Computers, Materials & Continua
DOI: 10.32604/cmc.2023.032220
Article

Tech Science Press

Multi-Zone-Wise Blockchain Based Intrusion Detection and Prevention System for IoT Environment

Salaheddine Kably[1,2,*], Tajeddine Benbarrad[1], Nabih Alaoui[2] and Mounir Arioua[1]

[1]Laboratory of Information and Communication Technologies, National School of Applied Abdelmalek, Saadi University, Tanger, Morocco
[2]Ecole Supérieure D'Informatique et du Numérique, TICLab, Université Internationale de Rabat, Sala El Jadida, Morocco
*Corresponding Author: Salaheddine Kably. Email: salaheddine.kably@gmail.com

Received: 10 May 2022; Accepted: 12 June 2022

Abstract: Blockchain merges technology with the Internet of Things (IoT) for addressing security and privacy-related issues. However, conventional blockchain suffers from scalability issues due to its linear structure, which increases the storage overhead, and Intrusion detection performed was limited with attack severity, leading to performance degradation. To overcome these issues, we proposed MZWB (Multi-Zone-Wise Blockchain) model. Initially, all the authenticated IoT nodes in the network ensure their legitimacy by using the Enhanced Blowfish Algorithm (EBA), considering several metrics. Then, the legitimately considered nodes for network construction for managing the network using Bayesian-Direct Acyclic Graph (B-DAG), which considers several metrics. The intrusion detection is performed based on two tiers. In the first tier, a Deep Convolution Neural Network (DCNN) analyzes the data packets by extracting packet flow features to classify the packets as normal, malicious, and suspicious. In the second tier, the suspicious packets are classified as normal or malicious using the Generative Adversarial Network (GAN). Finally, intrusion scenario performed reconstruction to reduce the severity of attacks in which Improved Monkey Optimization (IMO) is used for attack path discovery by considering several metrics, and the Graph cut utilized algorithm for attack scenario reconstruction (ASR). UNSW-NB15 and BoT-IoT utilized datasets for the MZWB method simulated using a Network simulator (NS-3.26). Compared with previous performance metrics such as energy consumption, storage overhead accuracy, response time, attack detection rate, precision, recall, and F-measure. The simulation result shows that the proposed MZWB method achieves high performance than existing works

Keywords: IoT; multi-zone-wise blockchain; intrusion detection and prevention system; edge computing; network graph construction; IDS; intrusion scenario reconstruction

1 Introduction

Intrusion detection and prevention system (IDPS) has been an emerging topic in Internet of Things (IoT) [1]. Nowadays, cyber-attacks are forensic attacks that damage in environment becomes high, and hence traditional intrusion detection system (IDS) requires unified architecture for security monitoring and control [2,3]. Previous approaches have been proposed a machine learning (ML) approaches for attacks detection and finally, it can be classified into either two classes (normal and malicious) or three classes (normal, anomaly, and suspicious) [4]. These approaches failed to apply to large volumes of intrusions and had low accuracy and precision [5]. Several existing methods implemented various deep learning techniques to detect the attacks efficiently [6,7]. Most of the attack patterns are similar to benign patterns, but it increases the risk of intrusions. Further, several network security tools such as firewall, and honeypot have been widely used, which are compromised by attackers and also does not suited for resource-constrained IoT or Industrial IoT (IIoT) applications [8].

Hence, a required lightweight security scheme is suited for limited storage capacity and computation power devices [9]. Security tools feature does not reflect high accuracy in intrusion, so it brings serious issues to predicting the presence of attackers and taking countermeasures for attacker behaviors. Due to a lack of accurate intrusion detection systems and security tools, the current heterogeneous IoT environment is vulnerable to some severe security attacks, namely, spoofing, distributed Denial-of-Service (DDoS), disruption, energy exhausting, and insecure communication attacks [10]. When the number of IoT devices increases gradually, then the number of vulnerabilities (unknown) likewise increases, which result in weaker security monitoring, normal/anomaly behaviors of any IoT device is very dynamic, and the different behavior of attackers cause energy wastage (IoT devices, security tools) and harm devices separately by compromising [11]. Thus, it is clear that the impact of security attacks varies for IoT devices. Furthermore, the detection schemes must be effectively performed to find the intrusions since IoT devices' security requirements and capabilities are heterogeneous in terms of events, memory, bandwidth, computational power, and energy [12].

To improve our previous work [13] with an IDS, the visualization of network in a graph is useful. Graph construction-based network identifies attacker's location and it can be easily isolated/disconnect the links from the legitimate nodes to the attackers [14]. Furthermore, it enhances the accuracy of intrusion detection and prevents the network from more damage. The major issue in our previous work, multi-zone Direct Acyclic Graph (DAG) Blockchain [13] in network graph construction is that it requires In IoT, blockchain is another security solution that not only detects a single type of attack, but also detects multiple types of attacks. Compared with the traditional IDS scenarios, blockchain mainly focuses on cyber-attacks with good tracing of behaviours and also provides a reliable connection to normal IoT devices [15,16]. Hence, security of IoT environment is improved and targeted intrusion prevention is reached while authenticating all IoT devices into the third party or security managers [17]. Evidence collection and analysis can be helpful in IDS, which compares the device pattern to the logically related transactions for attacks detection. Several research questions are addressed in this research, which is described as follows,

- Approaches for security management and attacker's isolation in a lightweight multi-zone DAG Blockchain
- IDPs can be detected in forensic attacks with all the different capabilities of IoT devices.

1.1 Motivation & Objectives

This paper's primary aim and scope are to design IDS for all security requirements and capabilities of heterogeneous IoT environments. Hence, our potential goals are, first, The detection and prevention of attacks. And secondly, collection of evidence and forensic analysis as we are motivated by some of the essential issues of IDPs as follows,

- High temporal/modified data: attackers are highly serious about making vulnerable or threats to legitimate devices. Attackers compromise the legitimate devices and send the fake information or modified information to the network or store it on the server.
- Lack of decentralized security mechanism: evidence, transmitted data (source and destination) information, and devices centrally stored pieces of information on any security server or system, which leads to a single point of failure. Internal or external attackers will easily hack all sensitive/non-sensitive information.
- High energy consumption and delay: timely detection of attackers reduces resource constraints of IoT devices. Currently, IoT devices are heterogeneous (bandwidth, computational power, energy, memory, and more).

The principal objective of this study is to detect and confirm the attack events occurrences and alert all the normal network devices in the environment. Hence, we designed some of the other objectives in this study. To perform preliminary analysis to analyze whether the devices are authenticated successfully.

- To acquire, and process all the evidence in a forensically sound manner for accurate intrusion detection.
- To follow the attack's detection by effective evidence collection, investigation, and analysis.
- To effectively isolate the compromised devices to prevent further intrusions and alert other devices about the compromised devices during intrusion scenario reconstruction.
- To preserve the security and privacy of all evidence by blockchain technology over the heterogeneous environment.

1.2 Research Contributions

The proposed MZWB improves the security aspect of our Lightweight Direct Acyclic Graph Blockchain solution for Enhancing the Resource-Constrained IoT Environment [13] in terms of high energy consumption, increased storage overhead and low accuracy. The major contributions of this work are described as follows,

- Firstly, we perform authentication for the IoT nodes to ensure the nodes' legitimacy by multi-zone-wise blockchain using Enhanced Blowfish Algorithm (EBA).
- Secondly, network graph construction is performed to manage the traffic caused by the devices using Bayesian DAG (B-DAG), considering numerous parameters such as link stability, intimacy number of transmissions, location, and distance between the nodes.
- Thirdly, Intrusion detection is performed based on a two-tier intrusion detection system to increase the accuracy of detecting the intrusions using Deep Convolutional Neural Network (DCNN) and Generative Adversarial Network (GAN).
- Finally, Prevent the IoT nodes by performing attack path detection using Improved Monkey Optimization (IMO) algorithm and intrusion scenario reconstruction by graph cut method.

This method achieves higher performance than existing works regarding energy consumption, storage overhead, responses time, accuracy, attack detection rate, precision, recall, and F-measure.

2 Literature Survey

Various existing works related to intrusion detection and prevention systems in the IoT networks are described in this section. Authors in [18] proposed blockchain-based method for intrusion detection using trust mechanism. The proposed collaboration-based intrusion network includes four components such as collaboration component, trust management, chain component, and peer-to-peer (P2P) communication. The node's trust value is classified into three levels: low, medium, and high, by evaluating the probability of the node. The trust value is used to evaluate the reputation of the target node. The alarm is generated based on the feedback from the decisions. The simulation result demonstrates that the proposed model achieves better robustness and intrusion detection performance under adversary scenarios. Here, all the transactions are stored in the blockchain; however, it takes much time for mining due to its linear structure, which is not suitable for a large-scale environment since it increases high energy consumption. A machine learning-based intrusion detection system, namely an intrusion detection tree, is proposed in this paper [19]. The proposed work includes four processes such as exploring the dataset, collecting raw data from the dataset, feature extraction and ranking, and constructing the resultant tree. After collecting the raw data preprocessing is initialized, which includes feature encoding and feature scaling. Then calculate the critical score for every feature for extracting the crucial features. Based on the essential features, the intrusion detection tree is constructed, which classifies the features into two classes, such as normal and anomal. The simulation result shows that the proposed model achieves better performance when compared to other machine learning algorithms. Here, intrusions are detected based on machine learning. However, it can only detect known patterns due to its limited training samples leading to increased false alarms.

