ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0373

A COMPARATIVE STUDY ON INTRUSION DETECTION SYSTEMS FOR SECURED COMMUNICATION IN INTERNET OF THINGS

R. Anushiya and V.S. Lavanya
Department of Computer Science, P.K.R. Arts College for Women, India

Abstract

The virtual and physical worlds are bridged using the largest digital mega-trend called the Internet of Things (IoT). Between mankind, new interactions and new business models are emerging due to the incremental growth in the Internet, machines, objects, and people connectivity. Secured communication is a typical challenge that is raised due to IoT high diversity, restricted computational resources, and protocols and standards. Because of the huge attack surface in IoT networks, they are highly vulnerable to various attacks, even with some security measures. So, for detecting attacks, it is necessary to design defense mechanisms. In IoT environments, it is highly crucial to have security defense measures like Intrusion Detection Systems (IDS). Hence, authentication and encryption traditional security countermeasures are not sufficient. At network level, to solve those issues and to protect Internet-connected frameworks, major solutions are provided by IDS. Highly unique challenges are faced by IoT specific characteristics like malware detection, ransomware, processor architecture heterogeneity, and the gap in security design. However, as in literature, various problems are raised in traditional IDS, like the high false alarm rate. In IoT, for intrusion detection, a detailed study of traditional Deep Learning (DL) and Machine Learning (ML) techniques and recent technologies is presented in this review. For presenting every selected work objective and methodology, they are analysed and this review work discusses their results. IoT systems cannot be secured by applying traditional security techniques directly due to their computational constraints and intrinsic resources. In real time, on IoT devices, unknown and known attacks are detected using ML techniques in IDS. An IDS is presented in this review and its working is independent of network structure and IoT protocols. This IDS do not require any prior knowledge of security threats. Therefore, for providing security as a service to IoT networks, an artificially intelligent IDS is developed. This review paper provides a clear discussion of various attack detection techniques, along with their benefits and drawbacks.

Keywords:

Genetic Algorithms (GA), Deep Learning (DL), Intrusion Detection Systems (IDS), Internet of Things (IoT)

1. INTRODUCTION

The virtual and physical worlds are bridged using the largest digital mega-trend called the Internet of Things (IoT). Between humankind, new interactions and new business models are emerging due to the incremental growth in the Internet, machines, objects, and people connectivity. Physical moving objects called “things are interconnected using IoT via the internet using sensors, electronic chips, and other hardware forms. Radio Frequency Identifier (RFID) tags are used to identify every device globally. With other connected nodes, these smart objects communicate and remotely they are able to be controlled and monitored. For a wide range of applications, IoT offers cloud computing services, service industries, and smart physical objects with pervasive connectivity. By 2020, there is a possibility to increase the connected device count through the internet to around 50 billion, as stated by IBM [1].

The number of communication networks will grow as smart objects connect and large amounts of data are shared via cloud infrastructure. The protection and entertainment, health, e-banking, e-shopping, education system, smart city development, and industry management for Human beings are using these IoT enabled technologies [2]. More interconnected objects, services, and people are the result due to the rapid growth in IoT. IoT also facilitates people lives. Deployment of IoT is restricted if it is not able to provide the required personal information and privacy security. It is highly important to develop a secured IoT environment. Electronic device networks are termed “IoT and use wireless technologies to communicate with each other. Data is exchanged between them, processed, and stored.

In various applications like the military, industry, transportation, smart homes, and IoT devices are used [3]. Security challenges are raised due to high diversity, restricted computational resources, protocols and standards of IoT device. By manufacturing setting, default passwords are set for IoT devices, which makes them easy for brute force attacks. Network security enhancement is highly important due to the computer system and its continuous growth. An interconnected system availability, integrity, and confidentiality needs to be preserved to maintain its security. Threats known as intrusions are used to attempt to destroy and violate the system availability, integrity, and confidentiality.

For malicious behaviors, the network is monitored using hardware devices or software services called intrusion detection systems. Based on the infrastructure type to be integrated, they are classified as network-based, application-based, and host-based networks [4]. New zero-day or unseen attacks will not be detected using these techniques. In a network, unusual deviations from normal monitored behaviours are examined for detecting intrusions in IDS based on anomalies. Anomaly detection techniques do not rely on pre-defined databases. Unknown attacks are able to be detected using this. Different intelligent detection techniques like semi-supervised, supervised and unsupervised machine learning, statistical analysis as well as techniques based on knowledge or hybrids of them are used in IDS based on anomaly. Typically, huge datasets are used for extracting information patterns in machine learning (ML) techniques. With respect to probability distribution, malicious events are spotted by using a network packet statistical attributes in statistical methods. Expert systems are adopted in knowledge-based techniques. For classifying network data as malicious or normal according to its attributes, smart leaning algorithms are used in ML IDS. Highly effective learning and searching algorithms are needed to deal with ever-increasing IoT devices and data with high dimensionality.

Metaheuristics are a well-regarded option of algorithms for solving hard-optimization problems in an acceptable time period. Searching for an optimal solution in such a vast search space is a difficult challenge. Metaheuristic ability to search on a global scale makes them a good alternative for hard-optimization problems. A strong global optimization metaheuristic algorithm is one that can strike a balance between discovery (global) and manipulation (local). Highly tough hard-optimization problems are able to be solved using metaheuristics, and they can be implemented easily [5]. Evolutionary algorithms based on trajectory or evolutionary algorithms based on population are the major classes of them. Population-based techniques are highly exploration-oriented techniques like Genetic Algorithm (GA). Algorithms based on Trajectory are exploitation-oriented techniques like Simulated Annealing (SA). They are also termed as single solution metaheuristics.

Swarm based and evolutionary algorithms are major classes of algorithms based on population. For solving multi-objective optimization problems, population-based algorithms are most widely used due to their structural nature [6]. For optimization, there exist two or three objective functions in multi-objective problems: maximization, minimization, or both. There is a conflict between these objectives. Therefore, enhancement of one object will degrade another objective. Therefore, for both objectives, multi-objective optimization output is not alone a solution. A trade-off solution set called the Pareto optimal set needs to be used. An external memory termed an archive is used in Multi-objective Particle Swarm Optimization (MOPSO). During the search process, in every iteration, computed non-dominated solutions are stored using an archive, which is considered as a major objective. For IoTs, classification error rate minimization and feature selection problems are addressed here. A feature selection technique based on the wrapper is the MOPSO algorithm, which is used to train the real-collected IoT data from the UCI repository to train and test the five unseen attacks.

