Hindawi
Computational Intelligence and Neuroscience
Volume 2023, Article ID 8981988, 24 pages
https://doi.org/10.1155/2023/8981988

Review Article

A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things

S. V. N. Santhosh Kumar,[1] **M. Selvi**,[2] **and A. Kannan**[2]

[1]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India*
[2]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India*

Correspondence should be addressed to S. V. N. Santhosh Kumar; santhoshkumar.svn@vit.ac.in

Received 8 October 2022; Revised 3 December 2022; Accepted 10 December 2022; Published 27 January 2023

Academic Editor: Anastasios D. Doulamis

Copyright © 2023 S. V. N. Santhosh Kumar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Internet of Things (IoT) is a distributed system which is made up of the connections of smart objects (things) that can continuously sense the events in their sensing domain and transmit the data via the Internet. IoT is considered as the next revolution of the Internet since it has provided vast improvements in day-to-day activities of humans including the provision of efficient healthcare services and development of smart cities and intelligent transport systems. The IoT environment, by the application of suitable security mechanisms through efficient security management techniques, intrusion detection systems provide a wall of defence against the attacks on the Internet and on the devices connected with Internet by effective monitoring of the Internet traffic. Therefore, the intrusion detection system (IDS) is a resolution proposed by the researchers to monitor and secure the IoT communication. In this work, a meticulous analysis of the security of IoT networks based on quality-of-service metrics is performed for deploying intrusion detection systems by carrying out experiments on secured communication and measuring the network's performance based on comparing them with the existing security metrics. Finally, we propose a new and effective IDS using a deep learning-based classification approach, namely, fuzzy CNN, for improving the security of communication. The major and foremost advantages of this system include an upsurge in detection accuracy, the accurate detection of denial of service (DoS) attacks more efficiently, and the reduction of false positive rates.

1. Introduction

The Internet of Things (IoT) is the next revolution of the Internet, where the smart objects are connected and managed using remote way through the Internet [1] as a backbone. Events in the deployed IoT environment are sensed by the devices [2]. Due to the resource restraint nature [3] of sensors in the IoT and the environment where they are deployed, the provision of efficient security is becoming a major challenge [4]. The deployment environment of IoT devices is susceptible to several types of attacks [5] by intruders such as hackers, malicious software, and viruses [6]. The main aim of these intruders is to launch various forms of attacks which lead to the breach of data integrity in the network [7]. Moreover, the intruder can launch a denial of service (DoS) attack [8] which can exhaust both the network and device resources [9] such as energy in the IoT environment. From the literature, we see that security in IoT is provided in many works by using cryptography-based security mechanisms [10] such as symmetric key cryptosystems and public key cryptosystems [11].

Since the IoT devices are resource inhibited, the use of cryptographic techniques in IoT security [12] results in significant communication and computation overhead. The design and deployment of intrusion detection systems (IDSs) are able to solve this issue. Therefore, IDSs have been used widely for monitoring and noticing impostors in IoT environments in order to provide efficient security in IoT communication [13, 14]. An IDS is a software which is running on the devices of IoT. The IDS monitors the

behaviour of the devices in the network and identifies the malicious activities, if any, that are carried out by the devices. When the intrusion (attack) is detected [15], it informs the device administrator, who takes the necessary actions to prevent such intrusions by isolating the malicious devices. In this way, the IDSs are useful to ensure device security in the IoT environment [16]. Intrusion detection systems are broadly categorized into two classes [17] depending on the type of intrusions explicitly, anomaly-based intrusions and fraud-based intrusions. The anomaly intrusions are carried out by the external attackers. On the other hand, misuse intrusions are carried out by the internal members of the IoT system who are provided with security credentials by the system administrator.

In another categorization performed depending on the type of intrusions, the IDSs are categorised into four, namely, IDS based on signature, IDS based on anomaly [18], IDS based on specification [19, 20], and hybrid approach-based IDS [21]. In IDS based on signatures [22], for each attack to be detected, it describes the attack pattern. In this scheme, a trigger message is raised when the attack matches the described pattern. By using this type of IDS, the known types of attacks can be detected more efficiently. The next category is anomaly-based IDS. In this scheme, data about the normal behaviour of the devices are obtained and values are set. If the device behaviour values, the IDSs consider it as suspicious behaviour [23, 24].

The anomaly IDS is making use of the location and temporal constraints to identify the malicious devices. Different types of attacks are in communication such as DoS attacks [25–27], Sybil attacks [28, 29], selective forwarding attacks [30–32], worm whole attacks [33], black hole attacks [34–36], sink hole attacks [37–39], jamming attacks, and false data injection attacks [40]. Therefore, many investigators paid their thoughts in the detection of one or more of these attacks by proposing different methods for intrusion detection and prevention. However, the user community is interested in knowing the most suitable method from all these methods for protecting their IoT environment, as there are no standard guidelines and suggestions provided in the literature for choosing the most suitable approach for intrusion discovery and inhibition for IoT applications. The current need of the IoT community is the availability of a single work that analyses all the prevailing IDSs for IoT and affords suitable guidelines and recommendations for selecting the best scheme for safeguarding their application.

Measuring the QoS is an imperative and challenging task. Many research studies used the false positive rate as an important metric for measuring the amount of security provided by IDSs. However, the attackers are carrying out the attacks to reduce the network performance and to consume the network resources for denying the opportunities to legitimate users from network access. This can be reduced more effectively by measuring the network capabilities and the service provided by the IoT. The measurement can be more efficient if and only if suitable metrics such as packet delivery ratio, delay, energy consumed, packets expected and accelerated by the nodes, and the overall network throughput are used for effective measurement of QoS and also for comparative analysis.

Intrusion detection systems (IDSs) are powerful mechanisms [41] used on the Internet to identify the anomalous behaviour of attackers based on their malicious activities. In this scenario, the IDSs must be developed not only to detect the known types of malicious attacks but also to detect the new types of attacks carried out on the data communicated through the Internet using different approaches. Therefore, both the IDSs that are either existing in the literature or that are being proposed newly must be evaluated for their capabilities with suitable metrics such as detection accuracy, false positive rate, and error rate. A realistic IDS evaluation needs to be tested with both benchmark datasets and also real datasets. Here, the benchmarking datasets are the most important basis since such datasets are created using large amounts of network data by using efficient construction methods and tested with real systems for statistical significance, fair comparison, and validation of computational methods. When a newly proposed machine learning algorithm is evaluated with the given dataset, the capability of the detection algorithm is demonstrated with high accuracy. Such algorithms are tested with real network environment also; they provide a similar performance. Therefore, it is necessary to test a new classification algorithm not only by varying the number of features but also by evaluating them using benchmark datasets.

The first dataset used in the evaluation of IDSs is the DARPA KDD 98 dataset. This was later extended to form the KDD'99 Cup dataset [42, 43]. This dataset consists of connection records that were created by considering various combinations of attack types and also by including the normal class, and they were used as the benchmark dataset for evaluating any network-based IDS. This dataset was developed by them by collecting and establishing their handmade and diverse test bed consisting of honeypots. Other types of datasets that were created for the effective evaluation of IDSs include the ISCXIDS 2012 dataset called the intrusion detection evaluation dataset proposed by Shivari et al. [44, 45], the realistic dataset generated by Haider et al. [46, 47], which was developed and validated using fuzzy rules, and finally the cloud intrusion detection dataset (CIDD) developed in 2017 by the Canadian Institute for Cyber Security [48].

In this work, the evaluations were carried out uniformly using the benchmark dataset KDD'99 Cup dataset which is discussed in [43, 49], and also, the works were validated using real network trace data. One of the major reasons for selecting the KDD Cup 99 dataset for evaluation of the IDS systems is that it was the widely accepted benchmark dataset used in most of the research works on IDS. This dataset consists of 41 attributes in which 38 are numeric attributes and the other 3 are symbolic attributes. Some of the attributes of this dataset are the duration attribute that describes the time duration (number of seconds), the network connection duration attribute which is a continuous data attribute, and protocol_type (A discrete data attribute

describing the transport and network layer protocols) including TCP and UDP.

In this paper, a survey of IDSs developed for securing the Internet communication is presented, discussed, and compared. The major contribution of this paper is that it not only proposes a new intelligent IDS but also provides a comprehensive survey and comparative analysis of intrusion detection systems present in the literature and hence suggests suitable methods and works that can increase the security of IoT networks. IoT attacks originate from the Internet, and therefore, this work includes attacks on computer networks, including both wired and wireless networks with and without mobility [50]. It considers both acknowledgement-based schemes and machine learning-based intelligent approaches that are used to increase the security of the devices.

The most important contribution of this paper is that it proposes a new intelligent IDS by extending the convolution neural network (CNN) with fuzzy rules for accurate decision making [51, 52]. Moreover, this work evaluates the existing IDSs that are also using fuzzy variables and compares them and detection time by employing suitable evaluation metrics such as false positive rate, energy consumed, packet delivery ratio, delay analysis, network throughput, and error rate in the IoT environment. Finally, it provides recommendations for choosing the best methods for designing and prevention, which are demonstrated through measurements and metrics, as well as the new IDS proposed in this work for IoT networks.

2. Literature Survey

Security of communication can be provided by using various methods including access control [53], optimization-based secure routing techniques [54], agent-based methods [55], temporal analysis [56], intrusion detection techniques developed for feature selection and classification, key management techniques, encryption and decryption methods, trust management techniques, firewalls, and application considerations [57–65]. Various authors have proposed a variety of mechanisms for providing security in IoT environments through IDS. In this section, the review of articles by various authors on IDS in the IoT has been provided with suitable analysis to highlight their benefits and limits in the field of IDS in the IoT [66–70]. Owais et al. [71] suggested a genetic algorithm-based [72] IDS for IoT. Moreover, their proposed algorithm generates intelligent rules for analysing the behaviour of the connected devices, so that it is possible to filter the malicious contents and also identify the malicious links present in the connected devices. The limitation of this work is that it has significant computation overhead and unknown attacks are not detected by this system accurately. Wang et al. [73] proposed the use of the hidden Markov model (HMM) for developing IDS. In their work, they considered efficiency, speed, and precision as the optimized parameters for evaluating their IDS. Their proposed technique is to detect the intrusions based on anomalous behaviour. Even though this system uses a statistical approach to handle novel situations, the detection accuracy is not uniform and hence lacks in security provision. Helai [74] suggested a signature-based IDS by applying data mining techniques. In this system, classification and pattern recognition methods have been employed to make a distinction on the normal behaviour from the abnormal behaviour of the devices, and hence, it improved the detection accuracy. However, this system is not suitable for an IoT environment since it involves more computational overhead.

Kolias et al. [75] proposed a security system which uses swarm intelligence in the development of the IDS. The parallel nature of SWAM intelligence has decreased the training time and hence improved the quality-of-intrusion detection in many situations. However, the behaviour of the rules generated in this system was not uniform, and a small change in one rule affected the others. Jaisankar et al. [76] carried out an investigation to IDS. In this work, they used fuzzy rough sets [77] for performing outlier detection-based intrusion detection. Gendreu and Moorman [78] have carried out a survey of IDS developed in the past for providing security to IoT. In this survey, the authors highlighted the general process of IDS and the current research challenges of IDS in the IoT. Moreover, the requirements for developing the quality IDS in an IoT environment are explained in this work. However, the latest trends and attack patterns necessitate further analysis, and new techniques are necessary.

Thangaramya et al. [79] proposed a secured model for outlier detection for wireless sensor networks. This article highlighted the open research challenges and provided the scope for future improvements in the methods used in the development of security in communication. Ammar et al. [80] explained the need for enhancing the security of IoT by providing security solutions for IoT. This work highlighted the basic idea for developing third-party security applications. Yang et al. [81] proposed a security model that analysed the security and privacy issues of the IoT. In this work, they have analysed the security issues on four layers. However, the detection and prevention measures for the attacks occurring in various layers are not provided in this work. Kouicem et al. [69] provided an inclusive investigation on reliability issues in the IoT. They explained the use of SDN since it is able to preserve both security and privacy more efficiently. However, they have observed that most of the existing approaches involve more computational complexities and overheads.

