An Adaptive Multi-Layer Architecture for IoT based IDPS for Attacks using Deep Learning Method

Sirajuddin Qureshi, Jingsha He, Saima Tunio, Nafei Zhu, Faheem Ullah, Ahsan Nazir, and Ahsan Wajahat

(Corresponding author: Nafei Zhu)

Faculty of Information Technology, Beijing University of Technology
Beijing 100124, China
Email: znf@bjut.edu.cn

(Received Dec. 8, 2021; Revised and Accepted May 6, 2022; First Online May 9, 2022)

Abstract

The extensive implementation of the Internet of Things (IoT) is vulnerable to security and privacy factors due to the increased use of Internet-enabled devices. The data without interaction between Human-to-Human or Human-to-Computer are shared by the IoT-enabled devices that create an intelligent system of systems. The data capable of transforming the lives of humans, businesses, and the universe are extracted by the IoT systems. But in a highly hostile environment such as the Internet, there are possibilities of an end number of cyber-attacks. For everyone, including consumers, firms, and Government Organizations, the primary concern is to protect IoT. However, the protection of the systems is ineffective due to the complication in the real-time detection of the attacks. In contrast, the complete prevention of attacks on any procedure does not exist forever. The research on competent Deep Learning based Intrusion Detection and Preventions Systems (DL-IDPS) conducive to IoT environments exists in limited numbers. IDPS has been offered numerous DL-based models in recent years. An analogy of specific deep autoencoding models and conventional IDS and NIDS datasets has been proposed in this research paper. Multi-Layer Architecture-IoT security, the Artificial Neural Networks (ANNs) are deployed for this IoT research. Each layer in the designed architecture has been assessed with ANNs of DL on the KDD Cup '99 detection of intrusion data set. The present technique's performance results over the KDD Cup '99 dataset are outperformed by this innovative research with 97.77% accuracy and 0.71% FAR.

Keywords: I Attacks; Deep Learning; Intrusion Detection System; IoT, Security

1 Introduction

With the help of the present network resources, the IoT connects real day-to-day objects to Internet for communicating and integrating data. The capability to collect data and share this information globally over the Internet is owned by these objects that are the interrelated digital devices or sensors. As a result, new applications and services are created by these communications between sensors, connectivity, and people and processes. The "Things" on the Internet of "Things" usually mean these digital devices or sensors. It has been suggested by the prediction of Transform Insights that 8.7 billion active IoT devices will exist globally by the end of 2020. In 2030, this study will rise to 25.4 billion at a Compound Annual Growth Rate (CAGR) of 11%. While for the period of the predictions, a short-range majority of IoT connections are expected (Bluetooth, Wi-Fi, and Zigbee). There is a crucial opportunity for the mobile ecosystem and the expected rapid growth of 1 billion in 2020 to 5.3 billion in 2030 in cellular network IoT connections. An amazing shift in the generation is revealed in the analysis done at further granular level: in 2030, there will be an increase in 5G connections to 3.3 billion, without any 3G connections leftover in the market, and by 2030, there will be merely 120 million 2G connections. 5G massive Machine-Type Communications (mMTC) is the area of drastic growth, and by 2030, that will inflate to 2.6 billion IoT connections from 160 million at the end of 2020.

The cellular networks and IoT devices demand the industries in the modern era like public security services, smart agricultural farming and smart transportations applications to extensively adopt emerging standards and technologies like the fifth-generation (5G) standard. The enhancement of standards for security is very much warranted as a result of the growing need for connectivity. In future, there will be a need for more automated, scalable

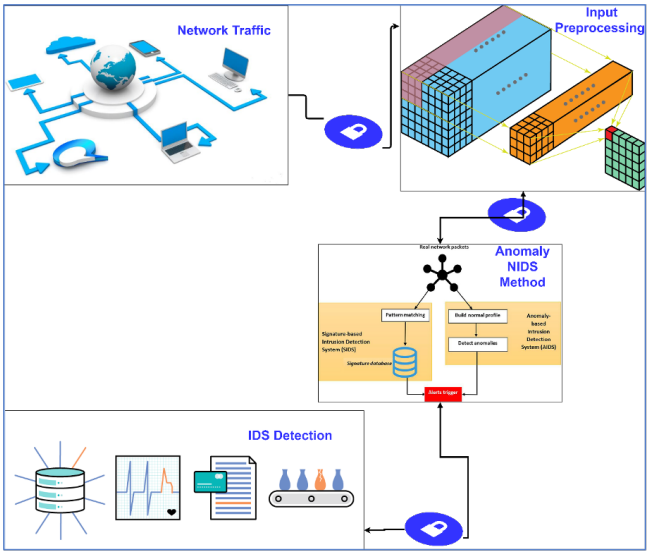

Figure 1: Model of data flow an anomaly-NIDS

and trustworthy network due to more threats.

In various applications like business development services, health care, and national security, IoT technology is more, and for smart-home environments, the usage is less. More security attacks on IoT networks are in succession with the growing demand, and IoT security is more susceptible to cyber security attacks. The distinct resources of IoT on a number of IoT devices are being targeted by these attacks in different forms. One or more devices in an IoT network that can be additionally used as a "resource" or "platform" for attacks like DDoS and illegal activities like pilfering opportunistic service, ransomware and exfiltration of information can tend to be compromised by these attacks.

A popular approach that applies anomaly detection techniques to network intrusion detection has been adopted in this work [4,21]. Searching unusual patterns in network traffic enables Network Intrusion Detection System (NIDS) to detect malevolent network activities. The usual flow of NIDS is illustrated in Figure 1. The detection of new zero-day attacks is one of the many significant features of such systems. But the difficulty in the practical situations is made away by some of the factors with the practical application of a NIDS. The following are some of the challenges in the perspective of Sommer *et al.* [22]: Labelled data shortage, presence of more errors, fundamental issues in assessing the system, and more intricacy and inconsistency in input data. Besides the competencies and demerits of the detection process, the system under security should be studied well to overcome these challenges.

Thus, with the aid of new technologies like Artificial Intelligence (AI), the need to develop security systems is significant for detecting and preventing fresh attacks. The application of Machine Learning (ML) techniques for finding the threat is feasible using one of the Intrusion Detection Systems (IDS) strategies. Correspondingly, there are noticeable developments in the research carried out on anomaly detection methods. Amidst research scholars and experts, more attention has been gained by DL techniques that detect anomalies [10].

The enormous quantity of IoT data is analyzed by deploying the DL aided Data Analytics techniques previously for enhancing customer service and network competency. The detection of possibly any dangerous behaviour and jamming any unusual behaviour are performed.

As opposed to unauthorized access, detecting and protecting the network are the objectives of these alarms. The unauthorized network access is in two forms viz., active attacks, where breaching or evading the secured systems is some of the network resources that undergo modification by the intruder, for instance, the inclusion of DDoS [14,29]. Hence, for detecting new kinds of DDoS and wormhole attacks, the Multi-Layer IoT Architecture for security model has been proposed and deployed using LSTM based DL capable of efficiently detecting malicious DDoS packets irrespective of their kinds. Particularly, the standard datasets for anomaly detection have shown remarkable outcomes due to the application of ANNs based autoencoding methods [19,27]. Since DL methods can obtain enriched interpretations from input and balance well with massive datasets, they deem to be especially alluring for NIDS [13, 14, 30].