Moreover, a modified multi-objective particle swarm optimization algorithm based on levy flight and double-archive mechanism (MOPSO-LFDA) is proposed to enhance diversity of solutions. The authentication and encryption traditional security countermeasures are not sufficient. In real time, unknown or known attacks are detected using ML techniques in IDS. So, for IoT intrusion detection, this review work identifies the best Deep Learning (DL) technique. Data mining techniques are integrated for spotting outliers and threats in smart IDS. Unseen threats have also been recognised by generalising smart IDS. Therefore, cross-training is applied in this review, where one set of attacks is used for training and another set of attacks is used for testing the algorithm.

The following gives the organisation of this paper. The background study is summarised in section 2 and it has three subdivisions, as mentioned below. Section 2.1 presents traditional techniques used for detecting intrusions in IoT. Section 2.2 presents ML techniques used to detect intrusions in IoT, and section 2.3 presents DL methods used for detecting intrusions in IoT. Issues from existing methods are introduced in section 3. Section 4 discusses the inferences that provides solutions to the current problems. Finally, a summary of the entire work is presented in section 5

2. BACKGROUND STUDY

In close related IoT networks like Cloud Computing (CC), mobile networks, and Wireless Sensor Networks (WSN), and in IoT, to articulate threat detection, various intrusion detection techniques have been proposed in the last few years. Validation strategy, threats, placement strategy, and detection techniques form the basis for IDS in IoT. IoT security development is still rudimentary. Across different IoT technologies, a wide attack range and placement techniques need to be adopted. Section 2.1 describes traditional techniques for detecting intrusions in IoT, Section 2.2 describes ML techniques for detecting intrusions in IoT, and Section 2.3 describes DL methods for detecting intrusions in IoT.

2.1 REVIEW OF TRADITIONAL METHODS FOR INTRUSION DETECTION IN IOT

Meidan et al. [7] propose an anomaly detection technique based on networks. Network behaviour snapshots are extracted using this method. From compromised IoT devices, anomalous network traffic emanating is detected using deep auto-encoders. For every device, deep auto-encoders are used for detecting IoT botnet attacks. From benign traffic data, statistical features are extracted and are used for training every device. Device compromise is indicated using detected anomalies while applying it to new IoT device data which is infected possibly. Continuous monitoring, anomaly detector training, feature extraction and data collection are the major stages in this proposed technique. In an enterprise setting, deployed IoT devices, which are infected by real-world botnets, are represented authentically and genuine attacks are executed. In the lab, nine commercial IoT devices that are infected are used for evaluating this technique. Two well-known botnets based on IoT called Bashlite and Mirai are used. Instant and accurate attack detection is done using the proposed technique as demonstrated in the evaluation. From a compromised IoT device, these attacks are launched which are part of a botnet.

In the Internet of Things (IoT), for medical image security, the Grasshopper Optimization and Particle Swarm Optimization (GO-PSO) technique was developed by Elhoseny et al. [8]. IoT medical image security is investigated by this using an innovative cryptographic model which has optimization techniques. In most cases, in hospitals, cloud servers are used for storing patient data. So, there is a need to ensure its security. For medical images, effective storage and secure transmission, there is a need to have another framework that is interleaved with patient information. In elliptic curve cryptography, hybrid swarm optimization, i.e., GO-PSO, is used for selecting the optimal key, which enhances the decryption and encryption process security level. In the IoT framework, medical images are secured using this technique. Results are compared from this execution, which identified a diverse encryption algorithm including its optimization technique. This algorithm produces a structural similarity index of 1 and peak signal-to-noise ratio values of 59.45dB.

For IoT botnet detection, Al Shorman et al. [9] introduced One Class Support Vector Machine (OCSVM) and the Grey Wolf Optimization algorithm (GWO). A recent swarm intelligence algorithm known as “GWO efficiency is being used to detect compromised IoT devices as a result of IoT botnet attacks.The OCSVM hyper parameters are optimised using this, and features, which are used for describing the IoT botnet problem, can also be computed using this. Over a new real benchmark dataset version, typical anomaly detection evaluation measures are used for evaluating the proposed method performance, and it proves the proposed method efficiency. For all IoT device types, with respect to G-mean, false positive, and true positive rate, all other algorithms are outperformed by the proposed technique, as shown in experimental results. This method minimises the selected feature count significantly while achieving low detection time.

For DDoS attack detection on the Internet of things (IoT), an Intrusion Prevention Algorithm (IPAM) has been formulated by Aldaej [10]. In modern Internet of things (IoT) devices, bandwidth is consumed by DDoS attacks. So, to enhance network and IoT device cyber security, a prevention technique has been proposed. In these networks, security is a major issue as they have some large, unpredictable node movements and they are self-configuring, wireless, and they do not require a pre-existing infrastructure. A DDoS attack is a highly ruthless challenge, and its detection is highly difficult. Network performance is greatly decreased because of this. Based on this bandwidth attack investigation and analysis, they proposed a technique. The Attacker nodes group is included in DDoS and is responsible for preventing legitimate users from accessing network resources and services.

For actively defending and preventing intrusions, procedures that are assumed as add-ons of IDS in IoT intrusion prevention systems. IDS detection procedures are used to detect DDoS attacks. Based on the proposed procedure, IDS generate a report after analysing the forensic analysis report. For resource-constrained IoT devices, a game theoretic technique for security is proposed by Sedjelmaci et al. [11]. Only during the expected time of the attack signature, the anomaly detection technique is activated. Between energy consumption, false positive rates, and detection rates, a balance is achieved using this. False positive counts can be minimised by combining these two detection methods.

A game theory-based reputation model is used to decrease false positive rates further. Current anomaly detection techniques are outperformed by this lightweight anomaly detection, as shown in the simulation results. For detecting attacks having a low false positive rate as well as a high detection rate, low energy is consumed by this in scaling mode, where there will be a high attacker and IoT device count. Current anomaly detection methods require high energy to exhibit a high detection rate. At every node, where nodes are not switching to idle time, permanent activation of these detection methods are required.