From the related works, the research gaps identified are that most of the prevailing IDSs presented in the literature are generic in nature, focusing on network security, and most of them do not focus on the use of deep learning-based computational intelligence for developing a reliable intrusion detection system. Therefore, they are not appropriate for providing efficient security in the IoT environment. The need of the current IoT communication is the provision of a flexible and more efficient security mechanism that can find the known as well as novel types of attacks and prevent them more intelligently using artificial intelligence (AI) and machine learning (ML) techniques [82]. In this work, we propose a new intelligent IDS by performing feature extraction, feature selection, and intelligent classification by

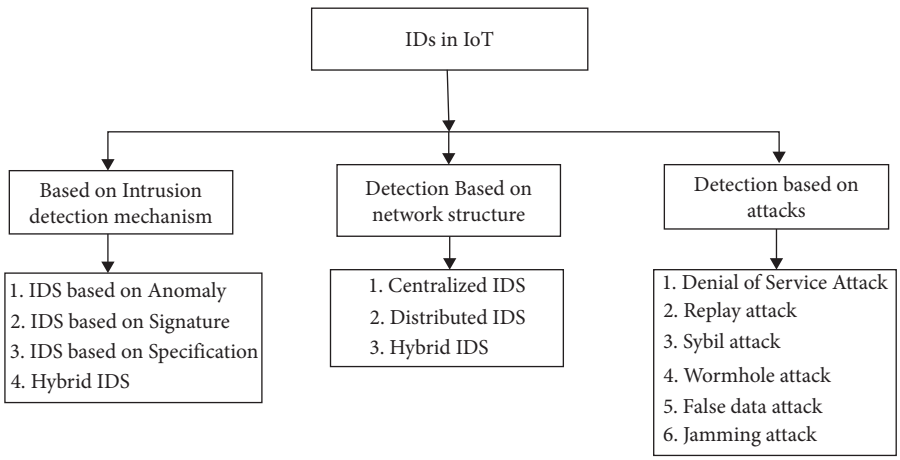

Figure 1: Taxonomy of IDS in IoT.

extending the CNN classifier with a fuzzy rule-based approach in which the fuzzy inference system identifies the intruders more effectively through efficient rule matching and also by performing deductive inference. Moreover, a comprehensive survey of IDSs in the IoT is also carried out in this work, which highlights the advantages and limitations of the prevailing IDSs available for the IoT environment and compares them with the proposed work. The major contributions of this work include the comprehensive literature survey, the identification of suitable metrics for comparison, the measurement of various parameters more efficiently by identifying the granularity of the measurement, and finally the proposal of a new IDS using deep learning techniques. Based on the experiments carried out in this work, it is found that the proposed intelligent IDS is more effective in terms of intrusion detection rates and also in the reduction of false positive rates.

3. Intrusion Detection Systems for IoT Communication

The IDS in IoT is classified into three groups built on their deployment, namely, the centralised IDS (CIDS), distributed IDS (DIDS), and hybrid IDS (HIDS). In CIDS, the analysis is carried out only on centralized servers, where they control all the devices present in the network. In this scheme, the IDS is normally placed on a centralized point of control for the devices [79] like end servers, cluster heads, and routers [83]. The IDS analyses the data available in the network traffic to detect intrusions [84]. The next type of IDSs used in IoT security is the distributed IDSs. In this scheme, the IDSs are deployed on the sensing nodes in the IoT devices. Each of the sensors will be able to analyse the sensed data to identify the behaviour of the nodes in IoT devices in order to detect the intrusions. The hybrid IDS is a collective mixture of centralized and distributive IDSs. The concept of this scheme is that the IDS is placed both in centralized servers and also in the sensing devices present in the IoT environment. The advantage of hybrid IDS is that intrusions can be detected both in the centralized server and also in the sensing devices [80].

4. Classification of IDS in the IoT

Figure 1 shows the taxonomy of IDS in IoT. The IDSs in the IoT are categorized into three groups, namely, IDSs based on the intrusion detection mechanism used [14, 85–88], IDSs where the detection is based on network structure, and IDSs developed by focusing on attack types.

The IDS-based mechanism is further subdivided into four categories, namely, anomaly detection, signature detection, and specification and hybrid IDS. The IDS detection based on network structure is further classified into CIDS, DIDS, and HIDS. The intrusion detection based on attacks is further classified into IDS for detecting denial of service attacks, reply attacks, Sybil attacks, wormhole attacks, false data injection attacks, and jamming attacks.

4.1. IDS Based on Anomaly Detection. Anomaly intrusion detection is a technique [89, 90] used to differentiate the normal behaviour of the devices from the abnormal behaviour. To detect the intrusion based on an anomaly, the behaviour of the devices is compared with the normal behaviour and a threshold (TH) value is used to find out if there is any deviation by a device that exceeds the threshold. Such a device will be labelled as a suspected device and will be observed over a period of time. If the anomaly in the behaviour continues in a device, it will be treated as a malicious device and will be isolated from communication with other devices. Various authors have proposed different techniques for providing security to the IoT environment based on anomaly detection.

Fu et al. [91] proposed an IDS technique on detecting various attacks that was developed using the mining technique. They have employed intrusion semantic techniques to detect the misbehaviour of the devices in an IoT environment. Their proposed system uses slice time window technique for accomplishing the intrusion detection. In this technique, the collected information about the devices is classified based on time analysis. In this system, the anomaly is detected by equating the existing data with the normal profile and checking whether there is a deviation. If the data

are inconsistent, then it is considered as intrusion. This technique has been evaluated based on theoretical analysis. However, there exists significant complexity in the comparison of data in real time, and hence, the network life is affected considerably. Ding et al. [92] suggested an innovative theory-based technique to detect the anomalies of devices in an IoT environment. In this system, information security is provided to the devices which utilize most network resources. The proposed system monitors malicious devices in order to identify selfish devices and intruders. Moreover, in this game-based model, each of the devices is allowed to use an optimal quantity. The devices utilize the network resources during data transmission to monitor and ensure against malicious devices which can cause vulnerability to the network. The advantage of this system includes its ability to detect the normal behaviour in the system. The constraint of this model is the lack of required detection accuracy.

Ragasegarar et al. [93] proposed distributed anomaly detection architecture for providing security to the devices. In this architecture, the grouping of devices is made using a hyperellipsoidal plane method. The information available on each device is used to detect the neighbourhood behaviour with respect to the abnormality of the devices both locally and globally that are present in the group. The devices collect the information available to identify the local and global abnormalities in the behaviour of the devices. Moreover, when the devices sense the data from the sensing domain, anomalies are detected based on the collected data. The advantages are the upsurge in network life time and reduction in computation overhead. The main limitation is the reduction in intrusion detection accuracy when the width of the hyperellipsoidal plane is expanded. Chen et al. [94] proposed a fusion-based protective technique to provide better defence against the attacks caused by the intruders. In this method, each device sends a one-bit message to the fusion cache for intrusion detection. The benefit of this method is that it is robust by nature. Moreover, the proposed method is not accurate in detecting unknown types of attacks.

Ham et al. [95] suggested an efficient anomaly-based intrusion detection technique to detect malware in the android operating system using a linear support vector machine. The benefits of this method are that it affords true positive and intrusion detection accuracy when it is equated with other existing approaches. The limitations are the existence of significant overhead in terms of computation. Moreover, the proposed method requires heavy implementation which can exhaust both the network and system resources of the devices in an IoT environment. Wang et al. [96] proposed an efficient security mechanism which can train and detect the intrusions in IoT devices in large scale to provide efficient IoT security services. The advantages of this method are in its ability to provide efficient intrusion detection at real time with better accuracy. Moreover, this method optimizes both system performance and network life time. The limitations are that it consumes more energy and will exhaust both network and system resources. Moreover, it is able to identify only a limited number of known attacks in the IoT environment.

Pongle and Chavan [33] proposed an IDS which is able to identify the worm hole assault based on their neighbour device and location information. The advantages of this method are its energy efficiency and real-time intrusion detection capability. Moreover, the proposed intrusion detection system improves QoS by decreasing packet overhead and improving the packet delivery ratio. Moreover, the proposed method is able to detect only a single type of attack which can be either known attacks or unknown attacks. Cervantes et al. [97] proposed an efficient IDS which is able to identify sinkhole attacks using watchdog and trust [98] management mechanisms to monitor the behaviour of the devices in an IoT environment. The advantages of this method are that it optimizes both network and system energy efficiency and improves QoS in the network in terms of minimizing packet and routing overheads, and it increases the packet delivery ratio. Moreover, the proposed method has low false-positive and false-negative rates. However, this model is able to detect only a limited number of attacks. Moreover, the proposed IDS is complex in terms of high computation overhead which is not desired in the IoT.

Summerville et al. [99] suggested a lightweight intrusion detection outline which is able to detect the various attacks. The proposed system detects the intrusions using deep packet analysis and the intrusion detection scheme is deployed in the IoT devices. The advantage of this method lies in its accurate intrusion detection capability. Moreover, the proposed IDS is lightweight in nature and has a low false positive intrusion detection rate. It enhances the QoS by reducing the communication overhead in the network. On the other hand, there exist significant computation and communication overheads during packet classification which consumes more energy and time. Moreover, the proposed IDS can only detect the known types of assaults which can be detected from the routed packets sent from the other devices in the IoT environment. Eliseev and Gurina [100] proposed an intrusion scheme which is able to observe the abnormal behaviour of the devices in the IoT environment. Their proposed intrusion system uses a correlation function which is based on the request–response method. The benefit of the planned method is that it is lightweight in nature and thereby consumes only the optimal quantity of resources in the network. Moreover, their suggested intrusion detection scheme offers an improved accuracy rate. The limitations are its queuing delay and communication delay. Furthermore, the suggested IDS is complex in terms of computational overhead which may exhaust the network resources quickly.

Grgic et al. [101] suggested a security framework for devices in the IoT which can identify the malevolent nodes in IPV6-based distributed systems. The proposed framework monitors the anomalous behaviour of the devices using collaborative processing to identify the attack. The advantages of the system framework are its energy efficiency and better intrusion detection accuracy. The limitations are its high false positive rate and that it will be able to detect only known types of assaults in an IoT environment. Sonar and

Upadhyay [102] designed a system which can identify various attacks using intellectual agents. In this model, the intelligent agents [103] are placed in the network server, and gateway devices are used to monitor the behaviour of incoming data traffic. The proposed system employs a blacklist and greylist colour differentiator to show the difference between malicious devices and legitimate devices. The advantages of their work are its low false high true positive rate. Moreover, the proposed work has better intrusion detection accuracy. The limitations are that the proposed IDS will not be viable for implementation in a reasonable amount of time and it does not provide device scalability.

Hodo et al. [104] suggested a system which can detect distributed DoS attacks using a three-layer artificial neural network (ANN). Four nodes act as the client, and one node acts as the server to perform data analytics. The server acts as a sink which receives the requests from the clients and responds to their requests. The advantages are that an expert system is built using a knowledge-based approach to efficiently analyse and detect DDoS attacks from the data packets which have been received from the server. Moreover, the proposed model optimizes the resources in real time and has a better ability to detect the malicious activities of the nodes. The limitations are that intrusion detection accuracy depends on probability estimation. Moreover, the expert system that uses the knowledge base should be trained more accurately to get better results. Table 1 gives the comparison of different IDSs based on anomaly detection.

4.2. IDS Based on Signature. An IDS based on signature provides better defence against the various network attacks based on the generated signature. In this system, the current behaviour of the network is matched with the malicious attack patterns to trace the type of attacks generated by the intruder. Many authors have proposed methods for providing security to IoT environments using a signature-based intrusion detection approach.

Amin et al. [105] suggested a signature for securing the Internet-protocol-based ubiquitous sensor networks. In this IDS, the signature for various attack patterns are generated. The generated attack patterns are stored as an array and kept in the bloom filter. When the data packets enter the bloom filter, it matches the attack pattern and filters them. Based on the pattern match, the type of attack is detected. The advantages of this method are that it has a lower false alarm rate and provides better intrusion detection accuracy. Moreover, the proposed model is lightweight in nature, and hence, it can perform better optimization [106] of the network resources. The limitations are that it can only detect a fixed pattern of attacks. Moreover, there is communication overhead during data transmission from nodes to the bloom filter. Oh et al. [107] designed an IDS, which can identify the various attack patterns using a matching engine. Here, the matching engine uses auxiliary shifting for the early identification of attacks. By doing so, the attacks can be early detected based on the matching pattern and can terminate the attack as early as possible. The advantages of the system are that it has improved computational complexity and has high intrusion detection accuracy with fixed, generated attack signature patterns. Moreover, it is scalable and ensures better memory utilization. The limitations are that it can only detect a finite number of known attacks based on the pregenerated signature patterns. Moreover, the proposed system cannot be implemented in real time.

