Journal of Information Systems and Telecommunication
Vol.11, No.1, January-March 2023, 31-40
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Providing a New Smart Camera Architecture for Intrusion Detection in Wireless Visual Sensor Network

Meisam Sharifi Sani[1*], Amid Khatibi Bardsiri[2]

[1]. Department of Computer Engineering, Tehran Branch, Islamic Azad University, Tehran, Iran
[2]. Department of Computer Engineering, Bardsir Branch, Islamic Azad University, Kerman, Iran

Received: 20 Jan 2021/ Revised: 04 Jan 2022/ Accepted: 27 Feb 2022

Abstract

The wireless Visual sensor network is a highly functional domain of high-potential network generations in unpredictable and dynamic environments that have been deployed from a large number of uniform or non-uniform groups within the desired area, cause the realization of large regulatory applications from the military and industrial domain to hospital and environment. Therefore, security is one of the most important challenges in these networks. In this research, a new method of routing smart cameras with the help of cloud computing technology has been provided. The framework in the cloud computing management layer increases security, routing, inter interaction, and other features required by wireless sensor networks. Systematic attacks are simulated by a series of standard data collected at the CTU University related to the Czech Republic with RapidMiner software. Finally, the accuracy of detection of attacks and error rates with the suggested NN-SVM algorithm, which is a combination of vector machines and neural networks, is provided in the smart cameras based on the visual wireless sensor networks in MATLAB software. The results show that different components of the proposed architecture meet the quality characteristics of visual wireless sensor networks. Detection of attacks in this method is in the range of 99.24% and 99.35% in the worst and best conditions, respectively.

Keywords: Intrusion Detection; Smart Cameras; Security; Visual Sensor Network; Cloud Computing.

1- Introduction

Sensor networks consist of several nodes, which have computational, communicational, and sensing capabilities. Usually physically small, and it is limited in the processing power, memory capacity, and power supply [1]. These limitations provide some issues, which many research efforts in this area are stemmed from. The dense extension of sensor nodes should allow the network to coordinate with unpredictable environments. A type of wireless sensor network is a visual or video sensor network [2]. since embedding inexpensive cameras with (high or low) resolution features in wireless sensors, it is possible to receive the visual data from the environment, making a new focal point for the network applications [3]. The unique feature of the sensors equipped with video cameras is imaging a target or a part of a region which are not necessarily near the camera. That is, the cameras are capable of capturing objects in extra in their line of sights [4]. Accordingly, in these networks, Closed Circuit Television cameras are used as a node or a group of nodes for different applications. Today, one of the systems used for controlling and monitoring life and workplaces as well as providing more security and relief is a Closed-Circuit Television camera. These systems are referred to as either imaging control systems or closed-circuit video equipment. According to the setting applied to the cameras and other equipment, the systems are highly applicable in different climatic conditions at days and nights [5]. In the wireless sensor networks, each sensor node acquires a specific standpoint [6]. The sensor standpoint of the environment is limited by the range and precision, possibly covering a restricted physical area. Therefore, area coverage also can be considered as an important design parameter in wireless sensor networks. Since sensor nodes may produce considerable redundant data, the similarly produced data packets from numerous nodes can be integrated to reduce the number of transmissions [7]. Data integration is a combination of data from different sources based on a given integration function. This method has been used in some routing protocols to increase energy efficiency and to optimize the data transfer. Signal

✉ **Meisam Sharifi Sani**
Meisam.sharifi.s@gmail.com

processing methods could also be used to integrate the data [8]. This approach is also referred to as data combining, in which the node can produce more precise output signals by using different methods to combine input signals and to remove the noise of the signals [9]. In other words, Closed Circuit Television cameras are small devices with onboard predefined sensors, capable of image processing, which are publically accepted [10][11]. Some of the most important tasks of the Closed Circuit Television cameras in the wireless networks are full environmental control and monitoring, providing a security basis, traffic control, tracking, etc. [12]. Many researchers have managed and controlled numerous processes in the networks by aiding the cameras [8][13]. On the other hand, considering limitations before visual sensor networks with smart Closed Circuit Television cameras, there are some factors such as routing, security, interactivity, customization, etc. [14]. Intrusion detection systems are one of the possible solutions to solve security problems in wireless sensor networks. An Intrusion Detection System is also referred to as a second line of defense, which is used for intrusion detection only; that is, Intrusion Detection System can detect attacks but cannot prevent or respond. Once the attack is detected, the IDSs raise an alarm to inform the controller to take action. There are two important classes of IDSs. One is rule-based Intrusion Detection System and the other is anomaly-based Intrusion Detection System. Rule-based Intrusion Detection System is also known as signature-based Intrusion Detection System which is used to detect intrusions with the help of built-in signatures. Rule-based Intrusion Detection System can detect well-known attacks with great accuracy, but it is unable to detect new attacks for which the signatures are not present in intrusion database. Anomaly based IDSs detect intrusion by matching traffic patterns or resource utilizations. Although anomaly based IDSs have the ability to detect both well-known and new attacks, they have more false positive and false negative alarms. Some IDSs operate in specific scenarios or with particular routing protocols [15].

