Threat Analysis in IOT Network Using Evolutionary Sparse Convolute Network Intrusion Detection System

https://doi.org/10.3991/ijoe.v19i03.37571

Alaa Q. Raheema(✉)
Civil Engineering Department, University of Technology, Baghdad, Iraq
40345@uotechnology.edu.iq

Abstract—Internet of Things (IoT) played a crucial role in various sectors such as automobiles and the logistic tracking medical field because it consists of distributed nodes, servers, and software for effective communication. Although, this IoT paradigm suffered from intrusion threats and attacks that cause security and privacy issues. Existing intrusion detection techniques fail to maintain reliability against the attacks. Therefore, in this work, IoT intrusion threat has been analyzed by using the sparse convolute network to contest the threats and attacks. The network is trained using sets of intrusion data, characteristics, and suspicious activities, which helps identify and track the attacks, mainly Distributed Denial of Service (DDoS) attacks. Along with this, the network is optimized using evolutionary techniques that identify and detect the regular, error, and intrusion attempts under different conditions. The sparse network forms the complex hypotheses evaluated using neurons, and the obtained event stream outputs are propagated to further hidden layer processes. This process minimizes the intrusion involvement in IoT data transmission. The effective utilization of training patterns in the network classifies the standard and threat patterns successfully. Then the effectiveness of the system is evaluated using experimental results and discussion.

Keywords—Internet of Things (IoT), intrusion threats, distributed denial of services, sparse convolute network, detection system, statistical analysis

1 Introduction

Internet of things (IoT) [1, 2] has a collection of network devices that are interconnected via near-field communication (NFC), Bluetooth, and Wi-Fi connections [3]. The IoT devices are widely utilized in smart appliances (thermostats, refrigerators, etc.), security systems, health care, computer peripherals, military, agriculture, etc. [4–6]. These IoT devices utilize the Internet Protocol (IP) to transmit the information from source to destination. This IP protocol identifies the computer to allow communication very fast without requiring human intervention. However, the IoT devices change human life in different applications, the threats to IoT lead to a significant security risk.

Every IoT device has specific characteristics [7], such as large data gathering, physical and virtual environment connection, complex environment creation, centralized architecture. These characteristics enable the IoT to function efficiently, but it causes threat actors abuse in communication. According to the Cisco report, around 10 billion IoT devices [8] are utilized by the world population to improve their lifestyle. The high utilization of IoT devices faces IoT security issues in the fast expansion of smart appliances because of connecting to the network. The device-linked IoT devices consist of home automation; thermostats, printers, refrigerators, etc., are operated with the help of artificial intelligence like Google Assistant, Amazon Alexa [9, 10]. Hence, hijacking [11] these devices are easy by sending spam emails, conscripted into a botnet, and privacy leaks. By considering these, IoT devices are developed by considering the security-related features [12]. Although, the IoT device utilization is increased, and the transmission of data is uncountable. The significant amount of data transmission and billions of connections leads to difficulties while managing and tracking data security [13–16]. The IoT devices are susceptible to weaponization and hijacking for the Distributed Denial of Service (DDoS) attacks [17], man-in-the-middle attack [18], targeted code injection [19], and spoofing [20]. In addition to this, the IoT devices are remotely controlled by the bad actors, creating a significant impact while transmitting data in the network. Therefore, managing and protecting the IoT security more essential to reduce the intermediate attacks in a network environment [21]. Then the security threats should be reduced by making the complete visible network, segmentation of IoT devices, monitoring, inspection and policy enforcement, and taking immediate automatic actions if the network influenced by attacks. The IoT security has been achieved by using the Intrusion Detection System (IDS) [22–24]. The IDS system uses various devices and software applications that help to monitor the network and predict malicious activities. Suppose the system or IoT devices face any violations of the security information and event management (SIEM) control [25] their activities. Here, SIEM integrates multiple source outputs and alarm filtering techniques to differentiate malicious activities [26]. The intrusions are prevented by four types: network-based, wireless intrusion, network behavior analysis, and host-based intrusion prevention system. These four types continuously monitoring the entire network, wireless network, and software packages, and the suspicious traffic are predicted successfully. This prevention process uses statistical anomaly-based, signature-based, and stateful protocol analysis for detecting the intrusion activities in the network [27]. These methods successfully predict the intrusion activities by examining network protocol with the predetermined and pre-configured attack patterns. Therefore, the intrusion detection system should design according to the threat patterns. The patterns are classified into misuse intrusion patterns [28] (it helps to predict the entire known threats by comparing the matching patterns) and anomaly intrusion [29] (this intrusion detects based on the network behavior). Sometimes, this system develops by combining the misuse and anomaly intrusion patterns to reduce the intermediate access. By considering these patterns, statistical analysis, evolutionary algorithm, protocol verification, rule-based, and machine learning techniques [30] are introduced to detect and prevent intrusion activities. The general description of these methods is illustrated in Table 1.

Table 1. Intrusion detection techniques

S. NO	Technique	Description
1	Statistical Analysis [31]	This analysis is comparing the current behavior with the set of predetermined baselines to the particular period.
2	Evolutionary algorithm [32]	It develops the application path that used to predict the model normal, error, and different behaviors according to the conditions
3	Protocol Verification [33]	The suspicious activities are predicted by checking the protocol field. However, the false-positive rate is produced due to the unspecified protocols.
4	Rules-based [34]	This technique predicts the intrusions by comparing them with the signatures.
5	Machine learning technique [35]	Evaluating the hypothesis with a set of nodes and the feedback process predicts the intrusions.

As discussed in Table 1, different techniques are incorporated in the IoT network to predict ht intrusion activities. Machine learning techniques provide satisfactory results because the network is trained using sets of intrusion data, characteristics, and suspicious activities, which helps identify and track the attacks, mainly Distributed Denial of Service (DDoS) attacks. By considering the impact of machine learning techniques in the intrusion threat analysis process, these evolutionary techniques are incorporated to manage the reliability against the attacks.

Then the rest of the paper is organized as follows; section 2 discussed the various research opinion regarding intrusion and threat analysis in IoT networks. Section 3 explores the working process of machine learning with the evolutionary technique-based threat analysis process. Section 4 discusses the efficiency of the introduced system and concludes in section 5.