Sun et al. [108] proposed an intrusion detection scheme which is able to detect malicious assaults using cloud eye in an IoT-based cloud environment. On the device side, the cloud eye uses an intelligent lightweight agent scanner to detect the malicious data from the incoming data packets. The server side of the cloud eye consists of a large database which can store the predefined attack patterns and is updated periodically. Their system employs Suspicious Bucket Cross Filtering (SBCF) to detect the malicious data from the data packets. The type of attack is identified based on matching patterns with a predefined attack signature pattern. The advantages of this system are that it provides trusted and secured services [109] without compromising privacy. Moreover, the proposed intrusion detection system provides better resource optimization and can efficiently detect attacks with limited predefined pattern signatures. The limitations are that it consumes more memory and has the ability to detect only a limited number of known and familiar attacks based on the pregenerated signature patterns. Table 2 shows the comparison of various IDSs developed based on the signature patterns.

4.3. IDS Based on Specification. IDS based on specification detects the intrusion specification normally. The detected intrusions are captured by the legitimate system for further analysis. In the past, many researchers have designed many IDSs based on their specifications to provide enhanced security to the IoT environment. Some of IDSs based on its specification are discussed in this section. Misra et al. [110] planned an IDS with the service oriented architecture (SOA) model in the IoT environment. In this IDS, the SOA is configured to act as middleware to provide the services to the IoT applications. The proposed IDS sends a DALERT control message to all the available nodes. When the requests by the particular devices to middleware exceed the limit which is set as threshold value, the system detects the possibility of vulnerability in the network. Based on this information, the network administrator detects the intrusions. The limitations are it has high false positive rate and it cannot be implemented in the real time. Moreover, this IDS can be able to detect only the intrusions and it is not able to confirm the attack. Murynets and Jover [111] designed an intrusion detection system which is able to detect intrusions from short message sender (SMS) by using volumetric and content-based techniques. The aim of volumetric analysis is to detect the intrusion based on the deviation of the predefined pattern. The main aim of the content-based algorithm is to track the devices in the IoT environment. By muting these two algorithms, the independent DoS attack can be detected efficiently. The advantages of these IDSs are that they provide better intrusion detection accuracy. The

Table 1: Comparison of different intrusion detection systems based on anomaly detection.

Author name	Mechanism used	Advantages	Limitations
Fu et al. [91]	Anomalies detection based on hierarchical distributed scheme	(1) Adaptive in nature (2) Low false positive rate (3) Less resource consumption	(1) Not suitable to handle unknown type of attacks (2) High latency
Ding et al. [92]	Providing security with non-cooperative based game theory	(1) High intrusion detection accuracy (2) Low computation overhead	(1) Low combination for IoT devices
Rajasegarar et al. [93]	Hyperellipsoidal cluster-based anomalies detection	(1) Better intrusion detection accuracy (2) Low communication overhead (3) Better utilization of network resources	(1) Intrusion accuracy deviates when width of hyperellipsoidal plane expands
Chen et al. [94]	Fusion-based intrusion defence mechanism to limit the attack damage	(1) Better robust in nature (2) Low communication overhead	(1) Network tropology known to attackers (2) Detects only limited number of known attacks (3) Complex implementation
Ham et al. [95]	Direct SVM built android malware detection	(1) Better true positive rate and low false alarm (2) Better intrusion detection accuracy	(1) More overhead (2) Complex implementation (3) Detects only limited number of assaults
Wang et al. [96]	Detecting intrusion based on online for large scale IoT devices	(1) Intrusion detection based on real time (2) Better optimization of network resources (3) Better computation overhead	(1) Only detects the limited set of attacks (2) Complex implementation
Pongle and Chavan [33]	Wormhole detection attack based on node location and information from neighbour nodes	(1) Better energy efficiency (2) Low overhead (3) Better intrusion detection accuracy	(1) High false positive rate (2) Only known type of attacks are detected
Cervantes et al. [97]	INTI based sink hole attack detection	(1) Better resource utilization (2) Low false positive rate and negative rate	(1) Can only detects only known types of attacks (2) High overhead
Eliseev and Gurina [100]	Correlation function-based anomalies detection behaviour of the network server using the request-response method	(1) Lightweight IDS implementation (2) Better reliability (3) High intrusion detection accuracy	(1) Consumes more network resources (2) High computation and computation overhead (3) Fails to detect the unknown types of attacks
Grgic et al. [101]	Malicious nodes detection in IPV6 IoT environment using adaptive distributed systems	(1) Better energy efficiency (2) Better intrusion detection accuracy (3) Tolerant to device failure	(1) Detects only some limited number of known attacks (2) Has high false positive rate
Sonar and Upadhyay [102]	Agent-based DDoS attack detection using the black list and grey list method	(1) Has low false positive and better true positive rate (2) Better intrusion detection accuracy	(1) Cannot be implemented in real time (2) Not scalable in nature (3) Only detects small number of known attacks
Hodo et al. [104]	ANN based detection of DoS attacks in IoT environment using MLP supervised learning	(1) Knowledge-based expert system (2) Better network resource optimization (3) Better intrusion detection accuracy even with incomplete data	(1) Probability-based estimation intrusion detection (2) More training is needed to get accurate detection of attacks

Table 2: Comparison of IDS based on signature.

Authors	Methodologies	Advantages	Limitations
Amin et al. [105]	Network intrusion-based detection system for IP-USN	(1) Better false alarm rate (2) Better intrusion detection accuracy (3) Better optimization of network resources (4) Lightweight in nature	(1) Moreover overhead due to redundant data transmission (2) Detects only limited number of assaults
Oh et al. [107]	Pattern matching engine based malicious node detection	(1) Low computational overhead (2) High intrusion detection accuracy with limited pregenerated signatures (3) Scalable in nature	(1) Detects only limited set of fixed attacks (2) Real time implementation is not possible
Sun et al. [108]	Malicious bodes detection system based on cloud eye an antimalware detection system	(1) Secured and trusted service with privacy (2) Better time and space complexity (3) Better intrusion detection accuracy	(1) Consumes more memory (2) Detects only very few type of attacks

limitations are that it has complex implementation tasks and does not have the ability to detect intrusions in real time.

Xia et al. [112] designed a new IDS which can identify the node internal attacks in the IoT environment. This IDS has been designed along with a privacy aware routing protocol which ensures the privacy of the nodes in the network. In the route maintenance phase, the malicious activities are detected with the help of neighbour nodes and also based on the traffic analysis of the node's past behaviour. The advantages are that it has better intrusion detection accuracy and a low expectancy. The limitations are its communication and computation overheads. Moreover, the system can identify only a restricted number of assaults. La et al. [113] proposed an IDS based on innovative model which can detect deceptive assaults. The system employs honeypots as defence tool, which is capable of analysing the incoming data packets based on the predefined intelligent rules. Any suspected data packets are further analysed by the honeypots. The advantage of this IDS is its better intrusion detection accuracy. The limitations are its overhead in the intrusion detection process which consumes more network resources in the IoT environment.

Ahmed and Ko [36] designed an IDS which can provide defence against the black hole attack. In local decision procedure, the data about relationships among the nodes is gathered by the neighbours to detect the malicious behaviours. The validity of the malevolent nodes identified at the local decision process is further verified by the global node verification phase. The advantages of this IDS are its real-time intrusion detection and its intrusion detection exactness. Furthermore, the recommended IDS has a better packet delivery ratio and provides good defence against black hole attacks in an IoT environment. The limitations are that it is planned only to detect black hole attacks and has high false positive and low true positive rates. Moreover, the accuracy of IDS decreases as the count of infected nodes increases.

Surendar and Umamakeswari [114] planned an IDS which can identify sinkhole assaults using intrusion detection based on a constraint-based specification model with a request-response method in the IoT environment. The observer node plays a vital role by checking the behaviour of all nodes to identify the nodes which drop packets. The advantages of this IDS are its low storage and computational overhead. The limitations are that intrusions are not detected in real time. Moreover, intrusion accuracy is inversely proportional to the total number of infected nodes. Fu et al. [115] proposed an IDS which can detect attacks using an automata model in the IoT environment. The proposed IDS has four main mechanisms, namely, event monitor, event data base, event analyser, and response event. The vital role of the event monitor is to check the activities in the network and transmit them in digital format to the event analyser. The role of the event database is to store the recorded events and differentiate them into normal data and abnormal data. The role of the event analyser is to analyse the stored data, and it works based on three submodules, namely, network structure learning module, action flow abstraction learning module, and intrusion detection module. The benefits of this IDS are its easy implementation and better intrusion detection rate. The limitations are its communications overhead and increased resource consumption. Moreover, this IDS has more delay and can be applied only to delay-tolerant networks.

Bose et al. [116] suggested an IDS which is able to detect the selective forwarding attack in the IoT environment. This IDS detects the intrusion in two ways, namely, CIDS and DIDS. In CIDS, the IDS is placed in the sink to detect the malicious nodes. In a distributed IDS, the intrusion detection scheme is located in the routing nodes. In this IDS, the nodes are monitored at two places. The first level of monitoring is carried out by the router nodes, and the second level of monitoring is carried out by the sink. Initially, the router nodes checked the performance of their neighbour and sent it to the sink. The sink cross checks the behaviour of the nodes and identifies the nodes that drop packets frequently. The nodes which release packets frequently are called "malevolent nodes," and they are isolated from the network. The advantages of this IDS are its easy implementation with less complexity. The limitations are its low intrusion detection accuracy and the fact that it consumes more network resources. Moreover, the proposed IDS has high computation and communication overhead.

Table 3: Comparison of IDS based on specification.

Authors	Methodologies	Advantages	Limitations
Misra et al. [110]	SOA-based attack detection based on the system model in IoT environment	(1) Better optimization of network resources (2) Better intrusion detection accurateness	(1) High true positive and false negative rates (2) Inability to detect the intrusion at the real time (3) Implementation is very complex
Murynets and Jover [111]	Contact- and volumetric-based intrusion detection for SMS in IoT environment	(1) Better intrusion detection rate (2) Better resource optimization	(1) Implementation is complex (2) Not a real-time IDS
Xia et al. [112]	An incentive-based internal attack detection mechanism based on neighbour nodes to provide truthful information	(1) Better intrusion detection rate (2) Low delay (3) Provides trust-based security during intrusion detection	(1) Overhead in terms of communication and computation (2) Can only detect the known number of limited attacks
La et al. [113]	Game theory model-based deceptive attack detection for honeypot-based IoT network	(1) Better intrusion detection accuracy (2) Real-time-based intrusion detection	(1) High overhead in terms of network resources (2) It has more coverage time
Ahmed and Ko [36]	Detection of black hole attack using efficient mitigations techniques for RPL networks in IoT environment	(1) Real-time intrusion detection with better accuracy (2) Enhancement in packet delivery ratio (PDR) (3) Better false positive rate	(1) This IDS detects only black hole attack (2) The intrusion accuracy decreases when the number of infected nodes increases (3) Overhead in terms of communication
Surendar and Umamakeswari et al. [114]	Specification based sink hole attack detection in IoT networks	(1) Better overhead in terms of storage (2) Better optimization of network resources	(1) Intrusion accuracy is indirectly proportional with number of infected nodes
Fu et al. [115]	Automata model-based uniform intrusion detection in IoT networks	(1) Its easy implementation and real time detection of intrusion (2) Less complexity (3) Better intrusion detection accuracy	(1) High consumption of network resources (2) High latency and computational overhead (3) It has high false positive rate when the percentage of infected node increases
Bose et al. [116]	Sequential probability ratio test-based selective forward attack detection based on probability of packet drop in IoT environment	(1) Better true positive rate with easy implementation (2) Complexity is low	(1) High consumption of network resources (2) Overhead in terms of communication and has high delay (3) False positive rate is high when the percentage of infected nodes increases
Liu et al. [117]	SFC and PCA algorithms-based attack detection in IoT environment	(1) Adaptiveness (2) Better false data alarm (3) Better intrusion detection accuracy	(1) The intrusion detection decreases when the volume of the data increases (2) Resource consumption is high

Liu et al. [117] have designed an IDS which can identify the intrusion. The proposed IDS classifies the data into low-risk and high-risk data. Moreover, SFC and PCA algorithms are employed for self-adjustment in the detection frequency. The advantages of this intrusion detection system are its high adaptiveness and better handling of false data alarm. The

limitations are its false positive rate. Moreover, the intrusion detection accuracy decreases when the volume of the data increases by the devices in IoT environment. Table 3 gives the comparison of IDSs developed based on specification.

4.4. IDS Based on the Hybrid Detection Method. The IDSs based on the hybrid method detect the abnormal behaviour of the nodes by combining the IDS based on anomaly detection and signature generation. The capability of the IDS is that it can identify the unknown types of attacks more efficiently which were not detected in IDS-based anomaly detection and signature generation.

