A Study on Artificial Intelligence-based Security Techniques for IoT-based Systems

Mustafa Al-Tahee[1,*], Marwa s. mahdi hussin[2], Mohammed Jameel Alsalhy[3], Hussein Alaa Diame[4], Noor Hanoon Haroon[5], Salem Saleh Bafjaish[6], Mohammed Nasser Al-Mhiqani[7]

[1]Medical Instruments Engineering Techniques, Al-Farahidi University, Baghdad, Iraq
[2]Computer Technologies Engineering, Al-Turath University College, Baghdad,Iraq
[3]Department Of Medical Devices Engineering Technologies, National University Of Science And Technology, Dhi Qar, Nasiriyah, Liaq
[4]Technical Computer Engineering Department, Al-Kunooze University College, Basrah, Iraq
[5]Department Of Computer Technical Engineering, Technical Engineering College, Al-Ayen University, Thi-Qar, Iraq
[6]College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar
Keele University (KU), Keele, United Kingdom, Staffordshire, ST5 5AA,
Emails: Mustafa Al-Tahee@Uoalfarahidi.Edu.Iq; Marwa.Saad@Turath.Edu.Iq; Sahi@Nust.Edu.Iq; Hussein. Alaa@ Kunoozu.Edu. Iq; Noor@Alayen.Edu.Iq; Salem.Bafjaish@gmail.com; Almohaiqny@gmail.com

Abstract

In a recent scenario, the Internet of Things (IoT**)** enables the Integration of disparate home automation systems into a unified network that can be managed from a single device, such as a smartphone. Connections to the Internet that aren't secure: A lack of security standards may make the Internet of Things devices vulnerable to assault, including hacking. Though current designs may address some security concerns inherent to the Internet of Things, most solutions suffer from two significant flaws. This only addresses a single threat at the level of IoT-edge architecture and cannot be expanded to deal with new threats as misunderstood obstacles. Second, its core operations are trustworthy and seldom require additional hardware to implement the advised security measures. The AI-SM-IoT framework is a three-tiered system incorporating security components based on AI motors into every IoT stack that communicates with the network's edge. AI motors were also added as a new transmission layer. This study suggests an AI-based security method for IoT environments (AI-SM-IoT system). This concept was based on the periphery of a network of AI-enabled security components for IoT disaster preparedness. The architecture recommends three main modules: cyber threat searching, intelligent firewalls for online applications, and cybercrime information. Based on the idea of the "cyberspace killing chain," the modules given detect, identify, and continue to identify the stage of an assault life cycle. It describes each long-term security in the suggested framework and demonstrates its usefulness in applications facing various risks. A distinct layer of AI-SM-IoT services is used to deliver artificial intelligence (AI) safety modules to address each risk in the boundaries layer. The architectural freedom from the project's essential regions and comparatively low latency, which offers safety as a service rather than an embedded network edge on the Internet of Things design, contrasted with the system framework's earlier designs. Based on the administration score of the IoT platform, throughput, security, and working time, it evaluated the proposed method

Keywords: Internet of Things; Security; Artificial Intelligence; Fog Computing; Sensors

1. Introduction to safety models

Computer vision and deep learning methods have sped up the development of AI systems to the point that they are commercially accessible and driving innovation in fields as diverse as medicine [1], finance [2], robotics [3],

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

manufacturing [4], commerce [5], the arts [6], and education [7]. Google has been using AI to cure fatal diseases based on a person's genetic makeup and family history. In addition, researchers have begun using AI physicians to prevent and diagnose illnesses. As a result, Technological development has been implemented in companies [8].

The Ministries of Sciences and information communications technology (ICT) said achieving adequate system performance in the respective sector, publishing a dataset setting plan across AI training, and testing data creation issues in many sectors to adopt AI methods [9]. The Government is encouraging "multilateral" video data establishments to enhance the creation of AIs with incorporated mental skills. It enhances AI's capacity to spot risky products, build AI's potential to cure disease, diagnose unusual behaviour in a surrounding area, and collect information from many sectors, including economy, allocation, medicine, and cultural history [10][11].

Current AI has been unable to provide sufficient evidence of the outcomes in supplying data on cognitive decisions and predictions; consequently, explainable AI is required to address the AI constraints limited to passive identification [12]. In 2018, the Defense Advanced Research Projects Agency (DARPA) pushed a comprehensive AI algorithm via the Explainable Artificial Intelligence (XAI) program, with the European Union (EU) as its primary emerging for an Intelligence algorithm by General Information Security Regulations (GISR) [13].

Machine learning is problematic because of the lack of accountability in its functioning, such as the flight recorder in a convolutional neural network [14][15]. Appropriate policies and technologies are necessary to overcome this dependability issue. The testing of the algorithms should particularly be strengthened to adapt daily life AI, like for medical diagnoses and automated vehicles, and the information on the ambiguity of evaluation as a consequence of the actions of the AI must be correctly employed [16]. Technology developments must be implemented for the Intelligent system, and mistakes must be minimized while a framework is adopted to protect against hostile assaults. In hospitals, Artificial Intelligence-based fuzzy-assisted Petri net (AI-FAS) is used to measure stress's effects on vital signs [17].

Intelligence techniques are appropriate for addressing invisible dangers. Various AI approaches for cyberattack searching on the border of the IoT infrastructure have been developed, and better outcomes have been produced to cope with new hazards. Establishing an AI-based safety architecture has been shown to aid in detecting, identifying, and allocating preexisting threats in the network's periphery. Placing a defensive system at the network's edge may reduce the impact of attacks and prevent them from penetrating deeper.

This research contains the following key contributions:

- Propose a safe IoT end-level structure based on various AI elements.
- AI engines are designed to secure the peripheral layer of the IoT context in defensive compounds based on provider architectures.
- heTest t proposed a safety implementation framework based on IoT services based on evaluation measures.

The remaining parts of the study are as follows: Section 2 shows the historical context of the preventative measures. In Section 3, we develop and implement the AI-based security mechanism for the IoT ecosystem that we propose. The software's analysis and performance assessment are shown in Section 4. Section 5 illustrates the conclusion and its future application.