Zhou et al. [12] developed Intrusion Detection System (IDS) techniques such as Modified Particle Swarm Optimization (MPSO), game theory, and Universal-Low Energy Adaptive Cluster Hierarchy (U-LEACH). On cluster head nodes, a clustering algorithm termed “ULEACH is used for selecting IDS. Perceptual node heterogeneity is considered comprehensively using the ULEACH clustering algorithm, via optimising node threshold computation. In this, the node overall performance, energy consumption rate, and residual energy are considered.

To enhance the heterogeneous perceptual network performance and extend the system lifetime, node utilisation is enhanced using this strategy. For game theory based IoT heterogeneous perceptual networks, the IDS framework and dynamic intrusion detection model are established further. An optimal defence strategy for balancing the system energy consumption and detection efficiency is obtained by applying MPSO. Effective detection of multiple network attacks and energy consumption minimization are achieved using the proposed strategy, as shown in experimental results. For the Internet of Things (IDPIoT), an adaptive intrusion detection and prevention system was introduced by Bakhsh et al. [13]. This enhances security along with device growth which is connected to the Internet. Existing intrusion detection systems are investigated in order to propose IDPIoT, which improves security and network- and host-based functionality. After receiving the packet, its behaviour is examined by proposed IDPIoT and based on this, packets are dropped or blocked.

In packet headers, to detect any anomalies or certain behaviour types, every packet header is checked by a detector agent. Pre-defined detection rules like logging matching, activation of altering systems, are used for making comparisons of data in the system analyzer. It sounds for logging messages and alarms, and to the output module, they are sent. Output data is saved in this system and for a pre-configured destination like a database or log file, it alerts the system. One essential security part is implemented for accomplishing major goals, which are the prevention system and intrusion detection. Against cyber-attacks, for IoT devices, in IDS, Software Defined Networking (SDN), lightweight cryptography, robust access control, and robust authentication are formulated by Tabassum and Lebda [14]. Against IoTs and their protective measures, different attack types are provided by this. Against IoT layers, various other attacks are also launched. These attacks are devastating and recurrent.

In IoTs, for preventing and detecting malicious activities, it is mandatory to secure endpoints, monitor the network and protect data in transfer. Thus, for securing data during transfer, in sensitive data storage and settings & privileges, they proposed a framework incorporating intrusion detection systems, lightweight cryptography, Robust Access Control and Robust Authentication. Using programming, the entire network is controlled securely via a trendy networking paradigm called SDN. For IDS, emerging fields are Artificial Intelligence (AI) and ML. Without any programming, computational learning theory and pattern recognition cognitive functions allow a system for deciding, deducing, and learning. In addition, it provided various metrics used in IDS for identifying various attacks. Because of its holistic approach to different combinations of potential security mechanisms, for IoT architecture, a valuable contribution is the proposed framework. With respect to usability, performance, and security, a framework can be implemented in the future and its effectiveness can be validated.

Using a pattern matching algorithm, a signature-based intrusion detection system is proposed by Sheikh et al. [15]. Known cyber-attack vectors like ipseep and smurfare detected effectively using this. Effective characterization and detection of attacks can be done effectively using the proposed algorithm, as shown in empirical evaluations done via real-world datasets with a very low false alarm rate. Simulation results suggest an optimistic scope for future research. This off-line IDS is transited as a real-time efficient Intrusion Detection and Prevention System (IDPS) using continuous endeavours.

Table.1. Inferences of Traditional Methods for Intrusion Detection in IoT

Author	Method name	Advantages	Disadvantages
Meidan et al. [7]	Network-based anomaly detection	Detect anomalous network traffic emanating	Traffic predictability are not defined and investigated empirically and theoretically.
Elhoseny et al. [8]	Grasshopper Optimization and Particle Swarm Optimization (GO-PSO)	Medical image security	Tamper localization scheme cannot be used for having content-based respectability as opposed to strict-integrity functionality
Al Shorman et al. [9]	Grey Wolf Optimization algorithm (GWO) and One Class Support Vector Machine (OCSVM)	IoT botnet detection	Worst local searching ability, slow convergence, worst solving precision
Aldaej [10]	Intrusion Prevention Algorithm (IPAM)	DDoS attack detection	It is only focused on DDoS attack detection
Sedjelmaci et al. [11]	Game theoretic technique	High detection rate	Secured wireless sensor network is not implemented with various low-power devices which are deployed in smart building
Zhou et al. [12]	Universal-Low Energy Adaptive Cluster Hierarchy (U-LEACH), game theory and Modified Particle Swarm Optimization (MPSO)	Reduces energy consumption	High dimensional space and has a low convergence rate
Bakhsh et al. [13]	Adaptive Intrusion Detection and Prevention system for Internet of Things (IDPIoT)	Detect any anomalies in packet header	It cannot support 5G networks for securing and building trust between network and service
Tabassum and Lebda [14]	Robust Authentication, Access Control, Software Defined Networking (SDN), Lightweight cryptography,	Identify various attacks against IoT layers	Large time-consuming
Sheikh et al. [15]	Pattern matching algorithm	Detects known cyber-attack vectors likesmurf and ipseep	It is not suitable for software privacy

These are used for network traffic detection with an aberrant nature and to safeguard networks from suspicious activities which are penetrated by networks. For the IoT, design architecture and an IDS methodology are proposed further. A search algorithm is used to detect different security breaches. This IDS system efficiency is shown using numerical results which were conducted using the NSL KDD cup dataset.

2.2 REVIEW OF ML METHODS FOR INTRUSION DETECTION IN IOT

Moustafa et al. [16] built an Artificial Neural Network (ANN), Naive Bayes (NB), and Decision Tree (DT) for securing Internet of Things network traffic (IoT). In IoT networks, an ensemble intrusion prevention approach is used to prevent disruptive incidents, such as botnet attacks against MQTT, HTTP and DNS protocols. Based on the feature analysis of these protocols, a new mathematical flow features are created.

Then, using these three ML methods, an AdaBoost ensemble learning system is built to analyse these feature effects and effectively identify malicious events. The proposed features are extracted and the ensemble methodology is evaluated using the UNSW-NB15 and NIMS botnet datasets via simulated IoT sensor data.

Using correntropy and correlation coefficient tests, the experimental findings indicate that proposed features have possible natural and malicious behavioural characteristics. Furthermore, as compared to each classification technique used in the process and three other state-of-the-art techniques, the proposed ensemble technique has a high detection rate and a low false positive rate.