2 Related works

Particle swarm optimization with gradient descent algorithm (PSO-Light) utilized in [36] to detect the intrusion activities in the Internet of Things (IoT). This system aims to resolve the poor scalability and low detection rate while recognizing intrusion activities. The PSO-Light algorithm derives the features are from input data and fed them into the one-class support vector machine to identify the malicious data. This process applied to the UNSW-NB15 dataset, and the PSO-Light approach recognize the shellcode, backdoor, and worm activities with maximum detection rate. Passban intelligent intrusion detection system created in [22] to prevent the IoT devices from intrusion activities. The created Passban helps identify malicious traffic such as SSH Brute force, Port scanning, and SYN flood attacks. This system resolves the existing accuracy and false positive rate challenges with a high detection rate. Three-layer supervised intrusion detection developed in [37] to detect the weakest IoT devices in smart home applications. First, the IoT device's normal and abnormal behaviors are classified, malicious packets are identified at the time of attack occurrence, and attacks like denial of service (Dos), spoofing, man-in-the-middle, and replay attacks are detected successfully.

This process detects multi-stage attacks with a minimum false positive rate. They introduce a genetic optimized deep belief network (GA-DBN) algorithm in [38] to create an effective intrusion detection model. This work predicts various types of attacks using different number genetic algorithm iterations and multiple hidden layers. The optimized classifiers classify the attacks with maximum detection rate on analyzing the NSL-KDD dataset. Also, this process minimizes the computation complexity. Two-tier classification model and dimension reduction algorithm applied in the Internet of Things Backbone network [39] to predict the anomaly-related intrusion detection. This process intended to detect the remote to local and user to root attacks by utilizing the linear discrimination and component analysis approach. The extracted features are proceeding with the help of K-nearest neighbor and Naïve Bayes to predict the suspicious actives. Introducing two-stage artificial intelligence (AI) related intrusion detection process in [40] to detect the abnormal activities in software-defined IoT (SD-IoT). This system aims to detect the signature and unknown attacks in SD-IoT. Here, the features are selected according to the bat algorithm with binary differential mutation and the weights of the system optimized random forest approach. This process detects abnormal activities with high accuracy and lower overhead. Stochastic Petri net (SPN) in [41] with different attack strategies for developing the intrusion detection system. This process improves the network lifetime using a set of parameter values and reduces intruder involvement in the Internet of things (IoT). This system considering several failure conditions to detect malicious attacks using 128 mobile sensor nodes. Analyzing and protecting network traffic in [42] using ensemble intrusion detection techniques and statistical flow features. This paper focuses on the different protocol-related malicious activities and the attacks detected using naïve Bayes, decision tree, neural network. This system developed using NIMS and UNSW-NB15 datasets, and different potential characteristics are extracted. From the derived features, malicious activities are removed based on the correlation coefficient and correntropy features. Thus, the system ensures the minimum false positive rate and high detection rate. Formulating multi-agent and multilayered game process in the Internet of things (IoT) in [43] to detect the intrusions. This system aims to prevent and avoid security-related vulnerabilities using multilayered game formulation. This process incorporated with the trust model to making the trust communication process. The system ensures security with minimum delay and maximum accuracy and throughput. Applying deep convolution neural networks in [44] to identify the intrusions in intelligent Internet of vehicles. The data-driven approach is linked with the rode side unite (RSU) load behavior to prevent attacks. These features are extracted according to the convolution neural network that aims to avoid RSU attacks. Machine learning techniques are utilized in [45] to detect the Malicious bot in IoT. This system aims to reduce the misclassification of malicious activities using effective network traffic features. The corrAUC approach is applied to select the features that work according to the wrapper technique. Features are chosen based on Shannon entropy and TOPSIS, which helps to classify malicious nodes in Bot-IoT successfully. According to the various researcher opinions, intruders and threats are detected with the help of machine learning techniques. Taking advantage of minimum false positive rate, maximum detection rate, and minimum complexity in this work, an optimized machine learning technique is utilized to analyze the threat activities in the Internet of Things (IoT).

3 Intrusion detection using optimized sparse convolution neural networks

This section discusses the optimized sparse convolution neural network-based intrusion detection in the Internet of Things (IoT). As discussed earlier, intrusions are prevented in any type like host, network, wireless, etc. This kind of data has been utilized to extract the anomaly features using introduced approaches. The extracted features are more helpful in predicting intrusions and threats with minimum complexity and maximum detection rate. Then the intrusion detection system is illustrated in Figure 1.

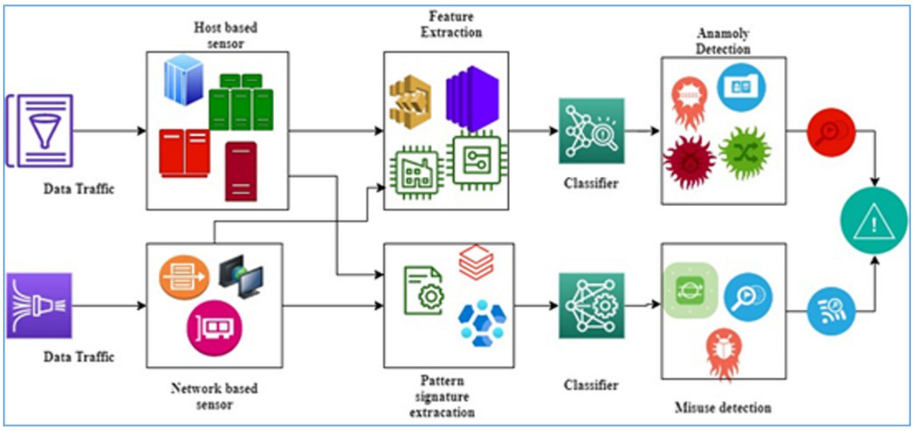


Fig. 1. Intelligent intrusion detection system in the Internet of Things (IoT)

This study's main objective is to detect threat and intrusion activities from the data traffic presented in the network and host reliably. The goal is achieved according to eqn (1), that is, the output of convolution layer feature map $O \in \mathbb{C}^{(g-s+1)*(w-s+1)*n} = \mathfrak{K} * \mathfrak{J}$ defined by

$$O(y,x,j) = \sum_{i=1}^{m} \sum_{u,v=1}^{s} \mathfrak{K}(u,v,i,j)\mathfrak{J}(y+u-1,x+v-1,i) \tag{1}$$

The objective is obtained from feature map $\mathfrak{J}$ in $\mathbb{C}^{g*w*m}$, here input feature map height and width are denoted as g, and w. convolutions kernel is $\mathfrak{K}$ with size s and n number of the output channel. During the threat identification process, the network uses zero paddings and one stride. The threat should be detected in a reliable and fast manner according to the sparse matrices. For this, the feature tensor should change according to sparse multiplication matrix-like $\mathfrak{J}\ to\ \mathfrak{J} \in \mathbb{C}^{g*w*m}$ and kernel $\mathfrak{K}$ to $\mathfrak{R} \in \mathbb{C}^{s*s*m*n}$ to $\mathfrak{P} \in \mathbb{C}^{m*m}$. Generally, kernel operation is performed with the multiplication of kernel $\mathfrak{K}$ and input $\mathfrak{J}$, which is replaced by $O \approx \mathfrak{R} * \mathfrak{J}$ that is defined as follows.