Various authors have proposed many IDSs based on the hybrid approach to enhance the security of devices in the IoT environment. Amin et al. [118] have designed the security framework which is able to detect attacks in the Internet protocol–ubiquitous sensor network (IP-USN). The proposed framework works on two modules, namely, Internet packet analyser (IPA) and the USN packet analyser. The main aim of these modules is to provide efficient analysis of the incoming data traffic. IPA module is further subdivided into two modules, namely, anomaly detector and pattern classifier. The vital role of the attack detector is to detect the various behaviours of the devices. The packet analyser detects the abnormal behaviour of the devices and maps it to the predefined patterns using a machine learning algorithm and groups them under a common label. The advantages of this IDS are its lightweight property and it has better false error detection rate. Moreover, the proposed IDS has a high positive intrusion detection rate. The limitations are the overhead of computation and the vulnerability to delay during intrusion detection.

Kasinathan et al. [119] have designed a security framework which can detect DoS attacks on the 6LoWPAN (IPv6 over Low-Power Private Area Network) in the IoT environment. The proposed framework efficiently analysed the incoming data packets in 6LoWPAN to detect the anomalies in the network. Once the intrusion is detected, the alarm is raised to the decision manager. The DoS protection manager validates the intrusion with preloaded signatures which are stored in the database. If the detected anomaly matches with the predefined digital signatures. The advantage of this IDS is false intrusion detection rate that is decreased and improved availability. The limitations are that this IDS can be implemented only to the network which is operated only in dynamic topology. Moreover, the predefined signatures are not updated frequently by the DoS protection manager.

Raza et al. [120] suggested an IDS which can identify the assaults based on routing in the IoT environment. The suggested IDS is designed using three modules. The first module consists of 6LoWPAN mapper; the vital role of the module is to gather the information in the network. The role of the second module is to analyse the collected information and detect intrusions in the network. The third module comprises of distributed firewall; the abnormal activities enter into the network and also handle packet drops in the network. The advantages of it are that this IDS can be extended to other networks. Moreover, the proposed IDS can be implemented in real time and has a high positive intrusion detection rate. The limitations are that it consumes more network resources and has improved communication and computation overhead.

Matsunaga and Toyoda [121] designed an IDS which can be able to detect the intrusion based on neighbour node broadcasting the latest rank based on the time stamp method. The system functions in two steps. In the first step, each node broadcasts its ranks to its neighbour nodes. In the second stage, the time stamp has been attached to each node to validate any anomalies. The advantage of this IDS is that it has more true positive intrusion detection rate, and it is highly scalable in nature. The limitations are it has overhead in terms of computation and communication. Moreover, the proposed IDS consumes a lot of resources which affects the network's consistency.

Sedjelmaci et al. [122] suggested an IDS based on a game theory approach with a hybrid intrusion detection method. The proposed IDS uses both anomaly- and signature-based methods to detect intrusions in the network. Nash equilibrium (NE) is computed for all the nodes. The computed NE score and the type of intrusion detection method employed are decoded. The advantage of this IDS is that it has low overhead. Moreover, the system has an improved intrusion detection rate and is lightweight in nature. The limitations are that it has a high latency and complex computational overhead. Shreenivas et al. [123] suggested an IDS where the attacks are detected based on EthereumX (ETX) value and geographical hints. The proposed IDS uses 6mapper to monitor the nodes behaviour in a directed acyclic graph (DAG) based on calculated ETX values, and the intrusion is detected. The advantages of this IDS are its improved intrusion detection accuracy and its real-time implementation. The limitations are its increased false positive intrusion detection accuracy.

Midi et al. [124] suggested an IDS which can detect attacks based on expert knowledge driven in the IoT environment. The expert knowledge driven system monitors the network to sense intrusions in the network. The advantages of this IDS are its high intrusion detection accuracy and better optimization of the network resources in terms of RAM and CPU usage. The limitations are its computation overhead which affects the network performance considerably. Sedjelmaci and Senouci [125] suggested an IDS which can detect wormhole and sinkhole attacks based on the game theory model in the IoT environment. The advantages of this IDS are its high intrusion detection accuracy and its lightweight nature. Moreover, the proposed IDS optimizes network resources. The limitations are that it has computational overhead which can affect the network performance considerably. Table 4 gives the comparison of hybrid-based intrusion detection methods.

5. Proposed Model

This paper consists of two components, namely, the survey of related works and the proposed work. For the effective evaluation of the existing and proposed systems, the

Table 4: Comparison of hybrid-based intrusion detection methods used in the IoT environment.

Authors	Methodologies	Advantages	Limitations
Amin et al. [118]	Detection of attacks using generalised architecture for IP-USN in IoT environment	(1) Better false intrusion detection rate (2) Better optimization of network resources	(1) Overhead in terms of computation (2) High latency
Kasinathan et al. [119]	Detection of abnormal behaviour of nodes and their matching signature using DoS protection manger	(1) IDS based on real time (2) Better false intrusion detection alarm (3) Better resource optimization1	(1) Works only with the network with dynamic tropology (2) The pregenerated signatures are not frequently updated by DoS protection manager
Raza et al. [120]	Detection of routing attacks based on integrated mini firewall-based anomaly detection and distributed firewall-based signature generation IDS in IoT environment	(1) Intrusion detection in real time (2) Overhead is minimal (3) Better intrusion detection accuracy	(1) Resource consumption by the network is high (2) False intrusion detection rate is high
Matsunaga and Toyoda [121]	Detection of attacks based timestamp to detect the inconsistency of nodes during broadcast of rank to the neighbour nodes	(1) Better overhead (2) False data intrusion detection is low (3) Better intrusion detection accuracy	(1) High consumption of network resources (2) High overhead in terms of computation
Sedjelmaci et al. [122]	Game theory-based effective attack detection using anomaly and signature detection techniques for IoT networks	(1) Better intrusion detection accuracy (2) Better false intrusion detection rate (3) Energy consumption by the nodes are high	(1) High latency (2) Computational overhead is high (3) Network resources are not optimized
Shreenivas et al. [123]	ETX metric and geographical hints-based attack detection in IoT	(1) Intrusion detection in real time (2) Better power optimization	(1) High false positive intrusion detection rate (2) Overhead in terms of computation and communication
Midi et al. [124]	Knowledge driven expect real time-based IDS for self-adapting IoT networks	(1) Better intrusion detection accuracy (2) Better utilization network and system resources (3) Low false intrusion detection rate	(1) Overhead in terms computation and communication
Sedjelmaci and Senouci [125]	Game theory-based worm hole, sink hole and black hole attack detection in IoT environment	(1) Better intrusion detection accuracy (2) Delay is minimal (3) Network resource consumption is low	(1) Overhead in terms computation and communication

following network set up has been used. The simulation parameters are shown in Table 5.

The overview of the intelligent IDS developed in this work is shown in Figure 2. The developed model consists of 7 major modules, namely, IoT IDS dataset, an administrator module, a data preprocessing module, a classification module, a decision manager, a fuzzy inference system, and a knowledge base. In this work, the KDD cup 1999 dataset that consists of 41 features has been used for developing the proposed system. The administrator module can be used as a user interface and also acts as the intrusion prevention module whenever the decision manager provides reports on intrusion and intruders. The data preprocessing module contains two submodules such as the feature analysis subsystem and the feature selection subsystem. The feature analysis subsystem computes the strengths of each of the 41 attributes present in the dataset and provides a measured score in the form of an information gain ratio. The feature selection subsystem selects the most contributing features with the help of the feature analysis subsystem and the fuzzy inference system. The selected features are given as feedback attributes to the classification module. The classification module analyses the features on its own and compares them with the features selected by the data preprocessing module. It applies fuzzy rules with the help of the fuzzy inference system and the decision. The decision manager has complete control over the system.

Therefore, the decision manager coordinates with all the other modules and makes the final decision on intrusions

Table 5: Simulation parameters.

Simulation parameters	
Parameter name	Parameter value
Network area (m^2)	500 m × 500 m
No. of sensor nodes	50–500 nodes
Basic routing protocols	LEACH protocol and AODV protocol
Mobility model (for mobile scenario)	Random way point mobility model
Transport layer protocols	TCP and UDP
Energy of nodes	2 J per node
Initial energy	0.5 J
Packet size	1024 bits
E_{elec}	50 nJ/bit

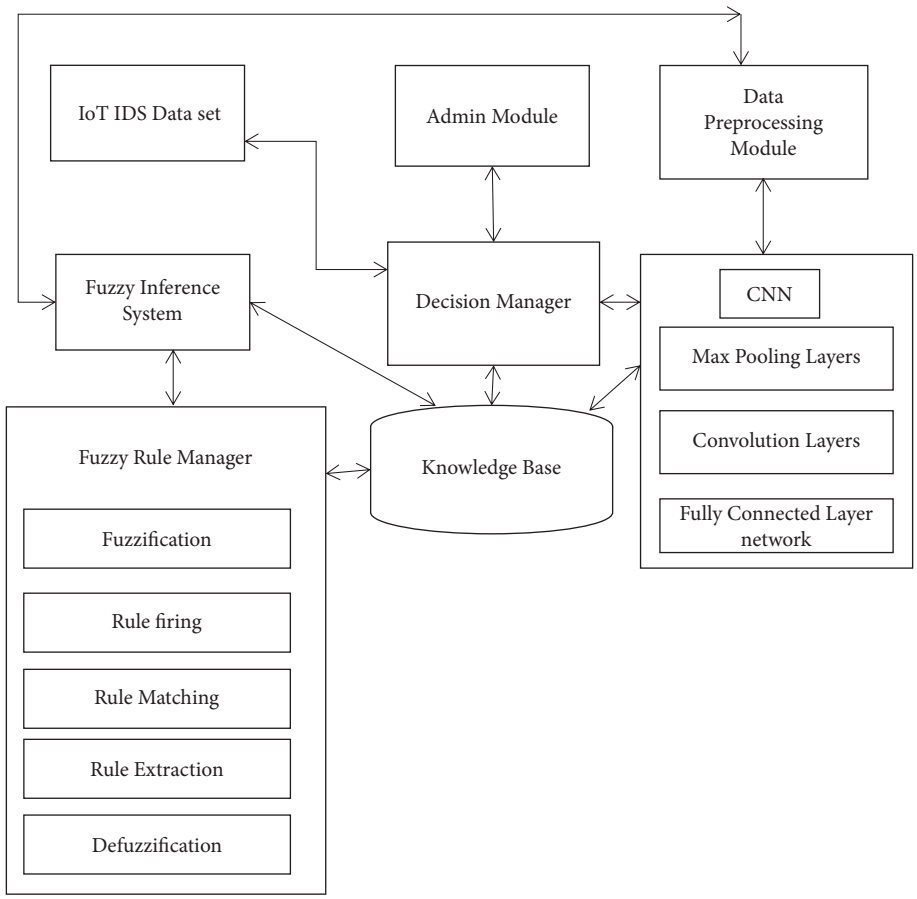

Figure 2: Architecture of the proposed system.

and notifies the intrusions and also about the intruders to the administrator module for taking actions including preventing the users and nodes from participation in the communication. The knowledge base present in this work consists of domain rules, general rules, and fuzzy rules which are used by the decision manger and classification module for making most efficient decisions.

5.1. Intelligent Feature Selection. The intelligent feature selection procedure [126] used in this work computes the information gain ratio for all the features present in the dataset. It uses a threshold for choosing the most subsidizing features based on the sensitivity of the information that is communicated through the IoT network. Based on the threshold and the information gain ratio and the usage history of users, the feature selection algorithm selects the optimal number of features for the particular application over the specified duration of time (Algorithm 1).

Table 6 shows the extracted dataset after applying the intelligent feature selection algorithm. Initially, all 41 attributes [127] from the IDS dataset were considered.

These features are given as feedback to the deep fuzzy CNN proposed in this work. Moreover, the fuzzy CNN compares the given features with other features selected by it

Input: Intrusion detection Dataset for IDS, 41 features existent in the dataset from set, Fuzzy rules and Threshold (Thres).
Output: Selected features with ranks
Step 1: Initialize number of features NFS = {}
Step 2: Read the IDS dataset (IoT _DS), feature Set (FS1, FS2. . .. . ..FS41), fuzzy Rules (FR1, FR2. . ...FRn), Thres.
$N = 71$
Step 3: For $i = 1$ to N do//finding the information gain ratio for the 71 features
Begin
Split (IoT dataset, AS1, AS2,. . .. . ..ASN, G1,G2)
$j = i + 1$;
Compute IGR values for all features (As1, AS2,. . .. .ASN) using the formulas
Info (G1) $= -\sum_{j=1}^{m} [\text{freq}(ASj, G1)/|G1|] \log_2 [\text{freq}(ASj, G1)/|G1|]$
Info (G2) $= \sum_{i=1}^{n} [|Gi|/|G2|] * \text{info}(Gi)$
IGR (AS_i) = $[\text{Info}(G1) - \text{Info}(G2)/\text{Info}(G1) + \text{Info}(G2)] * 100$
If IGR (ASi) ≥ Thres then
FS = FS U ASi;
End If
Step 4: Apply Fuzzy rules.
Step 6: Check features again using fuzzy rules and find the important features.
Return selected feature set.

