Journal of Harbin Engineering University Vol 45 No. 7
ISSN: 1006-7043 July 2024

Securing the Future of Hyper-Connected World : Mitigating Risks in 5G-Enabled Iot Environment

Shahid Amir[1], Rajni Mishra[2]
[1]Research Scholar, Chandigarh University, Gharuan, Mohali
[2]Assistant Professor, Chandigarh University, Gharuan, Mohali

Abstract
A network is a collection of interconnected devices, such as computers and organizations, that are used to exchange data with one another. It is defined as pairings of computers that have been used to share data or services via the web in computer language. There are two different kinds of networks: wireless and wired. In this protocol, the route—also known as the routing zone—is kept up within a small area. Multicasting is the foundation of this research project's path creation from source to destination. The RPL routing protocol uses the multicasting approach to construct a path from the source to the destination. After being implemented in NS2, the suggested strategy outperforms the current technique in simulation findings.
Keywords: *RPL, IoT, Multicasting.*

Introduction

The countless millions of connected gadgets that surround us are collectively referred to as the Internet of Things (IoT). In 1999, Kevin Ashton coined the phrase “Internet of Things” while working at Procter & Gamble on supply chain improvement [1]. Over the past 20 years, the term has expanded to cover a variety of uses across industries like utilities, farming, healthcare, and transportation. Although the term's definition has evolved, its core intent—to boost productivity and deliver information more rapidly than systems based on human interaction—remains unchanged. IoT devices continuously collect a range of personal data from us, including our contact list, schedule, history of browsing, position, and health information. The main drivers for gathering this delicate information are suitability and improving our lives through smart technology. As technology evolves, so do its responses to our daily needs [2]. For example, some devices can automatically turn off lights at a set time, detect emergencies like fires, or alert us to security breaches. However, these conveniences also bring considerable dangers to security. IoT-connected smart gadgets hold extremely confidential and intimate data, making it vulnerable to illegal access. This can pose considerable risks to user safety and well-being. For example, a hacker could gain access to home security cameras, compromising our privacy, or take control of autonomous vehicles, possibly endangering the driver severely [3].

The vast array of IoT devices presents serious security and privacy concerns. To meet user expectations, new IoT devices must have systems that ensure secure and private communication. If personal data isn't protected, users might avoid these devices. IoT networks face challenges like storage, data processing speed, privacy, and authentication. Additionally, IoT devices often lack the necessary security software and are generally simplistic [4], which opens the door to cyberattacks. It is crucial to explore new ways to improve IoT security as technology advances. One major risk to Internet of Things devices is distributed DDoS (distributed denial of service) assaults. These attacks flood a target with excessive traffic, aiming to disrupt servers, services, or online networks [5]. IoT devices typically lack robust security systems, and manufacturers often build low-cost systems with weak security, including hard-coded login credentials that hackers can easily crack [5]. Hackers aim to compromise thousands of IoT devices to create botnets or zombie armies for large-scale attacks. Even the most secure services can be overwhelmed by a DDoS attack using a large botnet. A notable example is the Mirai botnet attack, which demonstrated how IoT devices can be exploited to launch a massive DDoS attack, emphasizing the urgent need to strengthen IoT security.

The physical layer, network layer, and application layer are the three levels that make up an Internet of Things application [6]. Because each layer depends

on a different set of technologies, they can be attacked via Distributed Denial of Service (DDoS) attacks and other security risks. The physical layer, sometimes referred to as the perception layer, is made up of data sensors such as barcodes, RFIDs, and gateways. Its main responsibility is gathering environmental data and sending it to the network layer for additional processing. The data must be transferred from the physical layer to a data processing source via a network by the network layer. Lastly, users can communicate with the system through the application layer, which serves as an interface between them and the network layer. Given the diversity and extensive interconnectivity of IoT devices, ensuring their security is a significant challenge [7]. Potential attackers can exploit vulnerabilities at different layers, whether by manipulating physical components, interfering with network protocols, or initiating encryption assaults to obtain unapproved entry to gadgets. As a result, physical layer assaults, network layer attacks, and application layer attacks are the three general categories into which IoT attacks fall. Application layer attacks use malware, trojans, or viruses to infect user-facing programs, network layer attacks target the network infrastructure, and physical layer attacks involve tampering with hardware. An illustration of the different kinds of attacks associated with each layer in IoT networks can be found in Figure 1 [8].