Authors in [20] proposed intrusion detection system using system call graph, which includes the information of different techniques in a single structure. The proposed architecture includes two characteristics such as modularity and two stages. It includes four processes: intrusion detection stage, sequence time delay embedding, text classification, and system call graph, which improve detection accuracy. The graph is constructed with weight values for representing the importance of the transitions in system calls. A deep neural network combines the results of different techniques and provides two classes, such as normal and attack. The simulation result shows that the proposed model achieves a better detection and false-positive rate performance. An intrusion detection system is proposed to detect intrusions by using alert correlation analysis and prediction method [21]. The proposed work includes five processes such as intrusion action extraction, algorithm of session pruning, intrusion session rebuilding, and construction of intrusion scenario. Intrusions are extracted based on the similarity. The main aim of intrusion session rebuilding is to depict the original correlation between two actions. Session pruning section is used for some main reasons such as duplicate actions does not have any information about the intruders and reduces the effect of false positives and redundant data, and shorter action provides optimal results. The intrusion scenario is constructed using binary correlations that are extracted from pruned session. The experimental result demonstrates that the proposed model achieves better performance in alert correlation and constructing the intrusion scenarios. Here, complex attacks are detected successfully; however, the single stage attacks are not detected by binary correlation which reduces the security strength of the network.

Authors in [22] proposed intrusion detection system using a deep belief network (DBN) and improved genetic algorithm. A genetic algorithm provides an optimal network, and DBN is used to classify the intrusions. It detects the specific types of attacks with high accuracy. The proposed method reduces the complexity and training time without affecting the accuracy. The performance of the proposed work is evaluated using the NSL-KDD dataset. The simulation result shows that the proposed model achieves better performance in intrusion detection and complexity. However, the proposed method takes much time for training, which increases high latency, and it has less accuracy due to a lack of significant parameters, thus degrading the performance of the proposed work. Authors in [23] proposed honeypot-based intrusion detection system using the social leopard method for detecting Ransomware attacks. The proposed honeypot-based intrusion detection system includes a honey folder, audit watch, and complex event processing (CEP). Honey-folder extracts the traffic patterns and analyzes them for detecting the attacks using the social leopard algorithm, which provides the warning message to the user. CEP engine is used to correlate the various events from the network, which provides the malicious attacks and removes them from the network. The honey agent calculated the adaptive score, and it is forward to all features. The experimental result shows that the proposed model achieves better performance in detection time, accuracy, and rate than the existing works. Here, the adaptive score and events are used for detecting malicious nodes in the network. However, all this information's are forward through the public channel, which can easily access and modify by the attackers, reducing the security and attack detection accuracy.

Authors in [24] proposed blockchain-based collaborative intrusion detection in IoT-cloud networks. The proposed system includes four components such as cloud vendor, blockchain, cyber-security intrusion detection system (CIDS), and smart contract central coordinator unit. The blockchain-based privacy preservation in the cloud leads to high security. The information is encrypted and sent to the cloud node to ensure data integrity. The cloud vendors share the event logs and alert messages based on the malicious activities. Bidirectional LSTM (BiLSTM) is proposed for detecting intrusions in the network. The performance of the proposed work is evaluated using UNSW-NB15 and BoT-IoT datasets. Finally, the simulation shows that the proposed model achieves better performance in terms of time and reliability. Here, all the information is stored and processed from the cloud server, which is a time-consuming process that leads to high latency during intrusion detection, increasing the resource wastage of the devices. In addition, a hidden Markov-based cyber deception method is proposed for predicting the attack paths [25]. The proposed method includes graph analysis (reactive) and cyber deception method (proactive) for detecting attack paths. At first, the system predicts the intrusion and then predicts an attack path using Hidden Markov model (HMM) algorithm. It detects the optimal attack path from multiple paths, which helps to detect and prevent the attacks with minimum time; for optimal path prediction, this research used forward and backward algorithms. The simulation result shows that the proposed model achieves better performance for attack path prediction compared to an existing model. Here, the attack graph is constructed in a static manner which does not predict the newly entered attacks that leads to poor security. And the HMM detects the optimal path; however, it takes huge memory and computation time for dynamic graph construction to degrade the performance.

Authors in [26] proposed an approach to detect the intrusions (i.e., cyber-attacks) using deep learning. Initially, the Canadian Institute for cyber-security intrusion detection system (CICIDS2017) dataset was used to perform training and testing using a convolutional neural network (CNN). Training of dataset was performed to classify the network based on nine classes to classify various attacks such as DoS attack, Bot, web attack, port scan, etc. After training the dataset testing was performed to classify the network traffic as malicious or benign. Simulation results of this work are expressed in terms of accuracy, false alarm rate, training overhead, and detection rate. Authors proposed an approach for intrusion detection based on decision tree and rules for IoT networks with three sequential methods in [27]. Initially, input features are extracted from the dataset in the first method using Reduced-error Pruning (REP) tree. Based on these features classify the IoT network as benign or attack in the second method using JRip algorithm. In the third method, forest PA classifier was used to classify the network by the inputs such as dataset features, outputs of first and second methods. CICIDS2017 and BoT-IoT datasets were used for experimental analysis. The performance of this work is evaluated based on accuracy, overhead, etc. In [28], authors proposed an approach for intrusion detection in the IoT network hierarchically using graph neural networks by generating black-box attacks. Initially, Hierarchical adversarial attack (HAA) method was implemented to know the strategy of adversarial attack using graph neural network. For training, the dataset shadow generalized neural network (GNN) model was generated. Nodes with high priority of being attacked by the attackers are selected hierarchically in the node selection method using random walk with restart algorithm based on weight score calculation. Open source UNSW-SOSR2019 dataset was used in this work to perform simulation. The results of this work were shown based on precision and loss. Intrusion detection was performed in IoT based on multiple layer classification using deep learning in [29]. Initially, oversampling was performed using the synthetic minority oversampling technique (i.e., SMOTE) to increase the quality of the data. After successful oversampling, intrusion detection was performed based on single hidden layer feed-forward network (SLFN). To identify the type of attacks (i.e., intrusions) based on its activities using deep neural network (DNN). Four types of attacks are recognized by this method such as scan, DoS, MITM, and Mirai attacks. Simulation was performed using IoTID20 imbalanced dataset which was collected from a smart home monitoring application.

3 Major Problem Statement

The current IDPS scheme does not suited for early analysis and detection of cyber-attacks. Motivated by this great issue, in this study focuses on designing an accurate IDPS for IoT environment using blockchain. Further, we identified some of the specific issues of IDPS as follows, the network connectivity-based assessment of vulnerabilities was proposed in this paper [30]. The limitations of conventional alert-based visualization of attack scenario were addressed by this approach. The major problems of this research are listed as follows,

- The construction of attack scenarios was carried out based on several attributes of the attack, but the lack of consideration of node properties such as location will affect the analysis and will lead to false determination.
- The analysis of the constructed graph was performed in order to determine the presence and cause of the attack, but the major limitation of this approach is that only known attacks are identified, and the identification of unknown attacks is not considered.
- The analysis of the constructed graph was performed in order to determine the presence and cause of the attack, but the construction of the graph was performed in a static manner, whereas the attack process is dynamic in nature.

The identification and classification of attacks in the smart home application was proposed in this paper [31]. The security threats associated with the smart IoT devices were considered, and a hierarchical intrusion detection system was introduced. The main issues of this research are listed as follows,

- The supervised IDS (SIDS) identified the attack packets and classified them based on several features using the J48 classifier; however, labeling a massive set of data is not possible, and when trained with a small dataset, this approach possesses reduced accuracy.
- The hierarchical intrusion detection system possesses resistance only against a particular set of attacks in the network, but the IoT devices face various other security threats not mitigated by this approach.

- The hierarchical intrusion detection system was implemented in small-scale environments such as a smart home; adoption of this technique in large-scale environments degraded the performance of this approach.

- The forensics-based detection of intrusions in the industrial internet of things environment was proposed in this paper [32]. The limitations of existing approaches in handling long sequences of data were addressed by this approach. The major problems of this research are listed as follows,
  - o The Deep-IFS(DIFS) approach performed classification of network traffic into two categories such as normal and malicious using the supervised learning model however the proposed approach has limitations in dealing with imbalanced data which affects the accuracy of detection.
  - o The forensic based identification of attack packets doesn't ensure the integrity of the data transmitted in the network and doesn't provide the privacy to the data which attracted the attention of attackers.
  - o The Deep-IFS approach was said to identify attacks based on network forensics but the evidences considered for the purpose of analyzing the network packets were not described.

The blockchain based privacy preservation for forensic evidences was proposed in this paper [33]. The limitations in adopting digital forensics in IoT environment were considered and an effective approach for detecting the IoT based adversaries was presented. The major problems of this research are defined as follows,

- The blockchain based digital forensics in the IoT(BF-IoT) environment provided privacy preservation to the evidences by storing the evidences in blocks but the increase in number of evidences resulted in scalability issues which thereby degrades the performance of our approach.
- The forensics based analysis of evidences in the IoT environment considered huge amount of IoT devices for the purpose of acquisition of evidences but the legitimacy of these devices was not ensured.
- The evidences were acquired from huge amount of IoT devices for analyzing the data but the features considered for proper analysis of the evidences were not described in this approach.

