UDC 004
DOI: 10.15587/1729-4061.2022.269221

MANAGING SECURITY IN IOT BY APPLYING THE DEEP NEURAL NETWORK-BASED SECURITY FRAMEWORK

Nabeel Mahdy Haddad
PhD, Lecturer
Collage of Education
Misan University
Amarah, Iraq, 00964

Hayder Sabah Salih
PhD, Director/Head of the Scientific Affairs Section
Department of Private Education
Iraqi Ministry of Higher Education and Scientific Research
Baghdad, Iraq, 10024

Ban Salman Shukur
PhD, Lecturer
Department of Computer Science
Baghdad College
Economic Sciences University
Baghdad, Iraq

Sura Khalil Abd
Corresponding author
Doctor of Network and Communication Systems Engineering
Department of Computer Science and Information Technology
Universiti Tenaga Nasional
Jalan Ikram-Uniten, Kajang, Selangor, Malaysia, 43000
Department of Computer Engineering Techniques
Dijlah University College
Massafi str., Doura, Baghdad, Iraq, 10021
E-mail: sura.khalil@gmail.com

Mohammed Hasan Ali
PhD, Lecturer
Department of Computer Systems and Software Engineering
Imam Ja'afar Al-Sadiq University
Baghdad H.w., Najaf, Iraq, 16012

Rami Qais Malik
PhD, Lecturer
Department of Medical Instrumentation Techniques Engineering
Al-Mustaqbal University College
Hila, Babylon, Iraq, 10041

Security issues and Internet of Things (IoT) risks in several areas are growing steadily with the increased usage of IoT. The systems have developed weaknesses in computer and memory constraints in most IoT operating systems. IoT devices typically cannot operate complicated defense measures because of their poor processing capabilities. A shortage of IoT ecosystems is the most critical impediment to developing a secured IoT device. In addition, security issues create several problems, such as data access control, attacks, vulnerabilities, and privacy protection issues. These security issues lead to affect the originality of the data that cause to affects the data analysis. This research proposes an AI-based security method for the IoT environment (AI-SM-IoT) system to overcome security problems in IoT. This design was based on the edge of the network of AI-enabled security components for IoT emergency preparedness. The modules presented detect, identify and continue to identify the phase of an assault life span based on the concept of the cyberspace killing chain. It outlines each long-term security in the proposed framework and proves its effectiveness in practical applications across diverse threats. In addition, each risk in the borders layer is dealt with by integrating artificial intelligence (AI) safety modules into a separate layer of AI-SM-IoT delivered by services. It contrasted the system framework with the previous designs. It described the architectural freedom from the base areas of the project and its relatively low latency, which provides safety as a service rather than an embedded network edge on the internet-of-things design. It assessed the proposed design based on the administration score of the IoT platform, throughput, security, and working time

Keywords: Internet of things, security, artificial intelligence, fog computing, wireless sensors, security threats

Received date 03.10.2022
Accepted date 07.12.2022
Published date 30.12.2022

How to Cite: *Haddad, N. M., Salih, H. S., Shukur, B. S., Abd, S. K., Ali, M. H., Malik, R. Q. (2022). Managing security in iot by applying the deep neural network-based security framework. Eastern-European Journal of Enterprise Technologies, 6 (9 (120)), 38–50. doi: https://doi.org/10.15587/1729-4061.2022.269221*

1. Introduction

AI systems have been rapidly developed through computer vision and profound learning techniques in such a way as to be available on the market and drive innovations in different areas such as medical [1], financial [2], robotics [3], manufacturing [4], marketing [5], education [6], etc. Google has been working with genetic information and ancestry to treat terminal illnesses through AI to prolong the life expectancy of individuals [7]. In addition, scholars implemented AI doctors for illness control and diagnosis. As a result, Technological development has been implemented in companies [8].

The Ministries of Sciences and Information Communications Technology (ICT) said that achieving adequate system performance in the respective sector and 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 behavior in a surrounding area, and collect information from many sectors, including economy, allocation, medicine, and cultural history [10, 11].

In providing information on cognitive choices, and forecasts, the current AI has been unable to offer adequate proof of the outcomes; thus, explainable AI is necessary to solve the AI constraints confined to passive identification [12]. The European Union's main emerging for an Intelligence algorithm by the General Information Security Regulations (GISR) and pushed in 2018 a comprehensive AI algorithm via the XAI program, the Defence Advanced Research Programs Agency (DARPA) [13].

Machine learning is problematic because of the lack of accountability, 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 [17].

The mathematical model has guaranteed security precision on using AI based security method. The suggested security paradigm improves the efficiency of the whole system. Network Packet Delivery Rate Analysis, Delay Analysis, and Security Analysis are used to evaluate the results of the proposed AI-SM-IoT system. The entire system throughput is improved by the suggested AI-SM-IoT system, which has increased security and decreased process time. The vast majority of edge IoT layer equipment employs the same TCP/IP protocols; thus, it employs the same TCP/IP defensive mechanism to avoid suspicious network layer inquiries in the AI-SM-IoT system. The typical characteristics and capabilities and TCP/IP are used in this procedure (TCP). These protocols are essential for the safety of sensitive information in the IoT. The AI-SM-IoT procedure increased network security across all packet levels by 93.5 %. Raise the bar for data protection everywhere. Every user's actions are constantly being analyzed in an IoT setting. Learning and network parameter update procedures examine the user request and its associated parameters.

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 dangers. Efforts demonstrate that establishing AI-based safety architecture helps detect, identify and allocate existing hazards at the network's edge. It can minimize the spread of assaults or avoid their penetration to other levels by using a defense system on the network edge.

2. Literature review and problem statement

New security requirements have arisen at the network edge of IoT settings as IoT devices are used in various applications [18]. Various options and frames for protecting the Network edge layer were developed to deal with risk occurrence. By a heuristic technique, most offered designs can only solve certain safety problems between peripheral results in improved and one IoT framework functioning layer [19]. Even though the existing systems manage data security, the system's sustainability must be considered, which is a major problem.

The authors in [20] developed a Random Forest-based Ransomware Model. The classifier was tested and evaluated using the system Application Programming Interface (API) bundle data. While the suggested model performed successfully, it only depended on static testing to achieve features. With malware-humping tactics, this might fail. The authors proposed a detection algorithm for a network-driven ransomware assault. They used several methods for the training data to categorize the facts gathered. However, the system requires privacy protection techniques to manage access control in the IoT environment. The simulation outcomes show that the proposal can offer a satisfying security defense for diverse services and regulate security protection to evade energy fatigue, thereby enhancing working time and throughput. It must be distinguished that energy consumption is a long-term progression. At the same time, the forecast of harvesting power was restricted in a short time, which can be observed as an energy-aware cycle.