2- Problem Expression

Security and routing in sensor networks are very challenging due to the inherent characteristics of these types of networks, distinguishing them from other networks such as ad-hoc mobile networks or cellular networks that can be divided into 9 features, the most important differences of this network with other wireless networks. The first characteristic is that due to a large number of sensor nodes, it is not possible to build an addressing scheme. Therefore, the traditional IP-based protocols are not applicable for wireless sensor networks, because the ID maintenance overhead is very high. In the wireless sensor networks, sometimes receiving data is more important than understanding the data IDs which should be sent [16][17]. Secondly, sensing nodes located by the ad-hoc method should be self-organizing because the nodes ad-hoc locating requires systems to communicate and manage the resultant node distribution, especially the sensor network should be operated unsupervised [13]. Thirdly, in contrast to the conventional communication networks, almost all of the wireless network applications require transmitting the sensed data from numerous sources to a specific basic station. However, this characteristic does not prevent data flow in the other forms (for example, sending data in a multi-segment form or point to point) [18]. Fourthly, the sensor nodes are severely limited in energy, processing, and storage. Therefore, they need stringent resource management [19][20]. Fifthly, in the most applicable scenarios, the sensor network nodes except some of the mobile ones are usually fixed after locating. Nevertheless, in other traditional networks, the nodes are free to move, changing the topology frequently and unpredictably. In some usages, some sensor nodes can move and change their location (although with low mobility) [17]. Sixthly, sensor networks are pragmatic (i.e., the design requirements of the sensor network are changed based on the application of interest). For example, the challenging observation problem, which must be performed precisely with low delay, is different from periodic climate monitoring [5]. Seventhly, being informed about the sensor node's situation is highly important because data gathering usually relies on the location. This conditional awareness can be met by GPS devices although other methods independent from GPS are also practical for locating the problem in sensor networks [13]. Eighthly, data gathered by many sensor nodes in the wireless sensor network are typically related to a single phenomenon. Hence, the possibility of redundancy in the data is high. This redundancy should be extracted by the routing protocols to increase the usage of energy and bandwidth [13]. Finally, the wireless sensor networks are data-based because the data are requested based on the given features (i.e. feature-based addressing). A feature-based address consists of a query set of feature-value pairs [18]. Nowadays, researches on sensor network security field mainly focus on the following aspects:

1. Various attack resources such as networks, files, system logs, and processes cannot be used in wireless sensor networks, and we need to consider the feature information which can be applied to the wireless sensor network intrusion detection.
2. There are many new attacks in wireless sensor networks, which are different from traditional networks. How to improve the ability of the intrusion detection system to detect unknown attacks and select appropriate algorithms is a problem to be solved. Some algorithms are suitable for detecting known attacks, while others are suitable for detecting unknown attacks. Some algorithms are suitable

for a flat surface network structure, and some algorithms are suitable for a hierarchical network structure. We should select or design the appropriate algorithm according to the requirements of the network.

3. Wireless sensor networks have limited resources, including storage space, computing power, bandwidth, and energy. Limited storage space means that it is impossible to store large amounts of system logs on sensor nodes. The intrusion detection system based on knowledge is required to store large amounts of defined intrusion patterns. The system detects intrusion using pattern matching, and invasion behavior characteristics need to be stored in libraries. With the increase in invasion types, the scale of the feature library will also increase. Limited computing power means that the node is not suitable for running the intrusion detection algorithm which requires a lot of computation [21].

According to the mention of these features, it is known that routing is different in wireless visual networks from other wireless networks. Therefore, sending accurate information and securing routing in these networks can be useful. In this paper, we use an intrusion detection method based on ensemble learning algorithms in smart cameras based on wireless sensor networks. In this method, we use NN-SVM which is a combination of Support Vector Machine and Neural Networks.

3- Related Work

Various platforms have been proposed for wireless visual sensor networks. In this section, we study some of the most important cases proposed by different authors.

One study proposed a prototype of a cloud-based video recorder system under the Infrastructure as a Service (IaaS) abstraction layer in the cloud computing domain. This framework integrates a distributed file system to achieve a scalable, reliable, and virtualized architecture. In implementation design, Hadoop HDFS and HBase are integrated to reach scalability demand. This system provides scalable video recording, backup, and monitoring features. This framework integrates a distributed file system to achieve a scalable, reliable, and virtualized architecture. The paper shares a good experience while design an unlimited resource video recording system. In this method, the consumer bandwidth of the same quality of images as well as storage space in large networks with other methods has been used. They use open-source software, FFmpeg to transcending video resolution and format dynamically. The main problem with this software is that it is a CPU-compressed program, which can cause system bottlenecks if more people access the video from the same server [22].

Another study suggested a character order-preserving (COP)-transformation technique that allows the secure protection of video meta-data. The proposed technique has the merits of preventing the recovery of original meta information through meta transformation and allowing direct queries on the data transformed, increasing significantly both security and efficiency in the video meta-data processing, where the proposed technique was implemented for a real-world environment application, and its performance was measured. The method has the merit of increasing video meta-data efficiency significantly by allowing database query to take place in the same way as that adopted for plain-text files, without leaving the plain-text files exposed. The proposed mechanism accommodates match query, range search, and aggregation just as plain-text data would allow; furthermore, it allows the use of database indexes as they are and thus ensures processing efficiency. The proposed method characteristically divides the data into multiple chunks during encryption. A video meta-data query can therefore be executed based on the chunk ID that is assigned to the part of the video file that corresponds to the segment of the video footage. The proposed mechanism carries out decryption by avoiding the decoding of the whole Closed Circuit Television video data and instead obtains only the partial video data that satisfies the chunk-based search parameters. Efficiency, therefore, is ensured by the new method in terms of the data decoding performance [23].