In intrusion detection for IoT systems, Deng et al. [17] implemented Fuzzy C-means clustering (FCM) and Principal Component Analysis (PCA). Internet security and some core security technologies, such as fault tolerance and intrusion, intrusion detection, privacy protection, routing security, authentication and access control, key management, and device architecture are discussed, as well as the features of networking security and security issues.

Various types of intrusion detection technology are addressed, as well as their implementation in the IoT architecture. Compare and contrast the use of various intrusion prevention systems, and make a plan for the next step of testing. Studying network attack techniques using data analysis and ML tools has been a hot topic.

Improving the network intrusion detection rate with a single class element or detection model is extremely difficult. The proposed model accuracy is checked using publicly available databases.

For IoT security, Xiao et al. [18] proposed Reinforcement Learning (RL). Learning-based IoT protection mechanisms, such as IoT authentication, access management, intrusion identification, and secure offloading, have been shown to be promising in protecting IoTs. ML methods like supervised, unsupervised, reinforcement learning is used in IoT security solutions.

To maintain data privacy, ML-based IoT authentication, access management, secure offloading, malware identification schemes are used. Discuss the obstacles that must be solved in order to incorporate these ML-based security schemes in real-world IoT systems in this article.

Azmoodeh et al. [19] proposed Support Vector Machine (SVM) and Random Forest (RF) for detecting ransomware attacks by tracking Android device power consumption. To differentiate ransomware from non-malicious programs, ransomware energy consumption special local fingerprint is used.

The energy consumption series of applications is divided into various power usage subsamples, which are then labelled to create aggregated subsample class marks. Then prove that with respect to F-measure, precision, recall and accuracy, the proposed solution outperforms KNN, NN, SVM, and RF. Prototyping a proposed solution for implementation in a real-world IoT network, with the objective of validation and improvement, is one of the next steps.

For detecting intrusions in IoT, Mohamed et al. [20] created a Random Forest (RF) and Neural Network (NN). IDS focused on ML methods to be deployed as a service on IoT platforms. To detect intrusions, RF was used as a classifier, and then a NN classifier was used to detect the categorization of intruders. The Raspberry Pi 3 will serve as the central computer for all of the suggested solution implementations. The system serves as a connection between the top-level application layer and the end-node layer.

Since sensors typically have limited computing capacity, this service is a better fit for securing IoT network end nodes by watching and monitoring odd activities. The second component is an RF and NN-based cloud-based intrusion detector. It collects IoT traffic from the system in question, extracts features, and then classifies the extracted features. The data point is defined as interference or not using radio frequency (RF).

The observed intrusion is classified using NN. While the proposed model effectively detects intrusions, intruder categorization suffers from low precision and high bias, according to the experimental findings.

For fog-based attack detection, Rathore and Park [21] proposed an Extreme Learning Machine (ELM)-based Semi-supervised Fuzzy C-Means (ESFCM). Fog computing and a recently proposed ESFCM are used to build a fog-based threat detection system. Fog computing, which is a form of cloud computing, allows for attack detection at the network edge and facilitates distributed attack detection.

To deal with the labelled data problem, the ESFCM approach employs a semi-supervised FCM algorithm and an ELM algorithm to provide reasonable generalisation efficiency at a faster detection rate. The proposed framework outperformed the centralised attack detection framework on the NSL-KDD dataset, showing that the proposed framework outperformed the centralised attack detection framework. It had an 11ms detection time and a high accuracy score, to be precise.

When the proposed ESFCM approach is compared to standard ML classifiers, it reveals that it can manage named data and produce better results. Due to random weights and input bias assignment in proposed system, ELM could result in lower output. Such random weights and input can result in an ill-posed problem, where classification yields several solutions.

For software identified IoT, Li et al. [22] developed the Bat algorithm and Random Forest (RF) intrusion detection. In Software Specified IoT Networks, a two-stage AI-based intrusion detection system has been introduced. It makes use of SDN to assist with status tracking and traffic capturing from a global perspective. It blends and coordinates two IDS phases, namely, feature collection and flow classification, for identifying novel intrusions and has the capacity to self-learn.

To start, pick typical features using the Bat algorithm with swarm division and differential mutation. Then, to characterise flows, use RF to adaptively change sample weights using a weighted voting system. The updated intelligent algorithms pick more important features and achieve superior success in flow classification, according to the evaluation results. Intelligent intrusion detection has also been shown to have higher precision and lower overhead than existing systems.

In an Intrusion Detection System (IDS) for IoT, Bagaa et al. [23] suggested a One Class Support Vector Machine (OCSVM) and Software Defined Networking (SDN). A security architecture focused on ML that automatically copes with increasing security aspects of the IoT domain. For vulnerability reduction, this architecture uses Software Defined Networking (SDN) as well as Network Feature Virtualization (NFV) enablers.

This AI platform integrates a control agent and an AI-based reaction agent, all of which uses ML-Models for analysing network patterns and identifying anomalies in IoT networks. To accomplish its aims, the architecture makes use of supervised learning, a distributed data mining system, a neural network. The suggested scheme efficacy is illustrated by experimentation outcomes.

The attack distribution using data mining techniques, in particular, is incredibly efficient at detecting attacks with high efficiency and low cost. The experiment was tested in a real smart building scenario using one-class SVM for anomaly-based intrusion detection system (IDS) for IoT. Anomaly identification sensitivity was obtained. A feasibility analysis was carried out to identify possible viable options for implementation and stimulate exploration into open issues.

Anthi et al. [24] developed a three-layer Intrusion Detection System (IDS) for IoT networks that implements a supervised approach to detect a variety of typical network-based cyber-attacks. There are three major roles in the system: 1) define and profile the usual activity of each IoT system connected to the network; 2) distinguish malicious packets on the network while an attack is taking place; and 3) classify attack types that have been initiated.

A smart home testbed with eight common commercially available products is used to validate the system. The proposed

IDS architecture effectiveness is assessed by deploying 12 attacks from four major network-based attack categories: DoS, Man-In-The-Middle (MITM)/spoofing, surveillance, and replay.

The machine is also put through its paces in four situations, including multistage threats and dynamic sequences of events. This shows that the proposed architecture will predict which attack was implemented on which computer connected to the network successfully, as well as differentiate between IoT devices on the network and whether network operation is malicious or friendly.