In [21], the paper presented a multifunctional detection approach for locky malware discovery. The suggested model used the data for the system and control links of the malware, and the information was collected at both packets and stream levels. The trials showed better performance in precision in the selection tree. The methodology suggested showed its efficacy in accurately detecting ransomware assaults. Even though the system successfully identifies the malware, the system's effectiveness needs additional effort to select the tree header. Through the integration of IoT and Social Technologies, and with a focus on Security and Privacy concerns, this study has identified the abstract-level architecture for the digital transformation of organizations. Due to their limited security and emphasis on a single operating function, legacy devices pose a significant threat to the growing paradigm of everything being linked to everything else or the internet of everything.

Different detection algorithms have been developed based on in-depth learning [22]. For example, the study introduced a Deep Neural Network (DNN) based detection algorithm. The suggested model was trained and evaluated with data from Hypertext Transfer Protocol (HTTP) protocols describing cyberattack communication links. The findings indicated that the model suggested they could identify malware with 93.9 percent accuracy. The Long Short Term Memory (LSTM) classifier was used to identify ransomware assaults identically. During this process, the LSTM requires the optimization procedure to reduce the deviations between the malware prediction output. Compared to conventional approaches, the suggested model balances the network's energy consumption and streamlines the computational complexity. The power allocation policy for dynamic clustering utilizes limited area restricted along with few nodes.

The authors [23] found an effective solution for classifying API call-based data. In the study, the scientists used LSTM to use ransomware computing patterns. This model performed higher than the original LSTM. While the techniques mentioned above had shown decent results in malware detection, the identification had to be improved. The article presented an LSTM, Convolutional Neural Networks (CNN), and One-Class Gradient Boosting Machines (OCGM) malware detection algorithm. This work fails to concentrate on the weakest features in the malware analysis that causes to minimize the prediction rate. In contrast to the artificial bee colony and the genetic algorithm, the simulation tests demonstrate how the throughput, longevity, and jamming prediction are studied and how this improves the energy. The algorithm has some potential downsides, such as dealing with the residual energy, but these can be mitigated using powerful computational servers to manipulate the data.

In [24] presented secure IoT services that were an essential part of the IoT project for the edge layer in the medical environment. LSTM and CNN were employed for binary categorization since LSTM performed the greatest to vector a series of application actions into a vector supplied to determine the malware family. The suggested model showed substantial efficiency. It was quite sophisticated in pre-processing and information classification, which might impact identifying malware earlier. The provided model undergoes a thorough experimental validation to identify the analysis of ideal outcomes, and the findings are then looked at from many angles. Grasshoppers living in greater isolation have little chance of successfully creating a diverse solid energy with the resources they have at their disposal.

The model [25] addressed the peripheral layer authenticating gadgets in the Internet protocol stack. The suggested approach offered privacy and security between the network edge and the IoT gateway application server. Using machine learning, this work offers some useful insights into CPS security. It lays the path for further research and actualizes a full security architecture to safeguard CPS against cyberattacks both within and outside the system. The study shows, however, that ML approaches are crucial because of the massive amounts of data that need to be processed to identify different types of attacks. In [26] proposed a provider architecture as the gateway IoT environment for intelligent transport systems. Their design was based on the Diffie–Hellman curves and digital certificates technique for important data transfer purposes. Both security and performance analyses show that the approach is more secure. However, the constraints of the vast majority of IoT devices are not accurately reflected in this design. It employs the central authentication hub while providing a decentralized security architecture for the Internet of Things (IoT) based on blockchain's distributed ledger capabilities.

In [27] suggested the internet-of-things end-to-end mobile security module at the network edge of the smart energy domain. This design offered a strong service framework, but its operating area was restricted to the application level. The design protected edges-level nodes against active attacks caused by end-to-end encrypting and listening during communications when interactions with edge-level devices and a core network of the internet of things. The outcomes have shown that the desirable properties of an Artificial Immune System (AIS) make them a convincing selection for dealing with dynamic ecosystems like IoT. Yet, there is a lack of experimental studies for IoT, making it challenging to draw sufficient conclusions.

In [28] suggested a safe conceptual model with two alternative designs for the commercial use of IoT. The first secured design consists of three layers for the Future IoT level, and the next is a five-layer autonomous structure to deal with typical IoT security flaws. Many techniques were developed for the safety of the edge layer, based instead of giving a higher architectural feature on a specific implemented security feature. For ARM-based gadgets within the IoT ecosystem edge layers. Experimental results validated the viability of incorporating neural network methods into the IoT architecture. A user database is the foundation of this system, thus only approved devices will be supported.

In [29] suggested an architecture of trusted areas to interact which other devices their design. The structure was an extremely reliable device that caused a wide variety of network edges. It required external storage devices for applications to provide a confidence area for the network edge. Furthermore, this design cannot handle the security of functioning devices from end to end. Afterwards, the important aspects of this developing approach were identified in the inspiration of intelligent process utilization for IoT-based intelligent home applications and open-issue restriction usage. It is impossible to avoid dealing with discrete amounts, and a serious loss of information may result from collecting only a small sample size.

In [30], developed a secure topology for SeCNet, establishing a secure canal connecting connections to a device. This isolating design also preserved data transfer security using a key pair. This architecture was demanding resources and did not respond accordingly with limited resources. The findings verify that the proposed framework outperforms some of the most cutting-edge methods for discovering unusual attacks. Using random forests and 10 features from the BoT-IoT dataset, the suggested framework obtained a detection rate of up to 99.99 %. It has been found that the proposed model has a few constraints and obstacles, such as the difficulty of creating a cluster node for interplanetary file systems in a blockchain-IoT network. Second, integrating an intrusion detection system with intelligent contracts for use in fog nodes in real-time has its own set of challenges.

In [31] had put forward a cloud security application infrastructure. Their architecture benefits from virtualization and trustworthy computing to create a safe workplace for edge implies. The ideas' effectiveness was considered on the processor power and can only solve a few particular risks to edge-level electronics. For ARM-enabled Smart ecosystem data processing. The results demonstrate better performance by the suggested system in terms of scalability, resource efficiency, and agility over conventional IoT surveillance systems and other methods. On the other hand, an edge device (terminal/end) tends to be limited to computing at the edge of the network.

In [32] suggested a secure structure called TrustShadow. The structure advantages of the innovation TrustZone divide computer resources into specific areas. By reducing response loss and choosing untrustworthy devices less often, the suggested scheme's performance must strike a balance between users' security and resource usage needs. Distributed computing environments do not enhance the scalability of such applications.

Based on the survey, there are several problems with existing methods, such as network delay, less packet delivery ratio, and data security. Hence, an AI-based security method for IoT environment (AI-SM-IoT) system is suggested to overcome security problems in IoT networks.