2. In-Depth History of Precautionary Measures

Singh S. et al. [18] proposed the Convergence of blockchain and artificial intelligence in IoT networks for the sustainable smart city. Since IoT devices are utilized in many different contexts, there are now additional security needs for the network's edge where they are deployed. Several crucial reasons for the confluence of Blockchain and AI technologies, which will help establish a sustainable smart society, are discussed in depth in this paper. Solutions for improving blockchain security are discussed, with a brief overview of the most important elements that may be used to create a wide range of AI-powered transportation networks. New security recommendations and future standards for a sustainable smart city ecosystem are also discussed, along with the challenges that remain open and the direction of our future study.

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

Javaid, N et al. [19] proposed Intelligence in IoT-based 5G networks: Opportunities and challenges used. Various options and frames for protecting the Network edge layer were developed to deal with risk occurrence. By a heuristic technique, most of the offered designs can only solve specific safety problems between peripheral results in improved and one IoT framework functioning layer. Major concerns with 5G networks based on the Internet of Things (IoT) include high data rates, low latency, effective use of spectrum, and the coexistence of various network technologies. It will be necessary to use artificial intelligence (AI) to effectively utilize the vast amounts of data produced by the many IoT devices for the above criteria. Artificial intelligence techniques examine the data, identify trends, and interpret the information to guide the end devices.

Despite its impressive reliability, the topology necessitates the usage of external storage devices for applications to ensure the region at the network's periphery. Furthermore, this design cannot handle the security of functioning devices from end to end. A developed a secure topology for SeCNet, establishing a closed canal connecting connections to an instrument [20]. This isolating design also allowed the security of data transfer using a key pair to be preserved. This architecture was demanding regarding resources and did not respond with limited resources [21]. The structure advantages from the innovation TrustZone and divides computer resources into specific areas. To address these issues, the author suggests a system that employs artificial intelligence to ensure the safety of the Internet of Things (AI-SM-IoT) [22].

Proposed Artificial intelligence-based IoT security methodology (AI-SM-IoT)

This section defines the security analysis infrastructure for the network edge of Unified communications in a comprehensive and detailed way. The primary architecture is constructed on a framework with three layers and an all-embracing safety level for the network edge. There are two explanations for adopting a three-layer framework: there are not any single criteria for IoT network, no collective labour structure is available for every architect's layer, and it uses a three-layer design as the primary structuring, which is why the multiple levels of IoT network were more secure than some other existing models (i.e., four-layer structure) in recent projects. Three-layer specifies several security components in the suggested security protocol to provide a robust safety mechanism within the IoT atmosphere's network edge. AI-SM-IoT illustrates the fundamental perspective of the architecture proposed for communication with edge results improved with the various security components for each tier of the IoT ecosystem.

3.**1 Application layer security**

End devices often deal with IoT device apps via HTTP protocol at the protocol stack. The framework is intended for a reduced power draw and a minimal communication overhead for limited bandwidth and excellent traffic resilience. To ensure safe communication links and service providers, it suggests two distinct secure modules: standard application protocol Constrained Application Protocol (CoAP) serves as a kind of HTTP for restricted devices so that devices like embedded sensors interact on Cloud computing, be checked, and share information as a subsystem. CoAP can keep functioning when transmission control protocol (TCP) based technologies cannot be finalized handshake.

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

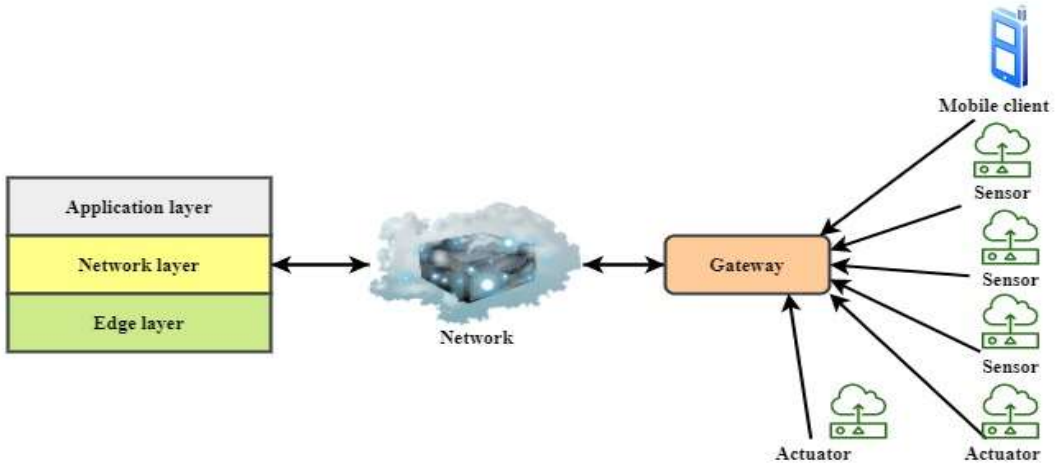


Figure 1: Proposed AI-SM-IoT system architecture

Figure 1 shows the whole architecture of the proposed AI-SM-IoT system. Each layer—the application layer, the network layer, and the edge layer—serves a different purpose. It uses mobile clients, sensors, and actuators. It demonstrates the cheap method for creating secure links between other hosts (edge endpoints) in the applications layer to ensure confidentiality and security. CoAP is a simple text-based protocol such as HTTP but works behind user datagram protocol (UDP) and is recommended. The most frequent encryption is done utilizing the security features of the datagram. An HTTP procedure is used via the rest API for most edge users in IoT settings. An intelligent framework acts in the system security to discover defects in the work order using the Internet protocol using artificial intelligence.

This system maintains that the deployment of edges improves from hackers by setting criteria for web services optimized by the AI engines.

Cyber risk parameter: The origin of attacks is one of the critical difficulties at the application level, and the right decision correlates to a danger. An assailant discovers the source of assaults and makes better judgments depending upon the nature of the attacking campaign by understanding the assailant's techniques, methods, and techniques at this level. The modern example is a profile perfectly matched device in the protocol stack. The subsystem in the protocol stack can allocate to its initial malicious user the fraudulent behaviour on the border layer systems and advises a similar objective against the threat.

