AN INTELLIGENT IOT ATTACK DETECTION FRAMEWORK USING EFFECTIVE EDGE AI BASED COMPUTING

V. S. Saranya
Research Scholar
Department of Computer Science and Engineering
Annamalai University
Annamalainagar – 608002

lord.shivam1988@gmail.com

Dr. G. Ramachandran
Associate Professor
Dept. of Computer Science & Engineering
Annamalai University
Annamalainagar – 608 002.
gmrama1975@gmail.com

Dr. S. Chakaravarthi
Professor
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India.
chakra2603@gmail.com

Abstract

More amount of IoT devices are included, weared in day today's lifestyle. These Internet of Things (IoT) devices are intelligent and makes ease the decision making processes by overcoming the challenges with the integration of Artificial Intelligence (machine learning and deep learning) techniques. It is necessary to ensure whether the collected intelligent information is utilized in secure manner. Slower data processing may lead to data breaches or leaks in data communication. Hence, to address the above-mentioned issue, this paper proposed a novel and secured intelligence framework. The proposed framework adopts edge computing to increase the speed of data processing in order to integrate the security essentials amid software applications and their associated networks. As this proposed framework is enabled with AI, discovering malicious threats become effective. Finally, the proposed framework achieves a maximum accuracy of 99.5% than any state of the art models.

***Keywords*: IoT, Artificial Intelligence, Edge Computing, Intrusion Detection.**

1. Introduction

With the advanced growth of electronic communication technologies and IoT, lifestyle is digitally connected [1]. IoT plays a vital role in building smart world by allowing connections amid billions of smart devices and gadgets. Making use of advanced cyber technologies, it is possible to manage traditional systems in effective and efficient manner. Enormous amount of IoT applications are cultivated and installed recently which is aimed with much comfortable lifestyle. But risks are increased against physical systems in terms of cyber vulnerabilities and threats. Large amount of security vulnerability cases are reported today. As per Kaspersky, IoT cyber-attacks are doubled in the first half of 2021 comparing to the previous year i.e., 1.51 billion IoT breaches are happened which implies an increase as 639 million [2]. Attacks like cryptocurrency mining, Distributed Denial of Service (DDoS) attacks played key roles in damaging the assets and stealing confidentiality of data [5][9]. Most of the attackers tried to get access in IoT networks through Telnet protocol which is a command line interface used for enabling remote communication. Based on the results, pandemic worsened IoT vulnerabilities with the persistence of IoT device usage. Most of them seem weak because of their inadequate security protocols.

Security of IoT devices and its applications becomes one of the most substantial problems [38]. Injection of malicious code and security breaches will limit the development and deployment of IoT applications and will

cause massive asset losses [3]. Providing sound security protection is a challengeable task for IoT applications along with resource limitations which seem main concerns [4]. Multiple research works are carried out for resolving the shortcomings of existing security methods [9][12][22]. Modern security algorithms such as Attribute-Based Access Control (ABAC), group signature scheme, homomorphic encryption and asymmetric key related solutions are utilized and they require devices with appropriate computational power and memory for execution [5][6]. There are some issues while applying them in multiple IoT devices especially smart end devices.

Though cloud technologies provide enormous amount of resources, it could not able to meet the requirements for providing effective services for IoT end devices. To resolve such kind of issues, edge computing technology is emerged for migrating the resources associated with computation and memory by forming an edge layer near IoT end device [7]. Thus, edge layer balances the loads of various tasks related to high level computation and resource on demand. This novel computing pattern simplifies resource management of IoT devices and also system performance is optimized [8-10]. In addition, it becomes a new spot for developing and deploying IoT end devices in secured manner. Few researchers worked in the proposals related to IoT security solutions on the basis of edge computing which is included in various fields like security designs, firewalls, Intrusion Detection Systems (IDS), authentication and authorization protocols and privacy preserving methods [11-16][30]. Still researches related to IoT security on the basis of edge computing is in beginning stage. Comprehensive reviews to be done towards various refined edge computing based IoT security models.

The key contributions of the work are summarized as below:

- Edge computing based Intrusion/Attack Detection framework is proposed by utilizing the optimal selection algorithms in runtime based on the data input.
- Data interchange in IoT environment is secured by increasing speed of data processing by applying edge computing.
- Quality of Service (QoS) value is improved for effective communication with the integration of security essentials.

The rest of the paper is organized with the following sections: Section II defines earlier existing works in detail, Section III details about edge computing technology and its importance, Section IV describes the proposed framework, Section V discusses the results obtained and finally the conclusion of this research work is delivered.

2. Related Work

Multiple research works are carried out for protecting IoT end devices against various intrusion attacks like Man-In-The-Middle (MITM), Distributed Denial of Service (DDoS) and so on. Availability of data in IoT ecosystem is a main constraint where various decision making processes are depended on real time data [39-44]. In this section, multiple threat detection approaches are detailed in elaborated manner.

Behavioural Modelling Intrusion Detection System (BMIDS) is proposed by utilizing immunity-inspired algorithms for categorizing behavioural patterns [17]. This anomaly detection system is based on IoT behaviours. For designing appropriate behaviour models, activities are monitored by making use of smart simulation environment. Objective of BMIDS is to maximize detection sensitivity through IoT end devices for diagnosing uniqueness amid behavioural patterns.

Semi-supervised anomaly detection system by making use of k-means algorithm is proposed for detecting network attacks [18]. Cluster is formed with the help of k-means algorithm by classifying typical samples in training phase. Distance based threshold value is computed to differentiate normal and abnormal samples by utilizing validation dataset. Samples which are far away from the centers of cluster are considered as anomalies. Labeled dataset NSL-KDD is utilized for testing proposed system's performance and detection result is attained with 80.119% accuracy.

With the integration of SDN and Blockchain, IoT based distributed Software Defined Networking (SDN) architecture is implemented [19]. Interaction among nodes is permitted without the help of central controller. Entire IoT controller environment is connected for effective communication by implementing distributed block chain. Amalgamation of flow control analyzer and packet migration components supports network functioning during attacking scenario. For accurate attack detection, various IoT device oriented attack simulations like ARP poisoning, DDoS and fake topology attacks are designed. Proposed technique reduces attack window detection time and it also fastens attack mitigation.