$$\mathfrak{K}(u,v,i,j) \approx \sum_{k=1}^{m} \mathfrak{R}(u,v,k,j)\,\mathfrak{P}(k,i) \tag{2}$$

$$\mathfrak{I}(y,x,i)=\sum_{k=1}^{m}\mathfrak{P}(i,k)\mathfrak{I}(y,x,k) \tag{3}$$

Then, for channel i, decompose the tensor ($\mathfrak{R}(.,.,i,.)\in\mathbb{C}^{s*s*n}$) into the product of matrix ($\mathfrak{S}_i\in\mathbb{C}^{q_i*n}$) and tensor ($\mathfrak{W}_i\in\mathbb{C}^{s*s*q_i}$) according to number base (q_i) that is defined in eqn (4).

$$\mathfrak{R}(u,v,i,j)\approx\sum_{k=1}^{q_i}\mathfrak{S}_i(k,j)\mathfrak{W}_i(u,v,k) \tag{5}$$

$$\mathfrak{V}_i(y,x,k)=\sum_{u,v=1}^{s}\mathfrak{W}_i(u,v,k)\mathfrak{I}(y+u-1,x+v-1,i) \tag{6}$$

From the denser decomposition process, the sparse convolution operation is performed using eqn (7).

$$O(y,x,j)\approx\sum_{i=1}^{m}\sum_{k=1}^{\mathfrak{W}_i}\mathfrak{S}_i(k,j)\mathfrak{V}_i(y,x,k) \tag{7}$$

Here, O (y, x, j) is formulated according to the single matrix multiplication of $\mathfrak{S}_i(k,j)$ and $\mathfrak{V}_i(y,x,k)$. During this computation, the first two dimensions $\mathfrak{S}_i(k,j)$ from $\mathfrak{R}(u,v,i,j)$ and $\mathfrak{V}_i(y,x,k)$ from $\mathfrak{V}_i(y,x,k)$. They are utilized from the sensor. This sparse convolution kernel value ensures the output of the threat's activities from a user action. However, the computation complexity should be reduced during the threat and intrusion activity detection process. The complexity of the system is measured in terms of counting the number of multiplications. Generally, the convolution network requires mns^2 $(g-s+1)$ $(w-s+1)$. But this work reduces the complexity using sparse kernel process; therefore, complexity is computed from non-zero sparse matrix γ and decomposition of a matrix.

$$\left(\gamma mn+\sum_{i=1}^{n}q_i\right)s^2(g-s+1)(w-s+1)+m^2gw \tag{8}$$

After reducing computation complexity, the matrix formulation problem is reduced by performing decomposition, which is defined in eqn (2 and 3). Then the fine-tuning process is applied to the network to improve the threat detection accuracy and specificity. In the fine-tuning phase, the objective function (eqn 9) is used to minimize the deviation while predicting threats in IoT.

$$minimize_{\mathfrak{P},\mathfrak{W}_i,\mathfrak{S}_i}\mathcal{L}_{net}+\lambda_1\sum_{i=1}^{m}\left\|\mathfrak{S}_i\right\|_1+\lambda_2\sum_{i=1}^{m}\sum_{j=1}^{q_i}\left\|\mathfrak{S}_i(j,.)\right\|_2 \tag{9}$$

The deviation should minimize using the logistic loss function $\mathcal{L}_{net}$ in network output. Element wise matrix defined in $\|.\|_1$ and $\|.\|_2$. Based on the above discussion, the objective of the work is achieved that is, reliable and minimum computation complexity is achieved while detecting threats in IoT. Further, the system's effectiveness improved using an effective training process that is done by using long-short term memory neural networks (LSTM). The training process aims to predict user behavior while the user attempts to perform IoT actions. According to the user behavior and respective features are used to detect the intruder and inside threat. Here, user behavior features are extracted according to the function of LSTM that helps predict anomalous activity. Consider the IoT network has a set of users such as $\{\mathfrak{u}_1, \mathfrak{u}_2, \ldots \mathfrak{u}_k\}$; each user having several actions (A) in a day $\mathcal{J}$. The user actions are represented as $A = \left[A_{\mathfrak{u}_{k,1}}, A_{\mathfrak{u}_{k,2}}, \ldots A_{\mathfrak{u}_{k,j}} \right]$. During the training process, $\mathfrak{u}_k$ actions $A_{\mathfrak{u}_{k,1}}$ in j day is derived that was utilized for the network training process. According to the $\mathfrak{u}_k$ and $A_{\mathfrak{u}_{k,1}}$ Neural networks extract features. Then the derived features are analyzed, and constructing the matrix (fixed-size) $\mathfrak{M}^{\mathfrak{u}_{k,j}}$ which contains user behavior-related temporal features. By utilizing these features, threat and normal activities are classified using the sparse convolution network in the testing phase. Then the overall network training process is illustrated in Figure 2.

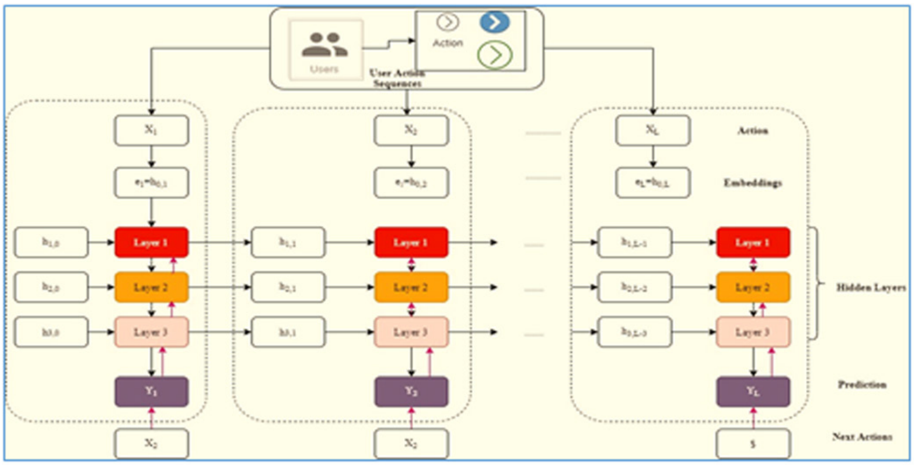


Fig. 2. Intruder actions training using long-short term network

Figure 2 illustrated that the LSTM based training process consists of input, embedding, hidden layer, and output layer. Each layer performs a specific function, and respective user behavior features are extracted. As discussed earlier, the output $\mathfrak{y}_t^{\mathfrak{u}_{k,j}} (1 \leq t \leq T)$ at time instance t is obtained by processing user actions $A_{\mathfrak{u}_{k,j}} = \left\{ X_1^{\mathfrak{u}_{k,j}}, X_2^{\mathfrak{u}_{k,j}}, \ldots .. X_T^{\mathfrak{u}_{k,j}} \right\}. X_t^{\mathfrak{u}_{k,j}} (1 \leq t \leq T)$ in LSTM network hidden layer $h_t^{\mathfrak{u}_{k,j}} (0 \leq l \leq 3, 1 \leq t < T)$. The dictionary should be created for IoT users and individual actions, which helps identify user behavior features. If the user logs in into the IoT device after an hour, that is represented as one and logged off the IoT device after an hour, defined as 2. These actions are converted to the one-vector format to get the exact user behavior in the hidden layer process. In general, the network has the input, weight, and bias values used to predict the output. Three hidden layer process is defined as follows

