Hindawi
Security and Communication Networks
Volume 2023, Article ID 3171334, 10 pages
https://doi.org/10.1155/2023/3171334

Research Article

IOT and Blockchain-Based Cloud Model for Secure Data Transmission for Smart City

Liwa H. Al-Farhani,[1] **Yahya Alqahtani**,[2] **Hamdan Ali Alshehri**,[2] **R. John Martin**,[2] **Sachin Lalar**,[3] **and Rituraj Jain**[4]

[1]*System Analysis, Control, and Information Processing, Academy of Engineering, RUDN University, Moscow, Russia*
[2]*Faculty of Computer Science and Information Technology, Jazan University, Saudi Arabia*
[3]*Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India*
[4]*Department of Electrical and Computer Engineering, Wollega University, Nekemte, Ethiopia*

Correspondence should be addressed to Rituraj Jain; jainrituraj@wollegauniversity.edu.et

Received 5 May 2022; Revised 6 December 2022; Accepted 2 May 2023; Published 20 May 2023

Academic Editor: Bharat Bhushan

The widespread use of the Internet of Things (IoT) technology has both good and bad things about it. There must be a full and reliable security system in place for the Internet of Things so that things can work together in a safe way and intrusions cannot happen. There are now many more ways to keep the Internet of Things safe, thanks to a detecting system. As machine learning and deep learning technologies have become better, a lot of good intrusion detection systems have been made. This kind of study is covered. These two types of security are compared in this study. The current machine-based intrusion detection system is broken down into more detailed categories based on detection technology, data source, architecture, and operating method. These categories are as follows: It is talked about how IoT security will grow in the future and how to understand its intrusion detection system too. In this paper, a cloud-based blockchain security model has been presented for secure data transmission over IoT.

1. Introduction

Smart cities, education, entertainment, energy distribution, financial services, healthcare, tourism, pandemic situation [1], data accumulation [2], and transportation all benefit from the increasing intelligence and widespread usage of Internet of Things (IoT) devices. However, commercialization is being pursued by both the private sector and the academic community. IoT device security is often neglected, putting consumers at risk and contributing to ecosystem imbalances. For example, a manufacturing employee inserting a virus-infected USB stick into a machine, a hospital's MRI machine compromised by malware, or a hacker directing an infusion pump to inject a lethal dose of a drug can have serious consequences. According to [3], by 2020, the cybercriminal damage budget will reach $6 billion per year, and there will be 50 billion IoT devices to protect. Furthermore, after the IoT is attacked [4], it will not only affect the IoT itself but also the entire ecosystem, including networks, applications, social platforms, and servers, that is, in the IoT system, as long as a single component or communication channel is destroyed, it may cause part or the entire network to be paralyzed. Therefore, while paying attention to the convenience brought by the Internet of Things, it is also necessary to consider the vulnerability of the Internet of Things [5].

Traditional security solutions already cover server, network, and cloud storage, most of these solutions can be deployed in IoT systems. Among them, cryptography [6] is used as the basis for ensuring information security, and the critical centre interacts with the sensor network or other sensor network convergence points to realize the essential management of the nodes in the network; the commonly used methods for data security protection include homomorphic encryption and ciphertext retrieval. and other security technologies such as authentication and access.

Control mechanisms, secure routing protocols, and network situational awareness and assessment techniques are essential security solutions. The diversity and heterogeneity of IoT make IoT system security different from traditional system security. (1) More and more physical devices are connected to wireless networks, which will expose more security issues to people with malpractice, which can lead to severe consequences, such as attacks on cars or infusion pumps, which can lead to casualties. (2) IoT security is a unique challenge, as the opponent is different from the past. It is no longer a hacker who seeks money or creates trouble but a national hacker system, facing a national-level cyber war. For example, in August 2017, a Saudi chemical plant was attacked by hackers, causing a large-scale explosion, which disrupted the production of petrochemical products. (3) IoT devices are produced by different companies and are eventually pieced together. Even if there is only one weak link, loopholes may arise. For example, if the car communication system company does not update the software, the car will be vulnerable to attack. (4) The environments where IoT devices are located are different. For example, no one pushes the patch to the connected refrigerator in time in-home life. In contrast, in an industrialized environment, patching a machine means that the device needs to stop working, which will cause certain economic losses. However, loss and the risk of hacking would be much lower than loss. Therefore, traditional system security techniques are no longer suitable for the new IoT environment.

Since its introduction into IoT security, experts have been working to improve the intrusion detection system (IDS) [7]. When it comes to protecting the integrity, privacy, and availability of a network or system, IDS is a proactive protection technique that employs a mix of software and hardware. Deep learning, machine learning, visual learning, and reinforcement learning have become more prominent with the rise of artificial intelligence and large data. They have achieved great success in image recognition and natural language processing. At the same time, on the Internet of the Things security field, many studies have combined intrusion detection systems with artificial intelligence technology and have achieved specific results. Early intrusion detection system reviews focused more on traditional IoT security techniques, such as feature selection algorithm-based intrusion detection system review by author [8], network-based intrusion detection systematic review of host-based intrusion detection by author [9], and a systematic review of intrusion detection based on network threat classification by author [10]. The previous literature provides researchers with a lot of valuable information.

The current machine-based intrusion detection system is broken down into more detailed categories based on detection technology, data source, architecture, and operating method. These categories are as follows: It is talked about how IoT security will grow in the future and how to understand its intrusion detection system too. An intrusion detection system is required to ensure network security and detect malicious attacks. This paper first compares the difference between traditional system security and the current stage of IoT security and classifies the intrusion detection system in detail from detection technology, data source, architecture, and working methods. Discussions and evaluations are conducted, and future directions are elaborated. To sum up, whether it is a neural network model, a swarm intelligence optimization algorithm, or a traditional machine learning algorithm, they interact to provide a better solution for the intrusion detection system.