3.2 Network layer security

Most dangers are contained in the TCP/IP stack protocols on the network topology. However, operations technologies (OT) standards such as Modbus also function in the network topology in a manufacturing environment. Consequently, the planning and control are given in AI-SM-IoT to have network security comparable to standard TCP/IP communications in this stack: The firewall (FW) depends on the network. Because firewalls are rudimentary network security measures, a rule-based method to restrict abnormal activity on the network level of the IoT ecosystem is needed. Most edge IoT application layer equipment uses the same TCP/IP protocols; thus, it has the same TCP/IP defense system to prevent suspicious network layer queries in the AI-SM-IoT system.

Intrusion-preventing system: This component is therefore included as the technology's security mechanism. The method, in terms of natural means, is employed extensively in the IoT context. It can defend the IoT infrastructure from most risks at the network level of customers on the edge device. The suggested design uses the component advantages of a skilled AI engine under a regular and harmful network pattern. The AI algorithm is taught to use present TCP/IP or existing traffic patterns for training purposes at the network topology of the border directly correlates.

Furthermore, in their activities, the edge-level devices might suffer connection problems due to security problems in their network topology. Denial service (DoS) attacks are brutal to cope with by primary security components like rules-based firewalls and handwriting systems. These are the common significant network

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

security problems on IoT devices. On the other hand, the most complex attacks are managed using knowledge modules such as AI-driven threat research and danger attribution. In this respect, the suggested networking and edge layers AI components construct profiling from the behaviour of gadgets and identify, prevent, and molecules behaviour.

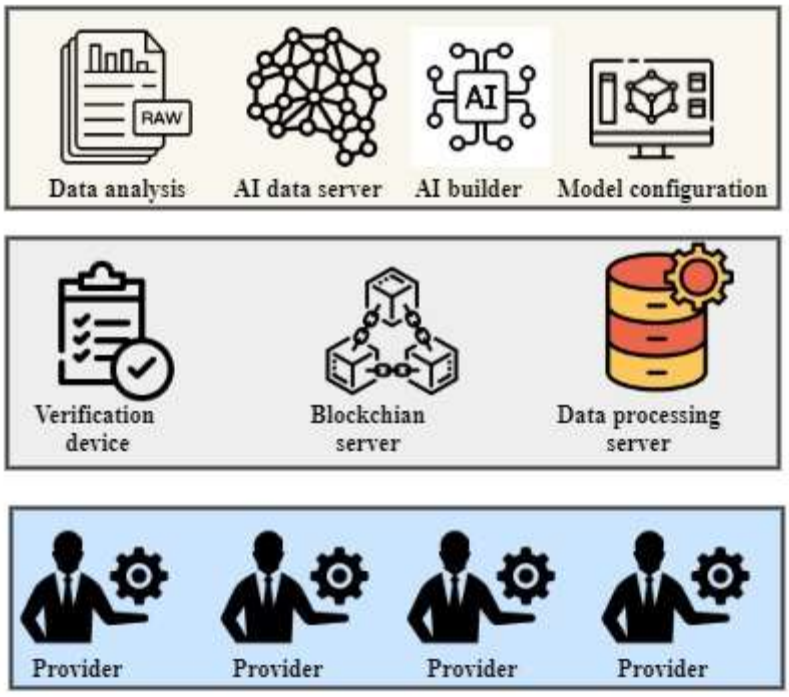


Figure 2: The suggested AI-SM-IoT system's layered architecture

Figure 2 depicts the multi-tiered design of the proposed AI-SM-IoT system. It is constructed on three levels, each with a specific purpose. The first layer includes data analysis, AI data server, AI builder, and model configuration models. The second layer comprises a verification device, blockchain server, and data processing server. The third layer consists of providers.

3.3 Edge layer security

There are several (edge layer) natural end unit standards. However, most menaces focus on edge gates since they significantly harm the IoT ecosystem. For example, in the 2016 Mirai assault, many IoT infrastructures caused massive downtimes. But there are multiple standards. Each device must communicate its acquired data to the backside structure of cloud storage at the infrastructure level. There seem to be three distinct approaches to linking end hardware to the internet-of-things back-end framework: (a) direct cloud connectivity, (b) direct field gateways connectivity, and (c) indirect connectivity via virtual private connections.

Hunting for cybersecurity threats: It concentrates on AI-driven safety modules for the Internet-things gateway because of their essential function in the surroundings. Irrespective of the type of communication between the equipment and its facilitator, the modules are suggested depending on the deployed gateway/device work agent. Threats arise in several respects in the module. For instance, a malicious risk or an alleged traffic pattern (i.e., a cap file) is provided as a pre-processed feature space in consecutive or discontinuous ways.

In other terms, a label of suspicious behaviour is assigned as an abnormality or normal. Abnormalities need further analysis for the present network of points to discover compromise indications. Two steps should be taken if there is any proof on each machine. First, the information is sent to the modules to see what action it needs to take. The next move is to contact the server module to determine the stage of an assault that affected the node.

The intelligence of cybersecurity threats: According to the danger of Cyber Kill Chain (CKC) classification, each hazard has its life cycle. Consequently, it contributes to the optimal judgment on the highest threat phase

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

following the discovery in the intermediate nodes. The modules in the presented work complement the operation behind the assault and provide an overview of the nature and source of the danger in the IoT ecosystem.

Concerning computer resource constraints on connected systems and memory storage in edge-level portals, it is necessary to build defensive measures compactly. There must be two ways to implement an IoT end security protection module. The first method is based on the architectural server side, implying that the AI engines are on top of the structure. The AI modules engine is put on the portals as one of the bridge functions in the second process.

3.4 Mathematical calculation

AI-SM-IoT system's elevated AI system library is one of its critical elements. This element has many classification models, irrespective of the implementation of the IoT infrastructure. With one sort of data, every classifier was trained. For instance, if the edge device has a harmful executable binary file format, the module's engine gateways must link to the learned models using the opcode, bytecode, and systems calling. It isolated this component from the reinforcement cage to stress the usefulness of algorithms on various design sets. It also suggested a new stream component for engine-independent operation. This component should collect, standardize, and convert environmental precept information and feeding motors for ongoing training.

