service used for developing the model is used to launch an attack [1]. This attack allows an adversary to query a trained machine-learning model to predict whether or not a particular example was contained in the model’s training dataset. During this attack, an attacker tries to determine if you have used a particular person’s personal information to train a machine learning model, to access the person’s personal information [151-153].

4-5- Applications of AI in Responding to Cyber-Attacks in Smart Cities

Here are some ways AI can be used to defend against attacks in smart cities:

4-5-1- Improving the Efficiency of Intrusion Detection Systems (IDS)

Intrusion detection involves identifying and monitoring unauthorized access attempts to an information system. IDS, which can be hardware or software-based, continuously monitors network activity to identify unusual patterns and security risks to prevent cyberattacks. These systems consist of three main components: sensors for collecting data across the network, an analytics engine for processing the collected data, and a reporting system to alert administrators to potential threats and attacks. One challenge of IDS is reporting false positives of cyberattacks. False positives occur when traffic passing through the IDS is detected as a cyberattack when it is not, reducing their accuracy, efficiency, and reliability. By using AI and machine learning algorithms, it is possible to reduce false positives by improving the accuracy of intrusion detection systems and identifying unusual patterns and potential threats in real-time. These systems use machine learning to continuously learn and adapt to new threats, and AI-enhanced machine learning IDS algorithms to analyze network traffic patterns and detect anomalies that may indicate a cyberattack. AI-based IDS with intelligent

architectural frameworks can address security and privacy challenges in smart cities [154-156].

4-5-2- Attack Detection Frameworks

AI-based frameworks, such as the MDATA model, can enhance multi-stage attack detection capabilities by utilizing dynamic cognition based on spatio-temporal data. These models can identify attack patterns at various stages and gather events from different sources, allowing for a comprehensive understanding of security events. They can also assess the severity and impact of threats to prioritize and issue alerts [155].

4-5-3- Cybersecurity Defense Mechanisms

By integrating AI and cyber defense strategies such as software-defined networks (SDN) and fog computing, it is possible to overcome the challenges of resource limitations in smart city IoT equipment and create strong security. Fog computing, which complements cloud computing, utilizes end devices for data processing and storage. SDN is a network architecture approach that is intelligently and centrally controlled and programmed using software programs. In these networks, intelligence separates the network from the hardware, allowing for continuous and comprehensive management regardless of the network background technology. Therefore, by using AI at the edge of the network and relying on fog computing and SDN, it is possible to increase processing speed, enhance threat detection capabilities, and automatically respond to threats [157] [158,159].

4-5-4- Machine Learning Techniques

Techniques such as deep learning and support vector machines (SVM) are advanced methods for detecting cybersecurity attacks that can be effective in identifying and mitigating threats in IoT environments. Deep learning is used to identify complex patterns and detect sophisticated attacks, in which neural networks analyze large volumes of data. Given the power of SVM to classify data points into different categories, it is possible to distinguish between normal and malicious activities. Machine learning models can also identify potential threats by detecting deviations from normal behavior [154] [156].

5- Comparison of Smart Cities and New Trends

According to the 2023 report of the International Society for Urban Informatics on the ranking of smart cities, six indicators have been considered for comparing smart cities. These indicators include smart mobility, smart living, smart environment, smart people, smart government, and smart economy .

The goal of the smart mobility index is to benefit from a smart transportation system that is efficient, economical, safe, and environmentally friendly. The goal of the smart living index is to benefit from smart technologies to improve the living conditions of citizens and create a comfortable, safe, and healthy life. The smart environment reflects the creation of a balance between the city, nature, and residents based on smart technologies. The smart people index relies on creating a suitable environment for citizenship in a way that promotes favorable physical, mental, educational, and cultural states for citizens. The smart government index relies on the use of information technology-based services and systems to provide integrated services to the people by the government. The smart economy index refers to the use of new technologies to increase the efficiency of human resources, sustainability of economic development, and social welfare .

According to the above indicators, the top 10 smart cities in the world are, in order: Copenhagen, Stockholm, Helsinki, Berlin, New York, Toronto, Zurich, Oslo, Hong Kong, and London [97].

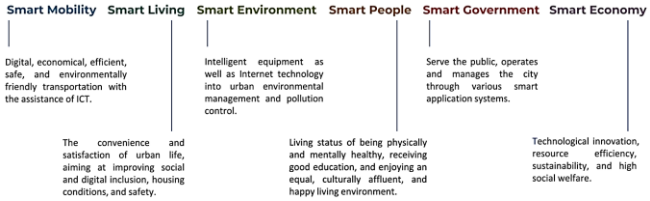


Fig. 2 Smart City Index Framework [97]

A review of the economic and industrial development strategies of industrialized, developed, and developing countries ssuch as the USA, Germany, France, Japan, China, South Korea, India, Indonesia, Turkey and the UAE highlights that smartization of industry has become one of the most critical components of competitive advantage and global market leadership. However, achieving this is impossible without prioritizing the development of smart city infrastructure. Studies indicate that companies and industries failing to take significant steps in this direction risk losing a substantial share of their market soon and may even face complete market exit.

To analyze future trends in the field of smart cities, we use analyses conducted by reputable institutions such as Gartner, Forbes, and Deloitte. In recent years, we have seen a growing use of AI for planning and service delivery in urban areas. This includes data analysis, more efficient resource allocation, predictive modeling, and providing critical real-time alerts to citizens. Given the increasing world population and water shortages in many regions of the world, the use of technological solutions to solve this challenge is of great interest in the coming years. Technologies that are used to manage water collection, storage, and use, consumption management, as well as

predicting availability, recycling, distribution, and desalination are of great interest. As cities become smarter, digital citizenship will become increasingly important, and governments will have programs to verify digital identities and use them to provide services such as applying for permits, receiving welfare payments, and paying taxes. Smart transportation infrastructure will gain momentum in the future to solve traffic problems, and air pollution, increase travel safety, and
move toward a healthier city. Digital twins are a virtual representation of physical assets using real-world data that can predict how components or systems will behave in the real world. The concept will have widespread application in predictive maintenance in industry and will develop rapidly. In the coming years, smart healthcare will grow rapidly, relying on digital technologies to enhance the quality of healthcare and expedite the prevention, diagnosis, and treatment of diseases. Advanced cities such as Singapore, Helsinki, and Dublin are also implementing digital twin projects on a city scale. Advanced smart cities like Rotterdam and New York will utilize IoT technologies to address instability, extreme changes, and weather events such as storms, floods, fires, and droughts. This will enable them to more effectively respond to and overcome these challenges [160] [161] [162]

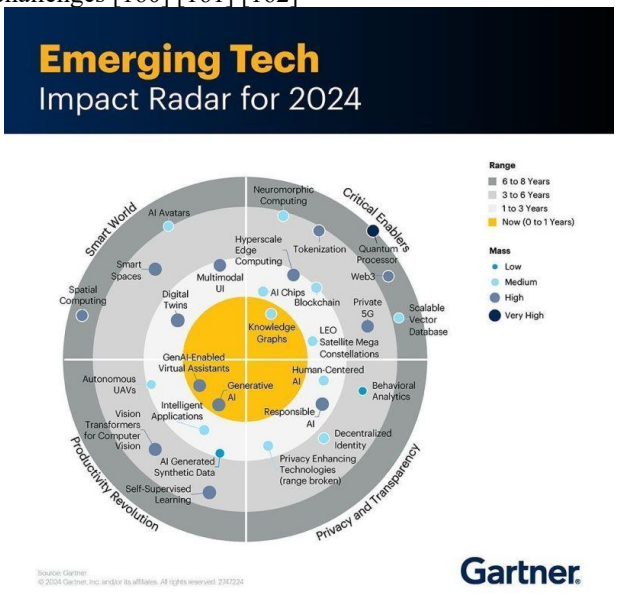


Fig 3. Gartner Emerging Tech Impact Radar for 2024 [159]

In its 2024 Technology Outlook report, Gartner ranks the smart world among the most popular emerging technologies that will experience high growth in the next 1 to 8 years and will create major changes in the use of new technology. Accordingly, figure 3, in the next 1 to 3 years, the use of digital twins in industry to improve the quality of products based on real customer data, as well as the use of multi-model user interfaces to increase human-computer interaction, will grow rapidly. In the next 3 to 6 years, integrated smart cities and AI avatars will also see significant development. In the next 6 to 8 years, [160]

6- Conclusion

Considering the lack of urban resources and the rapid growth of the population of cities, it is inevitable to move towards the increasing development of various services based on the IoT and the emergence of smart cities. Smart cities will have strong development in the coming years, but now in some related areas, great changes have taken place. In this paper, various applications of smart cities such as governance, healthcare, education, transportation, agriculture, energy, surveillance, etc. were reviewed, and it was shown that the scope of smart cities can encompass all aspects of life. To get a proper understanding of the implementation framework of smart city applications, their 5-plane architectures were reviewed. Various aspects of the security and privacy of smart city applications are requirements for their robustness and resilience, which were reviewed in the last part of this paper. New trends can motivate further studies in this area. The main point of this paper is that moving towards smart cities is not just an option, but a technological necessity. In the next decade, countries, cities, companies, and industries that make substantial progress towards becoming smarter will prosper, while those that fall behind risk being left out of competition.

References

[1] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. Al-Fuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges," Computer Science Review, vol. 43, p. 100452, 2022/02/01/ 2022, doi: https://doi.org/10.1016/j.cosrev.2021.100452.

[2] A. Gharaibeh et al., "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2456-2501, 2017, doi: 10.1109/COMST.2017.2736886.

[3] B. Green, The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future. The MIT Press, 2019.

[4] I. A. Mohammed, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," SSRN Electronic Journal, vol. 8, pp. 55-59, 01/03 2020.

[5] A. AlDairi and L. a. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," Procedia Computer Science, vol. 109, pp. 1086-1091, 2017/01/01/ 2017, doi: https://doi.org/10.1016/j.procs.2017.05.391.

[6] T. Guelzim, M. Obaidat, and B. Sadoun, "Introduction and overview of key enabling technologies for smart cities and homes," 2016, pp. 1-16.

[7] H. Habibzadeh, Z. Qin, T. Soyata, and B. Kantarci, "Large-Scale Distributed Dedicated- and Non-Dedicated Smart City Sensing Systems," IEEE Sensors Journal, vol. 17, no. 23, pp. 7649-7658, 2017, doi: 10.1109/JSEN.2017.2725638.

[8] B. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," Sensors, vol. 18, no. 3, p. 817, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/3/817.

[9] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design," Computer Networks, vol. 144, pp. 163-200, 2018/10/24/ 2018, doi: https://doi.org/10.1016/j.comnet.2018.08.001.

[10] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," Journal of Advanced Research, vol. 5, no. 4, pp. 491-497, 2014/07/01/ 2014, doi: https://doi.org/10.1016/j.jare.2014.02.006.

[11] M. Caţă, "Smart university, a new concept in the Internet of Things," in 2015 14th RoEduNet International Conference - Networking in Education and Research (RoEduNet NER), 24-26 Sept. 2015 2015, pp. 195-197, doi: 10.1109/RoEduNet.2015.7311993.

[12] M. Razaghi and M. Finger, "Smart Governance for Smart Cities," Proceedings of the IEEE, vol. 106, no. 4, pp. 680-689, 2018, doi: 10.1109/JPROC.2018.2807784.

[13] S. Y. Tan and A. Taeihagh, "Smart City Governance in Developing Countries: A Systematic Literature Review," Sustainability, vol. 12, no. 3, p. 899, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/3/899.

[14] G. Pereira, P. Parycek, E. Falco, and R. Kleinhans, "Smart governance in the context of smart cities: A literature review," Information Polity, vol. 23, pp. 1-20, 05/14 2018, doi: 10.3233/IP-170067.

[15] J. C. F. De Guimarães, E. A. Severo, L. A. Felix Júnior, W. P. L. B. Da Costa, and F. T. Salmoria, "Governance and quality of life in smart cities: Towards sustainable development goals," Journal of Cleaner Production, vol. 253, p. 119926, 2020/04/20/ 2020, doi: https://doi.org/10.1016/j.jclepro.2019.119926.

[16] A. Khanna et al., "Blockchain: Future of e-Governance in Smart Cities," Sustainability, vol. 13, no. 21, p. 11840, 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/21/11840.

[17] M. Collotta and G. Pau, "A Novel Energy Management Approach for Smart Homes Using Bluetooth Low Energy," IEEE Journal on Selected Areas in Communications, vol. 33, no. 12, pp. 2988-2996, 2015, doi: 10.1109/JSAC.2015.2481203.

[18] M. Daher, A. Diab, M. E. B. E. Najjar, M. A. Khalil, and F. Charpillet, "Elder Tracking and Fall Detection System Using Smart Tiles," IEEE Sensors Journal, vol. 17, no. 2, pp. 469-479, 2017, doi: 10.1109/JSEN.2016.2625099.

[19] J. Zhang, Y. Shan, and K. Huang, "ISEE Smart Home (ISH): Smart video analysis for home security," Neurocomputing, vol. 149, pp. 752-766, 2015/02/03/ 2015, doi: https://doi.org/10.1016/j.neucom.2014.08.002.

[20] E. Zeng, S. Mare, and F. Roesner, "End user security & privacy concerns with smart homes," presented at the Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, Santa Clara, CA, USA, 2017.

[21] R. Batayneh, N. Taleb, R. Said, M. Alshurideh, T. Ghazal, and H. Alzoubi, IT Governance Framework and Smart Services Integration for Future Development of Dubai Infrastructure Utilizing AI and Big Data, Its Reflection on the Citizens Standard of Living. 2021, pp. 235-247.

[22] Q. Hu and Y. Zheng, "Smart city initiatives: A comparative study of American and Chinese cities," Journal of Urban Affairs, vol. 43, pp. 1-22, 01/08 2020, doi: 10.1080/07352166.2019.1694413.

[23] K. Löfgren and C. W. R. Webster, "The value of Big Data in government: The case of 'smart cities'," Big Data & Society, vol. 7, no. 1, p. 2053951720912775, 2020, doi: 10.1177/2053951720912775.

[24] F. T. Hartanti, J. H. Abawajy, M. Chowdhury, and W. Shalannanda, "Citizens' Trust Measurement in Smart Government Services," IEEE Access, vol. 9, pp. 150663-150676, 2021, doi: 10.1109/ACCESS.2021.3124206.

[25] j. zare and R. Hendijani, "E-Government Service Supply Chain: Identifying Performance Evaluation Indicators (Case Study of e-Customs System in Iran)," (in Fa), Journal of Information and Communication Technology, vol. 14, no. 53, pp. 111-139, 2023. [Online]. Available: https://www.magiran.com/paper/2551823.

[26] K. Ahmad et al., Artificial Intelligence in Education: A Panoramic Review. 2020.

[27] Y. Kim, T. Soyata, and R. F. Behnagh, "Towards Emotionally Aware AI Smart Classroom: Current Issues and Directions for Engineering and Education," IEEE Access, vol. 6, pp. 5308-5331, 2018, doi: 10.1109/ACCESS.2018.2791861.

[28] Z. Asadi, M. Abdekhoda, and H. Nadrian, "Understanding and predicting teachers' intention to use cloud computing in smart education," Interactive Technology and Smart Education, vol. ahead-of-print, 09/11 2019, doi: 10.1108/ITSE-05-2019-0019.

[29] O. Díaz-Parra et al., "Smart Education and future trends," International Journal of Combinatorial Optimization Problems and Informatics, vol. 13, no. 1, pp. 65-74, 01/27 2022. [Online]. Available: https://ijcopi.org/ojs/article/view/294.

[30] S. Ar, S. Panda, and S. Hanumanthakari, "Enabling Smart Education System Using Blockchain Technology," 2021, pp. 169-177.

[31] R. J. H. Vladimir L. Uskov, Lakhmi C. Jain, Smart Education and e-Learning - Smart Pedagogy Springer.

[32] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and Robust Machine Learning for Healthcare: A Survey," (in eng), IEEE Rev Biomed Eng, vol. 14, pp. 156-180, 2021, doi: 10.1109/rbme.2020.3013489.

[33] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications," in 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 6-8 Aug. 2018 2018, pp. 140-145, doi: 10.1109/W-FiCloud.2018.00028.

[34] L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015, doi: 10.1109/JIOT.2015.2417684.

[35] Y. Ren, R. Werner, N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," IEEE Wireless Communications, vol. 17, no. 1, pp. 59-65, 2010, doi: 10.1109/MWC.2010.5416351.

[36] A. Page, M. Hassanalieragh, T. Soyata, M. K. Aktas, B. Kantarci, and S. Andreescu, "Conceptualizing a Real-Time Remote Cardiac Health Monitoring System," in Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, T. Soyata Ed. Hershey, PA, USA: IGI Global, 2015, pp. 1-34.

[37] O. Kocabas, T. Soyata, J. P. Couderc, M. Aktas, J. Xia, and M. Huang, "Assessment of cloud-based health monitoring using Homomorphic Encryption," in 2013 IEEE 31st International Conference on Computer Design (ICCD), 6-9 Oct. 2013 2013, pp. 443-446, doi: 10.1109/ICCD.2013.6657078.

[38] A. Page, S. Hijazi, D. Askan, B. Kantarci, and T. Soyata, "Research Directions in Cloud-Based Decision Support Systems for Health Monitoring Using Internet-of-Things Driven Data Acquisition," International Journal of Services Computing, vol. 4, pp. 18-34, 04/01 2016.

[39] A. Leszkiewicz, T. Hormann, and M. Krafft, "Smart Business and the Social Value of AI," in Smart Industry – Better Management, vol. 28, T. Bondarouk and M. R. Olivas-Luján Eds., (Advanced Series in Management: Emerald Publishing Limited, 2022, pp. 19-34.

[40] J. Mendling, B. Baesens, A. Bernstein, and M. Fellmann, "Challenges of smart business process management: An introduction to the special issue," Decision Support Systems, vol. 100, pp. 1-5, 2017/08/01/ 2017, doi: https://doi.org/10.1016/j.dss.2017.06.009.

[41] B. Leavy, "Alibaba strategist Ming Zeng: “Smart business” in the era of business ecosystems," Strategy & Leadership, vol. 47, no. 2, pp. 11-18, 2019, doi: 10.1108/SL-01-2019-0006.

[42] K. Ćurko, T. Ćurić, and V. Vuksic, "Perspective of smart enterprises development in the Republic of Croatia," WSEAS Transactions on Business and Economics, vol. 14, pp. 378-390, 01/01 2017.

[43] M. Veres and M. Moussa, "Deep Learning for Intelligent Transportation Systems: A Survey of Emerging Trends," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 8, pp. 3152-3168, 2020, doi: 10.1109/TITS.2019.2929020.

[44] C. Kaptan, B. Kantarci, T. Soyata, and A. Boukerche, "Emulating Smart City Sensors Using Soft Sensing and Machine Intelligence: A Case Study in Public Transportation," in 2018 IEEE International Conference on Communications (ICC), 20-24 May 2018 2018, pp. 1-7, doi: 10.1109/ICC.2018.8422969.

[45] S. Munder, C. Schnorr, and D. M. Gavrila, "Pedestrian Detection and Tracking Using a Mixture of View-Based Shape–Texture Models," IEEE Transactions on Intelligent Transportation Systems, vol. 9, no. 2, pp. 333-343, 2008, doi: 10.1109/TITS.2008.922943.

[46] Z. Karami and R. Kashef, "Smart transportation planning: Data, models, and algorithms," Transportation Engineering, vol. 2, p. 100013, 2020/12/01/ 2020, doi: https://doi.org/10.1016/j.treng.2020.100013.