$$\mathcal{J}_{l,t}^{\mathfrak{u}_{k,j}} = \sigma\left(\mathfrak{Z}_l^{(i,x)} h_{l-1,t}^{\mathfrak{u}_{k,j}} + \mathfrak{Z}_l^{(i,h)} h_{l,t-1}^{\mathfrak{u}_{k,j}} + \mathfrak{b}_l^{i}\right) \tag{10}$$

$$\mathfrak{f}_{l,t}^{\mathfrak{u}_{k,j}} = \sigma\left(\mathfrak{Z}_l^{(\mathfrak{f},x)} h_{l-1,t}^{\mathfrak{u}_{k,j}} + \mathfrak{Z}_l^{(\mathfrak{f},h)} h_{l,t-1}^{\mathfrak{u}_{k,j}} + \mathfrak{b}_l^{\mathfrak{f}}\right) \tag{11}$$

$$\mathfrak{o}_{l,t}^{\mathfrak{u}_{k,j}} = \sigma\left(\mathfrak{Z}_l^{(\mathfrak{o},x)} h_{l-1,t}^{\mathfrak{u}_{k,j}} + \mathfrak{Z}_l^{(\mathfrak{o},h)} h_{l,t-1}^{\mathfrak{u}_{k,j}} + \mathfrak{b}_l^{\mathfrak{o}}\right) \tag{12}$$

$$\mathfrak{g}_{l,t}^{\mathfrak{u}_{k,j}} = tanh\left(\mathfrak{Z}_l^{(\mathfrak{g},x)} h_{l-1,t}^{\mathfrak{u}_{k,j}} + \mathfrak{Z}_l^{(\mathfrak{g},h)} h_{l,t-1}^{\mathfrak{u}_{k,j}} + \mathfrak{b}_l^{\mathfrak{g}}\right) \tag{13}$$

$$\mathfrak{c}_{i,t}^{\mathfrak{u}_{k,j}} = \mathfrak{f}_{l,t}^{\mathfrak{u}_{k,j}} \odot \mathfrak{c}_{i,t-1}^{\mathfrak{u}_{k,j}} + \mathcal{J}_{l,t}^{\mathfrak{u}_{k,j}} \odot \mathfrak{g}_{l,t}^{\mathfrak{u}_{k,j}} \tag{14}$$

$$h_{l,t}^{\mathfrak{u}_{k,j}} = \mathfrak{o}_{l,t}^{\mathfrak{u}_{k,j}} \odot \tanh\left(\mathfrak{c}_{i,t}^{\mathfrak{u}_{k,j}}\right) \tag{15}$$

The above computations are utilized for training the features derived from the user actions. Here, $\mathfrak{c}_{i,0}^{\mathfrak{u}_{k,j}}$ and $h_{l,0}^{\mathfrak{u}_{k,j}}$ values are zero for entire three layers $one \leq l \leq 3$, $\odot$ represented as the element-wise multiplication and $\sigma(.)$ Denoted as the sigmoid function. These functions are applied to the hidden representation $\mathfrak{g}_{l,t}^{\mathfrak{u}_{k,j}}$ to identify the output in hidden units. Along with the value, $\mathcal{J}_{l,t}^{\mathfrak{u}_{k,j}}$ is updated and $\mathfrak{f}_{l,t}^{\mathfrak{u}_{k,j}}$ values are forgetting for getting the $\mathfrak{o}_{l,t}^{\mathfrak{u}_{k,j}}$ output value. This process repeated to investigating the user actions as $A = \left[A_{\mathfrak{u}_{k,1}}, A_{\mathfrak{u}_{k,2}}, \ldots A_{\mathfrak{u}_{k,j}}\right]$ for getting the exact output value $y_{l,t}^{\mathfrak{u}_{k,j}}$. At last, cross-entropy loss value is estimated by collating output $y_{l,t}^{\mathfrak{u}_{k,j}}$ with input $x_{t+1}^{\mathfrak{u}_{k,j}}$. Here dropout process is applied to reduce the overfitting data that helps to improve the overall recognition accuracy; also, the training process runs in different epochs. This process helps to derive the feature vectors $\mathfrak{H}^{\mathfrak{u}_{k,j}} = \left\{h_{3,1}^{\mathfrak{u}_{k,j}}, h_{3,2}^{\mathfrak{u}_{k,j}}, \ldots.. h_{3,T}^{\mathfrak{u}_{k,j}}\right\}$. Then the extracted features are transferred into the fixed-size illustration because it has to be given the input to the sparse convolution neural networks. The user $\mathfrak{u}_k$ any sequence actions $A_{\mathfrak{u}_{k,j}}$ defined in maximum $(N^{\mathfrak{u}_k})$ and minimum length $(n^{\mathfrak{u}_k})$ because the sequences are eliminated from this process which is having low length compared to $n^{\mathfrak{u}_k}$. This process helps to minimize the unwanted computation also maximize the threat detection time. Therefore, zeros are pad between $n^{\mathfrak{u}_k}$ to $(N^{\mathfrak{u}_k})$ to reach the extract features to maximum length. This process is performed to convert the $\mathfrak{H}^{\mathfrak{u}_{k,j}} = \left\{h_{3,1}^{\mathfrak{u}_{k,j}}, h_{3,2}^{\mathfrak{u}_{k,j}}, \ldots.. h_{3,T}^{\mathfrak{u}_{k,j}}\right\}$ feature to matrix $\mathfrak{M}^{\mathfrak{u}_{k,j}} - (N^{\mathfrak{u}_k} * V^{\mathfrak{u}_k})$ *dimension.* Then the formed $\mathfrak{M}^{\mathfrak{u}_{k,j}}$ is given as input to the sparse convolution matrix to analyzing user behavior to predict the threat and everyday activities. Consider, the IoT network has a different number of nodes, in which one node is treated as a server node, and the remaining nodes are a client for data transmission and analytic process. Here, traffic is continuously monitored to eliminate the modification that happened on live traffic; every user action (data transmission) server responds to the client sender node by providing replies. During this process, the sensor node's behavior has to be analyzed to eliminate the intermediate action. Then the IoT communication behavior and attacks are illustrated in Figure 3.