In this research, the security method of cloud-based wireless IP cameras has been investigated, and the types of open and non-commercial text tools have been used in their research. They chose NetCam because of its ease of setup and use as well as low cost, which makes it a potential item for home-networks. They have captured and investigated the traffic generated by this device, both in idle and during live streaming to a mobile device over the cloud. The security of this device has been investigated from several research areas including secure multimedia, network security, and cloud security. Authors have checked the traffic generated by the low-end, easy-to-setup, off-the-shelf wireless IP camera for the average home user. This method examines the precautions taken by IP camera manufacturers and evaluates the mechanisms of access control in place. Many security issues and privacy in the use of these devices ranging from minor to severe issues have been identified. The results are achieved, suggesting that recently popular and easy to set up, easy-to-use effective cloud-connected wireless IP cameras should not run security and privacy [24].

In this work, they have proposed a video surveillance architecture based on the idea of cloud computing. By using this approach, it is possible to provide the video surveillance as a service. This architecture is the possibility of having a portable and scalable system that can be used in various scenarios. This system is based on the middleware FIWARE and has been implemented in a real scenario. In addition, as a result of video analysis it is

possible to obtain explanations of what is happening in a monitored area, and then take the appropriate action based on that interpretation. On the other hand, with this approach they are also able to add different kind of sensors besides cameras, this method provided a management panel digital devices as in a IoT framework [25].

4- System Model

The security requirements in a routing algorithm should be able to establish a route appropriately and to maintain it. This means that it should not allow the invader nodes to prevent the construction or proper maintenance of the route. If an algorithm meets the following points, it can be called a secure algorithm [26].

1. The routing signal could not be forged.
2. The manipulated signals could not be injected into the network.
3. The routing messages do not be changed during transfer except in the ordinary procedure of the protocol.
4. Routing loops do not be created during invading actions.
5. The invader nodes do not change the shortest routes.
6. The impermissible nodes should be removed from the network. This is assumed considering that; network management has a role in initializing and distributing keys, etc.
7. The network manager to neither permissible nodes nor invader ones should not present the network topology because they can use it to destroy the network.

According to the abovementioned requirements, in this section, the proposed method is described by the flowchart. It is followed by detailing the steps in the flowchart. In this section, the total architecture is studied which can be defined to integrate the architecture of visual sensor network framework and Closed-Circuit Television cameras by cloud computation.

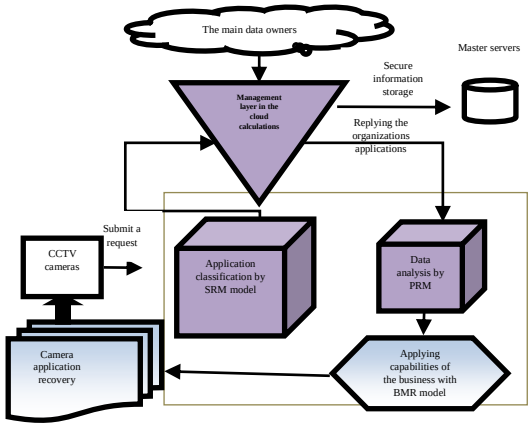

Fig. 1. The proposed reference model for locating the architecture of smart cameras in the cloud computation management layer [14]

As it can be seen in Fig 1, a smart camera routing in the wireless visual sensor network in the private environments is shown. These cameras outsource their data to the cloud computing environment, then this environment encodes the data and places them on its central and main servers. Each central server also consists of a series of hosts, providing the capability of data storage and management.

The sensor networks send their applications from the cloud computation in form of a query to the cloud computation management layer. This layer combined with some reference models in cloud computation send securely the received queries to the cloud computation. After recovering the data from the source or master servers, the recovered data are resent to the management layer in the cloud computation and are classified by the reference model [27], then are delivered to the smart cameras. In the next section, different parts of the proposed method are discussed and detailed.

4-1- Proposed Method

Considering the importance of cloud computation, in this section, the layer is studied and the location of the architecture of the smart camera is identified. One of the most important and applicable layers to locate the smart camera architecture in the wireless sensor network is the management layer in cloud computation. Layers in the architecture of the cloud computing reference Model in the proposed design.

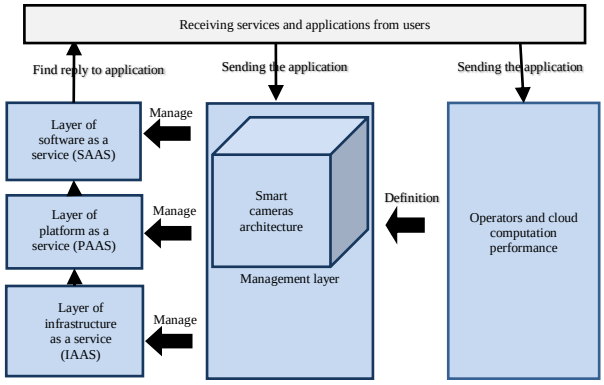

Fig. 2. The CCTV camera reference architecture model in the visual sensor networks and cloud computation.