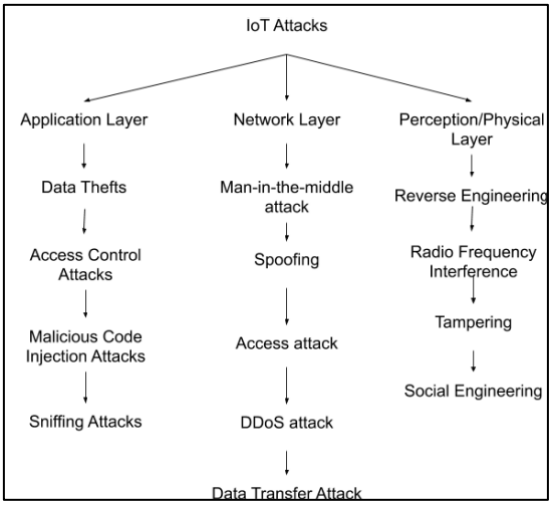


Fig 1: IoT security attacks by layer

1. Physical Layer Attack

Physical intrusions concentrate on physical devices in an effort to find new weaknesses within IoT systems. Reverse engineering, radio frequency interference, manipulation, and social engineering are some of the methods used in these attacks [9].

- Reverse Engineering: This technique involves an attacker methodically disassembling a device to discover susceptibilities. An intruder can identify known and novel weaknesses by dissecting its parts. They could then use these flaws to compromise other connected devices on a single network.
- Radio Frequency Interference: This kind of assault causes connectivity problems by utilizing a device to interfere with the radio frequency signals of IoT devices. The vulnerable device may experience RF interference and jamming while the intruder is in close proximity to it. [10].
- Tampering: This involves the physical alteration of an IoT device. By tampering with a device, the attacker may obtain confidential data, including encryption keys or login details.
- Social Engineering: This approach relies on manipulating end users to extract confidential information, often through deceptive interactions or misleading communications.

2. Network Layer Attacks

IoT devices use the network at the network layer to send data that they obtained from the physical layer to a server or other device for processing. The network layer has discovered the subsequent assaults and dangers to security. [11]:

Man in the Middle Attack: An IoT network node's data can be intercepted and modified by an attack known as man-in-the-middle. Any node in the network has the ability to intercept and read the contents of data packets that are not being

transmitted between devices. This assault aims to alter data on the Internet of Things network and cause traffic disruptions. Owing to their widespread presence in unprotected networks, open devices may act as possible sites of entry for these intrusions.

- Spoofing: In IoT, data is routed through network traffic utilizing IP addresses and encryption. Via transport protocols, an intruder can copy, modify, or reissue IP addresses, disrupting network traffic [12]. In Internet of Things networks, spoofing incidents can be carried out by a hacker using fictitious routing nodes, transmission pathways, and error signals.
- Access Attack: When a third party enters an IoT network and stays hidden for a long time, it's known as an access attack. The goal is to stealthily obtain highly confidential and susceptible data that could endanger the user and the Internet of Things network. IoT devices are particularly vulnerable to this kind of attack since they often send and receive important data [13].
- DDoS Attack: The incident occurs when a hacker floods a particular server with excessive bandwidth, causing the server to crash and preventing customers from accessing it. Although DDoS assaults are not unique to Internet of Things devices and applications, a lot of IOT devices are configured poorly, which makes them easy targets for attackers looking to expand their botnet armies. Notably, the Mirai botnet's intrusion took advantage of poorly setup Internet of Things devices.
- Data Transfer Attack: A large amount of data is transferred between sensors, servers, the cloud, and apps in IoT applications [14]. IoT applications are particularly vulnerable to attacks because of this intricate data flow that makes use of several technologies. Hackers may take advantage of the weaknesses that are created by the many paths that data takes inside IoT systems.

3. Application Layer Attack

Attacks using software are used to penetrate the application layer of IoT devices with the goal of obtaining sensitive information. These attacks target the data within this layer and can take several forms, including:

- Code and Database Injection Attacks: These occur when attackers identify vulnerable entry points to inject malicious code into IoT systems [15]. By using scripting techniques, harmful code is introduced into trusted sites or databases. This can give attackers unauthorized control over IoT accounts, potentially compromising the whole IoT network.
- Theft of Data: A large portion of the important data processed by IoT devices is actively communicated. Attacks via the internet are more likely to occur with data in transit than with fixed information. This heightened vulnerability can lead users to hesitate in entering private information into IoT devices, knowing that their data could be compromised.
- Sniffing Attacks: A malicious program is used in such assaults to track traffic on IoT networks. Data traveling across the network can be intercepted and accessed by attackers [16]. When secure data transmission protocols are lacking, this kind of assault is particularly successful, leaving IoT networks open to illegal listening in and breach of information.
- Phishing Attacks: These assaults trick people into opening what seem to be authentic messages, clicking on links in emails, or visiting unauthorized websites. Usually, links leading to harmful content—like malware or forms asking for personal information—are tricked users into clicking on them. The attacker then illegally collects this information.

Literature Survey

A. Arshad, et.al (2023) developed a system to detect botnet attacks [17]. An ensemble learning (EL) system was designed for detecting botnets attacks in network traffic. The system was emphasized on analyzing traffic and recognizing any suspected behavior which indicated that the botnet was present. A CTU-13 dataset was executed for developing and comparing the ML and DL based solutions. A new ensemble method (KDR) of k nearest neighbor, decision tree and random forest, was presented for detecting botnet attack precisely. The trial findings demonstrated that the presented solution yielded an accuracy of 99.7% in 12.99s. Hyperparameters were optimized to validate the performance. The suggested approach produced a workable solution to protect IoT nodes from botnet intrusions and was shown to be resilient against them.

A. Nazir, et.al (2024) presented a new Hybrid CNN-LSTM model to detect threats accurately and efficiently in IoT [18]. This model tackled the drawbacks of traditional techniques and made the IoT ecosystems more secure. The data taken from various datasets, like CICIDS2017, IoT-23, N-BaIoT,

was employed for computing the presented model. Fourteen kinds of attacks were considered for evaluating and testing this model. This model was worked robustly due to its potentials of detecting threats. For this, the security data was captured and analyzed in a successful way. The simulation depicted that the presented model offered an accuracy of 95% accuracy on initial dataset and 99% on last 2 datasets. Moreover, this model was effective for detecting IoT threats. In the end, the Principal Component Analysis (PCA) was projected for optimizing the data processing and utilizing the advanced optimization methods such as to quantize and prune the system and make the system applicable in resource-constrained IoT settings.

M. F. Saiyed, et.al (2024) suggested a new lightweight system called GADAD to detect higher- and lower-volume Distributed Denial of Service (DDoS) assaults in IoT networks [19]. Initially, a HL-IoT (High- and Low-volume intrusions in IoT) dataset was generated and processed in which DDoS assaults were comprised. Subsequently, a new and lightweight technique known as GAStats of GA and statistical parameters (Stats.) was adopted to select features. Eventually, the generated and the ToN-IoT datasets were applied to train 3 tree-based ML algorithms, namely RF, ET (Extra-Tree), and AdaBoost, with other algorithms concerning four universal performance indicators. The experiments indicated that the suggested system was efficient to find DDoS assaults in IoT framework mitigating the computation time as opposed to classic approaches.

S. A. Bakhsh, et.al (2023) introduced a deep learning-based method in which FFNN (Feed Forward Neural Networks), LSTM (Long Short-Term Memory), and RandNN (Random Neural Networks) algorithms were deployed for protecting IoT networks from cyberattacks [20]. The first algorithm was implemented for handling complex IoT network traffic patterns, and the latter one was effective to capture long-term dependances available in the flowing traffic. The last algorithm was emphasized on its potential to learn data for adapting and learning from network data. These algorithms utilized the defense methods against cyber-attacks and ensured that the sensitive data was secure. On CIC-IoT22 dataset, the results confirmed the supremacy of introduced method over traditional methods. This method provided an accuracy of 99.93% with first algorithm, 99.85% with second and 96.42% with last algorithm to detect intrusion.

A. B. F. Khan, et.al (2023) developed a new method for detecting reactive DDoS incidents in IoT scenario [21]. These attacks were prevented and mitigated for improving the security. The dynamic frequency hopping (DFH) system was exploited to actually change the framework□s operating frequency, and make the attacker incapable of interfering in system. The developed method was evaluated on NS with regard to loss, and computational time. The experimental results exhibited that the developed method was robust for diminishing the influence of reactive DDoS incidents around 95% at lower overhead. In addition, this method was proved effective to improve security in IoT systems against reactive assaults.

M. Aljebreen, et.al (2023) projected a novel approach named DDAD-SOEL to detect DDOS incidents in IoT platform [22]. This method was emphasized on recognizing DDoS attacks efficiently and automatically. The SO algorithm was adopted to select feature subset. After that, an ensemble of 3 DL methods: LSTM, BiLSTM, and DBN was put forward. In the end, the Adadelta optimizer (AO) was utilized to tune the parameters DL algorithms. The benchmark database was applied for simulating the projected method in terms of diverse parameters. The experimental results revealed that the projected method offered 99.81% accuracy to detect attacks. The applicability of this method was proved in diverse IoT deployments in several domains, such as medical, transportation, and smart cities.

Y. Alhasawi, et.al (2024) presented FL-DAD, a Federated Learning approach for identifying DDoS incidents. In this work, Convolutional Neural Networks (CNN) was adopted for recognizing DDoS incidents in an effectual way [23]. This approach was aimed at prioritizing data privacy when the data was processed at local level, the necessity to gather central data was avoided and efficacy to detect attacks was improved. This approach led to underline the efficiency to decentralize the learning procedure, which ensured the data privacy without any degradation of accuracy. The CICIDS2017 dataset was executed for simulating the presented approach. In results, the presented approach was proved robust for detecting attacks in huge-scale IoT

networks and balanced the data security with analytical efficiency.

F. Alasmary, et.al (2022) formulated an effectual solution for defending IoT devices against various unavoidable assaults [24]. Two models, namely IoT node detector and a server detector were implemented. The initial one was a lightweight classification algorithm which helped in monitoring egress traffic. The next was a precise algorithm which the IoT node employed for determining whether it was suspicious of a contributor to a DDoS attack. This algorithm was developed on the basis of formulated method called ShieldRNN for RNN/LSTM methods. The CIC-IDS2017 dataset was applied for computing the formulated method against traditional technique. The simulation exhibited the supremacy of formulated method to detect DDoS.

F. Alrowais, et.al (2023) devised a BNT-CBPOADL) method to detect attacks in IoT situations [25]. This method was focused on precisely detecting and classifying botnet assaults in IoT environment. The data was pre-processed using Z-score normalization. Moreover, the CBPOA method was utilized to select features and convolutional variational autoencoder (CVAE) technique to detect botnet. Finally, the arithmetical optimization algorithm (AOA) was utilized to tune hyperparameter of the CVAE algorithm. The Bot-IoT dataset was employed in experimentation. The results validated that the devised method was performed well in contrast to conventional methods and detected the botnet attacks at an accuracy of 99.50%.

X. Zhou, et.al (2022) suggested a new HAA (hierarchical adversarial attack) generation technique for providing a LBDA (level-aware black-box adversarial attack) method in which a graph neural network (GNN)-based method was utilized to detect intrusions in a restricted budget [26]. An intelligent technique based on the Shadow GNN algorithm saliency map methodology was designed to generate adversarial cases when the important feature components were identified and altered at smaller perturbations. Based on random walk with restart (RWR), a hierarchical node selection (HNS) method was created to choose a subset of more attack-prone nodes at a higher attack priority based on their structural characteristics and overall loss fluctuations in Internet of Things networks. The recommended method was simulated using the UNSW-SOSR2019 dataset. The outcomes validated the superiority of suggested technique over others in IoT scenarios.