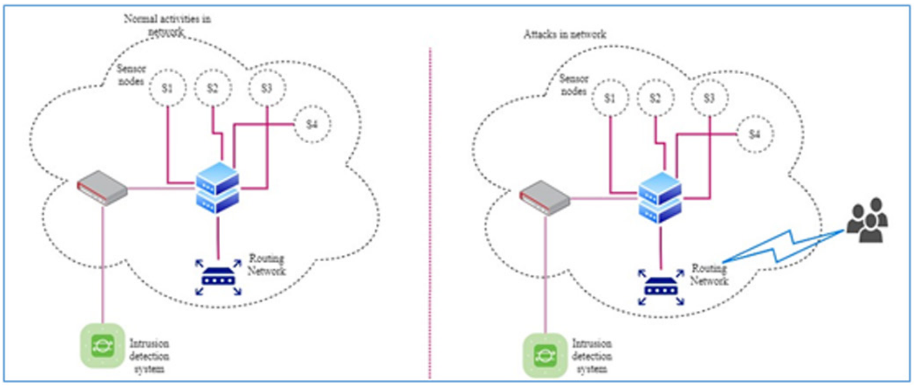


Fig. 3. IoT Experimental structure of intrusion detection system

As shown in Figure 3, the attacker attacks the server node because it analyzes transmitted data, login, and other responding processes. The DDoS attacks happened using a single host among the 10 million packets are transferred. Therefore, the attack must be detected according to user actions in a day. According to the above process, different features like several nodes, neighbor, leaving, joining, etc., information is extracted as features. Those derived features are more valuable to predict the intermediate access. In addition to this, the evolutionary computation algorithm is incorporated to predict the threat activities with minimum loss and high accuracy value. The evolutionary algorithm chooses the best solution for automatically created solutions using the fitness value. Here, the multi-objective evolutionary algorithm is used to find the optimal solution (Pareto set). The predicted solution x is greater than the other solution y. supposes the network does not have any more excellent value; at least one less than values are presented as the optimal solution. Here, sensor node features are continuously examined; if the server node characteristics face any changes, the alarm should be ringed to treat as intruder and attack. Then the efficiency of the system is evaluated using experimental results and discussions.

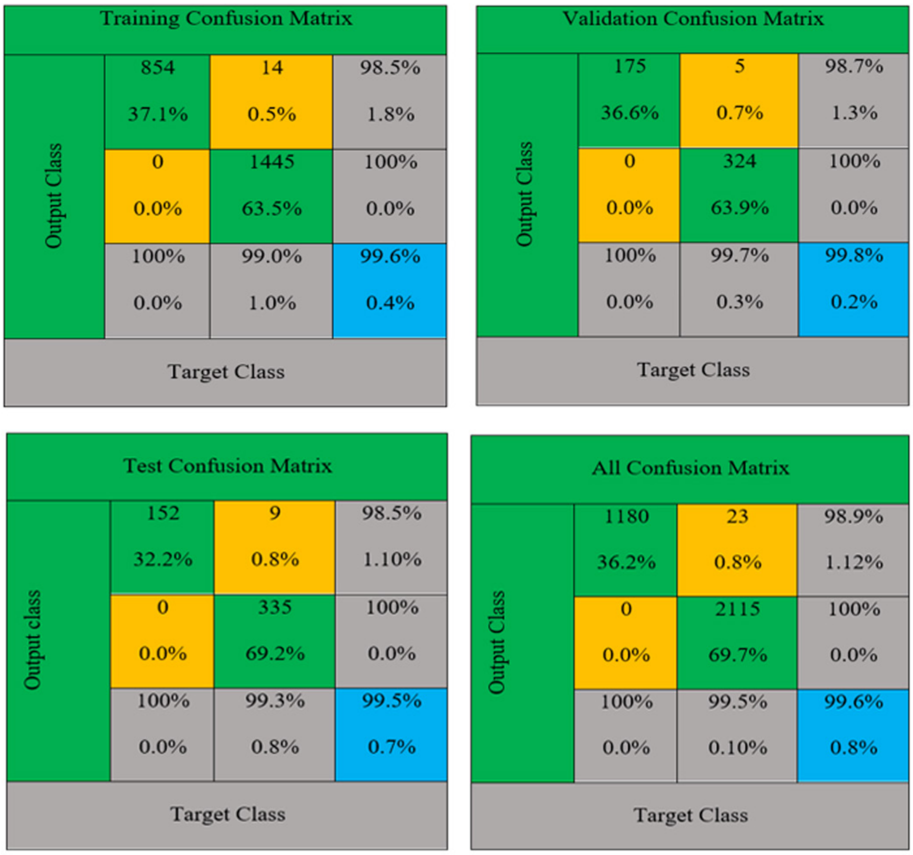
4 Results and discussion

This section evaluates the effectiveness of the evolutionary sparse convolution network (ESCNN) intrusion or threat detection system discussed in section 3. This system uses DDoS Evaluation Dataset [46] for evaluating the introduced system efficiency. The dataset aims to create the manage the network security on various attacks and traffic. The algorithm was developed to reduce the network overhead by using various DDoS attack-related feature examinations. Here, 2313 samples are utilized as training, 490 samples for validation, and 502 samples for testing. Then the data samples used in threat detection activities are illustrated in Table 2.

Table 2. Data sample description

S. No	Type of Attacks	Data Samples	Percentage
1	Distributed Denial of services (DDoS)	2138	65%
2	Normal	1180	35%

This dataset handles various DDoS attacks such as NTP, LDAP, DNS, NetBIOS, MSSQL, TFTP, SYM, WebDDoS, etc. These attacks are executed at a specific time on particular data. The collected samples are trained using the LSTM network, and the obtained results are illustrated in the confusion matrix shown in Figure 4.