On the basis of sampling with Least Square Support Vector Machine (LS-SVM), intrusions are detected [20]. This method has two stages. Training and testing datasets are combined for determining the size of sample. Optimum Allocation (OA) scheme is used by defining the size of training and testing. At first stage, dataset is categorized into predetermined subgroups of arbitrary instances. In the second stage, LS-SVM is incorporated for intrusion detection by extracting the samples which uses selective instances as input. Proposed algorithm is

referred as Optimum Allocation-based Least Square Support Vector Machine (OA-LS-SVM) algorithm. Further, KDD 99 database is used for system's performance evaluation.

Network behaviours of IoT end devices are extracted and statistical analysis method is utilized for Doshi et al's anomaly detection method [21]. It is found that Mirai and BASHLITE are two highly infectious botnets which compromised most of the IoT end devices. Mirroring port of switch is used for capturing typical network flow and 115 features are extracted. For maintaining separate model for every IoT end device, neural network autoencoder is used. With the sum of mean and standard deviation of samples, anomaly threshold value is computed. On the basis of experimental results, 100% True Positive Rate (TPR) is attained with some alarm elevations.

Mehmood et al proposed NB-MAIDS which concentrate on the improvisation of intrusion detection accuracy by utilizing network behaviours of IoT for feature selection [22]. Detecting and preventing DDoS attack, traffic of the devices associated with the home network is considered as ultimate aim. Naïve Bayes classification algorithm plays vital role for intrusion detection systems which is a light weighted algorithm used for pattern matching. Better performance is obtained while implementing NB algorithm with multiple agents. Secured IoT network layer is aimed from malicious DDoS traffic. Based on the experiment results detection accuracy is achieved as 91.99%.

Ahmed and Rajput worked in order to safeguard IoT end devices against DDoS attacks [23]. Development of IDSs is done using Naïve Bayes classification algorithm. Multi agent system comprised with a collection of autonomous agents is incorporated for learning IoT end devices. Then, Multi agent IDSs are deployed for observing abnormal network traffic amid nodes during communication. Four various agents are utilized which are collector agent, system monitoring agent, actuator agent and communication agent with respective roles. Data collection is performed by collector agent and the entire multi agent system is monitored by system monitoring agent. Actuator agent is meant for reacting against the detected attackers. At last communication agent communicates with other agents of the network regarding detection results. Results show that attack detection and prevention is fast and entire load is dispersed for agents in appropriate manner.

Block chain based intra and inter-domain DDoS attacks mitigation method is proposed [24]. It permits various SDN based domains for transferring secured information regarding attacks without any centralization method. Thus it provides attack mitigation in effective manner against attacks. Further, cost reduction of useless attack traffic is done. Smart contract-based method is proposed by making use of Ethereum smart contract technology to enhance security. In addition, flow sampling method is utilized for measuring randomness of data. At last, automatic detection of inside domain's traffic anomalies is succeeded using Bayes-based scheme. Results depict effective solution in terms of cost and flexible anomaly flow detection.

Anomaly detection framework is developed by adopting SDN, ML and fog computing technology [25]. It affords network control in the infrastructures of cloud and network edge. Various features are selected for ML computation and comparative parameters are formulated on the basis of cloud and fog network of IoT. For increasing DDoS attack detection accuracy, Recurrent Neural Network (RNN), Multi-Layer Perceptron (MLP) and Alternate Decision Tree (ADT) are utilized. An access list with a set of blacklist prefixes is maintained by every controller during mitigation stage. It is concluded that comparing with cloud infrastructure, fog computing performs better while detecting attacks.

Collaborative and intelligent network-based IDS, SeArch is proposed by Nguyen et al for software defined cloud IoT infrastructure [26]. Detection of anomalies and SDN based IoT gateway devices policy formulation are combined by making use of hierarchical layered intelligent IDS nodes for braking malicious traffic quickly. Collaborative attack detection is performed by locating multiple IDS at network edge and cloud. ML classification algorithms like Support Vector Machine (SVM) and Self Organizing Map (SOM) are utilized for detecting anomalies and making policies at every network level. Data samples of 30K from 3 various datasets are extracted along with TCP and ICMP features. It provides better accuracy for anomaly detection than existing centralized methods while evaluating performance.

Another decentralized IoT network security architecture BlockSecIoTNet is developed on the basis of block chain [27]. For effective attack detection SDN, block chain and fog computing technologies are used. To monitor and examine the entire IoT network continuously, SDN is used. Similarly, Ethereum blockchain technology is used for attack detection in decentralized manner which mitigates the issues related to single point of failure problem. Attack at fog node and edge node are detected which is simplified with the help of fog and edge computing. Earlier attack detection and mitigation is possible with low memory limitations, inexpensive computation and minimum latency. Edge network's attack detection and mitigation is implemented using deep learning algorithms. Attack detection model is dynamically updated to increase detection efficiency. Anomaly classifier is associated with different data formats like numeric, binary and nominal. It is observed that proposed framework mitigate IoT attacks with minimum time.

Yang et al concentrated on detecting and mitigating IoT based DDoS attacks by making use of SDN [28]. Précised features of IoT traffic are considered while edge computing technology is applied. Distributed anomaly detection method is faster and it didn't affect centralized controller during the scenarios of IoT attacks. Edge

gateway process the detection request which avoids controller intervention even in real time environment. Flow level features are taken as input for feature extraction. Mininet is used for experiment's simulation purpose. To categorize genuine flows amid DDoS flows, three various ML algorithms are utilized. Among them RF provided better results with 100% True Positive.