Algorithm 1: Intelligent fuzzy rule-based feature selection algorithm.

Table 6: Selected features list from the IDS dataset.

S. No.	Feature number	Feature name
1	2	protocol_type
2	4	src_byte
3	8	wrong_fragment
4	14	root_shell
5	15	su_attempted
6	19	num_access_shells
7	27	diff_srv_rate
8	29	srv_serror_rate
9	31	srv_diff_host_rate
10	32	dst_host_count
11	35	dst_host_diff_srv_count
12	36	dst_host_same_src_port_rate
13	37	dst_host_srv_diff_host_rate
14	38	dst_host_serror_rate

and applies fuzzy rules to find an optimal set of features. Finally, the optimal set of features is used by the fully connected network component of the fuzzy CNN for performing the classification, whose results are used to identify the intrusions more accurately.

5.2. Fuzzy Inference System. The fuzzy inference system consists of fuzzy rules, marching, rule firing, and rule execution components. In rule matching [128], first it performs fuzzification using a triangular membership function for all the attributes, and then, it forms the fuzzy rules. The decision manager takes the input from the fuzzy inference rules and executes it to take the decision. The sample set of fuzzy rules is given in Table 7.

5.3. Classification Algorithm. The new intelligent deep classification algorithm proposed and designed in this work is accomplished by using the CNN algorithm with IF. . .THEN rules. This deep fuzzy classifier performs both convolution and max pooling operations, where the convolution for two functions f and g is represented for the operator t using the integral given in the following equation as follows:

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\tau) g(t - \tau) d\tau = \int_{-\infty}^{\infty} f(t - \tau) g(\tau) d\tau. \quad (1)$$

Moreover, we used 9 max pooling layers and 10 convolution layers that are integrated with a fuzzy inference system for performing the classification task. All these layers together are operating on the dataset and providing the set of features to be used for classification.

$$f(x) = \left[\frac{(x + 1)}{x} \right]. \quad (2)$$

As the bias function in the fully connected network component of the proposed fuzzy CNN. If both are matching, it proceeds with the classification process. In cases of mismatch, it consults with the decision manager to provide feedback on the attributes to be used based on the sensitiveness of the attributes.

6. Analysis of Existing IDS Approaches

In this section, the performance analysis of various existing intrusion detection approaches [129–136] is based on performance metrics like intrusion detection accuracy (IDA), false positive intrusion detection rate (FPIDR), real time intrusion detection (RTID), fault tolerance rate (FTR), and network resource optimization (NRO) scalability. Table 8 gives the performance investigation of different intrusion detection approaches with the given performance metrics.

Figure 3 gives the performance of various categories of intrusion detection systems with various performance

Table 7: Fuzzy inference rules.

Flow type	Label	Attack type	No. of packets dropped	Decision
Low	Anomaly	DoS	High	Attacked
Low	Anomaly	Probe	High	Attacked
Low	Anomaly	L2R	Medium	Attacked
Medium	Normal	HTTP flooding	Medium	Attacked
High	Anomaly	R2L	Low	Attacked
Medium	Normal	UDP flooding	Medium	Attacked
High	Anomaly	ARP flooding	Low	Attacked
High	Normal	DoS-synflooding	High	Attacked
High	Normal	Normal	Low	Not attacked
High	Anomaly	DoS	High	Attacked
Low	Anomaly	L2R	Low	Attacked
High	Normal	Normal	Medium	Not attacked
Low	Anomaly	Normal	Low	Not attacked
High	Anomaly	R2L	Low	Attacked

Table 8: Performance investigation of different intrusion detection approaches.

IDS type	Authors	IDA	FPIDR	RTID	FTR	NRO	Scalability
IDS based on anomaly detection	Fu et al. [91]	√	×	√	√	×	√
	Ding et al. [92]	√	×	×	×	√	×
	Rajasegarar et al. [93]	√	×	×	×	×	×
	Chen et al. [94]	×	×	√	√	×	√
	Ham et al. [95]	√	√	×	×	×	×
	Wang et al. [96]	√	√	×	√	×	×
	Pongle and Chava [33]	×	×	√	×	√	×
	Carventes et al. [97]	√	√	×	×	×	√
	Thangaramya et al. [23]	×	×	×	×	√	×
	Grgic et al. [101]	√	×	√	×	√	×
	Sonar &Upadhyay [102]	√	√	×	×	×	×
	Hudo et al. [104]	√	√	√	×	×	×
IDS based on signature	Amin et al. [105]	√	√	×	√	×	×
	Sun et al. [108]	√	×	√	×	×	×
	Oh et al. [107]	×	×	√	×	×	√
IDS based on specifica tion	Misra et al. [110]	×	×	×	√	×	×
	Murynets and Jover [111]	√	×	×	×	√	×
	Xia et al. [112]	√	×	√	×	×	×
	La et al. [113]	√	×	√	×	×	×
	Ahmed and Ko [36]	√	√	√	×	×	×
	Surender and Umamakeswari [114]	√	√	√	×	√	×
	Fu et al. [115]	×	×	√	√	×	×
	Gara et al. [30]	√	×	×	×	×	×
	Liu et al. [117]	×	×	√	√	×	×
IDS based on the hybrid method	Amin et al. [118]	×	√	×	×	√	×
	Kasinathan et al. [119]	√	√	√	×	×	×
	Raza et al. [120]	×	×	√	×	×	×
	Matsunaga and Toyoda [121]	√	√	√	√	×	×
	Shreenivas et al. [123]	√	×	√	×	√	×
	Midi et al. [124]	√	√	√	×	√	×
	Sedjelmaci and Senouci [125]	√	√	√	×	√	×

metrics like intrusion detection rate (IDR), real time intrusion detection (RTID), fault tolerance rate (FTR), and network resource optimization (NRO) scalability.

As shown in Figure 3, IDS based on anomaly detection has a better false positive intrusion detection rate when compared with other categories IDS in the IoT environment. The reason for this improvement is that IDS based on anomaly detection monitors the data effectively to detect the irregular behaviour of the nodes and detect anomalies if there is a deviation from the normal behaviour. Hence, the IDS based on anomaly detection has better false positive rate. The percentage of intrusion detection accuracy and network resource optimization of IDS based on signatures is much higher compared with other IDS in the IoT environment.

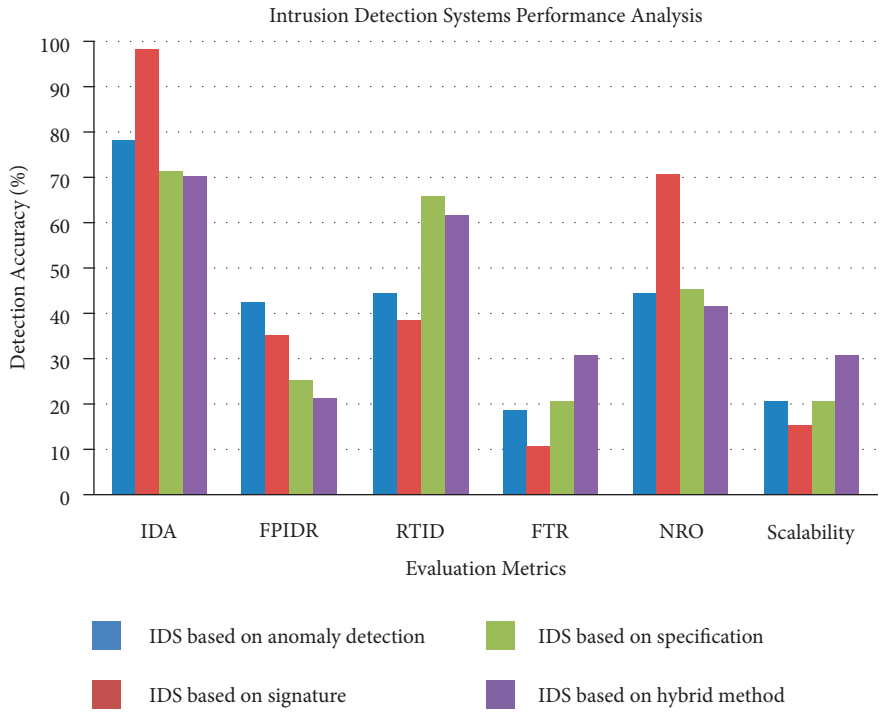

Figure 3: Performance analysis of various intrusion detection systems.

The reason for this performance is that an IDS based on signature efficiently monitors the incoming data to detect any anomalies. The detected anomalies are compared with the predefined signature attacks which are generated by the network administrator. If the detected anomalies match a predefined attack signature, the type of attack is detected. Moreover, the IDS based on signatures has better optimization of network resources. IDS based on the specification has higher real time intrusion detection system since most of the IDS are designed based on generic frame work which detects the intrusion efficiently. An ID based on a hybrid detection method has better scalability and is fault-tolerant by nature.

6.1. Simulation Results of the Proposed Work. The proposed system is executed in the NS3 simulator. The suggested system is compared with other prevailing systems using the performance parameters, namely, packet delivery ratio, delay, average energy consumption, network life time, DoS attack, probe attack, L2R attack, R2L attack, and finally security analysis. Figure 4 provides the comparative analysis based on packet delivery ratio (PDR) between the proposed IDS and the other three existing systems on the IDS.

From Figure 4, it is clear that the proposed IDS has a better PDR when equated with other related IDS works by Ding et al. [92], Chen et al. [94], and Wang et al. [96]. This improvement is possible because the proposed system uses the feedback from the results of the intelligent feature selection algorithm to select the dominant features based on information gain. Finally, it uses fuzzy-based CNN classifier to identify intrusions. Hence, the proposed system has a better PDR.

From the graph in Figure 5, we could prove that the proposed intelligent fuzzy CNN classifier presents a lower communication delay because it has better attack detection accuracy and efficiently identifies the malevolent nodes. Hence, it has better performance in communication delay. Figure 6 provides a comparative analysis of energy consumption in the network with other existing systems.

Figure 6 shows the proposed IDS consumes less energy in comparison with existing works such as the systems proposed by Ding et al. [92], Chen [94], and Wang [96] because the proposed system uses only a selected and optimal number of features and makes the classifier converge fast. Hence, the suggested system has optimal energy consumption than the other existing systems.

From the graph shown in Figure 7, we can understand that the proposed intelligent classifier has better network life-time analysis because it has better attack detection accuracy and efficiently identifies the anomaly. In the proposed work, the energy spent on communicating the packets sent by malicious nodes is eliminated, and hence, it increased the network lifetime as well. Figure 8 provides analysis in DoS detection accuracy of the proposed system with other existing approaches. From Figure 8, the proposed fuzzy CNN can detect DoS attacks more efficiently due to the use of fuzzy rules.

Figure 9 provides an analysis of probe attack detection in the network. The proposed fuzzy CNN detects the probe attacks more accurately with deductive inference.

Figure 10 provides the analysis of R2L attack for the proposed IDS with other existing systems.

From Figure 10, the proposed fuzzy CNN has more than 5% detection accuracy in comparison to existing systems.

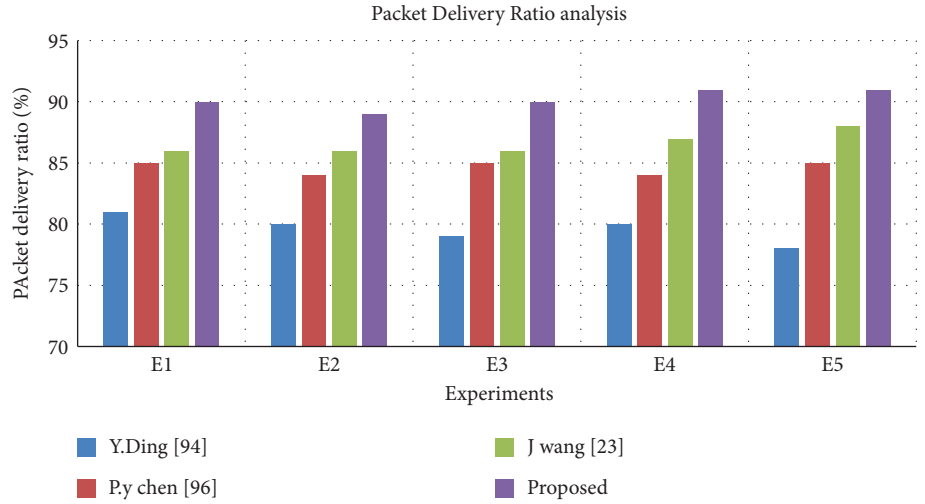

Figure 4: Packet delivery analysis.