The capability of IDSs based on DL, especially in detecting threats of zero-day or anonymous nature, along with their low False Alarm Rate (FAR), induced the researchers to lay more emphasis on this method. An innovative research idea that contains a Multi-Layer IoT architecture for DL-IDPS has been proposed in this paper. The fast detection of possible threats and an immediate response in succession to their occurrence are given. This is practically possible by applying DL algorithms in the IoT network to monitor the network data to classify activity either as DDoS or Wormhole for every layer in the IoT architecture. The challenges of the IoT context framed for resource constrictions, interoperability, heterogeneity and connectivity must be respected by such an IDPS. In most DL research on-network data security, the KDD 99' Cup [24] is used to detect a standard data set intrusion.

2 Related Works

Nowadays, IoT is widely formed by the ability of each device for generating and sharing data over the Internet. In recent times, the total number of devices linked with the Internet is anticipated by the researchers to cross 6.4 Billion by 2016 and by 2020, this number is expected to reach 20.8 billion [20, 28]. Many more devices, such as iPhone, iPad, iWatch, Smart TVs etc., are included in this list. IoT is defined by the European Research Cluster on IoT as "A powerful worldwide network infrastructure enabled with self-configuring abilities based on typical and interoperable communication protocols where there has been

the identification, real attribution and unreal personalities thus making use of intelligent interfaces and are flawlessly incorporated into the information network" [25,30]. In the following, we discuss the relevant information from the advanced IoT-NIDS security in order to obtain improved ideas related to IoT-NIDS frameworks and applications. Their detection mechanisms, frameworks and authentication stratagems are focused well. The reviewed IoT-NIDS papers provide a complete overview of the domain's growth from the first proposed solution to the recent days. The keys of the authors have started to be described in detail [17, 26].

A software application known as IDS observes the system or the networks' malicious activities to enable network security. The classification of IDS can be of various sorts. The categorization of IDS into Active and Passive is done based on their responsive nature. In the absence of any human interference, for the automatic blocking of malware attacks, an active IDS is designed while monitoring the network traffic and alerting the users are alone done by a passive IDS. Signature and Anomaly-based IDS are the alternative way of categorizing IDS. A database that contains familiar signatures and susceptibilities are accessed by the IDS in the approach based on signature. A comprehensive overview of the Attack known as a signature is included in each intrusion attack which detects and avoid future attacks.

Though the anomaly-based IDS's learning facilitates the detection of new intrusion attacks from the baseline patterns, the chief limitation of this method is frequent updating of the database. Attacks are performed when they differ significantly from the proven benchmark behaviours and trigger alarms—where the IDS is connected on the basic principle of another classification of the Intrusion detection system. The IDS is known as NIDS when the network segment is placed with an IDS. At the same time, the IDS is supposed to be Host-based IDSs, when it is placed in servers. There are more drawbacks in Host-based IDSs so that they may not be conducive for research purposes. The researchers focus on the utilization of ANN and DL for detecting security threats, along with the growth, complication, and variety of security attacks. ML must be embedded, and decision-making systems must be enhanced by IDS in order to detect security threats [8]. The application of DL by various studies in IDSs is done for conventional methods [2,7,9] and achieve remarkable results. From distinct surveys, the IoT-IDSs are detailed.

A kind of supervised ANN in an off-line IoT-IDS known as the Multi-Layer Perceptron (MLP) is deployed by the author in [11]. In every concealed and neuron of output layers, the MLP comprises three layers with sigmoid transfer function exists. The authors evaluate and detect the DoS/DDoS attacks in IoT networks based on the internet packet traces. Four client nodes and one server relay node are contained in a simulation utilized to assess the NIDS. The Denial - of - service activities have been carried out using a virtual machine node with 10 million UDP data packets from a host machine and three hosts at optimal speed. 2313 samples were contained in the training dataset, from which, for validation, 496 samples were used, and all of them were utilized for evaluation. With a false positive of 0.6%, the accuracy of overall attack detection was 99.4%. The quick detection of attacks and the resulting effective network stability is assured by such results. For NIDS, several classification-based techniques have been proposed. On two datasets viz., the UNSW-NB15 dataset and KDDCUP '99, a choice of classification algorithms that includes ANNs, Logistic Regression, naïve Bayes, and Decision Trees has been compared by the author [16]. A botnet detection system based on flow known as Disclosure is proposed by the author [5]. The Command-and-Control communication from benign network traffic is differentiated using a random forest classifier trained by the authors in a supervised way. The external reputation scores like Google Safe Browsing are used by Disclosure for minimizing the FPR. Two environments are used by the author for testing: a university network that is medium-sized and a network of a Tier 1 Internet Service Provider.

In recent times, the designs for handling IoT-DoS were proposed by many researchers. This initiative was taken to find IDS hybrid methods for improving network defences, such as adopting a hybrid system of misappropriation and detecting abnormality for a trusted training and attack packets correspondingly [3]. K-means, naïve Bayes and backpropagation neural network-based alternative hybrid method of IDS was proposed. With the aid of a voting-based mechanism, a distinct approach was proposed for deciding on the unusual behaviour [6]. The sinkhole's unpleasant behaviours and careful forwarding attacks in 6LoWPAN are detected by presenting a real-time hybrid IDS architecture. A simulator COOJA tool introduces another signature-based IDS design integrated with centralized and disseminated IDS modules [12]. Then, IoT-DDoS framework is executed on IoT devices. The network traffic-based DoS attacks are detected by design using IDS proposed by Razak and Salim [18]. The patterns that do not behave normally are obtained from network traffic and are compared with regular traffic. An alarm will be generated by the system if there are more outliners when compared to thresholds.

For the purpose of detecting DDoS attacks, an algorithm has been developed by the authors in [23] for increasing the advantages. Moreover, for detecting DDoS Attacks, the performance of various DL methods over ML techniques have been compared. The capability of DL to enhance the precision in detecting DDoS attacks happens inside IoT networks. [1] propose a Deep Belief-based IDS in this line. On the standard dataset CICIDS, improved performance in intrusion detection regarding F1-score, rate of detection and accuracy has been assured by this approach. Additionally, five remaining networks, which study the malicious network behaviour by getting pretrained, are loaded for the authors [15] to present DL based IDS, and within the limit of IoT network, an intru-