Research Work	Features	Technology used	Algorithms of Classification	Detection Method
Sharma et al [19] [2017]	All traffic, scanning attacks	Block chain, SDN	Mean and standard deviation technique	Traffic statistic
Doshi et al [21] [2018]	Behaviour learning, packet header fields, aggregate flow	Traditional Internet	Machine Learning	Anomaly detection
Mehmood et al [22] [2018]	Multi agent, DDoS traffic	Traditional Internet	Naïve Bayes Algorithm	NB-MAIDS
Houda et al [24] [2019]	Anomaly detection, Inter and intra-domain collaborative DDoS mitigation	Block chain, SDN	Collaborative approach, smart contract-based approach, flow sampling method	Bayes-base scheme
Shafi et al [25] [2019]	Cloud infrastructure, DDoS attacks	SDN and Fog computing	Entropy based	Anomaly detector
Nguyen et al [26] [2019]	Reconnaissance attacks	Block chain, SDN, Fog computing	Machine learning	Multiple IDS
Rathore et al [27] [2019]	Host-based, time-based, content and basic features	Block chain, SDN, Fog computing, Edge computing	Deep learning algorithms	Dynamic update of attack detection model
Yang et al [28] [2019]	DDoS attacks, IoT gateway as IDS	SDN and Edge computing	Machine learning	Multiple point defence mechanism
Wazid et al [29] [2019]	Remaining energy amount of an IoT sensor, Routing attacks	Edge computing	2 stages approach	RAD-EI
Singh et al [30] [2020]	MEC environment, Three classifiers	Mobile edge computing	C4.5 classifier, Naïve Bayes, Meta Adaboost M1	Hybrid Intrusion detection

Table 1. Summary of Existing Works

RAD-EI is an intrusion detection scheme proposed by Wazid et al which is focused on IoT routing attacks [29]. Typical traffic flow can be deviated and interrupt by malicious IoT sensors in routing attack. Every malicious sensor forwards the packets towards its nearer attacker node. Here anticipated information will not be received to edge node. This detection scheme has two phases. During phase 1, doubted attack nodes list is captured while they are available in network. Doubted attacker is discovered based on the computed energy level (drained battery). In phase 2, IoT sensor is decided whether it is attacker or normal node. Any IoT device which doesn't receive any reply messages then it is considered as attacker node.

Mobile Edge Computing (MEC) based hybrid intrusion detection framework is proposed [30]. It is focused on unknown attacks which are based on ML. Traffic of MEC environment is analyzed for identifying intrusions. Three distinct classifiers are utilized in these frameworks which are C4.5 classifier, Naïve Bayes classifier and Meta Adaboost M1. Based on the experimental results, it is observed that proposed framework has 90.25% accuracy with 1.1% FAR. Security of proposed framework is analyzed using game theoretical model. While comparing to existing models, it provides better results.

3. IOT and Edge Computing Background

3.1. *IoT basic components and Architecture*

IoT environment is a universal distributed network which allows communication among various devices/computers. Communication is carried either as in wired or wireless manner. Data exchange is ensured using such communication channel. Multiple physical objects, sensors are connected and it is applicable in various application areas which is effective in terms of cost and technology. IoT economy is vast worldwide. For effective IoT environment, multiple IoT components are interconnected to build basement for IoT architecture. IoT devices, IoT connectivity, IoT platforms and IoT Apps/Interfaces are the four basic components of IoT ecosystem. Those are layered for providing different IoT solutions based on their convenient and requirement.

Due to the dynamical nature of IoT domain day by day, novel technologies are applied and adopted. It is difficult to implement one architecture as main reference for all solutions [31]. Different research works are carried

out for developing IoT architectures in effective manner. Fig. 1 depicts the four basic components of IoT eco system.

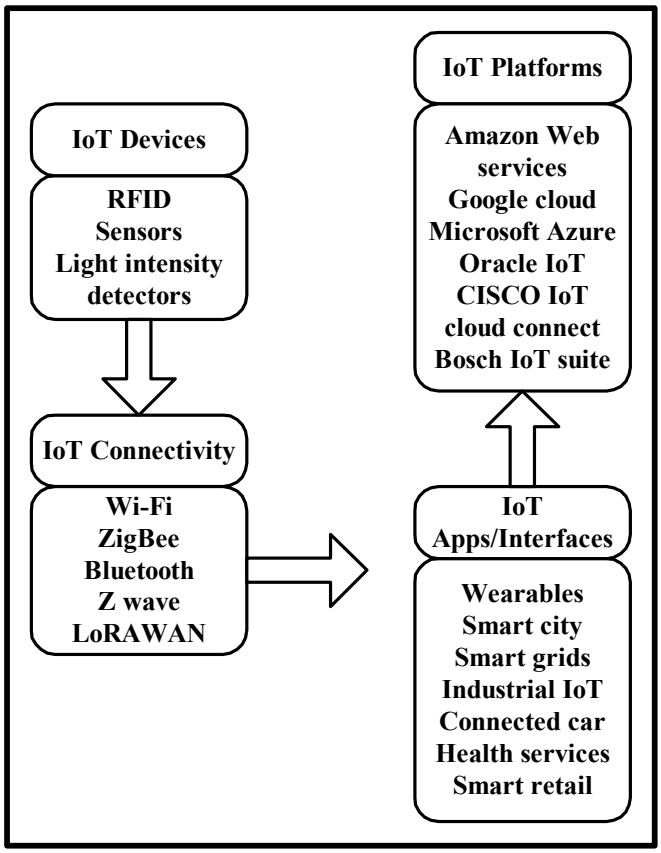

Fig.1. Basic IoT Components

IoT devices component contains the physical hardware devices and sensors. Based on the IoT solution, various hardware devices are utilized. Data is interchanged by the device in centralized manner. To resolve the connectivity issues of hardware devices, IoT gateways are used amid physical environment and IoT platform. Thus, IoT devices make their connection and data exchange is carried out within the domain.

Various IoT architectures are proposed considering all the basic components. Among them three layer, four layer and five layer IoT architectures are usual and frequently used. In three layer IoT architecture, there are 3 basic blocks which are perception layer, network layer and application layer [32][33]. Perception layer deals with devices and sensors. Network layer acts as an interface between perception and application layer where application layer states every IoT based applications.

Shortcomings of three layers IoT architecture are overcome by four layer IoT architecture in which fourth additional layer namely support layer is added [34]. Support layer is mainly meant for security. Two main tasks of support layer are authentication and forwarding information towards network layer. Five layer IoT architecture mainly concentrated over the constraints of security as well as memory [35]. Additional two layers are business and processing.

3.2. *Edge computing*

Market of edge computing is forecasted with the increase of USD 87.3 billion from USD 36.5 billion in between the years 2021 to 2026 [36]. Pandemic period of COVID 19 increased the global adoption of technology for the large scale sized organizations as well as SME because of its cost effective. With enhanced data control, minimal costs and faster processing edge computing fetches computation and data storage under same roof once data is generated. It is expected that in the year 2025, 75% of enterprises will process data using edge computing [37]. Real time data processing, reduced data throughput and secured data are the major advantages of edge computing. Latency problems related with cloud methods are avoided. Local data processing is performed at edge gateways which ensure data evaluation. Cloud dependency is reduced with this decentralized data processing.

Edge computing is applicable in various areas such as automated vehicles, healthcare systems, security solutions, retail advertising, smart speakers and video conferences. Fig. 2 depicts the basic edge computing based

IoT architecture. Today edge computing has become an enhancement of cloud by incorporating various functions like data aggregation, local data storage, monitoring based on AI and Machine to Machine (M2M) communication. While applied edge computing to IoT environment, it is contained with three elements namely edge, edge device and edge gateway.

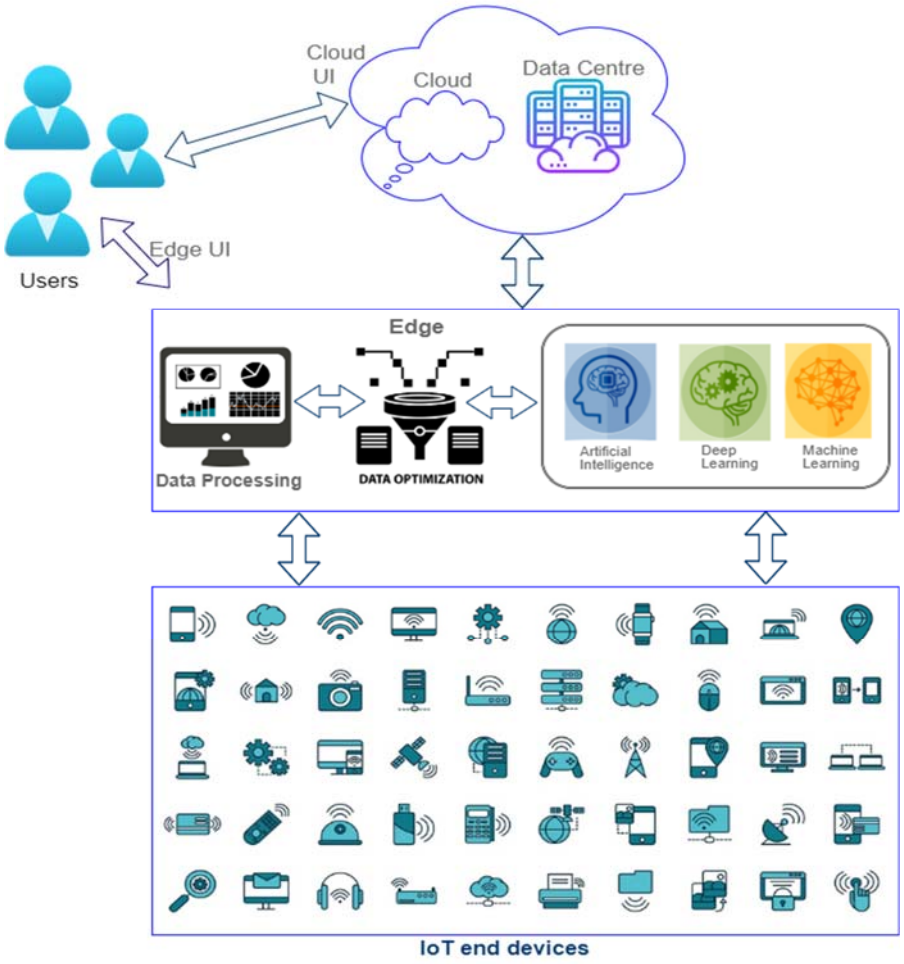

Fig. 2. Edge Computing based IoT Architecture

4. Proposed Framework – Edge AI Computing

Proposed security framework is divided into 4 phases which are feature extraction, edge computing, training and testing and validation. Proposed framework is portrayed in Fig. 3.

4.1. *Feature extraction*

Key processes of this first phase are data collection and data preprocessing. Input of this phase is dataset and output obtained is feature set. Network intrusion dataset UNSW-NB15 is utilized which is comprised with nine various recent attacks such as analysis, exploits, worms, backdoors, Denial of Service (DoS), shell code, reconnaissance, generic and fuzzers [38]. This dataset contains 49 features and it is divided into five main categories based on flow, content, basic, time and additional. The main features of the dataset are IP addresses, port number, attributes of TCP/IP and HTTP, network's time attributes, general purpose and connection features. UNSW-NB15 dataset overcomes the drawbacks of KDDCUP 99 and NSLKDD datasets and it seems better than them while considering number of attacks which is 4 types (DoS, PRB, U2R, R2L) only.

During data pre-processing, size of UNSW-NB15 dataset is minimized by removing the repeated data. Clustering method is helpful for discovering the similarities of behaviour among various types of dataset. Foremost, labels of dataset are eliminated. Cluster's quality and its required count is obtained by applying Silhouette coefficient and k-mean cluster algorithm is incorporated to manage cluster configurations. Testing is performed by making use of random data.

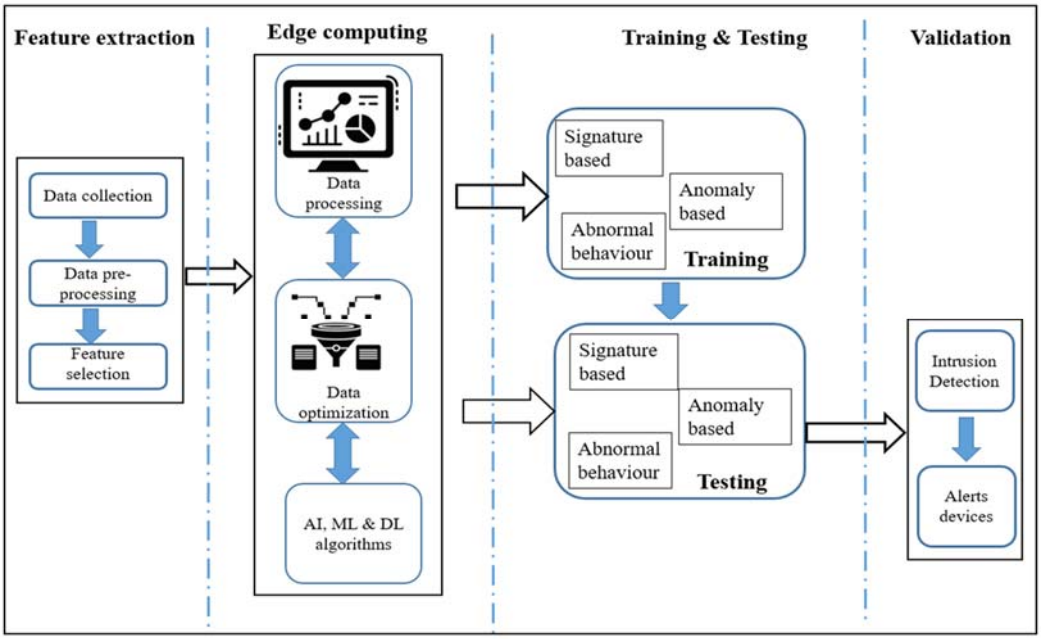

Fig. 3. Proposed Framework

In feature selection process, features of dataset are chosen by computing the value of Information Gain (IG). IG value defines the significancy of feature from the collected dataset. If the value is high, then it is considered that significance of that feature also high among others. IG is computed as follows

$IG(S, A) = H(S) – H(S|A)$

where IG(S, A) refers dataset information and S refers to the random variable, H(S) defines the dataset entropy (purity of dataset) before the occurrences of some change and H(S|A) states the dataset's conditional entropy while taking input variable A. Conditional entropy is computed by dividing dataset into clusters in every value observed.

$H(S|A) = \text{sum v in a } SA(v)/S * H(SA(v))$

where SA(v)/S defines the ratio of examples count of dataset with variable A which is valued v. H(SA(v)) defines entropy of sample cluster with variable A which is valued v. Based on the IG value, feature set is defined and forwarded for further phases.

4.2. *Edge computing*

In this proposed framework edge computing phase is divided into three parts which are data processing, data optimization and AI, ML and DL based algorithms selection. Feature set is considered as input for this phase. Further, data is optimized in this phase for improving better accuracy in intrusion detection. In this phase, data breach related attacks are avoided by choosing appropriate algorithms related to AI, ML and DL. Fig. 4 shows the experimental setup used in this research.

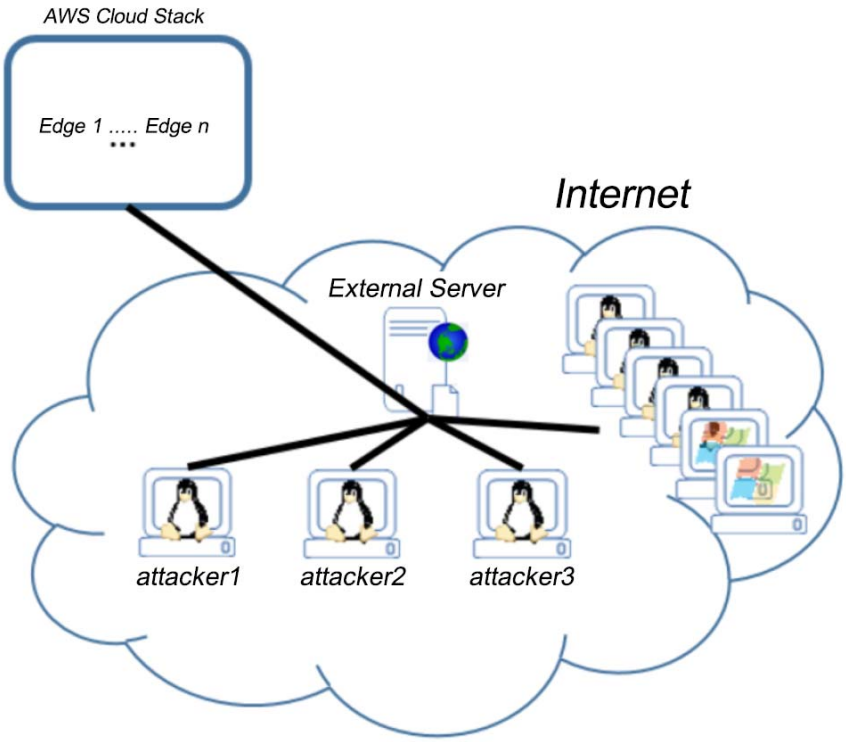

Fig. 4. Experimental Setup

5. Results

5.1. *Training and Testing*

UNSW-NB15 is utilized for both training and testing processes which is set of core network packets. For training 175,341 records are utilized while for testing 82,332 records are used in terms of various types of attack and normal types. Almost 70% of data samples are used for training phase and the balance 30% of data samples are utilized for testing phase.