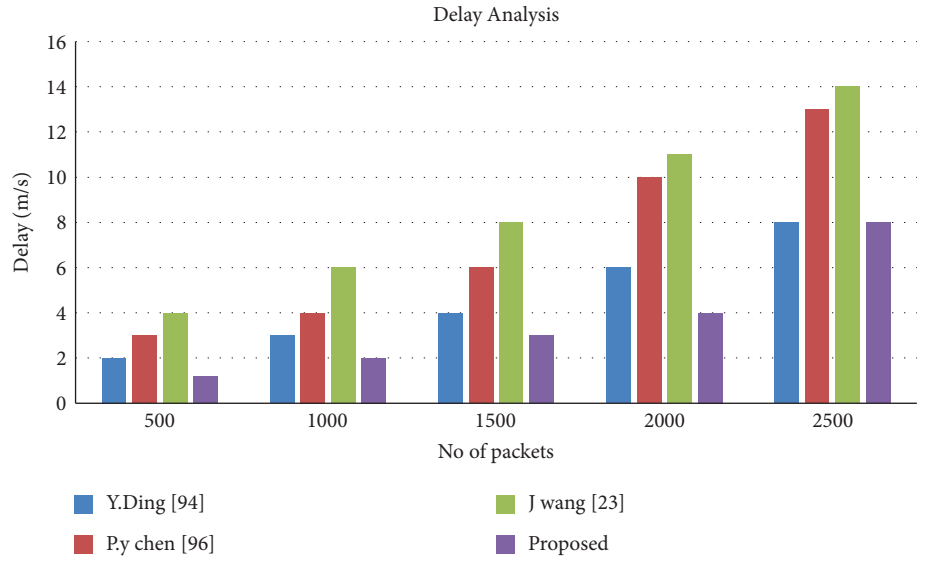

Figure 5: Delay analysis.

The use of a new bias function along with more classes of fuzzy rules enabled the proposed fuzzy CNN classifier to detect R2L attacks more reliably than the related classifier. Figure 11 provides the analysis of the overall security provided after applying the IDSs in the network based on comparisons.

From Figure 11, the overall security provided by the proposed IDS higher than the security provided by the related IDSs tested in the IoT. The security is increased since the proposed system identified the intruders more accurately and prevented the malicious nodes in the network communication of IoT.

Based on the survey made in this work, the following recommendations are provided:

(1) The hybrid intrusion detection systems are better candidates for providing security to the IoT environment since they detect identifiable and unidentifiable attacks

(2) In real-time IoT security environment, AI and ML-based techniques with an anomaly intrusion detection model can be deployed

(3) A secured routing algorithm must be developed by including the IDS component in the nodes to provide highly secured communication

(4) Feature selection and feature optimization tasks must be carried out to develop IDSs with a higher detection rate

(5) Rule optimization must be performed to reduce the detection time

To verify the usefulness of these suggestions, they were implanted into the new IDS developed in this work and

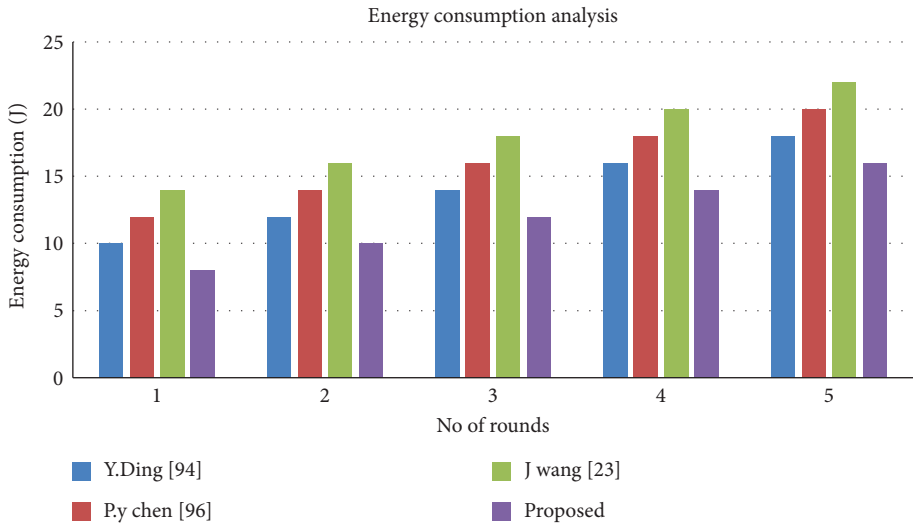

Figure 6: Energy consumption analysis.

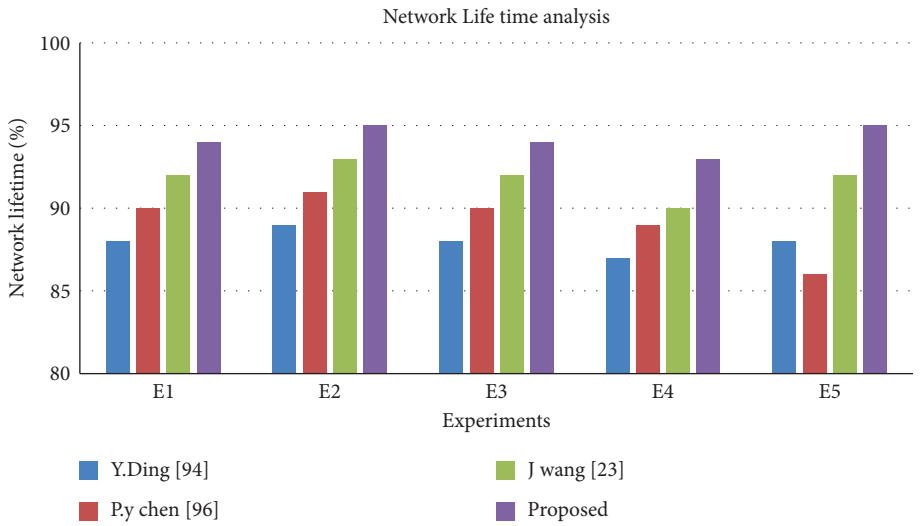

Figure 7: Analysis of network lifetime.

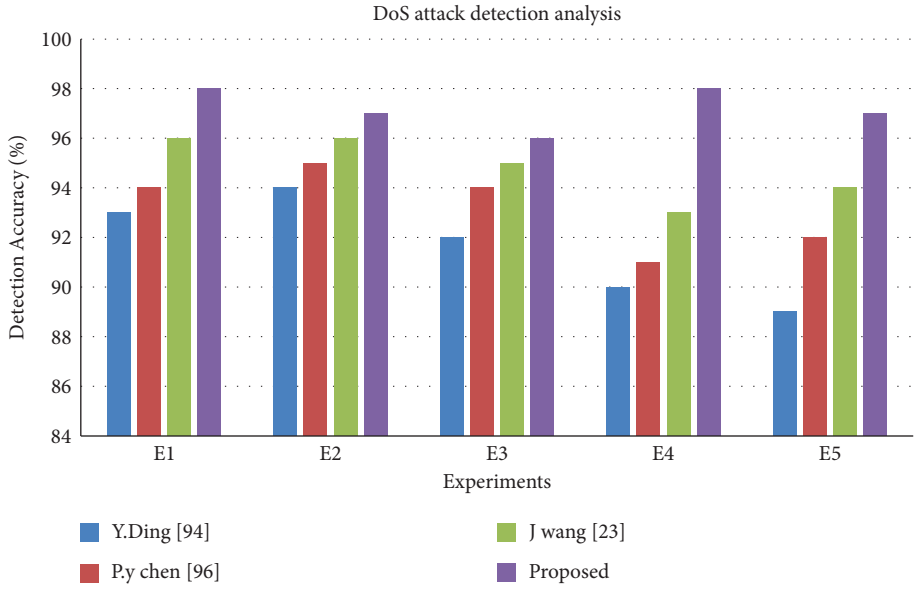

Figure 8: Analysis of DoS attack detection.

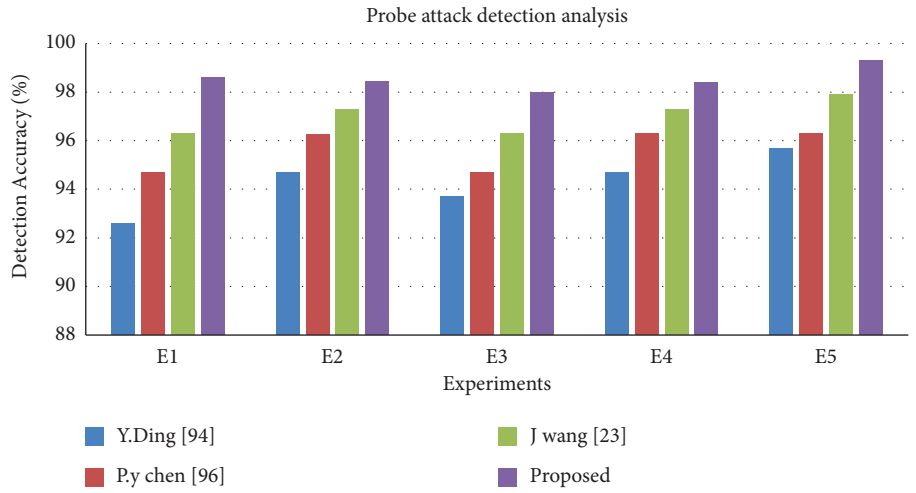

Figure 9: Analysis of probe attack detection.

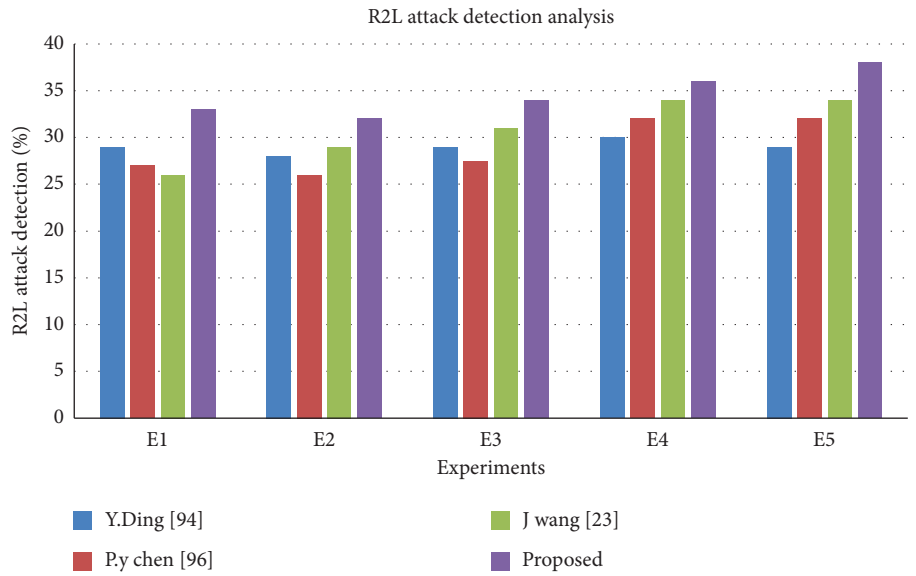

Figure 10: Analysis of R2L attack detection.