3. The aim and objectives of the study

The aim of the study is to design a secure terminal level of the Internet of Things (IoT) using different forms of artificial intelligence – AI engines are made to protect the IoT's periphery by enclosing it in protective compounds using provider designs. The (AI-SM-IoT) system is proposed as a viable solution to the security issues in IoT networks practically by means of Network Packet Delivery Rate, Delay Analysis, and Enhancing General Data Security.

To achieve this aim, the following objectives are accomplished:

– to improve the packet delivery rate by taking advantage of the killing chain with a greater level of security and less computational complexity;

– to reduce the network delay while transferring and accessing the information using a down sampler along with a deep classifier improves overall system efficiency;

– to control data security utilizing the blockchain encryption model and the killing chain.

4. Materials and methods

4. 1. Object and hypothesis of the study

This research contains the key contributions:

– propose a safe IoT end-level structure based on various AI elements;

– artificial Intelligence engines are designed to secure the peripheral layer of the IoT context in defensive compounds based on provider architectures;

– test the proposed safety implementation framework based on IoT services and evaluation measures.

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 an IoT network, no collective labor 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. It specifies several security components in the suggested security protocol to provide a robust safety mechanism within the IoT atmosphere's network edge. It illustrates the basic perspective of the architecture proposed for communication with edge results improved with the various security components for each tier of the IoT ecosystem. As a result, botnet attacks against the internet of things are very common. Malicious bots and malware are distributed over botnets, which are collections of compromised machines. IoT networks are vulnerable to botnet intrusion, which may compromise financial and personal security by installing ransomware, spyware, or other types of malware on otherwise secure devices. One typical method of exploiting IoT devices is to tamper with their firmware, which may cause data loss or corruption. Confidential information was stolen from us. Data theft is another prevalent IoT security concern, often perpetrated to obtain access to sensitive personal or financial data.

4. 2. 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 serves as a kind of HTTP for restricted devices so that devices like embedded sensors interact on Cloud computing, be checked, and shared information as a subsystem. Constrained Application Protocol can keep functioning when transmission control protocol (TCP) based technologies cannot be finalized. The end-to-end architecture of the proposed AI-SM-IoT system is depicted in Fig. 1.

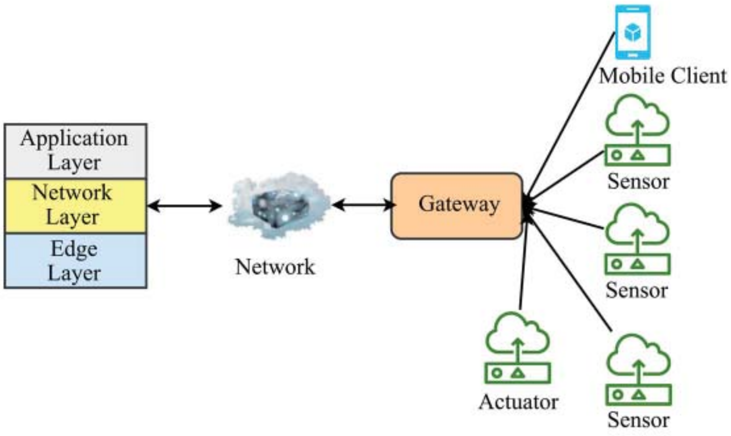


Fig. 1. The end-to-end architecture of the proposed AI-SM-IoT system

Fig. 1 illustrates the end-to-end architecture of the introduced AI-SM process. It has three layers: application, network, and edge later. It uses mobile clients, sensors, and actuators. It demonstrates the cheap method for creating secure links between different hosts (edge endpoints) in the applications layer to ensure confidentiality and security. Constrained Application Protocol 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. A smart 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 key 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 behavior on the border layer systems and advises a similar objective against the threat.

4. 3. Network layer security

Most dangers are contained in the TCP/IP stack protocols on the network topology. However, Operations Technologies (OT) standards such as Mudbus 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 normal 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 included as the technology's security mechanism. The system, in terms of actual mechanisms, is employed extensively in the IoT context. It can defend the IoT infrastructure from most of the 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 current TCP/IP or existing traffic patterns for training 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 tough to cope with by primary security components like rules-based firewalls and even handwriting systems. These are the common significant network security problem 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 behavior of gadgets and identify, prevent, and molecules behavior. The layered architecture of the proposed AI-SM-IoT system is denoted in Fig. 2. It has three layers, and the function of each layer is given below.

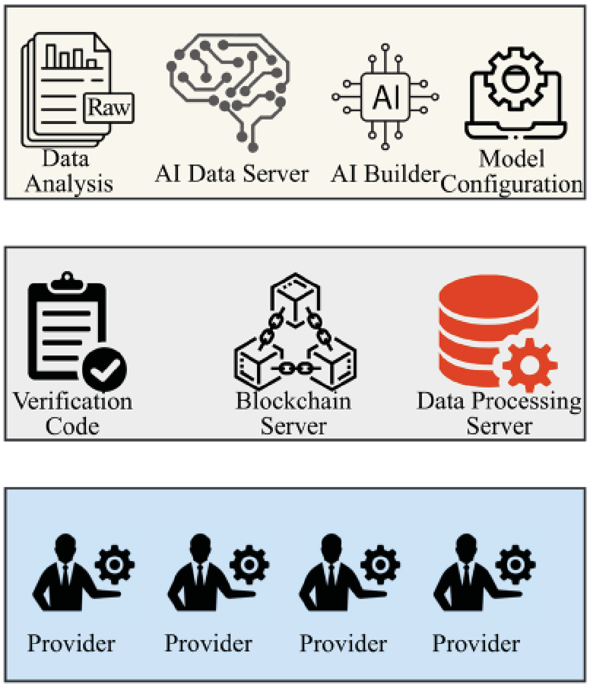


Fig. 2. The layered architecture of the proposed AI-SM-IoT system

The first layer includes data analysis, AI data server, AI builder, and model configuration models. The second layer consists of a verification device, blockchain server, and data processing server. The third layer consists of providers.

4. 4. Edge layer security

There are several (edge layer) real 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 of 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 Packet Capture (PCAP) file) is provided as a pre-processed feature space in consecutive or discontinuous ways.

In other words, a suspicious behavior label is labeled as an abnormality or normal. Abnormalities need to be analyzed further 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 danger has its life cycle. Consequently, it contributes to the optimal judgment on the highest threat phase 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 different 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 placed on the portals as one of the bridge functions in the second process.

4. 5. Mathematical calculation

AI-SM-IoT system's elevated AI system library is one of its critical elements. There are many classification models in this element, 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 called. 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. The block diagram of the proposed AI-SM-IoT system is shown in Fig. 3.