2. Intrusion Detection System Classification

Software and hardware are used to monitor a network or system to look for suspicious activity and send out alerts as soon as possible, protecting system resources such as integrity, privacy, and availability. In contrast to other security technologies, intrusion detection technology is a proactive defense technology that can stop unknown attacks [11]. A way to think about the intrusion detection system is the following way: Firewall: If you think of it as your house's front door lock, you would think of an intrusion detector as your house's security system. When the thief gets inside the building or the employees inside act like they are from another country, the monitoring system can start to go off. So, the intrusion detection system should be "placed" on the link where the traffic data of interest must pass through, so that it can see if there is an attack. Shown in Figure 1 is how its system is put together. The event generator gets events from all over the network and sends them to other parts of the system. The event analyzer looks at the events and tells the response unit if there is something wrong with them. In the event database, process data is kept. The response unit responds to the analysis results in a way that is based on the data. This paper grouped intrusion detection systems into groups based on their data sources, detection methods, working methods, and architecture. It is shown in Figure 2.

2.1. Classification Based on Detection Methods. From the perspective of detection methods, intrusion detection techniques are generally divided into misuse and anomaly detection techniques.

2.1.1. Based on Misuse Detection Technology. Misuse detection technology [12] is based on the principle of pattern matching, collects the characteristics of attack behavior, and establishes a signature database for it. When the monitored user behavior matches the records in the signature database, the system judges the behavior as an intrusion. Misuse detection technology can reduce the false-positive rate. Still, the false-negative rate will also increase. Once the attack characteristics change, the misuse detection technology will become incompetent. Existing misuse detection techniques are generally divided into misuse detection methods based on expert systems [13], misuse detection methods based on state transition analysis [14], keyboard monitoring-based misuse detection methods [15], and conditional probability-based methods.

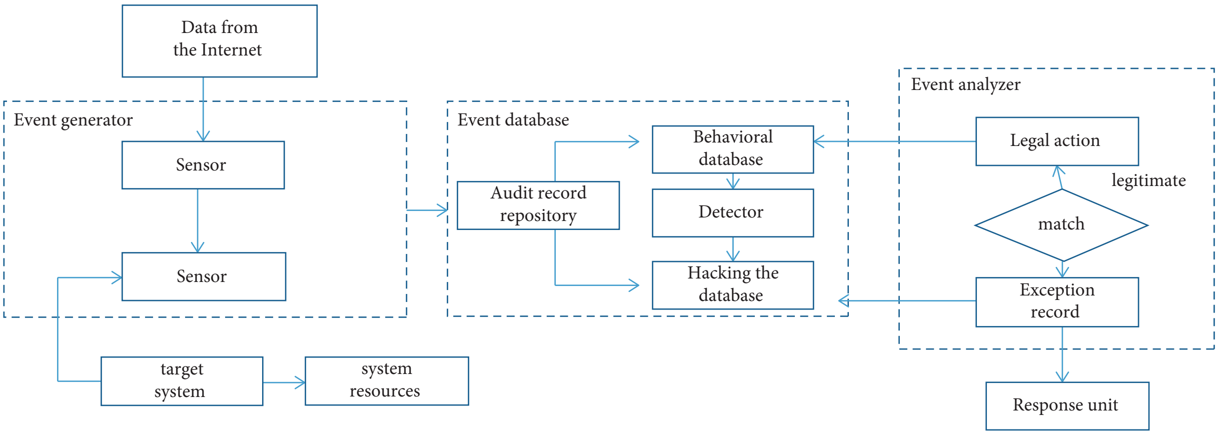

Figure 1: Intrusion detection system architecture.

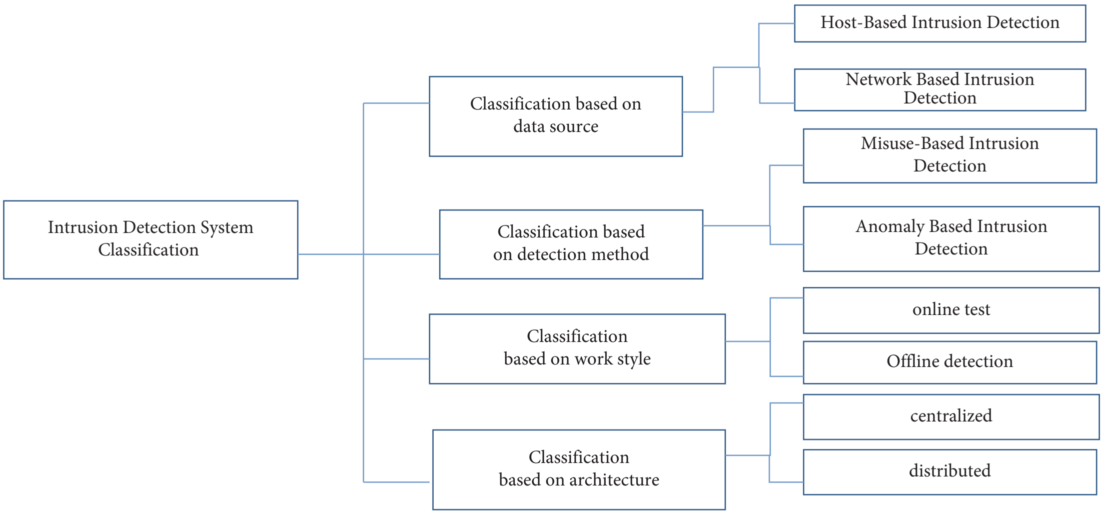
Intrusion Detection System Classification
Classification based on data source
Host-Based Intrusion Detection
Network Based Intrusion Detection
Classification based on detection method
Misuse-Based Intrusion Detection
Anomaly Based Intrusion Detection
Classification based on work style
online test
Offline detection
Classification based on architecture
centralized
distributed

Figure 2: Classification framework of intrusion detection system.