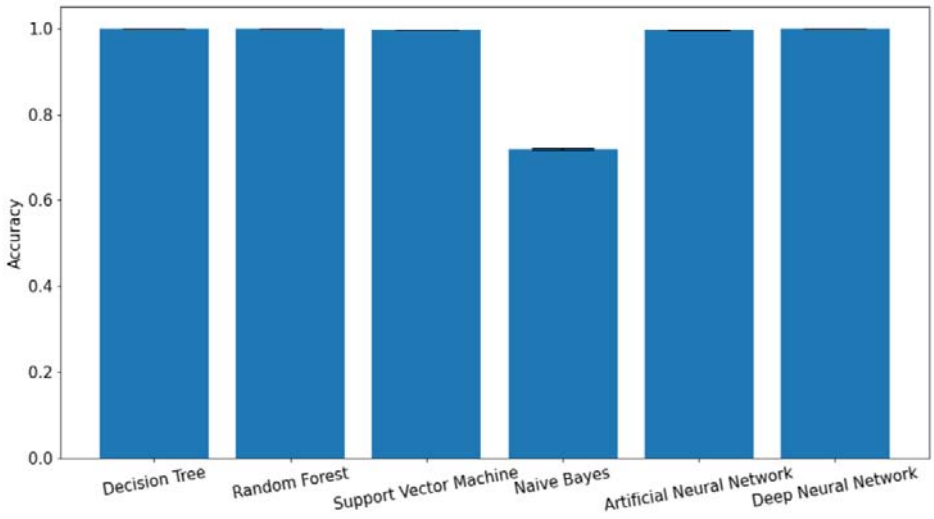

Fig. 5. Performance Results – Accuracy

Training and testing phase utilize the optimized feature set after edge computing phase as input set. Both training and testing are implemented based on signatures, anomalies and abnormal behaviours respectively. Attack signatures are meant by malicious patterns which are obtained by continuously monitoring inbound and outbound network traffic. Indicators of Compromise (IoCs) are utilized for signatures related to attack behaviours, recognized byte sequences and file hashes. There are various shortcomings regarding to signatures which are lack in the detection of unknown attacks. Encrypted traffic and altered attack pattern may also unable to detect while using signatures. To overcome those limitations in this proposed framework, anomalies and abnormal behaviours are also taken for training and testing additionally.

Anomalies are applied for training phase to test behavioural patterns in abnormal manner. Naïve Bayes classifier model is utilized for recovering from the limitations of signatures. Mainly, it is used for detecting unknown attacks. Naïve Bayes is probabilistic model which is familiar for classification. Bayes theorem is the root of Naïve Bayes classifier model which is also utilized. Fig. 5 to Fig. 8 shows the performance results of the given dataset.

```
------------------------ Decision Tree ------------------------
Accuracy: [0.9994506  0.99927062 0.99937482 0.99944112 0.99947901]
mean: 0.9994            std: 0.0001
------------------------ Random Forest ------------------------
Accuracy: [0.99947901 0.99939376 0.99948849 0.99955479 0.99950743]
mean: 0.9995            std: 0.0001
------------------------ Support Vector Machine ---------------------
Accuracy: [0.9961447  0.99604998 0.9962489  0.99560477 0.99543422]
mean: 0.9959            std: 0.0003
------------------------ Naive Bayes ------------------------
Accuracy: [0.72010723 0.71536152 0.72096922 0.72336576 0.71898681]
mean: 0.7198            std: 0.0026
------------------------ Artificial Neural Network ------------------
Accuracy: [0.9953206  0.99603103 0.99587    0.99562372 0.99524477]
mean: 0.9956            std: 0.0003
------------------------ Deep Neural Network ------------------------
Accuracy: [0.99842757 0.9983139  0.99826654 0.99867385 0.99856017]
mean: 0.9984            std: 0.0002
```