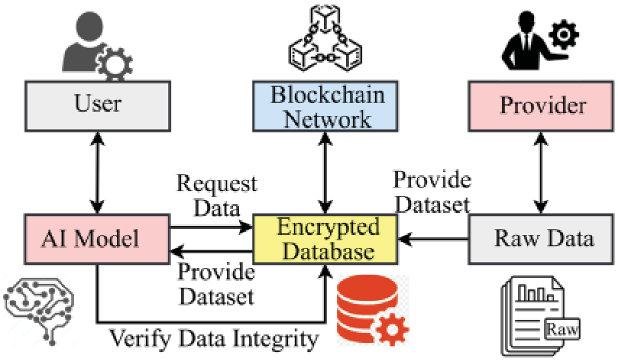


Fig. 3. The block diagram of the proposed AI-SM-IoT system

The block diagram has user, AI model, blockchain, and provider units. The encrypted database stores and processes the raw data from the user and provider. Two Deep Neural Networks (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 reduced model of high current density, the encapsulated characteristics are entered as an input to the classification, classifying the label. The problem that's 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.

4. 5. 1. Down sampler

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

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

where r denotes an input data r-th neuron, m is the inputs vector p-th dimensions of x_p, pth element/input vector property x_p and b_{qr} is the input r-th-neuron-input weight. The input has n neurons because the state vector is n dimensions. The number 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 (2)

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

where D is the concealed layer, q is the total neural of the layer, $\bar{y}_v^{D-1}$ is a neuronal output for layer D−1, and b_{qr}^D is the neuron's weight for layer D−1 to h neuron for layer D. v is used for the weight of layer D. The pictorial representation of is depicted in Fig. 4.

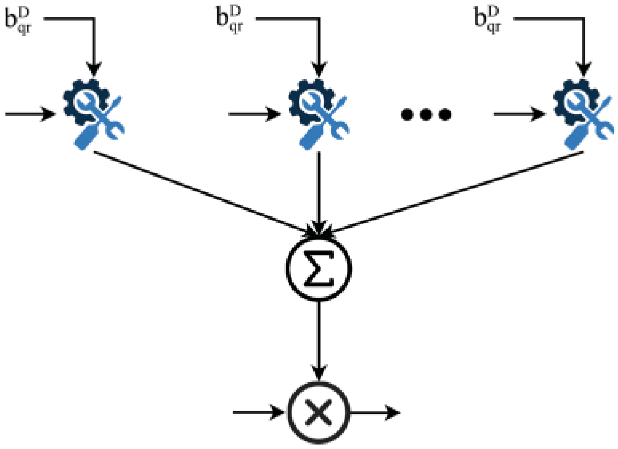


Fig. 4. Derivative Diagram of $\bar{y}_v^D$

It uses previous iteration results, calculation function, and other dependent factors to calculate the $\bar{y}_v^D$. The down sampler listed in this article is used to design products from high-dimensional input. Initially, the weights associating neurons were produced spontaneously in various layers.

4. 5. 2. Deep Learning 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 (3) based on the input data vector X_p

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

where u is the first layer function. $\bar{y}_p$ does the downsampler v. The Downsampler result generate the p-th-input vector output is supplied in the classification u. If the dimensions of $v(X_p)$ is the input data consists of a total of "n" neurons. 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.

4. 5. 3. Classifier weight training

The suggested solution has two DNNs:

1) downsampler v;
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.

The DNN classifier contains neuron layers that utilize the rectified linear unit (ReLU) activation function. The output layer depends on the softmax and cost function, which is observed as cross-entropy. Weight is the parameter within neural networks that converts input data within the DNN network's hidden layers. A neural network is a sequence of nodes or neurons. The neuron's signal intensity is measured in terms of these weights. The number chosen here will establish how much weight the input data has in determining the final output. Biases provide new, entirely positive features to a neural network that were not there before. That additional data is crucial for the neural network's forward propagating effectiveness:

1. Weight calculation.

In the first phase, output weights are produced independently for both samplers and classifiers. Now let's relate to this phase as $\overline{y}_s = 1$ to the output forecast. These results are expressed as the summarizing (4)

$$\overline{y}_s = 1 = \frac{(v \times u)}{n}. \tag{4}$$

The downloading function and grading function are denoted *u* and *v*. The number of samples is denoted *n*.

2. Computing error.

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

$$D_{s=1} = \frac{1}{x}\sum_{p=1}^{n}\overline{y}_s \log\left(Pr\left(\overline{y}_s\right)\right) + \left(1-\overline{y}_s\right)\log\left(Pr\left(1-\overline{y}_s\right)\right), \tag{5}$$

where $Pr\left(\overline{y}_s\right)$ indicates the likelihood that represents all *q*, $\overline{y}_s$ is 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 (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 (6)

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

The differential factor is denoted in $\frac{dD}{db_x^y}$. The classification function is denoted β. The basis function is denoted b_x^y. The variance is denoted δ. The speed and learning rate of the system is represented in (7), (8)

$$v_s = \frac{\mu_1 v_{s-1}}{\left(1-\mu_1\right)}\frac{dD}{db_x^y}. \tag{7}$$

$$r_s = \frac{\mu_2 r_{s-1}}{\left(1-\mu_2\right)}\frac{dD}{db_x^y}. \tag{8}$$

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 j-th of the neurons from hidden neurons to the i-th of some other concealed level or inputs layer is expressed in (9):

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

The basis function is denoted b_x^y and the scaling function is denoted β. The variance is denoted δ. The output layer function is denoted γ_x and the expected output is denoted $\hat{y}_s$. The speed and learning rate of the system is denoted in (10), (11)

$$v_s = \frac{\mu_1 v_{s-1}}{\left(1-\mu_1\right)}\gamma_x \overline{y}_s, \tag{10}$$

$$r_s = \frac{\mu_2 r_{s-1}}{\left(1-\mu_2\right)}\gamma_x \overline{y}_s. \tag{11}$$

The model parameters are denoted μ_1 and μ_2. The output layer function is denoted γ_x and the expected output is denoted $\overline{y}_s$. The previous speed and learning rate are denoted v_{s-1} and r_{s-1}. The output layer function is denoted in (12)

$$\gamma_x = \frac{\alpha'\left[\sum_{q=1}^{m}\frac{b_{qr}^D}{\overline{y}_v^{D-1}}\right]}{\sum_{r=1}^{n} w_{qr}}, \tag{12}$$

where *m* is the total layers of neurons, and n is the full layer of neurons. The downsampler values during this training stage are not adjusted. The weight factor is denoted w_{qr}. The basis function is denoted b_{qr}^D, and the output of the last layer is denoted $\overline{y}_v^{D-1}$. 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 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 outputs 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 values of the output neuron are fitted to the concealed layer, the importance of the concealed layer is adapted/updated to the input nodes. Note that classification v values are not adjusted, but the downsampler u values are adjusted.