2.1.2. Based on Anomaly Detection Technology. Anomaly detection techniques [12] are based on statistical analysis principles. First, we determine the characteristics of normal behavior and describe it with quantitative methods. When the user behavior deviates from the regular operation, it is defined as aggressive behavior. The efficiency of anomaly detection techniques largely depends on the completeness of typical user characteristics and the detection frequency. Unknown attacks can be effectively detected because each episode does not need to be defined. At the same time, the system can also adapt to user behavior changes through self-optimization and adjustment. However, with the continuous improvement of the model, the anomaly detection technology will consume more system resources, and the attack behavior at this stage is becoming more and more intelligent, so the ability to detect unknown attacks is gradually weakened. Existing anomaly detection techniques are generally divided into anomaly detection techniques based on a neural network [16], anomaly detection techniques based on pattern prediction [17], and anomaly detection techniques based on data mining [18].

2.2. Classification Based on Data Source. From the perspective of data sources, intrusion detection systems can generally be divided into host-based intrusion detection systems (Host Intrusion Detection System, HIDS) and network-based intrusion detection (Network Intrusion Detection System, NIDS). The comparison of the two is shown in Table 1.

2.2.1. Host-Based Intrusion Detection. Host or server system attacks are the main thing that HIDS [19, 20] looks for and responds to. People who work with HIDS use two main techniques, namely, anomaly detection techniques and misuse detection techniques. Using misuse detection technology and anomaly detection technology, the author [20] came up with a way to keep an eye on the data that the host collects. This system used log file analysis and BP neural network technology to keep an eye on the data the host collects. Consequently, it can help improve the detection rate and accuracy of the search. The author came up with a host-based botnet intrusion detection system that uses a genetic algorithm of anomaly detection technology to look at and

Table 1: Comparison of HIDS and NIDS.

Category	HIDS	NIDS
False positive	Few	A certain amount of
Underreporting	Related to technical level	Related to data processing capabilities (inevitable)
System deployment and maintenance	Regardless of network topology	Related to network topology
Detection rules	A small amount	A lot
Detection features	Event and signal analysis	Feature code analysis
Security strategy	Basic security policy (point policy)	Run security policy (line policy)
Security limitations	All events arriving at the host	Unencrypted in transit and nonconfidential information
Security risks	Violation	Method or means of attack

process each received data packet to see if there is deception caused by an outside attack to protect the system. HIDS can also protect the hosts it monitors from things such as the integrity of files, network packets sent to other hosts, the system registry and system log files, and more, as well as other things. They made a host-based intrusion system for Microsoft Windows XP and used pattern matching technology to look at the security event log file of Microsoft Windows XP to find out what kind of things were going on. There is an intrusion if the logs all say the same thing about the same thing. The author came up with a host intrusion detection system with a layered structure. Layered protection is used to keep the host safe in real time. In the first layer, a packet sniffer is used to record all the data packets that pass through the network. Sensitive information and features are then extracted from this data. The Naïve Bayes algorithm is used in the second layer to classify packets based on the sensitive data and features extracted from the first layer [21–23].

Compared with traditional security defense technologies, HIDS is cost-effective, has a low false-positive rate, and is suitable for encryption and exchange environments. But the disadvantage is that it relies more on the inherent log analysis capabilities of the host, and the process of auditing logs is highly vulnerable; HIDS can only monitor specific applications on the host, and the detection range will be limited; the cost of fully deploying HIDS is exceptionally high. It will also affect the performance of the host.

2.2.2. Network-Based Intrusion Detection. When the network card is in promiscuous mode, NIDS [24, 25] can watch the communication service on the whole network segment in real time. It does not matter if you use host-based intrusion detection or network-based intrusion detection. They all have some problems, so they keep getting better. They came up with a better way to detect network intrusions. First, they put a server node in a specific part of the network and then they put the intrusion detection system on the server before each data packet reaches the destination host. The destination host can not get data packets from outside the network. Even if some data packets are sent directly to it, they have to be sent to the server to be checked before they can keep going. If the server finds that the data packet is an invasion, throw it away right away. The system not only saves money, but it also has very good detection rates. The author came up with a way to detect network intrusions based on data mining. It uses two substages of data mining, called K-means clustering and FP-growth algorithms, to do this. Unsupervised K-means is used to find new attacks in this design. FP-growth is used to find out which attacks happen the most often. Data mining methods are a good addition to intrusion detection systems. Their cooperation helps high-level network records cut down on the amount of analysis the intrusion detection system has to do, which reduces the amount of time it takes and improves the system's accuracy. It is very important to make traditional network intrusion detection systems work in a virtual machine environment. This is what the author came up with a virtual machine-based network intrusion detection system. The intrusion detection system was installed in the virtual machine monitoring programme, and it was able to get network packets from the virtual bridge. It is a device in a virtual machine that moves packets from a physical device to a virtual interface. This is called a "virtual bridge." In the system implementation, a process is first made and then a virtual interface is given to the process. The process is in charge of detecting the data packets that are found in the virtual bridge to protect the virtual machine.

Network-based intrusion detection technology can detect and record unsuccessful attack behaviors, making it impossible for attackers to transfer evidence. In addition, it is much concealed and does not affect system performance when NIDS detects and responds to malicious behaviors in real-time. But the disadvantage is that NIDS can only see the communication of the directly connected network segment and cannot detect the data packets in different network segments, so the detection range is also limited. Detecting and handling encrypted sessions can also be challenging.

2.3. Classification Based on Architecture. From the architectural point of view, intrusion detection systems can be divided into centralized and distributed. The centralized intrusion detection systems analysis engine and control centre are in one system and cannot operate remotely. This architecture is simple, will not leak privacy due to communication, and will not affect network bandwidth. However, this method has poor scalability and configurability. On the other hand, the analysis engine and the distributed intrusion detection system are two systems that can be operated remotely through the network. At present, most intrusion detection systems are distributed. This architecture is highly scalable and secure, but it is also expensive to maintain.

2.4. Classification Based on Work Style. The intrusion detection system can be divided into online detection and offline detection from the working mode. Online detection can monitor data generation and analyze it in real-time. Although this method can protect the system in real-time, it is not easy to ensure real-time performance when the system is extensive in scale. On the other hand, offline detection analyses the intrusion behavior after it occurs. This method can handle many events but cannot promptly provide protection measures for the system.