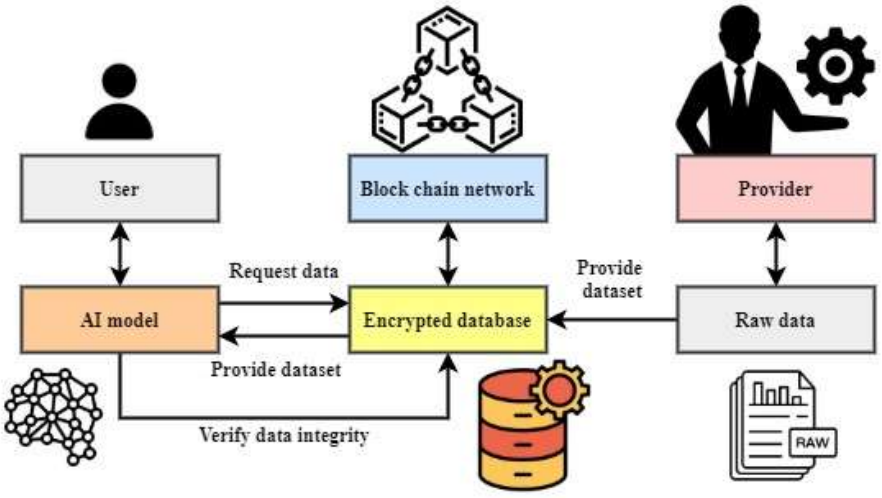


Figure 3: The block diagram of the proposed AI-SM-IoT system

Figure 3 depicts the proposed block diagram of the AI-SM-IoT system. It comprises the user, the AI model, the blockchain, and the supplier. The encrypted database stores and processes the raw data from the user and provider. The decrypted data is accepted from the AI model based on the user's utility. Two deep neural network (DNN) routines are used in the method. The first scheme is applied as downsampling, which results in a reduced sample of the top input. Then it is utilized as a predictor for the second procedure. After a concentrated example of high current density, the encapsulated characteristics are entered as an input to the classification, which classifies the label. The problem is how the downsampler can be trained because there is no goal value; therefore, the conventional workout method does not apply.

In comparison, classification processes are simple, as the goal values for every input sequence are accessible. Three stages are therefore taken to construct and train the entire model. 1) Create the first downsampler v. 2) Construct an original classifier. 3) Adapt downsampler/classifier weights/coefficients.

3.4.1 Down sampler

A DNN is employed as a downsampler v in which the input is X, and the result is negligible. Assume data set B in which the matching class labels. $\{y_1, y_2, \cdots, y_n\}$, the classes are $\{x_1, x_2, \cdots, x_n\}$. The neuronal output on the v input nodes is calculated using equation (1).

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

$$\bar{y}_v = v(x_p) = \alpha\left[\sum_{q=1}^{m} \frac{b_{qr}}{x_q}\right] \quad (1)$$

Where r denotes an input data r^{th} neuron, m is the inputs vector p^{th}dimensions of x_p, pth element/input vector propertyx_p and b_{qr} is the r^{th}input neuron-input weight, and $\alpha(.)$ is the activating characteristic in the input nodes. The information has n neurons because the state vector is n dimensions. The variable amount of neurons specified by the client would constitute several hidden units. The neuron inputs in the layer are the nerve cell outputs in the preceding layer. The result ($\bar{y}_v$) of a neuronal h at the concealed layer is calculated using equation (2)

$$\bar{y}^D{}_v = \alpha\left[\sum_{q=1}^{m} \frac{b^D{}_{qr}}{\bar{y}^{D-1}{}_v}\right] \quad (2)$$

D is the concealed layer, q is the total neural of the coating, $\bar{y}^{D-1}{}_v$It is a neuronal output for layers D−1, and $b^D{}_{qr}$Is the neuron's weight for layer D − 1 to h neuron for layer D. v is used for the importance of layer D.

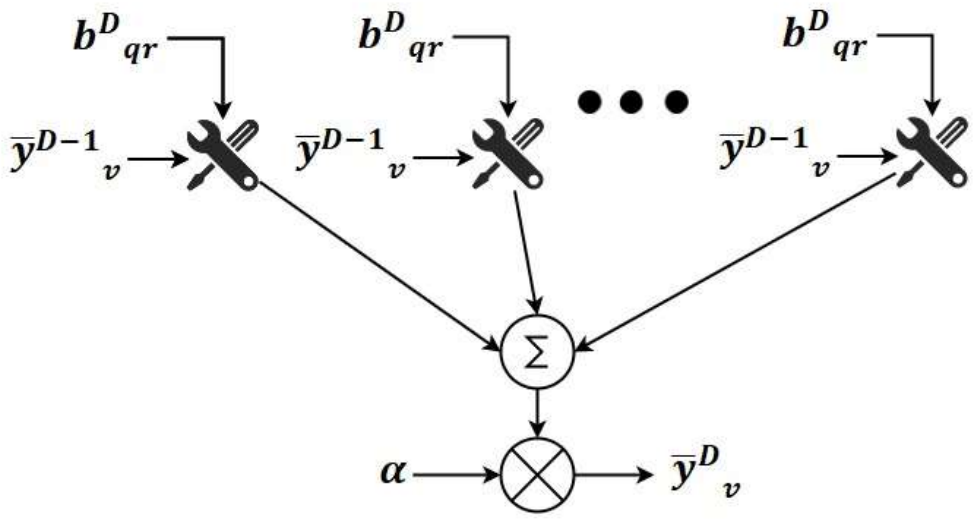


Figure 4. Derivative Diagram of $\bar{y}^D{}_v$

Figure 4 is a graphical illustration of the expression.$\bar{y}^D{}_v$. To determine the$\bar{y}^D{}_v$, it considers the previous iteration's output, the calculation function, and other parameters. The downsampler (DNN) listed in this article is used to design products from high-dimensional input. Initially, the weights associating neurons were produced spontaneously in various layers.

3.4.2. Classifier

DNN is created and utilized as an assault or non-assault to categorize the information as a functional u. The outcome of u is calculated using equation (3) based on the input data vector X_p:

$$\bar{y}_p = u[\bar{y}^p{}_v] = u\left(v(X_p)\right) \quad (3)$$

u is the first layer function. $\bar{y}_p$Does the downsampler v generate the path-input vector output? In short, the Downsampler result is supplied in the classification u. If the dimensions of $v(X_p)$ The input data consists of a total "n" neuron. The outputting layer includes only one neuron to provide a "zero" or "one" result (i.e., nonattack). One or more concealed layers with different neurons can exist.