Research Methodology

When establishing a path between two endpoints (S to D), the RPL routing protocol leverages broadcasting. The RPL routing protocol's broadcasting nature accounts for the network's extremely high bandwidth and long path establishment latency. The multicasting technique will be suggested in this research effort for the path creation between two endpoints. The trust mechanism for path building between two endpoints will serve as the foundation for the multicasting approach. The multicasting strategy will lower network latency and bandwidth usage. The trust of every network node will be determined when using the trust-based routing methodology. The number of packets delivered by any sensor node determines how trustworthy every single node in the network is. The cluster head node is the one that forwards the most packets throughout the network. The cluster head node is in charge of establishing the path to the target and receiving route request messages. There will be a predefined path with a minimum hop count and a maximum sequence number from the source to the destination. The number of packets transmitted by any sensor node in the network will be used to determine each node's level of trust. The node with the highest trust in the network was the one that forwarded the most packets. The trust establishes the sensor node's dependability. Data transmission will occur via the most dependable sensor node along the node path between two end points.

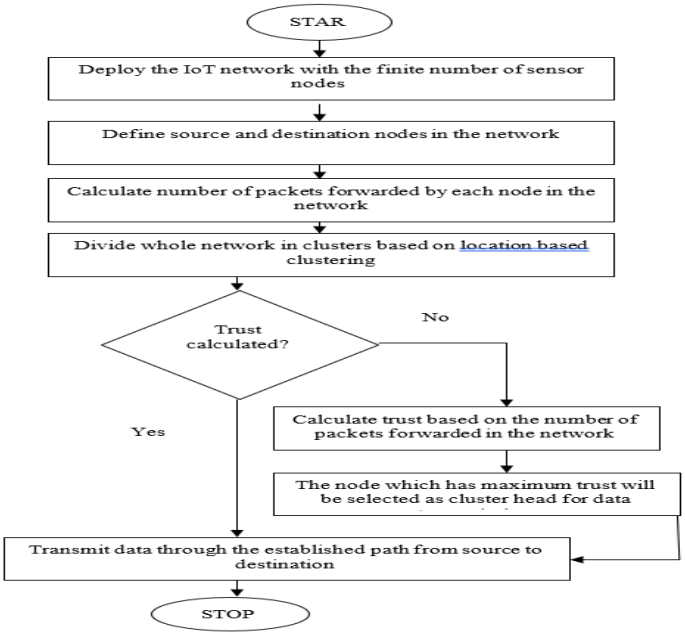


Fig 2: Proposed Flowchart

Result And Discussion

A simulation software will be utilized to mimic the actual moving characteristics of the nodes in a mobile ad hoc network. A predetermined number of randomly dispersed nodes with a predetermined number of links in a predetermined location will be used for the evaluation. We utilized Network Simulator 2 to put this suggested method into practice.

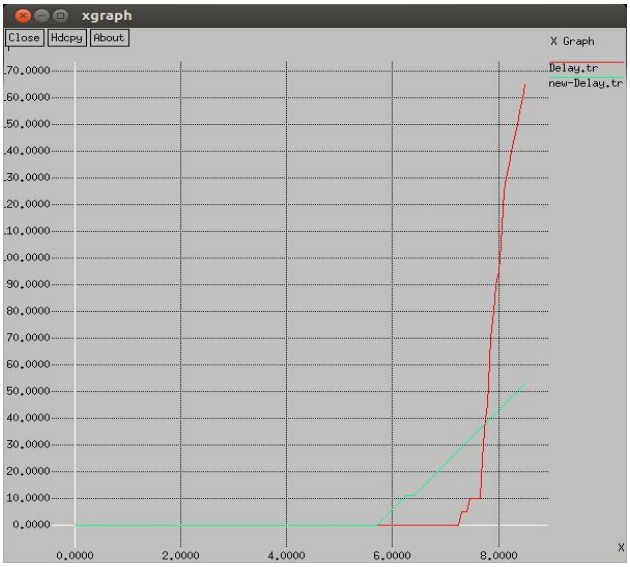
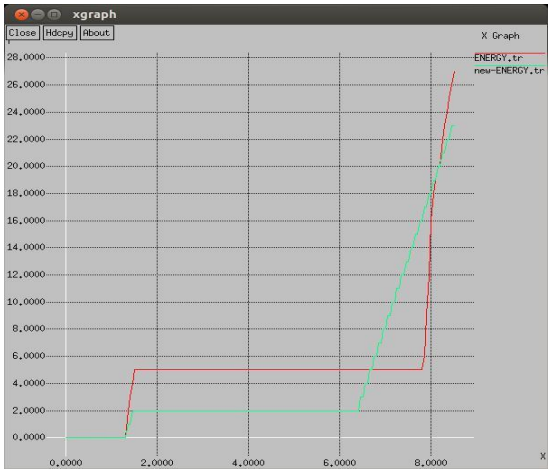