3. IoT-Based Smart City

To build and develop a smart city, the construction of the Internet of Things is the technical support and guarantee, and it is also the critical link between success and failure. The Internet of Things (IoT) is a rapidly emerging concept in modern wireless communication scenarios [1]. MIT first proposed this concept in 1999. Its basic idea is to use ubiquitous things or objects, such as radio frequency identification (RFID) tags, sensors, actuators, and mobile phones, to provide people with various real-time helpful information. There is no doubt that the most extraordinary charm of the concept of the Internet of Things lies in its multifaceted impact on people's daily life, thinking, and behavior. From the point of view of private users, the biggest attraction of the Internet of Things is the impact on the field of domestic life. The smart home will assist people's daily lives. Electronic technology is conducive to prolonging the average life expectancy. The convenience of information acquisition will provide residents with higher learning abilities. The examples of these application scenarios are only based on existing technologies. New paradigms will play a leading role in the near future, and people's lives will take on a whole new look under the influence of the Internet of Things.

Similarly, from the perspective of business users, the high degree of automation and mechanization brought by the Internet of Things will significantly reduce production costs and improve product quality; concepts such as human-machine integrated logistics and business management and real-time monitoring will also become a reality. Furthermore, with the innovation of information technology, the development of power electronics technology and the rise of pattern recognition technology, the concept and connotation of the Internet of Things have been enriched and developed: the replacement and popularization of smartphones have provided a better terminal carrier for the Internet of Things; the new proposed sensor technology offers a better perception method for the Internet of Things; the development of image recognition technology enables the Internet of Things system to process image and video information and become more intelligent. Therefore, the tasks to be realized by the Internet of Things are also more diverse, which can be summarized as learning real-time intelligent identification, positioning, tracking, monitoring, and managing items.

To realize the automation and intelligence of the interoperability of interconnected devices, the Internet of Things still needs further development in related knowledge industries [2]. From the point of view of the information flow required by the Internet of Things, a connection is established between things. With the increase in Internet coverage, there are more and more information sources and sinks in the entire information network. The corresponding data processing technology puts forward higher requirements and requires more capital and human resources. However, issues such as the credibility of information sources, security, and whether user privacy is violated still exist. With the development of data mining technology, the pattern of related problems will also change. Furthermore, how to reasonably handle the contradiction between society and technology will be a very challenging problem [3]. To sum up, the development of IoT technology requires a lot of humans, material resources, and social recognition, and the development still faces many difficulties.

In recent years, under the background of the international financial crisis, the development direction of various countries has gradually turned to high-tech industries. The introduction of the Internet of Things and Industry 4.0 allows for a new round of information technology revolution. All countries are seizing the opportunity and turning to the Internet of Things technology market that integrates various high and new technologies, encouraging some factories, research institutions, or economic entities to develop related projects to meet the technological requirements of advancing with the times. India has also incorporated the Internet of Things into a strategic emerging industry, adopted a series of policy measures to promote its development, and set off an upsurge in the research and construction of the Internet of Things. To find a new round of productivity growth points in the trend of the times, we seize the champion of future international economic development.

4. Proposed System Model

To ensure the safety of patients' medical data and the safety of system model parameters and improve the accuracy of lesion classification, we propose a system model for collaborative analysis of medical images.

4.1. System Model of Secure Image Collaborative Analysis. The system model of the collaborative analysis of images designed in this paper is shown in Figures 3 and 4, including two stages of data cleaning and lesion classification. In the data cleaning phase, the best cleaning effect provided by the private cloud is obtained from the consortium blockchain CBD (consortium blockchain for data cleaning). Model parameters (each private cloud shares its model through the CBD) are used to identify low-quality images that are no longer passed to the lesion classification stage. In the lesion classification stage, high-quality images obtained after data cleaning are mainly used for training and classification. The model parameters are securely transmitted through the API (application programming interface) gateway to the public cloud. The public cloud collects the model parameters of

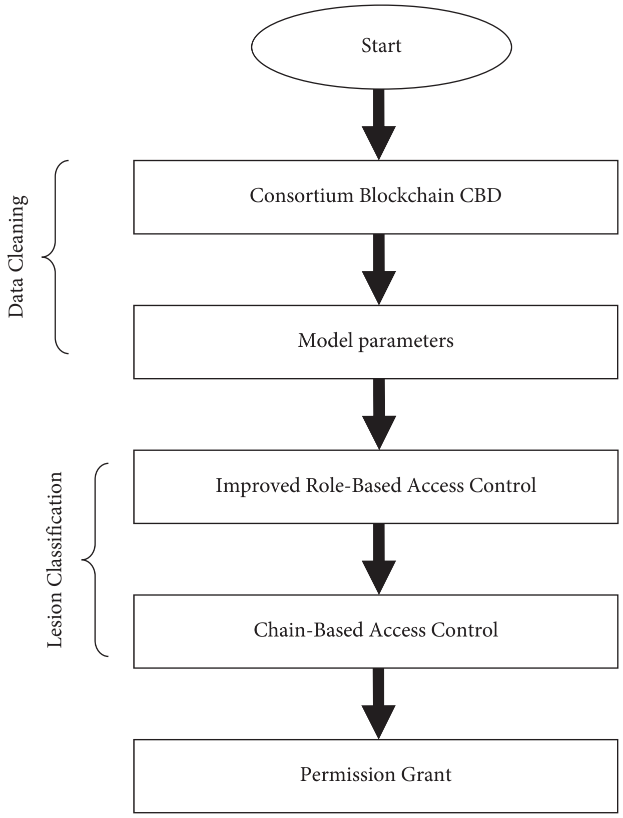
Start
Data Cleaning
Consortium Blockchain CBD
Model parameters
Lesion Classification
Improved Role-Based Access Control
Chain-Based Access Control
Permission Grant

Figure 3: Proposed flowchart.

each private cloud, obtains the global model using a weighted average, and then shares the global model with each private cloud. When the personal cloud requests services from the public cloud, the API gateway uses the consortium blockchain for classification (CBC) to perform identity authentication and access control on the private cloud to prevent illegal users from accessing the public cloud, as shown in Figure 3.