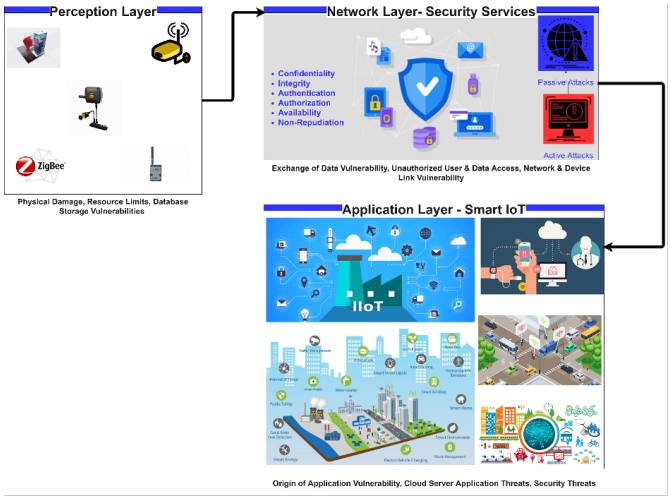

Figure 2: Threats to the internet of things with multi-layers

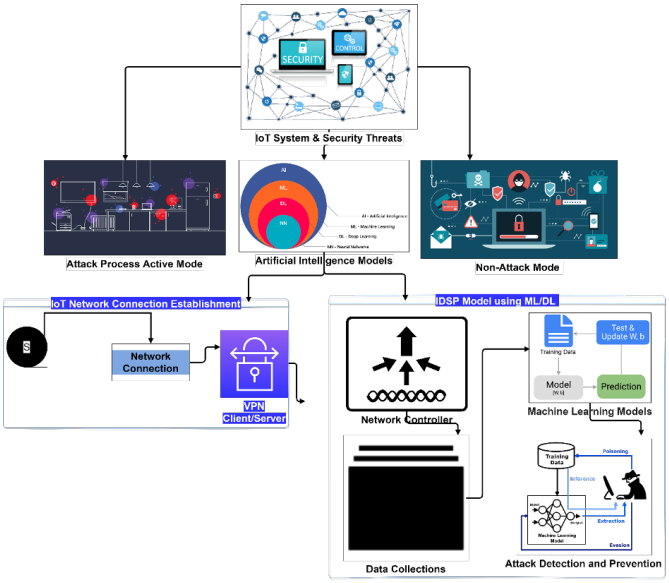

Figure 3: Schematic representation of DL's possible role in IoT security

sion is recognized. From a distinct point of view, IDS has been attempted to be designed by numerous researchers for increasing the merits of DL.

3 Preliminaries

The computer networks or devices are targeted by a cyberattack that carries out malicious activity [3]. In order to get unauthorized and loot data or disturb the usual operations of the system, network device or protocol susceptibilities are seemed to be utilized by the attackers. From domestic reasons to military intelligence, there can be demarcations in their motives.

3.1 IoT Threats

There can be two categorizations of IoT threats, as the IoT systems are diverse and are encountering heterogeneous challenges. The first categorization depends on the architectural layers of the IoT systems, whereas the second categorization of IoT threats depends on their difficulties in design. The physical environment is connected with the virtual one by the IoT systems. Figure 2 shows a typical representation of IoT framework. Sometimes, the transport encryption is ignored or applied in an invalid type because the insufficient capacity of the computational devices is the basis of IoT. Hence, easy traceability and discovery are featured by communications (Cipher Text-Only Attack, Man-In-The-Middle).

3.2 System Architecture

Prevention of attacks by acing on-demand security service using DL is the primary objective of our proposed IDPS for Multi-layer IoT. The potential to understand its neighbour and dissipatedly hear the wireless communication traffic in it and detection of intrusions at an initial stage are the chief concerns of posed IDS. The proposed IDPS works significantly in three phases, as shown in Figure 3, Mitigation Stage (MS), Anomaly Detection Stage (ADS) and Network Connection Stage (NCS). A suitable network adapter is ascertained and employed by the proposed IDPS to ease network traffic translation during the NCS in order to detect the sniffed network packets from its neighbourhood. The detection of abnormalities in the network traffic contained in the IoT network is performed by the Feed-Forward DL algorithm employed by the proposed IDPS during the ADS. As a result, if it comes crosswise of an intrusion, it responds pre-statedly in the MS according to the detected intrusion.

3.3 Multi-Layer IoT Security Model for Solutions

Since there is a protected data flow with confidentiality, reliability and authenticity, IoT security solutions are multi-faceted; the system is free from interruptions. The normal solutions may not work well since numerous devices and multi-modal data are dealt with by an IoT system over time. The invention of smart solutions is mandatory and appropriate to different kinds of data flow in the network. For the implementation on devices with varying memory sizes, there is a need to discover accessible solutions. The IoT system is simply susceptible to information, confidentiality and privacy leaks in a traditional open framework. The devices are dealt with by the multi-layered IoT architecture and their data at many levels, turning the system to be stronger. The processing of data generated by heterogeneous devices in an IoT network is done, and then it is stored in a number of ways before transmitting to many places. Limiting the

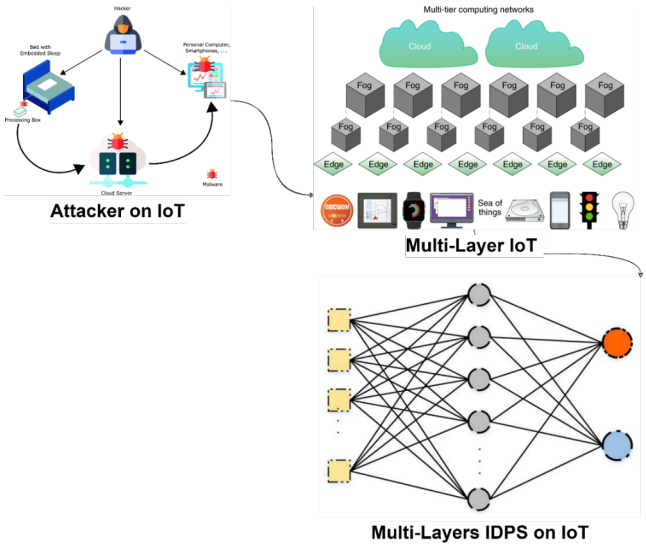

Figure 4: IoT network architecture: Multi-layering

neighbourhood or possibility of the elements makes the generation of enhanced performance across the IoT system impossible for a single-layer model. Whereas, based on the condition, by permitting the execution process at each level, i.e., from simple to complex, a multi-layered architecture is disseminated across the system.

We have evolved with robust architecture for monitoring intrusion detection activity in a erudite manner taking into account the above characteristics for IoT security solutions. The research is performed on an intrusion detection data that hold information about "normal" and "malware" connection types recorded in an IoT network since the IoT network security is going to be dealt with. DL algorithms are employed in a dataset, and supervised learning is used for classification besides traditional approaches. Therefore, a multi-layered architecture is developed, and weightless DL algorithms are applied to perform well for a long time. Likewise, in the system, the network load will be distributed, and hence it gets weightless and enhance the response time. Figure 4 shows the architecture.

The experiments for detecting abnormality are done with the help of Gated-Recurrent-Unit (GRU) and detected using Long-Short-Term-Memory (LSTM) and perform the assessment on the KDD Cup '99 intrusion detection data set acquired at several IDS layers.

4 Proposed Deep Learning based Intrusion Detection and Prevention

For detection of abnormality, the perceptual learning is used by the proposed IDPS as the ML algorithm. The main features (HEAD-TAGs) are mined by Data Aggregation and Exchange Module (DAEM) from the network packets, and for Binary Classification (BC), the DL module is to be fed after the network traffic is received from the Virtual Network Client module by DAEM. As shown in Figure 4, the execution of DAEM and Abnormal Detection module based on DL has been discussed.

Each input network packet is read by DAEM as string clusters. The different layers of the TCP/IP stack are the segments of each input network packet, and later on, for each layer, corresponding HEAD-TAGs are mined in string format as demonstrated in Algorithm 1. Then, for future reference, a label is chosen for each non-empty layer. Eventually, under the label of their corresponding layer, the mined header-tags are appended to a list. Any reiteration of HEAD-TAGs is removed by the DAEM in this way. As demonstrated in Algorithm 1, the DAEM too pipelines these lists back to the cache.