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

3.4.3. Training the weights of the classifier

The suggested solution has two DNNs: (1) downsampler v and (2) grader u. The concurrent learning of the two DNNs is not conceivable as one DNN result is input for the other outputs, and the outcome value of u is also unknown. The training is therefore carried out as follows.

1) Estimate using randomized weights produced.

2) Bug/loss computation.

3) Due to loss, update classification weights.

4) Bug/loss calculation.

5) Due to loss, downsampler weights were updated.

1) Weight calculation

In the first phase, output weights are produced independently for both samplers and classifiers. Let's connect this stage, denoted by$\bar{y}_s = 1$, to the anticipated result. Equation (4) provides a concise representation of these findings.

$$\bar{y}_s = 1 = \frac{(v \times u)}{n} \quad (4)$$

The downloading function and grading function are denoted $u\ and\ v$. The number of samples is marked n.

2) Computing error: The model is calculated with good binaries cross-entropy functional as outlined in equation (5) by false alarm:

$$D_{s=1} = \frac{1}{x}\sum_{p=1}^{n} \bar{y}_s \log(Pr(\bar{y}_s)) + (1 - \bar{y}_s) \log(Pr(1 - \bar{y}_s)) \quad (5)$$

Where $Pr(\bar{y}_s)$ indicates the likelihood that represents all q, $\bar{y}_s$ It is a nonattack among all q examples, and q is a sample of the entire dataset in information source D.

3) Classification of adjusted weights: After the loss is calculated using equation (5), the loss is replenished to the classifiers to adjust weights to reduce loss and improve classification results using the primary algorithm. The continuity equation is used to adjust weights that link the output value to the hidden state, and it is expressed in equation (6)

$$b_x^y = b_x^y - \beta \left(\frac{v_s}{\sqrt{r_s} - \delta}\right) \frac{dD}{db_x^y} \quad (6)$$

The differential coefficient is written as$\frac{dD}{db_x^y}$. β stands for the categorization function. The symbol for this fundamental operation is b_x^y. The variance is denoted δ. The speed and learning rate of the system is indicated in Equations (7) and (8)

$$v_s = \frac{\mu_1 v_{s-1}}{(1-\mu_1)} \frac{dD}{db_x^y} \quad (7)$$

$$r_s = \frac{\mu_2 r_{s-1}}{(1-\mu_2)} \frac{dD}{db_x^y} \quad (8)$$

β is the scaling function; the user should specify μ_1 and μ_2 model parameters. The differential function is denoted $\frac{dD}{db_x^y}$. The previous speed and learning rate are denoted. v_{s-1} and r_{s-1}. The weights are modified that link the jth of the neurons from hidden neurons to the ith of some other concealed level or inputs layer expressed in Equations (9)

$$b_x^y = b_x^y - \beta \left(\frac{v_s}{\sqrt{r_s} - \delta}\right) \gamma_x \bar{y}_s \quad (9)$$

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

The scaling function is represented by the symbol β, while the basis function is written as b_x^y. The symbol for this variation is δ. Let us designate $\overline{y}_s$ as the target value and γ_x As the output layer function, Equations (10) and (11) represent the system's speed and learning ability.

$$v_s = \frac{\mu_1 v_{s-1}}{(1-\mu_1)} \gamma_x \bar{y}_s \quad (10)$$

$$r_s = \frac{\mu_2 r_{s-1}}{(1-\mu_2)} \gamma_x \bar{y}_s \quad (11)$$

The model parameters are denoted μ_1 and μ_2. It is the function of the output layer γ_x, and $\bar{y}_s$ Is the predicted value considered here to form the equation? The previous speed and learning rate are denoted. v_{s-1} and r_{s-1}. The output layer function is denoted in equation (12)

$$\gamma_x = \frac{\alpha' \left[\sum_{q=1}^{m} \frac{b^D qr}{\bar{y}^{D-1}{}_v} \right]}{\sum_{r=1}^{n} w_{qr}} \quad (12)$$

m is the total layers of neurons, and n is the entire layer of neurons. The downsampler values during this training stage are not adjusted. Weight is represented byw_{qr}, basis function by$b^D{}_{qr}$, and output of the last layer by $\bar{y}^{D-1}{}_v$. During this training step, downsampler values are not adjusted. The adjusted computational function is denoted. α'.

4) Compute error/loss function: The model's mistake must be calculated according to the procedures outlined when the logistic regression is binary cross-entropy after being trained by the classifier.

5) Update downsampler weights: it includes a description of the computer error L model when the values of the classifiers are adjusted, but the downsampler scales have still not been taken. Cells on the convolution layer are accordingly updated to another concealed state or inputting layer for weights linking cells in the output units. It should be mentioned that the mismatch between the forecasted measured and simulated results must be recognized to determine the parameters that link concealed level cells to the output level cells.

Due to the unknown result for the downsampler u, the loss is calculated based on classifiers v and the intended input from the workout data. Steps (1)–(5) are performed for several periods until a predetermined mistake or the maximum number of times is reached. This mistake is transmitted to the output neuron and concealed downsampling layer links to modify the network weights. After the output neuron's values have been fitted to the hidden layer, the hidden layer's values are then adapted to the input nodes. Remember that although downsampler u values are modified, classification v values are not.

This subsection uses IoT models to construct the proposed AI-SM-IoT system. The mathematical model guarantees that the given model is correct. As a whole, the system benefits from the suggested security paradigm. In this part, we assess the effectiveness of the recommended AI-SM-IoT system.

4. Analyzing and assessing software

A Python language (Keras Package) was utilized to conduct the research, and some initial tests with a test and error technique defined the range of network variables. It selected settings concerning the performance measurements that yielded the better effect depending on the outcomes acquired. Internal control and internet flow communications protocols utilize the major attack surface. Assailants can utilize a framework for attacking them. In general, recognition is used to access the networking's virtual network, the domain name server (DNS) servers, the server software, versions of the operating system (OS), and data relevant to the worker. This data is used to discover access points and active applications in the following step and find flaws with the susceptibility library. Edge-IIoTset Cyber Security Dataset of IoT & IIoT dataset is used to get the simulated output at different speeds of packet transmission [33].