Research Solutions: The aforementioned issues are addressed by providing the following solutions. (1). In our work network is constructed based on location in order to increase the accuracy of intrusion detection that reduce false alarm rate. In addition, authentication is performed by using MZ Blockchain which increase the security of the network. (2). Here, we perform two tier intrusion detection system in which the first tier used DCNN for intrusion detection that classifies the packets into normal, malicious and suspicious. and second tier used 3C's based GAN for detecting adversaries using past evidences which are collected from blockchain that increase attack detection accuracy. In addition, this work is suitable for any environment (i.e., small scale and large-scale environment) which increase the performance and efficiency of this work. (3). Evidences are collected and analyzed for predicting the intrusions which are stored in the blockchain; hence the global edge extract the evidence and perform matching process between evidence and current suspicious packets in order to increase the accuracy of intrusion detection. (4). Here, attack graph is constructed and reconstructed in a dynamic manner using improved monkey optimization and graph cut algorithms which helps to detect the attacks in an accurate manner thus leads to high attack detection rate and accuracy. (5). In our work used MZ blockchain which is constructed by number of DAG blocks in a zone that increases the scalability and reduces the latency during mining thus increase the performance of the proposed work.

4 MZW-Blockchain System Model

The proposed MZWB system focuses on ensuring the security of the IoT environment by incorporating two-tier IDS model. The system model comprises of three layers namely perception layer, edge layer, and blockchain layer. In which the perception layer consists of n number of IoT devices ($N_i = N_1, N_2, \ldots, N_n$) which are register their information to the trusted authority in order to ensure the legitimacy. The second layer is the edge layer which is built by master-worker edge nodes that consists n number of worker edge nodes ($e_i = e_1, e_2, .., e_n$) and one master edge node. The worker edge nodes include a honeypot that helps to attract the attackers in the network. In this layer, first level intrusion detection is performed. Third layer is blockchain layer which includes blockchain server that performs second level intrusion detection. Here, we used Multi-zone-wise blockchain structure which consist multiple zones which improves the scalability and energy efficiency. The blocks are constructed based on DAG structure. The architecture of the proposed MZWB is shown in Fig. 1. The proposed work includes four consecutive phases which are listed as follows ,

- Secure Authentication
- Dynamic Graph Construction
- Two Tier Intrusion Detection System
- Intrusion Scenario Reconstruction

4.1 Secure Authentication

The IoT devices in the perception level are authenticated in order to ensure the legitimacy of the nodes. The authentication is carried out based on the metrics such as *Device ID, physically unclonable function (PUF), media access control address (MAC) address, and location of the node*. Initially, the registration of nodes is carried out in which the nodes register themselves to the Trusted Authority (TA) by submitting the credentials. These credentials are stored in blockchain in order to preserve the privacy. The TA generates secret key for the IoT nodes by implementing EBA**.** The Random ID will be created for the IoT node and will be updated periodically by the TA. Initially, the blowfish algorithm generates sub keys; this proposed work employs four sub keys. The sub keys are stored in B-array, the array element size is 32-bit which is set as $b[j]$. The sub keys are varied based on input keys which can be represented as,

$$b[j] = b[j]\, XOR\, (j+1) - th\ 32 - bits\ input\ key \tag{1}$$

The enhancement made in the conventional blowfish algorithm is generating chaos based key generation (sub keys) ($CK_1, CK_2, CK_3,\ and\ CK_4$) in which the generated key is completely chanciness in order and does not duplicate after number of cycles which can be formulate as,

$$Z_m + 1 = \forall\, Z_m\,(1 - Z_m) \tag{2}$$

where $\forall$ is variable that governs the chanciness of the keys, and Z_m denotes the confidence values that lie among (0, 1). The chaotic based key generation satisfies and evaluated in chaos theory which attains chaos features such as kindliness and chanciness. The chaotic features are expressed as,

$$Z_m + 1 = \left(\forall\, Z_m - Z^2 m + Z^3 m\right) / Z^2 m + G^2 m \tag{3}$$

$$G_m + 1 = \forall \ \left(1 - Z^3 m\right) \times \left(-6\ G^3 m - \left(\frac{7}{9}\right) G\right) \tag{4}$$

$$H_m + 1 = \alpha\ H_m \left(R_m - G_m\right) \times \left(\frac{3Z_m}{124}\right)^2 \tag{5}$$

$$R_m + 1 = \beta\ \ G^3 m \left(H_m - R_m\right) \times \sqrt{2} \tag{6}$$

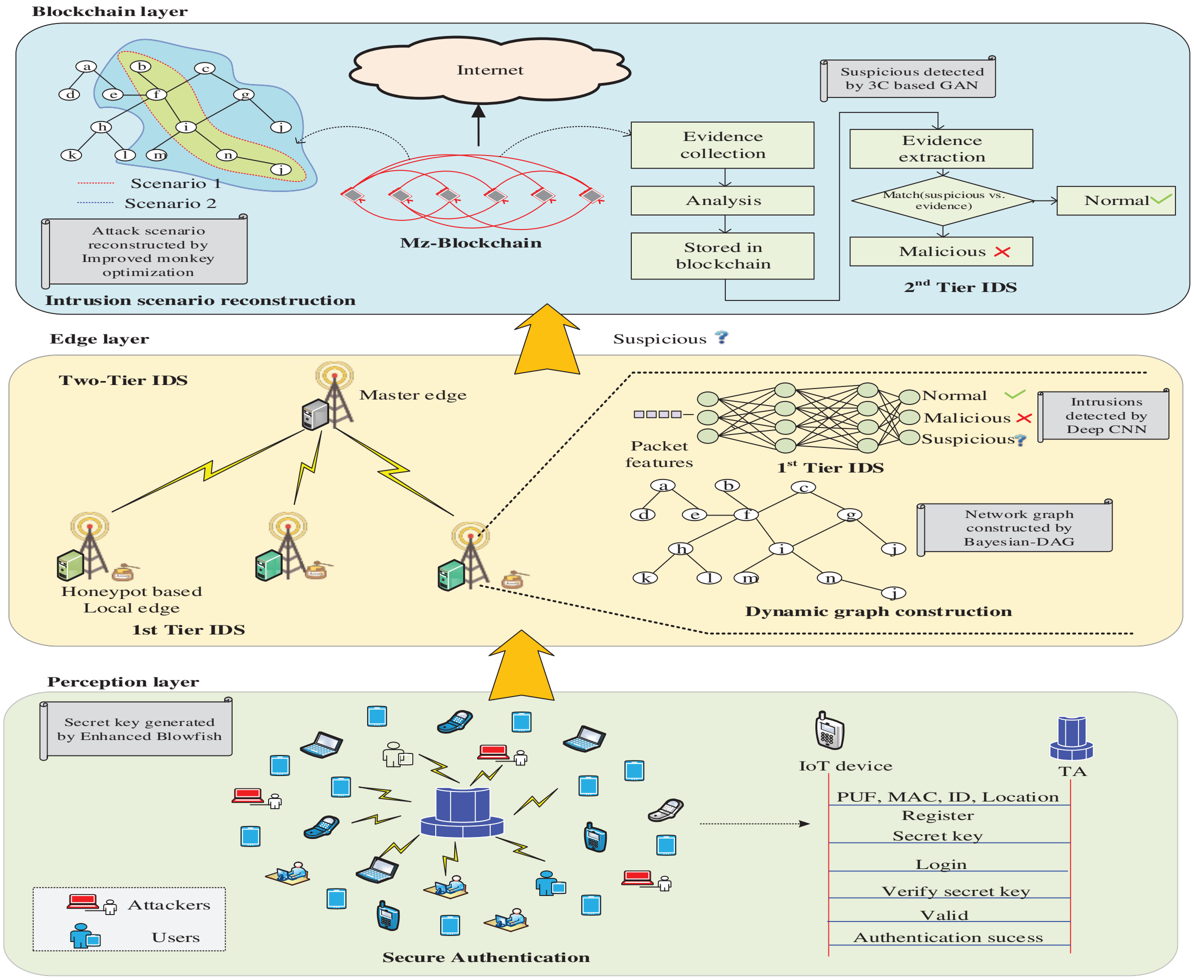

Figure 1: Architecture of proposed MZWB

From the above Eqs. (3), (4), (5) and (6) the sub keys are generated in which $Z_m, G_m, \ H_m, \ and \ R_m$ represents the confident values which the fitting to the interval of $(0, 1)\ 0 \leq Z_m, G_m, H_m, R_m \leq 1$, the variables $\forall, \ \alpha, \ and \ \beta$ governs the keys chanciness which the fitting to the interval of $(0, 1)\ 0 \leq \forall, \ \alpha, \beta \leq 1$. Initially the variable parameters such as $\forall, \ \alpha, \ and \ \beta$ are set and loaded, from the above mentioned equations the chaos based sub keys are generated, the generated sub keys are stored in $b\,[j]$, and random ID (r^i) is generated based on the user metrics such as Device ID, PUF, MAC address, and location of the node. This randomness in key generation improves the legitimacy of the nodes. The pseudocode for proposed chaos based key generation is provided below,

```
Enhanced Blowfish Algorithm ()
Input: Chaotic positive values and variable parameters
Output: Chaotic sub keys $CK_1, CK_2, CK_3,\ and\ CK_4$
Begin
    Set and load the $\forall,\ \alpha, \beta$
    Generate Chaotic sub keys using (3)–(6)
    Store sub keys in $b\,[j]$ using (1)
    Generate $r^i$ using authenticate metrics
    Update $r^i$ periodically
End
```