The proposed AI-SM-IoT system is designed in this section with IoT models. The mathematical model assures the accuracy of the proposed model. The proposed security model enhances the overall system effectiveness. The proposed AI-SM-IoT system outcomes are evaluated in the upcoming section.

5. Results of research AI-based security method for IoT environment (AI-SM-IoT) system

5. 1. Network packet delivery rate analysis

MATLAB software has thousands of features that may be used to create IoT applications, such as signal and image processing, predictive maintenance, feedback, supervisory control, machine learning, and optimization. This study utilized the cyber security dataset of [33]. 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. This work proposes a novel, centralized, decentralized, deep learning-based intrusion detection system that can employ IoT applications' realistic cyber security dataset. Specifically, the suggested testbed consists of seven layers: network functions virtualization, cloud computing, fog computing, blockchain network, edge computing, software-defined networking, the internet of things, and perception. OPNFV platform, Things Board IoT platform, Digital twin, Hyperledger Sawtooth, Mosquitto MQTT brokers, ONOS SDN controller, Modbus TCP/IP, ..., etc. are all examples of new technologies appearing at various layers to meet the essential needs of IoT applications. More than ten distinct types of IoT devices (including low-cost digital sensors for sensing humidity and temperature, an ultrasonic sensor for detecting water levels, a pH sensor meter for measuring a heart rate sensor, soil moisture, a flame detector, and so on) contribute to the data that make up the Internet of Things. This research identifies and analyses fourteen assaults against IoT and IIoT communication protocols, broken down into five categories: denial-of-service/distributed denial-of-service, information gathering, a man in the middle, injection, and malware. This research offers an initial exploratory data analysis and assesses the effectiveness of deep learning modes after processing and examining the provided realistic cyber security datasets. During this process, a software development toolkit is utilized to implement the discussed AI-based security method in an IoT environment. It selected settings concerning the performance measurements that yielded a better effect depending on the outcomes acquired. The primary attack surface is utilized in internal control and work order flow communications protocols. Assailants can use a framework to attack them. In general, recognition is used to access the networking's virtual network, the domain name server (DNS) servers, the server software, operating system versions (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. Fig. 5, *a*, *b* show the network throughput analysis of the proposed AI-SM-IoT system with lower and higher sending rates, respectively.

The packet generation rate varies from a minimum to a maximum level for the simulation analysis. The simulation outcomes of the proposed AI-SM-IoT system are evaluated over the different packet-sending rates. As the packet-generated rate increases, the proposed AI-SM-IoT system's respective simulation outcomes also increase. The proposed AI-SM-IoT system with higher safety and lower processing time enhances the system's overall throughput. Table 1 shows the network throughput analysis of the proposed AI-SM-IoT system.

Table 1

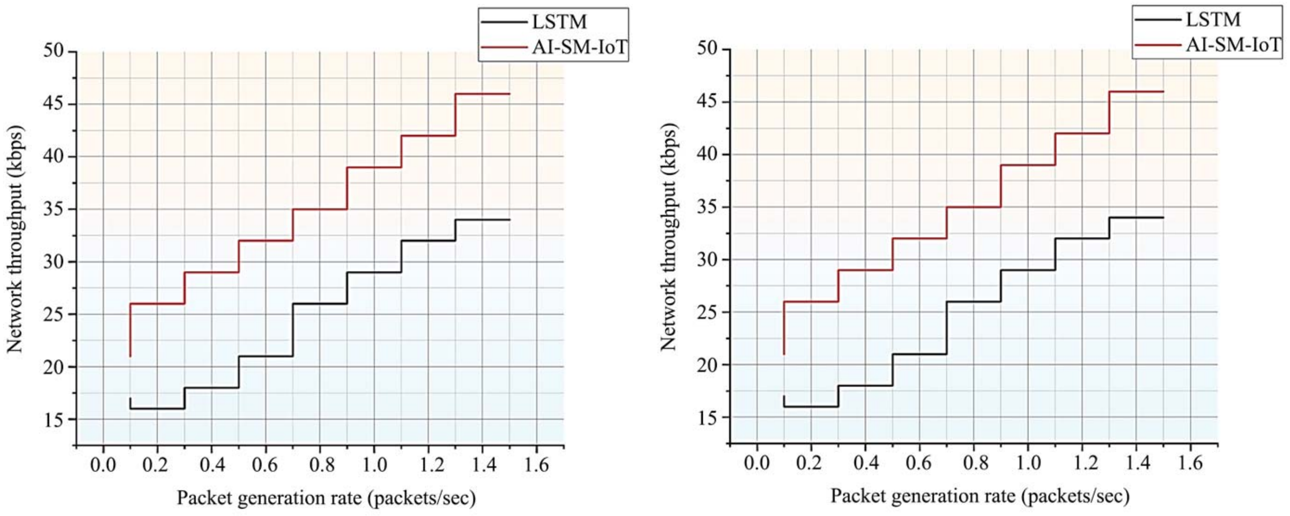
Network throughput analysis of the proposed AI-SM-IoT system

Packet generation rate (packets/sec)	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
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 simulation analysis of the proposed AI-SM-IoT system is analyzed by varying the packet generation rate from a minimum to a maximum level. The proposed AI-SM-IoT system outcomes of different packet sending rates, such as low and high levels, are analyzed. The proposed AI-SM-IoT system with a higher security level and lower computation complexity.