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

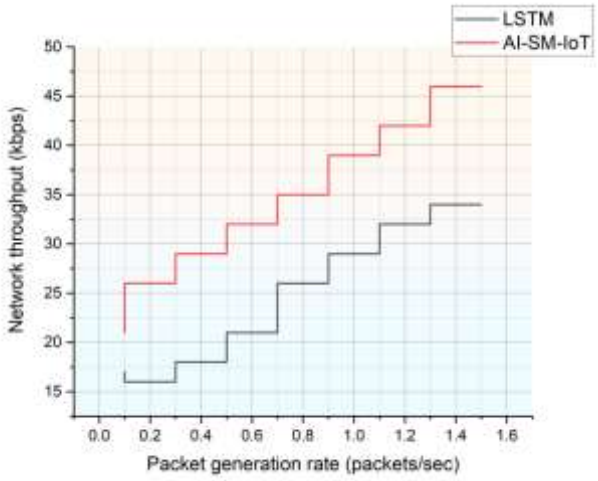


Figure 5(a): Performance evaluation of the proposed AI-SM-IoT network at a reduced data transmission rate

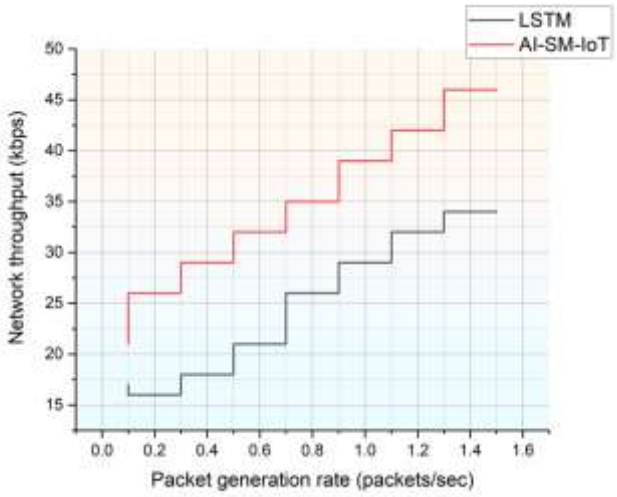


Figure 5(b): An evaluation of the proposed AI-SM-IoT system's network performance at a higher transmission rate

The network throughput analysis of the proposed AI-SM-IoT system is shown in Figures 5(a) and 5(b) for low and high sending rates, respectively. We generate packets at varying rates for the simulation study, from a minimum to a maximum. The effectiveness of the proposed AI-SM-IoT system is simulated and tested at different speeds of packet transmission. The simulation results of the proposed AI-SM-IoT system improve as the rate at which packets are created increases. The suggested AI-SM-IoT system improves its throughput thanks to increased security and decreased processing time.

Table 1: The suggested AI-SM-IoT system's network throughput is analyzed.

Rate of packet production (in packets per second).	LSTM (kbps)	AI-SM-IoT (kbps)	Packet generation rate (1000 packets/sec)	LSTM (kbps)	AI-SM-IoT (kbps)
0.1	17	21	0.1	18	25
0.3	16	26	0.3	23	29
0.5	18	29	0.5	26	32
0.7	21	32	0.7	29	36

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

0.9	26	35	0.9	31	39
1.1	29	39	1.1	35	42
1.3	32	42	1.3	37	46
1.5	34	46	1.5	39	49

The suggested AI-SM-IoT system's network throughput analysis is shown in Table 1. We simulate the proposed AI-SM-IoT system by changing the packet production rate from low to high. Results from the proposed AI-SM-IoT system are compared across several packet sending rates, including low, medium, and high—the proposed AI-SM-IoT system with a higher security level and lower computation complexity. As the packet generation rate increases, the respective network throughput also increases.

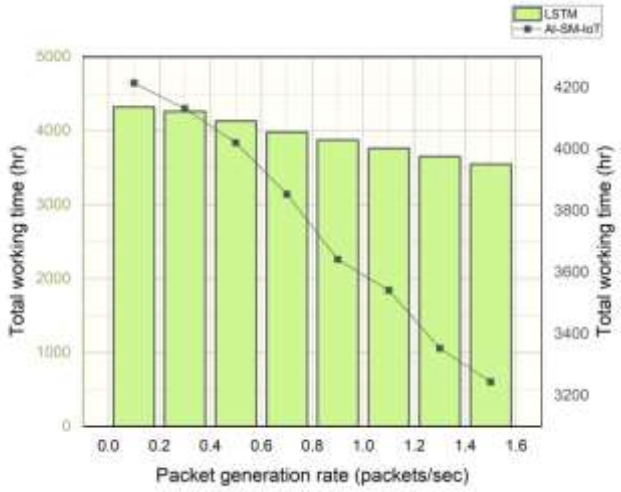
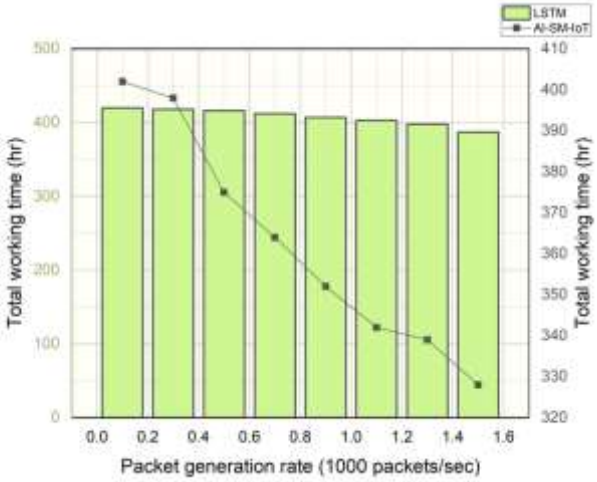


Figure 6(a): Estimating the amount of time it would take to implement the proposed AI-SM-IoT system **with a**



slower packet creation rate

Figure 6(b): Examining how much more quickly packets can be generated in the proposed AI-SM-IoT system

The examination of the AI-SM-IoT system's operating time for low and high packet generation rates is shown in Figures 6(a) and 6(b), respectively. Lower and higher generation rates are two examples of how the packet generation rate may be changed. Different transmitting rates are investigated, and their effects on the simulation results of the proposed AI-SM-IoT system are discussed. The results of the simulation are tracked and shown in several ways. Reduced complexity and an IoT module allow the proposed AI-SM-IoT system to outperform the current LSTM model in less time.