Algorithm 1 For sniffing network packets and extracting HEAD-tags

Input: HEAD-TAGs from Complete Data Sets in IoT

1: The function of Packet Filter (Pkt_Fltr) /Received Data Packers from IoT-Network*/
2: Extract Packet Access (Pkt_Acc) /*Get Packet Access from IoT-Network*/
3: Data Fragmentation the Pkt_Acc
4: For Each IoT-Layer
5: For Every Layer in Packet **Do**
6: Receive Data Packets from IoT Layer 1, Layer 2 and Layer 3
7: If Layer (1-3)= 0 **Then**
8: Fragmentation of Date Packets
9: End If
10: For Every Date Packets **Do**
End

The responsibility to categorize benign network traffic from malicious network traffic is taken by this module, the main ML engine of the proposed IDPS. For the purpose of detecting an anomaly, it uses an observable learning model. When the IDPS gets into the ADS that possesses the training and detection phase, this model is galvanized. Since the training also takes much time, it is carried out across a time and in off-line mode. On the tuples of attributes created during the pre-processing, the observable model undergoes training through supervised learning. With a BC label indicating a malevolent or benevolent network packet, each tuple is manually optimised before nurturing the tuple into the observable learning model. Before enabling the successive observable layer, the observable learning model utilizes information gain to separate the selected attributes at each observable layer. In the place of observable learning model, we use a feed-forward Deep-CNN model in this research. Filtering the input tuples, mapping them to an absolute proportion, and standardizing these proportions into a BC value are performed by the DL neural nodes at each layer. An abnormal tuple is signified by the BC value of '1' while a

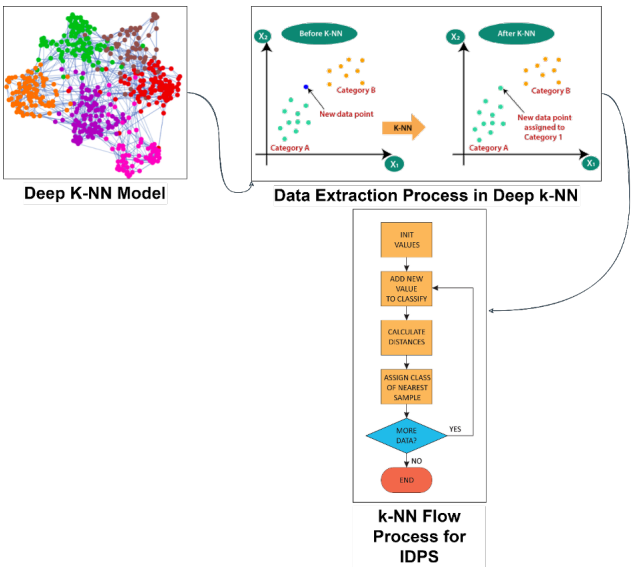

Figure 5: The D-k-NN is a result of IDS

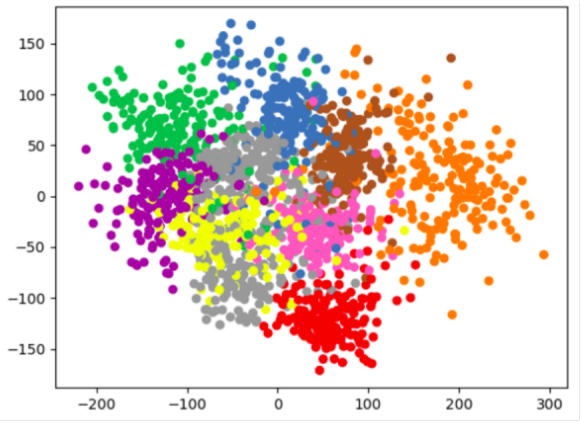

Figure 6: Principles of KNN procedure

benign tuple is denoted as '0'.

A DNN training is taken by the method we presented utilizing any typical DNN learning algorithm and changes the protocol observed for predicting the model on test data. In order to guarantee support from the training data, there is a comparison made between the internal elements' detection of patterns in the data at test time and those identified during training. Thus, it is guaranteed by our reasoning protocols that every transitional computation carried out by the DNN is dependable on its ultimate output, viz., the anticipation of label rather than assuming the model as a black-box and relying on its anticipation explicitly. Algorithm 2 contains the presentation of pseudo-code for our Deep k-Nearest Neighbors (D-k-NN) protocol. The reason for permitting D-k-NN algorithm for reinforcing the understanding and sturdiness of its anticipations by the Deep Neural Network (DNN) is to be analyzed. In Figure 5, the instinct behind D-k-NN is mentioned. Explaining the definition and the significance of assertion, understanding, sturdiness and their part in ML in argumentative situations are the consequences of the instinct.

D-k-NN is deemed to be a nonparametric method. The Euclidean Distance is frequently used by KNN classifiers as the distance metric. D-k-NN classification is demonstrated in Figure 6, where the classification is done on new input samples. Malevolent behaviour is denoted by the red circles, and the typical behaviour of the system is represented by the green circles in Figure 6. Based on the votes of the chosen number of its close-by neighbours, the new examples are categorized by the KNN classifier. It means that using most of the votes of its close-by neighbours, D-k-NN determines the anonymous sample class. The class of the hidden D-k-NN sample is categorized by the D-k-NN as normal behaviour as green represents the two neighbouring circles, i.e., normal behaviour in case the D-k-NN classification depends on two close-by neighbours ($k = 2$). The class of the anonymous sample is categorized as malevolent behaviour as the red circles, i.e., malicious behaviour represents the three and four neighbouring circles in case the KNN classification depends on three and four close-by neighbours ($k = 3$ and $k = 4$). For determining the optimal value of 'k's of a given dataset, a significant step is assessing heterogeneous values of 'k's during the cross-validation process. Depending on the datasets, the optimum k value often differs though the D-k-NN algorithm is an undemanding classification algorithm and successful on massive training datasets. So, the process of ascertaining the optimal value of k involves challenges and time loss. IDPS is benefited by D-k-NN classifiers.

A model was proposed to detect DDoS and wormhole attacks considering the IoT environment. The two layers of feature minimization are used for improving efficiency by curbing the features' dimensionality. Then, a 2-Tier classification model, which makes use of NB and D-k-NN classifiers, is deployed. For both attacks, good detection results are produced by the proposed model. IDPS based D-k-NN was developed by another research. In a wireless sensor network that is a significant unit of Multi-Layer IoT systems, the classification of nodes as normal or abnormal is done by the developed system. A competent and precise IDPS are the outcome of the proposed method.

Briefly, when a test input 'x' is presented:

1) To acquire the I representations output by DNN's layers, we run input 'x's through the DNN function: $\{f\lambda(x)|\lambda \in 1, 2, \cdots, l\}$.

2) The k's training points where one of the test inputs and representations at layer λ are nearby are discovered by using a locality-sensitive $H(f)$ based D-k-NN classifier for each of these representations $f\lambda(x)$.

3) The multi-set $\omega\lambda$ of labels allotted in the training dataset to the D-k-NN representations retrieved at the earlier step is collected for each layer λ.