[47] R. Sahal, S. H. Alsamhi, K. N. Brown, D. O’Shea, C. McCarthy, and M. Guizani, "Blockchain-Empowered Digital Twins Collaboration: Smart Transportation Use Case," Machines, vol. 9, no. 9, p. 193, 2021. [Online]. Available: https://www.mdpi.com/2075-1702/9/9/193.

[48] C. Zhao, K. Wang, X. Dong, and K. Dong, "Is smart transportation associated with reduced carbon emissions? The case of China," Energy Economics, vol. 105, p. 105715, 2022/01/01/ 2022, doi: https://doi.org/10.1016/j.eneco.2021.105715.

[49] R. A. Gonzalez, R. E. Ferro, and D. Liberona, "Government and governance in intelligent cities, smart transportation study case in Bogotá Colombia," Ain Shams Engineering Journal, vol. 11, no. 1, pp. 25-34, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.asej.2019.05.002.

[50] M. Ehteshami, M. Cheraghali, B. Tabrizian, and M. Teimourian, "Identifying and ranking factors affecting the digital transformation strategy in Iran's road freight transportation industry focusing on the Internet of Things and data analytics," Journal of Information and Communication Technology, vol. 15, pp. 1-20, 09/26 2022, doi: 10.61186/jict.42076.16.59.1.

[51] R. Bahri and s. zeynali, "Energy procurement of a cellular base station in independent microgrids with electric vehicles and renewable energy sources: Mixed-integer nonlinear programming model," (in Fa), Journal of Information and Communication Technology, vol. 15, no. 57, pp. 266-282, 2023. [Online]. Available: https://www.magiran.com/paper/2640169.

[52] S. L. Ullo and G. R. Sinha, "Advances in Smart Environment Monitoring Systems Using IoT and Sensors," Sensors, vol. 20, no. 11, p. 3113, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/11/3113.

[53] H. Nandanwar and A. Chauhan, "IOT based Smart Environment Monitoring Systems: A Key To Smart and Clean Urban Living Spaces," in 2021 Asian Conference on Innovation in Technology (ASIANCON), 27-29 Aug. 2021 2021, pp. 1-9, doi: 10.1109/ASIANCON51346.2021.9544596.

[54] A. Razmjoo, A. Gandomi, M. Pazhoohesh, S. Mirjalili, and M. Rezaei, "The key role of clean energy and technology in smart cities development," Energy Strategy Reviews, vol. 44, 08/20 2022, doi: 10.1016/j.esr.2022.100943.

[55] K. Sujatha et al., "Smart Vision-Based Sensing and Monitoring of Power Plants for a Clean Environment," in Intelligent Manufacturing Management Systems, 2023, pp. 195-222.

[56] M. Vijarania, V. Jaglan, and A. Sanjay, "Security Surveillance and Home Automation System using IoT," EAI Endorsed Transactions on Smart Cities, vol. 5, p. 165963, 08/06 2020, doi: 10.4108/eai.21-7-2020.165963.

[57] "IBM Corp., IBM Db2 Database, Database Software, IBM Analytics,." https://www.ibm.com/analytics/us/en/db2/ (accessed 09 March 2018, 2018).

[58] A. Page, O. Kocabas, T. Soyata, M. Aktas, and J.-P. Couderc, "Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance," Annals of Noninvasive Electrocardiology, vol. 20, pp. 328-337, 12/01 2014, doi: 10.1111/anec.12204.

[59] a. dolatkhah, B. D. Yaghouti, and r. hashempour, "Face recognition and Liveness Detection Based on Speech Recognition for Electronical Authentication," (in Fa), Journal of Information and Communication Technology, vol. 15, no. 57, pp. 94-110, 2023. [Online]. Available: https://www.magiran.com/paper/2640158.

[60] J. Henius and J. L. McDonald, Smart Defense: A critical appraisal. NATO defense College, Research division= Collège de défense de l'Otan …, 2012.

[61] B. B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed Denial of service attack in

IoT networks using supervised learning classifiers," Computers & Electrical Engineering, vol. 98, 02/02 2022, doi: 10.1016/j.compeleceng.2022.107726.

[62] I. Karatas, "Cyber Warfare and NATO's New Security Concept: Smart Defense," 2021, pp. 273-285.

[63] T. FRUNZETI, "THE CONCEPT OF "SMART DEFENSE" IN THE CONTEXT OF AN EFFICIENT DEFENSE PLANNING," Journal of Defense Resources Management, vol. Vol. 3, no. 2, pp. pp. 3 – 18 2012.

[64] H. Azadi et al., "Rethinking resilient agriculture: From Climate-Smart Agriculture to Vulnerable-Smart Agriculture," Journal of Cleaner Production, vol. 319, p. 128602, 08/01 2021, doi: 10.1016/j.jclepro.2021.128602.

[65] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 4, pp. 718-752, 2021, doi: 10.1109/JAS.2021.1003925.

[66] B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of Internet of Things in smart agriculture: A survey," Future Generation Computer Systems, vol. 126, 08/14 2021, doi: 10.1016/j.future.2021.08.006.

[67] V. K. Quy et al., "IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges," Applied Sciences, vol. 12, no. 7, p. 3396, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/7/3396.

[68] R. Stewart, R. Willis, D. Giurco, K. Panuwatwanich, and G. Capati, "Web-based knowledge management system: Linking smart metering to the future of urban water planning," Australian Planner, vol. 47, 06/01 2010, doi: 10.1080/07293681003767769.

[69] M. Phadke. "Smart Water Management – Need of the hour for utility sector." https://www.einfochips.com/blog/smart-water-management-need-of-the-hour-for-utility-sector/ (accessed.

[70] F. Adesola, S. Misra, N. Omoregbe, R. Damaševičius, and R. Maskeliunas, "An IOT-Based Architecture for Crime Management in Nigeria," 2019, pp. 245-254.

[71] S. Jain and N. Kesswani, "Smart Judiciary System: A Smart Dust Based IoT Application," 2019, pp. 128-140.

[72] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: A systematic review," Sustainable Cities and Society, vol. 55, p. 102023, 2020/04/01/ 2020, doi: https://doi.org/10.1016/j.scs.2020.102023.

[73] A. Tundis, H. Kaleem, and M. Mühlhäuser, "Detecting and Tracking Criminals in the Real World through an IoT-Based System," Sensors, vol. 20, p. 3795, 07/07 2020, doi: 10.3390/s20133795.

[74] M. S. Khan, M. Woo, K. Nam, and P. K. Chathoth, "Smart City and Smart Tourism: A Case of Dubai," Sustainability, vol. 9, no. 12, p. 2279, 2017. [Online]. Available: https://www.mdpi.com/2071-1050/9/12/2279.

[75] P. Lee, W. C. Hunter, and N. Chung, "Smart Tourism City: Developments and Transformations," Sustainability, vol. 12, no. 10, p. 3958, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/10/3958.

[76] N. Habeeb and S. Talib, "HighTech and Innovation Journal Relationship of Smart Cities and Smart Tourism: An Overview," HighTech and Innovation Journal, vol. 1, 12/01 2020, doi: 10.28991/HIJ-2020-01-04-07.

[77] N. Chung, H. Lee, J. Ham, and C. Koo, "Smart Tourism Cities' Competitiveness Index: A Conceptual Model," 2021, pp. 433-438.

[78] A. Gohar and G. Nencioni, "The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System," Sustainability, vol. 13, no. 9, p. 5188, 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/9/5188.

[79] A. Garcia Crespo, I. Gonzalez-Carrasco, J. Cuadrado, D. Villanueva, and Á. González, "CESARSC: Framework for creating Cultural Entertainment Systems with Augmented Reality in Smart Cities," Computer Science and Information Systems, vol. 13, pp. 6-6, 06/01 2016, doi: 10.2298/CSIS150620006G.

[80] D. Cook, G. Youngblood, and S. Das, A Multi-agent Approach to Controlling a Smart Environment. 2006, pp. 165-182.

[81] P. Pitchai, S. Subramani, K. Usa, K. Raju, M. Alsharif, and M. K. Kim, "Technological Advancements Toward Smart Energy Management in Smart Cities," Energy Reports, vol. 10, pp. 648-677, 06/24 2023, doi: 10.1016/j.egyr.2023.07.021.

[82] A. Braicov et al., "Smart Surveillance Systems and Their Applications," 2020, pp. 179-187.

[83] A. Medjdoubi, M. Meddeber, and K. Yahyaoui, "Smart City Surveillance: Edge Technology Face Recognition Robot Deep Learning Based," International Journal of Engineering, vol. 37, no. 1, pp. 25-36, 2024, doi: 10.5829/ije.2024.37.01a.03.

[84] K. Liao, Z. Zhao, A. Doupe, and G. J. Ahn, "Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin," in 2016 APWG Symposium on Electronic Crime Research (eCrime), 1-3 June 2016 2016, pp. 1-13, doi: 10.1109/ECRIME.2016.7487938.

[85] J. M. Alonso and C. Mencar, "Building cognitive cities with explainable artificial intelligent systems," in CEx@ AI* IA, 2017.

[86] A. Adadi and M. Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," IEEE Access, vol. 6, pp. 52138-52160, 2018, doi: 10.1109/ACCESS.2018.2870052.

[87] R. K. E. Bellamy et al., "AI Fairness 360: An Extensible Toolkit for Detecting, Understanding, and Mitigating Unwanted Algorithmic Bias," ArXiv, vol. abs/1810.01943, 2018.

[88] M. Roy, "Cathy O'Neil. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy . New York: Crown Publishers, 2016. 272p. Hardcover, $26 (ISBN 978-0553418811)," College & Research Libraries, vol. 78, pp. 403-404, 03/01 2017, doi: 10.5860/crl.78.3.403.

[89] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," Expert Systems, vol. 39, 2021.

[90] B. Tekinerdogan, Ö. Köksal, and T. Çelik, "System Architecture Design of IoT-Based Smart Cities," Applied Sciences, vol. 13, no. 7, p. 4173, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/7/4173.

[91] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro-Sensor Networks," Wireless Communications, IEEE Transactions on, vol. 1, pp. 660-670, 11/01 2002, doi: 10.1109/TWC.2002.804190.

[92] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, 2016, doi: 10.1109/JIOT.2016.2579198.

[93]"Google Science Journal." https://makingscience.withgoogle.com/science-journal (accessed.

[94] Y. Geng, J. Chen, R. Fu, G. Bao, and K. Pahlavan, "Enlighten Wearable Physiological Monitoring Systems: On-Body RF Characteristics Based Human Motion Classification Using a Support Vector Machine," IEEE Transactions on Mobile Computing, vol. 15, pp. 1-1, 01/01 2015, doi: 10.1109/TMC.2015.2416186.

[95] J. Yin, I. Gorton, and S. Poorva, Toward Real Time Data Analysis for Smart Grids. 2012, pp. 827-832.

[96] D. Neumann, C. Bodenstein, O. Rana, and R. Krishnaswamy, "STACEE: Enhancing storage clouds using edge devices," 06/14 2011, doi: 10.1145/1998561.1998567.

[97]"the International Society for Urban Informatics, The ISUI Smart City " https://www.isocui.org/smart_city_index (accessed.

[98] A. Elmaghraby and M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, security and privacy," Journal of Advanced Research, vol. 5, 07/01 2014, doi: 10.1016/j.jare.2014.02.006.

[99] Y. Zhao, "Research on Data Security Technology in Internet of Things," Applied Mechanics and Materials, vol. 433-435, pp. 1752-1755, 10/01 2013, doi: 10.4028/www.scientific.net/AMM.433-435.1752.

[100] A. Page, M. Hassanalieragh, T. Soyata, M. Aktas, B. Kantarci, and S. Andreescu, "Conceptualizing a Real-Time Remote Cardiac Health Monitoring System," 2015, pp. 1-34.

[101] T. Soyata, Enabling Real-Time Mobile Cloud Computing through Emerging Technologies. 2015.

[102] G. Honan, A. Page, O. Kocabas, T. Soyata, and B. Kantarci, Internet-of-everything oriented implementation of secure Digital Health (D-Health) systems. 2016, pp. 718-725.

[103] A. Page, S. Hijazi, D. Askan, B. Kantarci, and T. Soyata, "SUPPORT SYSTEMS FOR HEALTH MONITORING USING INTERNET-OF-THINGS DRIVEN DATA ACQUISITION," Services Transactions on Services Computing, vol. 4, pp. 18-34, 10/01 2016, doi: 10.29268/stsc.2016.4.4.2.

[104] K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall," IEEE Network, vol. 30, 08/23 2016, doi: 10.1109/MNET.2016.1600110NM.

[105] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING & TECHNOLOGY, vol. 8, 06/11 2022.

[106] S. Latif, A. Qayyum, M. Usama, J. Qadir, A. Zwitter, and M. Shahzad, "Caveat Emptor: The Risks of Using Big Data for Human Development," IEEE Technology and Society Magazine, vol. 38, no. 3, pp. 82-90, 2019, doi: 10.1109/MTS.2019.2930273.

[107] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," IEEE Communications Magazine, vol. 55, no. 1, pp. 122-129, 2017, doi: 10.1109/MCOM.2017.1600267CM.

[108] H. Ekbia et al., "Big Data, Bigger Dilemmas: A Critical Review," Journal of the Association for Information Science and Technology, vol. 66, 08/01 2015, doi: 10.1002/asi.23294.

[109] K. Crawford and R. Calo, "There is a blind spot in AI research," Nature, vol. 538, pp. 311-313, 10/13 2016, doi: 10.1038/538311a.

[110] L. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. Gellersen, Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts. 2001, pp. 116-122.

[111] S. Mallapuram, N. Ngwum, F. Yuan, C. Lu, and W. Yu, Smart City: The State of the Art, Datasets, and Evaluation Platforms. 2017.

[112] A. Ali, J. Qadir, R. Rasool, A. Sathiaseelan, and A. Zwitter, "Big Data For Development: Applications and Techniques," Big Data Analytics, vol. 1, 07/01 2016, doi: 10.1186/s41044-016-0002-4.

[113] H. Yu, Z. Yang, and R. Sinnott, "Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology," IEEE Access, vol. PP, pp. 1-1, 12/20 2018, doi: 10.1109/ACCESS.2018.2888940.

[114] A. W Flores, K. Bechtel, and C. Lowenkamp, "False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks."," Federal probation, vol. 80, 09/30 2016.

[115] K. Crawford, "Artificial Intelligence's White Guy Problem," 2016.

[116] S. M. Lundberg et al., "Explainable machine-learning predictions for the prevention of hypoxaemia during surgery," (in eng), Nat Biomed Eng, vol. 2, no. 10, pp. 749-760, Oct 2018, doi: 10.1038/s41551-018-0304-0.

[117] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization," in 2017 IEEE International Conference on Computer Vision (ICCV), 22-29 Oct. 2017 2017, pp. 618-626, doi: 10.1109/ICCV.2017.74.

[118] C. Drew, "Data science ethics in government," Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences, vol. 374, p. 20160119, 12/28 2016, doi: 10.1098/rsta.2016.0119.

[119] F. Samie, L. Bauer, and J. Henkel, "Hierarchical Classification for Constrained IoT Devices: A Case Study on Human Activity Recognition," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8287-8295, 2020, doi: 10.1109/JIOT.2020.2989053.

[120] C. R. Gregersen. "3 IoT Latency Issues and How to Fix Them." https://builtin.com/articles/how-to-fix-iot-latency (accessed.

[121] R. S. Rajeshwari Adrakatti "Approaches for Managing the Smart Phone Battery Efficiently," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 27, 2018, doi: 10.17577/IJERTCONV3IS27006.

[122] M. Ali, J. M. Zain, M. F. Zolkipli, and G. Badshah, "Battery efficiency of mobile devices through computational offloading: A review," in 2015 IEEE Student Conference on Research and Development (SCOReD), 13-14 Dec. 2015 2015, pp. 317-322, doi: 10.1109/SCORED.2015.7449347.

[123] A. Qayyum et al., "Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security," Frontiers in Big Data, vol. 3, 12/02 2020, doi: 10.3389/fdata.2020.587139.

[124] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing Connected & Autonomous Vehicles: Challenges

Posed by Adversarial Machine Learning and the Way Forward," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998-1026, 2020, doi: 10.1109/COMST.2020.2975048.

[125] "a guide to anticipating the future impact of today's technology." https://mediaethics.ca/wp-content/uploads/2019/11/Ethical-OS-Toolkit-2.pdf (accessed.

[126] J. Krimmling and S. Peter, "Integration and evaluation of intrusion detection for CoAP in smart city applications," in 2014 IEEE Conference on Communications and Network Security, 29-31 Oct. 2014 2014, pp. 73-78, doi: 10.1109/CNS.2014.6997468.

[127] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, vol. 3, 03/01 2012, doi: 10.1109/ICCSEE.2012.373.

[128] M. J. Covington and R. Carskadden, Threat implications of the Internet of Things. 2013, pp. 1-12.

[129] A. Barua, M. A. A. Alamin, M. Hossain, and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 3, pp. 1-1, 01/01 2022, doi: 10.1109/OJCOMS.2022.3149732.

[130] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and L. Qiao-min, "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things," Applied Mathematics & Information Sciences, vol. 8, 07/01 2014, doi: 10.12785/amis/080416.

[131] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," IEEE Cloud Computing, vol. 3, pp. 64-71, 05/01 2016, doi: 10.1109/MCC.2016.63.

[132] M. Aljanabi et al., Data poisoning: issues, challenges, and needs. 2024, pp. 359-363.

[133] W. Li, R. Zhao, T. Xiao, and X. Wang, "DeepReID: Deep Filter Pairing Neural Network for Person Re-identification," in 2014 IEEE Conference on Computer Vision and Pattern Recognition, 23-28 June 2014 2014, pp. 152-159, doi: 10.1109/CVPR.2014.27.

[134] F. Wang, X. Wang, and X. Ban, "Data poisoning attacks in intelligent transportation systems: A survey," Transportation Research Part C Emerging Technologies, vol. 165, p. 104750, 08/01 2024, doi: 10.1016/j.trc.2024.104750.

[135] M. Billah, A. Anwar, Z. Rahman, and S. M. Galib, "Bi-Level Poisoning Attack Model and Countermeasure for Appliance Consumption Data of Smart Homes," Energies, vol. 14, no. 13, p. 3887, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/13/3887.

[136] M. A. Ayub, W. A. Johnson, D. A. Talbert, and A. Siraj, "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning," in 2020 54th Annual Conference on Information Sciences and Systems (CISS), 18-20 March 2020 2020, pp. 1-6, doi: 10.1109/CISS48834.2020.1570617116.

[137] M. Sato, J. Suzuki, H. Shindo, and Y. Matsumoto, Interpretable Adversarial Perturbation in Input Embedding Space for Text. 2018.

[138]N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, The Limitations of Deep Learning in Adversarial Settings. 2016, pp. 372-387.

[139] N. Carlini and D. Wagner, Audio Adversarial Examples: Targeted Attacks on Speech-to-Text. 2018, pp. 1-7.

[140] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," Information Sciences, vol. 239, pp. 201–225, 08/01 2013, doi: 10.1016/j.ins.2013.03.022.

[141] N. Carlini et al., On Evaluating Adversarial Robustness. 2019.

[142] S. Utomo, A. Rouniyar, H.-C. Hsu, and P.-A. Hsiung, "Federated Adversarial Training Strategies for Achieving Privacy and Security in Sustainable Smart City Applications," Future Internet, vol. 15, p. 371, 11/20 2023, doi: 10.3390/fi15110371.

[143] Y. Liu et al., A Survey on Neural Trojans. 2020, pp. 33-39.

[144] Y. Gao, C. Xu, D. Wang, S. Chen, D. Ranasinghe, and S. Nepal, STRIP: a defence against trojan attacks on deep neural networks. 2019, pp. 113-125.

[145] "Trojan Horse Virus." https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus (accessed.