5. 2. Delay analysis

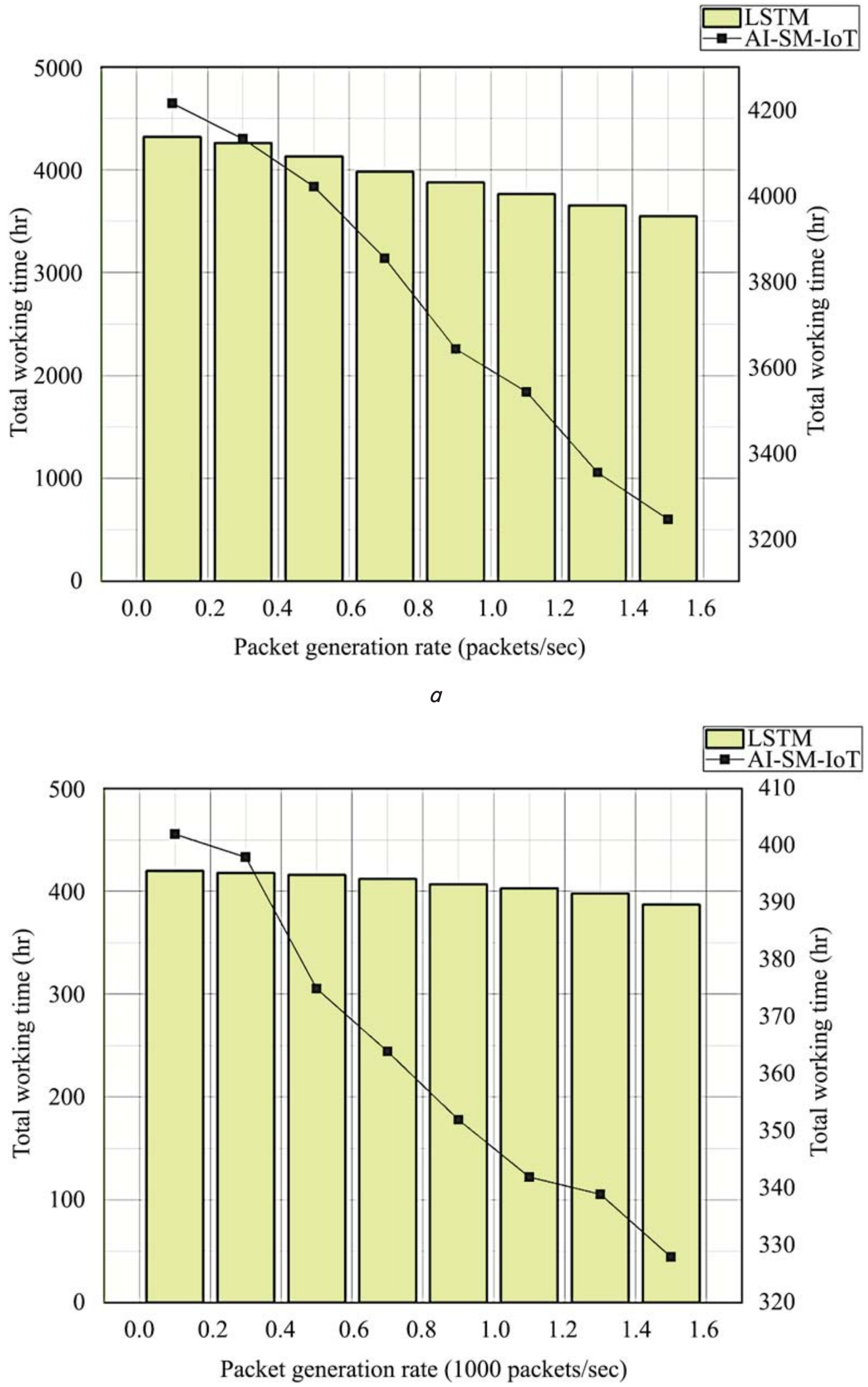
As the packet generation rate increases, the respective network throughput also increases. Fig. 6, *a*, *b* show the working time analysis of the proposed AI-SM-IoT system with lower and higher packet generation rates, respectively.



a

b

Fig. 5. Network throughput analysis of: *a* – higher sending rate; *b* – lower sending rate



a

b

Fig. 6. Working Time Analysis of proposed AI-SM-IoT System: *a* – Higher Packet Generation rate; *b* – Lower Packet Generation Rate

The packet generation rate is varied under two conditions: lower generation rate and higher generation rate. The respective simulation outcomes of the proposed AI-SM-IoT system are analyzed under different sending rates. The simulation outcome, such as the total working time required for the design, is monitored and plotted. The proposed AI-SM-IoT system with lesser complexity and IoT module exhibits lower working time than the existing model LSTM. Table 2 depicts the total working time analysis of the proposed AI-SM-IoT system.

The proposed AI-SM-IoT system is analyzed under lower and higher packet generation rate conditions, and the simulation outcomes are analyzed and tabulated. The proposed AI-SM-IoT system with IoT module and artificial intelligence model enhances the overall system performance. 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.

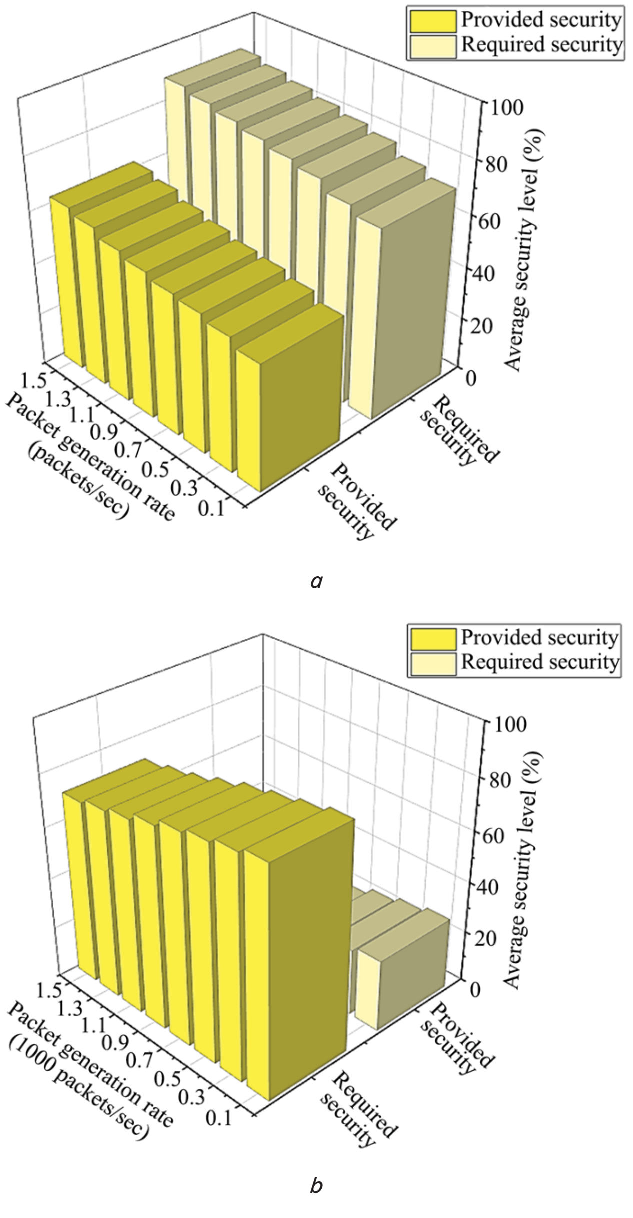
Table 2

Total working time analysis of the proposed AI-SM-IoT system

Packet generation rate (packets/sec)	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

5. 3. Network security analysis

Fig. 7, *a*, *b* show the security level analysis of the proposed AI-SM-IoT system with lower packet generation and higher packet generation rates, respectively.



a

b

Fig. 7. Security level analysis of proposed AI-SM-IoT System: *a* – higher packet generation level; *b* – lower packet generation level

The security level analysis of the proposed AI-SM-IoT system is done by varying the packet generation rate from lower to higher with two conditions: lower generation rate and higher generation rate. The simulation outcomes show that the proposed AI-SM-IoT system has a higher security level than the existing models. The proposed AI-SM-IoT system with artificial intelligence enhances overall security.