4.2 Dynamic Graph Construction

Once the authentication of IoT devices is completed the edge node constructs the network graph of the IoT devices in order to effectively manage the traffic produced by those devices. The IoT nodes in the network are constructed into B-DAG in which connectivity between the nodes is computed by the Bayesian probability. The construction of B-DAG is based on the factors such as *number of transmission, link stability, intimacy, location, and distance between the nodes*. The probabilistic way for labeling the relationship among variable is determine by Bayesian networks. In B-DAG model, the IoT nodes are signified as variables, edges between nodes are signified as relationship between them, parent nodes are roots, and children nodes are outcomes. The Conditional Probabilities (CDP) of the child nodes are stored distributively in parent node. The B-DAG network is expressed as,

$$B - DAG\,[(Q,\ \partial)] \tag{7}$$

where Q represents the network structure of Bayesian in DAG which can be represented as $Q = \left(V^{er}, E^{dg}\right)$ while $V^{er} = \left\{V_1^{er}, V_2^{er}, \ldots, V_n^{er}\right\}$ is the Bayesian network IoT nodes, E^{dg} is the edges among the nodes. ∂ is the network parameter of Bayesian which signifies the CDP for all nodes under the ailment of their parents.

If the E^{dg} among the IoT nodes is not present then B-DAG use factorization which can be formulated as,

$$pr\,(N/Q,\ \partial) = \prod\nolimits_{i=1}^{c} pr\left(N_i/\prod N_i, \partial_{N_i}\right) \tag{8}$$

where $pr\,(N/Q,\ \partial)$ is the global distribution of N nodes which is distributed locally for $N_i - th$ node with ∂_{N_i} which is ailment under their parent $\prod N_i$. All the traffic generated by the IoT devices is sent to the edge nodes for effective computation. Fig. 2 represents the B-DAG based network constructions in which vertices and edges of the parent and child nodes are represented.

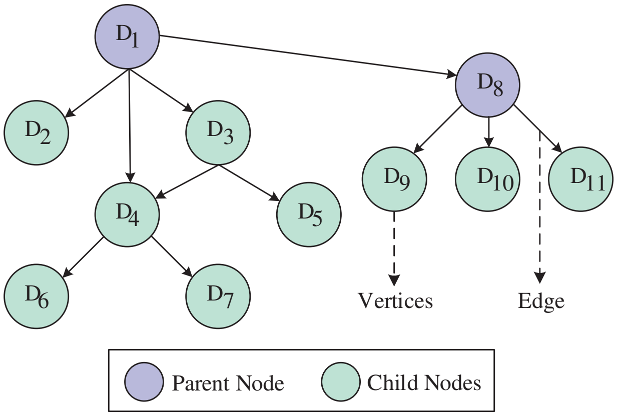

Figure 2: B-DAG based network construction

4.3 Two Tier Intrusion Detection System

The traffic generated by the IoT devices contains malicious data which when not analyzed and pruned will degrade the network performance and can cause total damage to the network. Therefore these network packets are analyzed by the 2 T-IDS. In the first tier, the packets are analyzed based on the significant packet flow features *(source bytes, destination bytes, destination host service count, count, same service rate, protocol type, service type, error rate, and flag).* The deep learning approach named DCNN is utilized in order to extract those packet features from the incoming packets and perform extensive classification. The proposed DCNN includes three layers such as convolutional layer, pooling layer and softmax layer. Initially, the convolutional layer extracts the flow features and generate feature map which is defined as follows,

$$Q_{ij} = A\left(FM \otimes w_{i:i+l-1,\,j+p-1} + B\right) \tag{9}$$

where B represent the bias function and $\otimes$ represent the convolution operation between filter matrix (FM) and input, w represent the weight values and the range of i represent from 1 to $(i + l - 1)$and j ranges from 1 to $j + p - 1$. Finally, the convolutional layer provides the feature map which is defined as follows,

$$F_m = [fm_{1,1}, fm_{1,2}, fm_{1,3}, \ldots, fm_{i+l-1}, j + p - 1] \tag{10}$$

Then pooling layer is performed the dimensionality reduction of the feature map which is defined as follows,

$$M_{ij} = Max\left(w_{i+l-1,\,j+p-1}\right) \tag{11}$$

Based on the extracted feature, softmax layer classifies the packets into three categories namely 1) normal, 2) malicious and Suspicious which is defined as follows,

$$Softmax\ \ (I_i) = \frac{Exp^{I_i}}{\sum_{i=1}^{n} Exp^{I_n}} \tag{12}$$

$$I_i = \sum w_i t_i + B \tag{13}$$

where I_i represent the input values of the softmax layer based on the input it classifies the packets. The local edge node prunes the malicious traffic and computes only the normal traffic. The suspicious traffic is fed to the second tier in which the forensics based detection of adversaries is carried out. The first tier is incorporated with Honeypot which acts as a normal entity to attract the attackers and gather their logic to train the proposed model.

The second tier of 2 T-IDS executes forensics based determination of nature of the suspicious packets. The suspicious packets may or may not be the malicious traffic which is to be analyzed deeper to determine its nature. In order to do so, the global edge node performs 3C's based forensic analysis. The 3C's denote the *Current location of device, context type, and count of the devices*. GAN is utilized to detect the suspicious packets nature. The proposed GAN includes two networks such as generator and discriminator. The process of generator is defined as follows,

$$Min_G Max_G U\left(\text{Ģ}, \mathfrak{D}\right) = \ \widehat{\mathrm{E}}_{y\sim r(y)}\left[log_{\mathfrak{D}}\left(y\right)\right] + \ \widehat{\mathrm{E}}_{y\sim r_{g(x)}}[log\left(1 - \mathfrak{D}\left(\text{Ģ}(x)\right)\right) \tag{14}$$

where $r\,(y)$ represent the distribution of real data and $r_{g(x)}$ represent the distribution data of generator. The performance of discriminator is defined as follows,

$$\mathfrak{D}\,(y)_{max} = r\,(y) + r_{g(y)} \tag{15}$$

The loss function of generator and discriminator is defined as follows,

$$loss_{\mathfrak{D}}\left(\mathfrak{D}, \text{Ģ}\right) = |f\,(r, l) - F(Gen\,(r)\,, r| \tag{16}$$

where f represent the extracted features and r represent the real features and l represent the latency features. After completed the training phase the GAN receives the input as extracted feature. Generator is trained for optimizing the loss function of discriminator. Discriminator receives the output of the generator as an input and then compares the suspicious packets to the normal and malicious packets to discover the intrusions. For that, it collects the evidence from the Multi-zone-wise Blockchain which are already analyzed and stored in the blockchain that includes the past evidence of the intrusions in the network. Hence, the GAN perform matching process between suspicious packets and evidence. Based on the matching process GAN classifies the spicious packets into two classes such as normal and malicious. Fig. 3 represents the two-tier IDS using DCNN and GAN.

4.4 Intrusion Scenario Reconstruction

Once the intrusion is detected in the network, it will be reconstructed for preventing the intruder node from others. For that we need to discover the attack path to refresh the network. The attack path is discovered based on the following metrics such *as one-hop relation, set of transaction and risk values.* Based on these metrics the proposed IMO discovers the attack path. The risk value of the node is calculated based on successive rate and risk probability. Initially, the nodes $N_i = \left(N_1, N_1, \ldots, N_{ij}, \ldots, N_{iDm}\right)$ $(1 \leq i \leq \mathfrak{M})$, the nodes current position is formulated as,

$$N_i = (n_{maxi} - n_{mini})\ .\mathfrak{r}\,(1, Dm) + n_{mini} \tag{17}$$

From the above equation, $\mathfrak{M}$ denotes the nodes population size, N_{ij} represents the nodes position i in the $j-th$ dimension (Dm), $n_{maxi} - n_{mini}$ denotes the interval of the nodes, and $\mathfrak{r}\,(1, Dm)$ random numbers which is distributed uniformly in a Dm dimensional vector. After node initialization, the nodes are trying to finding the solution for optimization problem by iterative manner. During searching process, the searching vectors $\nabla N_i = \left(\nabla N_1, \nabla N_2, \ldots, \nabla N_{ij}, \ldots \nabla N_{iDm}\right)(1 \leq i \leq \mathfrak{M})$ are generated randomly while the ∇N_i is engendered by random number generation matrix $\exists = \left(\exists_1, \exists_2, \ldots, \exists_{ij}, \ldots, \exists_{iDm}\right)$, the random number $\exists_{ij}$ is generated randomly over the interval [0, 1]. The ∇N_{ij} is represented by satisfying the following conditions which can be formulated as,

$$\nabla N_{ij} = \begin{cases} sa \ \ \exists_{ij} \leq e^{1-\dfrac{s^n}{s^n + 1 - it^n}} \\ 0 \ \ \exists_{ij} > e^{1-\dfrac{s^n}{s^n + 1 - it^n}} \end{cases} \tag{18}$$

where s^n denotes the searching number, and it^n. denotes the iteration numbers and the factor $sa\,(sa > 0)$ is the nodes size of the step per search. The nodes position pseudo gradient is computed as,

$$K'_{ij} = \left(K\left(N_i - \nabla N_i\right) - K\left(N_i + \nabla N_i\right)\right) / 2\nabla N_i \tag{19}$$