For the intrusion detection algorithm, Zheng et al. [25] presented an enhanced Linear Discriminant Analysis (LDA)-based Extreme Learning Machine (ELM) classification (ILECA). Improve the LDA first, then use it to reduce the dimension of the functionality. Additionally, characterise the dimensionality-reduced data using a single hidden layer neural network ELM algorithm.

Given high demand for detection efficiency among IoT sensors, the scheme not only guarantees intrusion detection accuracy, but also increases execution efficiency, allowing the intrusion to be identified rapidly. Finally, we used the NSL-KDD dataset to perform tests. The assessment results indicate that the proposed ILECA has strong generalisation and real-time characteristics, as well as improved detection accuracy over other popular algorithms.

For a Lightweight Intrusion Detection System, Fenanir et al. [26] developed a filter-based approach and a Decision Tree (DT) (LIDS). Lightweight IDS focused on feature collection and feature classification, two ML strategies. Because of its low computational cost, the filter-based approach was used to pick the features.

A comparison between Multilayer Perceptron (MLP), Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbor (KNN), DT, Naive Bayes (NB), and Logistic Regression (LR) is made for analysing feature classification algorithms. Three datasets, namely UNSW-NB15, NSL-KDD, and KDD Cup 99, are used in experimentation. Finally, due to better performance on various datasets, the system selected DT algorithm has finally

The findings of the study serve as a reference for selecting the best feature selection process for ML. Furthermore, the classifiers perform well by using the three correlation approaches used for minimising dataset dimension, like KTC, SCC and PCC.

For detecting attacks based on Message Queuing Telemetry Transport (MQTT), techniques like Random Forests (RF), Decision Trees (DT), Support Vector Machine (SVM), k-Nearest Neighbours (k-NN), Gaussian Naive Bayes (NB), and Logistic Regression (LR) are proposed by Hindy et al. [27]. The feature three abstraction levels, namely bidirectional flow, uni-directional flow, and packet-based features, are assessed.

Table.2. Inferences of ML Methods for Intrusion Detection in IoT

Author	Method name	Advantages	Disadvantages
Moustafa et al. [16]	ANN, NB, DT	High detection rate and low false positive rate	Independent variables become less interpretable
Deng et al. [17]	FCM and PCA	Improve network intrusion detection rate	Information Loss
Xiao et al. [18]	RL	Secure offloading and malware detection schemes to protect data privacy	It is only protecting data privacy
Azmoodeh et al. [19]	KNN, NN, RF and SVM	Detect ransomware attacks	It is not suitable for large data sets
Mohamed et al. [20]	RF and NN	Low accuracy and high bias	Does not perform IoT traffic Features selection regarding anomaly detection
Rathore and Park [21]	ELM-based ESFCM	Fog-based attack detection	It is causing an additional uncertainty problem, both in approximation and learning
Li et al. [22]	Bat algorithm and RF	Better accuracy with lower overhead	The algorithm too slow and ineffective for real-time predictions
Bagaa et al. [23]	OCSVM and SDN	High performance and low cost	It is does not perform very well when the data set has more noise
Anthi et al. [24]	Three-layer IDS	Detect cyber-attacks	It is only focused on Denial of Service (DoS), Man-In-The-Middle (MITM)/ spoofing, reconnaissance, and replay
Zheng et al. [25]	Improved LDA-based ELM	Detection accuracy increased	Small sample size problem
Fenanir et al. [26]	Filter-based method and DT	Good performance	Robust to outliers, due to their tendency to overfit
Hindy et al. [27]	LR, RF, DT, SVM, k-NN, Gaussian NB	Detect Message Queuing Telemetry Transport (MQTT)-based attacks	Does not perform well when feature space is too large

The simulated MQTT dataset is used in the evaluation and training process. With an open access license, this dataset is released to assist the research community in analysing challenges. Fitting of IDS requirements for MQTT-based network by proposed ML techniques is demonstrated using experimental results. Moreover, the results emphasise the importance of flow-based features for discriminating MQTT-based attacks from benign traffic.

2.3 REVIEW OF DL METHODS FOR INTRUSION DETECTION IN IOT

An adhoc DL attack detection mechanism is proposed by Diro and Chilamkurti [28]. IoT underlying distribution features are reflected by using this. Compared to traditional ML techniques, this deep model performance was compared to that of a centralised detection system, which evaluated the distributed attack detection. Using a DL model, superior performance is shown by the distributed attack detection systems when compared with centralised detection systems.

For cyber security, artificial intelligence successful adaption is shown using experimentation results. For example, in IoT application distributed architecture like smart cities, for attack detection, a system is designed and implemented. Over shallow models, for showing a deep model effectiveness, performance metrics like false alarm rate, detection rate, and accuracy are used in evaluation.

When compared with centralised algorithms, cyber-attacks are detected effectively using distributed attack detection as demonstrated in experimentation. In training, parameters are shared to avoid local minima. In attack detection, high effectiveness is shown by the deep model.

In the IoT intrusion detection and feature extraction algorithm, a deep migration learning model was introduced by Li et al. [29]. A deep migration learning model-based algorithm for IoT intrusion detection and feature extraction is proposed. With intrusion detection technology, a DL model is combined using this. Based on available algorithms and literature, a data feature extraction and migration learning model modelling scheme is introduced in this.

10% of this dataset is used in experimentation and for training. A comparison is made between the existing algorithm and the proposed algorithm. High detection efficiency and low detection time are produced by the proposed algorithm, as shown in experimental results. There is a great enhancement in the proposed algorithm effectiveness and efficiency when compared with error detection rate and detection rate of other attacks.

In the IoT network, for anomaly detection, a Random Forest (RF) model with Particle Swarm Optimization (PSO)-based feature selection has been formulated by Tama and Rhee [30]. With respect to False Alarm Rate (FAR), recall, precision, accuracy, on a well-known benchmarking dataset called NSL-KDD, evaluated the performance model. Using two statistical tests, we validated the performance difference among classifiers.

Based on experimental results using the NSL-KDD dataset, it is revealed that the proposed model outperforms the other two classifiers, namely Deep Neural Network (DNN) and Rotation Forest (RoF) with respect to all performance metrics. Based on statistical tests, the proposed model outperforms other classifiers involved in the experiment.