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

Table 2: The suggested AI-SM-IoT system's total working time analysis

Rate of packet production (in packets per second).	LSTM (hr)	AI-SM-IoT (hr)	Packet generation rate (1000 packets/sec)	LSTM (hr)	AI-SM-IoT (hr)
0.1	4321	4215	0.1	420	402
0.3	4261	4132	0.3	418	398
0.5	4132	4021	0.5	416	375
0.7	3982	3854	0.7	412	364
0.9	3876	3642	0.9	407	352
1.1	3765	3542	1.1	403	342
1.3	3654	3354	1.3	398	339
1.5	3548	3245	1.5	387	328

The suggested AI-SM-IoT system's entire working time analysis is shown in Table 2. Simulation results are examined and reported for both low and high packet generation rate settings for the proposed AI-SM-IoT system. Overall system performance is improved by the suggested AI-SM-IoT system's Integration of an Internet of Things module and an AI model. As the packet generation rate increases, the respective system performance decreases because the system requires a minimum level of computation at a lower packet generation rate.

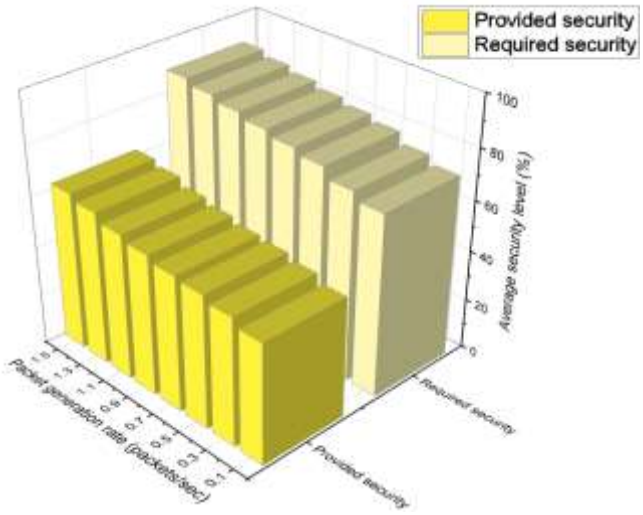


Figure 7(a): Examining the proposed AI-SM-IoT system's security from the perspective of the first packet generation stage

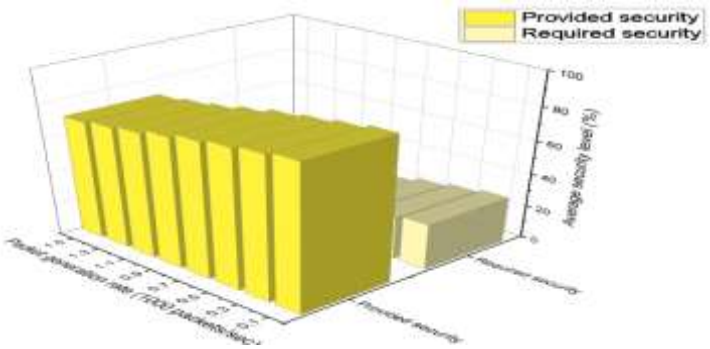


Figure 7(b): Higher-level packet generation security study of the proposed AI-SM-IoT system

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

The suggested AI-SM-IoT system's security level analysis is shown in Figures 7(a) and 7(b) for low and high packet creation rates, respectively. The suggested AI-SM-IoT system's security is evaluated under two scenarios, one in which the packet creation rate is low and the other in which it is high. The results of the simulations demonstrate that the suggested AI-SM-IoT system is more secure than the currently used models. The recommended AI-SM-IoT system uses AI to improve the overall safety of the network.
Here, let us look at the simulation findings for the proposed AI-SM-IoT system and compare them to the results from the current model. Artificial intelligence, an Internet of Things module, and preventive measures are all part of the proposed AI-SM-IoT system, which improves simulation results.

5. Conclusion and future scope

Safety issues are becoming increasingly significant as the Web's infrastructures develop quickly and growth emerges depending on its overall function. Safety and architectural models were presented in the literature again for the IoT end layer. While existing designs can solve specific safety issues in the IoT context, two primary weaknesses occur in most systems. First, it focuses on a single danger on IoT-edge architecture's level without the capacity to address emerging risks and even perceived challenges that it was initially intended to address. Secondly, its fundamental processes are reliable with external hardware requirements to achieve the recommended secure designs in most situations. This study proposes an artificial intelligence–powered security solution tailored to the Internet of Things (AI–SM–IoT). AI-SM-IoT created a three-tier structure with AI motors-based security components for every stack of IoT that interacts with the network edge. It also introduced AI motors as distinct layers and a transmission link. It collects all existing views from danger and makes each view convenient features and functionality to feed AI motors. The freedom of the operations from end system material is an essential benefit of the AI-SM-IoT design by providing an all-embracing AI security feature. The performance can be enhanced by using different classifiers and deep learning algorithms.

References

[1] Oniani, S., Marques, G., Barnovi, S., Pires, I. M., & Bhoi, A. K. (2021). Artificial Intelligence for the Internet of Things and Enhanced Medical Systems. In *Bio-inspired Neurocomputing* (pp. 43-59). Springer, Singapore.

[2] Su, J., Chu, X., & Kadry, S. (2020). Internet-of-Things-Assisted Smart System 4.0 Framework Using Simulated Routing Procedures. *Sustainability*, *12*(15), 6119.

[3] Abd El-Latif, A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., & Venegas-Andraca, S. E. (2020). Secure data encryption based on quantum walks for 5G Internet of Things scenario. *IEEE Transactions on Network and Service Management*, *17*(1), 118-131.

[4] Chakraborty, N., Li, J. Q., Mondal, S., Luo, C., Wang, H., Alazab, M., ... & Pan, Y. (2020). On Designing a Lesser Obtrusive Authentication Protocol to Prevent Machine-Learning-Based Threats in the Internet of Things. *IEEE Internet of Things Journal*, 8(5), 3255-3267.

[5] Jaber, M.M., 2015. Barriers faces telemedicine implementation in the developing countries : toward building iraqi telemedicine framework. ARPN Journal of Engineering and Applied Sciences, 10(4), pp.1562–1567.