Training Confusion Matrix

Output Class			
	854 37.1%	14 0.5%	98.5% 1.8%
	0 0.0%	1445 63.5%	100% 0.0%
	100% 0.0%	99.0% 1.0%	99.6% 0.4%

Target Class

Validation Confusion Matrix

Output Class			
	175 36.6%	5 0.7%	98.7% 1.3%
	0 0.0%	324 63.9%	100% 0.0%
	100% 0.0%	99.7% 0.3%	99.8% 0.2%

Target Class

Test Confusion Matrix

Output class			
	152 32.2%	9 0.8%	98.5% 1.10%
	0 0.0%	335 69.2%	100% 0.0%
	100% 0.0%	99.3% 0.8%	99.5% 0.7%

Target Class

All Confusion Matrix

Output Class			
	1180 36.2%	23 0.8%	98.9% 1.12%
	0 0.0%	2115 69.7%	100% 0.0%
	100% 0.0%	99.5% 0.10%	99.6% 0.8%

Target Class

Fig. 4. Confusion matrix

Figure 4 represented the confusion matrix value of training, testing, validation, and overall confusion matrix. The confusion matrix formed according to the false positive rate (FP) (it indicates the correct classification of the normal events-yellow box) and true positive rate (TP) (measures the correct classification of attack events-green box). Then the effective training and learning process improves the overall classification rate up to 99.6%. It was able to detect the DDoS attacks in IoT network traffics. The effective computation of this process improves the general network security and alerts the data transmission team in the earlier stage by avoiding network disruptions. Further, the excellence of the system is evaluated using different metrics such as accuracy (Acc)-measures the exact detection from entire data instances, Detection Rate (DR)-intrusion instances ratio, False Alarm Rate (FAR)-misclassification of normal instance, Precision (Pre)-how many attacks are classified correctly and Recall (Re)-detects the how many attacks are done in the model return.

$$\text{Accuracy} = \frac{\text{True positive} + \text{True Negative}}{\text{True positive} + \text{True Negative} + \text{False Positive} + \text{False Negative}} \tag{16}$$

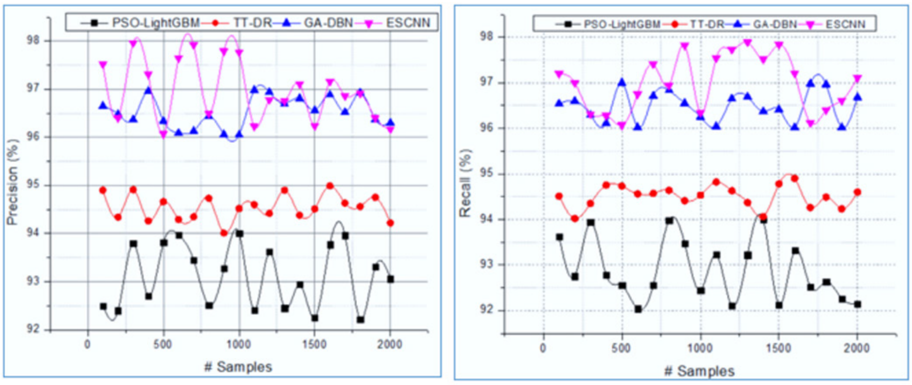
$$\text{Detection Rate (DR)} = \frac{\text{True Positive (TP)}}{\text{True Positive (TP)} + \text{False Negative (FN)}} \tag{17}$$

$$\text{False Alarm Rate (FAR)} = \frac{\text{False Positive}}{\text{True Negative} + \text{False Positive}} \tag{18}$$

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \tag{19}$$

$$\text{Recall} = \frac{\text{True Postive}}{\text{True Positive} + \text{False Negative}} \tag{20}$$

The discussed evolutionary sparse convolution network (ESCNN)classifies the abnormal activities in a reliable and fastest manner. The successful formulation of sparse matrix features from data traffic reduces the computation complexity with maximum accuracy. The obtained accuracy result is illustrated in Figure 4. The introduced ESCNN approach compared with existing research approaches such as Particle swarm optimization with gradient descent algorithm (PSO-Light) [30], genetic optimized deep belief network (GA-DBN) algorithm [33], Two-tier classification model, and dimension reduction algorithm (TT-DR) [34].



(a)

(b)

Fig. 5. (a) Precision and (b) Recall

According to Figure 5a, the ESCNN approach predicts the abnormal activities, i.e., threat in IoT environment, by analyzing user action sequences $A_{\mathfrak{u}_{k,1}}, A_{\mathfrak{u}_{k,2}}, \ldots A_{\mathfrak{u}_{k,j}}$ Using LSTM layers. The successful extraction of $\mathfrak{H}^{\mathfrak{u}_{k,j}} = \left\{ h_{3,1}^{\mathfrak{u}_{k,j}}, h_{3,2}^{\mathfrak{u}_{k,j}}, \ldots\ldots h_{3,T}^{\mathfrak{u}_{k,j}} \right\}$ It helps to identify the normal and abnormal activities while the user tries to execute the IoT environment. From the features, a sparse matrix is generated $\mathfrak{M}^{\mathfrak{u}_{k,j}} - (N^{\mathfrak{u}_k} * V^{\mathfrak{u}_k})$ That minimizes the computation complexity while extracting different activities in IoT. The successful identification of user behavior improves the overall precision value on the different number of samples. From the analyzed behavior, specific abnormal events are predicted correctly by using practical computation of $h_{l,t}^{\mathfrak{u}_{k,j}} = \mathfrak{o}_{l,t}^{\mathfrak{u}_{k,j}} \odot \tanh\left(\mathfrak{c}_{i,t}^{\mathfrak{u}_{k,j}}\right)$. This illustrated in Figure 5b, and the system minimizes the deviations in the fine-tuning phase $minimize_{\mathfrak{P},\mathfrak{W}_i,\mathfrak{S}_i} \mathcal{L}_{net} + \lambda_1 \sum_{i=1}^{m} \left\| \mathfrak{S}_i \right\|_1 + \lambda_2 \sum_{i=1}^{m} \sum_{j=1}^{q_i} \left\| \mathfrak{S}_i (j,.) \right\|_2$. The system improves threat prediction rate and minimizes the false alarm rate (Figure 6).