Algorithm 2 Algorithm 2 of Deep-k-Nearest Neighbor's

Input: DL-Training Data Set (X, Y), Measured Data Set (Xc, Yc) Trained K-NN 'F' with Frist Layers Number of 'Dc' of Nearest Neighbors Data Set 'Dz'
1: For Each Layer $\lambda \in 1, 2, \cdots, l$ Do
2: $D_\Gamma \leftarrow D_c$ points in X Closest to 'D_z' found w/ LSH tables
3: $D_{\omega\lambda} \leftarrow \{D_{Y_i} : D_i \in \Gamma\}$ Labels of 'c' inputs found
4: End For
5: $A = \{\alpha(x, y) : (x, y)(D_{X_c}, D_{Y_c})\}$
6: For Each label $j \in 1, 2, \cdots, n$ **Do**
7: $\alpha(z, j) \Leftarrow P\lambda \in 1, 2, \cdots, l | i \in \omega\lambda : i6 = D_j|$
8: $D_{p_j}(z) = |\{\alpha\epsilon \in A : \alpha \geq \alpha(D_z, D_j)\}||A|$
9: End For
10: Attack Manipulation $\Leftarrow$ Average Max. $j \in 1, 2, \cdots, n$ $D_{p_j}(z)$
11: Data Security $\Leftarrow 1 - MAX.J \in 1, 2, \cdots, n, j6 =$ Attack Manipulation $p_j(z)$
12: Integrity $\Leftarrow$ MAX. $J \in 1, 2, \cdots, nD_{p_j}(z)$
13: Return Attack Manipulation, Data Security, Integrity
14: End

4) According to the conformal AM's framework, to calculate the AM of our D-k-NN, all multi-sets $\omega\lambda$ are used.

The unsupervised training is performed to acquire the concealed layers' weights of this DBN model denoted by LWi, as displayed in Figure 7. Nonetheless, the primary weights are allotted by using the unsupervised training from where the parameters are generated. The transformation of DBN enables the creation of DNN, that is, a type of feed-forward ANN after the DBN is constructed efficiently. Due to this, for creating a classified DL model on each network transaction, a BC layer and label information are appended at the topmost layer of this DBN model. The stacking of the BC layer and label information in the DBN for converting it into a DNN is shown in Figure 8. Today, with the help of the label information, a bottom-up supervised learning method is utilized for training the DNN model. Each node in a DNN layer is allotted a weight parameter handled by the gradient descent approach during supervised learning.

A binary cross-entropy loss function attempts to reduce the model's total cost according to the proposed DNN model's unbiased process as indicated in Algorithm 3.

5 Implementation of Multi-Layer IoT Model on Deep Learning for IDS

When an intrusion is identified, a warning to the security administrator is permitted by this module to secure the system, and the accurate counteraction is applied. Preventing the infection of besieged devices and the exploita-

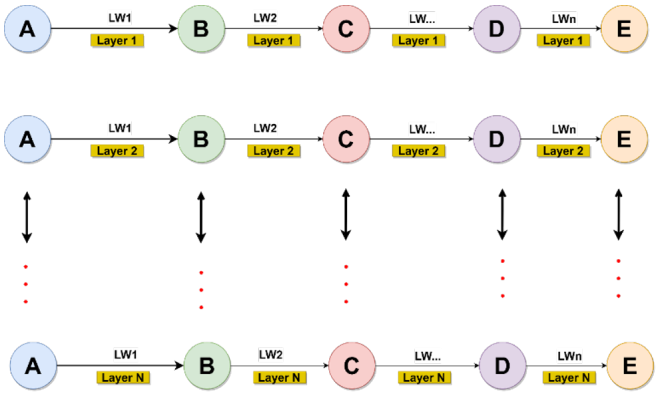

Figure 7: Deep belief network structure

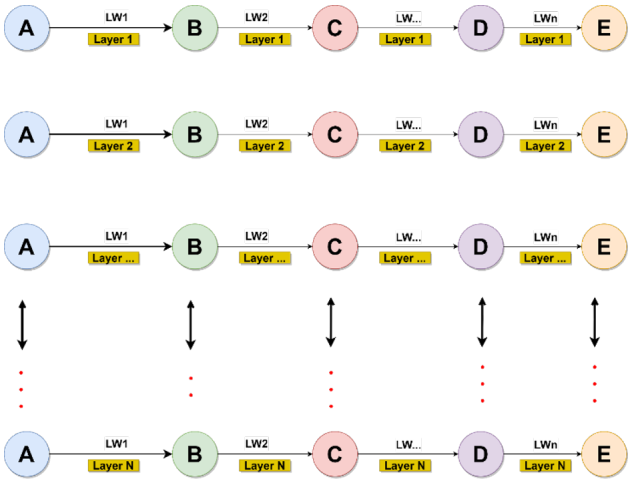

Figure 8: Deep neural network structure

Algorithm 3 The exploitation of deep-learning model for intrusion detection

Input: Number of all HEAD-TAGs from Primary Data Source in IoT
1: Attack Manipulation Function **(Primary Data Source)**
2: Confusion Matrix $\Leftarrow$ Primary Data Source
3: Extract Features from Confusion Matrix
4: State Trained Data Set (0,1) & Test Dataset (0,1)
5: Set Sequential DL Model
6: If Data Set =1 **Then**
7: Collect 0s and 1s Information Classification
8: AM $\Leftarrow$ Sequential DL Model
9: End If
10: Training Data Set, AM $\leftarrow$ Data Set
11: If Training Data Set =1, **Then**
12: Attack Manipulations (AM) $\Leftarrow$ Test Data Set
13: If AM =1, **Then**
14: Re-Train the DL Model
15: Else
16: Set Data Verification and Validation Phase
17: End If
18: End If
19: Sources of Classification Data $\Leftarrow$ AM
20: End If
End

tion of the whole system instigated by security attacks or anomaly behaviour are the utmost aims. The prevention system, besides the self-protective actions contrary to the familiar menaces, are briefed in this section. Based on the identified threat, there are two types of response in this prevention phase: passive and active prevention. As shown in the prevention system in Figure 9, the security administrator is given a quick warning immediately after detecting the threat at the first ML detection level.

In contrary to the particular device, the administrator is given the first alert regarding an in-progress hazard. To enable the operating environment to provide alerts well in advance in case of an emergency, the threat alert is given at the earliest. Once the detection of the second ML is over and a known threat is detected, the third ML level sends the accurate kind of threat to the device and deploys the already related security action autonomously. The ML models that had already considered the threats and their prevention actions are stockpiled in the fog. The administrator will be sent a new status alert regarding the existing status of the device. The passive phase, which doesn't need any human intervention, contains these first steps. Self-defending from the already familiar threats is the capability of the IoT system. The active prevention phase commences if the GFlow is tagged by the second ML level as anonymous. This phase requires the database's threats before several GFlows were identified as unknown, and the continuous learning module is yet to process it. The administrator had already annotated them. The name of the threats is updated in this case. The name of the threat associated with action by the table also needs updating if a security action had also been defined by the administrator for this threat. The memory usage of the fog layer is prevented by storing this database in the cloud. Also, to the whole IoT system, this is shared.