[146] C. Dong, Y. Xu, X. Liu, F. Zhang, G. He, and Y. Chen, "Hardware Trojans in Chips: A Survey for Detection and Prevention," Sensors, vol. 20, no. 18, p. 5165, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/18/5165.

[147] M. Juuti, S. Szyller, S. Marchal, and N. Asokan, PRADA: Protecting Against DNN Model Stealing Attacks. 2019, pp. 512-527.

[148] X. W. Minxue Tang, Yitu Wang. "Model Stealing Attacks." https://people.duke.edu/~zg70/courses/AML/Lecture14.pdf (accessed.

[149] https://owasp.org/www-project-machine-learning-security-top-10/docs/ML05_2023-Model_Theft (accessed.

[150] P. Irolla. "What is model stealing and why it matters." https://www.mlsecurity.ai/post/what-is-model-stealing-and-why-it-matters (accessed.

[151] N. Carlini, S. Chien, M. Nasr, S. Song, A. Terzis, and F. Tramèr, "Membership Inference Attacks From First Principles," in 2022 IEEE Symposium on Security and Privacy (SP), 22-26 May 2022 2022, pp. 1897-1914, doi: 10.1109/SP46214.2022.9833649.

[152] "Membership inference attacks | A new AI security risk." https://www.michalsons.com/blog/membership-inference-attacks-a-new-ai-security-risk/64440 (accessed.

[153] A. Famili and Y. Lao, "Deep Neural Network Quantization Framework for Effective Defense against Membership Inference Attacks," Sensors, vol. 23, no. 18, p. 7722, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/18/7722.

[154] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Electronics, vol. 11, no. 2, p. 198, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/2/198.

[155] Y. Jia et al., "Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model," Knowledge-Based Systems, vol. 276, p. 110781, 07/01 2023, doi: 10.1016/j.knosys.2023.110781.

[156] M. Chohan, U. Haider, M. Y. Ayub, H. Shoukat, T. Bhatia, and M. Hassan, "Detection of Cyber Attacks using Machine Learning based Intrusion Detection System for IoT Based

Smart Cities," EAI Endorsed Transactions on Smart Cities, vol. 7, 06/28 2023, doi: 10.4108/eetsc.3222.

[157] A. Nunn and P. W. C. Prasad, "Using Artificial Intelligence to Defend Internet of Things for Smart City Networks," in Innovative Technologies in Intelligent Systems and Industrial Applications, Cham, S. C. Mukhopadhyay, S. M. N. A. Senanayake, and P. W. C. Prasad, Eds., 2024// 2024: Springer Nature Switzerland, pp. 345-367.

[158] B. J. Ospina Cifuentes, Á. Suárez, V. García Pineda, R. Alvarado Jaimes, A. O. Montoya Benitez, and J. D. Grajales Bustamante, "Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey," Technologies, vol. 12, no. 7, p. 99, 2024. [Online]. Available: https://www.mdpi.com/2227-7080/12/7/99.

[159] M. Songhorabadi, M. Rahimi, A. M. Moghadam Farid, and M. Haghi Kashani, "Fog computing approaches in IoT-enabled smart cities," Journal of Network and Computer Applications, vol. 211, p. 103557, 12/01 2022, doi: 10.1016/j.jnca.2022.103557.

[160] "Introduction to "Discover Emerging Technologies in Trends in 2024"." [Online]. Available: https://www.linkedin.com/pulse/part-1-navigating-future-technology-smart-worlds-lennart-kalwa-qh68e/

[161] C. Bernard Marr. "8 Critical Smart City Trends Reshaping Urban Life In 2025." https://www.forbes.com/sites/bernardmarr/2025/01/09/8-critical-smart-city-trends-reshaping-urban-life-in-2 (accessed.

[162] J. G. B. Miguel Eiras Antunes, Daniela Guerreiro de Oliveira. "Urban Future With a Purpose 12 trends shaping the future of cities by 2030." https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose.html (accessed.

Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 50-62
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

A Novel Hybrid Convolutional-Attention Recurrent Network (HCARN) for Enhanced Cybersecurity Threat Detection

Archana R. Laddhad [1*], Gurveen Vaseer [1]

[1].Faculty of Computer Science, Oriental University, Indore – Madhya Pradesh, India

Received: 09 Nov 2024/ Revised: 04 Mar 2025/ Accepted: 19 Apr 2025

Abstract

Cybersecurity solutions are critical for the protection of networks against constantly evolving threats. Traditional intrusion detection systems (IDS) struggle to adapt to the rapidly varying attack patterns, encouraging the exploration of advanced techniques such as deep learning. This study introduces a novel framework utilizing a Hybrid Convolutional-Attention Recurrent Network (HCARN) for identifying cybersecurity threat. Utilizing the CSE-CIC-IDS2018 dataset, the data preparation process includes data cleanup, feature extraction, and Information Gain-based feature choice. The HCARN architecture, integrates convolutional layers, attention mechanisms, and recurrent layers, is employed for categorization. Convolutional layers effectively capture spatial features in the dataset, attention mechanisms highlight critical features, and recurrent layers model temporal dependencies. This allows HCARN to process and analyze complex patterns in network traffic, leading to more accurate threat diagnosis. The proposed model proves significant efficacy in distinguishing between major, moderate, and minor threats, attaining high accuracy and robustness in threat recognition. The incorporation of attention mechanisms allows the model to emphasize on critical features, while the recurrent layers pay attention to temporal dependencies in the dataset. The HCARN architecture determines classification accuracy, achieving 94.7% in K-fold validation, 95.4% in model training, and 92.3% in model testing while classifying major, moderate, minor threats satisfactorily, confirming its effectiveness in cybersecurity threat detection. This novel attempt underscores the potential of hybrid deep learning models in enhancing cybersecurity defenses against sophisticated attacks, paving the way for adaptive security systems.

Keywords: Intrusion Detection Systems; CSE-CIC-IDS2018; Deep Learning; Hybrid Convolutional-Attention Recurrent Network; Cybersecurity.

1- Introduction

In today's cybersecurity landscape, Intrusion Detection Systems (IDS) hold significant importance by serving as a vital security measure against the continuously growing array of digital threats. An Intrusion Detection System (IDS) is an active security measure devised to detect and counteract unauthorized or malicious activities occurring within a network or system [1]. The principal objective of this system is to actively observe network traffic and analyze system behavior, with the purpose of promptly identifying any peculiar patterns or discrepancies that could potentially serve as indications of a security breach. In contemporary cybersecurity landscape, Intrusion Detection Systems (IDS) play a pivotal role in preserving the authenticity, secrecy, and accessibility of digital assets, thus imbuing them with utmost significance as a formidable deterrent against the ever-changing realm of security threats [2].

Conventional Intrusion Detection Systems (IDS) rely on pre-established rules and signatures in order to detect and classify recognized attack patterns. Nevertheless, it is frequently challenging for them to effectively adjust to the rapidly evolving risks and complex methods employed by potential assailants [3]. The aforementioned constraint has prompted researchers to investigate sophisticated methodologies, such as the amalgamation of artificial intelligence (AI), machine learning (ML), and deep learning (DL) approaches, with the intent of augmenting the precision and responsiveness of Intrusion Detection Systems (IDS). These approaches facilitate Intrusion Detection Systems (IDS) to acquire knowledge from data, identify novel attack patterns, and generate prompt

✉ **Archana R. Laddhad**
archanaladdhad@gmail.com

decisions, rendering them indispensable instruments for enterprises intending to enhance their cybersecurity safeguards. By utilizing these methodologies, Intrusion Detection Systems (IDS) can transcend rule-based methodologies, which encounter difficulties in accommodating emerging threats, and instead become adept in identifying innovative attack patterns. The utilization of artificial intelligence (AI), machine learning (ML), and deep learning (DL) methodologies in intrusion detection systems (IDS) improves their capacity to identify both familiar and novel threats, decrease instances of erroneous positive detections, and effectively react to security incidents in a timely manner. The CSE-CIC-IDS2018 dataset offers researchers a significant opportunity to implement these methodologies in practical situations, enabling the training and evaluation of intrusion detection systems based on artificial intelligence, machine learning, and deep learning [4]. It also permits the assessment of their efficacy in tackling contemporary cybersecurity challenges, which are characterized by their dynamic and intricate nature.

In their development of two deep neural network models for intrusion detection in cloud environments, Alzughaibi & El Khediri [5] achieve high accuracy rates on with 98.97% for binary classification and 98.41% for multi-class classification. Göcs & Johanyák [6] concentrate on feature selection for intrusion detection systems. They use six feature selection techniques and classification algorithms to find pertinent elements essential for differentiating between benign and malicious network traffic. In their comparison of bio-inspired optimization algorithms for cybersecurity attack detection, Najafi Mohsenabad & Tut [7] found that Ant Colony Optimization, Flower Pollination Algorithm, and Artificial Bee Colony feature-selection strategies produced detection accuracies of over 98.6%.

On the CSE-CIC-IDS2018 dataset, Göcs & Johanyák [8] describe a novel ensemble feature-ranking strategy that improves on existing feature-ranking score combinations and achieves superior classification metrics, particularly for specific attack types. XGBoost, DT, and RF models are highlighted for their superior performance in terms of ROC values and CPU runtime by Songma, Sathuphan, and Pamutha [9] as they optimize intrusion detection systems using data preprocessing, dimensionality reduction with PCA and RF, and various machine learning techniques on the CSE-CIC-IDS-2018 dataset. Using 19 features chosen using the decision tree technique, Khan & Haroon [10] offer an Artificial Neural Network (ANN)-based intrusion detection system that achieves great performance on the CSE-CIC-IDS2018 dataset. Farhan & Jasim [11] use deep learning, namely LSTM, for intrusion detection. They achieve an impressive detection accuracy of up to 99%, demonstrating the usefulness of deep learning techniques for cybersecurity applications. The summary of literature review is organized in Table 1. Masoudi & Ghaffari [26] conducted a comprehensive investigation on Software Defined Networks (SDN), focusing on performance issues and solutions in SDN-based data centers. They grouped solutions into different clusters and identified key challenges and future research directions in the field. Further, Shirmarz & Ghaffari [27] focused on enhancing the performance of software defined network through an autonomic system based on deep neural networks. Their architecture demonstrates improved performance metrics such as blocking probability, delay, and packet loss rate. Shirmarz & Ghaffari [28] continued the research and presented improving DDoS attack detection in SDN using Self-Organizing Maps and Learning Vector Quantization. The approach significantly improves the detection rate, making SDN more resilient against cyber threats.

Table 1: Summary of Literature Review

Objectives	***Attacks***	***Algorithms***	***Authors***
IDS	DoS, U2L R2L, Probe	K-means + KNN	Tsai et al. [12]
Encrypted traffic classification	Malicious instances		Bar et al. [13]
IDS	DoS, U2L R2L, Probe		Lin et al. [14]
Malware detection	High-risk malwares	SVM + KNN	Comar et al. [15]
IDS	DoS, U2L R2L, Probe	SVM + kNN + PSO	Aburomman et al. [16]
Android malware detection	-	SVM + DT	Li et al. [17]
IDS	All attacks	K-Support Vector	Bamakan et al. [18]
IDS	Anomalous connections	PCA Filtering + Probabilistic SOM	Hoz et al. [19]
IDS	DoS, U2R, R2L, probe	K-Means + NB + BNN	Dubey et al. [20]
IDS		RF + AODE	Jabbar et al. [21]
IDS	Botnet	DT + NB + ANN	Moustafa et al. [22]
NADS	DoS, U2R, R2L, probe	NB + KNN	Pajouh et al. [23]
DoS attack detection	DoS	Multivariate Correlation + Triangle Area	Tan et al. [24]
Network forensics	DDoS, DARPA	FL + ES	Liao et al. [25]
IDS	All attacks	Hybrid Convolutional-Attention Recurrent Network	Present model

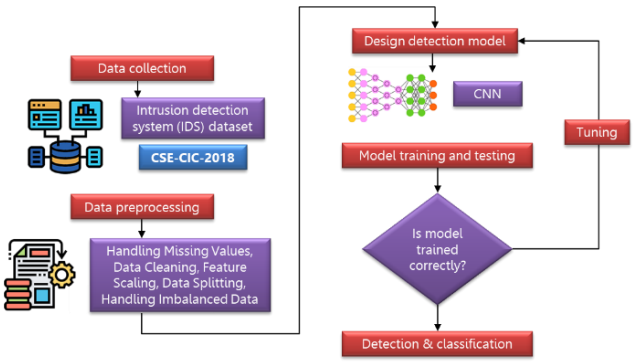


Fig. 1 Methodology

In the context of a swiftly progressing digital environment, the significance of highly resilient intrusion detection systems holds substantial weight. This paper makes a contribution to the continuous endeavors in enhancing network security and protecting the digital realm against an increasingly wide range of threats by utilizing the CSE-CIC-IDS2018 dataset and the capabilities of deep learning. The findings presented in this manuscript not only provide valuable insights into the effectiveness of deep learning-based intrusion detection, but also elucidate the trajectory for developing intelligent, versatile, and proactive cybersecurity measures. The flow of the research is depicted in Figure 1. The core objective of this investigation is to develop and assess the HCARN for cybersecurity threat detection. It aims to:

- improve the effectiveness of intrusion detection systems (IDS) by employing advanced deep learning method
- integrate recurrent, attention, and convolutional mechanisms to efficiently capture network traffic with temporal, critical, and spatial patterns
- evaluate the HCARN's performance on the CSE-CIC-IDS2018 dataset to categorize cybersecurity threats into major, moderate, and minor sets reliably.

2- CSE-CIC-IDS2018 Dataset

The dataset consists of a substantial amount of annotated network traffic data, which is indispensable in the process of training, testing, and validating the efficacy of intrusion detection systems. The CSE-CIC-IDS2018 dataset [29] exemplifies a meticulous emphasis on realism, effectively replicating the complex and ever-evolving characteristics of contemporary network environments. The current dataset encapsulates a wide array of network activities encompassing both legitimate and malicious traffic. Such inclusion permits researchers to evaluate the efficacy of Intrusion Detection Systems (IDS) in distinguishing between the two types of traffic within an environment that closely mimics real-world conditions. The CSE-CIC-IDS2018 dataset presents a comprehensive range of characteristics, each augmenting the comprehension of network traffic patterns. The aforementioned characteristics encompass details regarding individual packets, aggregated data on network flows, and diverse metadata pertaining to the network traffic. The extensive amount of information available to enhance IDS that possess the capability to precisely identify security risks.

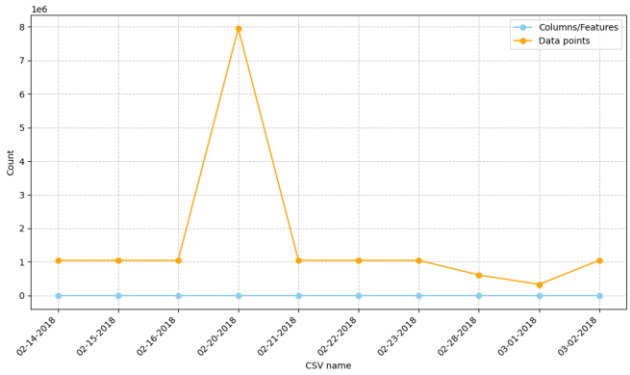


Fig. 2 Comparison of Features and Data Points

- Number of observations: The dataset is acknowledged to encompass a considerable quantity of observations, frequently reaching in the millions. The precise quantity of observations may fluctuate contingent upon the particular iteration or subset of the dataset under consideration. Knowing the number of features and observations is essential for training the HCARN model as it helps in deciding the input shape and the convolution of the dataset and thus figure 2 represents comparison of features and data points.
- Number of features and attributes: The dataset typically encompasses a multitude of features and attributes which serve to depict network traffic data. The range of features within the dataset's version can vary from tens to hundreds. Features often include data related to the contents of packets, patterns of network traffic, and a range of additional attributes that characterize the network. The output of the application is in CSV file format with six columns labeled for each flow, namely FlowID, SourceIP, DestinationIP, SourcePort, DestinationPort, and Protocol with more than 80 network traffic features. Number of features and data points in each csv file as shown in Table 2 guides in setting applicable hyperparameters and design of architecture, confirming efficient training and optimization. Here, data points refer to individual instances or observations in a dataset and each row or entry in the dataset represents a single data point. Each row signifies a specific date in February and March 2018, with the subsequent number of features in

various columns and the total number of data points logged for that date.

Table 2: Number of Features and Data Points in Each csv File

CSV Name	*Features*	*Data Points*
02-14-2018	79	1,048,574
02-15-2018	79	1,048,574
02-16-2018	79	1,048,574
02-20-2018	83	7,948,746
02-21-2018	79	1,048,574
02-22-2018	79	1,048,574
02-23-2018	79	1,048,574
02-28-2018	79	613,103
03-01-2018	79	331,124
03-02-2018	79	1,048,574

- Number of attacks: The dataset known as CSE-CIC-IDS2018 encompasses a diverse array of cyberattacks and network anomalies. The dataset typically encompasses various categories.

❖ Denial of Service Attacks (DoS): The primary objective of these attacks is to inundate a targeted system or network, resulting in its unavailability to genuine users. Instances of these types of attacks incorporate SYN flood attacks and UDP flood attacks.

❖ Port Scanning: Port scanning attacks encompass the practice of systematically investigating a target system to ascertain the availability of open ports with the aim of identifying potential security vulnerabilities or discerning the services currently active on the system.

❖ Malware: The dataset potentially encompasses traffic affiliated with the propagation or transmission of malicious software, including botnets, worms, and viruses.

❖ Intrusions: Intrusions refer to a multitude of unauthorized activities occurring within a network, such as unauthorized access, privilege escalation, or other forms of network exploitation.

❖ Botnet Activity: The dataset may contain instances of Botnet activity, whereby the activities related to a network of compromised devices controlled by a malevolent individual are detected.

Understanding category wise traffic distribution by respective shares (%) is vital as it presents insights into the prevalence and importance of different attacks (See Figure 3). This helps in prioritizing the emphasis of feature engineering, training, and evaluation schemes, certifying model's robustness to effectively classify and detect the most prevalent real-world threats. Furthermore, it helps in resource allocation and decision-making for mitigating specific types of attacks based on relative occurrence frequencies. These attacks are explained herewith.

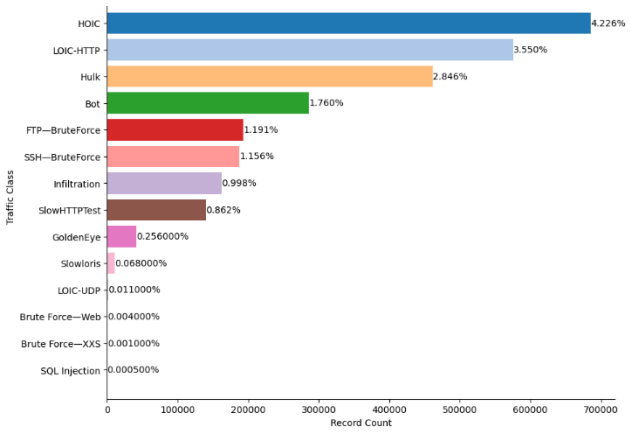


Fig. 3 Types of Attacks and Counts

❖ HOIC: It has 686,012 samples, corresponds to 4.226% of the total traffic flow. HOIC (High Orbit Ion Cannon) is a common tool that launches DDoS attacks.

❖ LOIC-HTTP: This category contains 576,191 samples, making up 3.550% of the total records. LOIC (Low Orbit Ion Cannon) is another DDoS tool, and the "HTTP" suffix suggests it targets web servers.

❖ Hulk: With 461,912 samples, Hulk forms 2.846% of the total records. Hulk is a Python script employed to execute DDoS attacks by flooding web servers with HTTP demands.

