FMDB *Transactions on Sustainable Computing Systems*

IoT-SecNet: A Trust-based Framework for Enhancing Security in IoT Communications and Network Layer Protocols

R.P. Pranav[1,*], R.P. Prawin[2], P. Paramasivan[3], T. Shynu[4], R. Subhashni[5]

[1,2]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[3,4]Department of Research and Development, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
[5]Department of Computer Science and Applications, St. Peter's Institute of Higher Education and Research, Chennai, Tamil Nadu, India.
pranavramesh2004@gmail.com[1], prawinrp2002@gmail.com[2], paramasivanchem@gmail.com[3], shynu469@gmail.com[4], subhashniraj2018@gmail.com[5]

Abstract: The Internet of Things (IoT) integrates cloud computing, big data, and data mining to become a vital 21st-century technology. IoT uses hardware, software, and communication protocols to connect and share data amongst devices. However, IoT's increasing usage raises security concerns, especially due to its ubiquitous communication infrastructure. IoT ecosystems depend on communication protocols to connect hardware and application software and enable real-world device deployment. Due to their openness, these protocols are vulnerable to DoS, DDoS, and buffer overflow attacks despite their importance. Thus, a complete framework to protect these protocols at the communication and network layers is needed. This study proposes an IoT-SecNet (Secure Network), a Trust-based Framework to improve security across IoT communication protocols. This framework verifies sensor data and sends request packets for processing, ensuring security and effective traffic management across IoT layers. Through experimental assessments, we show a 90% accuracy rate in identifying assaults and compare it to existing security solutions. Our architecture protects against threats by maintaining high communication layer protocol throughput and low delay.

Keywords: Internet of Things (IoT); Trust-Calculation Framework; Communication Protocols; Cyber Threats; Sensor Data Evaluation; Traffic Management; Network Security; Denial of Service (DoS); Distributed Denial of Service (DDoS).

Received on: 29/01/2024, **Revised on:** 18/03/2024, **Accepted on:** 05/05/2024, **Published on:** 03/06/2024

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCS

DOI: https://doi.org/10.69888/FTSCS.2024.000201

Cite as: R.P. Pranav, R.P. Prawin, P. Paramasivan, T. Shynu, and R. Subhashni, "IoT-SecNet: A Trust-based Framework for Enhancing Security in IoT Communications and Network Layer Protocols," *FMDB Transactions on Sustainable Computing Systems*., vol. 2, no. 2, pp. 96–106, 2024.

1. Introduction

The Internet of Things (IoT) refers to a network of smart technologies connected to the Internet, offering diverse services based on user needs. It holds the potential to save lives during medical emergencies, enhance daily living and work efficiency, and achieve tasks autonomously by gathering various types of data from the environment for instant processing and smart decision-making. This data is then sent to the cloud for further analysis using communication software. IoT finds applications in various fields, such as smart homes, healthcare, cities, parking systems, industries, and even wearable tech. However, despite its many

[*]Corresponding author.

benefits, security remains a major concern in the realm of IoT [10]. Security vulnerabilities in IoT devices have been exposed, making them attractive targets for cyber attackers seeking unauthorized access to device data for malicious purposes. IoT devices often have limited storage and processing capabilities, with manufacturers prioritizing new features and cost-efficiency over security [11].

Consequently, security risks are often overlooked or treated as an afterthought during product development, resulting in devices with attractive features but inherent security flaws, making them prime targets for cybercriminals. IoT devices are susceptible to various types of attacks, including spoofing, Denial of Service (DoS), and replay attacks, primarily due to their resource constraints [12]. SCADA and 6LoWPAN protocols, being among the most widely used in IoT, are particularly important to secure against vulnerabilities. Therefore, our focus is on safeguarding these protocols to ensure the integrity and security of IoT systems [13].

As the most widely used IoT protocol, our main focus is to protect SCADA and 6LoWPAN protocol vulnerabilities.

- We first analyzed the vulnerabilities of different software, such as SCADA, CoAP, MQTT, 6LoWPAN, LORAWAN, and RPL protocol. We revealed the major causes that are ignored during protocol implementation and that affect the security.
- Based on the analysis, we proposed a secure framework for IoT Communications and Network Layer Protocols where
- Firstly, the data of all the users is collected in the initial layer, i.e., the Things Layer.
- Secondly, the trust value is calculated in the communication layer to check whether the user is verified and legitimate.
- Lastly, if the trust value of the user is less than the predefined trust value, i.e., 0.5, then the user can access the cloud for storage and processing, or else the access will be denied.

The rest of the paper is structured as follows: Section 2 presents the related work of a selection of recently exposed vulnerabilities in IoT devices, along with existing solutions proposed for detecting and protecting the vulnerabilities. Section 3 deals with the framework for the security of IoT communication and network layer. Section 4 describes the experiments and results of the proposed framework. Finally, Section 5 concludes the paper and reports further work on the topic.

2. Literature Review

Gan et al. [1] conducted a comprehensive analysis of Internet of Things (IoT) security, presenting their findings at the International Conference on Internet Technology and Applications. Their research explores various facets of IoT security, focusing on vulnerabilities within the IoT landscape and potential mitigation strategies. As IoT devices proliferate across different sectors, understanding security risks becomes crucial for both manufacturers and consumers. Gan et al. [1] likely investigate the challenges posed by unsecured IoT devices, data breaches, and unauthorized access, providing valuable insights into effective security measures. By addressing these vulnerabilities, their study contributes to the ongoing discourse surrounding IoT security, aiming to enhance the overall security framework and protect users' sensitive information. Moreover, the analysis likely emphasizes the need for a multifaceted approach to security, combining technical solutions with policy frameworks and user education. The findings of their research serve as a vital resource for stakeholders looking to strengthen their IoT security strategies, ensuring a more secure and resilient IoT ecosystem.

Zhang et al. [2] present a thorough examination of IoT security in their paper showcased at the IEEE Fourth International Conference on Data Science in Cyberspace. Their study delves into contemporary research on IoT security, highlighting the significance of addressing emerging threats within the rapidly evolving digital landscape. By analyzing various security challenges, including data integrity, authentication, and privacy concerns, Zhang et al. [2] provide insights into the current state of IoT security and its implications for future developments. Their work likely discusses potential countermeasures that can enhance the security posture of IoT systems, including advanced encryption methods, machine learning techniques for anomaly detection, and secure communication protocols. Additionally, the research may identify gaps in current security frameworks and suggest directions for future research to tackle these issues effectively. The insights garnered from their study contribute to a deeper understanding of IoT security challenges, ultimately guiding practitioners and researchers in developing more robust and resilient IoT systems.

Tawalbeh et al. [3] make significant contributions to the discourse on IoT privacy and security through their study published in Applied Sciences. Their research addresses the pressing challenges posed by privacy and security issues in IoT systems, focusing on the importance of safeguarding user data in an interconnected world. Tawalbeh et al. [3] likely investigate various threats to privacy, including data breaches, unauthorized access, and surveillance risks, proposing solutions to enhance the overall security and privacy of IoT deployments. Their study may emphasize the necessity for comprehensive security policies and technologies that ensure user trust and compliance with data protection regulations. Furthermore, the research likely explores the role of encryption, authentication mechanisms, and secure data storage solutions in mitigating privacy risks. By

providing practical recommendations and insights, Tawalbeh et al. [3] contribute to the development of a safer IoT environment, highlighting the importance of addressing privacy concerns alongside security challenges to foster user confidence in IoT technologies.

Husnain et al. [4] contribute to the literature on IoT security with their study published in Sensors, focusing on the prevention of vulnerabilities in the MQTT protocol through the implementation of an IoT-enabled intrusion detection system. Their research aims to address the specific security concerns associated with MQTT, a widely used protocol for lightweight messaging in IoT applications. Husnain et al. [4] likely examine the potential vulnerabilities that can be exploited by attackers, such as unauthorized access and data interception, emphasizing the need for robust security measures. By developing an intrusion detection system tailored for IoT environments, their study provides valuable insights into enhancing the security of IoT systems against potential threats targeting MQTT vulnerabilities. The research may also explore the integration of machine learning techniques for anomaly detection, allowing for real-time identification of suspicious activities. Overall, Husnain et al. [4] 's work contributes significantly to the understanding of protocol-specific vulnerabilities and the development of effective security strategies to safeguard IoT communications.

Zhang et al. [5] offer valuable insights into ongoing challenges and research opportunities in IoT security in their work presented at the IEEE 7th International Conference on Service-Oriented Computing and Applications. Their study addresses the evolving landscape of IoT security, highlighting persistent challenges such as data breaches, device authentication, and secure communication. By analyzing these issues, Zhang et al. [5] identify critical areas for future research, aiming to develop innovative solutions to enhance the security of IoT systems. Their research likely discusses emerging trends in IoT security, including the adoption of blockchain technology for secure transactions and the use of artificial intelligence for threat detection and prevention. Furthermore, the study may explore the importance of collaboration between industry stakeholders, researchers, and policymakers in addressing these challenges effectively. By providing a comprehensive overview of current issues and future directions in IoT security, Zhang et al. [5] contribute to the ongoing discourse on developing secure and resilient IoT ecosystems.

Kasinathan et al. [6] investigate denial-of-service (DoS) detection in 6LoWPAN-based Internet of Things (IoT) systems in their study presented at the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Their research focuses on identifying methods for detecting and mitigating DoS attacks that target 6LoWPAN networks, which are commonly used in IoT applications due to their low power and bandwidth requirements. Kasinathan et al. [6] likely examine various detection techniques, including signature-based, anomaly-based, and hybrid approaches, to enhance the security of IoT deployments. By providing insights into the effectiveness of different detection strategies, their study aims to improve the resilience of IoT systems against DoS attacks, which can severely disrupt network operations and degrade service quality. Additionally, the research may explore the integration of real-time monitoring tools and response mechanisms to mitigate the impact of such attacks. Overall, Kasinathan et al. [6] contributions are essential for enhancing the security of 6LoWPAN networks and ensuring reliable IoT operations in various applications.

Ghazanfar et al. [7] present "IoT-flock," an open-source framework for IoT traffic generation, in their work showcased at the International Conference on Emerging Trends in Smart Technologies (ICETST). Their research focuses on the development of a versatile tool for simulating IoT traffic patterns, which can aid in the evaluation and testing of IoT systems and protocols. Ghazanfar et al. [7] likely discuss the importance of generating realistic traffic scenarios to assess the performance and security of IoT applications. By providing a framework that allows researchers and developers to simulate various traffic conditions, their study contributes to the advancement of testing methodologies for IoT systems. The open-source nature of IoT-flock encourages collaboration within the research community, fostering innovation and enabling the development of more robust IoT solutions. Additionally, the research may explore the implications of IoT traffic patterns on network performance and security, emphasizing the need for effective monitoring and management strategies. Overall, Ghazanfar et al. [7] 's work plays a significant role in enhancing the reliability and security of IoT systems through improved testing and evaluation methods.

Lin et al. [8] conducted a comprehensive survey on the Internet of Things (IoT) in their work published in the IEEE Internet of Things Journal. Their study examines various aspects of IoT, including architecture, enabling technologies, security, privacy, and applications. Lin et al. [8] likely provide a thorough overview of the current state of IoT technology, discussing the interconnections between different components and the challenges that arise from this complexity. By addressing critical areas such as security and privacy, their research highlights the importance of developing integrated solutions that ensure the safe deployment of IoT systems. Additionally, the survey may explore future trends in IoT, including advancements in artificial intelligence, edge computing, and data analytics, which have the potential to transform IoT applications. Lin et al. [8] 's comprehensive analysis serves as a valuable resource for researchers, practitioners, and policymakers seeking to understand the multifaceted nature of IoT technology and its implications for various sectors.

Lata et al. [9] investigate the challenges and enabling technologies for building secure and reliable Wireless Sensor Networks (WSN) for the Internet of Things (IoT) in their study published in IEEE Access. Their research focuses on the security challenges associated with WSNs, which are integral to many IoT applications. Lata et al. [9] likely examine various threats to WSN security, including eavesdropping, node compromise, and denial-of-service attacks. By analyzing these vulnerabilities, their study proposes solutions and enabling technologies to ensure the trustworthiness and dependability of IoT systems. The research may discuss the importance of secure communication protocols, authentication mechanisms, and data integrity measures in building robust WSNs. Furthermore, Lata et al. [9] may highlight the role of network management techniques and distributed algorithms in enhancing the security posture of WSNs. Their contributions are essential for developing secure and reliable IoT deployments, ultimately ensuring the successful implementation of IoT solutions across various industries.

3. Proposed Security Framework for Communication and Network Layer Protocols

In this paper, we have developed a heuristic trust calculation architecture to verify whether the user would be allowed to access the cloud infrastructure for storage and processing or not, which includes the three important layers.

- Things Layer
- Communication Layer
- Cloud Infrastructure

3.1. Things Layer

It is the first layer of our proposed architecture, and it comprises sensors, which play a vital role in IoT (Internet of Things) systems by gathering data from the real world and enabling digital representation of the physical environment. When data is to be sent to communication layer, sensors can give metadata and contextual information about the Packet Header, such as IP address, the time when the data packet was in and when data packet was out using time stamp, the port number used while login, and the encryption type previously utilized such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish Algorithm, Homomorphic Cryptosystem, and so on.

3.2. Communication Layer

It is the second layer of our proposed architecture, where protocols are used to transmit data and facilitate communication between IoT devices, gateways, and back-end systems. It is also known as the communication layer. It refers to the many technologies, protocols, and networks that permit information transfer in an IoT environment where security is very important, so security protocols such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman Algorithm (RSA), Transport Layer Security (TLS), are often used to establish secure connections in the IoT communication layer. For data transmission between devices, gateways, and back-end systems, the IoT communication layer employs a variety of protocols, namely SCADA, 6LOWPAN, etc. Data is transmitted from IoT devices to cloud-based platforms or back-end systems for storage, processing, and analysis via the communication layer, so strong security methods are required to ensure the integrity, confidentiality, and privacy of data sent between devices and back-end systems. Thus, they can proceed further to the cloud for storage and processing.

3.3. Cloud Infrastructure

It is the third layer of our proposed architecture, where the cloud platform provides two important services: cloud storage and cloud processing. IoT devices generate large amounts of data, and the cloud provides scalable and dependable storage for this data. Cloud storage services enable organizations to store and manage data generated by IoT devices cost-effectively and efficiently. The cloud allows for data permanence, accessibility, and long-term storage, ensuring that vital IoT data is not lost. The cloud provides sophisticated computing capabilities and analytics tools for processing and analyzing IoT data. Depending on the application, IoT data can be analyzed in real-time or in batches. Cloud-based analytic platforms can extract useful insights from IoT data, perform complicated data analysis, and offer predictive or prescriptive analytics, allowing organizations to make educated decisions based on the data.

3.4. Role of Our Proposed Framework

The role of our architecture is to calculate the trust value of the user in the communication layer for the security purpose of different protocols like RPL, LORAWAN, 6LOWPAN, etc., so that they can proceed further for cloud storage and processing of data. The diagrammatic representation below defines the whole architecture.