For pre-training of Back propagation Neural Networks (BPNN), an evolutionary algorithm called Improved Cuckoo Search (ICS) is proposed by Li et al. [31]. This enhances stability and accuracy. The defect of falling into local minima is surmounted in BPNN using this pre-training process, and its efficiency is enhanced greatly. For a miniature IoT system, Information Security Risk Assessment (ISRA) is used in the neural network. This study performed the simulation experimentation to validate the proposed algorithm performance. Despite the proposed method successful development, there are still aspects of the algorithm that can be further improved. For minimising running time, further enhancement of this algorithm is required. To a single system, the risk assessment model is limited.

In this ISRA process, all other neural networks are outperformed by ICS-BPNN as illustrated in a demonstrated example.

In IoT environments, for detecting security threats, a DL-based Intrusion Detection System (DL-IDS) is developed by Otoum et al. [32]. The Stacked-Deep Polynomial Network (SDPN) and Spider Monkey Optimization (SMO) are the DL algorithms. In the literature, there are various IDS, but their dataset management and optimum feature learning are very poor. Attack detection accuracy is affected significantly because of this.

To achieve optimum detection recognition, SDPN and SMO algorithms are combined in the proposed module. In datasets, optimum features are selected using SMO, and data is classified as anomalies or normal using SDPN. DL-IDS detects various types of anomalies, including remote-to-local (R2L) attacks, probe attacks, User-to-Root (U2R) attacks, and Denial of Service (DoS) attacks, among others. With respect to F-score, recall, precision, and accuracy, better performance is achieved using DL-IDS as indicated in extensive analysis.

For IoT network threat analysis, an Artificial Neural Network (ANN) was introduced by Hodo et al. [33]. IoT threat analysis is done using ANN and these threats are combated. Internet packet traces are used for training a supervised ANN called multi-level perceptron. Its ability to thwart Distributed Denial of Service (DDoS) attacks has been tested.

On an IoT network, threat and normal pattern classification are focused on using this. against a simulated IoT network, validated an ANN procedure. Different DDoS/DoS attacks can be detected successfully with high accuracy using this proposed scheme, as demonstrated in experimentation results.

An Intrusion Detection System (IDS) based on Software Defined Networking (SDN) was formulated by Wani and Revathi [34], which acts as a countermeasure against such threats. With centralised control, a programmable network architecture is formulated by decoupling control and data planes in SDN. In an IoT network, abnormal activityis rectified using IDS based on SDN, where, in real time, network traffic is examined.

Flexible IDS is made possible by SDN programmability features, and it does not give any overburden to forwarding devices. On a simulated IoT network, an SDN-based IDS mechanism is run. As exhibited in the experimentation results, various attacks are detected with high accuracy and efficiency in an IoT environment.

For IoT networks, a Feed-Forward Neural Networks (FFNN) intrusion detection system is proposed by Ge et al. [35]. Through DL concept application, traffic flow is classified using a novel intrusion detection technique in IoT. A newly published IoT dataset is adopted and at packet level, from field information, generic features are generated.

For multi-class and binary classification including information theft, reconnaissance, distributed denial of service, denial of service attacks against IoT devices, a FFNN model is developed. A processed dataset is used in experimentation and high classification accuracy is obtained using this proposed scheme.

For botnet attack detection in IoT, a DL Convolutional Neural Networks (CNN) based IDS solution termed as BotIDS was developed by Idrissi et al. [36]. Using a specific Bot-IoT dataset, against some well-known botnet attacks, the IDS is designed, implemented, and tested in this way. With a prediction execution time less than 0.34 ms, with minimised validation loss and with high validation accuracy, promising results are obtained by BotIDS when compared with other DL techniques like GRU, LSTM and RNN.

For the Internet of Things (IoT), to detect intrusion, a Deep Neural Network (DNN) was introduced by Liang et al. [37]. A DL, blockchain, and multi-agent system algorithm-based hybrid placement strategy is used for designing, implementing, and testing intrusion detection systems. The following modules are present in that system: response, analysis, data management, and data collection.

Systems are tested using data mining, NSL-KDD, and the National Security Lab knowledge discovery dataset. From the transport layer, in attack detection, DL algorithm efficiency is demonstrated using experimentation results. As indicated in experimental results, DL algorithms are highly suitable for intrusion detection in the IoT network environment.

For IoT network security, for building a security solution, a Bidirectional Recurrent Neural Network (BRNN) is formulated by Dushimimana et al. [38] and it has high durability. In dealing with multimodal and voluminous heterogeneous data, remarkable results are shown by ML and DL in intrusion detection. Using the Recurrent Neural Network (RNN) architecture, better results are produced.

From the data, non-essential variables are identified and removed using a feature selection mechanism. The prediction model accuracy is not affected by this. Due to the flexibility of Principal Component Analysis (PCA), it is implemented as a Random Forest (RF) algorithm in this case, and in ML algorithms it can be used easily. Without tuning hyper-parameters, production is allowed and multiple decision trees are built using this. To get a highly stable and accurate prediction, they are merged together.

The Gated Recurrent Neural Network (GRNN) and Recurrent Neural Network (RNN) are outperformed by a novel algorithm named BRNN. Using forward and backward hidden neurons, future and past information are considered in this to produce better results.

For IoTs, a Random Neural Network based heuristic Intrusion Detection System (RNN-IDS) has been proposed by Larijani et al. [39]. After selecting features from the NSL-KDD dataset, at various learning rates, neurons are trained and tested. The proposed scheme is analysed by adopting two techniques where there is an enhancement in RNN-IDS accuracy.