Fig 2, the sent smart cameras routing to the cloud computation sends the reference application model to the management layer and operator layer. If any specific action is needed to be performed on the application, it is done in the operator layer, and the result is sent to the management layer. Considering the application type in the layer, in which the architecture of the smart camera is also located, the required management is applied according to the wireless visual sensor network, and the model of

interest is selected for the needed operations on the camera routing. Finally, delivering the client's response.

4-2- Proposed Method Pseudo Code

As earlier mentioned, the layer of infrastructure as a service has much more connected to the cloud computation management layer. According to the research need, it is assumed necessary to provide smart cameras locating steps in the cloud computation management layer in form of a pseudo code. In this section, according to the proposed innovation in the previous steps as well as following the provided flowchart and descriptions, the algorithm of interest is presented.

```
Function My_FEAF2.0_Cloud (Request R, String LN)
{
Input:
R: request of customer;
LN: Location Name of Customer;
Initialization:
C=CreateRequest (R, LN);
SPR_Model(C);//category Request
Master=SendRequest (R, LN) ;//send request to cloud and select master server
SD=Service_Delivery(R);//delivery request with Service Delivery Layer
SML=SendToManagementLayer (SD);
Process_Request_With_MLayer (SML);
SendToInfrastructureLayer (SML);
Tasks=Partitioning_Requests (SML);
Initialize Network Unit;
Initialize Storage Unit;// initialize Units of Infrastructure Layer
Initialize Compute Unit;
i=0;
While (Not End of Tasks)
{
CT=Compute (Tasks[i]);
Storeage_Cell[i]=StoreCTResult(CT);
i++;
}
SendToNextLayer (Storeage_Cell);
SendEndResultTo_DeliveryLayer (Result, R);
AR=Analyse_Result (Result, R);
SetBMR (AR);
Delivery_EndResultByCustomer (AR);
Output:
Result of Request;
}
```

ALGO 1. The proposed method algorithm

As it can be seen, the ALGO 1 is precisely based on the architecture and flowchart provided in the previous section, and the algorithm implementation steps are proportional to the steps provided in the previous section. In the input section of this pseudo-code, the application and user's name are received in the next step of the application's request function and the type of application will be checked after the initial examination is sent to the cloud management layer. The processing management layer is carried out and sent to the infrastructure layer in this layer. After that, it is calculated by the working computing unit, and the phase is sent to the storage unit. Finally, it shows the analyzed result.

5- Simulation and Experimental Results

In this section, the available cloud reference architectures and the proposed one are compared. It is noteworthy that the provided assessment is based on the comparison of the factors of architectures. Only some important measures are assessed in the comparison. Then, the proposed method in this paper is simulated using, RapidMiner software, and compared to other detection methods for security evaluation, detection of attacks in MATLAB software. The specifications related to the system by which the proposed method was implemented and the results were evaluated are shown in table 1.

Table 1. The system specifications for simulation and results assessment

Hardware/Software	Specifications
Operating system	Windows 7
Operating system type	32 bytes
RAM	4 GB- 3.06 usable
Processor	Intel processor- 7 (Core™) i7 CPU –) Q 720 @ 1.60GHz 1.60 GHz

5-1- Proposed Method Assessment According to the Security Features

In the internet-based environments, preserving users' security and privacy is of great importance. This is more important for the clients who provide their information to the cloud via smart cameras. In the proposed architecture that the combination of vector machines and neural networks algorithm, a simulation was performed by using Rapid Miner software to test and evaluate the data transfer security and providing services to the client through smart cameras. The obtained results are discussed in the following.

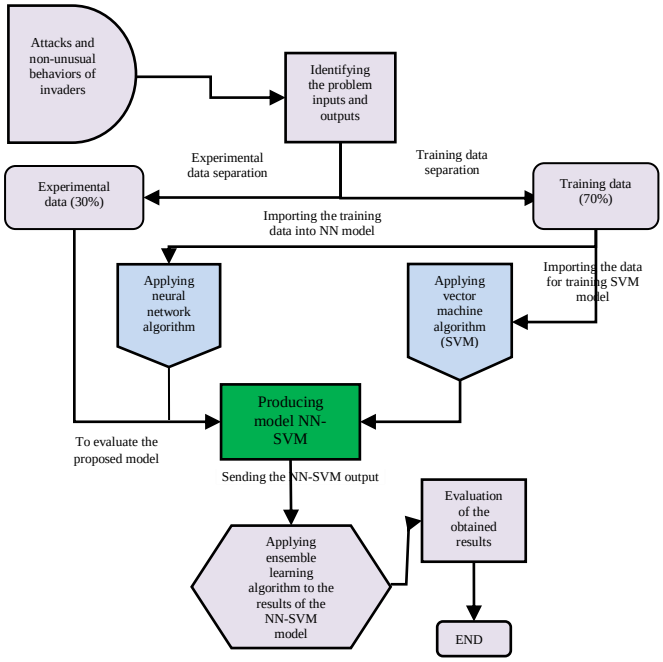

Fig. 3. The flowchart of applications security for CCTV cameras of the cloud computation by using the proposed NN-SVM method

Fig 3, the flowchart of applications and transfers security for smart cameras in visual networks in the proposed cloud computation architecture is shown.