Fig. 6. Performance Results – Standard Deviation and Mean

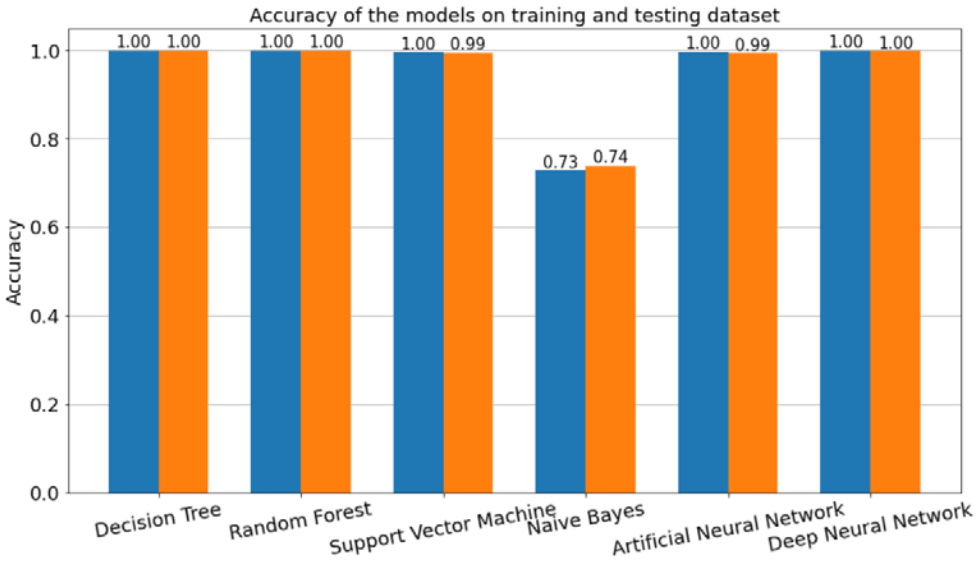

Fig. 7. Accuracy - Training and Testing

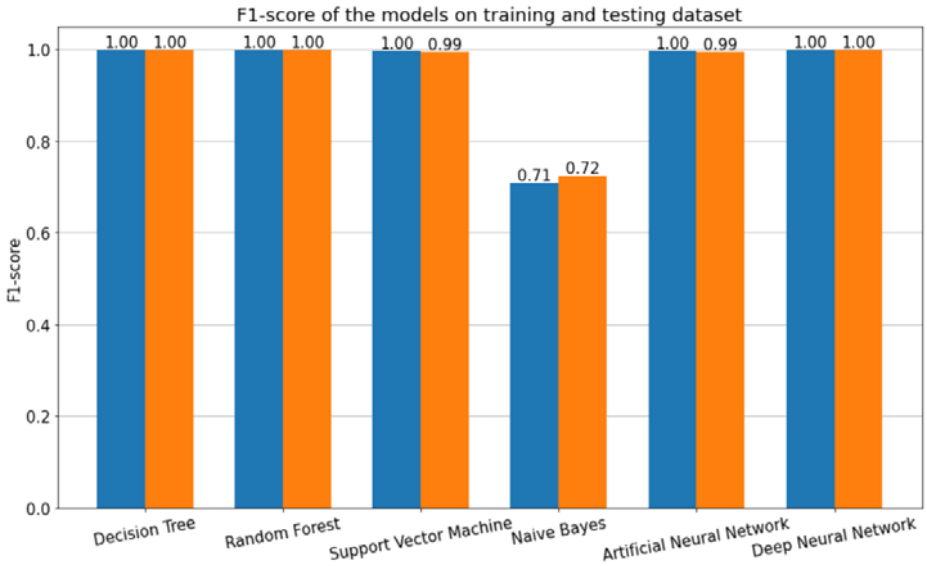

Fig. 8. F1 Score - Training and Testing

Similarly to enhance the detection accuracy, abnormal behaviours of network traffic is also monitored and analyzed other than signatures and anomalies. For observing and analyzing abnormal behaviours in both training and testing phases, AdaBoost M2 algorithm is utilized. For multi-class classification solutions, AdaBoost M1 and AdaBoost M2 models are utilized. AdaBoost M2 overcomes the shortcomings related to the maximized classification errors of AdaBoost M1.

5.2. *Validation*

It is the final phase of proposed framework which discovers intrusion and alert end devices based on the comprehensive processing of previous phases. All types of intrusions are analyzed from UNSW-NB15 dataset. Fig. 7 and Fig. 8 show the experimental results in terms of performance measure such as accuracy and F1-score.

6. Conclusion

This research paper proposes an IoT intrusion detection framework by adopting Artificial Intelligence and Edge Computing technologies. It mainly concentrated on issues of data breaches and information in security because of slower data processing. It aims for effective threat detection by maintaining the integrity of security essentials in between IoT applications and its IoT ecosystem. Quality of Service is improved by decreasing latency of IoT communication. Proposed framework's automated feature helps in the avoidance of manual intervention errors. It is light weighted and combat against data obfuscation techniques of intruders with the implementation of AI's privacy preserving techniques. Experimental results provide better results than earlier approaches which imply effective and efficient IoT threat detection.

Conflicts of Interest: The authors have no conflicts of interest to declare

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications", IEEE Internet of Things (IoT) Journal, 4, no. 5, 1125-1142, 2017.
[2] https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/
[3] K. Sha, W. Wei, A. Yang, W. Shi, "Security in internet of things: opportunities and challenges", In Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016), 2016.
[4] K. Sha, et al., "On security challenges and open issues in internet of things", Future Gener. Comput. Syst. 83 (2018) 326–337.
[5] S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi, "Intrusion Detection System to detect Wireless attacks in IEEE 802.11 networks", IET networks, July 2019, Volume 8, Issue 4, pp. 219- 232, IET.
[6] S. Chen, P. Zeng, K.R. Choo, X. Dong, "Efficient ring signature and group signature schemes based on q-ary identification protocols", Comput. J. 61 (4) (2018) 545–560.
[7] M. Alramadhan, K. Sha, "An overview of access control mechanisms for internet of things", In Proceedings of the 26th International Conference on Computer Communications and Networks (ICCCN 2017), 2017.
[8] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, "Edge computing: vision and challenges", IEEE Internet. Things J. 3 (5) (2016) 637–646.
[9] S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi, "A Survey on malware analysis and mitigation techniques", Computer Science Review, May 2019, Elsevier, (SCIE).
[10] R. Errabelly, K. Sha, W. Wei, T.A. Yang, Z. Wang, "Edgesec: design of an edge layer security service to enhance internet of things security", In Proceedings of the First IEEE International Conference on Fog and Edge Computing (ICFEC 2017), 2017.
[11] X. Tao, K. Ota, M. Dong, H. Qi, K. Li, "Performance guaranteed computation offloading for mobile-edge cloud computing", IEEE Wireless Commun. Lett. 6 (6) (2017) 774–777.