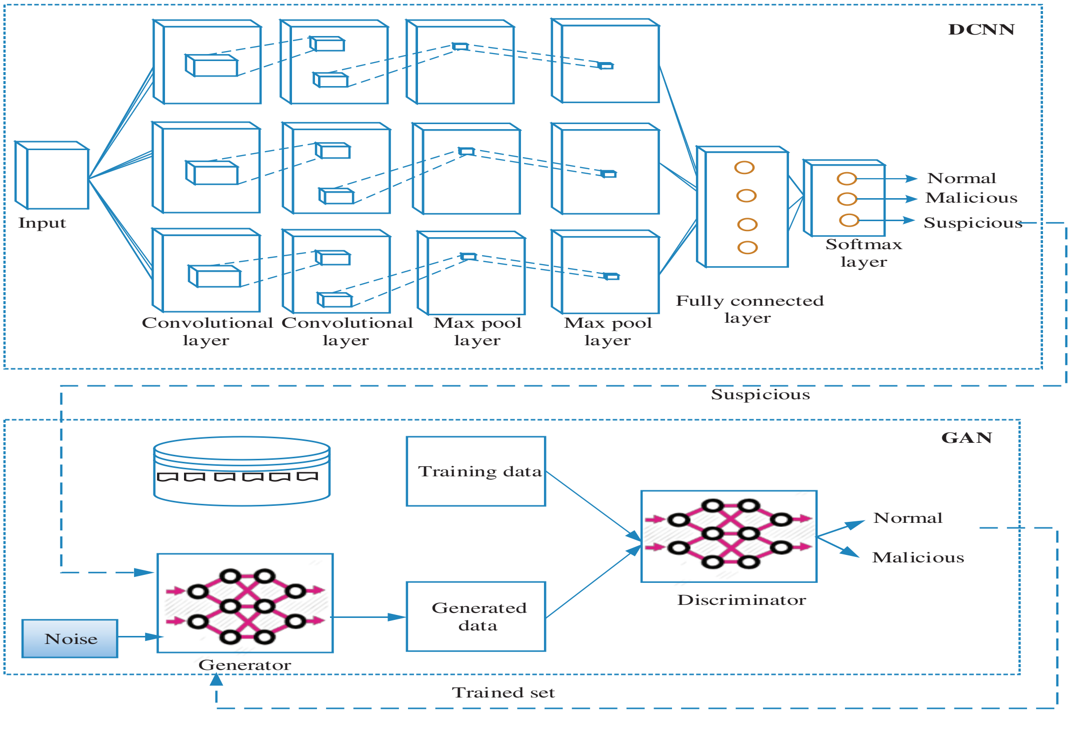

Figure 3: DCNN and GAN based IDS

In which $K'_{ij} = \left(K'_1\left(N_i\right), K'_2\left(N_i\right), \ldots, K'_D\left(N_i\right)\right)$. The updation of nodes N_i to T_i is done only when $K\left(\,T_i\right) < K\left(\,N_i\right)$, while $T_i = \left(T_1, T_2, \ldots, T_{ij}, \ldots, T_D\right)$ in the range of $n_{maxi} - n_{mini}$. The searching process will be repeated untill reaching the maximum s^n. After searching, each node searches its own path and look for optimal path. If there is any best path than the current path, the nodes select the optimal best path which can be formulated as,

$$T_{ij} = N_{ij} + \blacksquare \left(axis_j - N_{ij}\right) \tag{20}$$

From the above equation, $axis_j = \left(\sum_{i=1}^{\mathfrak{m}} N_{ij}\right) / \mathfrak{M}$ while $axis_j = (axis_1, axis_2, \ldots, axis_D)$ is the axis of the node.

After discover the attack path we perform the attack scenario reconstruction. For that purpose we proposed **Graph Cut** algorithm which reconstruct the network graph into two scenarios such as attack scenario 1 and attack scenario 2, in which the first scenario is attack path and second scenario represent the one hop relation between the attack nodes. The nodes current position is represented as N_{ij}, the reconstruction is done for two scenarios as $s1 \in N \ and \ s2 \in N$. This process targets to find the scenarios based on the T_{ij} as $T_{ij} \in \{0, 1\}$. Here 0 denotes the $s1$ and 1 denotes the $s2$. For construct the efficient network with less energy consumption the paths nature such as path region (pr) and boundary of the path (pb) will be aggregated which can be formulated as,

$$E\left(T_{ij}\right) = E_{pr}\left(T_{ij}\right) + E_{pb}\left(T_{ij}\right) \tag{21}$$

where $E_{pr}\left(T_{ij}\right)$ is formulated as,

$$E_{pr}\left(T_{ij}\right) = \sum_{(i,j)} -ln\left(prob\left(T_{ij}\right)\right) \tag{22}$$

The T_{ij} could be 0 for $s1$ and 1 for $s2$. The $E_{pb}\left(T_{ij}\right)$ is defined as the forfeit for one hop relation between nodes which can be formulated as,

$$E_{pb}\left(T_{ij}\right) = \sum_{(i,j)\in\beth} \aleph e^{-\varphi||N_1 - malN||^2} \frac{1}{dis\left(N_1 - malN\right)} .\omega\left(T_{ij} \neq malN\right) \tag{23}$$

where,

$$\omega\left(T_{ij} \neq malN\right) \begin{cases} 1 & if \ T_{ij} \neq malN \\ 0 & otherwise \end{cases}, \beth \ is \ the \ set \ of \ N's$$

$dis\left(N_1 - malN\right)$represents the Euclidean distance between nodes and the malicious node, and φ is the control parameter which can be formulated as,

$$\varphi = \frac{1}{2EXP\left(||N_1 - malN||^2\right)} \tag{24}$$

The EXP denotes the expectation over theT_{ij}, for a nodes which is more likely close (one hop relation) to the malicious nodes will be given high forfeit and vice versa. This process helps to prevent the network from intruders that increase the efficiency and security of this work. The pseudocode for the intrusion scenario reconstruction is give below,

```
Intrusion Scenario Reconstruction ()
Input: $N_i = (N_1, N_1, \ldots, N_{ij}, \ldots, N_{iDm})$
Output: $E(T_{ij})$
Begin
   For all iterations do
      Generate searching vectors using (18)
      If ($K(T_i) < K(N_i)$)
            update search vectors $N_i$ to $T_i$
            Else
            Repeat searching untill maximum $s^n$
      End
      Discover optimal path using (20)
      Compute $E_{pr}$ and $E_{pb}$ using (22) and (23)
      Reconstruct network using (21)
End
End
```

5 Experimental Results

The experimental evaluation of the proposed MZWB approach for performance analysis is described in this section. The analysis results illustrates that the proposed MZWB method attains high security with efficient detection and prevention of intrusions. This section is further divided into four sub-sections they are simulation setup, use-case scenario, comparative analysis and research summary.

5.1 Simulation Setup

This sub-section explains about the simulation of the proposed MZWB method. Network simulator version 3.26 (NS-3) tool is used for performing simulation. This simulation tool affords the specifications easily which are correlated with the proposed MZWB method. This proposed MZWB method is experimented in 1000 m x1000 m simulation environment. The system specifications of this simulation are shown in Tab. 1 and the simulation parameters of this environment is described in Tab. 2.

Table 1: System specifications

Software specifications	OS	Ubuntu 14.04 LTS
	Network Simulator	NS-3.26
Hardware Specifications	Hard Disk	500GB
	RAM	4GB

Table 2: Simulation parameters

Parameters	Description
No. of Trusted Authority	1
No. of IoT devices	100
No. of Master Edge	1
No. of Honeypot Edge	2
Blockchain	1
Standard	IEEE 802.11
Packet time interval	0.1 s
Packet size	512 kb
No. of packets	∼1000
Generation rate of packers	12 packets per second
No. of Zones	5
Simulation time	100 s
Mobility	Random
Area	1000×1000
Modules	IoT module Wi-Fi module Internet module

5.2 Simulation Setup

In recent times, IoT devices are widely spread in all applications, especially for smart city to improve resource management. The smart city environment contains heterogeneous data which are sensitive so, it must be secure. But, unwanted intrusions increase the security threats that lead to security and privacy issues. These issues will be solved by the proposed MZWB method. This proposed MZWB approach can easily be adaptable for every application of IoT. Fig. 4 illustrates the diagrammatic representation of the smart city application scenario as an example that consists of numerous IoT devices which are used for various applications such as smart healthcare, smart parking, smart surveillance, smart shopping, smart building and smart lighting. Initially, all the IoT devices register themselves to the TA based on several metrics such as PUF, device ID, etc., for authentication. Store these credentials in blockchain to increase privacy. For efficient traffic management between the IoT devices, network graph is constructed dynamically by the edge node. Mitigate the malicious users in the smart city based on two-tier intrusion detection. Intrusion scenario is reconstructed to prevent the one-hop node over the network from various attacks. The sensors' tasks and applications are described in Tab. 3.