Data between private and public clouds can only be exchanged after authentication is passed for data security. Therefore, this paper designs two access control schemes, namely, an improved role-based access control scheme (RAC) and a consortium chain-based access control scheme (BAC). In RAC, we consider functional rights and data rights. RAC ensures that only legitimate users can use authorized software features and access approved datasets in the HIS for each private cloud, enabling data cleansing and lesion classification. In BAC, the public cloud provides services in the form of APIs. Each private cloud exchanges data with the public cloud through an API gateway. API gateway is a private cloud and a tunnel router between public clouds. In addition, it is a load balancer and even an authorization and access manager. Clients can access data with permission granted by a third-party authority in traditional information systems. In this solution, the private cloud can be accessed through the API.

The BAC in the gateway requests data directly from the public cloud while verifying the identity and permissions of the private cloud. Both RAC and BAC protect the security and privacy of data while reducing the complexity of setting authorization permissions and authenticating valid users. In addition, two consortium chains are deployed on the gateway ode in private cloud nodes and APIs to protect data security and privacy. The first is the Consortium Chain (CBD), which saves deep learning models during the data cleaning phase. The second is the consortium chain (CBC), which keeps logs, private cloud identity, and permissions during the classification phase.

5. Experimental Setup and Result Analysis

In this paper CloudSim environment has been used to simulate the result and different machine learning technique has been use to evaluate the performance of proposed work. The model is simulated and evaluated using the NSL-KDD data set. The results demonstrate that the GA-DBN algorithm can significantly enhance the recognition rate of intrusion detection, reduce the model's complexity, and lower the model's number of models without compromising the model's classification accuracy. In addition, the model is applicable to classification and identification in addition to intrusion detection in the Internet of Things, and the network structure may be adaptively altered for different data sets. However, because the research compares only the KDD99 and NSL-KDD datasets, which are devoid of widespread attacks at the time of writing, the experimental results are limited; the model contains specific restrictions for each form of attack. However, no model structure exists that is capable of detecting all four assault types simultaneously, as shown in Table 2 and Figures 5–7.

For network-based intrusion detection, the author presented a hybrid deep learning model based on convolutional neural networks (CNN) and weight drop. A convolutional neural network is a feed-forward neural network that performs convolutional computations and has a deep structure. It is one of the most representative deep learning algorithms. It is capable of both supervised and unsupervised learning. Convolutional neural networks handle a large number of features with a small amount of computation due to the convolutional kernel's hidden layer parameter sharing and the sparsity of interlayer connections. The author employs a deep convolutional neural network to extract essential elements from large amounts of data and then passes the output of the pooling layer to a weight drop long short-term memory (WDLSTM) network to learn the feature relationships in such a way that they retain long-term dependencies, avoid gradient disappearance, and discard some repeated features to avoid overfitting caused by repeated connections. The approach is validated using the UNSW-NB15 data set, and it produces satisfactory results when compared to other algorithms; it also consumes less time. However, experimental results indicate that the detection rate for expected behavior is one on the UNSW-NB15 dataset. However, it does not have a high degree of precision when it comes to attacks involving a little amount of data. Backdoor and worms attacks, for example, have an accuracy rate of 0.50. The episode's accuracy is 0.44, but the DOS attack's accuracy is much lower at 0.32, resulting in a high false-positive rate.