The proposed AI-SM-IoT system is analyzed in this section, and the simulation results are compared with the existing model. The proposed AI-SM-IoT system with artificial intelligence, IoT module, and safety measures enhances the simulation results.

6. Discussion of AI-based security method for IoT environment (AI-SM-IoT) system results

This article presents a robust framework for securing the Internet of Things devices. The first phase gathers data from IoT devices to characterize the consumer. The literature is full of attacks on cyber-physical systems, all of which must be mitigated. The process continues with attacks like replay attacks, denial of service, jamming, time synchronization, stealth time synchronization, false data injection, and so on. The study uses the two secure modules, the standard application protocol and Transmission Control Protocol (TCP), to manage the information transmission. During this process, an intelligent deep-learning model ensures overall data security. Here the deep learning model validates every component to ensure the authorized users in the IoT cloud environment. This process provides data security with minimum unauthorized activities. In addition, the firewall uses the rudimentary network, which uses the rules-based approach that predicts abnormal movements with minimum latency in the IoT ecosystems. The AI-based security method for the IoT environment (AI-SM-IoT) system uses various deep learning features, classification processes, and weight updating procedures that help to identify the abnormal activities in the IoT environment with minimum latency and high throughput rate, which is described in Fig. 5, *a*, *b*. In addition, the overall delivery rate of the packet is described in Table 1. The obtained results are higher efficiency compared to the existing methods. Moreover, the system ensures the minimum working time for entire packets described in Table 2.

Rather than relying on often single points of failure in traditional IoT authentication methods, this study suggests a blockchain-based AI authentication technique. A private blockchain is built amongst cluster heads in a single wireless sensor network, bringing together the decentralized nature of blockchain with the distributed nature of IoT nodes. The peculiarities employed in the proposed work include a deep learning network to manage the security of the IoT network, with the following sub-goals in mind. (1) decrease network latency during information transfer and access by combining a down sampler and deep classifier; (2) manage data security by combining a blockchain encryption model and a killing chain. The study controls data flow using two encrypted modules the standard application protocol and the Transmission Control Protocol (TCP). An advanced deep learning model monitors the procedure to guarantee the safety of every data. In this case, the deep learning model verifies all parts to ensure that only authorized users can access the IoT cloud. This method protects sensitive information while limiting the possibility of outside interference. Furthermore, the firewall prevents unauthorized access to the network, and the rules-based approach anticipates anomalous activity in IoT ecosystems with low latency. All wireless sensor network nodes have their base stations recorded in the distributed ledger. Data registration between cluster heads and regular nodes and cross-communication authentication are finalized in this paradigm. Finally, examining IoT devices' performance and security demonstrates the scheme's dependable efficiency and security.

Fig. 5, *a* shows the network throughput study of the proposed AI-SM-IoT system with lower sending rates, and Fig. 5, *b* shows the analysis with more excellent shipping rates compared with LSTM [23]. The proposed AI-SM-IoT system improves the system throughput due to its increased security and decreased processing time. Worktime analysis of the proposed AI-SM-IoT system is displayed in Fig. 6, *a* (Higher Packet Generation Rate) and *b* (Lower Packet Generation Rate). Different transmitting rates are examined to compare the simulation results for the proposed AI-SM-IoT system. Results from the simulation are tracked and shown to determine how much time will be needed to complete the design. Reduced complexity and an IoT module allow the proposed AI-SM-IoT system to outperform the current LSTM [23] model in less time.

The suggested AI-SM-IoT system's security analysis is depicted in Fig. 7, which compares two different packet creation rates (greater and lower, respectively). Results from computer simulations demonstrate that the proposed AI-SM-IoT system is more secure than competing approaches.

However, this study requires optimized techniques to enhance the overall intelligent techniques' efficiency. During the classification process, the network must select the optimized weight value to reduce the deviation between the outputs. Therefore, optimization techniques are incorporated to improve the overall abnormal activities in the IoT environment. The research issues are resolved by applying the meta-heuristic optimization method. In addition, the research work incorporated encryption techniques to enhance overall security with a high packet delivery rate in the IoT cloud environment. The security and respective efficiency is described in Fig. 7, a, *b*. Fig. 7 depicts that the introduced system attains high security and ensures the maximum packet delivery rate with minimum delay.

Solution robustness in the face of fluctuating conditions

The constraining effect occurred immunity to the shifting conditions that affect anything. Following classifier training, the logistic regression is a binary cross-entropy model's error must be computed according to the guidelines provided. When the classifier values are changed, but the downsampler steps are not yet performed, the L model of a computer error is described. By adjusting the weights of the connections between cells in the output units, the convolution layer can transition to a new hidden state or input layer. Remember to notice the discrepancy between predicted, measured, and simulated outcomes to zero in on the parameters connecting secret-level cells to the outputs-level cells.

The one limitation of deep learning approaches is that it needs a large amount of data for model testing.

The high price of implementing AI is cited as a drawback of the research. Integrating privacy and security requirements might be challenging if many different IoT devices exist. For some companies, the time, energy, and money required to optimize for all devices may be too great, leading them to go for subpar solutions to save money.

The potential for future networks and gadgets to gain insight from their actions, anticipate their users' next moves and enhance their efficiency and discernment. Connecting devices and programs across different platforms are of utmost importance. Applications for the IoT must be built with the understanding that future technologies will require a focus on data collecting and interpretation.

Despite the obstacles, AI's most significant problem is balancing the requirement for vast volumes of organized or standardized data with individuals' right to privacy. The fundamental concern is privacy, which is the root cause of many other difficulties, including governmental involvement.

7. Conclusions

1. Network Packet Delivery Rate: the packet production rate varied between 25 kbps and 49 kbps, and the simulation study of the proposed AI-SM-IoT system is performed. Improved security and reduced computational complexity characterize the proposed AI-SM-IoT system.

2. Delay Analysis: the proposed AI-SM-IoT system's simulation results at varying transmission rates. Compared to the current model, the suggested AI-SM-IoT system's 328-hour operating period for a packet creation rate of roughly 1.5 is much more manageable due to its simpler design and IoT module. Achieving the same accuracy with LSTM requires 387 hours. The learning process increases the abnormal prediction rate, and the network parameters are updated continuously, reducing the delay compared to the existing methods.