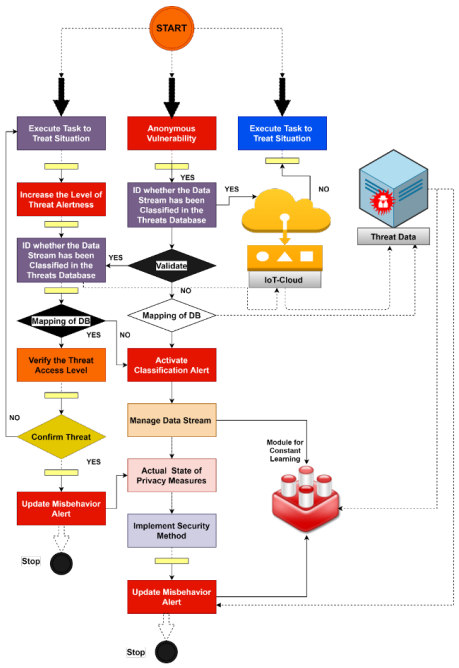

Figure 9: Threat prevention using IoT and the cloud date flow diagram

6 Results and Discussion

The execution of the proposed IDPS on Multi-Layer IoT networks is discussed. The Deep Neural Network (DNN) executed by python is the base of the proposed DL-IDPS. The DNN generated for the proposed DL-IDPS is implemented and tested by python. The comprehensive outcomes of each IDS classifier acquired employing a Gated-Recurrent-Unit (GRU) neural network are also provided. Because the representation of data in detecting abnormality is generally a matrix, it eases the implementation process of anomaly-based IDPS. The 10% KDD CUP '99 dataset is chosen for training and testing the DL algorithms, as depicted above. As shown in the architecture diagram, the types of Attacks at the concerned TCP/IP are the basis for splitting the dataset into various layers. As the attack type doesn't belong to the Link Layer category, it is not considered part of this research. As shown in Table 1, the entire attack types in the dataset come into one of the three TCP/IP layer categories.

Based on the type of Attack, each sample is read and added to a new dataset. Out of the 392,367 test samples contained in the dataset for the Application Layer IDS, the "normal" test samples are 90,145, and one of the attack types is the categorization of the remaining samples. Before the three categorical features contained in the dataset are fed as input to the algorithm model and must be encoded into numerical form. The encoding of the attributes like "Protocol Type", "Service", and "Flag" into numerical values is performed. The training data are supposed to be 80% of the data, and the testing data are 2% of the data for every dataset. The features set and the respective label set is the categorization of each dataset.

The label "normal" is encoded as [0s/1s], and "all other attack types" is encoded as [1s/0s]. Thus, the assessment metrics like FPR, AUC, Recall, Accuracy, and Precision are used for classification. In this section, we have depicted the graphical representation of the five metrics: F1-score, Precision, Recall, and the proposed DL-IDPS's training time requirement over 200 separate runs. Two parts are contained in each run: training and the testing cycle.

6.1 Investigation of DDoS Attack

The proposed IDS proves comparatively more Precision (0.9) and Recall (0.94) than the remaining IDSs that demonstrated 0.8 Precision and 0.9 Recall, as shown in Figure 10. It is noted that contrary to DDoS and wormhole attack, the IDS performs better. However, the range of the F1-score (0.918) for both the proposed IDS and

Table 1: Network and transport layer attacks

Layer	Attack Types
Application	PoD, Data_Buffer_Over_Flow, Load_Threat_Module, N_Map, Guess_Pwd, FTP_Write, Multi_Hop
Transport	Neptune, Tear_Drop, Port_Sweep, Data_Buffer_Over_Flow, N_Map
Network	Data_Over_Flow, PoD, IP_Spoof
All Layer IDS	Active and Passive attack types

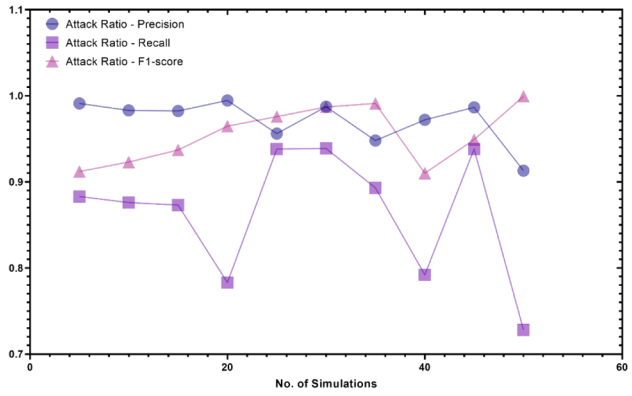

Figure 10: DDoS attack performance evaluation using Precision, Recall, and F1-score

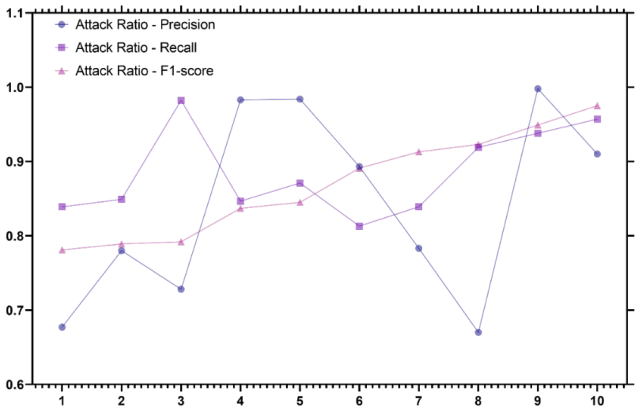

Figure 11: Wormhole DDoS attack performance evaluation using Precision, Recall, and the F1-score

other IDSs is between 0.8–0.9. The dependability of the proposed DL-IDPS is established by testing it on DDoS and Wormhole attacks in test-bed made using actual IoT sensors.

A. Investigation of Wormhole Attack The F1-score values, Recall, and Precision for our proposed DL-IDPS and the remaining works are observed from Figures 11 to have normalized to an average rate of 0.9. It is to be noted that the ID undergoes training before these tests, thus keeping the training time constant. In a real-network system, it can be viewed that the proposed intrusion detection system's performance does not have much demarcation than the simulated network traffic. Also, based on Rules-Based Techniques, we implemented other IDPSs to make a comparison with the literature.

6.2 Performance Metrics

Using the KDD Cup '99 labelled testing dataset, the proposed DL-IDPS for detecting an anomaly in Multi-Layer-IoT networks is tested using DL. 19843 is comprised in the testing dataset, i.e., 33.333% of input dataset wherein 6 values are contained in each record; transmission-to-reception ratio, reception-rate, transmission rate, information regarding BC label and data-value, transmission mode, duration, SRC_IP, and DESTN_IP. The IoT sensors and COOJA simulator read data-value information, time, SRC_IP, and DESTN-IP. In contrast, the reception rate, transmission rate, transmission mode, and transmission-to-reception ratio are provided with values calculated from other features acquired from the simulations. The malevolence or benevolence of the network transaction is represented by the BC label information.

The labelled training dataset containing 39686, i.e., 66.667% of the input dataset, was used to train the DNN. However, by not providing the BC label information that discloses the belongingness of each record in the testing dataset in the BC, the DNN is operated against the testing dataset. In other words, without any BC labels, the DNN was performed against a testing dataset. The DL model generates 39686 predictions in the form of "0" or "1" as the unlabelled records of the testing dataset are 39686. Next, with the actual labels of the testing dataset for each record, the comparison was made between the results acquired from the testing and Table 2 and Figure 12 shows the results.

It can be assumed from Table 2 that when the '70' time-steps are given to the input, the performance of the model is enhanced. Hence, for the further experiments of the All-Layers IDS in the research, this value is selected. In Figure 13, the plots that influence the time-steps and the learning rate on FAR, Recall and Precision in training for All-Layer IDS classifier are observed.

