IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

# Identifying the Effects of Security Measures on QoS Variations for IoT Networks

**Ms. Suman Devi[1], Ms. Jyoti[2]**

Department of Computer Science and Engineering, CDLU, Sirsa[1]

Department of Technical Education, Govt. Polytechnic Dhangar, Fatehabad[2]

**Abstract**: Many technical advancements have led to the formation of the Internet of Things (IoT), which facilitate the worldwide networking of internet-enabled objects. These gadgets, which are often referred to as "smart gadgets," have the ability to send, receive, and manage data. It is a widely held belief that the IoT is a technology seeing rapid growth and user acquisition. The flawless transfer and receipt of data is essential to the Internet of Things' functionality. Moreover, it is essential to provide an outstanding level of Quality of Service (QoS) and avoid severe energy constraints for battery-powered devices. One emerging trend in the IoT is the proliferation of networked gadgets. To safeguard the gadgets and the data they generate, stringent security measures are being implemented. The purpose of this work is to examine approaches that have been developed to protect source and sink nodes in order to prevent data breaches and unauthorized access. The purpose of this study is to examine the algorithms, with a special emphasis on the Ad-hoc On-Demand Distance Vector (AODV) protocol, on the QoS of IoT -connected networks. Selective data recognition is made possible by QoS systems, which maximize network traffic use. By using this technique, the network's reach is increased, information is used as efficiently as possible, and prompt delivery of the best internet service is ensured. The goal of this project is to put the K-Nearest Neighbors (KNN) method to use in detecting and eliminating malware, or malicious software. The accuracy of forecasts was greatly improved by using these models cautiously. MATLAB software was used in the development of the models. By using these algorithms, the study provides information that can be used to progress the resilience and security of Internet of Things networks against possible attacks.

**Keywords:** K–Nearest Neighbor, Internet of Things (IoT), Quality of Service (QoS), Malware detection, Wireless Network, Security

## INTRODUCTION

The Internet of Things (IoT) is a network that facilitates the connection and surveillance of tangible items over the internet. Connected items, such as computer devices, digital machines, electrical appliances, and household appliances, own their own digital identity. They are able to share data with other objects in their environment, enabling intelligent connectivity and communication. As we consider the means of connectivity such as tablets, laptops, computers, and mobile phones facilitated by the Internet of Things (IoT), it is important to note that devices may establish connections autonomously, without the need for human-to-human or human-to-digital device contact. Service providers have created many apps to meet the needs of IoT consumers. The users' expectations for the quality of services (QoS) in an application may vary individually, and similarly, the QoS requirements will fluctuate for different IoT applications. It is essential to establish precise quality indicators for every application to enable users to articulate their expectations and allow service providers to make necessary adjustments. The researchers should prioritize the establishment of clear and concise Quality of Service (QoS) metrics to accurately delineate the expectations of consumers of IoT services[1].

Due to the rapid advancement of the internet, the prevalence of cyber dangers has also escalated, mostly due to the proliferation of malware. Malware is a computer application specifically designed to cause damage to another user's machine via various means. In the current day, there exists a wide variety of malware, which individuals get from illicit sources in order to intensify assaults on computer systems. Consequently, it becomes exceedingly challenging for antivirus scanners to provide comprehensive protection for a computer.[2-3] Malware, often known as malicious software, is a program that infiltrates a computer system without the user's consent, with the intention of causing damage to the system or extracting confidential information. Malicious software, sometimes known as malware, is software intentionally designed to carry out destructive actions as intended by an attacker. Malwares are categorized into many types based on their behavior, propagation, and infection methods. These types include viruses, worms, Trojan Horses, root-kits, spyware, backdoors, botnets, and adware, among others.The user's text is [4]. Each day, a multitude of novel malwares are being created, while old malwares are continuously adapting and developing in their composition, making them more challenging to identify.

  

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025
DOI: 10.17148/IJARCCE.2025.14225

According to the latest report by Symantec on online threats, an astounding 317 million novel forms of malware were identified. Given the growing number of new samples on a daily basis, it is essential to use automated tools and techniques for malware analysis in order to differentiate between harmful and harmless code. The majority of commercial anti-virus software use a signature-based approach for classifying malware. This approach involves comparing unidentified malwares with a repository of recognized harmful software in order to determine if the file is a malware or harmless. A signature serves as a distinctive identifier for a binary file. The identification of malware is accomplished by the use of static analysis, dynamic analysis, or hybrid analysis techniques, and thereafter stored inside a signature database. An inherent drawback of this approach is the need for regular updates to the signature database due to the rapid proliferation of new malwares on a daily basis [5-6].

The Internet of Things (IoT) facilitates the connection between the physical world and the computer world. With the growing use of technology, the concerns over privacy are also on the rise. Various forms of assaults, including as spoofing, DDoS attacks, jamming, malware, and eavesdropping, are emerging as significant dangers. Compact IoT devices are limited in their ability to perform computationally demanding and time-sensitive security tasks. Currently, IoT devices use authentication methods to safeguard against identity-based attacks, ensuring that source nodes are correctly recognized. Additionally, access control measures, secure offloading mechanisms, and malware detection systems are implemented to avoid privacy breaches. These approaches are rarely used for tiny IoT devices such as outdoor sensors, resulting in the lack of recognition of spoofing attacks on them [7]. Machine learning algorithms may be used on both tiny and big IoT devices. The following methods are included: Supervised Learning encompasses several algorithms such as support vector machine, naïve Bayes, neural network, deep neural network, random forest, and K closest neighbor. These algorithms are used to analyze network traffic or app traces of IoT devices and create classification or regression models [8-10].

## LITERATURE SURVEY

As stated by the author in [11], the primary issues in WSNs and IoT are minimizing power use to extend network lifespan and enhancing security. The ESRA model proposed in reference [9] utilizes Mamdani Fuzzy logic to determine an energy efficient path for communication. The system chooses the optimal path by taking into account the values of Quality of Service (QoS) indicators. It is feasible to change the location of sink nodes, and the new route is established by determining the position of the present sink node. This method exhibits minimal power consumption by using path dependability to establish routes. Cluster-based routing methods result in higher energy consumption owing to the inclusion of several intermediary nodes along the communication path.

The authors in [12] have used a double level unequal clustering algorithm (DLUC) to mitigate the problem of heightened power consumption in clustering algorithms. This algorithm effectively distributes the load of traffic across the clusters. Since the cluster heads don't change how information moves between the nodes, the number of clusters and nodes that are connected to the transmission line has gone down. By using accurate time intervals for data framing and making the best use of available bandwidth, you can avoid congestion and keep interference between control packets to a minimum. Both of these plans are needed to keep traffic from building up. Also, networks may use less energy if data loss happens less often. It's important to keep in mind that this method doesn't take into account movement or the different sizes of clusters, which are both big reasons why networks use more power.

This section's goal is to show a number of methods that have been created to keep track of the location information of either the source node or the sink node, and sometimes both nodes, while understanding how an Internet of Things application works. Not only have we looked into how security methods affect quality of service (QoS) measures like speed, end-to-end delay, and packet delivery ratio, but we have also looked into how they affect energy economy. Only the letter "A" has been entered by the user. The physical details of the starting point are shown below. Making sure that networks are safe is now a very hard problem for researchers, mostly because of the source location privacy (SLP) problem. Without Source position Privacy (SLP), it becomes simpler to determine the position of source nodes and get access to the data before it is sent via the communication line [13]. The path constructed by the sensors comprises a source node, many intermediate nodes, and sink nodes. These intermediary nodes use hopping techniques to send data packets. Research suggests that attackers may readily ascertain the source location, even with partial knowledge of the locations of nodes in the current path being used [14-15]. Therefore, it is essential to create SLP algorithms in order to protect IoT networks from security intrusions.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

## PROPOSED METHODOLOGY

The proposed methodology can be elucidated using the block diagram depicted in Figure 1 and Figure 2. It is evident from these diagrams that no existing integrated algorithm has been investigated that can enhance both network security and the quality of service (QoS) of the entire network. As a result, our study focuses on a complex field that encompasses several elements, such as addressing security concerns like anonymity, route security, and data security, as well as enhancing Quality of Service (QoS) via activities like route selection and improving node performance. Owing to the extensive range of domain choices, algorithm integration often presents challenges. Hence, an additional need for doing this study is to create a unified algorithm that can effectively address the two fundamental elements of the wireless network, namely security and QoS. The K-Nearest Neighbors (KNN) algorithm is often used for malware identification and prevention in machine learning. However, this study aims to show that it can also be used for QoS optimization and security improvement in a wireless network. By doing so, it will boost the overall performance of the network.

**Case -1-** VANET is a network that may expand without limits and is not affected by the amount of nodes it contains. VANET facilitates communication between vehicles (V2V) and between vehicles and infrastructure (V2I). Both types of communications include nodes collecting information from other nodes or from an RSU, which must be reliable. Vehicular Ad Hoc Networks (VANETs) have distinct security requirements to ensure effective communication among vehicles. VANETs are specifically designed for nodes that have high mobility and an unlimited network topology. They are intended to convey time-critical information securely. Routing protocols may be classified into two categories for communication: Proactive and Reactive. AODV is a routing mechanism that operates on a demand-based and reactive basis. AODV establishes a route only when there is a specific need. The system utilizes a route request-response method to make a request for route finding. It then establishes the ideal path based on the returned answer. In the V2I communication environment, the RSU that the vehicle passes by may often have link disconnections with the 1-hop vehicle on the path to the destination vehicle due to vehicle movement. In this scenario, AODV restores the disrupted connection by instructing the RSU to transmit a route error (RERR) message to the predecessors. However, in the context of the vehicular network, the RSU lacks prior information about routes, so it must actively search for a new path to reach the target vehicle. This technique is onerous in the vehicle network due to its restricted wireless connection capacity.

We suggest implementing a backup route mechanism inside the coverage area of the RSU that was passed by, with the aim of minimizing the frequency of route recoveries. The process of creating an alternative route from the previously visited RSU

## ANALYSIS AND DISCUSSIONS

An analysis of the papers examined in the review indicates that while the routing algorithms can effectively preserve some of the QoS parameters such as end-to-end delay, throughput, and packet delivery ratio, a significant number of location privacy algorithms struggle to strike a balance between energy consumption and security. The majorities of the papers we have examined have effectively enhanced the security of source or sink nodes. However, the inclusion of fake packets in the route has resulted in higher energy consumption. An inverse relationship exists between energy usage and network longevity.

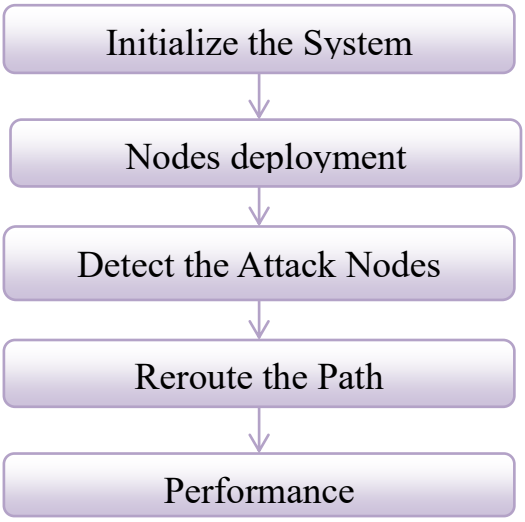


Fig.1 Simulation Flow Diagram

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

The network lifespan is diminished due to the heightened energy consumption resulting from the adoption of privacy algorithms. This presents a significant difficulty in implementing security and privacy algorithms for IoT devices with limited energy resources.

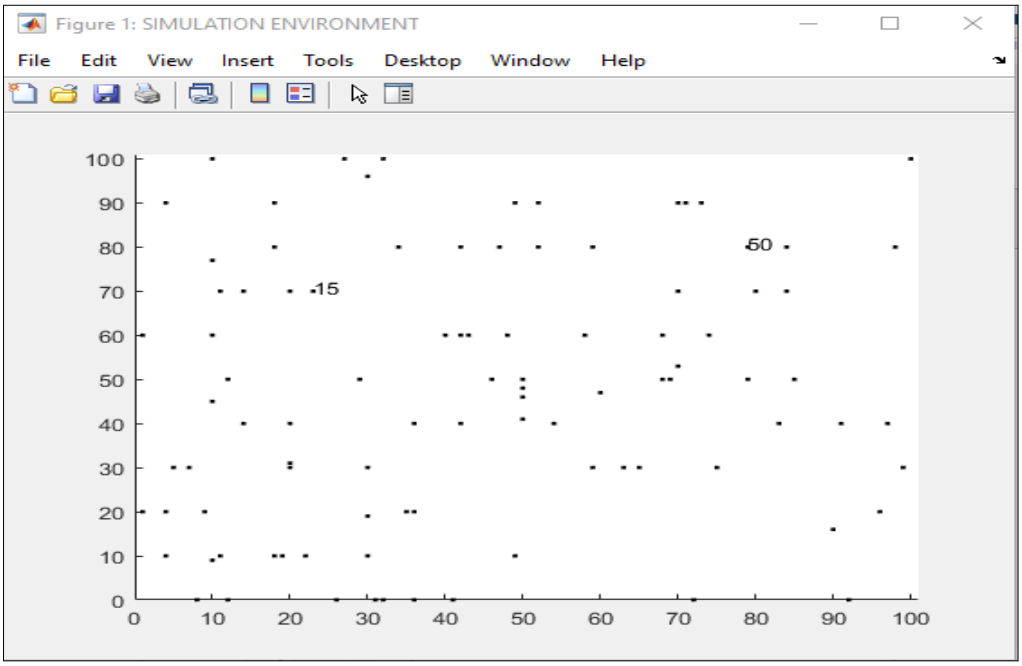


Fig.2 Initialization Network

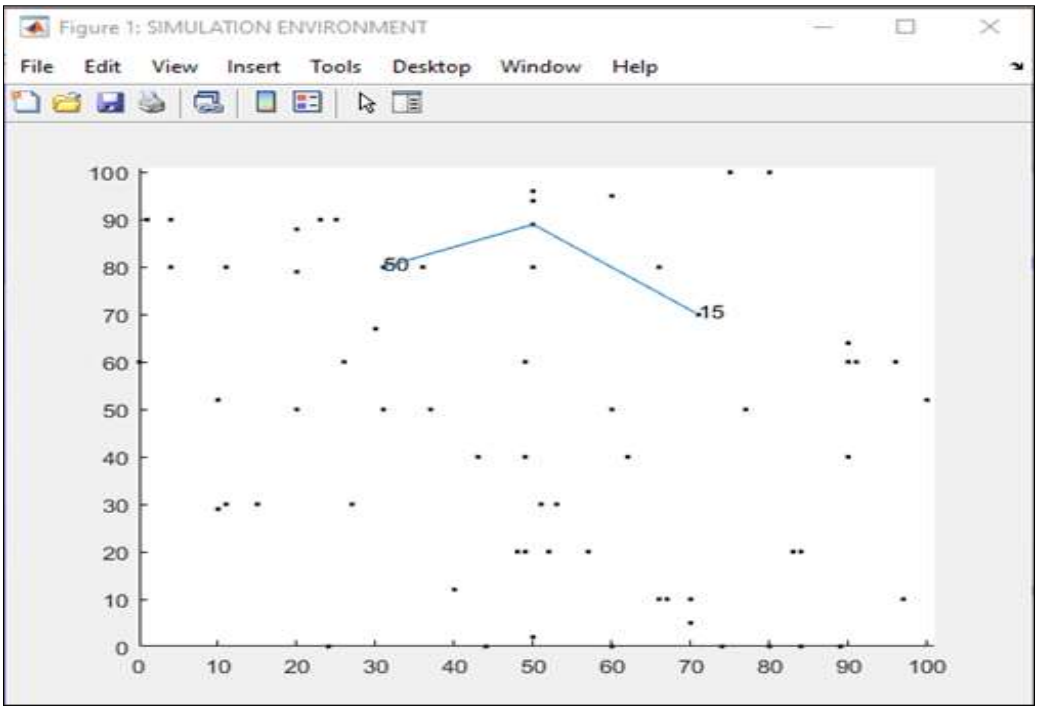


Fig.3 Node To Node Data Transfer

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

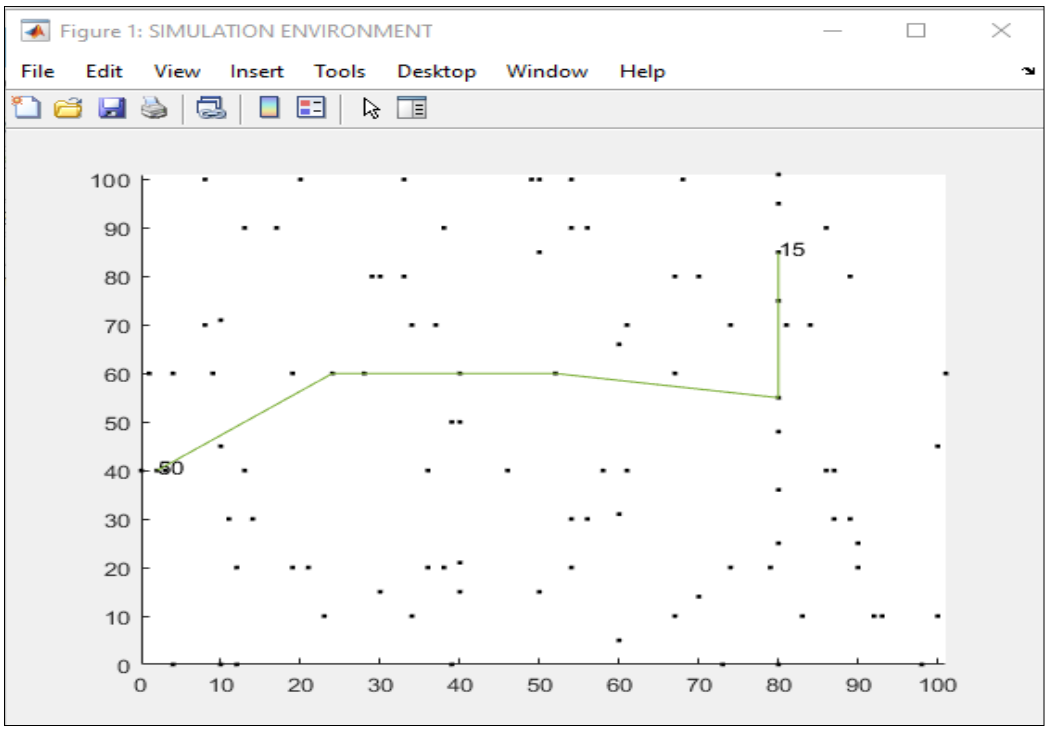


Fig.4 AODV Paths for Each Change in Vehicle Position Into a Structure

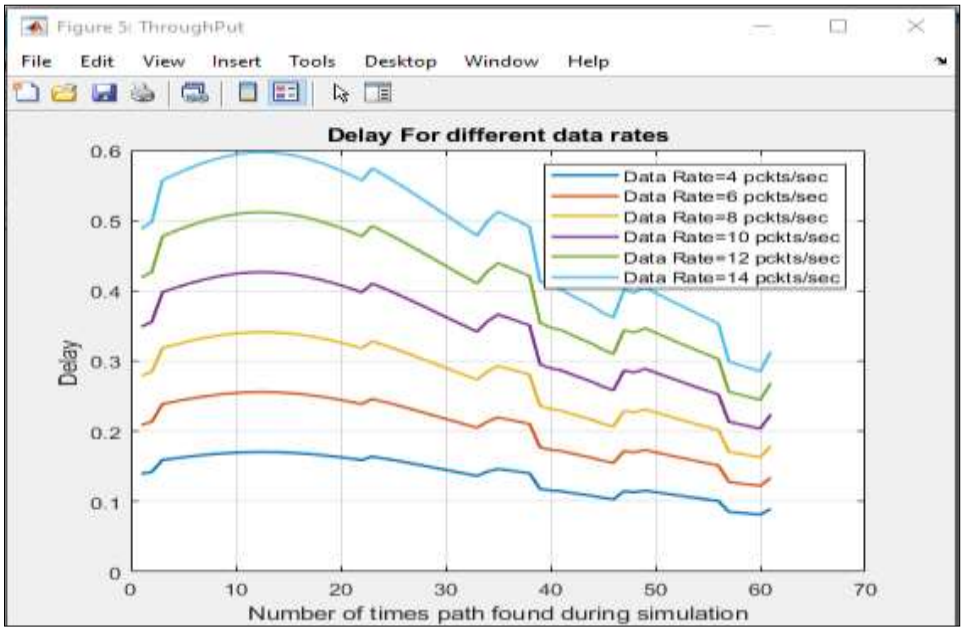


Fig.5 Delay for Different Data Rates

Source node -> path node-> destination node

Path node, we have 100 node the data transmit from source to destination through nearest available nodes the data delay transmission through path showing in the fig. 5

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

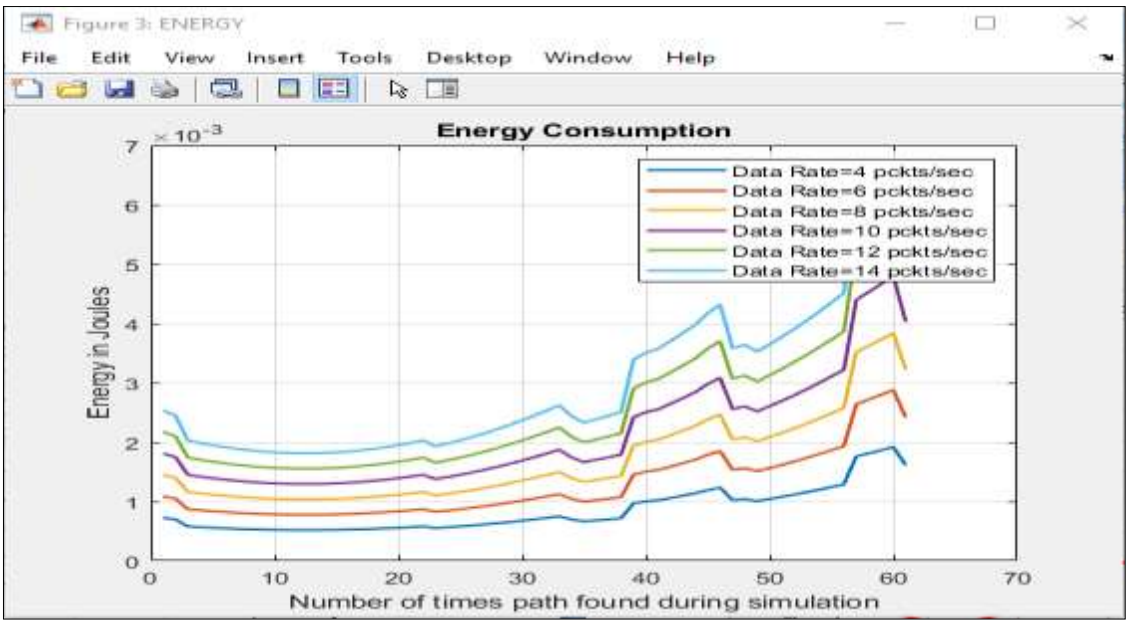


Fig.6 Energy Consumption for Different Data Rates

The data transmit from source to destination through nearest available nodes the data energy consumption for different data rates transmission through path showing in the fig. 6


Fig.7 Number of Path Found During Simulation

The data transmit from source to destination number of path found during simulation showing in the fig.7

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

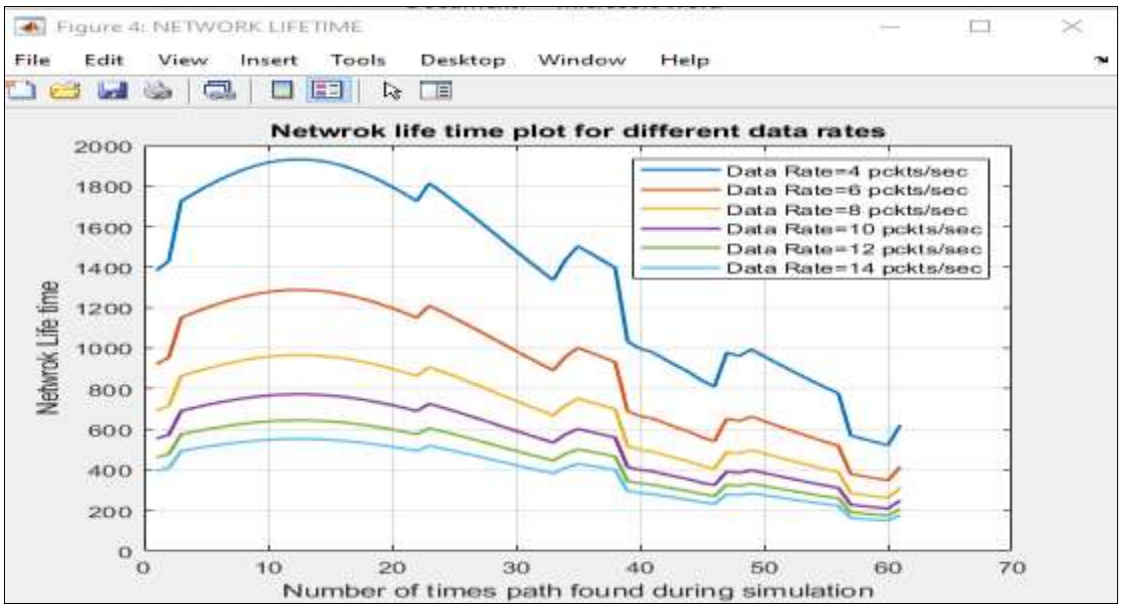


Fig.8 Network Life Time for Different Data Rates

The data transmit from source to destination through nearest available network life time for different data rates while data transmission through path showing in the fig. 8

**Case-2**

**Malware Detection** -As the picture shows, the system will start by setting up a normal wireless network. This network will use standard algorithms to improve service quality and make sure the network is safe. When one of the performance evaluation metrics is not met, both this security performance and the QoS performance will be fine-tuned. As a direct result of the proposed work, the following things are likely to happen: showing in the fig. 9

- Improved QoS for any kind of wireless network
- Adaptive security for wireless networks
- A KNN algorithm will be used for performing Malware detection
- Flexibility in terms of security and QoS of the network

Employing machine learning enables the network to constantly adjust its configuration, ensuring it remains up-to-date with the most recent security and Quality of Service (QoS) capabilities. The enhancement of Quality of Service (QoS) will lead to an improvement in the response rate for security assaults.

**Sink Node Location**- The nodes situated at the receiving end of the networks are referred to as sink nodes. Privacy methods for sink placement are crucial for safeguarding sink nodes from attackers. Without sink location privacy techniques, attackers may easily determine the precise position of the sink in order to get access to the data packets at the receiving end.

**Source and Sink Location**- In their study, the authors used a K-means clustering method [27] to maintain the spatial information of both the source and destination nodes in IoT-based Wireless Sensor Networks (WSNs). To provide protection, several counterfeit nodes are used for both the source and destination nodes, but the authentic source and sink nodes remain undisclosed. A clustering strategy is used to transmit data packets to many sink nodes. This method ensures the integrity of data transfer and preserves the length of the routing route. By transmitting the actual packets via the quickest path, the delay has been minimized. The suggested protocol demonstrates improved safety time values, however it does not prove to be energy efficient owing to the proliferation of counterfeit sink nodes.

**Learning-Based IoT Malware Detection:** IoT devices may use supervised learning methods to assess the runtime behaviors of applications in order to identify malware. The K-NN based malware detection algorithm categorizes network traffic by assigning it to the class that has the highest number of objects among its K closest neighbors.

**K-NN** K-closest neighbor (KNN) is an unsupervised data categorization technique that assigns labels to new samples based only on their proximity to the nearest neighbors [2][3]. The k-NN approach is characterized by its simplicity, intuitiveness, and ease of fast implementation. It is considered one of the most straightforward and widely used algorithms in machine learning. The user's text is incomplete and does not convey any information. In KNN-CV, the training data

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

set is divided into three parts: the training data, the cross-validation data, and the testing data. When using this algorithmic approach, we have limitations in maximizing the use of the training dataset. K-Fold KNN is a method that maximizes the use of available data.

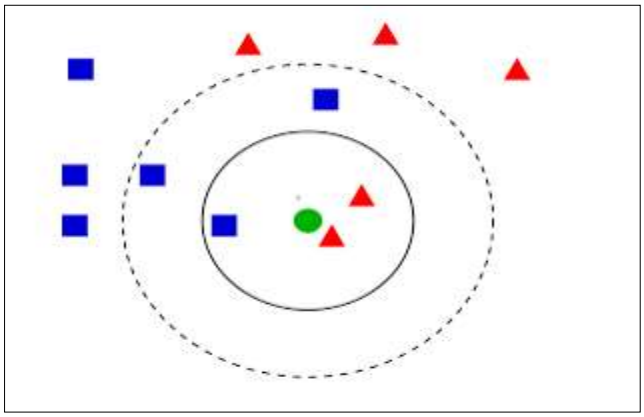

Fig. 10: An abstract of KNN

• Partition the available training data set into two subsets: one for training purposes and the other for testing purposes. Our KNN model's accuracy will be determined only using testing data.
• Now divide the Training data into K equal halves, repeating this process K times.
• Now, let's allocate three portions for training and one part for assessment. Modify this arrangement to generate potential instances for Every K values in order to get the Optimal K.

**Data evaluation** The research use k-Fold Cross Validation as the assessment data. In the process of cross validation, the dataset is partitioned into k folds. During each iteration, every fold is used once as test data and the leftover fold is utilized as training data. This procedure is continued until all the data has been reviewed.

After getting the distribution of training data and test data from evaluating the model using k-Fold Cross Validation, the data is categorized using k-NN to determine the correctness of the model being constructed. This process is iterated until the k-Fold reaches a value of 10 or until the maximum degree of accuracy is achieved. Once the k-FCV technique has been used to evaluate and determine the training data and test data, the subsequent stage involves commencing the data classification process using the k-NN method. The k-NN approach involves many research steps.

- Calculate the numerical value of k.
- Compute the Euclidean distance between the test data and the training data in the dataset.
- Show the Euclidean distance in increasing order.
- Determine the shortest distance of k.

The outcomes of data categorization using the k-NN technique


Fig.11 test result dataset

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

This module is of utmost importance since it focuses only on training our model to accurately predict the kind of malware, as stated in the dataset module. We used two renowned modeling approaches to train our model on the provided dataset, which consists of several characteristics, in order to predict the nature of harmful material. Subsequently, we compared the results obtained from both models after training them on the specific dataset using the KNN Classifier. The KNN model utilizes the clustering approach to partition the whole dataset into a predetermined number of clusters, with each cluster having a centroid as its cluster head. During each iteration, the centroid of a certain cluster is updated when a new node is added to the cluster. Various distance algorithms, such as those used for estimating the distance between instances, are used. i. The Euclidean Distance: This approach is mostly used for input variables that are expressed as real numbers and may be represented by the following mathematical formula:

$$\text{Euclidean Distance}(x, xi) = \text{sqrt}\ (\ \text{sum}(\ (xj - xij)\text{^}2\ )\ )$$

Hamming Distance: It is helpful in calculating distance between binary valued input- variables.

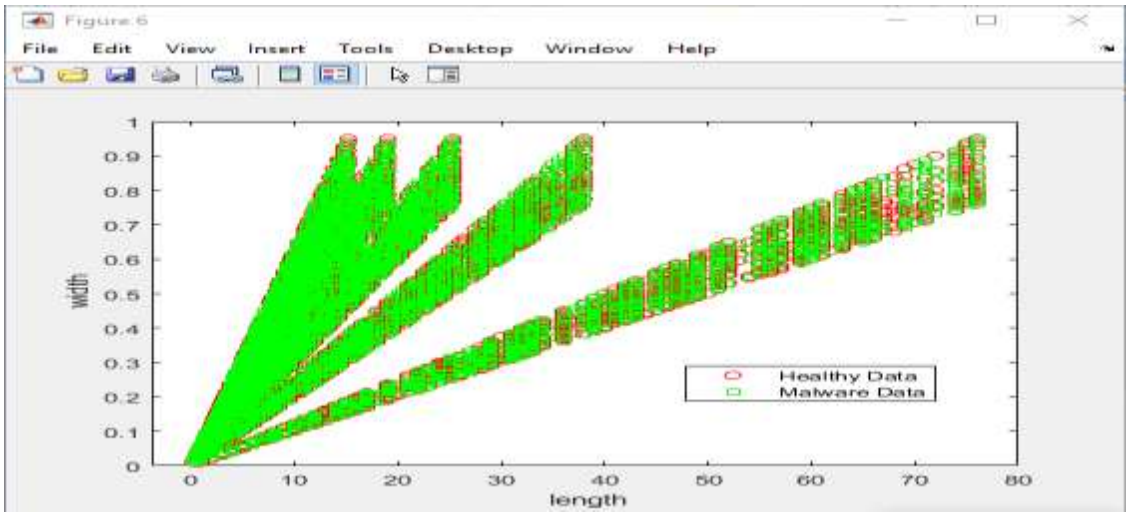


Fig.12 traning of malware and heathy data


Fig.13 seprate the malware and healthy data

In the fig x axis showing the iteration and Y axis showing the different category set of datas

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

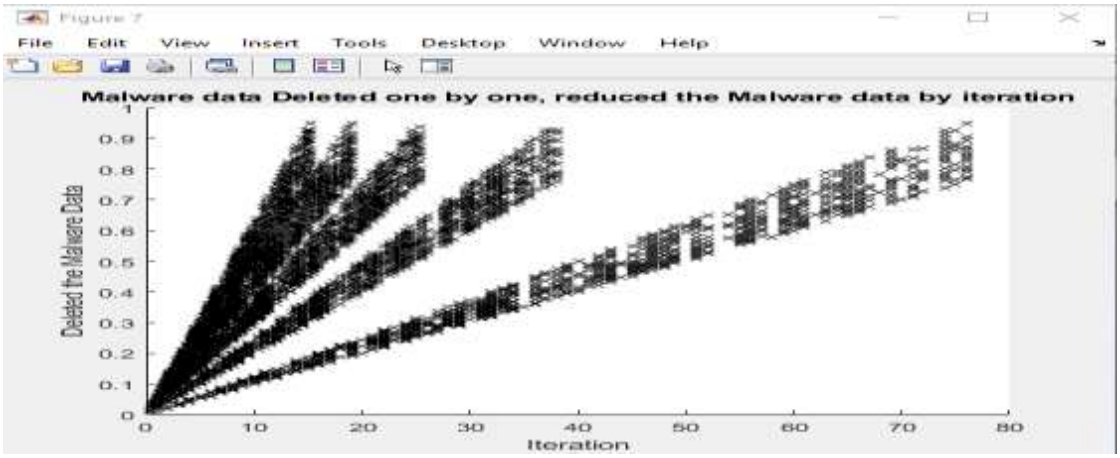


Fig.14 malware data delation

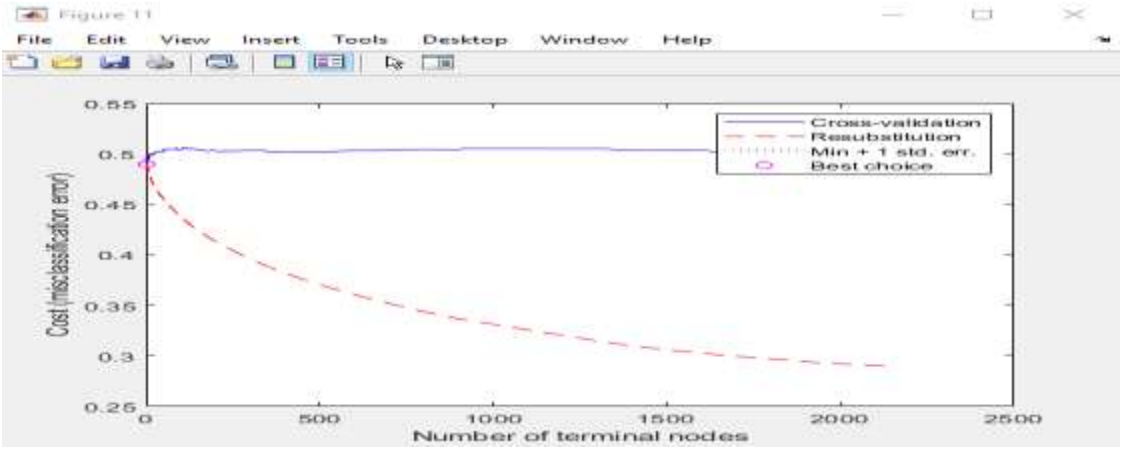


Fig.15 cross validation

It enhances our data use and provides us with much more insights into the effectiveness of our algorithm. Cross-validation is a technique that involves repeatedly splitting a small data sample into subsets to assess the performance of machine learning models. The user's input specifies a solitary parameter, denoted as "k," which determines the quantity of groups that a certain data sample will be divided into. The k-fold cross-validation entails iteratively doing the cross-validation technique numerous times and calculating the average outcome across all folds from each iteration. This implies that the outcome is anticipated to be a more precise approximation of the actual unknown mean performance of the model on the dataset, as determined by the standard error calculation.

Table 1 IoTQOS Result

| **Parameters values** | **Parameters values** |
|---|---|
| Average PDR | 274.825140 |
| Average Through | 206.118855 |
| Average Delay | 206.118855 |
| Average Energy | 84.594327 |

The Internet of Things (IoT) is an emerging technology that is undergoing significant advancements to provide enhanced services to society. This survey article elucidates the roles of the levels in the Internet of Things (IoT) architecture, while the taxonomy delineates the characteristics that determine the quality of services. The metrics pertaining to service quality improvement were also provided. In the future, it is possible to expand this by suggesting novel methodologies to tackle issues such as unreliable connections, traffic congestion, node malfunctions, data loss, limited node lifespan, and network congestion. This will ultimately improve the Quality of Service in the Internet of Things (IoT). Only a limited number of measures were considered in this study. Elaborate explanations of the measures may be provided at a later time.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

The Internet of Things (IoT) is a technology that is growing quickly and is going through a lot of changes right now so that people can get better services. In this survey report, the architecture explains what each layer of the Internet of Things does, and the taxonomy explains the factors that determine the quality of the services. Also, the metrics that need to be worked on to improve the quality of the services as a whole were given. In the future, this can be expanded by suggesting new ways to deal with problems like unstable links, traffic, node failure, packet loss, lifetime of node, congestion, and other similar problems in order to improve Quality of Service in the Internet of Things (IoT). Only a few different metrics were looked at in this work. In the future, the metrics can be explained in greater detail.