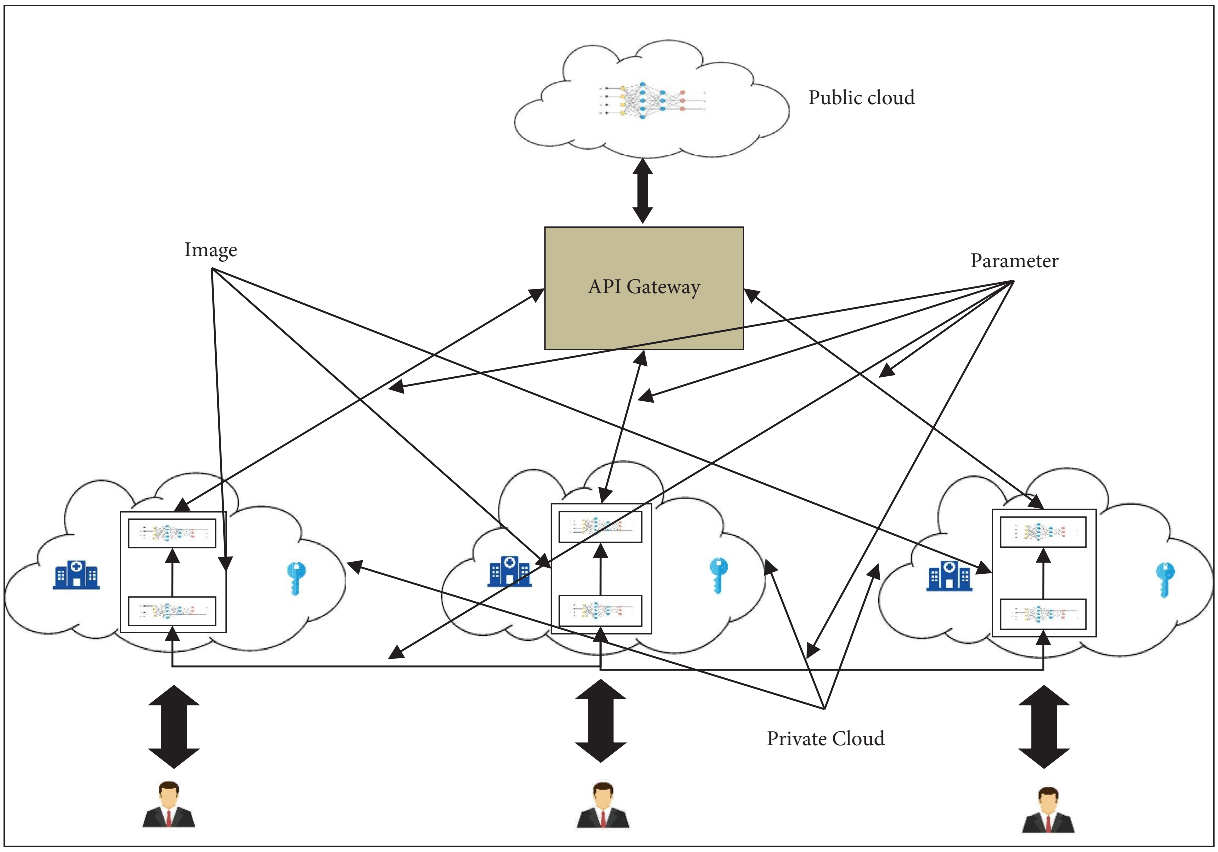

Figure 4: The model of the secure image collaborative analysis system.

Table 2: Comparison of machine learning based intrusion detection systems.

Machine learning	Data set	Confusion matrix		
		ACC	TPR	FPR
DNN + LSTM [5]	KDD99	0.85	0.86	0.81
BP + LM [6]	KDD99	0.92	0.91	0.86
DBN + GA [9]	NSL-KDD	0.93	0.92	0.89
CNN + WDLSTM [14]	UNSW-NB15	0.91	0.92	0.94
HKELM + KPCA + DEGSA [15]	KDD99	0.89	0.86	0.85
DFNN + RRS-K–means [16]	UNSW-NB15	0.88	0.86	0.85
DT + PIO [17]	KDD99 UNSW-NB15 TE	0.92	0.94	0.91
SVM [20]	NSL-KDD	0.89	0.91	0.78
Proposed model	KDD99 NSL-KDD UNSW-NB15	0.94	0.93	0.95

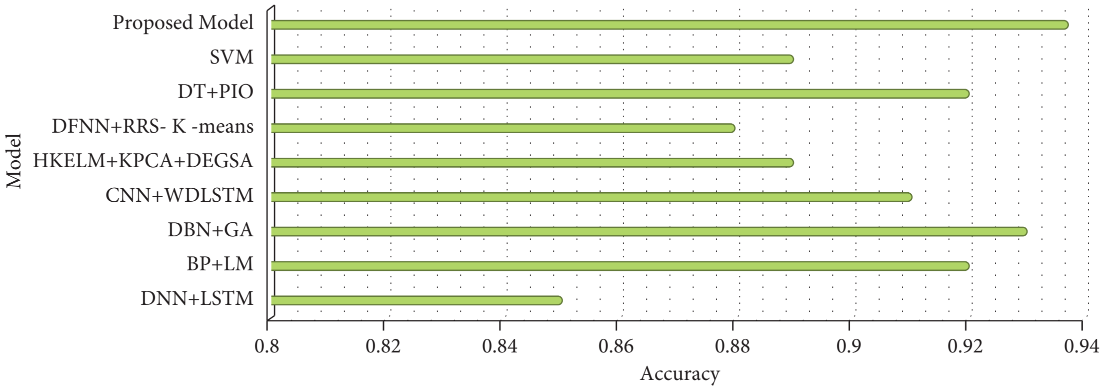

Figure 5: Comparative analysis of accuracy of proposed work with recent trend.

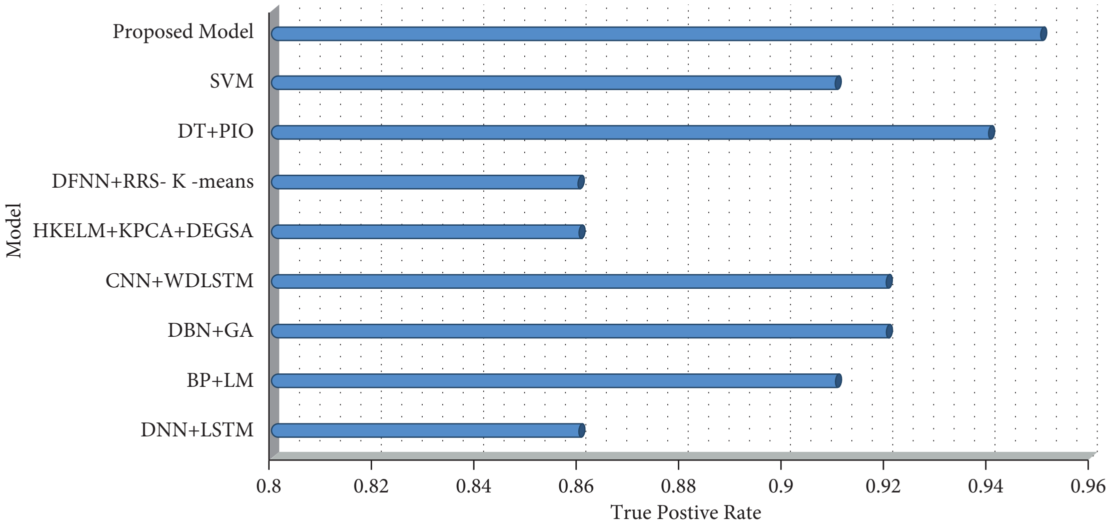

Figure 6: Comparative analysis of true positive rate of proposed work with recent trend.