3. Improve overall data security. This process uses the standard application protocol and Transmission Control Protocol (TCP). These protocols help to ensure data security in the IoT network. This process improved the overall network security by 93.5 % of accuracy for various packet levels. The IoT environment is continuously examined to evaluate every user's activities. The user request and respective parameters are analyzed with the training process and network parameter updating procedure.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

Manuscript has no associated data.

References

1. Oniani, S., Marques, G., Barnovi, S., Pires, I. M., Bhoi, A. K. (2020). Artificial Intelligence for Internet of Things and Enhanced Medical Systems. Studies in Computational Intelligence, 43–59. doi: https://doi.org/10.1007/978-981-15-5495-7_3
2. Su, J., Chu, X., Kadry, S., S, R. (2020). Internet-of-Things-Assisted Smart System 4.0 Framework Using Simulated Routing Procedures. Sustainability, 12 (15), 6119. doi: https://doi.org/10.3390/su12156119
3. El-Latif, A. 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. doi: https://doi.org/10.1109/tnsm.2020.2969863
4. Chakraborty, N., Li, J.-Q., Mondal, S., Luo, C., Wang, H., Alazab, M. et al. (2021). On Designing a Lesser Obtrusive Authentication Protocol to Prevent Machine-Learning-Based Threats in Internet of Things. IEEE Internet of Things Journal, 8 (5), 3255–3267. doi: https://doi.org/10.1109/jiot.2020.3025274
5. Manogaran, G., Mumtaz, S., Mavromoustakis, C. X., Pallis, E., Mastorakis, G. (2021). Artificial Intelligence and Blockchain-Assisted Offloading Approach for Data Availability Maximization in Edge Nodes. IEEE Transactions on Vehicular Technology, 70 (3), 2404–2412. doi: https://doi.org/10.1109/tvt.2021.3058689
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. doi: https://doi.org/10.1002/cae.22375
7. Wang, W., Jackson Samuel, R. D., Hsu, C.-H. (2020). 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. doi: https://doi.org/10.1080/22797254.2020.1755998
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, 25 (20), 12989–12999. doi: https://doi.org/10.1007/s00500-021-06075-8
9. Mohamed Shakeel, P., Baskar, S., Sarma Dhulipala, V. R., Mishra, S., Jaber, M. M. (2018). RETRACTED ARTICLE: Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks. Journal of Medical Systems, 42 (10). doi: https://doi.org/10.1007/s10916-018-1045-z
10. Amudha, G., Narayanasamy, P. (2018). Distributed Location and Trust Based Replica Detection in Wireless Sensor Networks. Wireless Personal Communications, 102 (4), 3303–3321. doi: https://doi.org/10.1007/s11277-018-5369-2
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, 127 (1), 767–792. doi: https://doi.org/10.1007/s11277-021-08404-4
12. Malarvizhi Kumar, P., Choong Seon, H. (2021). RETRACTED ARTICLE: Internet of Things-Based Digital Video Intrusion for Intelligent Monitoring Approach. Arabian Journal for Science and Engineering. doi: https://doi.org/10.1007/s13369-021-05902-2
13. Manickam, A., Jiang, J., Zhou, Y., Sagar, A., Soundrapandiyan, R., Dinesh Jackson Samuel, R. (2021). Automated pneumonia detection on chest X-ray images: A deep learning approach with different optimizers and transfer learning architectures. Measurement, 184, 109953. doi: https://doi.org/10.1016/j.measurement.2021.109953
14. Sheron, P. S. F., Sridhar, K. P., Baskar, S., Shakeel, P. M. (2019). A decentralized scalable security framework for end-to-end authentication of future IoT communication. Transactions on Emerging Telecommunications Technologies, 31 (12). doi: https://doi.org/10.1002/ett.3815
15. Amudha, G. (2021). Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions. Wireless Personal Communications, 127 (1), 85–105. doi: https://doi.org/10.1007/s11277-021-08094-y
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. doi: https://doi.org/10.1016/j.future.2021.01.028
17. Nguyen, T. N., Liu, B.-H., Nguyen, N. P., Dumba, B., Chou, J.-T. (2021). Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks. IEEE Transactions on Power Delivery, 36 (4), 2264–2273. doi: https://doi.org/10.1109/tpwrd.2021.3061358
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. doi: https://doi.org/10.1016/j.scs.2020.102364
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. doi: https://doi.org/10.1109/mcom.2018.1800036
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. doi: https://doi.org/10.1109/jiot.2020.2982417
21. Mendhurwar, S., Mishra, R. (2019). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15 (4), 565–584. doi: https://doi.org/10.1080/17517575.2019.1600041
22. Mukherjee, A., Goswami, P., Yang, L., Sah Tyagi, S. K., Samal, U. C., Mohapatra, S. K. (2020). Deep neural network-based clustering technique for secure IIoT. Neural Computing and Applications, 32 (20), 16109–16117. doi: https://doi.org/10.1007/s00521-020-04763-4

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. doi: https://doi.org/10.1016/j.comcom.2020.03.004
24. Alqaralleh, B. A. Y., 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. doi: https://doi.org/10.1007/s00779-021-01543-2
25. Ahmed Jamal, A., Mustafa Majid, A.-A., Konev, A., Kosachenko, T., Shelupanov, A. (2021). A review on security analysis of cyber physical systems using Machine learning. Materials Today: Proceedings. doi: https://doi.org/10.1016/j.matpr.2021.06.320
26. Cui, Z., Xue, F., 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, 1–1. doi: https://doi.org/10.1109/tsc.2020.2964537
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. doi: https://doi.org/10.1016/j.jnca.2020.102537
28. Poniszewska-Maranda, A., Kaczmarek, D., Kryvinska, N., Xhafa, F. (2018). Studying usability of AI in the IoT systems/paradigm through embedding NN techniques into mobile smart service system. Computing, 101 (11), 1661–1685. doi: https://doi.org/10.1007/s00607-018-0680-z
29. Zaidan, A. A., Zaidan, B. B. (2018). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artificial Intelligence Review, 53 (1), 141–165. doi: https://doi.org/10.1007/s10462-018-9648-9
30. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R. (2020). 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). doi: https://doi.org/10.1002/ett.4112
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. doi: https://doi.org/10.1109/access.2019.2941978
32. Li, D., Deng, L., Liu, W., Su, Q. (2020). Improving communication precision of IoT through behavior-based learning in smart city environment. Future Generation Computer Systems, 108, 512–520. doi: https://doi.org/10.1016/j.future.2020.02.053
33. Edge-IIoTset Cyber Security Dataset of IoT & IIoT. Available at: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot