SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549 / https://doi.org/10.14445/23488549/IJECE-V10I4P102

Volume 10 Issue 4, 9-20, April 2023
© 2023 Seventh Sense Research Group®

Review Article

Security and QoS (Quality of Service) Related Current Challenges in IoT

Shital Pawar[1], Meghana Lokhande[2], Sandip Thite[3], Jyothi A. P.[4], Rucha Samant[5,] Rohini Jadhav[6], D. B. Jadhav[7]

[1]Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune, Maharashtra, India.
[2]Department of Computer Engineering, Pimpri Chinchawad College of Engineering, Pune, Maharashtra, India.
[3]Department of Computer Engineering, Vishwakarma University, Pune, Maharashtra, India.
[4]Department of Computer Science and Engineering, Ramaiah University of Applied Sciences, Bengaluru, India
[5]R. H. Sapat College of Engineering, M. S. and Research, Nashik, Maharashtra, India.
[6]Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India
[7]Department of Mechanical Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.

[1]Corresponding Author : shitalp16@gmail.com

Received: 03 March 2023 Revised: 06 April 2023 Accepted: 18 April 2023 Published: 30 April 2023

Abstract - *IoT technologies have permitted the linking of devices all around the globe through the Internet. Because of their capacity to send, receive, and analyze data, the gadgets are sometimes referred to as smart devices. It is regarded as one of the fastest-growing technologies, with a rising number of users on a daily basis. The volume of data transferred or received across networks, assuring the approaches used to address the energy restrictions of lithium-ion devices and the Quality of service (QoS), all enhance the effective adoption of IoT. The network-level Parameters include delay, speed, jitter, and packet loss. With the rising deployment of IoT devices connected, it is vital to concentrate on both device security and data privacy as it travels across networks. We sought to study the approaches utilized to safeguard the locations of both input nodes from invading and the impact of all the security protocols on the QoS of IoT in this paper.*

Keywords - *IoT (Internet of Things), Security, Deep learning, QoS (Quality of Service), Machine learning.*

1. Introduction

The system which allows physical items to be connected and monitored across the Internet is referred to as the Internet of Things (IoT). Items or things with their own digital identity, such as computer devices, digital machines, energy or household appliances, and so on, are linked to the surrounding objects and can exchange data, allowing the objects to interact and converse intelligently [1]. Things become linked without demanding contact between two humans or between a person and some digital device when we think about becoming connected via laptops, mobiles, computers, and many other smart devices with the assistance of an IoT. In order to fulfil the requirements of IoT consumers, service providers have created a variety of apps. The quality of the services (QoS) users request for a program may fluctuate individually, and equally, QoS will vary for distinct IoT applications. For any application, the quality metrics should be precisely stated so that the user may specify his expectations and internet companies can make modifications appropriately. As a result, researchers should focus on defining QoS (Quality and Service) indicators to define IoT service expectations [2].

1.1. QoS (Quality of Service)

QoS (Quality of Service) regulates network capability and capacity to offer a dependable backbone for IoT connection. To provide secure and predictable services, the QoS will regulate bandwidth, delays, packet loss delay variation etc., by categorizing traffic and registering channel limitations [3]. The IoT is a computer environment in which various items are connected inside the current internet infrastructure and via intelligent social apps to deliver useful services. A quality plan for various Software applications provides a good framework for evaluating application qualities related to the quality model. Generally, every significant quality attribute of a software programme must be described and assessed wherever feasible using verified or generally recognized metrics.

A quality model must be customized to create acceptance criteria and analyze a specific application area [4]. The management of the quality of IoT would be a logical consequence of the trends. However, this indicates that the quality of IoT systems differs significantly from assessing the quality of traditional software systems. It is mostly owing to the features of IoT nodes and IoT applications, which are different from those offered by traditional software systems. IoT systems are a complex fusion of several technologies like wireless networks, sensors etc. [5].

1.2. Architecture of IoT

The IoT architecture consists of various layers shown in fig. 1.

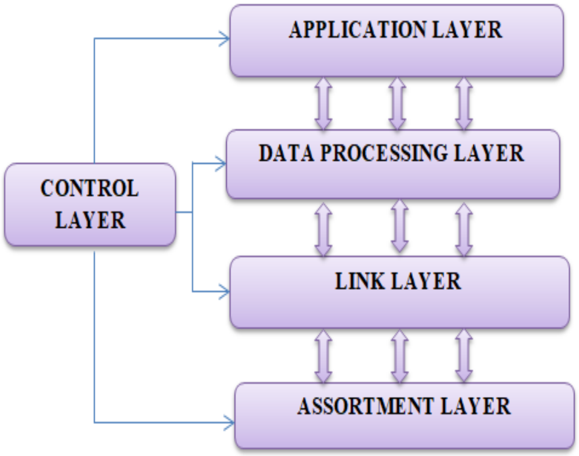

Fig. 1 IoT architecture

1.2.1. Control Layer

It is referred to as a key layer in the IoT architecture. The developer will specify the real job that this layer must do. This layer manages the whole process from the assortment layer to the application layer.

1.2.2. Assortment Layer

The sensors gather data from the physical world. The data from the sensor are perceived in the assortment layer. The assortment layer transmits this data to the processing layer through various smart electronic devices and communication technologies. Bluetooth, Zigbee, and other communication technologies are examples. This layer is constructed with smart objects, enabling users to gather real-time data from their surroundings. The link, application, and data processing layers are all connected via Smart objects [6].

1.2.3. Link Layer

The link layer is responsible for connecting the different levels. This layer transports data from smart objects to the application and data processing layers. It connects an application layer with a data processing layer [59].

1.2.4. Application and Data Processing

The information storage and analysis are carried out at the application and data processing layers. The data collected from smart devices will the transmitted to the application layer, where the data will be processed. The Data will not be saved directly to the cloud. Before being stored, the data will be first examined and then processed for future actions. This procedure aids in the preservation of the information's quality. Following examination, the obtained data is retained in accordance with the demands of the consumers [59].

2. QoS Parameters in IoT

There is no industry standard available for IoT architecture. IoT architectures are classified as 3-layer, 4-layer, and 5 -layer designs. The IoT architectures will differ depending on the applications. The IoT Quality of Services is divided into three categories. They are as follows: I Application layer QoS, (ii) Network layer QoS, and (iii) Sensing /assortment layer QoS. Each layer has its own set of Quality of Service (QoS) criteria. The QoS is evaluated in the services process based on the characteristics like Time Served, Availability of service, Service Delayed, Service Reliability, Service Load, Service Preference, Accuracy of information, as well as Cost of Network Deployment are application layer QoS characteristics. The taxonomy of QoS parameters in IoT is shown in Fig. 2 [8].

2.1. IoT- QoS Metrics

2.1.1. Bandwidth

Maximum number of packets transmitted from the source to the destination in a specific time slot called bandwidth. The word bandwidth refers to the rate at which data is transmitted in megabits per second [8].

2.1.2. Efficiency and Throughput

The number of packets transmitted from source to destination in a specific time period is called throughput. Bits per second are used to measure throughput [9].

2.1.3. The Ratio of Packet Loss

The number of packets that do not arrive at their destination during transmission is referred to as packet loss. The total count of packets delivered and the total count of packets received are used to calculate the packet loss [9].

2.1.4. Packet Delivery Ratio

It compares the total count of received packets with the total count of received packets at the node level.

2.1.5. Delay

Delay is defined as the time required to send a packet from source to destination compared to real-time. $D = T_{at} - T_{et}$, Where D stands for the delay, T_{at} stands for the actual time, and T_{et} stands for the time required for execution.

2.1.6. Time Required for Network Connection

It is the time needed by the server to receive the incoming request. If the service request is not executed within the specified period, the connections timeout error may occur.

2.1.7. Jitter

Jitter refers to the whole delay time for the packet transformation from source to destination.

2.1.8. Interoperability

Interoperability occurs when communication takes place between two devices that operate on separate platforms.

2.1.9. Reliability

If the data from sending node to receiving node is transmitted without any packet loss and security rupture, then that service is known as a reliable service [10].

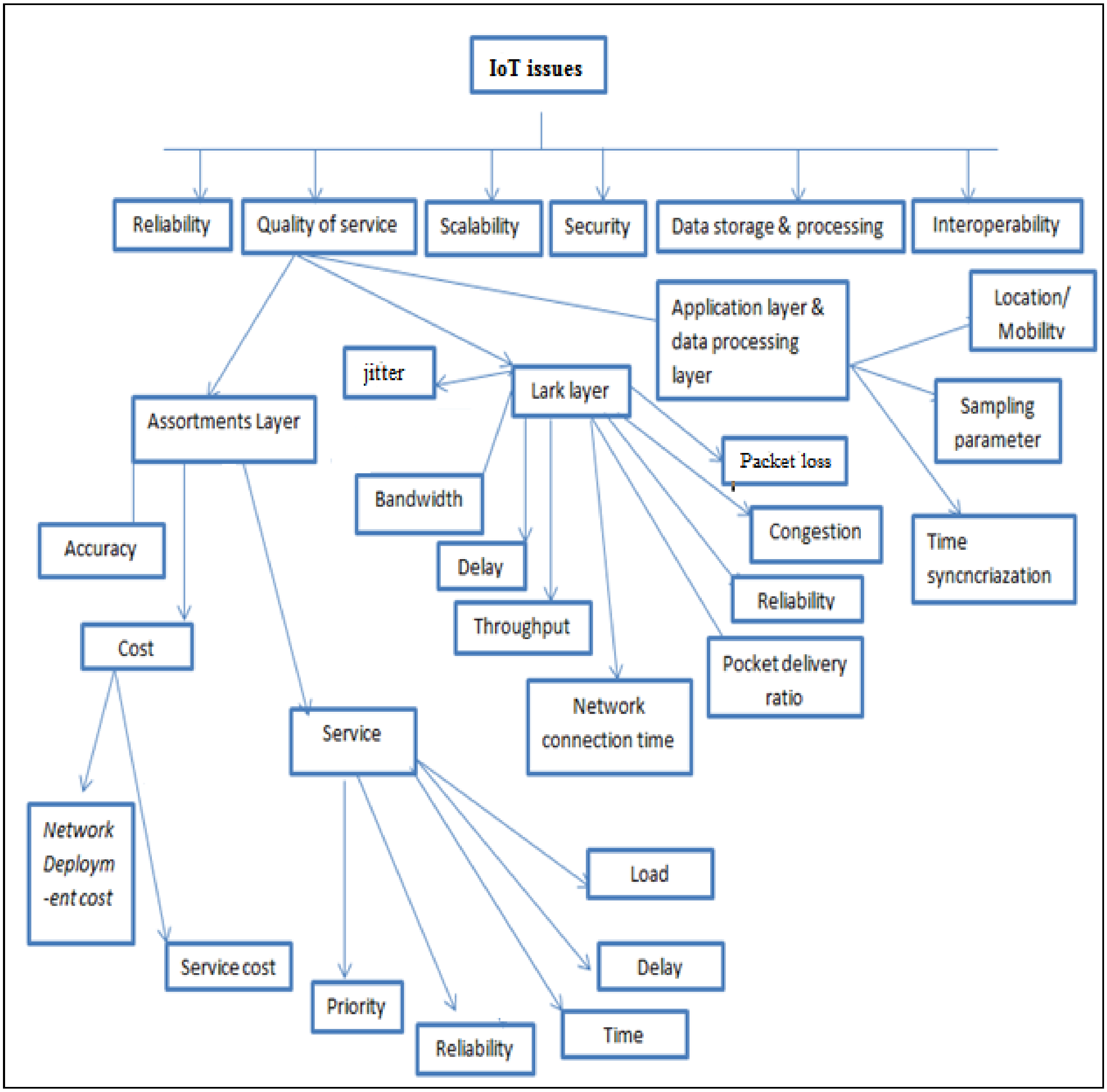

Fig. 2 Quality of service parameters in IoT

2.1.10. Congestion

Whenever a packet is transferred, the execution procedure delays the packet delivery rate. This delay might be caused by a lack of bandwidth or sending too many requests in the same route. As a result, the packet would have to wait till the preceding transmission has finished. As a result, there is congestion in the way [62].

3. Security of IoT

IoT Security encompasses both the physical device and internet security, influencing the procedures, technology, and actions required to safeguard IoT devices. It includes industrial equipment, smart energy grids, factory automation, entertainment gadgets, and other devices not typically intended for network security. Internet of Things security must protect the systems, data, connections etc., from various security threats that target the four types of vulnerabilities [13].

- Attacks on the data communication across the different devices and servers in IoT.
- Lifecycle attacks on IoT devices as they transmit from the user into maintenance.

- Software attacks here on the device
- Physical assaults that directly target the device's chip.

A strong IoT security portfolio enables developers to secure devices from all sorts of vulnerabilities while installing the secure communication that best meets their application's requirements. Cryptography technologies aid in the prevention of communication assaults, while security services guard against lifecycle attacks. To defend against software attacks, isolation measures may be deployed, while tamper mitigation and corner attack avoidance technologies are required against physical assaults on the network [14].

Many authors have worked on the current security issues in IoT, which are summarized as follows:

Suo H. *et al.* 2012 examined the present level of development in advanced components like encryption techniques, authentication protocols, sensor privacy laws, and cryptography, as well as a short explanation of the challenges [18]. He stated that there is a need to develop a framework for providing security to IoT systems. Applying security techniques at every individual layer of IoT architecture is very challenging. The most challenging element of security using cryptography is key management. It won't be easy to comply with IoT regulations and guidelines.

Al-mawee, W., in 2012, studied about various issues in IoT healthcare applications like privacy and security for disabled users. For that**,** a multitude of Smart home (IoT) solutions for people with visual impairments were discovered and classified. Then, secrecy issues in different IoT scenarios and publicized IoT-based answers were investigated. Ultimately, the thesis specifies the confidentiality of IoT applications for visually impaired individuals [17].

Jiang et al., in 2016, introduced an untraceable two-factor authentication scheme for WSNs. The proposed scheme offers additional security features and resists different attacks [19]. The suggested scheme offers additional security measures and is resistant to a wide range of popular attacks.

Vignesh R. *et al.*, in 2017, narrates security problems within and across the IoT layer. For that provides a survey as well as an investigation and analysis of the present state and status of IoT devices (IoT) privacy. The current status of IoT research is mostly focused on access control and authentication protocols. However, with the fast advancement of technology, it is very critical to integrate the latest networking protocols like IPv6 and 5G to achieve the gradual mash-up of IoT architecture [20].

Challa **S.** *et al.*, in 2017, presented an authenticated key creation method for IoT systems based on new signatures. The proposed method is executed on an NS2 simulator, demonstrating the system's feasibility in the simulation results [21].

Srinivas D. *et al.*, in 2017, presented security and privacy issues in Multi-gateway WSN. For that, he proposed a novel WSN authentication and key bio-hashing agreements. Biohashing makes it easier to eliminate fake acceptance rates without increasing false refusal. Using the BAN logic, the author proves the mutual authentication of the proposed method. The proposed method is secure from well-known authentication protocol attacks with the informal security analysis [22].

Shen J. *et al.*, 2018 present an efficient multilayer authentication protocol for WBANs and a secure session key generation mechanism in this paper. The author presents a new certificate-less authentication protocol with no pairings that uses the ECC algorithm to provide less computational cost and high security. The author mainly addressed the security issues during the data transmission phase of WBANs [23].

Malik, R., in 2018, presented a review study which gives information on the Internet of Things strategy. This study paper also examines the design features of IoT architecture, its components, and numerous IoT security challenges that may be created to get better results. The author stated that a possible privacy concern is no sensor standardization. The system's performance is being hampered by the growing number of gadgets [24].

Dammak M. *et al.*, in 2019, proposed a lightweight authentication scheme for users based on tokens. This scheme minimizes the processing overhead and conserves energy for devices used for authentication by applying lightweight operations. It is developed to resist the most common security threats. It is a tough competitor to already popular technologies for secure authentication in IoT contexts [26].

Sheikh A. *et al.*, in 2019, states that with the increasing number of IoT devices in IoT network, it becomes critical to focus on device security and data security as it is transported across the networks. In this research, the author attempted to investigate the techniques used to secure the location of input and output sites from breaching and the influence of these security strategies here on the QoS of IoT networks [4]. There is a need to focus on device as well as data security. Further machine learning techniques can be applied to enhance the QoS of IoT systems [4].

Threats, S. in 2019 states IoT security threats can be reduced with the help of blockchain, fog computing, edge computing, and machine learning. In order to make use of blockchain, fog and edge computing and ML techniques for providing security in IoT networks, the few performances, as well as security challenges, must be resolved [27].

Verma N. *et al.* 2019 evaluate the basis of IoT via various investigations, followed by security difficulties in IoT subject to numerous audits of the vision and security concerns, risks on the Perception Layer, and many applications. The motivation for this study was established by providing an appropriate assessment of research drifts in IoT security from 2011 to 2016 [28].

Tawalbeh, L. *et al.,* in 2020, proposed new IoT layered architectures, both generic & enhanced, including privacy-related features, along with layer identifying, in this work. The proposed IoT platform, including cloud/edge capabilities, was created and tested. The lowest phase is defined by Amazon Web Service's IoT nodes, which are created as Vms (AWS). The author created encryption keys to permit content transit between the tiers of the planned Cloud/Edge-based IoT paradigm [29].

The survey, A. C. (2020) This article analyses the different concepts of the IoT, defines and emphasizes its main technologies and uses, and presents the next framework as a solution to the difficulties. IoT concerns were investigated to boost research and development in the industries [30].

Shafik W. *et al.* in 2020 gave a complete analysis of the key performance of IoTs in this paper. The major IoTs have been further researched and evaluated, such as IoT security, IoT load control, IoT power management, and IoT electricity consumption efficiency in many computing parts [31].

Stout, W. M. S. and Urias, V. E. 2020 examined the IoT building blocks to grasp the peculiarities of different IoT domains better**.** The Internet of Things has a tiered approach. This layered approach accepts point (or single-layer) security solutions while ignoring the advantages of cross-layer solutions [32].

Shobha R. *et al.* in 2021 tells that According to investigations of current research models, most of the solutions to the security problems are provided by using various kinds of encryption techniques, which have been shown to be efficient in safeguarding the attack surfaces of communication channels in IoT while also promoting reduced energy consumption. Integration of technology such as machine learning, blockchain, artificial intelligence-based fuzzy logic approaches and elliptical cryptographic functions has helped to strengthen the security of IoT networks [33].

Nasr Abosata, in 2021 categorizes risks and viable security mechanisms for IoT layers. Consequently, the threat is related to one or many layers of the architecture and is accompanied by a literature study on prospective IoT software solutions. This also critically analyses available IoT or Industrial IoT solutions depending on multiple security techniques, including different protocols, networking, encrypting, etc., and penetration testing devices [34].

Sadique, K. M. *et al.,* in 2018, introduced a basic generic model of six layers that may describe any IoT system. A well-implemented distributed intelligence model on this tiered approach would provide total IoT security. The use of computer science in IoT is expanding across all sectors, including IoT security. While machine learning techniques improve the IoT paradigm, they also create security concerns [62].

Hewage, I. T. A., *et al.* 2020 states security, privacy, and confidentiality are major challenges to the realization of the IoT, as are heterogeneity management, network capacity limitations, and the management and processing of huge amounts of data to deliver appropriate information or services and enable an efficient regulatory strategy in the area of the Internet of Things [35].

It has been observed that in terms of the overall performance of attack detection in IoT systems, the deep learning technique provides outstanding results in comparison with linear techniques. Still, it is not as effective as ensemble approaches [47]. LR technique performance is poor compared to DT and XgBoost techniques. The majority of ML techniques are confined to trained datasets only. Hence, these techniques cannot perform effectively with different datasets because of various threat patterns [48]. The use of ML techniques which provides better results with a limited number of features, is suitable for IoT systems, as it requires less computational power. The most effective classifier for identifying injection attacks is a decision tree [49].

The system developed using the CART algorithm of DT requires minimum computational power and is useful for identifying cyber-attacks in the intelligent system environment. The performance of the CART classifier is greater as compared to Naïve Bayes. The misuse/signature-based attack detection method is unable to identify unidentified attacks. The anomaly detection method is another kind of method used for attack detection, which can be able to detect unidentified attacks. However, this method results in a large number of false positive alerts, and this method is difficult to implement for IoT systems due to the complicated structures of IoT devices. The ML techniques can detect a variety of attacks. However, most researchers have used old datasets like KDDNSL, ISCX, KDDCUP99 etc. The latest dataset, like N-BaIoT, contains 10 different attack samples, which can be used to develop an attack detection model [50].

Neural network like FNN is well suitable for binary classification, but it's not much use for multiclass attack detection. A specific difficulty while using DL techniques for enhancing IoT systems' security is maintaining an appropriate balance between minimum false alerts and better accuracy. The performance of BiLSTM is reduced in the case of the detection of sophisticated attacks. While in the case of DNN, as the size of the training dataset increases, the execution time also increases. Hence, to overcome all these problems, there is a need to develop an IDS system [51].

3.1. Security Challenges in IoT

Table 1. Security challenges and further scope [17-21] [34-46]

Security requirements	Security Challenges	Further scope
Authentication	Mutual authentication system needs to be implemented before starting any communication between various communicating devices.	Powerful authentication methods are necessary to prevent the system from unauthorized access.
Privacy	Profiling and tracking Localization Secure data transmission	Frameworks for overall privacy preservation Context-specific privacy strategies Privacy protecting motivations based on Game theory.
Confidentiality	Lightweight primitives Consumption of fewer resources	Lightweight encryption algorithms need to be developed for IoT. Efficient, comprehensive frameworks lightweight security provisioning by using SDNs
Secure routing	Secure path establishment Providing security to malicious nodes Quick recovery from failure	Designing of routing protocols for IoT network performance Effective control of routing operations
resilient and strong management	Attack resilience Early detection of attacks Self-stabilization of the security protocol Rapid recovery from losses/failures	Centralized frameworks for management based on SDN. Merging the latest security mechanisms like blockchain and SDN with traditional IoT security methods.
Detection of attacks (DDOS and insider)	Detection of DoS and insider attacks, which are resource efficient. Resource efficient countermeasures. Applying ML/DL techniques on real-time IoT systems to detect attacks.	Providing lightweight solutions to IoT devices as they are resource constrained. Centralized SDN detection and mitigation algorithms. The performance and time, as well as space complexity of ML/ DL techniques, also must be improved further. The categorization of additional threats by using DL techniques is necessary for providing security.
Lightweight security solution	Converting traditional security methods into lightweight security methods as IoT devices are being resource constrained.	Transferring certain processing/computation to the fog layer. Simplifying the method for key formation.
Intrusion detection	Develop a real-time Intrusion Detection System for IoT and increase the scope of threats identification. Evaluation of the effect of IDS on the accuracy, usage of energy and performance of IoT devices.	Industrial IoT needs the development of modern intrusion detection techniques to ensure the security of linked systems and offered services. Prevention measures for various cyber-attacks or violations of the Industrial IoT infrastructure require more development in the future.
Device monitoring	Applying ML techniques to track the abnormal behaviour of IoT devices.	Evaluation of various QoS parameters of IoT systems for effectively analyzing the data traffic on the network.

3.2. Machine Learning and Deep Learning Techniques for Security

Table 2. Comparison of ML and DL techniques for providing security in IoT

Author	Year	Classifier type	Type of attack	Dataset	ML/DL techniques	Accuracy	Further scope
Hector et al. [47]	2019	Multiclass	DoS MitM Intrusion	Real-time dataset	LSTM GRU	93.37 % 96.08%	Ensemble techniques can be used for further work. In future, ids can be reinforced with these techniques.
Khalid et al. [48]	2022	Binary	Botnet	UNSW-NB15	LR DT XGBoost	78% 94% 93%	The ML model will be prepared to train on massive data sets successfully.
Tarek et al. [49]	2022	Binary	Injection attack	AWID	DT RF SVM	96.81% 98.88% 97.58%	The developed system can be compared deeply with respect to learning time, accuracy, count of epochs etc.
Chuw et al. [50]	2020	Binary	Botnet	N-BaIoT	CART classifier NB	99% 58%	Developing a more efficient attack detection system to secure IoT devices is necessary.
Alaa et al. [51]	2022	Binary	Intrusion	BoT-IoT	CNN LSTM GRU	99.7% 99.8% 99.6%	In the future, the scope is available to discover a new dataset for intrusion detection on IoT systems. This research could be widened to consider the variety of other classifiers for obtaining better performance.
Himani et al. [52]	2021	Multiclass	DDoS DoS Reconnaissance Theft.	BoT-IoT	SVM RF DT ANN LR KNN	82.2% 99% 99% 99.4% 33.37% 99%	Accuracy for multiclass attack detection can be improved further.
Himani et al. [52]	2021	Binary	DDoS DoS Reconnaissance Theft.	BoT-IoT	SVM RF DT ANN LR KNN	96.2% 99.9% 99% 93% 92.5% 99.1%	A variety of attacks on the IoT network system can be detected further by using the collected dataset.
Shahid et al. [53]	2020	Multiclass	DoS malicious operation malicious control data type probing spying scan	DS2OS	ANN SVM DT Random Neural Network	98.55% 98.39% 99.08% 99.20%	More comprehensive and real-time evaluations can further be carried out on the designed RaNN model**.**
Minhaz et al. [54]	2021	Binary	DDOS	CICIDS2017	RF -1DCNN RF-MLP	99.63% 99.58%	The development of an online DDoS attack detection system using ML/DL techniques which will be helpful in protecting IoT networks.

Mohmud ul et al. [55]	2019	Multiclass	Data probing DoS Data probing Malicious activity Wrong setup	DS2OS	SVM LR ANN RF DT	98.2% 98.3% 99.4% 99.4% 99.4%	It is necessary to do more scientific investigation on real-time data for detecting various attacks.
Vigna et al. [56]	2021	Binary	DOS	NSL KDD	RF KNN LR	99% 98% 82%	For the detection of attacks in IoT networks, the methodology can be investigated further for efficient feature selection.

SVM classifier provides better outcomes for detecting anomalies, while its performance is poor for multiclass attack detection. LR provides excellent results for detecting anomalies with respect to the accuracy, but the parameters like recall, precision etc., results give false alerts. The performance of LR techniques is very worst in the case of multiclass attack detection. Hence, the LR technique is not appropriate for detecting attacks in IoT systems. The performance of the RF technique is very high as it provides 99% for detecting anomalies and attacks in IoT systems [52].

Blockchain technology and the RaNN technique can be combined together to build a strong security framework for IIoT systems. The performance of RaNN is greater than other ML techniques like SVM, ANN and DT. The SVM is not a good option for larger datasets, as it has a high learning rate. The RaNN approach resulted in high values for other metrics such as recall, precision, F1 score etc. [53]. It has been observed that the RF and DT provide better values for accuracy, F1 score, precision etc., than other ML techniques. The outcome of ANN is also good, but DT outperformed ANN for multiclass attack detection. Though the RF technique provides better results for detecting cyber-attacks on IoT systems, it cannot guarantee that, while dealing with huge quality of data RF will operate in the same way as other undetected issues. Hence, additional research is required [54]. Many researchers have applied ML techniques on available datasets for the detection of attacks in IoT. While dealing with real-time data, several issues might arise. More investigation, which focuses on real-time data, is required to resolve these issues [55]. The performance of the LR technique is poor compared with the RF technique for detecting various attacks in the IoT system. The performance of the RF and KNN techniques is better. Because of the inadequate selection of features, the ml approaches are primarily likely to misclassify harmful traffic flows. The challenge is about how to choose efficient features for precise malicious threat identification in IoT systems requires further investigation [56-58].

3.3. Suggestion to Improve Performance of ML/Techniques for Security in IoT

Compared to other machine learning techniques, the RF technique can be employed for the security of IoT systems as it provides very good results for detecting various attacks. The observation from available research results is that the machine learning techniques offer better results for binary classification, i.e. detection of anomalies, compared to multiclass attack detection. Hence, it is necessary to apply deep learning techniques to achieve better results for detecting various attacks in multiclass attack detection. Extraction and selection of features is one of the most essential tasks in DL techniques, as selecting the best features results in getting the best results.

Every deep learning technique has some limitations. Hence, using hybrid DL models to detect attacks in an IoT environment is beneficial. Many researchers have used the available datasets to detect various attacks. Still, it is essential to use real-time data to obtain more precise results in the IoT environment. In order to provide lightweight solutions to IoT, the time and space complexity of ML Techniques needs to be reduced. To improve the performance of ML techniques and accuracy, other factors like precision, F1 score etc., must be higher. Appropriate feature selection is most important for ML techniques to improve attack detection efficiency in IoT systems. Among all the ML techniques, the RF technique provides better accuracy for detecting attacks in IoT systems. Nevertheless, this doesn't guarantee that RF will function in this manner in the context of huge data or other unidentified issues. So, further research will be required.

4. Quality of Service in IoT

White, G. *et al.* 2017 state the presence of many heterogeneous devices that are likely resource-constrained and mobile in an IoT environment has raised concerns about the quality of service (QoS). Researchers recommend that using quality models like ISO/IEC 25010, which was used to define the quality components in this mapping, will assist in evaluating the trade-off between alternative techniques. A variety of QoS factors must be considered while evaluating the service quality of any IoT application. Each layer of the IoT architecture must implement QoS methods to provide a sufficient amount of QoS for security-sensitive IoT applications. [12].

Kim, M. in 2016, stated Internet of Things application is a complicated fusion of several technologies such as wireless networks, embedded systems, sensors, and connections. The existing ISO 9126 QoS approach is not appropriate for evaluating IoT applications. The author proposed a new evaluation method for IoT applications by utilizing the ISO 9126 quality attributes. This study proposes a quality model for IoT applications based on the IA-QM. This model has included four different quality attributes that could be applied to determine the overall efficiency of IoT systems [3].

Subash K. *et al.,* in 2019, conducted a survey to discover QoS parameters, and a taxonomy of layer-wise QoS parameters for IoT was published. The study also focuses on IoT QoS measurements. Each statistic has a distinct role to play in increasing the quality of IoT services. In IoT, the data is transmitted from one layer to another in the form of packets. There are several challenges to transmitting fake packets, modifications in the packets, packet loss etc. By addressing these issues, service quality and security could be enhanced. Each QoS parameter contributes in a different way to raising service quality in IoT [2].

Kimbugwe, N. *et al.*, in 2021, presented a comprehensive assessment of how DL approaches have been used to improve QoS in IoT. QoS in IoT-based solutions is violated when system security and privacy are breached or when IoT capabilities are not adequately managed. The author discovers Machine Learning models and methods reported in cutting-edge research and reviews publications, and determines which are most often employed in dealing with IoT QoS concerns. The DL techniques can be applied to improve the QoS of IoT systems. DL techniques are currently used to revolutionize a number of IT industries because of their numerous benefits as a technique based on information. In order to establish and assure strong QoS in the IoT system, it is unclear exactly how DL techniques have actually to be utilized. Additionally, it is unclear which DL techniques are most suitable for a variety of facets of QoS in the IoT system [5].

T. Manivannan et al., in 2020, state QoS concerns such as jitter (delay variation) and transport rate are identified based on 8 applications and 40 services. A preventative paradigm for QoS in IoT applications is presented to accommodate different degrees of real-time and delay-tolerant traffic in sensor networks. Three layers are included in the suggested model. This paradigm promotes clients to communicate news in IoT applications in as little time and with as little delay as possible. This investigation allows the researcher to separate QoS concerns in IoT applications to address booking issues [59].

5. Research Gap for QoS

According to the literature, research on IoT has been conducted to investigate the issue and cause: Quality of service assessment of IoT applications on security problems. As seen by the research, numerous strategies have been used to combat this issue as it has grown on a wide scale. With changing technology, a corresponding shift has occurred. There is a need to investigate and evaluate the elements that fail to manage the current issue even after applying the previously implemented technologies. The range of most current research is confined to either origin of the issue or the answers to it. However, the literature is deafeningly quiet on how to improve the implementation of current technology to avoid the issue of IOT application quality of service assessment. In addition to having current technology, the issue of IoT quality service and security is becoming more prevalent [37-40].

Many researchers have evaluated various QoS parameters like latency, delay, bandwidth etc. which are related to the performance of IoT applications. Very less number of researchers have considered the security-related parameters for IoT applications. Any security threat in an IoT application can affect the performance of that application. Hence it is necessary to consider the security-related parameters while evaluating the performance of IoT applications. Considering security-related issues while evaluating QoS parameters of critical IoT applications like healthcare is most important. A lot of research was carried out on various facets of QoS, like the detection of intrusions by using DL techniques. Several QoS issues with the application of DL techniques received comparatively less attention [5]. As the number of IoT devices increases rapidly, it is essential to focus on the QoS of data transferred over the network and the QoS of IoT applications/gadgets [59].

6. Conclusion and Limitations

The IoT has become a significant technology for interconnecting multiple networks today. The significance is shown by the observation that Around 2008, a growing proportion of internet-connected devices outnumbered the world's growing population. Machines have decreased physical work and efforts in today's fast-paced society since a man can accomplish whatever he can conceive with the push of a button. Despite some limitations, such as the lack of standardization of sensors, which poses a potential privacy issue, and the growing number of devices, which causes problems in system functioning, IoT is an essential facet as it aspires to improve the essence of life by joining various devices and applications. At each tier, the framework is vulnerable to assaults. As a result, there are several security concerns and needs that must be addressed. The current status of IoT research is mostly focused on identity management control protocols. With the fast advancement of technology, it is critical to integrate new networking protocols, such as IPv6 and 5G, in order to accomplish the gradual mash-up of IoT architecture.

References

[1] Parul Goyal et al., “Internet of Things: Applications, Security and Privacy: A Survey,” *Materials Today: Proceedings*, vol. 34, pp. 752–759, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] K. Subash et al., “Quality of Service in the Internet of Things (Iot) – A Survey,” *ReTell*, vol. 21, pp. 1-9, 2019. [Google Scholar] [Publisher Link]

[3] Mi Kim et al., “A Quality Model for Evaluating Iot Applications,” *International Journal of Computer and Electrical Engineering*, vol. 8, no. 1, pp. 66–76, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[4] Anjum Sheikh, Asha Ambhaikar, and Sunil Kumar, “Quality of Services Improvement for Secure Iot Networks,” *The International Journal of Engineering and Advanced Technology*, vol. 9, no. 2, pp. 5127–5135, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Nasser Kimbugwe, “Application of Deep Learning for Quality of Service Enhancement in Internet of Things: A Review,” *Energies*, vol. 14, no. 19, pp. 1–27, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Md Husamuddin, and Mohammed Qayyum , “Internet of Things: A Study on Security and Privacy Threats,” *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, pp. 93-97, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] L.H. Patil et al., "Voip Based Wifi Calling System*," SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 9, pp. 7-9, 2019. [CrossRef] [Publisher Link]

[8] Nasar Abosata, “Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications,” *Sensors*, vol. 21, no. 11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Arbia Riahi Sfar et al., “A Roadmap for Security Challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] AbdelRahman H. Hussein, “Internet of Things (IOT): Research Challenges and Future Applications,” *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 10, no. 6, pp. 77–82, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Preetha S, Sagar J, and Krishna Pooja P, "Security Issues Faced by Internet of Things: A Survey," *International Journal of Recent Engineering Science*, vol. 7, no. 3, pp. 1-6, 2020. [CrossRef] [Publisher Link]

[12] Gary White et al, “Quality of Service Approaches in Iot: A Systematic Mapping,” *Journal of Systems and Software*, vol. 132, pp. 186-203, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Anurag Tiwari, and Harishchandra Maurya , “Challenges and Ongoing Researches for IOT (Internet of Things): A Review,” *International Journal of Engineering Development and Research*, vol. 5, no. 2, pp. 57–60, 2017. [Google Scholar] [Publisher Link]

[14] N Alhalafi, and Prakash Veeraraghavan, “Privacy and Security Challenges and Solutions in IOT: A Review,” *IOP Conference Series: Earth and Environmental Science*, vol. 322, no. 1, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Noor Mohamad, M.B, and Hassan, W.H, “Current Research on Internet of Things (Iot) Security: A Survey,” *Computer Networks*, vol. 148, pp. 283-294, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] Srinivasan Sridharan, "Machine Learning (ML) in A 5G Standalone (SA) Self Organizing Network (SON)," *International Journal of Computer Trends and Technology*, vol. 68, no. 11, pp. 43-48, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Wassnaa AL-mawee et al., *Privacy and Security Issues in Iot Healthcare Applications for the Disabled Users a Survey*. [Google Scholar] [Publisher Link]

[18] Hui Suo et al., “Security in the Internet of Things: A Review*,” 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, pp. 648–651, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[19] Qi Jiang et al., “An Untraceable Temporal-Credential-Based Two-Factor Authentication Scheme Using ECC for Wireless Sensor Networks,” *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[20] Ryoichi SASAKI et al., “Security on Internet of Things (Iot) Systems,” *The Journal of Information Science and Technology Association*, vol. 67, no. 11, pp. 577–581, 2017. [CrossRef] [Publisher Link]

[21] Sravani Challa et al., "Secure Signature-Based Authenticated Key Establishment Scheme for Future Iot Applications," *IEEE Access*, vol. 5, pp. 3028-3043, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jangirala Srinivas et al., “Secure and Efficient User Authentication Scheme for Multi-Gateway Wireless Sensor Networks,” *Ad Hoc Networks*, vol. 54, pp. 147-169, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jian Shen et al., “A Lightweight Multi-Layer Authentication Protocol for Wireless Body Area Networks,” *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Rohit Malik, Dr. Kamna Solanki, and Dr. Sandeep Dalal, “Literature Review on Security Aspects of Iot,” *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, pp. 123–127, 2018. [CrossRef] [Publisher Link]

[25] Zhohov, Roman, “*Evaluating Quality of Experience and Real- Time Performance of Industrial Internet of Things*,” Diploma theses and Master's theses, 2018. [Google Scholar] [Publisher Link]

[26] Maissa Dammak et al., “Token-Based Lightweight Authentication to Secure Iot Networks,” *2019 16th IEEE Annual Consumer Communications and Networking Conference, CCNC 2019*, pp. 1–4, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] Threats, S, “A Survey on Iot Security: Application,” *IEEE Access*, 2019.

[28] Navneet Verma, "Iot Security Challenges and Counters Measures," *The International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 1519–1528, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[29] Lo'ai Tawalbeh et al., "Applied Sciences Iot Privacy and Security: Challenges and Solutions," *Applied Science*, vol. 10, no. 12, pp. 1–17, 2020. [CrossRef] [Publisher Link]

[30] Rosilah Hassan et al., "Internet of Things and Its Applications: A Comprehensive Survey," *Symmetry*, vol. 12, no. 10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Wasswa Shafik et al., "A Study on Internet of Things Performance Evaluation*," Journal of Communications Technology, Electronics and Computer Science*, no. 28, pp. 1-19, 2020. [Google Scholar] [Publisher Link]

[32] Stout, W. M. S., and Urias, V. E, "Challenges to Securing the Internet of Things," *2016 IEEE International Carnahan Conference on Security Technology (ICCST),* 2016. [CrossRef] [Google Scholar] [Publisher Link]

[33] Rachit, Shobha Bhatt, and Prakash Rao Ragiri, "Security Trends in Internet of Things: A Survey," *SN Applied Sciences*, vol. 3, no. 1, pp. 1–14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[34] Nasr Abosata, "Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," *Sensors*, vol. 21, no. 11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[35] Dmitrii Dikii, and Aleksey Tikhomirov, "Detection of Dos Attacks Exploiting SUBSCRIBE Messages of the MQTT Protocol," *International Journal of Computers and Applications*, vol. 44, no. 6, pp. 579-585, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[36] Asiri Hewage, "IOT Security: A Review," [Google Scholar] [Publisher Link]

[37] Vaishali Hitesh Patel, and Sanjay Patel, "A Review on IoT Security: Challenges and Solution Using Lightweight Cryptography and Security Service Mechanisms Offloading at Fog," *ICICNS 2020,* [CrossRef] [Google Scholar] [Publisher Link]

[38] Shital Pawar, and Dr. Suhas Patil, "Current Security Challenges in Internet of Things," *International Journal of Research in Electronics and Computer Engineering*, vol. 7, no. 2, pp. 2399-2401, 2019. [Google Scholar] [Publisher Link]

[39] Promise R. Agbedanu et al., "Using Incremental Ensemble Learning Techniques to Design Portable Intrusion Detection for Computationally Constraint Systems," *International Journal of Advanced Computer Science and Applications(IJACSA),* vol. 13, no. 11, pp. 33-45, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[40] Abdussalam Ahmed Alashhab et al., "Low-Rate Ddos Attack Detection Using Deep Learning for SDN-Enabled Iot Networks," *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 13, no. 11, pp. 371-377, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[41] Waqas Aman, and Firdous Kausa, "Towards a Gatewaybased Context-Aware and Self-Adaptive Security Management Model for Iot-Based ehealth Systems," *International Journal of Advanced Computer Science and Applications*. vol. 10, no. 1, pp. 280-7, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[42] Abdussalam Ahmed Alashhab et al., "Experimenting and Evaluating the Impact of Dos Attacks on Different SDN Controllers," *IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, pp. 722-727, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[43] Souradip Roy et al., "A Lightweight Supervised Intrusion Detection Mechanism for Iot Networks," *Future Generation Computer Systems*, vol. 127, pp. 276–285, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[44] Lubna Fayez Eliyan, and Roberto Di Pietro, "Dos and Ddos Attacks in Software Defined Networks: A Survey of Existing Solutions and Research Challenges," *Future Generation Computer Systems,* vol. 122, pp. 149- 171, vol. 122, pp. 149-171, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[45] Sana Ullah Jan et al., "Toward a Lightweight Intrusion Detection System for the Internet of Things," *IEEE Access*, vol. 7, pp. 42 450–42 471, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[46] Waqas Aman, and Fatima Najla Mohammed,, "A Comprehensive Assessment Framework for Evaluating Adaptive Security and Privacy Solutions for Iot E-Health Applications," *International Journal of Advanced Computer Science and Applications (IJACSA),* vol. 13, no. 10, pp. 613-623, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[47] Hector Alaiz-Moreton et al., "Multiclass Classification Procedure for Detecting Attacks on MQTT-Iot Protocol," *Complexity,* vol. 2019, pp.1-11, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[48] Khalid Alissa et al., "Botnet Attack Detection in Iot Using Machine Learning," *Computational Intelligence and Neuroscience,* vol. 2022, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[49] Tarek Gaber et al., "Injection Attack Detection Using Machine Learning for Smart Iot Applications," *Physical Communication,* vol. 52, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[50] Chaw Su Htwe et al., "Botnets Attack Detection Using Machine Learning Approach for Iot Environment," *Journal of Physics: Conference Series*, pp. 1-7, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[51] Alaa Mohammed Banaamah, and Iftikhar Ahmad, "Intrusion Detection in Iot Using Deep Learning," *Sensors*, vol. 22, no. 21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[52] Himani Tyagi, and Rajendra Kumar “Attack and Anomaly Detection in Iot Networks Using Supervised Machine Learning Approaches,” *Revue d'Intelligence Artificielle*, vol. 35, no. 1, pp. 11-21. [CrossRef] [Google Scholar] [Publisher Link]

[53] Shahid Latif et al., “A Novel Attack Detection Scheme for the Industrial Internet of Things Using A Lightweight Random Neural Network,” *IEEE Access*, vol. 8, pp. 89337 – 89350, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[54] Minhaz Bin Farukee et al., “Ddos Attack Detection in Iot Networks Using Deep Learning Models Combined With Random Forest as Feature Selector,” *Advances in Cyber Security, Communications in Computer and Information Science*, vol. 1347, pp. 118-134, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[55] Mahmudul Hasan et al., “Attack and Anomaly Detection in Iot Sensors in Iot Sites Using Machine Learning Approaches,” *Internet of Things*, vol. 7, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[56] V Sri Vigna Hema, S Devadharshini , and P Gowsalya, “Malicious Traffic Flow Detection in IOT Using Ml Based Algorithms,” *International Research Journal on Advanced Science*, vol. 3, no. 5, pp. 68-76. [CrossRef] [Google Scholar] [Publisher Link]

[57] Srabana Pramanik, Deepak. S. Sakkari, and Sudip Pramanik, "Remediation Measures to Make the Insecure Internet of Things Deployment Secure," *International Journal of Engineering Trends and Technology*, vol. 70, no. 6, pp. 155-164, 2022. [CrossRef] [Publisher Link]

[58] Adel Rajab et al., "Cryptography Based Techniques of Encryption for Security of Data in Cloud Computing Paradigm," *International Journal of Engineering Trends and Technology*, vol. 69, no. 10, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[59] T. Manivannan, and P. Radhakrishnan, “Preventive Model on Quality of Service in IOT Applications,” *International Journal of Mechanical and Production Engineering Research and Development*, vol. 10, no. 3, pp. 1247–1264, 2020. [Google Scholar] [Publisher Link]

[60] P.Maxmillon, and R.Franklin, "A Review on Authentication and Security Maintenance in Wireless Sensor Network," *SSRG International Journal of Mobile Computing and Application*, vol. 3, no. 2, pp. 10-13, 2016. [CrossRef] [Publisher Link]

[61] Suhas B R, Shreyas Ganesh, and Nalina V, "Green Network and Communication," *International Journal of Recent Engineering Science*, vol. 5, no. 4, pp. 1-4, 2018. [CrossRef] [Publisher Link]

[62] Kazi Masum Sadique, Rahim Rahmani, and Paul Johannesson, “Towards Security on Internet of Things: Applications and Challenges in Technology,” *Procedia Computer Science*, vol. 141, pp. 199–206, 2018. [CrossRef] [Google Scholar] [Publisher Link]