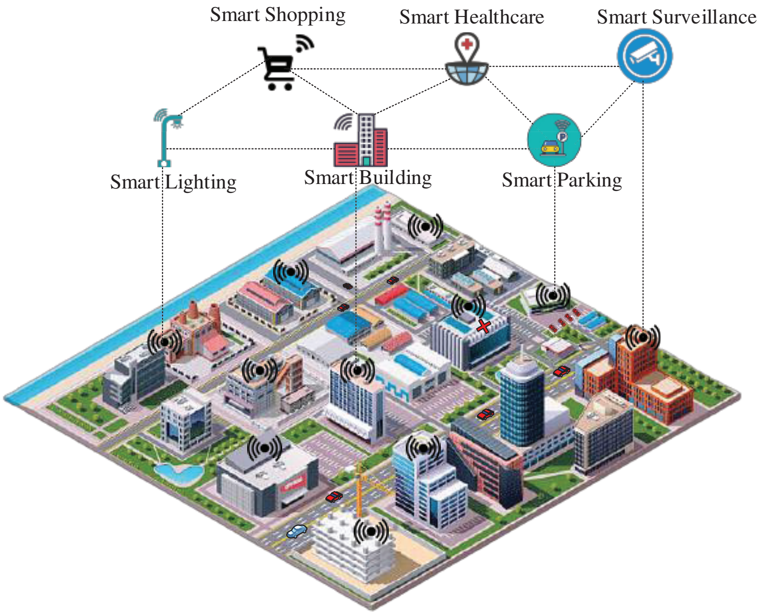

Figure 4: Smart city application scenario

Table 3: Applications and tasks of smart-city sensors

IoT devices	Tasks	Applications
Ultrasonic Sensor	To detect the distance based on directivity, and sound pressure	For smart vehicle parking purpose.
LDR Sensor	It detects the light intensity based on light wavelength	For smart street lighting
RFID sensor	To track and identify objects based on radio frequency	For smart shopping purpose
Infrared sensor	To detect the heat and motion of the objects	For smart surveillance management
Smart wearable	To monitor health conditions such as BP, heart beat rate etc.	For emergency health care
Temperature and Humidity sensor	To detect the temperature and humidity level inside the building	For smart building purpose

5.3 *Comparative Analysis*

(a) Impact of storage overhead

The storage overhead (So) is defined as the ratio of the total amount of bytes (T^b) stored to the original node size (N^{size}) which can be formulated as,

$$So = \frac{T^b}{N^{size}} \tag{25}$$

Fig. 5 represents the storage overhead comparison of proposed work to the existing works in terms of number of transactions. From the figure it is shown that, when the number of transactions getting increases storage overhead also increases among that our proposed work achieves less storage overhead this is due to exploitation of multi zone blockchain in which the IoT nodes are divided as zones and their information are stored as blocks, that improves the security and reduce complexity, and B-DAG based network construction also reduced the storage overhead as it reduces the energy consumption by ensuring the connection between the nodes. The existing works SIDS and ASR limits with effective network construction and lacks with employing blockchain technology leading to increase in storage overhead. The proposed work achieves storage overhead rate of 2 which is higher than the existing approaches.

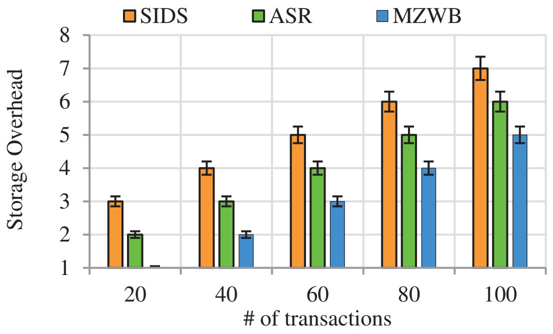

Figure 5: Storage overhead *vs.* # of transactions

(b) Impact of Response time

Response time (τ) is amount of time passed among starting and ending of tasks which can be formulated as,

$$\tau = T^{start} - T^{end} \tag{26}$$

where $T^{start} - T^{end}$ represents the passed time between the tasks (T) between start to end.

Fig. 6 represents the response time comparison of proposed work to the existing works in terms of number of devices. From the Fig. 6 it is shown that, when the number of devices getting increases response time also increases. The proposed MZWB method achieves less response among the existing works this is due to secure authentication using EBA algorithm process in which the malicious nodes are pruned out initially and only legitimate nodes are taken for further processing hence there in no chance the packet dropping which reduce the response time whereas in the existing works SIDS and ASR lacks with authentication hence leads to high packet dropping thereby increasing high response time. The proposed work achieves less response time of 8 ms than the existing works.

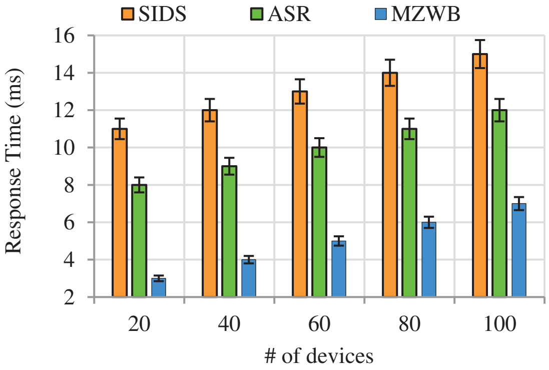

Figure 6: Response time *vs.* # of devices

(c) Impact of Accuracy

The process of accurate detection of attacks even though the number of devices getting increased in known as accuracy (Ac) which can be formulated as,

$$Ac = \frac{Ʒ + \varrho}{Ʒ + ℄ + \varrho + ʇ} \tag{27}$$

where Ʒ *and* ϱ denotes the true positive and true negative respectively while ℄ *and* ʇ denotes the false positive and false negative respectively.

Fig. 7 represents the accuracy comparison of proposed work with existing works in terms of number of devices. From the Fig. 7 it is shown that, when the number of devices is getting increased accuracy rate also increased. The proposed MZWB method achieves better accuracy than the existing works this is due to proposing of two-tier intrusion detection system in which first tier exploits DCNN algorithms for malicious node classification which classifies three classes as normal, malicious and suspicious. The second tire exploits GAN algorithm and classify the suspicious nodes as normal and malicious which improves the accuracy of the model. The existing works SIDS and ASR lacks with classification of suspicious packets which leads to security threats and reduce the accuracy. The proposed work achieves accuracy of 20.2% higher than the existing works.

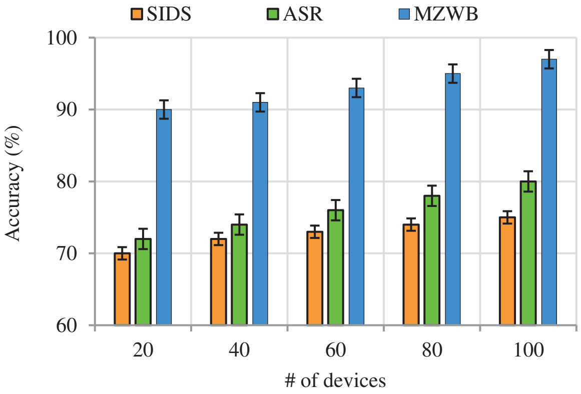

Figure 7: Accuracy *vs.* # of devices

(d) Impact of Attack Detection Rate

The rate of attacks detection when the increasing number of devices is known as attack detection rate which can be formulated as,

$$ADR = \frac{attacks\ detected}{Increasing\ devices} \tag{28}$$

Fig. 8 represents the attacks detection rate comparison of proposed and existing works with respect to number of devices in which when the number of devices getting increases the attack detection rate also getting increases. From that Fig. 8, our proposed MZWB achieves high attack detection rate due to two-tier intrusion detection system and intrusion reconstruction scenario. In two-tier intrusion detection system, the first tier exploits DCNN algorithms for malicious node classification which classifies three classes as normal, malicious and suspicious. The second tier exploits GAN algorithm and classify the suspicious nodes as normal and malicious. In intrusion reconstruction scenario, the attacks paths are discovered by using IMO algorithm, and reconstruction is done by using graph cut algorithm which improves the attack detection rate. The existing work ASR performs attack detection by constructing attack detection graph whereas node properties, dynamicity are not considered leads to inefficient attack detection thereby decreasing in attack detection rate. The proposed work achieves attack detection rate of 0.2 higher than the state of the art works.

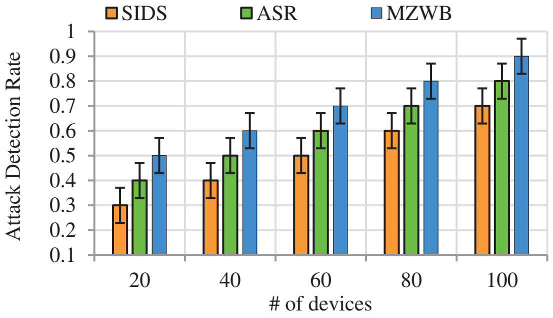

Figure 8: Attack Detection rate *vs.* # of devices

(e) Impact of Attack Detection Rate

Precision ($\mathfrak{p}$) is defined as the ratio of $\mathfrak{z}$ to the sum of $\mathfrak{z}$ *and* $\mathfrak{L}$ rates respectively which can be formulated as,

$$\mathfrak{p} = \frac{\mathfrak{z}}{\mathfrak{z} + \mathfrak{L}} \tag{29}$$

Fig. 9 represents the precision comparison of proposed work to the existing works with respect to number of devices. From the figure it is shown that, when the number of devices getting increases precision rate also increases among that our proposed work experiences drastic increase which is due to secure authentication process and two-tier intrusion detection system. The secure authentication process exploits EBA algorithm which provides legitimacy to the IoT nodes by considering several metrics and random ID is also generate and updated periodically. The accurate attacks detection in the network is carried out by two-tier method in which first tier exploits DCNN for classifying the nodes as malicious, normal, and suspicious, and the second tier exploits GAN which classifies the suspicious nodes as normal and malicious. The above mentioned improves the precision rate while the existing works SIDS and ASR limits with detection of known attacks which degrade the precision rate thereby affecting accuracy. The proposed work achieves precision rate of 21% higher than the existing works.