Table 2 Compare the Proposed Results with Existing Work

| Parameters | Proposed Work | Existing Work[1] |
|---|---|---|
| | AODV-KNN | RL-QRP |
| Avg Delay | 290.65 | 351 |
| Avg Energy | 173.05 | 196.3 |
| Avg PDR | 144.15 | 136.7 |
| Avg Through | 108.11 | 136.7 |

## CONCLUSION

The suggested system successfully enhances source to destination security without impacting the network's lifespan. However, there is still potential for decreasing energy usage in both the transmission and reception paths. Research on algorithms for maintaining the positions of source and sink nodes suggests that the usefulness and adoption of IoT applications by customers depend on achieving a balance between quality of service, energy efficiency, and security. To fulfill the security demands of IoT networks, it is essential to ensure data security and safeguard the location of transmitting and receiving nodes. The limited energy capacity of battery-powered IoT devices significantly affects the practicality of implementing security algorithms. We have enumerated some aspects that impact the longevity and security of IoT networks. Fog computing, cognitive radio networks, and machine learning are viable solutions for addressing the quality of service (QoS) and security challenges associated with the Internet of Things (IoT). Service providers may use these technologies for real-time applications after they have identified the needs of the end customers. The degree of security differs among applications, nevertheless, if breached or attacked by adversaries, it may result in significant losses for the end users. Insufficient security in healthcare apps may jeopardize an individual's life and even represent a danger to national security if military applications fail to adequately protect their IoT equipment. Our next study aims to use machine learning techniques to enhance the security and quality of service (QoS) in Internet of Things (IoT) networks.

## REFERENCES

[1]. Manisha Bhatnagar Dolly Thankachan(2021) Identifying the Effects of Security Measures on QoS Variations for IoT Network: An Application Perspective Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021). IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

[2]. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. “Internet of Things security: A survey”. In: Journal of Network and Computer Applications 88 (2017),pp. 10–28.

[3]. C. Alcaraz, P. Najera, J. Lopez, and R. Roman. “Wireless sensor networks and the internet of things: Do we need a complete integration?” In: 1st International Workshop on the Security of the Internet of Things (SecIoT’10). 2010.

[4]. J. Arkko, D. Thaler, and D. McPherson. “IETF RC 7452: architectural considerations in smart object networking”. In: IETF, Fremont, US (2015).

[5]. M. A. Bhabad and S. T. Bagade. “Internet of things: architecture, security issue and countermeasures”. In: International Journal of Computer Applications 125.14 (2015).

[6]. G. Breed. “Wireless ad hoc networks: basic concepts”. In: High frequency electronics 1 (2007), pp. 44–47.

[7]. L.-H. Chang, T.-H. Lee, S.-J. Chen, and C.-Y. Liao. “Energy-efficient oriented routing algorithm in wireless sensor networks”. In: 2013 IEEE International Conference on Systems, Man, and Cybernetics. IEEE. 2013, pp. 3813–3818.

[8]. M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally. “Internet of things (iot): Research, simulators, and testbeds”. In: IEEE Internet of Things Journal 5.3 (2017), pp. 1637–1647.

[9]. A. Chhabra, V. Vashishth, A. Khanna, D. K. Sharma, and J. Singh. “An energy efficient routing protocol for wireless internet-of-things sensor networks”. In: arXiv preprint arXiv:1808.01039 (2018)

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 2, February 2025

DOI: 10.17148/IJARCCE.2025.14225

[10]. HamidiĞ Alaoui, Z, El Belrhiti El Alaoui, A. FMĞ MAC: A fastĞ mobility adaptive MAC protocol for wireless sensor networks. Trans Emerging Tel Tech. 2020; 31:e3782. https://doi.org/10.1002/ett.3782

[11]. Kumar, S, Sharma, B, Singh, AK. An efficient algorithm for backbone construction in cognitiveradionetworks.IntJCommunSyst.2020;33:e4345. https://doi.org/10.1002/dac.4345

[12]. DadashiGavaber, Morteza, Rajabzadeh, Amir, "BADEP: Bandwidth and delay efficient application placement in fog-based IoT systems", Transactions on Emerging Telecommunications Technologies, 2020

[13]. Gomes, PH, Krishnamachari, B. TAMUĞ RPL: Thompson sampling based multichannel RPL. Trans Emerging Tel Tech. 2020; 31:e3806.

[14]. H. Liang, S. Yang, L. Li, and J. Gao. "Research on routing optimization of WSNs based on improved LEACH protocol". In: EURASIP Journal on Wireless Communications and Networking 2019.1 (2019), p. 194.

[15]. K. L. Lueth. IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year. https://iot-analytics.com/iot-2019-in-review/. Accessed: 2020-3-13.

[16]. K. L. Lueth. IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally. https://iot-analytics.com/iot- platform- companies- landscape2020/. Accessed: 2020-04-09

[17]. K. L. Lueth. The Effect of the Internet of Things on Sustainability. https://iotanalytics.com/effect-iot-sustainability/. Accessed: 2020-04-09.

[18]. K. L. Lueth. Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. https : //iot analytics.com / internet -of - things -definition/. Accessed: 2020-3-13.

[19]. Z. Magubane, P. Tarwireyi, and M. O. Adigun. "Evaluating the Energy Efficiency of IoT Routing Protocols". In: 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC). IEEE. 2019, pp. 1–7.

[20]. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. "Internet of things (IoT) security: Current status, challenges and prospective measures". In: 2015 1 International Conference for Internet Technology and Secured Transactions (ICITST) IEEE. 2015, pp. 336–341.

[21]. M. A. Mahmud, A. Abdelgawad, and K. Yelamarthi. "Energy efficient routing for Internet of Things (IoT) applications". In: 2017 IEEE international conference on electro information technology (EIT). IEEE. 2017, pp. 442–446.

[22]. R. Minerva, A. Biru, and D. Rotondi. "Towards a definition of the Internet of Things (IoT)". In: IEEE Internet Initiative 1.1 (2015), pp. 1–86.

[23]. F. Muhammad, W. Anjum, and K. S. Mazhar. "A critical analysis on the security concerns of internet of things (IoT)". In: International Journal of Computer Applications (0975 8887) 111.7 (2015).

[24]. A.-S. K. Pathan and C. S. Hong. "A secure energy-efficient routing protocol forWSN". In: International symposium on parallel and distributed processing and applications. Springer. 2007, pp. 407–418

  