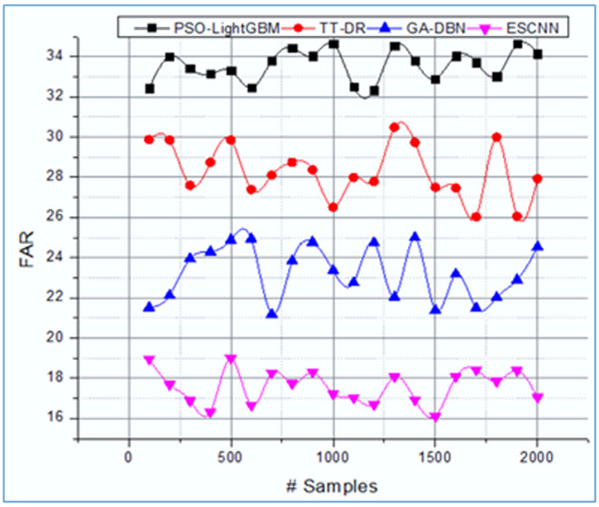


Fig. 6. False alarm rate

The effective computation of $\mathfrak{K}(u,v,i,j)\mathfrak{I}(y+u-1,x+v-1,i)$ sparse multiplication and decomposition of denser and convolution operations help to identify the data traffic feature map. In addition to this, the evolutionary algorithm minimizes the computation problem, and fine-tuning process helps to improve the overall attacks prediction rate. The long-short term neural network training process in different layers $\mathfrak{c}_{i,t}^{\mathfrak{u}_{k,j}} = \mathfrak{f}_{l,t}^{\mathfrak{u}_{k,j}} \odot \mathfrak{c}_{i,t-1}^{\mathfrak{u}_{k,j}} + \mathcal{J}_{l,t}^{\mathfrak{u}_{k,j}} \odot \mathfrak{g}_{l,t}^{\mathfrak{u}_{k,j}}$ helps to reduce the false attack prediction rate. The minimum false alarm rate directly indicates the ESCNN approach maximizes the overall attack detection accuracy and detection rate shown in Table 3.

Table 3. Attack detection rate

S. No	Methods	Accuracy	Detection Rate
1	PSO-Light [30]	93.56	94.29
2	GA-DBN [33]	94.18	95.92
3	TT-DR [34]	93.90	94.23
4	ESCNN	99.29	98.98

The above Table 3 clearly, indicates that the ESCNN approach recognizes the attacks with a maximum detection rate (98.9%). In addition to this, the method classifies the normal and abnormal activities with high recognition accuracy (99.29%). Thus, the process ensures high reliability, fast computation, and reduce computation complexity.

5 Conclusion

Thus, the paper analyzing the evolutionary sparse convolution network (ESCNN) intrusion and threat activities in the Internet of things (IoT). Here, DDoS Evaluation Dataset information is utilized to process the discussed intrusion detection system. The collected data is split into training, testing, and validation set. The data are trained according to the different layers of long-short term networks, which improves the attack detection accuracy. With the help of trained information, testing details are classified by extracting the feature and form the sparse matrix construction. This process improves the overall attack detection accuracy with a minimum false alarm rate. The MATLAB tool implemented the system, and the system ensures 99.98% detection rate and 99.29% accuracy with minimum computation complexity. In the future, the system's effectiveness improved using a meta-heuristic optimizer to estimate the global solution of attack prediction.

6 References

[1] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Computers & Electrical Engineering,* vol. 84, p. 106627, 2020. https://doi.org/10.1016/j.compeleceng.2020.106627

[2] N. A. Jassim and H. Salim, "Design and implementation of smart city applications based on the internet of things," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 3, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[3] V. A. Arowoiya, A. E. Oke, C. O. Aigbavboa, and J. Aliu, "An appraisal of the adoption internet of things (IoT) elements for sustainable construction," *Journal of Engineering, Design and Technology,* 2020. https://doi.org/10.1108/JEDT-10-2019-0270

[4] Á. Verdejo Espinosa, J. L. López, F. Mata Mata, and M. E. Estevez, "Application of IoT in healthcare: keys to implementation of the sustainable development goals," *Sensors,* vol. 21, no. 7, p. 2330, 2021. https://doi.org/10.3390/s21072330

[5] H. Wen *et al.*, "A quantum chaotic image cryptosystem and its application in IoT secure communication," *IEEE Access,* vol. 9, pp. 20481–20492, 2021. https://doi.org/10.1109/ACCESS.2021.3054952

[6] I. A. Aljazaery and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[7] S.-J. Ahn, "Three characteristics of technology competition by IoT-driven digitization," *Technological Forecasting and Social Change,* vol. 157, p. 120062, 2020. https://doi.org/10.1016/j.techfore.2020.120062

[8] V. Morfino and S. Rampone, "Towards near-real-time intrusion detection for IoT devices using supervised learning and apache spark," *Electronics,* vol. 9, no. 3, p. 444, 2020. https://doi.org/10.3390/electronics9030444

[9] D. F. Del Rio, B. Sovacool, and M. Martiskainen, "Controllable, frightening, or fun? Exploring the gendered dynamics of smart home technology preferences in the United Kingdom," *Energy Research & Social Science,* vol. 77, p. 102105, 2021. https://doi.org/10.1016/j.erss.2021.102105

[10] R. S. Dixit and S. L. Choudhary, "Internet of Things Enabled by Artificial Intelligence," in *Towards Smart World*: Chapman and Hall/CRC, 2020, pp. 173–196. https://doi.org/10.1201/9781003056751-10

[11] F. Hategekimana, T. J. Whitaker, M. J. H. Pantho, and C. Bobda, "IoT device security through dynamic hardware isolation with cloud-based update," *Journal of Systems Architecture,* vol. 109, p. 101827, 2020. https://doi.org/10.1016/j.sysarc.2020.101827

[12] F. Humaira, M. S. Islam, S. A. Luva, and M. B. Rahman, "A secure framework for IoT smart home by resolving session hijacking," *Global Journal of Computer Science and Technology,* 2020. https://doi.org/10.34257/GJCSTGVOL20IS2PG9

[13] S. Pirbhulal, W. Wu, K. Muhammad, I. Mehmood, G. Li, and V. H. C. de Albuquerque, "Mobility enabled security for optimizing IoT based intelligent applications," *IEEE Network,* vol. 34, no. 2, pp. 72–77, 2020. https://doi.org/10.1109/MNET.001.1800547

[14] J. Antoniou, "Using game theory to address new security risks in the IoT," in *Game Theory, the Internet of Things and 5G Networks*: Springer, 2020, pp. 21–42. https://doi.org/10.1007/978-3-030-16844-5_2

[15] H. T. ALRikabi and H. T. Hazim, "Secure Chaos of 5G wireless communication system based on IOT applications," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[16] H. Salim, A. H. M. Alaidi, A. S. Abdalrada, and F. T. Abed, "Analysis of the efficient energy prediction for 5G wireless communication technologies," *International Journal of Emerging Technologies in Learning,* vol. 14, no. 8, pp. 23–37, 2019. https://doi.org/10.3991/ijet.v14i08.10485

[17] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," *The Journal of Supercomputing,* vol. 76, no. 7, pp. 5320–5363, 2020. https://doi.org/10.1007/s11227-019-02945-z

[18] O. Toutsop, P. Harvey, and K. Kornegay, "Monitoring and detection time optimization of man in the middle attacks using machine learning," in *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, 2020: IEEE, pp. 1–7. https://doi.org/10.1109/AIPR50011.2020.9425304

[19] B. Kuang, A. Fu, L. Zhou, W. Susilo, and Y. Zhang, "DO-RA: data-oriented runtime attestation for IoT devices," *Computers & Security,* vol. 97, p. 101945, 2020. https://doi.org/10.1016/j.cose.2020.101945