Table.3. Inferences of DL Methods for Intrusion Detection in IoT

Author name	Method	Advantages	Disadvantages
Diro and Chilamkurti [28]	Distributed DL attack detection mechanism	Distributed attack detection can better detect cyber-attacks	Lack of ability to be spatially invariant to the input data
Li et al. [29]	Deep migration learning model	Higher detection efficiency	Not focus effectively reduce clustering time and solve data clustering spatial constraints
Tama and Rhee [30]	RF model with PSO	Anomaly detection in IoT network	Low convergence rate in the iterative process
Li et al. [31]	ICS to pretrain a BPNN	Improving the accuracy and stability	Slow rate of convergence
Otoum et al. [32]	DL-IDS	Detect security threats	Large time consuming
Hodo et al. [33]	ANN	Higher accuracy and can successfully detect various DDoS/DoS attacks	Only focused on DDoS/DOS attacks
Wani and Revathi [34]	SDN	Higher accuracy	High computational cost and large time-consuming
Ge et al. [35]	FFNN	High classification accuracy	Not focused on software privacy
Idrissi et al. [36]	Baptized BotIDS, based on DLCNN	Higher validation accuracy, lower validation loss	Do not encode the position and orientation of object
Liang et al. [37]	DNN	Detecting attacks from the transport layer	It is not suitable for real-time environment
Dushimimana et al. [38]	BRNN	More accurate and stable prediction	It is not focused on multimodal data on the intrusion detection
Larijani et al. [39]	RNN-IDS	Higher accuracy	Slow convergence and large time-consuming

In recognising anomalous traffic from normal patterns, high accuracy is shown by proposed intelligent intrusion detection when compared with other ML algorithms as suggested in experimentation results.

3. ISSUES FROM EXISTING METHODS

In organisations, services are offered constantly using systems, applications, and data storage. These are connected using IoT and it provides a gateway for cyber-attacks. Security challenges are raised due to IoT devices' high diversity, their restricted computational resources, and protocols and standards. Authentication and encryption traditional security countermeasures are not sufficient.

For practitioners, to safeguard their industrial and economic strategies, a fundamental concern is network security promotion. It is very easy to compromise IoT devices when compared with desktop computers. This increases the occurrence of IoT-based botnet attacks.

New techniques to detect attacks launched from compromised IoT devices need to be developed to mitigate this new threat, and there is a need to differentiate between attacks based on IoT which are milliseconds long and those that are hours long. For IoT technology large-scale successful deployment, privacy and security concerns need to be mitigated. In IoT networks, relevant information handling makes IoT device security a fundamental issue.

With broken cryptography, it acts as a second defence wall. Security is a major issue in recent days. In addition, for assuring Internet of Things security, components like availability, integrity and confidentiality are required.

4. INFERENCES

At network level, to solve those issues and to protect Internet-connected frameworks, major solutions are given by IDS. However, it is highly important to know how to convert traditional IDS into intelligent IDS, which resembles intelligent IoT. The feature selection problem is tackled using IDS. This paper gives an insight into the usage of ML techniques in detecting anomalies in network intrusion detection systems. To enhance the performance of the intrusion detection system, in the Network Intrusion Detection System, different ML techniques can be combined with Swarm Optimization techniques to detect anomalies in the future. Anomalous network traffic emanating from compromised IoT devices is detected using deep auto-encoders.

In modern IoT devices, bandwidth is consumed by DDoS attacks. So, to enhance network and IoT device cyber security, a prevention technique has been proposed. Only during the expected time of the attack signature, the anomaly detection technique is activated. For the IDPIoT, an adaptive intrusion detection and prevention system has been introduced. This enhances security along with device growth which is connected to the Internet. Existing intrusion detection systems are investigated in order to propose IDPIoT, which improves security and network- and host-based functionality.

5. CONCLUSION

IoT networks are highly affected by substantial attacks. In recent years, various IoT threats have emerged, and large-scale malicious attacks have been triggered. So, for protecting IoT networks, the most commonly used technique is IDS. Security challenges are raised due to IoT devices' high diversity, their restricted computational resources, and protocols and standards. Because of the huge attack surface in IoT networks, they are highly vulnerable to various attacks, even with some security measures. So, for detecting attacks, it is necessary to design defence mechanisms. In IoT environments, it is highly crucial to have security defence measures like IDS. Hence, authentication and encryption traditional security countermeasures are not sufficient. Highly unique challenges are faced by IoT devices' specific characteristics. At network level, to solve those issues and to protect Internet-connected frameworks, major solutions are given by IDS. However, as in literature, various problems are raised in traditional IDS, like the high false alarm rate. In IoT, for intrusion detection, a detailed study of traditional DL and ML techniques and recent technologies is presented in this review.

REFERENCES

[1] G.J. Joyia, R.M. Liaqat and A. Farooq, "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain", *Journal of Communication*, Vol. 12, No. 4, pp. 240-247, 2017.

[2] R. Patan and A.H. Gandomi, "Improving Power and Resource Management in Heterogeneous Downlink OFDMA Networks", *Information*, Vol. 11, No. 4, pp. 203-216, 2020.

[3] S. Kannan, G. Dhiman, and M. Gheisari, "Ubiquitous Vehicular Ad-Hoc Network Computing using Deep Neural Network with IoT-Based Bat Agents for Traffic Management", *Electronics*, Vol. 10, No. 7, pp. 785-796, 2021.

[4] V. Chang, B. Gobinathan, A. Pinagapan and S. Kannan, "Automatic Detection of Cyberbullying using multi-feature based Artificial Intelligence with Deep Decision Tree Classification", *Computers and Electrical Engineering*, Vol. 92, pp. 1-17, 2021.

[5] T. Karthikeyan, K. Praghash and K.H. Reddy, "Binary Flower Pollination (BFP) Approach to Handle the Dynamic Networking Conditions to Deliver Uninterrupted Connectivity", *Wireless Personal Communications*, Vol. 48, No. 1, pp. 1-20, 2021.

[6] P. Johri, "Improved Energy Efficient Wireless Sensor Networks using Multicast Particle Swarm Optimization", *Proceedings of International Conference on Innovative Advancement in Engineering and Technology*, pp. 1-6, 2020.

[7] Y. Meidan, M. Bohadana and Y. Mathov, "N-Baiot-Network-based Detection of IoT Botnet Attacks using Deep Autoencoders", *IEEE Pervasive Computing*, Vol. 17, No. 3, pp. 12-22, 2018.

[8] M. Elhoseny, K. Shankar and S.K. Lakshmanaprabu, "Hybrid Optimization with Cryptography Encryption for Medical Image Security in Internet of Things", *Neural Computing and Applications*, Vol. 32, No. 15, pp. 1-15, 2018.

[9] A. Al Shorman, H. Faris and I. Aljarah, "Unsupervised Intelligent System based on One Class Support Vector Machine and Grey Wolf Optimization for IoT Botnet Detection", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 7, pp. 2809-2825, 2020.