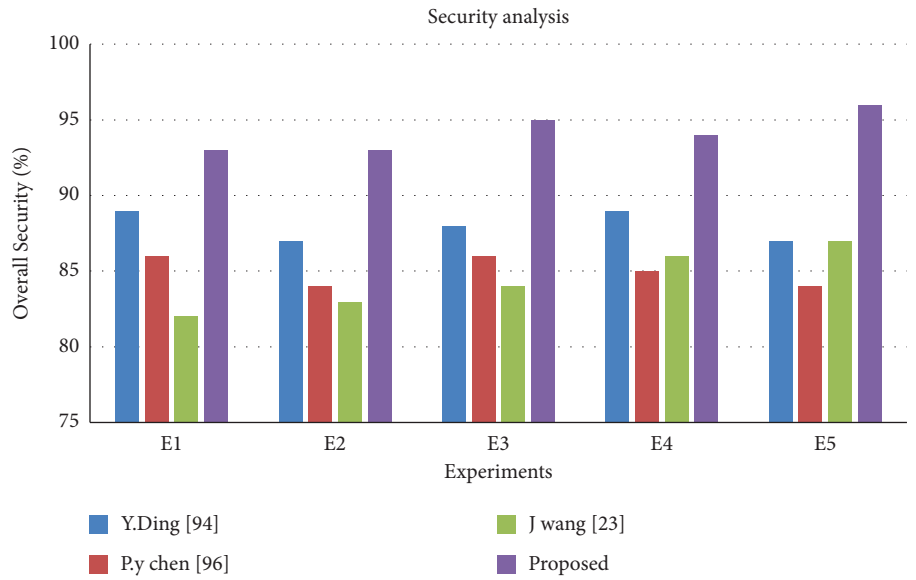

Figure 11: Security analysis of the proposed system.

tested. Based on the experimental verification, this survey provided the guidelines for the development of intelligent IDS for IoT.

7. Conclusion and Future Challenges

In this paper, we provide a detailed analysis of IDS developed in the IoT environment that are presented by various researchers. In addition, we proposed a new intelligent IDS using fuzzy CNN to overcome the limitations of the IDSs present in the literature. The IDS in IoT presented in this paper was subdivided into four categories, namely, IDS based on anomaly detection, signature, specifications, and hybrid method for performing the comparative analysis. Under each category, an in-depth analysis of various existing IDS protocols is carried out. Moreover, the performance analysis of each category of IDS are carried out based on various performance metrics like network resource optimization, false positive intrusion detection rate, and scalability. Finally, the intelligent IDS which is developed in this work utilizes information gain ratio for selecting prominent features. For intrusion classification, the intelligent fuzzy-based CNN classifier is employed to accurately classify the intrusion based on QoS parameters. The proposed intelligent classifier is simulated using the NS3 simulator, and it is compared with the performance metrics, namely, packet delivery ratio, delay, average energy consumption, network life time, DoS attack, probe attack, L2R attack, R2L attack, and finally security analysis. The proposed system is enhanced by security by more than 10%, the network life time by more than 5% and the detection accuracy by 4% than the existing works. The future plan of the suggested system is to apply the proposed intelligent IDS to an IoT-based network with dynamic network topology.

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.

Authors' Contributions

Dr. A Kannan, senior professor, Vellore Institute of Technology, has provided the expert advice and carried out the revision of the manuscript.

Acknowledgments

We thank the Vellore Institute of Technology, Vellore, India for providing the funding to this manuscript.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] P. L. R. Chze and K. S. Leong, *A Secure Multi-Hop Routing for IoT Communication*, pp. 428–432, IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014.

[3] N. N. Srinidhi, S. Dilip Kumar, and K. R. Venugopal, "Network optimizations in the internet of things: a review," *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 1–21, 2019.

[4] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[5] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[6] S. R. Zahra and M. Ahsan Chishti, "RansomWare and internet of things: a new security nightmare," in *Proceedings of the 2019 9th International Conference on Cloud Computing*, pp. 551–555, Noida, India, November 2019.

[7] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, Second Quarter 2019.

[8] L. Liang, K. Zheng, Q. Sheng, and X. Huang, "A denial of service attack method for an IoT system," in *Proceedings of the 2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, pp. 360–364, Fuzhou, June 2016.

[9] C. Gray, R. Ayre, K. Hinton, and R. S. Tucker, "Power Consumption of IoT Access Network Technologies," in *Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW)*, pp. 2818–2823, London, June 2015.

[10] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[11] J. M. Carracedo, M. Milliken, P. Kaur Chouhan et al., "Cryptography for security in IoT," in *Proceedings of the 5th International Conference on Internet of Things: Systems*, pp. 23–30, Berlin, April 2018.

[12] A. Karati, C. I. Fan, and R. H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10431–10440, Dec, 2019.

[13] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3474–3484, April 2020.

[14] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[15] I. Kang, M. K. Jeong, and D. Kong, "A differentiated one-class classification method with applications to intrusion detectiofication method with applications to intrusion detection," *Expert Systems with Applications*, vol. 39, no. 4, pp. 3899–3905, 2012.

[16] M. Eskandari, Z. H. Janjua, M. Vecchio, F. Antonelli, and I. D. S. Passban, "Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, 2020.

[17] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[18] R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," in *Proceedings of the 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, pp. 141–147, Mysuru, May 2017.

[19] A. Le, J. Loo, and M. Chai, "A specification-based IDS for detecting attacks on RPL-based network topology," *Information*, vol. 7, no. 2, p. 25, 2016.

[20] R. Sekar, A. Gupta, J. Frullo et al., "Specification-based anomaly detection: a new approach for detecting network intrusions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 265–274, Zhengzhou China, March 2002.

[21] X. Tong, Z. Wang, and H. Yu, "A research using hybrid RBF/Elman neural networks for intrusion detection system secure model," *Computer Physics Communications*, vol. 180, no. 10, pp. 1795–1801, 2009.

[22] U. Sheikh, H. Rahman, H. S. Al-Qahtani, T. Kumar Hazra, and N. U. Sheikh, "Countermeasure of Attack Vectors Using Signature-Based IDS in IoT Environments," in *Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 1130–1136, Zhengzhou China, November 2019.

[23] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, and A. Kannan, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT," *Computer Networks*, vol. 151, pp. 211–223, 2019.

[24] S. V. N. Santhosh Kumar, Y. Palanichamy, M. Selvi, S. Ganapathy, and A. Kannan, "Energy efficient secured K means based unequal fuzzy clustering algorithm for efficient reprogramming in wireless sensor networks," *Wireless Networks*, Springer, Berlin, Germany, pp. 1–22, 2021.

[25] L. Jingna, "An analysis on DoS attack and defense technology," in *Proceedings of the 2012 7th International Conference on Computer Science & Education (ICCSE)*, pp. 1102–1105, Zhengzhou China, January 2012.

[26] C. Zhang and R. Green, "Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network," in *Proceedings of the 18th Symposium on Communications & Networking*, pp. 8–15, Berlin, Germany, June 2015.

[27] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 110, no. 4, pp. 1637–1658, 2020.

[28] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis &defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259–268, Montreal, QC, Canada, April 2004.

[29] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil attack detection scheme for a centralized clustering-based hierarchical network," *Proceedings of the Trust- com/BigDataSE/ISPA*, vol. 1, pp. 318–325, 2015.

[30] F. Gara, L. B. Saad, and R. B. Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs," in *Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 276–281, Valencia, Spain, June 2017.

[31] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proceedings of the 20th International Parallel and Distributed Processing Symposium*, p. 8, Cluj-Napoca, Romania, April 2006.

[32] A. Mathur and M. Newe, "Defence against black hole and selective forwarding attacks for medical WSNs" in the IoT," *Sensors*, vol. 16, no. 1, p. 118, 2016.

[33] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in internet of things," *International Journal of Computer Application*, vol. 121, no. 9, pp. 1–9, 2015.

[34] G. Soni and R. Sudhakar, "A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT," in *Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 377–383, Noida, India, September 2020.

[35] W. Meng, W. Li, and L.-F. Kwok, "Efm: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism," *Computers & Security*, vol. 43, pp. 189–204, 2014.

[36] F. Ahmed and Y.-B. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," *Security and Communication Networks*, vol. 9, no. 18, pp. 5143–5154, 2016.

[37] Y. Liu, M. Ma, X. Liu, N. N. Xiong, A. Liu, and Y. Zhu, "Design and analysis of probing route to defense sink-hole attacks for internet of things security," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 356–372, 2020.

[38] K. Mabodi, M. Yusefi, S. Zandiyan, K. Mabodi, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *The Journal of Supercomputing*, vol. 2, pp. 1–26, 2020.

[39] S. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: challenges, solutions and future directions," in *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5772–5781, Koloa, December 2016.

[40] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[41] M. H. Ali, B. A. D. Al Mohammed, A. Ismail, and M. F. Zolkipli, "A new intrusion detection system based on fast learning network and particle swarm optimization," *IEEE Access*, vol. 6, pp. 20255–20261, 2018.

[42] S. Ganapathy, P. Vijayakumar, Y. Palanichamy, and A. Kannan, "An intelligent CRF based feature selection for effective intrusion detection," *The International Arab Journal of Information Technology*, vol. 13, no. 1, pp. 44–50, 2016.

[43] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Applications*, pp. 1–6, Ottawa, July 2009.

[44] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Computers & Security*, vol. 31, no. 3, pp. 357–374, 2012.

[45] A. Jamalipour and S. Murali, "A taxonomy of machine learning based intrusion detection systems for the internet of things: a survey," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9444–9466, 2022.

[46] R. Rajendran, S. V. N. Santhosh Kumar, Y. Palanichamy, and K. Arputharaj, "Detection of DoS attacks in cloud networks using intelligent rule based classification system," *Cluster Computing*, vol. 22, no. 1, pp. 423–434, 2019.

[47] W. Haider, J. Hu, J. Slay, B. Turnbull, and Y. Xie, "Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling," *Journal of Network and Computer Applications*, vol. 87, pp. 185–192, 2017.

[48] I. Sharafaldin and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 108–116, Portugal, January 2018.

[49] W. Lee, S. J. Stolfo, P. K. Chan et al., "Real time data mining-based intrusion detection," *Proceedings of Information Survivability Conference and Exposition II*, vol. 1, pp. 89–100, 2001.

[50] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," in *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, pp. 29–36, Raleigh, North Carolina, July 2011.

[51] S. S. Sivatha Sindhu, S. Geetha, and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," *Expert Systems With Applications*, vol. 39, 2012.

[52] B. Senthilnayaki, K. Venkatalakshmi, and A. Kannan, "Intrusion detection system using fuzzy rough set feature selection and modified KNN classifier," *The International Arab Journal of Information Technology*, vol. 16, no. 4, pp. 746–753, 2019.

[53] P. Puneeth, T. Bhanuteja, M. Selvi, S. V. N. Santhoshkumar, and A. Kannan, "Privacy-enhanced access control for providing efficient security in cloud environment," *Advances in Intelligent Systems and Computing Proceedings of Third International Conference on Intelligent Computing, Information and Control Systems*, vol. 1415, pp. 815–825, 2022.

[54] S. Vijayalakshmi, S. Bose, G. Logeswari, and T. Anitha, "Hybrid defense mechanism against malicious packet dropping attack for MANET using game Theory," *Cyber security and applications*, vol. 1, Article ID 100011, 2022.

[55] S. Veeraraghavan, S. Bose, K. Anand, and A. Kannan, "An intelligent agent based approach for intrusion detection and prevention in adhoc networks," *International Conference on Signal Processing, Communications and Networking ICSCN*, vol. 07, pp. 534–536, 2007.

[56] M. Selvi, R. Logambigai, S. Ganapathy, L. Sai Ramesh, H. K. Nehemiah, and A. Kannan, "Fuzzy temporal approach for energy efficient routing in WSN," *Proceedings of International Conference on Informatics and Analytics*, vol. 117, no. 5, pp. 1–117, 2016.

[57] R. Fotohi, M. Abdan, and S. Ghasemi, "A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks," *Journal of Grid Computing*, vol. 20, no. 3, pp. 22–26, 2022.

[58] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions," *Cluster Computing*, vol. 7, pp. 1–28, 2019.

[59] M. Mahdavisharif, S. Jamali, and R. Fotohi, "Big data-aware intrusion detection system in communication networks: a deep learning approach," *Journal of Grid Computing*, vol. 19, pp. 46–28, 2021.

[60] S. Bose and A. Kannan, "Detecting denial of service attacks using cross layer based intrusion detection system in wireless ad hoc networks," in *Proceedings of the International Conference on Signal Processing, Communications and Networking, ICSCN'08, IEEE*, pp. 182–188, Chennai, India, March 2008.

[61] S. Viswanathan, R. S. Bhuvaneswaran, S. Ganapathy, and A. Kannan, "Euler phi function and gamma function based elliptic curve encryption for secured group communication," *Wireless Personal Communications*, vol. 125, no. 1, pp. 421–451, 2022.

[62] G. Logeswari, S. Bose, and T. Anitha, "An intrusion detection system for SDN using machine learning," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 867–880, 2023.

[63] S. Latif, M. Driss, W. Boulila et al., "Deep learning for the Industrial Internet of Things (IIoT): a comprehensive survey of techniques, implementation frameworks, potential applications, and future directions," *Sensors*, vol. 21, no. 22, p. 7518, 2021.