Fig 3: Delay Comparison

The recommended and existent techniques' delays are evaluated for effectiveness analysis, as illustrated in figure 3. Analyses show that the suggested approach has a lower delay than the current approach.



No of nodes	22
Routing protocol	ZRP
Antenna type	Omi directional
Standard	802.11
Queue	Priqueue
Packet size	1000
Interval	0.05 m second
No of packets in queue	50

Fig. 4. Energy Consumption Comparison

Figure 4 depicts a comparison between the proposed and existing techniques based on the consumed energy. comparing the suggested approach to the other, the former consumes less energy.

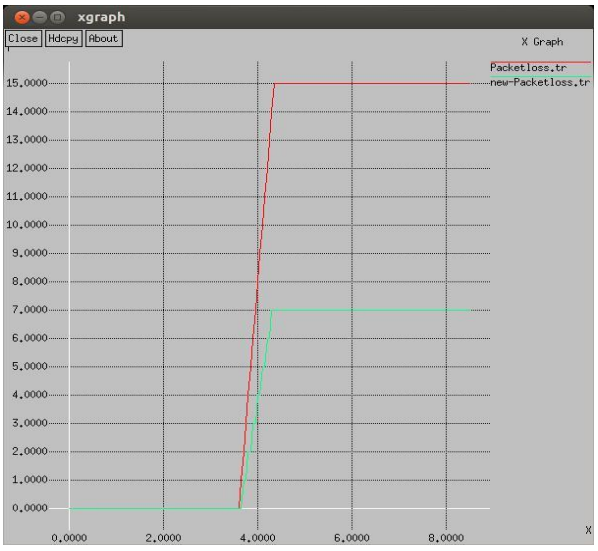


Fig. 5. Packet loss Comparison

Figure 5 compares the proposed technique's package loss with the existing approach. Comparing the suggested method to the existing approach, there is less packet loss.

Conclusion

It is a kind of hybrid routing technique where nodes are localized within smaller networks. This protocol integrates the benefits of proactive and on-demand routing systems. In each zone, proactive routing is used to facilitate faster neighbor communication. The inter-zone communication uses on-demand routing to cut down on pointless communication. The network is separated into different routing zones based on the distance between the mobile nodes. It has been determined that the broadcasting technique, which establishes the path from the source to the destination, increases bandwidth usage and delay. Multicasting is a technology used to build paths with the least amount of latency and usage of bandwidth.

References

[1] J. R. Elias, R. Chard, J. A. Libera, I. Foster and S. Chaudhuri, "The Manufacturing Data and Machine Learning Platform: Enabling Real-time Monitoring and Control of Scientific Experiments via IoT," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-2.

[2] S. S. Swarna Sugi and S. R. Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," 2020 3rd

International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1164-1167.

[3] M. Afroz, N. Hasan and M. I. A. Hossain, "IoT Based Two Way Safety Enabled Intelligent Stove with Age Verification Using Machine Learning," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-5.

[4] N. Karmous, M. O. -E. Aoueileyine, M. Abdelkader and N. Youssef, "IoT Real-Time Attacks Classification Framework Using Machine Learning," 2022 IEEE Ninth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2022, pp. 1-5.

[5] H. Pandey and S. Prabha, "Smart Health Monitoring System using IOT and Machine Learning Techniques," 2020 Sixth International Conference on Bio Signals, Images, and Instrumentation (ICBSII), Chennai, India, 2020, pp. 1-4.

[6] S. M. Shahriar, H. I. Peyal, M. Nahiduzzaman and M. A. H. Pramanik, "An IoT-Based Real-Time Intelligent Irrigation System using Machine Learning," 2021 13th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, 2021, pp. 277-281.