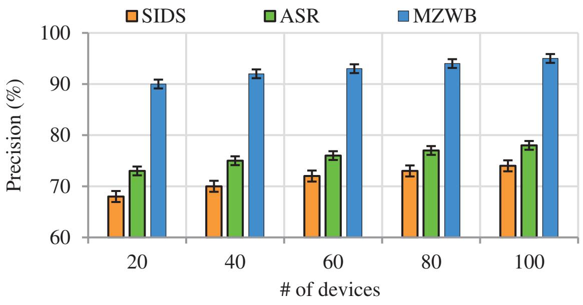

Figure 9: Precision *vs.* # of devices

(f) Impact of Attack Detection Rate

Recall ($\mathfrak{R}$) rate is defined as the ratio of $\mathfrak{Z}$ to the sum of $\mathfrak{Z}$ *and* $\mathfrak{L}$ respectively which can be formulated as,

$$\mathfrak{R} = \frac{\mathfrak{Z}}{\mathfrak{Z} + \mathfrak{L}} \tag{30}$$

Fig. 10 shows the recall rate comparison of proposed work to the existing works with respect to no. of devices in which the number of devices increases recall rate also increases. The proposed work achieves high recall rate among the existing works even though the number of users getting increased this is due to intrusion reconstruction scenario. This process utilizes IMO and graph cut algorithms for discovery of attack path and reconstruction respectively by considering various nodes properties and heterogeneity whereas the state of the art works ASR employs attack reconstruction method even though they achieve less recall rate due to static manner graph construction while the attacks held by the attackers are dynamic in nature leads to less recall rate. The proposed work achieves 13% higher than the existing works.

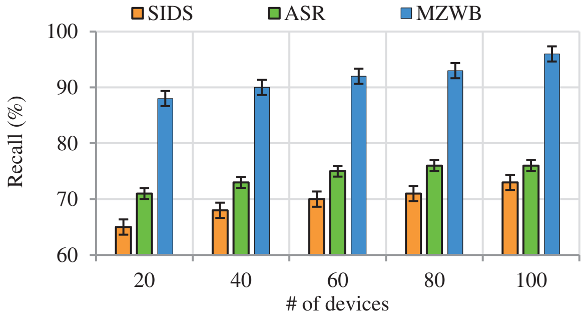

Figure 10: Recall *vs.* # of devices

(g) Impact of F-measure

F-measure is defined as the ratio of product of $\mathfrak{p}$ *and* $\mathfrak{R}$ to the sum of $\mathfrak{p}$ *and* $\mathfrak{R}$ with multiplication of 2 which can be formulated as,

$$F - measure = 2 * \frac{\mathfrak{p} \times \mathfrak{R}}{\mathfrak{p} + \mathfrak{R}} \tag{31}$$

Fig. 11 represents the F-measure comparison of proposed work to existing works with respect to number of devices. From the figure it is shown that, when the number of devices getting increases F-measure also increases among that our proposed work achieves high F-measure rate this is due to proposing of secure authentication process and intrusion reconstruction scenario. The secure authentication process exploits EBA for ensuring legitimacy of the users in which the illegitimate nodes are pruned out the initial stage, and in attack reconstruction scenario the paths where the attack held are discovered and reconstructed by using IMO algorithm and graph cut algorithm respectively in which properties of node and its heterogeneity are considered which improves the F-score rate whereas the existing work SIDS lacks with drastically less F-measure rate as it did not considers legitimacy of the node thereby achieving less precision and recall rates respectively. The proposed work achieves F-measureof 11 higher than the existing works. The full comparisons of the existing works are shown in Tab. 4.

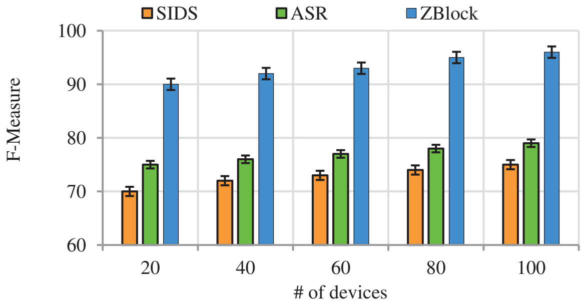

Figure 11: F-Measure *vs.* # of devices

Table 4: Comparison between MZWB and existing works

Approaches	Objective	Methods/Algorithms	Comments
SIDS	Supervised approach based three layer intrusion detection systems for cyber-attack detection in IoT networks.	Three ML algorithms for identification of device, anomaly detection, and attack detection respectively.	• Performance degradation • High complexity • Detect only known attacks
ASR	Attack graph and data mining based attack scenario reconstruction technique with known liabilities.	Four step methods such as mapping of alerts, generation of attack sequence, clustering of attack sequence, and improvement of attack scenario.	• Low false positive rate • Less attack detection accuracy • Not considered heterogeneity of nodes

(Continued)

Table 4: Continued

Approaches	Objective	Methods/Algorithms	Comments
DIFS	Intrusion detection system for IIoT-Fog environment using deep learning techniques.	Local gated recurrent unit and multi-head self-attention layer.	• Less detection accuracy • Low false positive rate
BF-IoT	Blockchain based approach for investigation of digital forensics in IoT	IoT forensic chain framework for providing security, invariability and trackability.	• Scalability issues • Legitimacy is not ensured • Less recall rate
MZWB	Attack detection and prevention in edge enabled IoT devices using Multi-zone-wise blockchain based on forensic evidence.	EBA algorithm for ensuring legitimacy, B-DAG for network construction, DCNN and GAN for IDS, and IMO and graph cut algorithm for reconstruction of attack scenario.	• No scalability issues • Better performance • High false positive rate • High detection accuracy • Less complexity

5.4 Security Analysis

The security of the IoT devices is mainly considered in the proposed MZWB method. Security and privacy issues are occurred due to various attacks by malicious nodes. Various attacks are mitigated by detecting and preventing it in the proposed MZWB approach and such attacks are as follows,

- DDos Attack: This attack is caused by transmitting unwanted packets by multiple malicious nodes to increase the traffic that increases the risk of accessing the network by the legitimate nodes. It is occurred in perception layer. In the proposed MZWB method, this attack is mitigated by performing authentication to validate the legitimacy of the IoT nodes using Multi-zone-wise blockchain.

- IP Spoofing: This attack is caused by duplicating the IP address of the legitimate node for accessing the network. To overcome this attack, we perform authentication in the proposed MZWB method initially, so this attack can’t tamper the network. Authentication is performed by considering several credentials such as PUF, MAC address, device ID and location of the node to mitigate this attack.

- Replay Attack: The nature of this attack is to act as legitimate IoT nodes to access the network. So it is difficult to mitigate this attack. To mitigate this attack, two-tier intrusion detection is performed in which the suspicious nodes are classified using GAN in the proposed MZWB method. In addition, all the transactions are recorded in the Multi-zone-wise blockchain to mitigate replay attack.

• Data Tampering: This attack is caused by modify or destroy the data. To mitigate this attack, all the transactions are recorded in Multi-zone-wise blockchain in this way we mitigate this attack effectively.

5.5 Research Summary

This subsection explains the performance of the proposed work. Figs. 5–11 illustrates the comparison of the performance metrics in storage overhead, response time, accuracy, attack detection rate, precision, recall, and f-measure. The proposed work achieved less storage overhead due to DAG-based network construction and Multi-zone-wise blockchain. By performing authentication and two-tier intrusion detection system and intrusion scenario reconstruction, this research achieves a high attack detection rate, accuracy, precision, recall, and f-measure. Tab. 5 illustrates the numerical analysis of the proposed and existing works, which provides the average values of the performance metrics. The research highlights of this research are listed as follows,

- The network's security is ensured by performing secure authentication in which the enhanced blowfish algorithm is utilized to create the secret key for the IoT devices for authentication.
- To reduce the complexity, the network is constructed as a graph structure using Bayesian DAG by considering the number of transmissions, link stability, intimacy, location, and distance, reducing the overhead during packet transmission.
- The intrusions are detected by proposing a two-tier intrusion detection system, in which the first tier IDS is performed by extracting the packet features for detecting known patterns. The unknown or suspicious patterns are sent to the next level IDS by extracting the evidence from the blockchain in order to classify the suspicious packets into normal or malicious.
- The attack scenario is reconstructed by improved monkey optimization and graph cut algorithm, which dynamically reconstructs the scenario for preventing the legitimate nodes from intrusions that improve the performance of the proposed work.
- The attacks in the network are mitigated by implementing MZ blockchain-based network in which the transactions between the nodes are stored and verified by the blockchain to enhance scalability and reduce complexity.