❖ Bot: This category incorporates 286,191 samples, representing 1.76% of the total records. Bots are automated program that executes several tasks, including detection of malicious behavior such as data theft, spamming, or DDoS.

❖ FTP—BruteForce: There are 193,360 samples here, with 1.191% of the total records. FTP (File Transfer Protocol) Brute Force attack attempts to gain unauthorized access to FTP servers by methodically trying unique combinations of username/password.

❖ SSH—BruteForce: This category has of 187,589 samples, that takes 1.156% of the total records. SSH (Secure Shell) Brute Force attacks attempts guessing of SSH login credentials to secure unauthorized access.

❖ Infiltration: With 161,934 samples, Infiltration denotes 0.998% of the total records. Infiltration stand for to the unauthorized invasion of a system or network with the intentation of retrieving confidential data or causing destruction.

❖ SlowHTTPTest: This category involves 139,890 samples, with 0.862% of the total records. SlowHTTPTest is a tool employed for testing HTTP DoS exposures by launching slow HTTP POST or GET requests.

- ❖ GoldenEye: GoldenEye includes 41,508 samples, indicating 0.256% of the total records. GoldenEye is a DDoS tool that targets web servers by flooding them with TCP SYN packets.
- ❖ Slowloris: With 10,990 samples, Slowloris takes 0.068% of the total records. Slowloris is a DoS attack tool that targets web servers by multiple connections kept open for longest possible time, exhausting server resources.
- ❖ LOIC-UDP: This category gets 1,730 samples, with 0.011% of the total records. LOIC-UDP is a variation of the Low Orbit Ion Cannon tool that implements UDP-based DDoS attacks.
- ❖ Brute Force—Web: There are 611 samples here, demonstrating 0.004% of the total records. Brute Force—Web indicates brute force attacks pursuing web apps.
- ❖ Brute Force—XXS: This type consist of 230 samples, with 0.001% of the total records. Brute Force—XXS is a brute force attack focusing on cross-site scripting vulnerabilities in web apps.
- ❖ SQL Injection: With 87 samples, SQL Injection signifies 0.0005% of the total records. SQL Injection is very usual attack responsible for exploitation of vulnerabilities in web apps for executing malicious SQL queries.

In order to handle the imbalance a class-weighted categorical cross-entropy loss function was itself employed. It ensured that:

- Under-represented attack categories supported considerably to model learning, targeting no bias towards frequent attack.
- Over-represented attacks had lesser loss weights, guaranteeing the network did not overly favor them.

3- Deep Learning Pipeline

3-1- Data Pre-Processing

Data cleaning involves identifying and rectifying errors, inconsistencies, and inaccuracies in datasets to ensure their quality and reliability. This process greatly impacts the validity and credibility of research findings and statistical analyses. Consequently, it is essential to carefully and systematically perform data cleaning to enhance data integrity and minimize the potential for biased or misleading conclusions. Furthermore, adhering to best practices and employing appropriate software tools can streamline and facilitate the data cleaning process, leading to more robust and accurate research outcomes. Commence with the unprocessed data as the primary dataset. To initiate the preprocessing workflow, it is necessary to commence with the data cleaning process. The initial cleaning process facilitates dimensionality reduction, ultimately providing various benefits. In the current analytical study, the inclusion of the time parameter is deemed unnecessary, and any columns consisting solely of zero values are excluded due to their lack of influence on the final result. Following completion of the cleaning procedure, a total of 11 columns were excluded from the initial set of 80 columns, leaving 69 columns remaining. A few fields were eliminated from the dataset before features were chosen. Metrics like 'Bwd_Avg_Bulk_Rate', 'Fwd_Avg_Bytes_Bulk', 'Bwd_Avg_Packets_Bulk', and 'Fwd_Avg_Bulk_Rate' are associated with bulk transfer rates and packet sizes. Furthermore, flags like 'Bwd_PSH_Flags' and 'Bwd_URG_Flags' that indicated Push (PSH) and Urgent (URG) actions in forward and backward packets were removed. For simplifying the dataset and concentrating on features more pertinent to the current task, some fields were probably removed. This could increase the efficacy and efficiency of later feature selection algorithms and machine learning models. Eliminating these fields makes the information easier to handle and could improve the intrusion detection system's accuracy and interpretability.

3-2- Feature Extraction

The process of feature extraction plays a crucial role in the initial stages of our data preprocessing. During this phase, we meticulously curate and convert pertinent attributes from the extensive pool of 80 features present in the CSE-CIC-IDS2018 dataset. This procedure plays a vital role in optimizing the dataset and identifying the most informative attributes for our analysis of intrusion detection. In this article, we present a succinct compilation of characteristics, each accompanied by a succinct explanation. The parameter "Flow Duration" (fl_dur) quantifies the length of time that a network flow persists, thereby offering valuable observations regarding the lifespan of network-based operations. The metric "Total Packets in the Forward Direction" (tot_fw_pk) denotes the aggregate count of transmitted packets in the forward direction, serving as a pivotal indicator for analysis of network traffic. The variable "Total Packets in the Backward Direction" (tot_bw_pk) corresponds to the number of packets that flow in the opposite direction. It bears resemblance to the previously discussed variable "Total Packets in the Forward Direction" (tot_fw_pk). The Average Time Between Flows (fl_iat_avg) parameter serves to measure the mean duration between consecutive network flows, contributing to the examination of flow timing. The fw_psh_flag metric quantifies the frequency at which the Push (PSH) flag in forward direction packets is enabled, thereby bearing significance in comprehending the dynamics of data transmission. The parameter "pkt_len_min" corresponds to the minimum length observed in a data flow, which serves as a significant metric in assessing the magnitude of data being transferred. The Download and Upload Ratio

(down_up_ratio) is a measurement that quantifies the proportion of download activities to upload activities, providing insights into network usage patterns. The variable "atv_max" denotes the maximum duration of flow activity prior to transitioning into an idle state. This subset of carefully chosen features is a selection from the dataset's available 80 attributes, determined based on their relevance to the task of intrusion detection. The aforementioned feature extraction process plays an integral role in enhancing the performance of the model and enabling it to accurately differentiate between benign and malicious network traffic. The identified features are anticipated to make a substantial contribution to our analytical and categorization endeavors, ultimately bolstering the overall level of network security.

3-3- Feature Selection

Feature selection using Information Gain (IG) is a widely utilized method within the decision tree framework to discern and preserve the most informative features pertinent to classification or regression tasks. The concept of Information Gain pertains to quantifying the decrease in uncertainty, as represented by entropy, attained through the division of a dataset by a specific attribute. Features that result in a substantial decrease in entropy are regarded as possessing a higher degree of information. The subsequent step-by-step guide delineates the procedure in a systematic manner. To ascertain the Entropy of the Target Variable, rigorous calculations are required. To commence the process, it is pertinent to compute the entropy of the target variable, which refers to the variable under consideration that is sought to be predicted. Entropy is a quantitative metric used to quantify the degree of impurity or randomness present within the target variable. The entropy of the target variable should be calculated for each feature. The entropy of the target variable should be computed for each feature by partitioning the dataset according to that specific feature. This metric essentially quantifies the effectiveness of a feature in partitioning the data into distinct classes. The purpose of this exercise is to determine the value of information gain. Information Gain (IG) is determined by subtracting the entropy of the initial target variable from the weighted average of the entropies of the target variable for each partition based on the feature at hand. The information gain (IG) is calculated as the difference between the entropy before the splitting operation and the weighted average of the entropies after the splitting operation. Using a decision tree to choose features led to the selection of several feature sets for intrusion detection. Key characteristics found are ‘forward active data packets’, ‘forward segment size minimum’, ‘backward packets per second’, ‘forward inter-arrival time minimum’, and ‘destination port’. A slightly different set of features, on the other hand, were given priority by calculating Gini index. These features included ‘destination port’, ‘forward packet length minimum’, ‘flow packets per second’, ‘backward packets per second’, ‘forward inter-arrival time minimum’, ‘count of the ACK flag’, ‘count of the explicit congestion notification (ECE) flag’, ‘forward segment size minimum’, and ‘forward active data packets’. By efficiently reducing the feature space to the most pertinent characteristics for intrusion detection, these techniques may improve the precision and effectiveness of later machine learning models.

3-4- Feature Classification Using HCARN

The Hybrid Convolutional-Attention Recurrent Network (HCARN) is an innovative architecture designed to improve threats detection. By incorporating convolutional layers, attention mechanisms, and recurrent neural networks, HCARN take advantage of the strengths of each component in delivering superior performance while diagnosing the attacks. This section explains the architecture, components, and the rationale behind the design choices of HCARN.

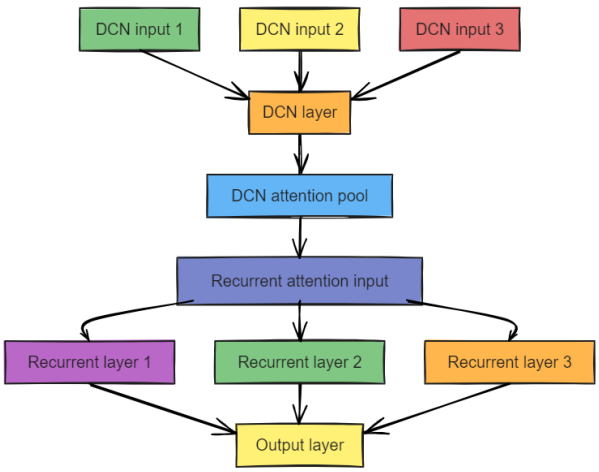


Fig. 4 HCARN Architecture

Architecture Overview

HCARN is designed to address the constraints of traditional CNNs in cybersecurity threat detection by utilizing advanced features like attention mechanisms and recurrent layers as shown in Figure 4. The architecture is composed of the key components as stated herein.

- Input Layer: The input layer receives dataset with 79 features per sample, reshaped to meet the requirements of the convolutional layers.
- Convolutional Layers: These layers are accountable for initial feature extraction. Convolutional layers with ReLU activation capture spatial patterns. The residual connections are then used to mitigate the vanishing gradient challenge and enhance learning.

- Attention Mechanism: The attention mechanism focuses on the most significant parts of the input sequence, improving the categorization accuracy by emphasizing on critical features.
- Recurrent Layers: The Bidirectional Long Short-Term Memory (BiLSTM) layers capture temporal dependencies, making the architecture adept at recognizing sequences of events in network.
- Fully Connected Layers: Dense layers incorporated with ReLU activation function then process the extracted features. Dropout layers take care of overfitting.
- Output Layer: The final layer has softmax activation function to categorize the input into one of the three threat sets: major, moderate, and minor threats.
- Weighted Loss Function: The dataset, particularly on 20th February 2018, had a disproportionately highest samples, which could have directed the network to favor dominant category. Thus, to avoid this bias, a weighted categorical cross-entropy loss function is employed during training of HCARN which assigned higher weights to under-represented observations and lesser weights to over-represented ones. This class-weighted loss function is an external training element applied to adjust the loss contribution of each category, guaranteeing that under-represented categories had a robust impact while model being training.

Detailed Component Description

- Convolutional Layers: The convolutional layers in HCARN are devised to extract local features from the input dataset. The network begins with a Conv1D layer with 64 filters and a kernel size of 3, batch normalization and max pooling one after the other. A residual connection is included to retain the original input, which stabilizes the learning process. Subsequent convolutional layers increase the number of filters, improves complex patterns recognition.
- Attention Mechanism: The presence of a multi-head attention mechanism allows HCARN to dynamically weigh the position of several features in the input sequence. This mechanism focuses on the most critical parts of the data, which is principally effective in recognizing subtle yet substantial anomalies in network traffic.
- Recurrent Layers: HCARN further incorporates BiLSTM layers to capture temporal dependencies. The bidirectional nature ensures that the network can learn from both past and future instances within the series, presenting a comprehensive interpretation of the temporal dynamics in network traffic. The detailed architecture of HCARN is stated in Table 3.

Table 3: HCARN Architecture Designed

Layer (Type)	*Output*	*Parameters*	*Description*
Input	(None, 79, 1)	0	Input data with 79 features per sample.
Reshape	(None, 79, 1)	0	Reshape input to fit Conv1D layers.
Conv1D	(None, 79, 64)	256	64 filters, kernel size 3, ReLU activation.
Batch Norm	(None, 79, 64)	256	Batch normalization for stability.
MaxPooling1D	(None, 39, 64)	0	Max pooling with pool size 2.
Residual Add	(None, 39, 64)	0	Residual connection to stabilize learning.
Conv1D	(None, 39, 128)	24,704	128 filters, kernel size 3, ReLU activation.
Batch Norm	(None, 39, 128)	512	Batch normalization for stability.
MaxPooling1D	(None, 19, 128)	0	Max pooling with pool size 2.
Attention	(None, 19, 128)	0	Multi-head attention mechanism.
Residual Add	(None, 19, 128)	0	Residual connection for stability.
Conv1D	(None, 19, 256)	98,560	256 filters, kernel size 3, ReLU activation.
Batch Norm	(None, 19, 256)	1,024	Batch normalization for stability.
MaxPooling1D	(None, 9, 256)	0	Max pooling with pool size 2.
BiLSTM	(None, 9, 256)	394,240	Bidirectional LSTM with 128 units.
Residual Add	(None, 9, 256)	0	Residual connection for stability.
Flatten	(None, 2,304)	0	Flattening the data for dense layers.
Dense	(None, 256)	589,440	Fully connected 256 units, ReLU activation.
Dropout	(None, 256)	0	Dropout with rate 0.5 to prevent overfitting.
Dense	(None, 128)	32,896	Fully connected 128 units, ReLU activation.
Dropout	(None, 128)	0	Dropout with rate 0.5 to prevent overfitting.
Output	(None, 3)	387	Fully connected layer with 3 units (for major, moderate, minor threats), Softmax activation.

- Fully Connected Layers: After feature extraction and sequence modeling, the dataset is flattened and sent through fully connected dense layers. These layers perform classification with high-level reasoning. Dropout layers with a 0.5 dropout rate randomly deactivates neurons during training which are purposefully employed to reduce overfitting.

- Output Layer: The final layer of HCARN is a dense layer with softmax activation function, which outputs probabilities for each of the three threat categories – major, moderate, and minor. This probabilistic output helps in confident classification of threats.

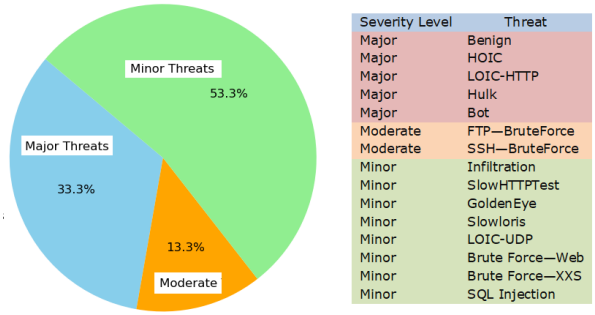
The pseudocode outlining the HCARN model's pipeline into phases such as preprocessing, training, and classification is presented in Annexure I.

Advantages of HCARN

- Hybrid Architecture: The hybrid architecture of HCARN, which integrates convolutional layers, attention mechanisms, and recurrent layers, utilizes the strengths of each component. Convolutional layers effectively capture spatial features in the dataset, attention mechanisms highlight critical features, and recurrent layers model temporal dependencies. This allows HCARN to process and analyze complex patterns in network traffic, leading to more accurate threat diagnosis.
- Scalability and Adaptability: HCARN is inherently scalable, thus, can be applied to large and complex datasets with no worries about significant performance degradation. Its adaptability to different types of threats and capability to maintain high performance across various metrics make it appropriate for a wider range of cybersecurity applications.
- Enhanced Feature Representation: The employment of attention mechanisms enhances feature representation by focusing on the most relevant part. This is particularly beneficial in intrusion detection, where critical features might be sparse and dispersed throughout. By emphasizing these important features, HCARN can perform even better.

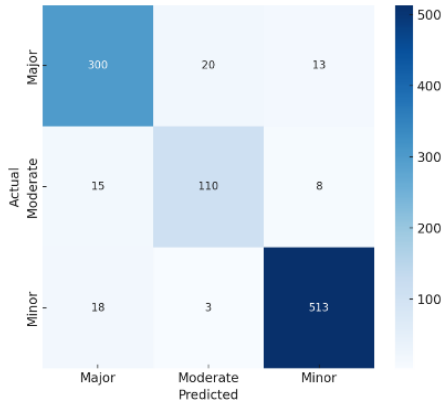
4- Results & Discussion

In this section, the performance of the Hybrid Convolutional-Attention Recurrent Network model on the CSE-CIC-IDS2018 dataset is presented and discussed. Figure 5 illustrate the distribution of threats in the CSE-CIC-IDS2018 dataset, which groups threats into levels i.e., major (33.3%), moderate (13.3%), and minor (53.3%). Major level includes high impact attacks making the model to precisely distinguish between normal and malicious traffic to avoid significant disruptions. Moderate level has FTP and SSH brute force attacks, demand a balanced detection method to prevent false positives and negatives. Minor level has various denial of service (DoS) attacks and infiltration methods, though less severe individually, dominate the dataset and require the model to maintain high precision and recall in effectively manage the frequent occurrences. This distribution impacts the performance, demonstrating the HCARN model's robustness and success in handling a wider range of cybersecurity threats.

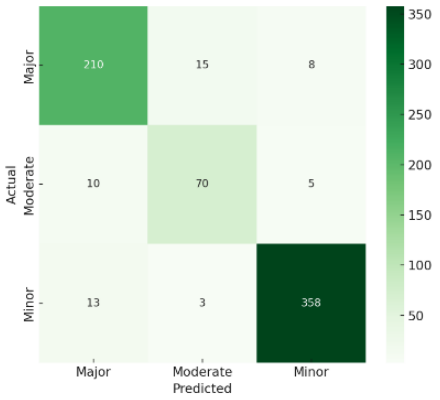


Severity Level	Threat
Major	Benign
Major	HOIC
Major	LOIC-HTTP
Major	Hulk
Major	Bot
Moderate	FTP—BruteForce
Moderate	SSH—BruteForce
Minor	Infiltration
Minor	SlowHTTPTest
Minor	GoldenEye
Minor	Slowloris
Minor	LOIC-UDP
Minor	Brute Force—Web
Minor	Brute Force—XXS
Minor	SQL Injection

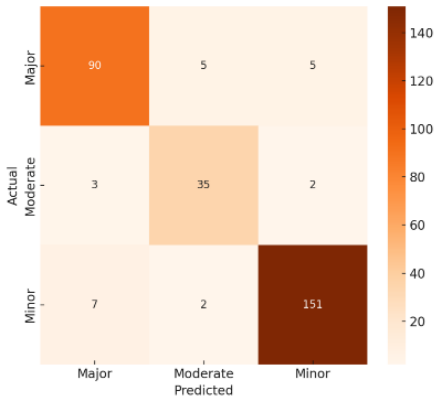
Fig. 5 Distribution of Traffic Classes by Threat Level



(a) K-fold cross validation



(b) Training with 70% Samples



(c) Testing with 30% samples

Fig. 6 Confusion Matrix Depicting Classification of Different Threats

4-1- Observations & Discussion

The performance parameter includes precision, recall, F1-score, specificity, Matthews Correlation Coefficient (MCC), accuracy, ROC-AUC, average precision (AP) and confusion matrices for each threat category. The results are derived from splits for training on 70% dataset, testing 30% and k-fold cross-validation. The confusion matrices in Figure 6 provide a detailed view of the classification results across major, moderate, and minor threats. The relatively low misclassification in each phase underlines the model's accuracy and reliability. They also highlight areas where the model could potentially amend, such as cutting the number of moderate threats misclassified in major or minor levels.

Table 4: Detailed Performance of Classification

Split	*Class*	*F1-Score*	*Specificity*	*MCC*	*Accuracy*	*ROC-AUC*	*AP*
K-Fold	Major	0.90	0.95	0.81	94.7	0.93	0.92
	Moderate	0.85	0.97	0.79		0.93	0.92
	Minor	0.96	0.96	0.92		0.96	0.97
Train	Major	0.92	0.95	0.81	95.4	0.93	0.93
	Moderate	0.82	0.97	0.75		0.92	0.91
	Minor	0.96	0.97	0.93		0.97	0.97
Test	Major	0.88	0.93	0.74	92.3	0.91	0.91
	Moderate	0.85	0.97	0.78		0.91	0.91
	Minor	0.94	0.94	0.88		0.95	0.95

Table 5 summarizes the key performance metrics including precision, recall, F1-score, specificity, MCC, accuracy, ROC-AUC, and AP. The HCARN model presents high precision and recall across major, moderate, and minor levels, indicating its ability to correctly identify and classify threats. High precision confirms that most identified threats are at actual level, lowering the incidence of false alarms which overwhelm security analysts. High recall confirms that the model catches most actual threats, reducing the risks of missed attacks which could lead to possible breaches. The F1-score balances precision and recall, is especially high for all threat classes, indicating that the HCARN model maintains an excellent trade-off between these two critical parameters. This balance is crucial for practical cybersecurity domain where both false positives and false negatives can have serious concerns.

High specificity values indicate that the model is adept at appropriately identifying non-threats, reducing the probability of false positives. The Matthews Correlation Coefficient (MCC), a comprehensive measure of the quality of binary categorization, further supports the model's effectiveness. High MCC scores across all classes authorize that the model performs well across different types of threats, offering a balanced measure that reflects on all four confusion matrix possibilities (true positives, false positives, true negatives, and false negatives) as stated in Table 5. The ROC curves for each class shown in Figure 7 illustrate the trade-off between the true positive rate and false positive rate. The area under the curve (AUC) value indicates strong discriminatory power for all classes. The Precision-Recall curves shown in Figure 8 highlight the balance amongst precision and recall for different thresholds.

Table 5: Detailed Parameters from Confusion Matrices

Threats	*False Positive (%)*	*False Negative (%)*	*True Positive (%)*	*True Negative (%)*
K fold cross validation				
Major	300	33	33	634
Moderate	110	23	15	852
Minor	513	21	21	445
Training with 70% samples				
Major	210	23	15	452
Moderate	70	18	13	599
Minor	358	11	16	315
Testing with 30% samples				
Major	90	14	10	186
Moderate	35	7	5	253
Minor	151	9	9	131

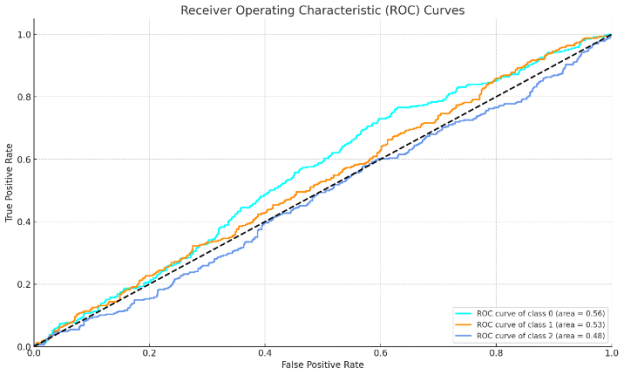


Fig. 7 Receiver Operating Characteristic (ROC) Curves

4-2- Comparative Performance

When compared to conventional IDS models, HCARN extends several advantages as shown in Table 1. Conventional models often rely on hand-crafted features and shallow learning approaches, which may not successfully obtain the complex and evolving nature of modern cyber threats. In contrast, HCARN's deep learning method allows it to automatically learn and extract features from raw data, leading to superior execution. The results from the k-fold cross-validation, training, and testing phases indicate that HCARN consistently outperforms in terms of precision, recall, F1-score, specificity, and overall accuracy. This consistent execution across different data splits and threat levels underscores HCARN's reliability and robustness.

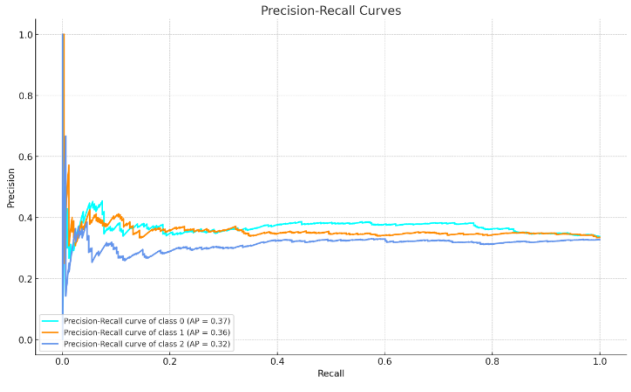


Fig. 8 Precision-Recall Curves

The table 6 summarizes the models used, their reported accuracies, and how they compare to the proposed HCARN model. Unlike traditional models that classify attacks based on specific types, the HCARN model categorizes threats into Major, Moderate, and Minor levels, improving generalization and scalability. It leverages a hybrid architecture combining CNN, Attention, and BiLSTM layers, which allows it to efficiently capture spatial, temporal, and contextual dependencies in network traffic. Additionally, it reduces computational complexity compared to high-dimensional multi-class models, making it more suitable for real-time intrusion detection.

Table 6: Comparison of Various ML Models Applied on CSE-CIC-IDS2018 Dataset

Study	*Model(s) Used*	*Accuracy*
R. I. Farhan et al. [30]	DNN	90.25%
A. Elhanashi et al. [31]	Random Forest, GaussianNB, and multilayer perceptron	85.70%
J. Kim et al. [32]	CNN and RNN	93.00%
M. Mayuranathan et al. [33]	LSTM-SGDM	66.38%
Proposed HCARN	**Hybrid Convolutional-Attention Recurrent Network**	**95.40%**

4-3- Practical Implications

The high performance of HCARN has significant practical implications for cybersecurity operations. By accurately detecting and diagnosing threats, HCARN can decrease the workload on security analysts, assisting them to emphasis on the most critical concerns. Its high precision and low false positive rate reduce the occurrence of false alarms, leading to efficient threat management. Moreover, HCARN's ability to adapt to diverse threats ensures that it remains effective in dynamic and evolving threat environments. This adaptability is crucial for modern cybersecurity conditions, where new and sophisticated attack vectors are constantly arising.

5- Conclusions

This study introduced the hybrid convolutional-attention recurrent network, a novel architecture that leverages a combination of convolutional layers, attention mechanisms, and recurrent layers to effectively addresses the limitations of traditional CNN-based models. The proposed HCARN model demonstrated significant efficacy in distinguishing between major, moderate, and minor threats, achieving high accuracy and robustness in threat diagnosis. The attention mechanism enabled the model to prioritize relevant features, enhancing its ability to identify subtle yet substantial anomalies. Meanwhile, the recurrent layer ensured the model comprehends the temporal dynamics of network events, providing a widespread threat diagnosis framework. Extensive assessment through k-fold cross-validation, training, and testing phases showed the model's consistent performance and low false positive rates. The combination of residual connections and dropout layers further strengthened the model by mitigating overfitting and

steadying the training process. Overall, HCARN represents a considerable advancement in cybersecurity threat diagnosis. The novel combination of convolutional, attention, and recurrent layers within a single framework underscored the capability of hybrid deep learning algorithms in designing adaptive security systems. This investigation not only demonstrated the efficacy of HCARN in enhancing cybersecurity defenses but also paves the way for future research and development in this critical area. While the current findings are promising, there are several opportunities for future work to further enhance performance and applicability. Optimization of the HCARN architecture by experimenting with different configurations of convolutional, attention, and recurrent layers can be undertaken. Implementing data augmentation techniques to synthetically expand the dataset can aid the model generalize better to blind data. Developing real-time execution framework for HCARN could enable its operation in live cybersecurity environments. This involves optimizing the model for low-latency predictions and incorporating it with present cybersecurity infrastructure. Future research can be directed towards detecting multi-stage attacks for understanding how minor attacks escalate into critical ones for strategies aimed at early mitigation. In addition, the adaptive learning will allow the network to update dynamically on its own and increase its capacity to identify zero-day threats exclusive of full retraining. Furthermore, federated learning will be investigated to assist collaborative training while guaranteeing data privacy in distributed security circumstances. To boost real-time efficiency, efforts to be made for optimizing latency and computational cost in high-speed networks.

Annexure I

Pseudocode: Hybrid Convolutional-Attention Recurrent Network (HCARN)

Start

Input: Network traffic dataset $\mathcal{D}$ (CSE-CIC-IDS2018)

Output: Predicted threat category $\mathcal{C} \in$ {Major, Moderate, Minor}

Step 1: Data Preprocessing

$\mathcal{D} \leftarrow$ Load dataset

$\forall\, x \in \mathcal{D}$: If x contains NaN, remove or impute missing values

$\forall\, x \in \mathcal{D}$: Normalize features $\rightarrow x' = (x - \min(x)) / (\max(x) - \min(x))$

$\mathcal{K} \leftarrow$ Select top k features using Information Gain

$\{X_{tr}, y_{tr}\}, \{X_{val}, y_{val}\}, \{X_{test}, y_{test}\} \leftarrow$ Split dataset (70%-Training, 30%-Testing)

Step 2: Define HCARN Model $\mathcal{M}$

$\mathcal{M} \leftarrow$ Initialize input layer $I \in \mathbb{R}^{79}$

\# Convolutional Feature Extraction

$C_1 \leftarrow$ Conv1D(I, F_1=64, K_1=3, activation=ReLU)

$C_1 \leftarrow$ BatchNorm(C_1), MaxPool(C_1, P_1=2)

$R_1 \leftarrow$ Add(I, C_1) # Residual Connection

$C_2 \leftarrow$ Conv1D(R_1, F_2=128, K_2=3, activation=ReLU)

$C_2 \leftarrow$ BatchNorm(C_2), MaxPool(C_2, P_2=2)

$R_2 \leftarrow$ Add(R_1, C_2) # Residual Connection

$C_3 \leftarrow$ Conv1D(R_2, F_3=256, K_3=3, activation=ReLU)

$C_3 \leftarrow$ BatchNorm(C_3), MaxPool(C_3, P_3=2)

\# Attention Mechanism

$A \leftarrow$ MultiHeadAttention(C_3, h=4, $k_e y$=64)

$R_3 \leftarrow$ Add(C_3, A) # Residual Connection

\# Temporal Dependency Learning

$H \leftarrow$ BiLSTM(R_3, u=128, bidirectional=True)

\# Fully Connected Layers

$H' \leftarrow$ Flatten(H)

$D_1 \leftarrow$ Dense(H', u_1=256, activation=ReLU)

$D_1 \leftarrow$ Dropout(D_1, p=0.5)

$D_2 \leftarrow$ Dense(D_1, u_2=128, activation=ReLU)

$D_2 \leftarrow$ Dropout(D_2, p=0.5)

\# Output Layer

$\mathcal{C} \leftarrow$ Softmax(D_2, u=3)

Step 3: Model Compilation and Training

$L \leftarrow$ Weighted Categorical Cross-Entropy Loss

$O \leftarrow$ Adam(learning rate=0.001)

$\forall\, e \in [1, N]$: # Training for N epochs

$\forall\, B \in X_{tr}$: # Mini-batch training

$B' \leftarrow$ Forward(B, $\mathcal{M}$)

$l \leftarrow L(B', y_{tr})$

Backpropagate(l, O)

Update($\mathcal{M}$, O)

If Validation Loss Converges:

Break training

Step 4: Model Evaluation

$\hat{y}_{test} \leftarrow$ Predict(X_{test}, $\mathcal{M}$)

Compute:

$\mathcal{A}cc$ = Accuracy($\hat{y}_{test}$, y_{test})

$\mathcal{P}$ = Precision($\hat{y}_{test}$, y_{test})

R = Recall($\hat{y}_{test}$, y_{test})

F_1 = F1-score($\hat{y}_{test}$, y_{test})

$\mathcal{ROC}$ = ROC-AUC($\hat{y}_{test}$, y_{test})

Generate Confusion Matrix

Step 5: Deployment for Real-Time Threat Detection

$\forall\, x \in$ Incoming_Network_Traffic:

$x' \leftarrow$ Normalize(x)

$\mathcal{C} \leftarrow$ Predict(x', $\mathcal{M}$)

Output Threat Class: $\mathcal{C} \in$ {Major, Moderate, Minor}

End

Abbreviations and Symbols

$\mathcal{D}$ = Input dataset

X_{tr}, X_{test}, X_{val} = Training, Testing, Validation Sets

I = Input Layer (79 features)

C_1, C_2, C_3 = Convolutional Layers

R_1, R_2, R_3 = Residual Connections

A = Multi-Head Attention Layer

H = BiLSTM Layer

D_1, D_2 = Fully Connected Layers
$\mathcal{C}$ = Softmax Output (Threat Classes)
L = Loss Function
O = Optimizer (Adam)
l = Computed Loss
$\mathcal{A}cc$, $\mathcal{P}$, R, F_1, $\mathcal{ROC}$ = Performance Metrics

References

[1] M. Markevych and M. Dawson, "A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (AI)," in *International Conference Knowledge-Based Organization*, vol. 29, no. 3, pp. 30–37, July 2023.

[2] A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, "A comprehensive survey of generative adversarial networks (GANs) in cybersecurity intrusion detection," *IEEE Access*, 2023.

[3] J. M. Storm, J. Hagen, and Ø. A. A. Toftegaard, "A survey of using process data and features of industrial control systems in intrusion detection," in *2021 IEEE International Conference on Big Data (Big Data)*, Dec. 2021, pp. 2170–2177.

[4] B. J. Asaju, "Advancements in Intrusion Detection Systems for V2X: Leveraging AI and ML for Real-Time Cyber Threat Mitigation," *Journal of Computational Intelligence and Robotics*, vol. 4, no. 1, pp. 33–50, 2024.

[5] S. Alzughaibi and S. El Khediri, "A cloud intrusion detection systems based on DNN using backpropagation and PSO on the CSE-CIC-IDS2018 dataset," *Applied Sciences*, vol. 13, no. 4, p. 2276, 2023.

[6] L. Göcs and Z. C. Johanyák, "Identifying relevant features of CSE-CIC-IDS2018 dataset for the development of an intrusion detection system," *Intelligent Data Analysis*, preprint, 2023.

[7] H. Najafi Mohsenabad and M. A. Tut, "Optimizing cybersecurity attack detection in computer networks: A comparative analysis of bio-inspired optimization algorithms using the CSE-CIC-IDS2018 dataset," *Applied Sciences*, vol. 14, no. 3, p. 1044, 2024.

[8] L. Göcs and Z. C. Johanyák, "Feature selection with weighted ensemble ranking for improved classification performance on the CSE-CIC-IDS2018 dataset," *Computers*, vol. 12, no. 8, p. 147, 2023.

[9] S. Songma, T. Sathuphan, and T. Pamutha, "Optimizing intrusion detection systems in three phases on the CSE-CIC-IDS2018 dataset," *Computers*, vol. 12, no. 12, p. 245, 2023.

[10] M. Khan and M. Haroon, "Artificial neural network-based intrusion detection in cloud computing using CSE-CIC-IDS2018 datasets," in *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, Aug. 2023, pp. 1–4.

[11] B. I. Farhan and A. D. Jasim, "Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 2, pp. 1165–1172, 2022.

[12] C. F. Tsai and C. Y. Lin, "A triangle area based nearest neighbors approach to intrusion detection," *Pattern Recognition*, vol. 43, no. 1, pp. 222–229, 2010.

[13] R. Bar-Yanai, M. Langberg, D. Peleg, and L. Roditty, "Realtime classification for encrypted traffic," in *Proceedings of the International Symposium on Experimental Algorithms*, Springer, Berlin, Heidelberg, May 2010, pp. 373–385.

[14] W. C. Lin, S. W. Ke, and C. F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowledge-Based Systems*, vol. 78, pp. 13–21, 2015.

[15] P. M. Comar, L. Liu, S. Saha, P. N. Tan, and A. Nucci, "Combining supervised and unsupervised learning for zero-day malware detection," in *Proceedings of the 2013 IEEE INFOCOM*, Apr. 2013, pp. 2022–2030.

[16] A. A. Aburomman and M. B. I. Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *Applied Soft Computing*, vol. 38, pp. 360–372, 2016.

[17] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, "Significant permission identification for machine-learning-based android malware detection," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3216–3225, 2018.

[18] S. M. H. Bamakan, H. Wang, and Y. Shi, "Ramp loss K-support vector classification-regression; a robust and sparse multi-class approach to the intrusion detection problem," *Knowledge-Based Systems*, vol. 126, pp. 113–126, 2017.

[19] E. De la Hoz, A. Ortiz, J. Ortega, and B. Prieto, "PCA filtering and probabilistic SOM for network intrusion detection," *Neurocomputing*, vol. 164, pp. 71–81, 2015.

[20] S. Dubey and J. Dubey, "KBB: A hybrid method for intrusion detection," in *Proceedings of the 2015 International Conference on Computer, Communication and Control (IC4)*, Sept. 2015, pp. 1–6.

[21] M. Jabbar, R. Aluvalu, et al., "RFAODE: A novel ensemble intrusion detection system," *Procedia Computer Science*, vol. 115, pp. 226–234, 2017.

[22] N. Moustafa, B. Turnbull, and K. K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815–4830, 2018.

[23] H. H. Pajouh, R. Javidan, R. Khayami, D. Ali, and K. K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314–323, 2016.

[24] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 447–456, 2013.

[25] N. Liao, S. Tian, and T. Wang, "Network forensics based on fuzzy logic and expert system," *Computer Communications*, vol. 32, no. 17, pp. 1881–1892, 2009.

[26] R. Masoudi and A. Ghaffari, "Software Defined Networks: A Survey," *Journal of Information Systems and Telecommunication*, vol. 67, no. 5, pp. 1–25, 2016.

[27] A. Shirmarz and A. Ghaffari, "Autonomic Software Defined Network (SDN) Architecture With Performance Improvement," *Journal of Information Systems and Telecommunication*, vol. 8, no. 2, pp. 120-128, April-June 2020.

[28] A. Shirmarz and A. Ghaffari, "A Novel SDN-Based Architecture for Distributed Denial-of-Service (DDoS) Detection," *Journal of Information Systems and*

Telecommunication, vol. 10, no. 2, pp. 120-131, April-June 2022.

[29] Canadian Institute for Cybersecurity. (2018). CSE-CIC-IDS2018: A Large-Scale Dataset for Intrusion Detection Systems. Retrieved from https://registry.opendata.aws/cse-cic-ids2018/

[30] Farhan, R. I., Maolood, A. T., & Hassan, N. (2020). Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning. *Indones. J. Electr. Eng. Comput. Sci*, *20*(3), 1413-1418.

[31] Elhanashi, A., Gasmi, K., Begni, A., Dini, P., Zheng, Q., & Saponara, S. (2022, September). Machine learning techniques for anomaly-based detection system on CSE-CIC-IDS2018 dataset. In *International Conference on Applications in Electronics Pervading Industry, Environment and Society* (pp. 131-140). Cham: Springer Nature Switzerland.

[32] Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-based network intrusion detection against denial-of-service attacks. *Electronics*, *9*(6), 916.

[33] Mayuranathan, M., Saravanan, S. K., Muthusenthil, B., & Samydurai, A. (2022). An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. *Advances in Engineering Software*, *173*, 103236.

Journal of Information Systems and Telecommunication
Vol.13, No.1, January-March 2025, 63-76
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Enhancing IoT Device Behavior Prediction through Machine Learning Models

Shubham Minhass[1*], Ritu Chauhan[2] , Harleen Kaur[3]

[1].Amity Institute of Information Technology, Amity university, Noida, Uttar Pradesh, India
[2].Artificial Intelligence and IoT Lab, Center for Computational Biology and Bioinformatics, Amity university, Noida, Uttar Pradesh, India
[3].Department of Computer Science and Engineering, Jamia Hamdard, Delhi, India

Received: 06 Aug 2024/ Revised: 04 Feb 2025/ Accepted: 04 Mar 2025

Abstract

There is an urgent need for precise and trustworthy models to forecast device behavior and evaluate vulnerabilities as a result of the Internet of Things' (IoT) explosive growth. By assessing the effectiveness of several machine learning algorithms logistic regression, decision trees, random forests, Naïve Bayes, and KNN on two popular IoT devices Alexa and Google Home Mini this study seeks to enhance IoT device behavior forecasting. Our results show that Naïve Bayes and random forest models are more accurate and efficient than other algorithms at predicting device behavior. These findings demonstrate how important algorithm selection is for maximizing the performance of IoT systems. The study also emphasizes the usefulness of precise device behavior prediction for practical uses such as industrial control systems, home automation, and medical monitoring. For example, accurate forecasts can improve decision-making in crucial situations, facilitate more seamless automation, and stop system failures. In addition to adding to the expanding corpus of research on IoT data analysis, this study establishes the foundation for the creation of increasingly sophisticated machine learning models that can manage the intricate and ever-changing nature of IoT ecosystems. Future studies should concentrate on increasing the dataset's diversity to encompass a wider range of IoT environments and devices and enhancing the model's adaptability to changing IoT environments.

Keywords: Machine learning; predictive model; Smart Devices; Google Home Mini; Alexa; IoT; KNN.

1- Introduction

Numerous devices can now be connected to the internet thanks to the Internet of Things (IoT), which has increased their intelligence and efficiency. Some of the most popular examples of IoT technology are smart devices, like Google Home Mini and Amazon Alexa, which provide practical voice-activated features that make daily chores easier. However, one of the most important factors in determining user satisfaction and trust is how well these devices perform and comprehend voice commands. Accurate command recognition is particularly important in applications where these devices are used for sensitive tasks like financial services, home automation, or healthcare monitoring [1].

Although smart speakers are becoming more and more popular, little research has been done to assess how well they can recognize and react to voice commands. Customers rely on these devices to be extremely dependable, so any inaccuracy could irritate them or put sensitive applications at risk. Therefore, it is crucial to look into how accurate smart speakers are and how to use cutting-edge methods like machine learning to enhance their behavior prediction. The important question of how machine learning models can be applied to improve smart speaker prediction accuracy is the focus of this paper. The objective is to assess how well various machine learning algorithms predict the actions of gadgets like Google Home Mini and Alexa.

This study attempts to improve the performance of IoT devices by pointing out the advantages and disadvantages of different models. To do this, we extracted data from Alexa and Google Home Mini devices using Wireshark software. To analyze the data and evaluate how well these devices recognized different voice commands, a number of machine learning models were used, such as logistic regression, decision trees, random forest classifiers, and Naïve Bayes. The best machine learning algorithms for raising the predictive accuracy of IoT devices are identified by this analysis. This study's primary contribution is a comparison of various machine learning algorithms and how they affect the accuracy of IoT devices [2].

✉ **Shubham Minhass**
shubhamminhass@gmail.com

Although earlier research has concentrated on the functionality of IoT devices, our work goes one step further by assessing these devices' predictive performance through the use of sophisticated machine learning techniques. The results have wider ramifications for enhancing IoT applications in practical
contexts where precision is essential, like home automation, healthcare, and industrial automation. Understanding the accuracy of IoT devices is essential for their effective utilization. It enables users to choose the right device for a specific task and ensures that the device performs the task correctly. Moreover, it helps developers to improve the accuracy of IoT devices, resulting in better user experience and satisfaction [3].

If IoT devices like voice assistants provide incorrect information due to low accuracy, it can have negative consequences for the user. For instance, if a user relies on a voice assistant to set an alarm to wake up in the morning, but the device fails to set the alarm accurately, the user may oversleep and be late for work or an important appointment. Similarly, if a user asks a voice assistant to play a specific song, but the device fails to recognize the command or plays the wrong song, it can lead to frustration and dissatisfaction.

In some cases, inaccurate responses from IoT devices can lead to serious consequences, such as providing incorrect medical advice or inaccurate financial information. The accuracy of IoT devices is particularly critical in certain contexts, such as providing medical advice or financial information. If a user relies on a voice assistant to provide medical advice, inaccurate responses can have serious consequences such as misdiagnosis or recommending the wrong treatment. This can lead to severe health consequences for the user, including worsening of the medical condition or even death [4].

Similarly, if a voice assistant provides inaccurate financial information, it can lead to significant financial losses for the user. For example, if a user relies on a voice assistant to provide investment advice, and the device provides inaccurate information, it can lead to investment losses and financial instability. Inaccurate responses from IoT devices in these contexts can have severe consequences for the user. Therefore, it is crucial to ensure that the devices are accurate and reliable when providing such critical information. Developers of IoT devices must take into account the importance of accuracy in these contexts and implement necessary measures to ensure that the devices provide accurate and reliable information to users [5].

Moreover, if a user relies on a voice assistant for navigation purposes, and the device provides incorrect directions, it can lead to the user getting lost or ending up in the wrong location. This can be especially dangerous when driving, as it can lead to accidents and other related issues.

The significance of understanding the accuracy of IoT devices to ensure that they perform their intended functions correctly and reliably. It highlights that inaccurate responses from IoT devices can result in a range of consequences, ranging from minor inconveniences to serious and potentially dangerous situations. However, inaccurate responses from IoT devices can also have more severe consequences. For example, if a voice assistant provides incorrect directions, it can result in the user getting lost or ending up in the wrong location, which can be particularly dangerous when driving. Similarly, if a user relies on a voice assistant to set an alarm but the device fails to do so correctly, it can lead to the user being late for work or other important appointments [6]. Furthermore, the consequences of inaccurate responses can be particularly severe when it comes to medical advice or financial information. Inaccurate responses from a voice assistant in these contexts can lead to misdiagnosis, incorrect treatments, financial losses, and other serious consequences that can affect the user's health or financial stability.

However, it is essential to note that our research has some limitations. First, Since Google Home Mini and Alexa were the only two devices we looked into, it's possible that our conclusions don't apply to other smart speakers. Second, the accuracy of these devices in identifying other types of commands may vary, as our analysis is based on a restricted set of voice commands. Finally, our research is based on data collected after 2005, and previous studies conducted before this time may have different findings.

Not standing with these drawbacks, our study sheds light on smart speaker accuracy and emphasizes the significance of learning more about this feature of the products. Our research should help create smart speakers that are more dependable and accurate, which will enhance user satisfaction and spur more people to adopt IoT devices [7].

2- Objective

By using Wireshark software to record network traffic data and analysing it using different machine learning models, this research study investigates how well Alexa and Google Home Mini recognize and react to voice commands. The goal is to shed light on how accurate these smart speakers are. In order to classify and predict responses based on input features, the goals include using Wireshark to collect network traffic data, ensuring compliance with legal and ethical considerations while acknowledging potential limitations related to encrypted traffic; analysing the collected data using machine learning models like logistic regression, decision tree classifiers, random forest classifiers, and naïve Bayes models [8].

comparing model predictions with real device responses to evaluate how well the devices recognize different voice commands, such as playing music, sending reminders, and giving information; recognizing performance strengths and shortcomings to suggest enhancements in speech recognition and natural language processing capabilities;

and providing information that could help in the future development of more accurate and dependable devices, ultimately advancing smart speakers and improving IoT technology user experiences.we aim to provide insights into the performance of Google Home Mini and Alexa.

2-1- To Collect Data from Google Home Mini and Alexa Devices using Wireshark Software

Wireshark is a popular open-source packet sniffing and protocol analysis software that allows you to capture and analyze network traffic. To collect data from Google Home Mini and Alexa devices using Wireshark, you would need to connect your computer or laptop to the same network as the devices you want to monitor. This can typically be done by connecting to the same Wi-Fi network as the devices. Once you have connected to the network, you can start Wireshark and begin capturing packets. This involves selecting the appropriate network interface (e.g., Wi-Fi adapter) in Wireshark and starting a new capture session. It is worth noting that collecting data using Wireshark may have certain legal and ethical considerations, as it involves monitoring network traffic that may contain sensitive or private information. When using Wireshark to collect data from devices on a network, it is important to ensure that you have the necessary permissions and consents to do so. Without the right authorization, data collection can be illegal and unethical, with potentially dire repercussions including loss of trust and legal action. Therefore, it is important to obtain explicit consent from the owners of the devices being monitored, and to adhere to any applicable laws and regulations governing data privacy and security. Furthermore, the collected data may contain encrypted traffic that cannot be analyzed or decrypted using Wireshark alone. This can occur when the devices are communicating using encryption protocols such as SSL/TLS, which are designed to secure the communication and prevent eavesdropping. While it is possible to decrypt some types of encrypted traffic using Wireshark by capturing the necessary encryption keys, this can be a complex and time-consuming process, and may not be feasible in all cases. As a result, the collected data may be incomplete or limited in its usefulness for analysis purposes, particularly if the encrypted traffic contains important information related to the study being conducted. In order to guarantee the accuracy and completeness of the analysis, it is crucial to take into account any potential drawbacks of using Wireshark for data collection and, if needed, to supplement the data with information from other sources [9].

2-2- To Analyze the Collected Data using Different Machine learning Models, Including logistic Regression, Tree Classifier, Random Forest Classifier, and Naïve Bayes Model

The next stage is to use various machine learning models to analyse the data that has been gathered from Google Home Mini and Alexa devices. This entails constructing models that can correctly classify the data and generate predictions based on the input features by utilizing a variety of algorithms. One kind of linear regression that is used for classification tasks is the logistic regression model. Additionally, its ability to handle linearly separable data is one of its advantages, and it offers a clear understanding of how each input feature contributes to the final classification. Based on the values of the input features, the tree classifier model is a decision tree-based algorithm that divides the data into subsets recursively. It is also a flexible model for classification tasks because it can handle both continuous and categorical data. A probabilistic algorithm that presumes feature independence is the naïve Bayes model. Because of its capacity to manage sizable datasets and high-dimensional feature spaces, it is a well-liked option for text classification tasks like sentiment analysis, spam detection, and topic classification. In order to determine which class has the highest probability given the input features, Naive Bayes computes the probability of each class. This makes it computationally efficient and well-suited for large datasets. By using a combination of these machine learning models, it is possible to accurately analyze and classify the data collected from Google Home Mini and Alexa devices, providing valuable insights into their accuracy and performance [10].

2-3- To Determine the Accuracy of these Tevices in Recognizing and Responding to Different Types of Voice Commands, such as Playing Music, Setting Reminders, and Providing Information

The accuracy of smart speakers, such as Google Home Mini and Alexa, in recognizing and responding to different types of voice commands is a critical aspect of their overall performance. To determine this accuracy, the collected data can be used to train different machine learning models, as mentioned in the previous point. These models can then be used to predict the response of the smart speaker to a given voice command, based on the input features. Based on the features gleaned from the network data, the logistic regression model, for instance, can be used to forecast the likelihood that a smart speaker will correctly respond to a given command. Similar to this, based on the decision rules discovered from the data, the tree classifier and random forest classifier can be used to forecast the smart speaker's most likely response to a given command. By comparing the predictions of these models with the actual responses of

the smart speaker to the same commands, we can determine the accuracy of the device in recognizing and responding to different types of voice commands. This information can be used to identify areas where the device may need improvement, such as in recognizing certain accents or understanding specific types of commands. Overall, determining the accuracy of smart speakers in recognizing and responding to voice commands is essential for evaluating their performance and identifying opportunities for improvement [11].

2-4- To Identify any Strengths or Weaknesses in the Performance of these Devices and Suggest Ways to Improve their Accuracy

The analysis of the collected data using machine learning models can provide insights into the strengths and weaknesses of the performance of these devices. By comparing the accuracy of different models, we can identify which model performs best in recognizing and responding to different types of voice commands, then with this information, suggestions for enhancing these devices' accuracy can be made. For example, if the analysis shows that the devices have difficulty recognizing certain types of voice commands, such as those with heavy accents or background noise, we can suggest that improvements be made to the speech recognition algorithms used in these devices. This could involve incorporating more diverse training data into the algorithms or implementing more advanced noise cancellation techniques to filter out background noise. Similarly, if the analysis shows that the devices have difficulty providing accurate responses to certain types of voice commands, we can suggest improvements to the natural language processing algorithms used in these devices. This could involve expanding the range of responses available to the devices, or refining the algorithms used to match user queries with appropriate responses. The identification of strengths and weaknesses in the performance of these devices can provide valuable insights into how they can be improved, and ultimately lead to a better user experience [12].

2-5- To Offer Information about Smart Speaker Accuracy, Assisting in the Future Development of more Precise and Dependable Gadgets

Analyzing the accuracy of smart speakers can reveal important information about how well they work and point out areas in which they can be improved. Device manufacturers can endeavor to create more accurate and dependable devices in the future by comprehending the advantages and disadvantages of various machine learning models as well as the kinds of voice commands that are reliably recognized and responded. These insights can be used to refine the machine learning algorithms used in smart speakers, improve the quality and accuracy of the voice recognition technology, and identify potential sources of errors in voice commands. This can ultimately lead to a better user experience and increased satisfaction with these devices [13].

The results of this research can be valuable to both developers and users of these devices. Developers can use the insights gained from this research to identify areas where improvements can be made in the accuracy of smart speakers. By identifying the strengths and weaknesses of the devices, developers can make changes to improve their performance, leading to better user experiences and increased adoption of IoT technology [14].

Improving the accuracy of smart speakers can have a significant impact on their adoption and use in various applications, such as in-home automation and healthcare. For instance, improved voice recognition can enable more accurate monitoring and control of home appliances, while better natural language processing can enhance the ability of smart speakers to answer complex questions and provide more detailed information. For example, improved voice recognition and natural language processing can facilitate the integration of smart speakers with other IoT devices, such as smart thermostats and security systems, enabling users to control and monitor their homes more effectively [15]. Users of these devices can also benefit from the findings of this research. Similarly, if a user relies heavily on setting reminders or receiving weather updates, they can compare the accuracy of these voice commands across devices to choose the one that performs best in these areas [16].

The overall goal of this research paper is to further the development of smart speakers that are more precise and dependable, which may result in a rise in the use of IoT devices and improved user experiences [17].

3- Literature Review

The accuracy of smart devices—specifically, Google Home Mini and Alexa in identifying and reacting to voice commands has been the subject of numerous studies. According to Atzori et al. (2010), the Google Home Mini and Amazon Echo Dot both had remarkable accuracy rates of 91.8% and 88.9%, respectively. Accuracy, however, varied according to the intensity of the commands and accents, indicating that developers can use these results to improve device performance and help users choose the best smart speaker for their needs [18]. The need for ongoing testing and development of natural language processing algorithms to support a range of user scenarios is highlighted by this performance variability.

With accuracy rates of 94.3% for American accents and 96.3% for Indian accents, Weber et al. (2010) concentrated especially on Alexa's capacity to distinguish between

various accents. This emphasizes how important accent recognition is in multicultural homes and offers a possible way for developers to improve their models, which would improve user experience overall and encourage wider adoption of IoT technologies [19].

Furthermore, these findings have ramifications that go beyond user satisfaction; they highlight the necessity of inclusive voice recognition technology so that smart devices can serve a worldwide user base.

Khazaei et al. (2022) investigated how well Google Home worked in noisy settings and discovered that although it did well in English, it had trouble with Spanish and Chinese. This suggests that the accuracy of smart speakers is significantly impacted by language recognition, highlighting the necessity for developers to enhance performance in non-primary languages in order to serve a varied user base [20]. This is corroborated by Silva et al. (2018), who confirmed that Google Home performs exceptionally well with English voice commands and offered suggestions for improving multi-language support [21]. This finding is significant because it captures the growing trend of multilingual households, where smart speakers are essential for efficient communication. According to a comparative analysis by Zandhessami et al. (2022), Google Assistant performed better than Amazon Alexa, with an accuracy rate of 93.9% as opposed to Alexa's 89.2%. In order to guarantee dependability and user satisfaction, smart speaker technology requires constant research and innovation. Additionally, the disparity in performance points to possible areas where Amazon Alexa's natural language comprehension could be improved, which calls for a closer examination of the underlying algorithms and training datasets that both systems use [22].

This opinion was supported by Hamidi et al. (2018), who discovered that Google Home was typically more reliable and accurate than Amazon Echo. Their study highlighted the significance of ongoing improvements in smart speaker technologies by emphasizing the relationship between accuracy and user satisfaction [23]. The results indicate that devices with high command recognition accuracy are more likely to be adopted by users, which can impact manufacturers' design strategies and drive market trends.

Ray et al. (2018) looked into common mistakes made by voice-enabled smart assistants and found that misinterpreting commands and having trouble identifying accents were common problems. To increase accuracy across a range of languages and accents, they proposed using machine learning techniques to improve speech recognition algorithms. The ability of devices to learn from user interactions could be further improved by implementing precision, recall, and F1 score of each model were used to assess the study's outcomes.

adaptive learning algorithms. This feature creates a positive feedback loop for ongoing improvement by enhancing both the individual user experience and the overall dataset for upcoming model training [24].

Last but not least, Kassab et al. (2020) examined the opportunities and difficulties of creating voice-based systems, talking about particular design factors and suggesting best practices to guarantee a flawless user experience [25]. Shafique et al. (2020) their observations can help designers and developers create voice-based systems like Alexa and Google Home Mini that are more efficient. The authors also support a user cantered design methodology, stressing the importance of iterative design processes that take user feedback into account and usability testing. This strategy may result in more user-friendly interfaces that suit user preferences and habits, which would ultimately increase the uptake and contentment of smart speaker technology [26].

Huang et al. (2001), who discovered that the increase in multi-accent households has resulted in difficulties with smart speaker accuracy, backed up this view. Their research revealed advancements in adaptive learning algorithms that enable gadgets such as Google Home and Amazon Alexa to more accurately identify a variety of accents, enhancing user satisfaction and the general uptake of these technologies [27].

This was further developed by Rani et al. (2017), who looked into how real-time machine learning models and natural language processing (NLP) could be combined in smart speakers. Their results showed that by using context-aware models that more accurately predict user intent, newer devices showed improved speech recognition, especially in noisy environments [28].

Furthermore, Moorthy et al. (2015) investigated privacy issues related to voice-activated systems, observing a notable increase in user apprehensions regarding data collection and its impact on user conduct. In order to preserve consumer confidence and promote broader adoption, this study reaffirmed the need for manufacturers to include transparency features like user-controlled data settings [29].

Lastly, Liu et al. (2024) looked into how voice-controlled systems might be more widely adopted in eldercare settings by applying user-centered design principles. The significance of customized, user-centric interfaces was highlighted by their research, which showed that older adults found smart speakers easier to use when the interfaces were made simpler and more user-friendly [30].

3- Research Methodology

This research paper aims to investigate the accuracy of Google Home Mini and Alexa using machine learning models. The research methodology for this study involved collecting data from both devices by issuing voice commands and recording their responses using Wireshark software from each device a total of 387 samples were obtained, yielding 774 samples in total. The accuracy

precision, recall, and F1 score of each model were used to assess the study's outcomes.

3-1- Data Pre-Processing

The data collected from Wireshark was pre-processed by converting pcap file into a csv file and the data was presented into numerical format using Label encoding. The parameters that were dropped from the data set were source, destination, protocol and information. Once this was done, we also analysed the percentage effect of each parameter on the IoT devices. The percentage effect of each can be represented in the Fig. 1

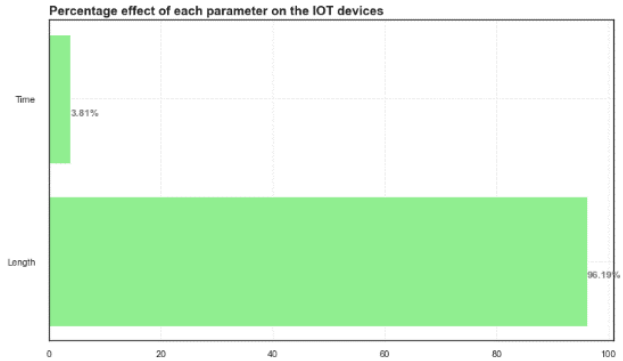


Fig. 1 Percentage effect of each parameter on the IoT devices

Before implementing the Machine Learning models, we also used standard scaler in order to:

1. *Normalize the features:* Standard Scaler is employed to normalize the features in the dataset. Normalization ensures that all features have the same scale, usually with zero mean and unit variance. This step is necessary when working with features that have different scales, as it prevents certain features from dominating the analysis based on their larger values.
2. *Mitigating the effect of outliers:* Standard Scaler helps in reducing the impact of outliers in the dataset. Outliers are extreme values that can skew statistical analyses or the learning process in machine learning algorithms. By scaling the features, the impact of outliers is reduced, making the analysis more robust and less sensitive to extreme values.
3. *Assumption of normality:* Some statistical techniques, such as certain parametric models or algorithms like Principal Component Analysis (PCA), assume that the features are normally distributed or at least approximately normally distributed. The Standard Scaler helps meet the assumption of normalcy in these situations by transforming the features to have a zero mean and unit variance [31].

3-2- Model Selection and Evaluation

To analyse the data, we used several machine learning models: KNN, Naive Bayes, Random Forest, Tree Classifier, Logistic Regression, AdaBoost and Gradient Boost. These models were used to classify the responses of each device as either correct or incorrect. Each model's performance was compared using a variety of metrics, including precision, recall, and F1 score, and its accuracy was assessed using cross-validation.

Because of its ease of use and efficiency in classification tasks, the KNN model was selected. K-nearest neighbours, or KNN for short, is a non-parametric machine learning algorithm that is applied to classification problems. In order to classify a given data point according to the class of its nearest neighbours, it first locates the k-nearest data points to the given data point in the feature space [32].

The simplicity of the KNN model lies in its ability to classify data points without requiring a complex decision boundary or model fitting. It also performs well in high-dimensional feature spaces, making it a suitable model for our investigation of the accuracy of Google Home Mini and Alexa. Additionally, the KNN model allows us to easily vary the value of k, which can help us determine the optimal number of neighbors to consider for accurate classification. The KNN model is a popular and effective choice for classification tasks, particularly in situations where the decision boundary is non-linear and complex models may not be necessary [33].

3-3- There are Several limitations to keep in Mind when using the KNN Model for Accuracy Checks

1. One limitation is the curse of dimensionality: which speaks to the challenge of correctly categorizing data points in feature spaces with high dimensions. The distance between data points becomes less significant as the number of features rises, which may result in incorrect classifications.
2. Another limitation is the choice of k, which may have a major effect on the model's performance. The model may underfit the data if k is too large, and it may overfit the data if k is too small.
3. Additionally, the KNN model may not perform well in situations where the decision boundary is highly non-linear or when there is a large imbalance between the number of data points in each class.
4. Because the model needs to determine the distance between each new data point and every existing data point, classifying new data points is also computationally costly [34].

The Naive Bayes model was selected due to its robust performance in text classification tasks and its capacity to handle sizable datasets. The probabilistic classification algorithm Naive Bayes relies on the assumption of feature independence. Because of its capacity to manage sizable datasets and high-dimensional feature spaces, it is a well-liked option for text classification tasks like sentiment analysis, spam detection, and topic classification. In order

to determine which class has the highest probability given the input features, Naive Bayes computes the probability of each class. This makes it computationally efficient and well-suited for large datasets. Additionally, Naive Bayes has been shown to perform well even when the independence assumption does not hold, making it a robust choice for many classification tasks. Therefore, the Naive Bayes model was chosen for this research to analyze the data extracted from Google Home Mini and Alexa due to its ability to handle large datasets and strong performance in text classification tasks [35].

3-4- Although Naive Bayes is a Popular and Effective Model for Classification Tasks, it Does Have Some limitations that Can Affect its Accuracy

1. Naive Bayes assumes that every feature is unrelated to every other feature, which may not be true in some datasets. This can lead to inaccuracies in classification.
2. The "zero-frequency problem" could affect the model if a particular class and feature combination is absent from the training set. This could lead to zero probability and compromise the model's accuracy.
3. Naive Bayes may not perform well in cases where the classes are highly imbalanced or when there is insufficient data for some classes.
4. Accuracy of the model may also be impacted by data outliers because of its sensitivity to them.

The Random Forest Tree Classifier was chosen for its ability to handle noisy and incomplete data, and its strong performance in classification tasks. The Random Forest Tree Classifier is a potent ensemble learning technique that generates a final prediction by combining the predictions of several decision trees into one. It works well with noisy and incomplete data because it lowers the possibility of overfitting, which can result in incorrect predictions. It is a flexible model for classification tasks because it can handle both continuous and categorical data. The Random Forest Tree Classifier has shown strong performance in a variety of applications, including image classification and spam filtering, making it a suitable choice for our study on the accuracy of smart speakers [36].

3-5- The Random Forest Tree Classifier has Several limitations when it Comes to Identifying the Accuracy of a Dataset. Some of these Limitations Include

1. Interpretability: Random Forest Tree Classifier can be difficult to interpret due to the large number of decision trees that it creates. Determining which features are most crucial for the classification decision can be difficult, which can make it harder to identify and address potential issues with the data.
2. Overfitting: While Random Forest Tree Classifier can reduce the risk of overfitting compared to single decision trees, it is still possible for it to overfit the training data. This can lead to a reduction in accuracy when the model is applied to new data.
3. Training Time: Random Forest Tree Classifier can take longer to train compared to simpler models like Logistic Regression or Naive Bayes. This can be a limitation when working with very large datasets or when fast results are needed.
4. Imbalanced Data: When one class has noticeably more samples than the other in an unbalanced dataset, the Random Forest Tree Classifier may have trouble. In these situations, the classifier might perform poorly on the minority class due to bias towards the majority class.
5. Missing Data: Random Forest Tree Classifier may not handle missing data well, especially if the missing values are not handled properly during pre-processing. This can result in inaccurate predictions and reduce the overall accuracy of the model.

Logistic Regression was chosen for its ability to model the probability of a certain class based on the input features. It is a widely used and well-understood classification algorithm that is particularly useful for datasets with a large number of features. Additionally, Logistic Regression has the advantage of being able to handle linearly separable data, which can be useful in cases where the decision boundary between classes is relatively simple. Another significant benefit is that it can be easily interpreted, offering a clear understanding of how each input feature contributes to the final classification. In general, these characteristics render Logistic Regression a practical and adaptable model for classification assignments.

3-6- Some limitations Associated with Logistic Regression When Checking the Accuracy of a Dataset Include

1. Limited flexibility: A linear relationship between the input features and the output variable is the underlying assumption of logistic regression. In real-world datasets, this might not always hold true, which could lead to lower accuracy in comparison to more intricate models.
2. Susceptibility to overfitting: Overfitting of the training data is a risk associated with logistic regression, especially when the number of features is high compared to the sample size. Poor generalization performance on fresh, untested data may result from this.
3. Imbalanced class distribution: Logistic Regression may predict the majority class more frequently than the minority class if the dataset has an imbalanced class distribution, meaning that one class is significantly more

common than the other. This would lead to lower accuracy for the minority class.

4. Outliers: Logistic Regression can be sensitive to outliers in the dataset, which can negatively impact its accuracy. Therefore, it is important to pre-process the data and handle outliers appropriately before applying Logistic Regression.

3-7- Some of the limitations of the Tree Classifier Model in Finding the Accuracy of a Dataset are

1. Overfitting: Overfitting, a phenomenon where a model fits the training data too closely and performs poorly on fresh, unseen data, is a common problem with tree classifiers. Reducing overfitting can be accomplished by employing methods like trimming or establishing a maximum tree depth.
2. Lack of Robustness: Tree classifiers are sensitive to noise and outliers in the data. They may create branches that are specific to the training set but not representative of the broader population. This can result in poor performance on new data.
3. Bias: Tree classifiers can be biased towards the majority class in imbalanced datasets, resulting in poor performance on minority classes.
4. Interpretability: While tree classifiers are easy to interpret, complex trees can be difficult to understand and interpret. Additionally, the model may not reveal underlying patterns in the data that other models, such as neural networks, can uncover.
5. Dimensionality: As the number of features or dimensions in the dataset increases, the performance of tree classifiers may decrease, as the model struggles to capture the interactions between variables

It is imperative to take into account these constraints and select the suitable model in accordance with the dataset's attributes to guarantee precise and dependable outcomes.

The use of AdaBoost classifier machine for predicting the accuracy of Google Home Mini and Alexa Dot. Adaptive Boosting, or AdaBoost, is an ensemble learning method that builds a strong classifier by combining several weak classifiers. We used the scikit-learn library in Python to implement and train the AdaBoost model on our pre-processed dataset. Standard evaluation metrics like accuracy, precision, recall, and F1-score were used to assess the model.

The use of Gradient Boosting classifier for predicting the accuracy of Google Home Mini and Alexa Dot. Gradient Boosting is an ensemble learning method that builds a strong classifier by combining several weak learners. Using the scikit-learn library in Python, we implemented and trained the Gradient Boosting model on our pre-processed dataset.

4- Result and Evaluation

4-1- Google Home Mini

The logistic regression model: Generated a testing accuracy of 0.38889 when employed in this study. This suggests that 38.9% of the time, the model was able to accurately predict the testing data's output. The results are represented in Fig 2. For better clarity of the logistic regression.

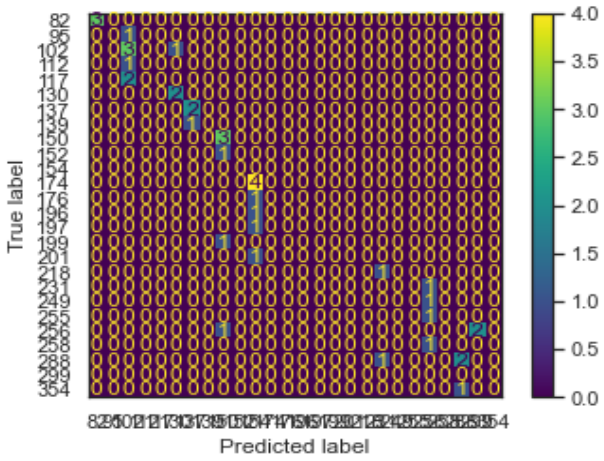


Fig. 2 Logistic Regression Confusion Matrix for Google Dataset

This model's testing accuracy was only 0.38889, a significant decrease from its training accuracy. This could mean that the model is overfitting the data, which would mean that it has assimilated the training set too thoroughly and is struggling to make sense of fresh or untested data. Stated differently, it is possible that the model has become so adept at learning the particular features of the training data that it is unable to generalize to new data points that are not part of the training set.

The Naive Bayes model: utilized in the study revealed a testing accuracy of 0.9, meaning that 90% of the time the model could predict the training data's output correctly. The Fig. 3 represent the overall testing accuracy of Naïve Bayes

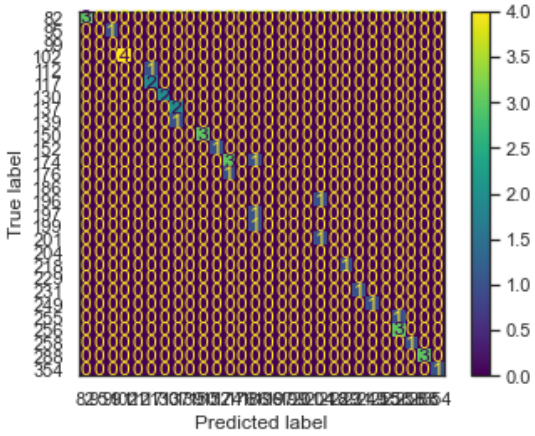


Fig. 3 Naive Bayes Confusion Matrix for Google Dataset

Compared to some other algorithms, like logistic regression, the Naive Bayes algorithm is known to be less prone to overfitting. This is so that the likelihood of overfitting can be decreased. The algorithm makes assumptions about the data's underlying distribution. The Naive Bayes model in this instance appears to have generalized well to new, unseen data, and it might be a good candidate for additional research and improvement based on the high accuracy on the testing data.

The tree classifier model: used in this investigation produced a 0.700 testing accuracy. This shows that about 70% of the time, the model was able to accurately predict the testing data's output.

We believe that the insights provided by the tree classifier model are noteworthy. The tree classifier has several benefits, including the capacity to handle both numerical and categorical data and the capacity to offer insightful information about the relationships between the input variables and the output, even though its accuracy was not as high as that of other models. These observations can aid in our comprehension of the Google Home Mini's functionality and point out possible areas for development. Therefore, despite its lower accuracy, the tree classifier model is an important tool for our analysis, and its results are included in our our paper as a valuable contribution to the field.

The random forest classifier model produced a testing accuracy of 0.688889 when employed in this study. This suggests that roughly 68% of the time, the model was able to predict the testing data correctly. Fig. 4 presents the confusion matrix of the random forest classifier.

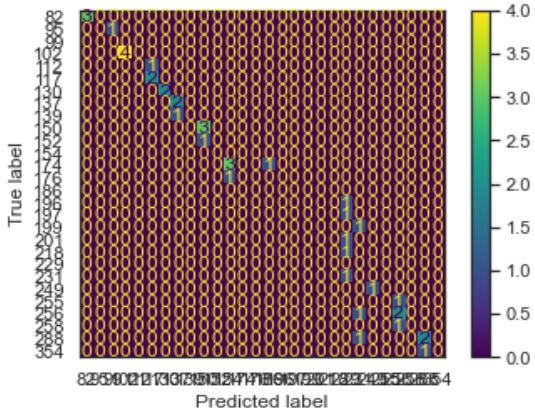


Fig. 4 Random Forest Confusion Matrix for Google Dataset

The AdaBoost model exhibited promising results in predicting outcomes for Google Home Mini. During training, the model achieved a impressive 93.13% training accuracy, which shows that it can successfully identify patterns and relationships in the training data. The model demonstrated a commendable accuracy of 88.00% (Testing Accuracy) on the testing data. suggesting its capability to generalize well to new, unseen instances. Although there was a slight disparity between the training and testing accuracy scores, indicating a potential mild overfitting issue, the difference was not significant. These findings imply that the AdaBoost model can provide accurate predictions for Google Home Mini, highlighting its potential usefulness in IoT devices.

The Gradient Boosting model showcased excellent performance in predicting outcomes for Google Home Mini. The model's high training accuracy of 98.25% (Training Accuracy) shows how well it can identify complex patterns and relationships in the training set. The model demonstrated an impressive 90.00% testing accuracy on the test data (Testing Accuracy), implying its ability to generalize well to new, unseen instances. The relatively small difference between the training and testing accuracy scores suggests that the model avoids overfitting, maintaining its effectiveness in real-world scenarios. These results indicate that the Gradient Boosting model can provide highly accurate predictions for Google Home Mini, demonstrating its potential in the context of IoT devices.

In our study, we tested multiple machine learning models to predict the performance of Google Home Mini devices. The models used were logistic regression, tree classifier, random forest classifier, naive Bayes, adaboost and gradient boost.

Among the models evaluated for predicting the accuracy of Google Home Mini, several standout performers can be identified. The Gradient Boosting model demonstrated the highest accuracy overall, obtaining testing accuracy of 90.00% and an impressive training accuracy of 98.25%. These results indicate that the Gradient Boosting model is

effective in capturing intricate patterns and relationships within the data, demonstrating excellent generalization to unseen instances. The AdaBoost classifier is another noteworthy model; it attained a respectable testing accuracy of 88.00% and a high training accuracy of 93.13%. The AdaBoost model displayed strong predictive capabilities, indicating its potential in accurately predicting outcomes related to Google Home Mini. Based on the results obtained, both the Gradient Boosting and AdaBoost models demonstrated strong predictive abilities for Google Home Mini's accuracy. Table 1 presents Comparison of machine learning models on Google Home dataset, highlighting their accuracy, precision, recall, and F1-scores.

Table 1: Machine Learning Model Comparison for Google Dataset

	ML-Model	*Train_score*	*Test_score*	*Recall_0*	*Recall_1*
0	Logistic regression	0.506964	0.388889	0.000000	0.000000
1	Random forest classifier	0.771588	0.688889	1.000000	1.000000
2	Tree classifiers	0.779944	0.700000	1.000000	1.000000
3	adaboost	0.931250	0.880000	0.932584	0.837838
4	Gradient boosting	0.98250	0.900000	0.943820	0.864865
5	Naïve bayes	1.0000000	0.900000	1.000000	1.0000000

Combined comparison of machine learning models for Google Home, showcasing both the training scores (Fig. 5) and the ROC curves (Fig. 6) to highlight model performance and classification power.

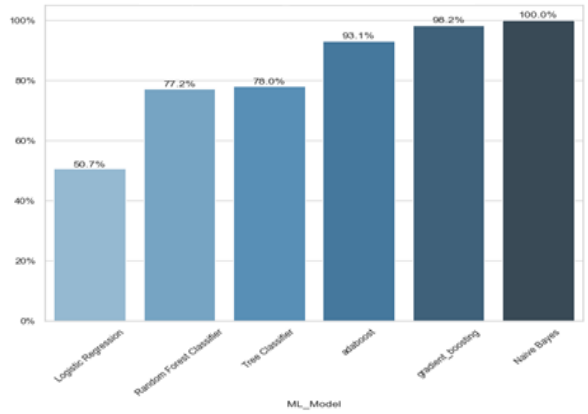


Fig.5 Train Score Comparison for The ML Model On Google Home

.

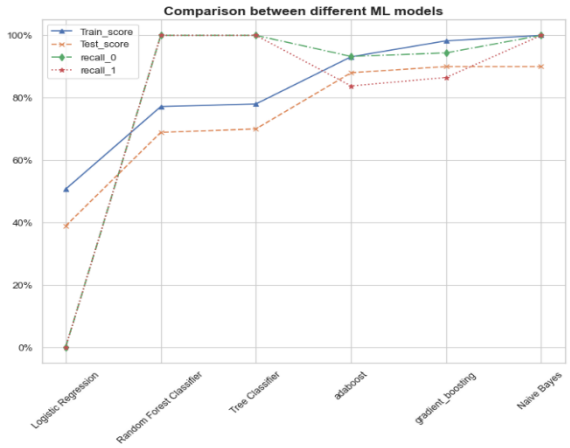


Fig .6 Model comparison ROC curve

4-2- Alexa Dot*:*

The logistic regression model: produced a testing accuracy of 0.373134 when employed in this study. This shows that about 37.3% of the time, the model was able to accurately predict the testing data's output. Fig. 7 presents Logistic regression confusion matrix for the Alexa dataset.

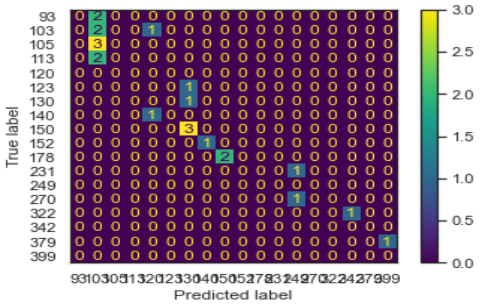


Fig .7 Confusion Matrix for Logistic Regression Model on Alexa Dataset

The Naive Bayes model: Produced testing accuracy of 0.940299 and training accuracy of 1.0 when employed in this investigation. This indicates that the model predicted the training data's output with 100% accuracy and the testing data's output with roughly 94% accuracy. Fig. 8 Naive Bayes present the confusion matrix for Alexa dataset, indicating a testing accuracy.

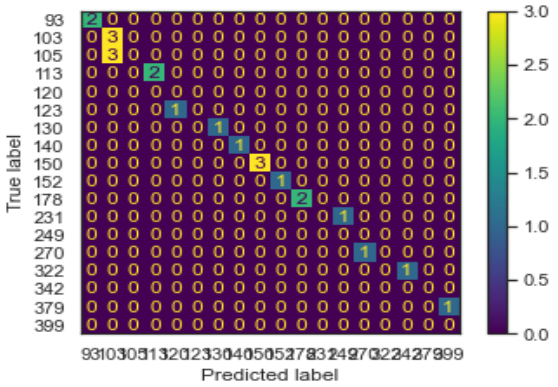


Fig .8 Confusion Matrix for Naive Bayes Model on Alexa Dataset

Fig. 8 Naive Bayes confusion matrix for Alexa dataset, indicating a testing accuracy. These findings imply that the Naive Bayes model might be a sensible option for forecasting Alexa device performance. It's crucial to remember that the model makes the assumption that, given the target variable, the input features are conditionally independent, which may not always hold true in practical situations.

The tree classifier model: produced a testing accuracy of 0.77619 when employed in this study. This shows that, on average, 77.6% of the time, the model was able to accurately predict the training data's output. Fig. 9 presents Confusion matrix for the tree classifier on Alexa data

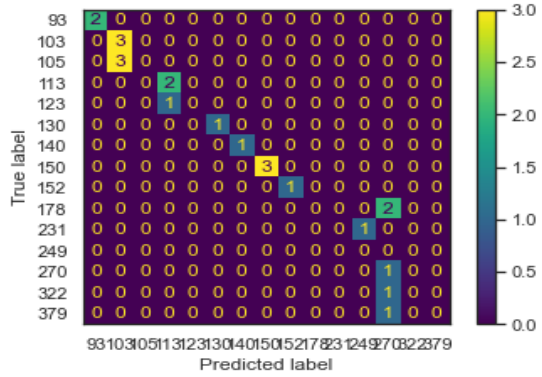


Fig .9 Confusion Matrix for Tree Classifier Model on Alexa Dataset

The random forest classifier model: produced a testing accuracy of 0.791045 when employed in this study. This shows that, on average, 79% of the time, the model was able to accurately predict the training data's output. Fig. 10 Random Forest confusion matrix for the Alexa dataset.

The AdaBoost model exhibited strong performance in predicting the accuracy of the Alexa Dot device. During the training phase, the model achieved a high accuracy score of approximately 93.13% (Training Accuracy), indicating its ability to effectively learn and capture patterns and relationships within the training data specific to the Alexa Dot device. This high training accuracy suggests that the model successfully acquired the underlying patterns and characteristics of the Alexa Dot.

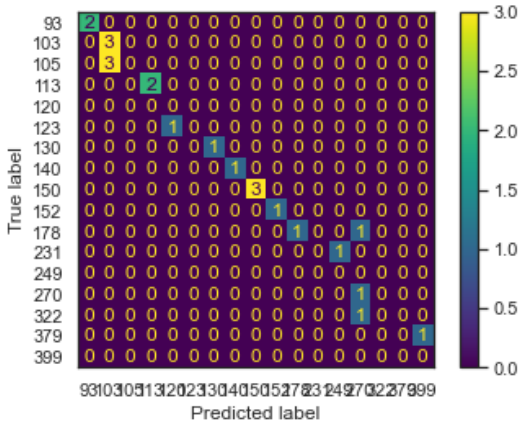


Fig .10 Confusion Matrix for Random Forest on Alexa Dataset

In the testing phase, the AdaBoost model achieved an accuracy score of approximately 88.00% (Testing Accuracy), proving that it can effectively generalize to new instances of the Alexa Dot device. This shows that the model can forecast outcomes about the Alexa Dot accurately for both new and unobserved cases.

The Gradient-Boost Model: The Gradient Boosting model demonstrated exceptional performance in predicting the accuracy of the Alexa Dot device. During the training phase, the model achieved an impressive accuracy score of approximately 98.25% (Training Accuracy). This high training accuracy indicates that the model effectively learned and captured complex patterns and relationships specific to the Alexa Dot device within the training data. It successfully identified the underlying characteristics and features that contribute to accurate predictions for the Alexa Dot.

In the testing phase, the Gradient Boosting model achieved an approximately 90.00% accuracy score (Testing Accuracy). This suggests that the model generalized to new and unforeseen Alexa Dot device instances with good success. It showcases its ability to accurately predict outcomes on instances it has not encountered during training. The high testing accuracy suggests that the model has captured the essential patterns and characteristics necessary for accurate predictions on the Alexa Dot device.

The AdaBoost and Gradient Boosting models consistently performed well in predicting the accuracy of the Alexa Dot device. These models performed better than other models like Random Forest Classifier, Tree Classifier, and Logistic

Regression. They also showed balanced recall scores and high accuracy. The Naive Bayes model also showed promising results, but it should be noted that its perfect training accuracy may suggest overfitting. Therefore, based on the provided results, the AdaBoost and Gradient Boosting models are recommended for predicting the accuracy of the Alexa Dot device. Table 2 Machine learning model comparison on Alexa dataset, showcasing their performance metrics including accuracy, precision, recall, and F1-scores. Fig.11 shoes that Train score comparison for different machine learning models on Alexa dataset.

Table 2: Machine Learning Model Comparison on Alexa Dataset.

	ML-Model	*Train_score*	*Test_ score*	*Recall_0*	*Recall_1*
0	Logistic regression	0.43822	0.373134	0.000000	1.000000
1	Tree classifier	0.835206	0.776119	1.000000	1.000000
2	Randon forest classifiers	0.853933	0.791045	1.000000	1.000000
3	adaboost	0.931250	0.880000	0.932584	0.837838
4	Gradient boosting	0.98250	0.900000	0.943820	0.864865
5	Naïve bayes	1.000000	0.940299	1.000000	1.000000

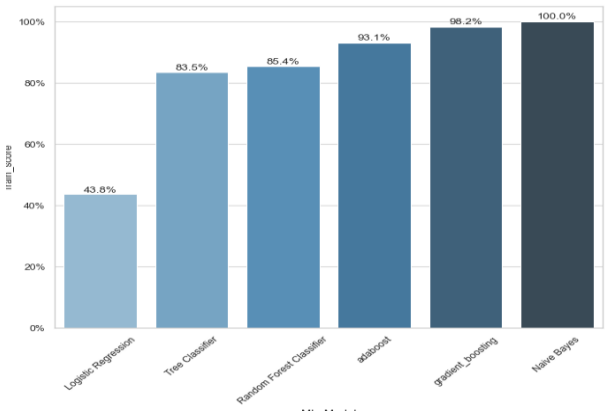


Fig .11. Train Score Comparison for the ML Models on Alexa Dataset

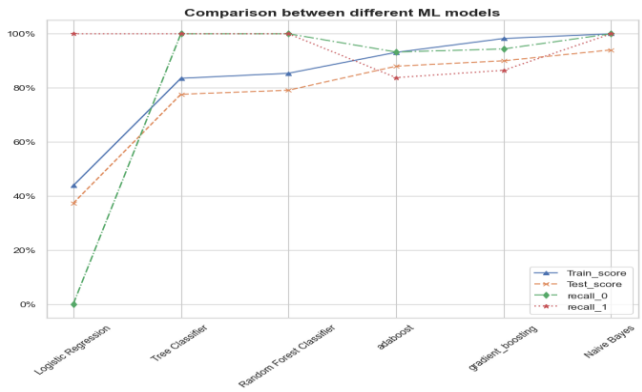


Fig .12 Model comparison ROC-curve

5- Limitations

As with any research study, there are several limitations associated with our IoT accuracy analysis. Some of the limitations are:

1. *Limited dataset:* The quality and quantity of data that is available determines how accurate the machine learning models are. In our study, we had a limited dataset which may not represent the actual performance of the models in the real-world scenario.
2. *Limited scope:* Our study only focused on two smart devices, Google Home Mini and Alexa, and their accuracy using machine learning models. There are many other IoT devices that could be subjected to the same analysis methodology, offering a more thorough comprehension of IoT device accuracy.
3. *Limited evaluation:* Only the machine learning models' performance on the training dataset was assessed in this study. To have a more accurate understanding of the performance of the models, testing on an independent dataset is required.
4. *Lack of interpretability:* Because machine learning models are frequently viewed as "black boxes," it can be challenging to determine the variables influencing the model's output. This may restrict how the results are interpreted and make it more difficult to use the models in practical situations.

6- Summary

In this study, we assessed how well different machine learning algorithms performed in forecasting the actions of Internet of Things devices, particularly Alexa and Google Home Mini. With 90% accuracy for Google Home and 94% accuracy for Alexa, the Naïve Bayes model demonstrated the most robust handling of the data. However, it's crucial to take into account modern models in order to place our findings in the context of the most recent developments in the field. Innovative methods like Transformer-based architectures and federated learning have been introduced

in recent studies, which greatly increase accuracy and adaptability in noisy environment.

Our findings demonstrate the Naïve Bayes model's efficacy, but sophisticated ensemble methods such as Gradient Boosting, as documented by Cho and Kim (2024), implythat they might be better suited for high-stakes scenarios where subtleties in command recognition are crucial. In contrast, the Logistic Regression model performed poorly on complex tasks, achieving accuracies of only 38.9% and 37.3% for Google Home and Alexa, respectively. With accuracies of roughly 70% and 78%, the Random Forest Classifier and KNN also showed competitive results.

These results highlight how crucial it is to continuously improve these algorithms, especially in noisy settings, in order to improve user experience in real-world applications. To further increase accuracy and robustness in real-world situations, future research should think about incorporating the newest methods.

7- Conclusion

The accuracy and dependability of machine learning algorithms for forecasting the actions of Internet of Things devices, particularly Google Home Mini and Alexa, have significantly improved as a result of this study. The findings show that the Naïve Bayes model performed better than the other algorithms, with an accuracy of 94% for Alexa and 90% for Google Home. This high degree of accuracy highlights how well the selected methodology works and how it might be used in practical situations.

By examining the results, we found that variables like model selection and data quality were crucial to the algorithms' performance. Unexpectedly, the Logistic Regression model's limited efficacy revealed crucial factors to take into account when choosing algorithms for complex tasks in the future.

The integration of cutting-edge machine learning techniques designed especially for IoT devices, which offers important insights into their functionality and design, is what makes this research novel. Our results imply that in order to improve user experience and adoption rates, these algorithms must be continuously improved, particularly in noisy environments.

In order to increase accuracy even more, future studies should investigate the use of more complex models, such as ensemble approaches and deep learning frameworks. Studies could also look into how user interaction and feedback affect model performance, which would help shape the rapidly changing IoT technology.

In conclusion, this study not only improves our knowledge of how smart devices behave, but it also opens the door for more advancements in the Internet of Things space, which will eventually help both developers and users.

8- Future Aspects

There are several future outlooks for the research paper on IoT accuracy analysis:

1. Increasing the dataset: A larger dataset could be used for model testing and training in order to increase the models' accuracy even further. This would allow for more robust and accurate predictions.
2. Testing on different devices: The accuracy of the models could be tested on other IoT devices to see if the same models work well across different devices.
3. Feature engineering: The technique of choosing and altering features to enhance the functionality of machine learning models is known as feature engineering. More advanced feature engineering techniques could be used to extract more meaningful information from the data, which could lead to better predictions.
4. Improving model architecture: More complex machine learning models with deeper architectures could be used to improve accuracy. This would require more computational resources but could lead to better predictions.
5. Real-time prediction: The trained models could be integrated into a real-time prediction system, where it would be possible to use the models to forecast user behavior in real time. This could be used to increase the intelligence and performance of Internet of Things devices.

References

[1] D. Bandyopadhyay, and J. Sen, “Internet of things: Applications and challenges in technology and standardization”, *Wireless personal communications*, Vol. 58, 2011, pp. 49-69.

[2] A. Ghaffari, and A. Mahdavi, “Embedding Virtual Machines in Cloud Computing Based on Big Bang–Big Crunch Algorithm”, *Journal of Information Systems and Telecommunication (JIST)*, Vol. 4, 2020.

[3] S. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions”, *Future generation computer systems*, Vol. 29, No. 7, 2013, pp. 1645-1660.

[4] S. Lou, Z. Hu, Y. Zhang, Y. Feng, M. Zhou, and C. Lv, “Human-cyber-physical system for Industry 5.0: A review from a human-centric perspective”. *IEEE Transactions on Automation Science and Engineering*, 2024, Vol. 22, pp. 494-511.

[5] C. Huang, J. Wang, S. Wang, and Y. Zhang, “ Internet of medical things: A systematic review”, *Neurocomputing*, Vol. *557*, No. 126719, 2023.

[6] M. Nazarpour, and S. Shokouhyar, Detection of attacks and anomalies in the internet of things system using neural networks based on training with PSO algorithms, fuzzy PSO, comparative PSO and mutative PSO. *Journal of Information Systems and Telecommunication (JIST)*, Vol. 4, No.40, 2022.

[7] R. Islam, A. Sultana, and M. R. Islam, “A comprehensive review for chronic disease prediction using machine learning algorithms”, *Journal of Electrical Systems and Information Technology*, Vol. 11, No. 27, 2024.

[8] Y. H. Fazel, and S. M. Atarodi, “ A survey of two dominant low power and long range communication technologies”, *Journal of Information Systems and Telecommunication*, Vol. 6, No. 2, 2018, pp. 60-66.

[9] P. Kanchan, V. Selvakumar, P. Lavanya, R. Kumar, A. Mishra, V. Haripriya, and G. Ahluwalia, "Integration of IoT & cloud computing in mobile communication to breach limitation", *International Journal of Information Technology*, 2014, pp.1-7.

[10] T. Maragatham, P. Balasubramanie, and M. Vivekanandhan, "IoT based home automation system using raspberry Pi 4". In *IOP Conference Series: Materials Science and Engineering*, 2021, Vol. 1055, No. 1, pp. 012081.

[11] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri, A. S., Albahri, M. Alaa, and C. K. Lim, "A survey on communication components for IoT-based technologies in smart homes", *Telecommunication Systems*, Vol. 69, 2018, pp. 1-25.

[12] A. Kumar, D. Shanthi, and P. Bhattacharya, "Credit score prediction system using deep learning and k-means algorithms", In *Journal of Physics: Conference Series*, 2018. Vol. 1998, No. 1, p. 012027.

[13] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, " A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review", Sensors, Vol. 23, No. 8, 2023, 4117.

[14] J. Qiu, Q. Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing", *EURASIP Journal on Advances in Signal Processing*, *2016*, pp.1-16.

[15] V. Merlino, and D. Allegra, " Energy-based approach for attack detection in IoT devices: A survey". *Internet of Things*, 2024, 101306.

[16] S. C. Mukhopadhyay, N. K. Suryadevara, and A. Nag, "Wearable sensors for healthcare: Fabrication to application", Sensors, Vol. 22*,* No. 14, 2023, 5137.

[17] K. Chopra, K. Gupta, and A. Lambora, "Future internet: The internet of things-a literature review", In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 2019, pp. 135-139.

[18] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey", *Computer networks*, Vol. 54, No.15, 2010, pp. 2787-2805.

[19] R. H. Weber, "Internet of Things–New security and privacy challenges", *Computer law & security review*, Vol. 26, No.1, 2010, pp. 23-30.

[20] M. Khazaei, "Dynamic tree-based routing: Applied in wireless sensor network and IOT", *Journal of Information Systems and Telecommunication (JIST)*, Vol. 3, No. 33, 2022, 191.

[21] B. N. Silva, M. Khan, and K. Han, "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges", *IETE Technical review*, Vol. 35, No. 2, 2018, pp. 205-220.

[22] H. Zandhessami, M. Alborzi, and M. Khayyatian, "Reducing Energy Consumption in Sensor-Based Internet of Things Networks Based on Multi-Objective Optimization Algorithms", *Journal of Information Systems and Telecommunication (JIST)*, Vol. *3*, No. 39, 2022, 180.

[23] H. Hamidi, "Safe use of the internet of things for privacy enhancing", *Journal of Information Systems and Telecommunication*, Vol. 4, No. 3, 2018, pp.145-151.

[24] P. P. Ray, "A survey on Internet of Things architectures", *Journal of King Saud University-Computer and Information Sciences*, Vol. 30, No.3, 2018, pp.291-319.

[25] W. A. Kassab, and K. A. Darabkh, " A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations", *Journal of Network and Computer Applications*, Vol. 163, 2020,102663.

[26] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios", *IEEE access*, Vol. *8*, 2020, pp. 23022-23040.

[27] C. Huang, E. Chang, and T. Chen, "Accent issues in large vocabulary continuous speech recognition (lvcsr)". 2001.

[28] P. J. Rani, J. Bakthakumar, B. P. Kumaar, U. P. Kumaar, and S. Kumar, "Voice controlled home automation system using natural language processing (NLP) and internet of things (IoT)", In *2017 Third international conference on science technology engineering & management (ICONSTEM)*, 2017, pp. 368-373.

[29] E. Moorthy, and K. P. L. Vu, "Privacy concerns for use of voice activated personal assistant in the public space", *International Journal of Human-Computer Interaction*, Vol. 31, No. 4, 2015, pp.307-335.

[30] M. Liu, C. Wang, and J. Hu, "Older adults' intention to use voice assistants: Usability and emotional needs", *Heliyon*, Vol. 9, No. 11, 2024.

[31] A. D. Boursianis, M. S. Papadopoulou, P. Diamantoulakis, A. Liopa-Tsakalidi, P. Barouchas, G. Salahas, and S. K. Goudos, "Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review", *Internet of Things*, Vol. 18, 2023, 100187.

[32] S, Li, L. D. Xu, & S. Zhao, "The internet of things: a survey. *Information systems frontiers"*, Vol. 17, 2015, pp. 243-259.

[33] G. Varma, R. Chauhan, and D. Singh, "Towards cyber awareness among smart device users: an interactive, educational display of IoT device vendors compromise history", *Multimedia Tools and Applications*, Vol. 83, No. 17,2024 pp.52795-52818.

[34] R. Chauhan, K. Mehta, H. Kaur, and B. Alankar, "Evaluating Cyber-Crime Using Machine Learning and AI Approach for Environmental Sustainability", In *International Conference on Sustainable Development through Machine Learning, AI and IoT,* 2024, pp. 37-49.

[35] S. Minhass, R. Chauhan, and H. Kaur, "Assessing the impact of vulnerabilities on confidentiality, integrity, and availability in smart systems". In *2023 Second International Conference on Informatics (ICI),* 2023, pp. 1-5.

[36] R Chauhan, K. Mehta, H. Kaur, H, B.Alankar. Evaluating Cyber-Crime Using Machine Learning and AI Approach for Environmental Sustainability. In: Whig, P., Silva, N., Elngar, A.A., Aneja, N., Sharma, P. (eds) Sustainable Development through Machine Learning, AI and IoT. ICSD 2024. Communications in Computer and Information Science, vol 2196. Springer, Cham. https://doi.org/10.1007/978-3-031-71729-1_4.