[6] Zheng, W., Muthu, B., & Kadry, S. N. (2021). Research on the design of analytical communication and information model for teaching resources with cloud-sharing platform. *Computer Applications in Engineering Education*, *29*(2), 359-369.

[7] Wang, W., Jackson Samuel, R. D., & Hsu, C. H. (2021). Prediction architecture of deep learning assisted short long term neural network for advanced traffic critical prediction system using remote sensing data. *European Journal of Remote Sensing*, *54*(sup2), 65-76.

[8] Rauf, H. T., Gao, J., Almadhor, A., Arif, M., & Nafis, M. T. (2021). Enhanced bat algorithm for COVID-19 short-term forecasting using optimized LSTM. *Soft Computing*, 1-11.

[9] Ali, M.H., Zolkipli, M.F., Mohammed, M.A., and Jaber, M.M., 2017. Enhance of extreme learning machine-genetic algorithm hybrid based on intrusion detection system. Journal of Engineering and Applied Sciences, 12(16).

[10] Amudha, G., & Narayanasamy, P. (2018). Distributed location and trust based replica detection in wireless sensor networks. *Wireless Personal Communications*, 102(4), 3303-3321

[11] Nguyen, T. N., Le, V. V., Chu, S. I., Liu, B. H., & Hsu, Y. C. (2021). Secure Localization Algorithms Against Localization Attacks in Wireless Sensor Networks. *Wireless Personal Communications*, 1-26.

[12] Kumar, P. M., & Seon, H. C. (2021). Internet of things-based digital video intrusion for intelligent monitoring approach. *Arabian Journal for Science and Engineering*, 1-11.

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

[13] Manickam, A., Jiang, J., Zhou, Y., Sagar, A., Soundrapandiyan, R., & Samuel, R. D. J. (2021). Automated pneumonia detection on chest X-ray images: A deep learning approach with different optimizers and transfer learning architectures. *Measurement*, *184*, 109953.
[14] Ali, M.H., Jaber, M.M., Abd, S.K., Rehman, A., Awan, M.J., Vitkutė-Adžgauskienė, D., Damaševičius, R., and Bahaj, S.A., 2022. Harris Hawks Sparse Auto-Encoder Networks for Automatic Speech Recognition System. *Applied Sciences (Switzerland)*, 12(3).
[15] Amudha, G. (2021). Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions. *Wireless Personal Communications*, 1-21.
[16] Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*, 123, 1-13.
[17] Hussein, A.F., ALZubaidi, A.K., Habash, Q.A., and Jaber, M.M., 2019. An adaptive biomedical data managing scheme based on the blockchain technique. *Applied Sciences (Switzerland)*, 9(12).
[18] Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society*, *63*, 102364.
[19] Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. *IEEE Communications Magazine*, *56*(10), 94-100.
[20] Mao, B., Kawamoto, Y., & Kato, N. (2020). AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things. *IEEE Internet of Things Journal*, *7*(8), 7032-7042.
[21] Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: an architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, *15*(4), 565-584.
[22] Mukherjee, A., Goswami, P., Yang, L., Tyagi, S. K. S., Samal, U. C., & Mohapatra, S. K. (2020). A deep neural network-based clustering technique for secure IIoT. *Neural Computing and Applications*, *32*(20), 16109-16117.
[23] Vimal, S., Khari, M., Crespo, R. G., Kalaivani, L., Dey, N., & Kaliappan, M. (2020). Energy enhancement using Multiobjective Ant colony optimization with Double Q learning algorithm for IoT-based cognitive radio networks. *Computer Communications*, *154*, 481-490.
[24] Alqaralleh, B. A., Vaiyapuri, T., Parvathy, V. S., Gupta, D., Khanna, A., & Shankar, K. (2021). Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Personal and Ubiquitous Computing*, 1-11.
[25] Jamal, A. A., Majid, A. A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2021). A review on security analysis of cyber-physical systems using Machine learning. *Materials Today: Proceedings*.
[26] Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing*, *13*(2), 241-251.
[27] Aldhaheri, S., Alghazzawi, D., Cheng, L., Barnawi, A., & Alzahrani, B. A. (2020). Artificial Immune Systems approaches to secure the Internet of things: A systematic review of the literature and recommendations for future research. *Journal of Network and Computer Applications*, *157*, 102537.
[28] Poniszewska-Maranda, A., Kaczmarek, D., Kryvinska, N., & Xhafa, F. (2019). Studying usability of AI in the IoT systems/paradigm through embedding NN techniques into mobile smart service systems. *Computing*, *101*(11), 1661-1685.
[29] Zaidan, A. A., & Zaidan, B. B. (2020). A review on the intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artificial Intelligence Review*, *53*(1), 141-165.
[30] Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2021). A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4112.
[31] Sultana, T., & Wahid, K. A. (2019). IoT-guard: Event-driven fog-based video surveillance system for real-time security management. *IEEE Access*, *7*, 134881-134894.
[32] Li, D., Deng, L., Liu, W., & Su, Q. (2020). Improving communication precision of IoT through behavior-based learning in a smart city environment. *Future Generation* Computer Systems, 108, 512-520.
[33] Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access, 10, 40281-40306.

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023

[34] Saeed, V. A. (2024). A Framework for Recognition of Facial Expression Using HOG Features. International Journal of Mathematics, Statistics, and Computer Science, 2, 1–8. https://doi.org/10.59543/ijmscs.v2i.7815

[35] Mohammed, M.A., Lakhan, A., Abdulkareem, K.H., Zebari, D.A., Nedoma, J., Martnek, R., Kadry, S. and Garcia-Zapirain, B., 2023. Homomorphic federated learning schemes enabled pedestrian and vehicle detection system. *Internet of Things*, p.100903.

[36] Dinçer, H. Yüksel, S. & Eti, S.(2023). Identifying the Right Policies for Increasing the Efficiency of the Renewable Energy Transition With a Novel Fuzzy Decision-Making Model. Journal of Soft Computing and Decision Analytics, 1(1), 50-62. https://doi.org/10.31181/jscda1120234

Doi: https://doi.org/10.54216/FPA.130112
Received: April 05, 2023 Revised: June 26, 2023 Accepted: September 08, 2023