Table 5: Numerical analysis of proposed and existing works

Performance Metrics	SIDS	ASR	MZWB
Storage overhead	5 ± 0.3	4 ± 0.2	3 ± 0.1
Response time (ms)	13 ± 0.4	10 ± 0.3	5 ± 0.2
Accuracy (%)	72.8 ± 0.2	76 ± 0.2	93.2 ± 0.2
Attack detection rate	0.5 ± 0.3	0.6 ± 0.2	0.78 ± 0.1
Precision (%)	71.4 ± 0.4	75.8 ± 0.3	92.8 ± 0.2
F-measure	72.8 ± 0.2	77.1 ± 0.2	93.2 ± 0.1

6 Conclusion and Future Work

The MZWB method is proposed to improve security with high scalability and low latency in the IoT network. First, all the IoT nodes are authenticated in the Multi-Zone-Wise blockchain to validate the nodes' legitimacy using Enhanced Blowfish Algorithm by considering device ID, PUF, MAC address, and location. Then, to reduce the traffic of IoT devices, the network graph is constructed by the edge node using the B-DAG method based on link stability, location, distance, intimacy, and several transmissions. Improve the intrusion detection performance by performing two-tier detection in the edge layer. In the first tier, extraction of packet features to classify the packets in terms of normal, malicious, and suspicious using DCNN. The local edge node prunes the malicious node. In the second tier, the evidence is further classified by the global edge node based on current location, context type, and count using GAN to classify the suspicious evidence as normal and malicious. Finally, to prevent the intrusions by detecting the attack path using the IMO algorithm and reconstructing the network using the graph cut method. The proposed MZWB method achieves better performance when compared with the existing. In the future, we will mitigate various types of attacks in the environment using Multi-zone-wise Blockchain.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori and R. N. Mir, "A novel multi-xgent and multilayered game formulation for intrusion detection in internet of things (IoT)," *IEEE Access*, vol. 8, pp. 98481–98490, 2020.

[2] X. C. Yin, Z. G. Liu, L. Nkenyereye and B. Ndibanje, "Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach," *Sensors (Switzerland)*, vol. 19, no. 22, 2019, https://doi.org/10.3390/s19224952.

[3] G. Kumar, R. Saha, C. Lal and M. Conti, "Internet-of-forensic (IoF): A blockchain based digital forensics framework for IoT applications," *Futur. Gener. Comput. Syst*, vol. 120, pp. 13–25, 2021.

[4] A. Amouri, V. T. Alaparthy and S. D. Morgera, "A machine learning based intrusion detection system for mobile internet of things," *Sensors (Switzerland)*, vol. 20, no. 2, 2020, https://doi.org/10.3390/s20020461.

[5] M. Zhong, Y. Zhou and G. Chen, "Sequential model based intrusion detection system for IoT servers using deep learning methods," *Sensors (Switzerland)*, vol. 21, no. 4, pp. 1–21, 2021.

[6] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," *Sensors (Switzerland)*, vol. 19, no. 9, 2019, https://doi.org/10.3390/s19091977.

[7] K. Fotiadou, T. H. Velivassaki, A. Voulkidis, D. Skias, S. Tsekeridou *et al.* "Network traffic anomaly detection via deep learning," *Inf*, vol. 12, no. 5, pp. 1–17, 2021.

[8] Z. A. Khan and U. Abbasi, "Reputation management using honeypots for intrusion detection in the internet of things," *Electron*, vol. 9, no. 3, pp. 1–30, 2020.

[9] B. S. Khater, A. W. B. A. Wahab, M. Y. I. Bin Idris, M. A. Hussain and A. A. Ibrahim, "A lightweight perceptron-based intrusion detection system for fog computing," *Appl. Sci*, vol. 9, no. 1, 2019, https://doi.org/10.3390/app9010178.

[10] M. Zhou, L. Han, H. Lu and C. Fu, "Intrusion detection system for IoT heterogeneous perceptual network based on game theory," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 284, pp. 459–471, 2019.

[11] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things," *IEEE Internet Things J*, vol. 7, no. 1, pp. 379–388, 2020.

[12] S. Kably, M. Arioua and N. Alaoui, "Lightweight blockchain network architecture for IoT devices," in *the 3rd Int. Symp. on Advanced Electrical and Communication Technologies (ISAECT2020),* Kenitra-Rabat, Morocco, pp. 1–6, 2020, https://doi.org/10.1109/ISAECT50560.2020.9523686.

[13] S. Kably, M. Arioua and N. Alaoui, "Lightweight direct acyclic graph blockchain for enhancing resource-constrained IoT environment," *Computers Materials & Continua*, vol. 71, no. 3, pp. 5271–5291, 2022.

[14] A. S. Alqahtani, K. A. Abuhasel and M. Alquraish, “A novel decentralized analytical methodology for cyber physical networks attack detection,” *Wirel. Pers. Commun*, no. 0123456789, 2021, https://doi.org/10.21203/rs.3.rs-346046/v1.

[15] C. Liang, B. Shanmugam, S. Azam, A. Karim, A. Islam *et al.,* “Intrusion detection system for the internet of things based on blockchain and multi-agent systems,” *Electron*, vol. 9, no. 7, pp. 1–27, 2020.

[16] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He *et al.,* “Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems,” *IEEE Internet Things J.*, vol. 4662, no. 0, 2021, https://doi.org/10.1109/JIOT.2021.3053842.

[17] A. A. Elsaeidy, A. Jamalipour and K. S. Munasinghe, “A hybrid deep learning approach for replay and DDoS attack detection in a smart city,” *IEEE Access*, vol. 9, pp. 154864–154875, 2021.

[18] K. Zhang, F. Zhao, S. Luo, Y. Xin and H. Zhu, “An intrusion action-based IDS alert correlation analysis and prediction framework,” *IEEE Access*, vol. 7, pp. 150540–150551, 2019, https://doi.org/10.1109/ACCESS.2019.2946261.

[19] W. Li, Y. Wang, J. Li and M. H. Au, “Toward a blockchain-based framework for challenge-based collaborative intrusion detection,” *Int. J. Inf. Secur*, vol. 20, no. 2, pp. 127–139, 2021.

[20] Y. Zhang, P. Li and X. Wang, “Intrusion detection for IoT based on improved genetic algorithm and deep belief network,” *IEEE Access,* vol. 7, no. c, pp. 31711–31722, 2019.

[21] I. H. Sarker, Y. B. Abushark, F. Alsolami and A. I. Khan, “IntruDTree: A machine learning based cyber security intrusion detection model,” *Symmetry (Basel)*., vol. 12, no. 5, pp. 1–15, 2020, https://doi.org/10.3390/SYM12050754.

[22] F. J. Mora-Gimeno, H. Mora-Mora, B. Volckaert and A. Atrey, “Intrusion detection system based on integrated system calls graph and neural networks,” *IEEE Access*, vol. 9, pp. 9822–9833, 2021.

[23] S. Sibi Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi and B. Raman, “Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks,” *IEEE Access*, vol. 8, pp. 169944–169956, 2020.

[24] O. Alkadi, N. Moustafa, B. Turnbull and K. K. R. Choo, “A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks,” *IEEE Internet Things J*, vol. 8, no. 12, pp. 9463–9472, 2021.

[25] M. A. R. Al Amin, S. Shetty, L. Njilla, D. K. Tosh and C. Kamhoua, “Hidden markov model and cyber deception for the prevention of adversarial lateral movement,” *IEEE Access*, vol. 9, pp. 49662–49682, 2021.

[26] S. Ho, S. Al Jufout, K. Dajani and M. Mozumdar, “A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network,” *IEEE Open J. Comput. Soc.*, vol. 2, no. January, pp. 14–25, 2021.

[27] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour and H. Janicke, “RDTIDS: Rules and decision tree-based intrusion detection system for internet-of-things networks,” *Futur. Internet*, vol. 12, no. 3, pp. 1–14, 2020.

[28] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu *et al.,* “Hierarchical adversarial attacks against graph neural network based IoT network intrusion detection system,” *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9310–9319, 2022, https://doi.org/10.1109/JIOT.2021.3130434.

[29] R. Qaddoura, A. M. Al-Zoubi, H. Faris and I. Almomani, “A multi-layer classification approach for intrusion detection in IoT networks based on deep learning,” *Sensors*, vol. 21, no. 9, pp. 1–21, 2021.

[30] H. Hu, J. Liu, Y. Zhang, Y. Liu, X. Xu *et al.,* “Attack scenario reconstruction approach using attack graph and alert data mining,” *J. Inf. Secur. Appl*, vol. 54, 2020, https://doi.org/10.1016/j.jisa.2020.102522.

[31] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos and P. Burnap, “A supervised intrusion detection system for smart home IoT devices,” *IEEE Internet Things J*, vol. 6, no. 5, pp. 9042–9053, 2019.

[32] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty and M. Ryan, “Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment,” *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7704–7715, 2021.

[33] S. Li, T. Qin and G. Min, “Blockchain-based digital forensics investigation framework in the internet of things and social systems,” *IEEE Trans. Comput. Soc. Syst*, vol. 6, no. 6, pp. 1433–1441, 2019.