[12] D. Arivudainambi, K.A. Varun Kumar, S. Sibi Chakkaravarthy, P. Visu, "Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance", Computer Communications, Vol.147, November, 2019, pp.50-57, Elsevier.
[13] R. Hsu, J. Lee, T. Quek, J. Chen, "Reconfigurable security: edge-computing-based framework for IoT", IEEE Network, 32 (5), (2018), 92–99.
[14] H. Hu, W. Han, G. Ahn, Z. Zhao, "Flowguard: building robust firewalls for software defined network", In Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, 2014.
[15] H. Haddadi, V. Christophides, R. Teixeira, K. Cho, S. Suzuki, A. Perrig, "Siotome: an edge-isp collaborative architecture for IoT security", In Proceedings of 1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), 2018.
[16] R. Roman, R. Rios, J. Onieva, J. Lopez, "Immune system for the internet of things using edge technologies", IEEE Internet of Things Journal (2018) 1–8.
[17] R. Lu, K. Heung, A. Lashkari, A.A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," IEEE Access 5 (2017) 3302–3312.
[18] Z. Ali, M.S. Hossain, G. Muhammad, I. Ullah, H. Abachi, A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates", Future Gener. Comput. Syst. 85 (2018) 76–87.
[19] M. Du, et al., "Big data privacy preserving in multi-access edge computing for heterogeneous internet of things", IEEE Commun. Mag. 56 (8) (2018) 62–67.
[20] Arrington, B., Barnett, L. Rufus, R. and Esterline, A. (2016), "Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms", 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, 2016, pp. 1-6.
[21] Karsligil, M.E., Yavuz, A.G., Guvensan, M.A., Hanifi, K., Bank, H. (2017). "Network intrusion detection using machine learning anomaly detection algorithms", 25th Signal Processing and Communications Applications Conference (SIU), IEEE (2017), 10.1109/siu.2017.7960616.
[22] S. Sibi Chakkaravarthy, V. Vaidehi and Steven Walczak, "Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles", Journal of Medical Systems, Vol.44, Article 29, Springer, 2020.
[23] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H, Park, "DistBlockNet: A distributed blockchains-based secure SDN Architecture for IoT networks", IEEE Commun. Mag. 55 (9) (2017) 78–85.
[24] Kabir, E., Hu, j., Wang, H., Zhuo, G. (2018), "A novel statistical technique for intrusion detection systems", Future Generation Computer Systems. Vol.79, Issue 1, pp. 303-318.
[25] R. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices", 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, 2018, pp. 29-35. doi: 10.1109/SPW.2018.00013
[26] Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multiagent system-enriched IDS for securing IoT against DDoS attacks", J. Supercomput., vol. 7, no. 10, pp. 5156–5170, 2018.
[27] Ahmed, S., Rajput, A, "Threats to patients privacy in smart healthcare environment", In Lytras, M., et al. (eds.) Innovation in Health Informatics: A Smart Healthcare Primer. Elsevier, Ams-terdam, The Netherlands (2019).
[28] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract", IEEE Access, vol. 7, pp. 98893–98907, 2019.
[29] Shafi Q., Qaisar S., Basit A. (2019) "Software Defined Machine Learning Based Anomaly Detection in Fog Based IoT Network", In Misra S. et al. (eds) Computational Science and Its Applications – ICCSA 2019. ICCSA 2019. Lecture Notes in Computer Science, vol 11622. Springer.
[30] D. Sangeetha, S. Sibi Chakkaravarthy, Suresh Chandra Satapathy, Vaidehi V, Meenaloshini Vimal Cruz, "Multi Keyword Searchable Attribute Based Encryption for efficient retrieval of Health Records in Cloud", Multimedia Tools and Applications, Springer, 2021.
[31] Nguyen, T. G., Phan, T. V., Nguyen, B. T., So-In, C., Baig, Z. A., & Sanguanpong, S. (2019). "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks", IEEE access, 7, 107678-107694.
[32] Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", Journal of Network and Computer Applications, Volume 143, 2019, Pages 167-177, ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2019.06.019.
[33] Y. Yang, J. Wanf, B. Zhai and J. Liu (2019), "IoT-Based DDoS Attack Detection and Mitigation Using the Edge of SDN", Cybersapce Safety and Security, 11th International Symposium, CSS 2019 Guangzhou, China, December 1–3, 2019.
[34] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, N. Kumar, and J. J. P. C. Rodrigues, "RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment", International Journal of Communication Systems, 2019, https://doi.org/10.1002/dac.4024
[35] Singh, A., Chatterjee, K. & Satapathy, S.C. "An edge based hybrid intrusion detection framework for mobile edge computing", Complex Intell. Syst. (2021). https://doi.org/10.1007/s40747-021-00498-4
[36] Jabraeil Jamali M.A., Bahrami B., Heidari A., Allahverdizadeh P.,Norouzi F. (2020) "IoT Architecture", Towards the Internet of Things. EAI/Springer Innovations in Communication and Computing. Springer, Cham
[37] Burhan,M., Rehman, R.A., Khan, B. and Kim, BS.,(2018). "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey", Sensors 2018, 18, 2796; doi:10.3390/s18092796
[38] S. Sibi Chakkaravarthy, Pranav Kompally, Saraju P Mohanty and Uma Chopalli, "MyWear: A Novel Smart Garment for Automatic Continuous Vital Monitoring", IEEE Transactions on Consumer Electronics, IEEE, Vol. 67, No. 3, pp. 214-222, 2021.
[39] Cannaday, B., (2019). "The Fundamental IoT Architecture", Available at: https://www.losant.com/blog/the-fundamental-iot-architecture [Accessed on 3rd March 2020]
[40] Darwish, D, "Improved Layered Architecture for Internet of Things", Int. J. Comput. Acad. Res. (IJCAR) 2015, 4, 214–223.
[41] Sethi, P., Sarangi, S.R. (2017), "Internet of Things: Architectures, Protocols, and Applications", J. Electr. Comput. Eng. 2017.
[42] https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=133384090&utm_source=Email&utm_medium=Acoustic_ICT_APAC&utm_campaign=Acoustic_Edge_Computing_Market_03_Nov_2021
[43] https://www.ibm.com/in-en/cloud/edge-computing?utm_content=SRCWW&p1=Search&p4=43700055270654453&p5=b&gclid=EAIaIQobChMIx7Oz856D9AIV3ZlmAh2u3AiSEAAYASAAEgK7JvD_BwE&gclsrc=aw.ds
[44] Moustafa, Nour, and Jill Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set", Information Security Journal: A Global Perspective 25, no. 1-3 (2016): 18-31.

Authors Profile

Ms. V.S. Saranya is Research scholar in Department of Computer Science and Engineering, Annamalai University. She is currently doing her research in A Secured Framework for Enhanced and Efficient communication in IoT Ecosystem in Computer Science, Annamalai University since 2018. Her research interest includes Cloud Computing and IoT.

Dr. G. Ramachandran is an Associate Professor in Department of Computer Science and Engineering, Annamalai University with over 21 years of experience. He completed Ph.D degree in Computer Science and Engineering in the year 2014. He published several papers in international conferences and journals. His research interest includes Computer Networks, Network Security, Distributed Computing, Mobile Ad hoc Networks and Big Data.

Dr. S. Chakaravarthi is Professor in Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai with over 22 years of experience. He completed Ph.D. degree in Computer Science and Engineering in the year 2015. He published several papers in international conferences and journals. His research interest includes Computer Networks, Network Security, Distributed Computing, Machine Learning, Data Science.