The flowchart in Fig 3 shows the identifying procedure of the attacks to the smart cameras in visual networks according to the proposed method, which is combined from the support vector machine algorithm, and neural network as well as cumulative strategy. In this research, the proposed method is named NN-SVM. Considering the flowchart, first, the dataset related to the applied attacks on the smart cameras in visual networks, so-called the dataset of attacks to the system is imported to evaluate the proposed NN-SVM method. After that, the problem inputs as variables or features related to the dataset are identified. The feature indicating the attack type or application normality is also determined.

To evaluate the security and to model the proposed framework in this research, it was needed to use some datasets for testing the security. Therefore, there are not so many datasets to evaluate whether abnormal behaviors of the systems in the smart cameras exist in the visual networks. Studying basic used kinds of literature in this research, it was seen that most of the papers have exploited Malware Capture Facility Project (MCFP) dataset. This dataset was compiled at CTU University in the Czech Republic [28]. The files on each dataset are usually very large so they are stored in a server at the university. This dataset has various versions from which the newest one was used for evaluation. This is the most commonly used dataset for detecting systems abnormal behaviors and for evaluating the security of architecture in cloud computation. MCFP dataset includes 1048576 records with 39 features.

Out of 39 available features, 38 are defined as the system input and one is defined as the system output. By logging of the 39 features, 15 ones are selected as prominent features by the university. The first 14 features summarized in the following table indicate the features related to a system's abnormal behavior in form of an attack. The 15th feature as the last one is as the placed attack. Using the first 14 features, the last one (label) can be identified.

Due to the large size of the feature set and to facilitate the evaluations, 10 percent of the records were chosen randomly for the chosen set to include 10500 records with the same features. The dataset includes all of the attacks such as Botnet, DDOS, CVUT[1], etc. which are occurred for each system, organization, or individual's application. For correct evaluation, all of the attacks are considered as the same which 1654 records did not contain attacks, and 8855 records include attacks and system abnormal behaviors. Various available features in the dataset are summarized in Table 2.

Table 2. List of features and related characteristics

Feature name	Description	Type
Star Time	Start time	Continuous
Dur	Connection duration	Discrete
Proto	Protocol	Discrete
srcAddr	Source Address	Continuous
Sport	Source Port	Continuous
Dir	Directory	Discrete
DstAddr	Destination Address	Discrete
Dport	Destination Port	Continuous
State	State	Continuous
sTos	Source application service	Discrete
dTos	Destination offered service	Discrete
ToPackt	Number of packets	Continuous
TotByes	Number of bytes	Continuous
SrxBytes	Size of packet	Continuous
Label	Label (output)	Discrete

The last feature, which is considered as the attack type applied on the smart cameras in the visual networks, is divided into 5 categories, showing the applied attack types. The attacks are classified as follows:

Number 1 shows normal behaviors. Other numbers from 2-5 show abnormal behaviors, which are Botnet, attacks. Therefore, Botnet attacks are divided into 4 categories, which are known as Botnet type 1, Botnet type 2, Botnet type 3, and Botnet type 4.

All of the 15 features mentioned are used as the training model, and the last feature of the label is used to identify the type of attacks and abnormal behavior of the system. According to the procedure, the related data including these 15 features as the training samples are imported in the simulator. After performing and applying the proposed methods to the

1. It is among the most important attacks and abnormal behaviors applied by the hackers on the smart cameras in the visual networks.

related data, the training samples are introduced with no label. In this step, considering 14 features of interest, attacks and system abnormal behaviors are identified, and a label is attached, showing what the type of attack is.

Then, the imported data are separated into two training and experimental sections. The training data are used to produce the models related to the support vector machine (SVM) and neural network (NN) algorithms among the most commonly used algorithms to identify breaches. The experimental data are exploited to evaluate the precision and error of the proposed method. To this end, 70% and 30% of the data are considered as the training and experimental data, respectively. Now, the training data are applied to the NN and SVM models to produce the related model. Finally, the experimental data are applied to the produced model, and for each sample of the experimental data, it is identified that the sample is whether an attack or a normal application. The cumulative strategy is applied to the results and outputs of the NN and SVM models, performing the last identification finally.

Considering the above flowchart, the proposed method was implemented by RapidMiner software. The modeling related to the SVM algorithm is seen in fig 4.

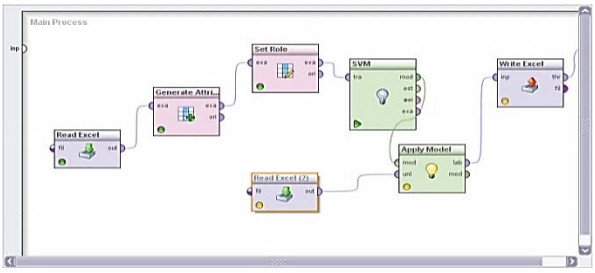

Fig. 4. SVM model for modeling and identifying attacks in the cloud computation

The training data of 70% are applied to the Generate Attribute control, determining the problem inputs. Then, the problem output is identified by the Set Role control. Finally, the SVM algorithm is performed on the training data, and the related model is produced as Apply Model. Then, Read Excel imports the experimental data into the bottom section; finally, it is applied to the produced model called Apply Model, generating the results. The models related to the NN algorithm are seen in Fig 5.

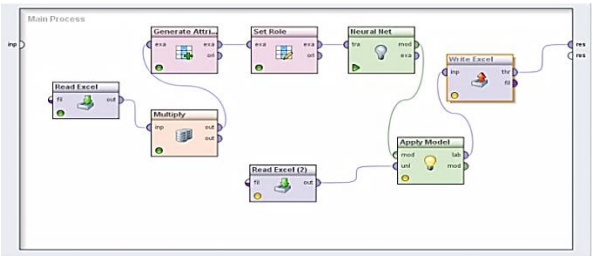

Fig. 5. The neural network model for generating the model and identifying attacks in the cloud computation

The assessment results for the proposed architecture security in the cloud computation by using the proposed NN-SVM method are as follows.

Table 3. Results and identification precision of the attacks by using the NN-SVM algorithm

Sample	Type of the main attack	Attack identification by SVM method	Attack identification by neural network	SVM error	NN error
1	1	1.659860319	1.046367543	0.65986	0.046368
2	1	1.604163382	1.01363806	0.604163	0.013638
3	1	1.586164829	1.005893113	0.586165	0.005893
4	1	1.576049401	1.003681723	0.576049	0.003682
5	1	1.570627125	1.002386739	0.570627	0.002387
6	2	2.683608079	1.298985549	0.683608	0.701014
7	2	2.676240453	1.993326485	0.67624	0.006674
8	2	2.6·2283178	1.298272655	0.682283	0.701727
9	3	4.618082618	3.222731178	1.618083	0.222731
10	3	2.997662624	2.820934385	0.002337	0.179066
11	3	3.166524806	2.914030606	0.166525	0.085969
12	5	6.006369533	4.742892198	1.00637	0.257108
13	5	5.995303345	4.826195301	0.995303	0.173805

Checking Table 3. the types of attacks to the smart cameras in visual networks were identified by using various methods. As an example, in row 13, the attack is of type 5 which is a storage database in the system. By applying the SVM algorithm to the related sample, the answer of 5.9 is obtained, which the final solution is acquired by rounding it up or down. By rounding 5.9, the answer is 6 to which the attack is not identified correctly; this is a negative point. However, the neural network identified it correctly as 4.8; that is a plus. Combining the two algorithms due to neural network algorithm has higher precision than the SVM, and because the answers are not similar, the solution of the model is chosen identifies better.

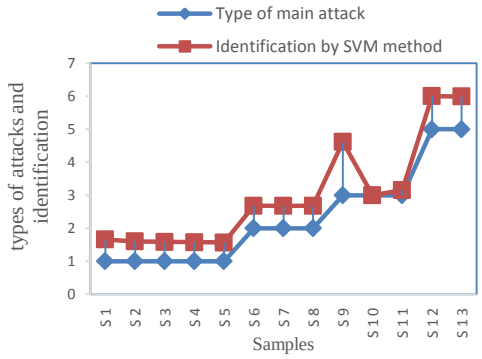

Fig. 6. Preserving the security of the smart cameras in visual networks in the proposed architecture by using a support vector machine algorithm

In fig 6, discrepancies of the SVM algorithm identification are shown for 13 samples of the applied attacks to the smart cameras in visual networks in MATLAB software. At each step you can see the number of detected attacks in the vertical axes, this number is compared to the type of

attacks stored in the database. Finally, the attack is detected by the SVM algorithm.

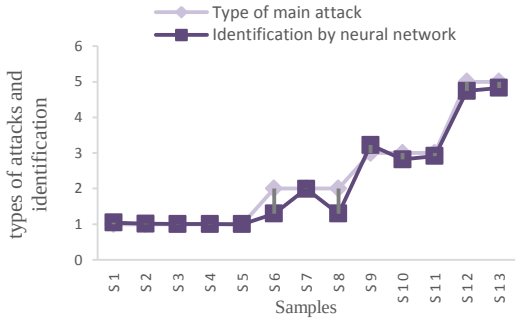

Fig. 7. Preserving the security of the smart cameras in visual networks in the proposed architecture by using a neural network algorithm

As it can be seen in fig 7, it is evident in figure 7 that attacks are identified by using the proposed algorithm in the architecture with a very low discrepancy, allowing breach detection to the proposed architecture. In the following figure, discrepancies of the neural network algorithm identification are shown for 13 samples of the applied attacks and in vertical axes has shown the number of obtained attacks in every step according to the proposed architecture security features in MATLAB software.

By viewing in Fig 8, attacks are identified by the proposed algorithm in the architecture with a very low discrepancy, allowing breach detection to the proposed architecture. It is noteworthy that the neural network algorithm has a much lower discrepancy compared to the support vector machine algorithm in attack identification.

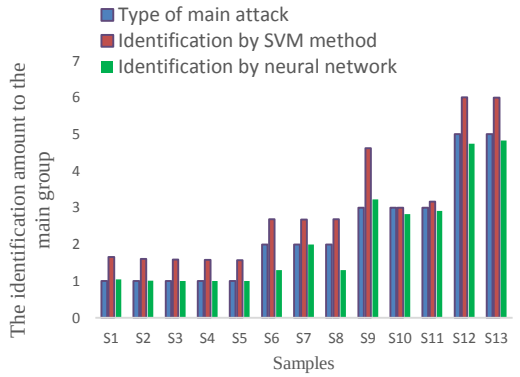

Fig. 8. Comparison of the precision of the proposed NN-SVM method for preserving the security of the proposed architecture

In Fig 8, the number of attacks identified using SVM and NN methods versus the main attacks to the smart cameras in visual networks is shown.