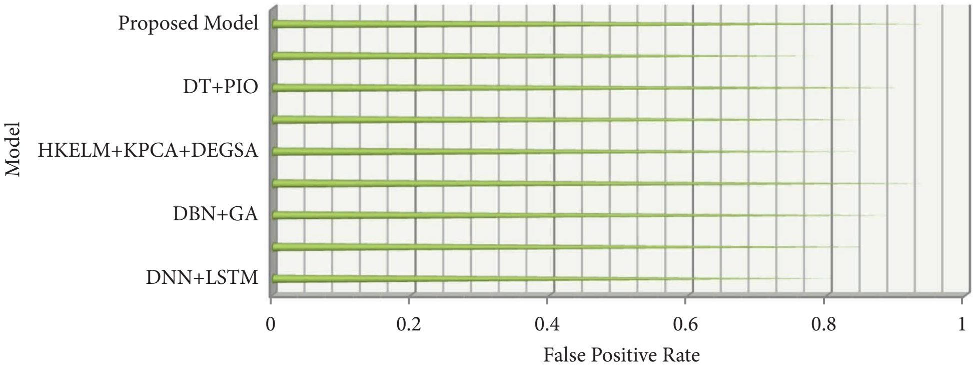

Figure 7: Comparative analysis of false positive rate of proposed work with recent trend.

The author presented the KPCA-DEGSA-HKELM intrusion detection system, which is based on abuse. PCA (principal component analysis) is a linear relationship-specific principal component analysis algorithm. However, while dealing with nonlinear interactions, the contribution rate of each principle component is excessively distributed, and therefore kernel principal component analysis (KPCA) is presented. To begin, the algorithm maps the original data to the high-dimensional space using the kernel function, converting the indivisible data to separable data in the high-dimensional space. Then, the PCA technique is used to reduce the dimension and extract features. ELM (extreme learning machine) is a machine capable of extreme learning. It is a single hidden layer feed-forward neural network. It is appropriate for both supervised and unsupervised learning tasks. It is capable of randomly initialising the weights and biases of the inputs and obtaining the appropriate output weights. Thus, convergence occurs more quickly, learning is more effective, and it is easier to obtain the ideal global solution. However, prediction accuracy for unknown attacks is rather low, and hence the hybrid kernel function extreme learning machine (HKELM) is developed to increase generalisation ability. Differential evolution algorithms include DE (differential evolution algorithm) and GSA (gravitational search algorithm) that increased efficiency of detection. The SDK is validated against the NSK-KDD benchmark dataset, and the findings indicate that it performs well in detecting intrusion assaults. However, binary classification validation is performed using only the NSL-KDD dataset, and the experimental results have some limitations. The algorithm is not faster than other models, although being three times faster than the ELM algorithm; placing the algorithm on the fog node may introduce additional security problems; if an attacker gains control of the fog node, it will lose control, resulting in increased losses.

The author came up with a way to choose features for IoT intrusion detection technologies based on the pigeon-inspired optimizer (PIO). The continuous pigeon-inspired optimizer is a new linearization method that calculates the speed of pigeons using cosine similarity, which leads to faster convergence. Decide tree (DT) is the algorithm used by the author. In machine learning, DT is both a prediction model and a tree structure that shows how object attributes and object values are linked together in a way that can be used to make predictions. Each node is an attribute, and each branch is a possible value for that attribute. Each leaf node is a type of object. People use DT to learn how to classify things. It is better at dealing with how features interact than other classifiers. In order to build an intrusion detection system, we need to pick out the right parts and then use the DT classifier to figure out what is normal and what is not. By using the improved PIO algorithm and the DT classifier, we can make sure that we have a high rate of detection and a low rate of false positives. It shortens the time the system is running. However, the article only talks about two types of data and does not include data for more types. For two types, the accuracy of NSL-KDD is only 0.883, which does not meet author expectations for performance improvement. When it comes to binary classification, the method gets a score of 0.998 out of 1.

The author developed a simple technique for detecting intrusions based on support vector machines (SVM). SVM is a generalized linear classifier that uses the supervised learning method to conduct binary classification on data. It demonstrates numerous distinct advantages in tackling problems with a small sample size, high-dimensional pattern recognition, and linear inseparability. The author employs simply the packet arrival rate attribute and extracts three characteristics, average, maximum, and median, to determine whether network traffic is anomalous, considerably reducing training time; the SVM is optimized using linear functions, polynomial functions, and radial basis functions; increasing the temporal window size also enhances the classifier's performance to a certain amount. The system performs admirably in terms of classification accuracy and detection time. However, the algorithm's detection range is very narrow, and it is simple to overlook the features of modest traffic changes, allowing attackers to infiltrate.

The author suggested an anomaly intrusion detection system based on two-layer dimension reduction and two-tier classification (TDTC) that primarily detects low-frequency band attacks, such as R2L U2L. The first layer, principle component analysis for feature dimensionality reduction, is an unsupervised learning technique that reduces the NSL-KDD dataset's 41 features to 35 by producing irrelevant features from the initial linked components. The smaller feature space decreases the system's overhead dramatically; the second layer of dimensionality reduction employs linear discriminate analysis (LDA), a supervised learning technique, to which is use to ensure that each sample output is dimensionality reducted. This enables more accurate classification, which speeds up intrusion detection. Combining these two technologies decreases processing and makes IoT systems more suited. The second stage is to classify the data using the Naïve Bayes algorithm (NB) and K-nearest neighbor (KNN). NB is a supervised learning technique that makes use of probability and statistics knowledge to categorise sample data sets, assuming that the feature conditions are unrelated. It requires fewer parameters, is less prone to missing data, and utilises a straightforward method. KNN is given a training data set; for each new input instance, it finds the k examples in the training data set that are the closest match to the example; the majority of these k instances belong to a certain class. The model is segmented. This class is insensitive to outliers and has a high accuracy of classification. The author first utilises NB to discover anomalies in the dimensionality-reduced data and then sends the detection results to KNN for reclassification, which has a lower false-positive rate and a greater detection rate. While the technique performs well on the NSL-KDD dataset, it is not restricted to that dataset and can be extended to real-time data traffic detection.