[10] A. Aldaej, "Enhancing Cyber Security in Modern Internet of Things (IoT) using Intrusion Prevention Algorithm for IoT (IPAI)", *IEEE Access*, Vol. 8, pp. 1-9, 2019.

[11] H. Sedjelmaci, S.M. Senouci and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices", *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 10, pp. 9381-9393, 2017.

[12] M. Zhou, L. Han, H. Lu and C. Fu, "Intrusion Detection System for IoT Heterogeneous Perceptual Network", *Mobile Networks and Applications*, Vol. 33, No. 1, pp. 1-14, 2020.

[13] S.T. Bakhsh, S. Alghamdi, R.A. Alsemmeari and S.R. Hassan, "An Adaptive Intrusion Detection and Prevention System for Internet of Things", *International Journal of Distributed Sensor Networks*, Vol. 15, No. 11, pp. 1-20, 2019.

[14] A. Tabassum and W. Lebda, "Security Framework for IoT Devices against Cyber-Attacks", *Proceedings of International Conference on Internet of Things*, pp. 1-18, 2019.

[15] T.U. Sheikh, H. Rahman, H.S. Al-Qahtani and T.K. Hazra, "Countermeasure of Attack Vectors using Signature-Based IDS in IoT Environments", *Proceedings of IEEE 10th Annual Conference on Information Technology, Electronics and Mobile Communication*, pp. 1130-1136, 2019.

[16] N. Moustafa, B. Turnbull and K.K.R. Choo, "An Ensemble Intrusion Detection Technique based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things", *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp. 4815-4830, 2018.

[17] L. Deng, D. Li, X. Yao and D. Cox, "Mobile Network Intrusion Detection for IoT System based on Transfer Learning Algorithm", *Cluster Computing*, Vol. 22, No. 4, pp. 9889-9904, 2019.

[18] L. Xiao, X. Wan, X. Lu and Y. Zhang, "IoT Security Techniques based on Machine Learning: How do IoT Devices use AI to Enhance Security?", *IEEE Signal Processing Magazine*, Vol. 35, No. 5, pp. 41-49, 2018.

[19] A. Azmoodeh, A. Dehghantanha, M. Conti and K.K.R. Choo, "Detecting Crypto-Ransomware in IoT Networks based on Energy Consumption Footprint", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 9, No. 4, pp. 1141-1152, 2018.

[20] T.A. Mohamed, T. Otsuka and T. Ito, "Towards Machine Learning based IoT Intrusion Detection Service", *Proceedings of International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, pp. 580-585, 2018.

[21] S. Rathore and J.H. Park, "Semi-Supervised Learning based Distributed Attack Detection Framework for IoT", *Applied Soft Computing*, Vol. 72, pp. 79-89, 2018.

[22] J. Li, Z. Zhao and R. Li, "AI-based Two-Stage Intrusion Detection for Software Defined IoT Networks", *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 2093-2102, 2018.

[23] M. Bagaa, T. Taleb and J.B. Bernabe, "A Machine Learning Security Framework for IoT Systems", *IEEE Access*, Vol. 8, pp. 1-12, 2020.

[24] E. Anthi, L. Williams, 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.

[25] D. Zheng, Z. Hong, N. Wang and P. Chen, "An Improved LDA-based ELM Classification for Intrusion Detection Algorithm in IoT Application", *Sensors*, Vol. 20, No. 6, pp. 1-19, 2020.

[26] S. Fenanir, F. Semchedine and A. Baadache, "A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things", *Revue d'IntelligenceArtificielle*, Vol. 33, No. 3, pp.203-211, 2019.

[27] H. Hindy, E. Bayne and M. Bures, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study", *Proceedings of International Conference on Network*, pp.1-14, 2020.

[28] A.A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things", *Future Generation Computer Systems*, Vol. 82, pp. 761-768, 2018.

[29] D. Li, L. Deng, M. Lee and H. Wang, "IoT Data Feature Extraction and Intrusion Detection System for Smart Cities based on Deep Migration Learning", *International Journal of Information Management*, Vol. 49, pp. 533-545, 2019.

[30] B.A. Tama and K.H. Rhee, "An Integration of PSO-Based Feature Selection and Random Forest for Anomaly Detection in IoT Network", *Proceedings of International Conference on Web Technologies*, pp. 1-6, 2018.

[31] S. Li, F. Bi and W. Chen, "An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking", *IEEE Access*, Vol. 6, pp. 10311-10319, 2018.

[32] Y. Otoum, D. Liu and A. Nayak, "DL-IDS: A Deep Learning-based Intrusion Detection Framework for Securing IoT", *Proceedings of International Conference on Transactions on Emerging Telecommunications Technologies*, pp.1-16, 2019.

[33] E. Hodo, X. Bellekens and A. Hamilton, "Threat Analysis of IoT Networks using Artificial Neural Network Intrusion Detection System", *Proceedings of International Symposium on Networks, Computers and Communications*, pp. 1-6, 2016.

[34] A. Wani and S. Revathi, "Analyzing threats of IoT Networks using SDN based Intrusion Detection System (SDIoT-IDS)", *Proceedings of International Conference on Next Generation Computing Technologies*, pp. 536-542, 2017.

[35] M. Ge, X. Fu, N. Syed and Z. Baig, "Deep Learning-Based Intrusion Detection for IoT Networks", *Proceedings of International Conference on Dependable Computing*, pp. 256-265, 2019.

[36] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui and H. El Fadili, "Toward A Deep Learning-Based Intrusion Detection System for IoT Against Botnet Attacks", *IAES International Journal of Artificial Intelligence*, Vol. 10, No. 1, pp. 1-13, 2021.

[37] C. Liang, B. Shanmugam, S. Azam and A. Karim, "Intrusion Detection System for the Internet of Things based on

Blockchain and Multi-Agent Systems", *Electronics*, Vol. 9, No. 7, pp. 1-27, 2020.

[38] A. Dushimimana, T. Tao and R. Kindong, "Bi-Directional Recurrent Neural Network for Intrusion Detection System (IDS) in the Internet of Things (IoT)", *International Journal of Advanced Engineering Research and Science*, Vol. 7, No. 3, pp. 524-539, 2020.

[39] H. Larijani, J. Ahmad and N. Mtetwa, "A Heuristic Intrusion Detection System for Internet-of-Things (IoT)", *Proceedings of International Conference on Intelligent Computing*, pp. 86-98, 2019.