In Fig. 9. The error of attacks identification by using SVM and NN methods versus the main attacks are shown. In this way, we have been able to distinguish more accuracy by combining two vector machines and neural network algorithms, and the attacks that are sent towards smart cameras in visual wireless networks will be more accurate.

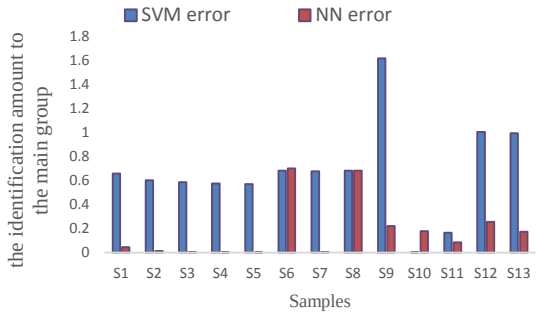

Fig. 9. Comparison of the error of the proposed NN-SVM method for identifying the attacks to the smart cameras in visual networks

Considering the calculation of the proposed method precision using Rapid Miner, the precisions were 99.24% and 99.35% in the best and worst conditions, respectively. Therefore, the proposed NN-SVM method for the architecture in this research preserves the data security for the smart cameras in visual networks with applicable precision. It defeats the attack when observing one of the proposed frameworks.

Table 4 shows the comparison of the results of the proposed method with other methods. In this research, the accuracy criterion is one of the important design criteria and we compare it with other methods. The table below shows the accuracy of the proposed method with other popular methods.

Table 4. Comparison of accuracy, call accuracy, and error detection to maintain security in the proposed method with other methods.

Detecting Attacks	**Proposed Method**	**Liner-SVM** [29]	**RBF** [29]
Accuracy	99.35%	98.19%	98.21%
Error	0.65%	1.81%	1.79%

In general, the two most important criteria for detecting attacks to maintain security in the proposed methods are accuracy and error detection, which, as shown in the table above, the proposed method in these two cases works better than the methods mentioned in the source [29]. As can be seen, the accuracy of the proposed method has improved by about 1.16% compared to the Liner-SVM method and has improved by about 1.14% compared to the RBF method.

6- Conclusion

A network of visual sensor networks is distributed from smart camera devices that can process and fuse images from a scene from different perspectives to some of the more useful forms of individual images. Visual sensor

networks are useful in applications that include area monitoring, tracking, and environmental monitoring. Visual sensor networks (VSNs) are receiving a lot of attention in research, and at the same time, commercial applications are starting to emerge. They use wireless communication interfaces to collaborate and jointly solve tasks such as tracking persons within the network. VSNs are expected to replace not only many traditional, closed-circuit surveillance systems but also to enable emerging applications in scenarios such as elderly care, home monitoring, or entertainment. The highly sensitive nature of images makes security and privacy in VSNs even more important than in most other sensor and data networks. In the current research, a novel framework is provided by aiding the cloud computing technology. Then, the detection of attacks on smart cameras in wireless sensor networks was analyzed with the proposed algorithm of NN-SVM. This method has been simulated with systematic attacks collected at the CTU University-related Czech Republic with RapidMiner software. Finally, the Accuracy of detection of attacks and the proposed method error was implemented in MATLAB software. The results show that the proposed algorithm has been able to provide security requirements for smart cameras in visual wireless networks.

References

[1] V. D. Kale, “Recent Research Trends in Cloud computing,” vol. 6, no. 2, pp. 406–409, 2013.

[2] A. Boukerche et al., “A new solution for the time-space localization problem in wireless sensor network using UAV,” in Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications - DIVANet ’13, 2013, pp. 153–160, doi: 10.1145/2512921.2512937.

[3] Y. Charfi et al., “A pervasive smart camera network architecture applied for multi-camera object classification,” Proc. IEEE, vol. 96, no. 2, pp. 636–641, May 2009, doi: 10.1109/ICDSC.2009.5289377.

[4] B. Rinner, T. Winkler, M. Quaritsch, B. Rinner, W. Schriebl, and W. Wolf, The evolution from single to pervasive smart cameras Epigenetic regulation of stress induced drug tolerance View project VECTO-Vehicle Energy Consumption Calculation Tool View project THE EVOLUTION FROM SINGLE TO PERVASIVE SMART CAMERAS. 2008.

[5] P. Chen et al., “Citric: A low-bandwidth wireless camera network platform,” in 2008 2nd ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC 2008, 2008, doi: 10.1109/ICDSC.2008.4635675.

[6] P. Saastamoinen, S. Huttunen, V. Takala, M. Heikkilä, and J. Heikkilä, “Scallop: An open peer-to-peer framework for distributed sensor networks,” in 2008 2nd ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC 2008, 2008, doi: 10.1109/ICDSC.2008.4635712.