6. Conclusion

The Internet of Everything has penetrated every corner of life, such as intelligent parking lots, intelligent environment testing, smart grid, automatic vehicle diagnosis, and other fields. However, industries have failed to validate their quality and safety as they strive to innovate and develop more connected products. At this stage, the Internet of Things is a double-edged sword. A damaged node may affect the equipment of the entire network. Therefore, an intrusion detection system is required to ensure network security and detect malicious attacks. This paper first compares the difference between traditional system security and the current stage of IoT security and classifies the intrusion detection system in detail from detection technology, data source, architecture, and working methods. Discussion and evaluations are conducted, and future directions are elaborated. To sum up, whether it is a neural network model, a swarm intelligence optimization algorithm, or a traditional machine learning algorithm, they interact to provide a better solution for the intrusion detection system. The quality of an intrusion detection system depends on whether the system structure is centralized or distributed, based on anomaly detection or misuse detection, whether the data is captured in real-time or offline, and whether the information is labeled or unlabeled. Therefore, using various machine learning algorithms and other strategies for different attacks will produce different results, as shown in Table 2. Because the differences in deployment methods cannot be compared one-to-one, it is more inclined to summarize the performance.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Islam, A. Al Amin, and S. Y. Shin, "FBI: a federated learning-based blockchain-embedded data accumulation scheme using drones for internet of things," *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 972–976, 2022.

[2] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using internet of drone things," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 166–173, 2021.

[3] Y. Gong, S. Mabu, C. Chen, Y. Wang, and K. Hirasawa, "Intrusion detection system combining misuse detection and anomaly detection using Genetic Network Programming," in *Proceedings of the 2009 ICCAS-SICE*, pp. 3463–3467, Fukuoka, Japan, August 2009.

[4] P. Widulinski and K. Wawryn, "A human immunity inspired intrusion detection system to Search for infections in an operating system," in *Proceedings of the 2020 27th International Conference on Mixed Design of Integrated Circuits and System (MIXDES)*, pp. 187–191, Lodz, Poland, June 2020.

[5] M. Kumar and A. K. Singh, "Distributed intrusion detection system using blockchain and cloud computing infrastructure," in *Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, pp. 248–252, Tirunelveli, India, June 2020.

[6] S. Ouiazzane, M. Addou, and F. Barramou, "Toward a network intrusion detection system for geographic data," in *Proceedings of the 2020 IEEE International conference of Moroccan Geomatics (Morgeo)*, pp. 1–7, Casablanca, Morocco, May 2020.

[7] A. Borkar, A. Donode, and A. Kumari, "A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS)," in *Proceedings of the 2017 International Conference on Inventive Computing and Informatics (ICICI)*, pp. 949–953, Coimbatore, India, November 2017.

[8] J. Yu, P. Tian, H. Feng, and Y. Xiao, "Research and design of subway BAS intrusion detection expert system," in *Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 152–156, Chongqing, China, October 2018.

[9] S. Ouiazzane, M. Addou, and F. Barramou, "A multi-agent model for network intrusion detection," in *Proceedings of the 2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, pp. 1–5, Rabat, Morocco, October 2019.

[10] Z. S. Malek, B. Trivedi, and A. Shah, "User behavior pattern -signature based intrusion detection," in *Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 549–552, London, UK, July 2020.

[11] Q.-V. Dang, "Studying the Fuzzy clustering algorithm for intrusion detection on the attacks to the Domain Name System," in *Proceedings of the 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, pp. 271–274, London, UK, July 2021.

[12] X. Zhan, H. Yuan, and X. Wang, "Research on block chain network intrusion detection system," in *Proceedings of the 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, pp. 191–196, Xi'an, China, September 2019.

[13] C. M. Ou, "Host-based intrusion detection systems inspired by machine learning of agent-based artificial immune systems," in *Proceedings of the 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA)*, pp. 1–5, Sofia, Bulgaria, July 2019.

[14] L. Hong, "Immune mechanism based intrusion detection systems," in *Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, pp. 568–571, Wuhan, China, April 2009.

[15] D. S. Bauer and M. E. Koblentz, "NIDX-an expert system for real-time network intrusion detection," in *Proceedings of the 1988 Proceedings. Computer Networking Symposium*, pp. 98–106, Washington, DC, USA, August 1988.

[16] H. Lu and J. Yang, "Danger theory of immune systems and intrusion detection systems," in *Proceedings of the 2009 International Conference on Industrial Mechatronics and Automation*, pp. 208–211, Chengdu, China, May 2009.

[17] M. E. Pamukov and V. K. Poulkov, "Multiple negative selection algorithm: improving detection error rates in IoT intrusion detection systems," in *Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 543–547, Bucharest, Romania, September 2017.

[18] E. D. Alalade, "Intrusion detection system in smart home network using artificial immune system and extreme learning machine hybrid approach," in *Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1-2, New Orleans, LA, USA, June 2020.

[19] Y. Shen, Y. Fei, L. F. Zhang, A. Ji-yao, and M. L. Zhu, "An intrusion detection system based on system call," in *Proceedings of the 2005 1st IEEE and IFIP International Conference in Central Asia on Internet*, p. 4, Bishkek, September 2005.

[20] A. Garg and P. Maheshwari, "A hybrid intrusion detection system: a review," in *Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1–5, Coimbatore, India, January 2016.

[21] A. Khannous, A. Rghioui, F. Elouaai, and M. Bouhorma, "MANET security: an intrusion detection system based on the combination of Negative Selection and danger theory concepts," in *Proceedings of the 2014 International Conference on Next Generation Networks and Services (NGNS)*, pp. 88–91, Casablanca, Morocco, May 2014.

[22] G. Zhu, H. Yuan, Y. Zhuang, Y. Guo, X. Zhang, and S. Qiu, "Research on network intrusion detection method of power system based on random forest algorithm," in *Proceedings of the 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, pp. 374–379, Beihai, China, January 2021.

[23] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: a survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[24] E. M. Campos, P. F. Saura, A. González-Vidal et al., "Evaluating federated learning for intrusion detection in internet of things: review and challenges," *Computer Networks*, vol. 203, Article ID 108661, 2022.

[25] A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking back-enabled machine learning techniques," *Computers and Electrical Engineering*, vol. 98, Article ID 107716, 2022.