The information regarding True-Negatives (TN), False-Negatives (FN), False-Positives (FP) and True-Positives (TP) is furnished by the confusion matrix in Figure 14. For the All-Layer IDS classifier, Table 3 presents the total matrix values with the ideal hyper-parameter combi-

Table 2: Criteria for all layer IDS classifier

Time Steps	Training Dataset Precision	Training Dataset Recall	Training Dataset F1-score
5	0.9981	0.9192	0.9457
10	0.983	0.923	0.987587
15	0.9373	0.901	0.98668
20	0.984	0.9033	0.0991
25	0.9634	0.9004	0.09585
30	0.967	0.945	0.9921
35	0.974	0.9678	0.912
40	0.983	0.9193	0.9003
45	0.99912	0.94609	0.90103
50	0.9548	0.9844	0.93534

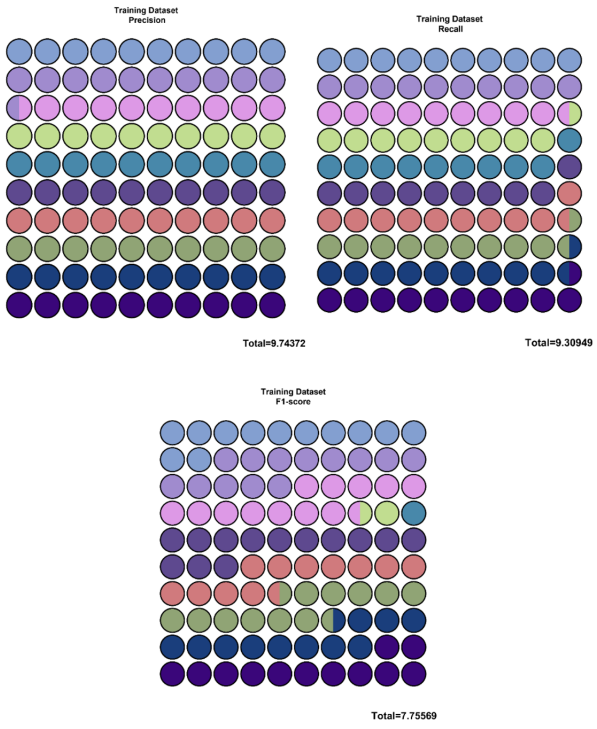

Figure 12: The labelled testing dataset from the KDD Cup '99

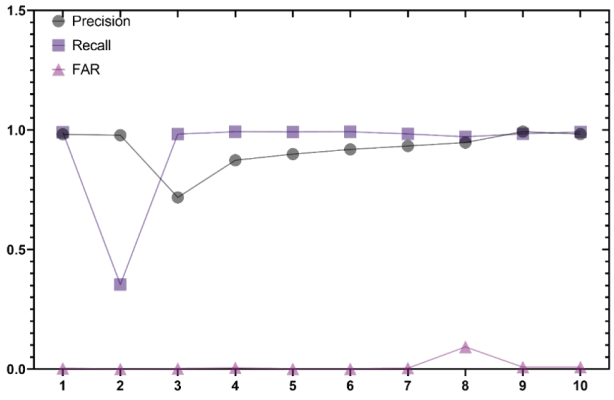

Figure 13: Precision, Recall, and F1-score for IoT layer classifications

nation (Time-Steps = 40, Learning Rate = 0.01).

Table 3: Confusion matrix for IDS with multiple layers

TN	FT	FN	TP
78191	1349	7681	31029

The accuracy of 95.04% regarding the warning given on the unusual network traffic in the Multi-Layer-IoT network is shown by the proposed DL based IDPS. The ability to produce results very accurately using DL for anomaly-based IDPS is meant to be high percentage of accuracy.

The accuracy of 95.04% regarding the warning given on the unusual network traffic in the Multi-Layer-IoT network is shown by the proposed DL based IDPS. The ability to produce results very accurately using DL for anomaly-based IDPS is meant to be high percentage of accuracy. The minimum FAR is made by a highly accurate classifier. Since an IDPS with maximum FAR is expen-

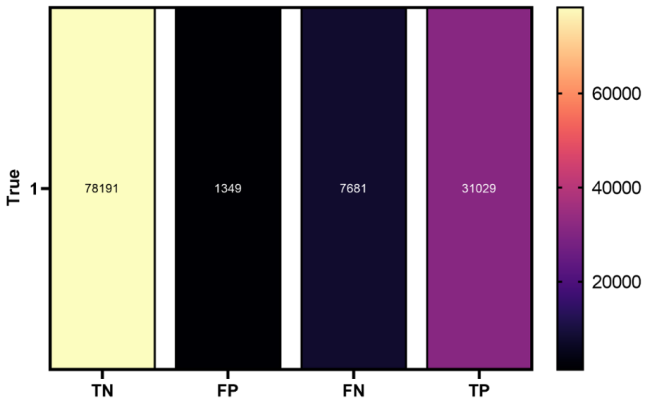

Figure 14: IoT layer IDS confusion matrix

sive to handle the alarms with abnormalities though they don't have anomalies, they might not be utilized. This happens even a FPR of 4.58% is shown by the proposed IDPS. The IDPS's cumulative loss rate that has a FNR is equivalent to this value. The impact on the sensitivity of the system or Recall has also got significance. The 4.58% sensitivity of the proposed IDPS indicates that the DL model's FNR is 2.37%. The DL model's FNR shows the possibility of the anomalies surpassing the IDPS unnoticed. The percentage is essential and reveals the extent to which the device can take the risk, though this percentage's performance is not decided upon. The essentiality of the IoT data decides whether to accept this percentage or not, whereas 4.58% is trivial, and this cannot be pulled down to 0% by any IDPS. For instance, human life is not threatened by these intrusions if this miscalculated percentage might be acceptable. The overall accuracy of the proposed DL-IDPS is more compared to the current operations of Fuzzy Neural Network. Since obtaining accuracy in detection seems that BC is adequate, it is explicit from the results that the number of classifiers is inaccurate to the Multi-Layer-IoT environment. Moreover, when compared to the conventional NIDS, the performance of the proposed DL-IDPS is better.

7 Conclusion

Across the world, the pervasiveness of IoT has been progressing fast in recent years. The inter-disciplinary research has implemented DL techniques for IoT security for the first time as it is innovative in some way. In a Multi-Layer-IoT network, a lightweight architecture has been proposed for an IDPS. The proposed IDPS was tested on DDoS, wormhole attacks and 200 runs. At every classifier, this has minimized the dataset size, and the performance is improved in the form of FAR, accuracy and training time. To categorize the data at every IDS classifier, the DL algorithms have been applied. Besides active and practical response, our proposal also features scalability and concern for limited resources, autonomy, flexibility and stretchability, and design integrity. For the purpose of simulations, the Gated-Recurrent-Unit Neural Network is applied to KDD Cup '99 dataset. Before the standardization of accuracy at 95%, a firm increase of IDS rate of up to the first 30 runs is recorded. The complete training of the proposed DL-IDPS within the first 30 runs is indicated by this. The observation shows that before the proposed DL-IDPS received comprehensive training, it displayed an average FAR of 4%. This tendency suggests that by not using much of the computational and power resources, the proposed DL-IDPS can secure the Multi-Layer-IoT networks effectively and reliably.

References

[1] Q. Abu Al-Haija and S. Zein-Sabatto, "An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks," *Electronics*, vol. 9, no. 12, p. 2152, 2020.

[2] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," *Procedia Computer Science*, vol. 60, pp. 708–713, 2015.

[3] M. Bahrololum, E. Salahi, and M. Khaleghi, "Anomaly intrusion detection design using hybrid of unsupervised and supervised neural network," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 1, no. 2, pp. 26–33, 2009.

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, *Network traffic anomaly detection and prevention: concepts, techniques, and tools*. Springer, 2017.

[5] L. Bilge, D. Balzarotti, W. Robertson, E. Kirda, and C. Kruegel, "Disclosure: detecting botnet command and control servers through large-scale netflow analysis," in *Proceedings of the 28th Annual Computer Security Applications Conference*, 2012, pp. 129–138.

[6] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach," *Computer Communications*, vol. 98, pp. 52–71, 2017.

[7] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[8] L. Deng, D. Li, X. Yao, and H. Wang, "Retraction note to: Mobile network intrusion detection for iot system based on transfer learning algorithm," *Cluster Computing*, vol. 24, no. 1, pp. 589–589, 2021.

[9] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017.

[10] E. Gherbi, B. Hanczar, J.-C. Janodet, and W. Klaudel, "An encoding adversarial network for

anomaly detection," in *Asian Conference on Machine Learning*. PMLR, 2019, pp. 188–203.
[11] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of iot networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2016, pp. 1–6.
[12] P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis, "A signature-based intrusion detection system for the internet of things," *Information and Communication Technology Form*, 2018.
[13] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," *arXiv preprint arXiv:1312.6114*, 2013.
[14] S. Latha and S. J. Prakash, "A survey on network attacks and intrusion detection systems," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2017, pp. 1–7.
[15] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77 396–77 404, 2020.
[16] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 military communications and information systems conference (MilCIS)*. IEEE, 2015, pp. 1–6.
[17] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.
[18] T. A. Razak *et al.*, "A study on ids for preventing denial of service attack using outliers techniques," in *2016 IEEE International Conference on Engineering and Technology (ICETECH)*. IEEE, 2016, pp. 768–775.
[19] V. Škvára, T. Pevnỳ, and V. Šmídl, "Are generative deep models for novelty detection truly better?" *arXiv preprint arXiv:1807.05027*, 2018.
[20] S. Smith, "Iot connected devices to triple to over 38bn units," *Juniper Research*, 2015.
[21] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, "An overview of ip flow-based intrusion detection," *IEEE communications Surveys & Tutorials*, vol. 12, no. 3, pp. 343–356, 2010.
[22] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *2010 IEEE symposium on security and privacy*. IEEE, 2010, pp. 305–316.
[23] B. Susilo and R. F. Sari, "Intrusion detection in iot networks using deep learning algorithm," *Information*, vol. 11, no. 5, p. 279, 2020.
[24] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *2009 IEEE symposium on computational intelligence for security and defense applications*. Ieee, 2009, pp. 1–6.
[25] O. Vermesan, P. Friess *et al.*, *Internet of things-from research and innovation to market deployment*. River publishers Aalborg, 2014, vol. 29.
[26] H. Zhao, Q. Chen, W. Shi, T. Gu, and W. Li, "Stability analysis of an improved car-following model accounting for the driver's characteristics and automation," *Physica A: Statistical Mechanics and Its Applications*, vol. 526, p. 120990, 2019.
[27] H. Zhao, D. Xia, S. Yang, and G. Peng, "The delayed-time effect of traffic flux on traffic stability for two-lane freeway," *Physica A: Statistical Mechanics and its Applications*, vol. 540, p. 123066, 2020.
[28] H. Zhao, H. Yue, T. Gu, C. Li, and D. Zhou, "Low delay and seamless connectivity-based message propagation mechanism for vanet of vcps," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3385–3402, 2021.
[29] H. Zhao, H. Yue, T. Gu, and W. Li, "Cps-based reliability enhancement mechanism for vehicular emergency warning system," *International Journal of Intelligent Transportation Systems Research*, vol. 17, no. 3, pp. 232–241, 2019.
[30] B. Zong, Q. Song, M. R. Min, W. Cheng, C. Lumezanu, D. Cho, and H. Chen, "Deep autoencoding gaussian mixture model for unsupervised anomaly detection," in *International conference on learning representations*, 2018.

Biography

Sirajuddin Qureshi received his bachelor's degree in Computer Sciences from Quaid-e-Awam University of Engineering, Science & Technology, Pakistan. Afterwards, he pursued his Master's in Information Technology from Sindh Agricultural University Tandojam, Pakistan. Currently he is pursuing PhD in Information Technology at Beijing University of Technology, China. He has nine research publications to his credit as main author and co-author, which featured national and international journals and conferences. Sirajuddin's research areas includes but not limited to Network Forensics Analysis, Digital Forensics, Cyber security, Computer Networks and Network Security.

Jingsha He received the bachelor's degree in computer science from Xi'an Jiaotong University, China, and the master's and Ph.D. degrees in computer engineering from the University of Maryland, College Park, MD, USA. He worked for several multinational companies in USA, including IBM Corp., MCI Communications Corp., and Fujitsu Laboratories. He is currently a Professor with the Faculty of Information Technology, Beijing University of Technology(BJUT), Beijing. He has published more than ten articles. He holds 12 U.S. patents. Since August 2003, he has been published over 300 papers in scholarly journals and international conferences. He also holds over 84 patents and 57 software copyrights in China and authored nine books. He was a principal investigator of

more than 40 research and development projects. His research interests include information security, wireless networks, and digital forensics.

Saima Tunio received the BSIT(Hons) with gold medal from Sindh Agricture University Tandojam, Pakistan. Afterwards, she pursued her MSIT from Isra University Hyderabad, Pakistan. Currently she is pursuing PhD in Information Technology at Beijing University of Technology, China.She has more than five research publications to her credit as main author and co-author, which featured national and international journals and conferences. Saima's research areas includes but not limited to Information security.IoT security, Digital Forensics, Cyber security, Computer Networks.

Nafei Zhu received the B.S. and M.S. degrees from Central South University, China, in 2003 and 2006, respectively, and the Ph.D. degree in com- puter science and technology from the Beijing University of Technology, Beijing, China, in 2012. She was a Postdoctoral Research Fellow with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, from 2015 to 2017. She is currently an Associate Professor with the Faculty of Information Technology, Beijing University of Technology. She has published over 20 research papers in scholarly journals and international conferences. Her research interests include information security and privacy, wireless communications, and network measurement.

Faheem Ullah received the M.S degrees from the Xian Jiaotong University, China,in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Technology, Beijing, China. His research interests include information security, Blockchain and data mining. He has received awards and honors from the China Scholarship Council (CSC), China.

Ahsan Nazir has received his M.Sc degree from University of Engineering and Technology Lahore in 2016. From September 2015 to August 2018 he worked as software Engineer at Dunya Media group Lahore since September 2018 he is doing PhD in Software Engineering from Beijing University of Technology , Beijing China. He has published more than 10 journals and conference papers.His area of research include eGovernment,IoT,Software Engineering and Machine learning applications.

Ahsan Wajahat received the B.S. and M.S degrees in information technology from the Sindh agriculture University, Pakistan, in 2012 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Beijing University of Technology, Beijing, China. His research interests include machine learning, information security, forensic network and data mining. He has received awards and honors from the China Scholarship Council (CSC), China.