[7] “Mohajer, Amin, Maryam Bavaghar, Rashin Saboor, and Ali Payandeh. "Secure dominating set-based routing protocol in MANET: Using reputation." In 2013 10th International ISC Conference on Information Security and Cryptology (ISCISC), pp. 1-7. IEEE, 2013.”

[8] W. Dargie and C. Poellabauer, Fundamentals of Wireless Sensor Networks. 2010.

[9] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, “The evolution of MAC protocols in wireless sensor networks: A survey,” IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 101–120, 2013, doi: 10.1109/SURV.2012.040412.00105.

[10] K. Langendoen and N. Reijers, “Distributed localization in wireless sensor networks: a quantitative comparison,” Comput. Networks, vol. 43, no. 4, pp. 499–518, Nov. 2003, doi: 10.1016/S1389-1286(03)00356-6.

[11] F. Gherardi and L. Aquiloni, “Sexual selection in crayfish: A review,” Crustac. Monogr., vol. 15, no. August, pp. 213–223, 2011, doi: 10.1163/ej.9789004174252.i-354.145.

[12] A. Wyner and J. Ziv, “The rate-distortion function for source coding with side information at the decoder,” IEEE Trans. Inf. Theory, vol. 22, no. 1, pp. 1–10, Jan. 1976, doi: 10.1109/TIT.1976.1055508.

[13] S. Soro and W. Heinzelman, “A Survey of Visual Sensor Networks,” Adv. Multimed., vol. 2009, pp. 1–21, 2009, doi: 10.1155/2009/640386.

[14] M. Malathi, “Cloud computing concepts,” in 2011 3rd International Conference on Electronics Computer Technology, 2011, vol. 6, pp. 236–239, doi: 10.1109/ICECTECH.2011.5942089.

[15] N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion Detection Systems in Wireless Sensor Networks : A Review,” vol. 2013, 2013, doi: 10.1155/2013/167575.

[16] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, “Wireless multimedia sensor networks: applications and testbeds,” in Proceedings of the IEEE, 2008, vol. 96, no. 10, pp. 1588–1605, doi: 10.1109/JPROC.2008.928756.

[17] M. Ahmadi and S. M. Jameii, “A Secure Routing Algorithm for Underwater Wireless Sensor Networks,” Int. J. Eng., vol. 31, no. 10, pp. 1659–1665, Oct. 2018, doi: 10.5829/ije.2018.31.10a.07.

[18] M. Quaritsch, B. Rinner, and B. Strobl, “Improved agent-oriented middleware for distributed smart cameras,” in 2007 1st ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC, 2007, pp. 297–304, doi: 10.1109/ICDSC.2007.4357537.

[19] A. Doblander, A. Zoufal, and B. Rinner, “A novel software framework for embedded multiprocessor smart cameras,” ACM Trans. Embed. Comput. Syst., vol. 8, no. 3, pp. 1–30, Apr. 2009, doi: 10.1145/1509288.1509296.

[20] S. R. Taghizadeh and S. Mohammadi, “LEBRP - A lightweight and energy balancing routing protocol for energy-constrained wireless ad hoc networks,” Int. J. Eng. Trans. A Basics, vol. 27, no. 1, pp. 33–38, 2014, doi: 10.5829/idosi.ije.2014.27.01a.05.

[21] R. Zhang, “Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division,” vol. 2019, no. 1, 2019.

[22] C.-F. Lin, S.-M. Yuan, M.-C. Leu, and C.-T. Tsai, “A Framework for Scalable Cloud Video Recorder System in Surveillance Environment,” in 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted

Computing, 2012, pp. 655–660, doi: 10.1109/UIC-ATC.2012.72.

[23] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia," Electronics, vol. 8, no. 4, p. 412, Apr. 2019, doi: 10.3390/electronics8040412.

[24] A. Tekeoglu and A. S. Tosun, "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam," in 2015 24th International Conference on Computer Communication and Networks (ICCCN), 2015, vol. 2015-Octob, pp. 1–6, doi: 10.1109/ICCCN.2015.7288421.

[25] L. Valentín, S. A. Serrano, R. Oves García, A. Andrade, M. A. Palacios-Alonso, and L. Enrique Sucar, "A CLOUD-BASED ARCHITECTURE FOR SMART VIDEO SURVEILLANCE," ISPRS - Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci., vol. XLII-4/W3, no. 4W3, pp. 99–104, Sep. 2017, doi: 10.5194/isprs-archives-XLII-4-W3-99-2017.

[26] K. K. Basu, "Organisational culture and leadership in ERP implementation," Int. J. Strateg. Chang. Manag., vol. 6, no. 3/4, p. 292, 2015, doi: 10.1504/IJSCM.2015.075919.

[27] D. Bijwe, "International Journal of Computer Science and Mobile Computing Database in Cloud Computing-Database-as-a Service (DBaas) with its Challenges," Int. J. Comput. Sci. Mob. Comput., vol. 4, no. 2, pp. 73–79, 2015.

[28] M. Grill and J. Stiborek, "An Empirical Comparison of Botnet Detection Methods An Empirical Comparison of Botnet Detection Methods," no. September, 2014, doi: 10.1016/j.cose.2014.05.011.

[29] "Intrusion Detection System Based on Cost Based Support Vector Machine," 2016, doi: 10.1007/978-3-319-40415-8.