[20] K. M. Malik, A. Javed, H. Malik, and A. Irtaza, "A light-weight replay detection framework for voice controlled IoT devices," *IEEE Journal of Selected Topics in Signal Processing,* vol. 14, no. 5, pp. 982–996, 2020. https://doi.org/10.1109/JSTSP.2020.2999828

[21] O. H. Yahya, R. M. Al_Airaji, and M. Faezipour, "Using internet of things application for disposing of solid waste," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 3, pp. 4–18, 2020. https://doi.org/10.3991/ijim.v14i13.13859

[22] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, “Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices,” *IEEE Internet of Things Journal,* vol. 7, no. 8, pp. 6882–6897, 2020. https://doi.org/10.1109/JIOT.2020.2970501

[23] M. A. Rahman, A. T. Asyhari, L. Leong, G. Satrya, M. H. Tao, and M. Zolkipli, “Scalable machine learning-based intrusion detection system for IoT-enabled smart cities,” *Sustainable Cities and Society,* vol. 61, p. 102324, 2020. https://doi.org/10.1016/j.scs.2020.102324

[24] H. T. H. H. Alrikabi, “Enhanced data security of communication system using combined encryption and steganography,” *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[25] M. Vielberth, “Security Information and Event Management (SIEM),” 2021. https://doi.org/10.1007/978-3-642-27739-9_1681-1

[26] H. Caldeira, “Security Information and Event Management (SIEM) Implementation Recommendations to Enhance Network Security,” *PhD diss., Utica College,* 2021.

[27] K. Gai, M. Qiu, L. Tao, and Y. Zhu, “Intrusion detection techniques for mobile cloud computing in heterogeneous 5G,” *Security and Communication Networks*, vol. 9, no. 16, pp. 3049–3058, 2016. https://doi.org/10.1002/sec.1224

[28] N. Guizani and A. Ghafoor, “A network function virtualization system for detecting malware in large IoT based networks,” *IEEE Journal on Selected Areas in Communications,* vol. 38, no. 6, pp. 1218–1228, 2020. https://doi.org/10.1109/JSAC.2020.2986618

[29] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, “Machine learning for the detection and identification of internet of things devices: a survey,” *IEEE Internet of Things Journal,* vol. 9, no. 1, pp. 298–320, 2021. https://doi.org/10.1109/JIOT.2021.3099028

[30] U. Bodkhe and S. Tanwar, “Secure data dissemination techniques for IoT applications: research challenges and opportunities,” *Software: Practice and Experience,* vol. 51, no. 12, pp. 2469–2491, 2021. https://doi.org/10.1002/spe.2811

[31] A. J. A. Majumder, C. B. Veilleux, and J. D. Miller, “A cyber-physical system to detect IoT security threats of a smart home heterogeneous wireless sensor node,” *IEEE Access,* vol. 8, pp. 205989–206002, 2020. https://doi.org/10.1109/ACCESS.2020.3037032

[32] M. A. Khan and K. A. Abuhasel, “An evolutionary multi-hidden Markov model for intelligent threat sensing in industrial internet of things,” *The Journal of Supercomputing,* vol. 77, no. 6, pp. 6236–6250, 2021. https://doi.org/10.1007/s11227-020-03513-6

[33] K. B. Jalbani, A. H. Jalbani, and S. S. Soomro, “IoT Security: to Secure IoT Devices with Two-Factor Authentication by Using a Secure Protocol,” in *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*: IGI Global, 2020, pp. 98–118. https://doi.org/10.4018/978-1-7998-2803-7.ch006

[34] S. Dange and M. Chatterjee, “IoT botnet: the largest threat to the IoT network,” in *Data Communication and Networks*: Springer, 2020, pp. 137–157. https://doi.org/10.1007/978-981-15-0132-6_10

[35] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, “Security and privacy in IoT using machine learning and blockchain: threats and countermeasures,” *ACM Computing Surveys (CSUR),* vol. 53, no. 6, pp. 1–37, 2020. https://doi.org/10.1145/3417987

[36] J. Liu, D. Yang, M. Lian, and M. Li, “Research on intrusion detection based on particle swarm optimization in IoT,” *IEEE Access,* vol. 9, pp. 38254–38268, 2021. https://doi.org/10.1109/ACCESS.2021.3063671

[37] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, “A supervised intrusion detection system for smart home IoT devices,” *IEEE Internet Things*, vol 6, pp. 9042–9053, 2019. https://doi.org/10.1109/JIOT.2019.2926365

[38] Y. Zhang, P. Li, and X. Wang, “Intrusion detection for IoT based on improved genetic algorithm and deep belief network,” *IEEE Access,* vol. 7, pp. 31711–31722, 2019. https://doi.org/10.1109/ACCESS.2019.2903723

[39] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, 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. https://doi.org/10.1109/TETC.2016.2633228

[40] J. Li, Z. Zhao, R. Li, and H. Zhang, "Ai-based two-stage intrusion detection for software defined iot networks," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2093–2102, 2018. https://doi.org/10.1109/JIOT.2018.2883344

[41] H. Al-Hamadi, R. Chen, D.-C. Wang, and M. Almashan, "Attack and defense strategies for intrusion detection in autonomous distributed IoT systems," *IEEE Access,* vol. 8, pp. 168994–169009, 2020. https://doi.org/10.1109/ACCESS.2020.3023616

[42] 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. https://doi.org/10.1109/JIOT.2018.2871719

[43] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A novel multi-agent and multilayered game formulation for intrusion detection in Internet of Things (IoT)," *IEEE Access,* vol. 8, pp. 98481–98490, 2020. https://doi.org/10.1109/ACCESS.2020.2997711

[44] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, "Data-driven intrusion detection for intelligent internet of vehicles: a deep convolutional neural network-based method," *IEEE Transactions on Network Science and Engineering,* vol. 7, no. 4, pp. 2219–2230, 2020. https://doi.org/10.1109/TNSE.2020.2990984

[45] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal,* vol. 8, no. 5, pp. 3242–3254, 2020. https://doi.org/10.1109/JIOT.2020.3002255

[46] M. Gniewkowski, "An overview of DoS and DDoS attack detection techniques," in *International Conference on Dependability and Complex Systems*, 2020: Springer, pp. 233–241. https://doi.org/10.1007/978-3-030-48256-5_23

7 Author

Alaa Q. Raheema, Civil Engineering Department, University of Technology, 10001 Baghdad, Iraq.

Article submitted 2022-12-21. Resubmitted 2023-01-20. Final acceptance 2023-01-23. Final version published as submitted by the authors.