[7] U. Arul, A. A. Prasath, S. Mishra and J. Shirisha, "IoT and Machine Learning Technology based Smart Shopping System," 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 2022, pp. 1-3.

[8] V. T. Hayashi et al., "Improving IoT Module Testability with Test-Driven Development and Machine Learning," 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 2021, pp. 406-412.

[9] S. Kavitha, V. R. Karumanchi, T. S. Rajeswari, V. C. Jadala, S. H. Raju and M. Kavitha, "Machine Learning based Authentication of loT Devices in Traffic Prediction for ITS," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1530-1534.

[10] Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan and S. Khorsandroo, "Anomaly Detection on IoT Network Intrusion Using Machine Learning," 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2020, pp. 1-5.

[11] M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," in IEEE Access, vol. 8, pp. 114066-114077, 2020.

[12] H. Lee, S. Kim, D. Baek, D. Kim and D. Hwang, "Robust IoT Malware Detection and Classification Using Opcode Category Features on Machine Learning," in IEEE Access, vol. 11, pp. 18855-18867, 2023.

[13] W. Ma, X. Wang, M. Hu and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," in IEEE Access, vol. 9, pp. 65066-65077, 2021.

[14] T. Gaber, A. El-Ghamry and A. E. Hassanien, "Injection attack detection using machine learning for smart IoT applications", Physical Communication, vol. 173, no. 4, pp. 5363-5365, 16 March 2022.

[15] D. Mishra, B. Naik and S. Vimal, "Light gradient boosting machine with optimized hyperparameters for identification of malicious access in IoT network", Digital Communications and Networks, vol. 9, no. 1, pp. 125-137, 12 October 2022.

[16] R. Banavathu and S. Meruva, "Efficient secure data storage based on novel blockchain model over IoT-based smart computing systems", Measurement: Sensors, 10 March 2023.

[17] A. Arshad, M. Jabeen and H. Jia, "A novel ensemble method for enhancing Internet of Things device security against botnet attacks", Decision Analytics Journal, vol. 23, pp. 12-20, 23 August 2023.

[18] A. Nazir, J. He and M. S. Pathan, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem", Ain Shams Engineering Journal, vol. 13, pp. 45-53, 4 April 2024.

[19] M. F. Saiyed and I. Al-Anbagi, "A Genetic Algorithm- and t-Test-Based System for DDoS Attack Detection in IoT Networks," in IEEE Access, vol. 12, pp. 25623-25641, 2024.

[20] S. A. Bakhsh, M. A. Khan and J. Ahmad, "Enhancing IoT network security through deep learning-powered Intrusion Detection System",

Internet of Things, vol. 24, pp. 196-204, 13 September 2023.

[21] A. B. F. Khan, M. M. Hussain and M. A. Gunavathie, “DDoS attack modeling and resistance using trust-based protocol for the security of Internet of Things”, Journal of Engineering Research, vol. 11, no. 2 pp. 58-65, 1 April 2023.

[22] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama and M. A. Hamza, "Enhancing DDoS Attack Detection Using Snake Optimizer with Ensemble Learning on Internet of Things Environment," in IEEE Access, vol. 11, pp. 104745-104753, 2023.

[23] Y. Alhasawi and S. Alghamdi, "Federated Learning for Decentralized DDoS Attack Detection in IoT Networks," in IEEE Access, vol. 12, pp. 42357-42368, 2024.

[24] F. Alasmary, S. Alraddadi, S. Al-Ahmadi and J. Al-Muhtadi, "ShieldRNN: A Distributed Flow-Based DDoS Detection Solution for IoT Using Sequence Majority Voting," in IEEE Access, vol. 10, pp. 88263-88275, 2022.

[25] F. Alrowais, M. M. Eltahir, S. S. Aljameel, R. Marzouk, G. P. Mohammed and A. S. Salama, "Modeling of Botnet Detection Using Chaotic Binary Pelican Optimization Algorithm with Deep Learning on Internet of Things Environment," in IEEE Access, vol. 11, pp. 130618-130626, 2023.

[26] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. -K. Wang, "Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9310-9319, 15 June15, 2022.