[64] M. Y. Aldarwbi, A. H. Lashkari, and A. A. Ghorbani, "The sound of intrusion: a novel network intrusion detection system," *Computers & Electrical Engineering*, vol. 104, Article ID 108455, 2022.

[65] W. Qiu, Y. Ma, X. Chen, H. Yu, and L. Chen, "Hybrid intrusion detection system based on Dempster-Shafer evidence theory," *Computers & Security*, vol. 117, Article ID 102709, 2022.

[66] T. Sherasiya, H. Upadhyay, and H. Patel, "A survey: intrusion detection system for internet of things," *International Journal on Computer Science and Engineering*, vol. 5, no. 2, pp. 91–98, 2016.

[67] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[68] S. Anwar, J. Mohamad Zain, M. F. Zolkipli et al., "From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, pp. 39–24, 2017.

[69] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: a top–down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[70] Y. Zhang, N. Meratnia, and P. J. Havinga, "Outlier detection techniques for wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 159–170, 2010.

[71] S. Owais, V. Snasel, P. Kromer, and A. Abraham, "Survey: using genetic algorithm approach in intrusion detection systems techniques," in *Proceedings of the 2008 7th Computer Information Systems and Industrial Management Applications*, pp. 300–307, Ostrava, Czech Republic, June 2008.

[72] P. Ramasubramanian and A. Kannan, "A genetic-algorithm based neural network short-term forecasting framework for database intrusion prediction system," *Soft Computing*, vol. 10, no. 8, pp. 699–714, 2006.

[73] P. Wang, L. Shi, B. Wang, Y. Wu, and Y. Liu, "Survey on HMM based anomaly intrusion detection using system calls," in *Proceedings of the 2010 5th International Conference on Computer Science & Education*, pp. 102–105, Ostrava, Czech Republic, June 2010.

[74] R. G. M. Helali, "Data mining based network intrusion detection system: a survey," in *Proceedings of the Novel Algorithms and Techniques in Telecommunications and Networking*, pp. 501–505, Newyork, NY, USA, March 2010.

[75] C. Kolias, G. Kambourakis, and M. Maragoudakis, "Swarm intelligence in intrusion detection: a survey," *Computers & Security*, vol. 30, no. 8, pp. 625–642, 2011.

[76] N. Jaisankar, S. `pathy, Y. Palanichamy, A. Kannan, and K. Anand, "An intelligent agent based intrusion detection system using fuzzy rough set based outlier detection," *Soft Computing Techniques in Vision Science*, vol. 395, pp. 147–153, 2012.

[77] K. Selvakumar, L. Sairamesh, and A. Kannan, "Wise intrusion detection system using fuzzy rough set-based feature extraction and classification algorithms," *International Journal of Operational Research*, vol. 35, no. 1, pp. 87–107, 2019.

[78] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in *Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 84–90, Vienna, Austria, April 2016.

[79] K. Thangaramya, K. Kulothungan, S. Indira Gandhi, M. Selvi, S. Kumar, and A. Kannan, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN," *Soft Computing*, vol. 24, pp. 16483–16497, 2020.

[80] M. Ammar, G. Russello, and B. Crispo, "Internet of things: a survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[81] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[82] W. Yassin, Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "Intrusion detection based on K-Means clustering and Naïve Bayes classification," in *Proceedings of the 2011 7th International Conference on Information Technology in Asia*, pp. 1–6, Vienna, Austria, June 2011.

[83] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo et al., "Data randomization and cluster-based partitioning for botnet intrusion detection," *IEEE Transactions on Cybernetics*, vol. 46, no. 8, pp. 1796–1806, Aug, 2016.

[84] D. E. Denning, "An Intrusion Detection Model," *IEEE Transaction on Software Engineering*, vol. 13, pp. 222–232, 1987.

[85] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in *Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, pp. 1169–1176, Taipei, June 2017.

[86] A. A. Gendreau and M. Moorman, "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things," in *Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 84–90, Vienna, March 2016.

[87] H. E. Hendaoui and H. Youssef, "FID: fuzzy based intrusion detection for distributed smart devices," in *Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1330–1337, Hammamet, January 2017.

[88] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: a comprehensive investigation," *Computer Networks*, vol. 160, no. No.4, pp. 165–191, 2019.

[89] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Systems with Applications*, vol. 29, no. 4, pp. 713–722, 2005.

[90] G. Perdisci, G. G. Roberto, and W. Lee, "Using an Ensemble of One-Class SVM Classifiers to Harden Payload-Based Anomaly Detection Systems," in *Proceedings of the 6th International Conference on Data Mining (ICDM'06)*, pp. 488–498, Newyork, NY, USA, March 2006.

[91] R. Fu, K. Zheng, D. Zhang, and Y. Yang, "An intrusion detection scheme based on anomaly mining in Internet of Things," in *Proceedings of the 4th IET International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2011)*, pp. 315–320, Kyoto, Japan, June 2011.

[92] Y. Ding, X. W. Zhou, Z. M. Cheng, and F. H. Lin, "A security differential game model for sensor networks in context of the internet of things," *Wireless Personal Communications*, vol. 72, no. 1, pp. 375–388, 2013.

[93] S. Rajasegarar, A. Gluhak, M. Ali Imran et al., "Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks," *Pattern Recognition*, vol. 47, no. 9, pp. 2867–2879, 2014.

[94] P. Y. Chen, S. M. Cheng, and K. C. Chen, "Information fusion to defend intentional attack in internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 337–348, 2014.

[95] H. S. Ham, H. H. Kim, M. S. Kim, and M. J. Choi, "Linear SVM-based android mal- ware detection for reliable IoT services," *Journal of Applied Mathematics*, vol. 2014, Article ID 594501, 10 pages, 2014.

[96] J. Wang, Q. Kuang, and S. Duan, "A new online anomaly learning and detection for large-scale service of Internet of Thing," *Personal and Ubiquitous Computing*, vol. 19, no. 7, pp. 1021–1031, 2015.

[97] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 606–611, IEEE, Ottawa, ON, Canada, May 2015.

[98] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. Khannah Nehemiah, and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1475–1490, 2019.

[99] D. H. Summerville, K. M. Zach, and Y. Chen, "Ultra-lightweight deep packet anomaly detection for Internet of Things devices," in *Proceedings of the 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–8, Nanjing, China, June 2015.

[100] V. Eliseev and A. Gurina, "Algorithms for network server anomaly behaviour detection without traffic content inspection," in *Proceedings of the 9th Inter- National Conference on Security of Information and Networks*, pp. 67–71, ACM, Newyork NY USA, Feburary 2016.

[101] K. Grgic, D. Zagar, and V. KrizanovicCik, "System for malicious node detection in IPv6-based wireless sensor networks," *Journal of Sensors*, vol. 2016, Article ID 6206353, 20 pages, 2016.

[102] K. Sonar and H. Upadhyay, "An approach to secure internet of things against DDoS," in *Proceedings of the International Conference on ICT for Sustainable Development*, pp. 367–376, 2016.

[103] S. Ganapathy, P. Yogesh, and A. Kannan, "Intelligent agent based intrusion detection system using enhanced multiclass SVM," *Computational Intelligence and Neuroscience*, vol. 2012, Article ID 850259, 10 pages, 2012.

[104] E. Hodo, X. Bellekens, A. Hamilton et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *Proceedings of the 2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, NewYork, NY, USA, June 2016.

[105] S. O. Amin, M. S. Siddiqui, C. S. Hong, and J. Choe, "A novel coding scheme to implement signature based IDS in IP based sensor networks," in *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management–Workshops*, pp. 269–274, New York, NY, USA, June 2009.

[106] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systemsfish coptimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, 2015.

[107] D. Oh, D. Kim, and W. W. Ro, "A malicious pattern detection engine for embedded security systems in the Internet of Things," *Sensors*, vol. 14, no. 12, pp. 24188–24211, 2014.

[108] H. Sun, R. Wang and J. S. Buyya, CloudEyes: cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices," *Software: Practice and Experience*, vol. 47, no. 3, pp. 421–441, 2016.

[109] A. R. Rajeswari, K. Kulothungan, S. Ganapathy, and A. Kannan, "A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1076–1096, 2019.

[110] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning au- tomata based solution for preventing distributed denial of service in Internet of things," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber*, pp. 114–122, Washington, DC, USA, June 2011.

[111] I. Murynets and R. P. Jover, "Anomaly detection in cellular machine-to-machine communications," in *Proceedings of the 2013 IEEE International Conference on Communications (ICC)*, pp. 2138–2143, IEEE, June 2013.

[112] Y. Xia, H. Lin, and L. Xu, "An AGV mechanism based secure routing protocol for internet of things," in *Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing*, pp. 662–666, Newyork, NY, USA, June 2015.

[113] Q. D. La, T. Q. S. Quek, S. Lee, and H. Jin, "Deceptive attack and defense game in honeypot-enabled networks for the internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, 2016.

[114] M. Surendar and A. Umamakeswari, "InDReS: an intrusion detection and response system for internet of things with 6LoWPAN," in *Proceedings of the International Conference on Wireless Communications, Signal Processing and Net-Working (WiSPNET)*, pp. 1903–1908, Chennai, India, March 2016.

[115] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, "An automata based intrusion detection method for internet of things," *Mobile Information Systems*, vol. 2017, Article ID 1750637, 13 pages, 2017.

[116] S. Bose, S. Bharathimurugan, and A. Kannan, "Multi-layer integrated anomaly intrusion detection system for mobile adhoc networks," in *Proceedings of the 2007 IEEE International Conference on Signal Processing, Communications and Network*, pp. 360–365, Chennai, India, June 2007.

[117] L. Liu, B. Xu, X. Zhang, and X. Wu, "An intrusion detection method for internet of things based on suppressed fuzzy clustering," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, Article ID 113, 2018.

[118] S. O. Amin, Y. jig Yoon, M. S. Siddiqui, and C. S. Hong, "A novel intrusion detection framework for IP-based sensor networks," in *Proceedings of the International Conference on Information Networking, 20 09*, pp. 1–3, Newyork, NY, USA, April 2009.

[119] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detec- tion in 6LoWPAN based internet of things," in *Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 600–607, Berlin, Germany, June 2013.

[120] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusion detection in the in- ternet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[121] T. Matsunaga and I. Toyoda, "Low false alarm attackers detection in RPL by considering timing inconstancy between the rank measurements," *IEICE Communications Express*, vol. 4, no. 2, pp. 44–49, 2015.

[122] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology," in *Proceedings of the 2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Dublin, Ireland, June 2016.

[123] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy*, pp. 31–38, Seoul, Korea, May 2017.

[124] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalis - a system for knowledge–driven adaptable intrusion detection for the internet of things," in *Proceedings of the 2017 IEEE 37th International Conference on Distributed Comput- Ing Systems (ICDCS)*, pp. 656–666, Atlanta, GA, USA, April 2017.

[125] H. Sedjelmaci and T. Senouci, "An accurate security game for low-resource IoT devices," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381–9393, 2017.

[126] S. W. Lin, K. C. Ying, C. Y. Lee, and Z. J. Lee, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection," *Applied Soft Computing*, vol. 12, no. 10, pp. 3285–3290, 2012.

[127] K. Anand, S. Ganapathy, K. Kulothungan, P. Yogesh, and A. Kannan, "A rule based approach for attribute selection and intrusion detection in wireless sensor networks," *Procedia Engineering*, vol. 38, pp. 1658–1664, 2012.

[128] L. Prema Rajeswari and A. Kannan, "An active rule approach for network intrusion detection with enhanced C4.5 Algorithm," *International Journal of Communication*, vol. 4, pp. 285–385, 2008.

[129] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019.

[130] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, "Network intrusion detection: based on deep hierarchical network and original flow data," *IEEE Access*, vol. 7, pp. 37004–37016, 2019.

[131] S. Ganapathy, K. Kulothungan, S. Muthuraj Kumar, M. Vijayalakshmi, P. Yogesh, and A. Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," *EURASIP Journal on*

Wireless Communications and Networking, vol. 2013, no. 1, pp. 271–316, 2013.

[132] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. Santhosh Kumar, M. Selvi, and K. Arputharaj, "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," *IET Communications*, vol. 14, no. 5, pp. 888–895, 2020.

[133] A. L. Muna, E. Sitnikova, N. HawawrehMoustafa, and S. Elena, "Identification of malicious activities in industrial internet of things based on deep learning modelfication of malicious activities in industrial internet of things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[134] C. Xiang and S. M. Lim, "Design of multiple-level hybrid classifier for intrusion detection system," *IEEE Transactions on System, Man, Cybernetics, Part A, Cybernetics*, vol. 2, no. 28, pp. 117–122, 2002.

[135] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018.

[136] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.