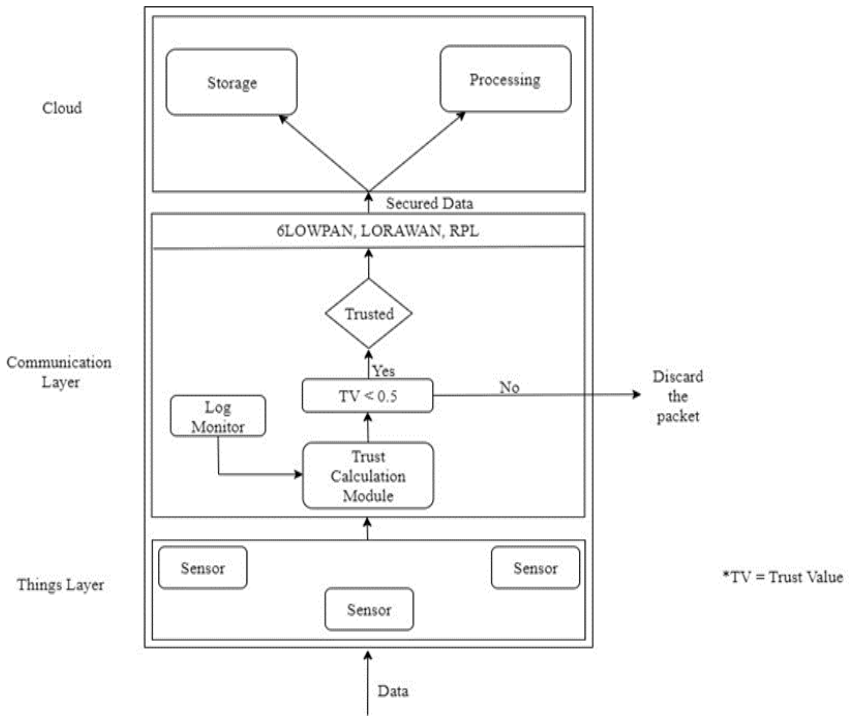

Figure 1: IoT-SecNet: Architecture of Trust Calculation Framework

In Figure 1, we can see the presence of the Things Layer, Communication Layer, and Cloud Infrastructure, where sensors initially play a vital role in collecting input data for every user. Those data need to be sent to the cloud for storage and processing of their data, but as per research, most of the data packets face security issues in the communication layer. So, in our work, we have designed a trust calculation module where the trust value of every data packet is calculated. If the calculated trust value is less than the set threshold value, i.e., 0.5, then the data packet passes through protocols like 6LOWPAN, LORAWAN, RPL, etc., to the cloud for further work.

3.4.1. Modules in Communication Layer

In our designed architecture, we have used two important devices, namely Log Monitor and Trust Calculation Module, which are described below:

3.4.1.1. Log Monitor

A Log Monitor at the IoT communication layer is a system or tool that captures, analyses, and monitors log data generated by IoT devices, gateways, and sensors. It provides insights into communication processes, assists with troubleshooting, monitors performance, and improves the overall reliability and efficiency of IoT connectivity. It collects log messages that provide information on various events, mistakes, or activities that occur throughout communication procedures.

Log monitors help to ensure the security of IoT communication. They look for security-related events in logs, such as unauthorized access attempts, unusual communication patterns, or probable security breaches, where organizations can discover and respond to security risks or vulnerabilities by tracking and analyzing security-related logs, ensuring the integrity and confidentiality of IoT communication. Here in our work, we have used a log monitor to verify the pattern in which the data packet was received. If there is a change in the pattern in incoming data packets, then the log value is assigned as ’1’; else, it is assigned as ’0’. Hence, the log value of the data packet is sent to the Trust Calculation Module for further work. Thus, the log monitor plays a crucial role in maintaining the seamless operation and effective management of IoT communication systems by boosting their performance, security, and reliability.

3.4.1.2. Trust Calculation Module

It is the most vital part of our designed architecture, where the trust value of every incoming data packet of the user is sent via. Sensors are calculated as follows:

$$Trust\ Value\ (TV) = Risk\ Value\ (RV) * Exposure\ Value\ (EV)$$

Here, the Trust Value again comprises 2 more modules, namely:

3.5. Risk Computation Module

In the Internet of Things, the risk computation module navigates to the idea of "risk value," which refers to the assessment or quantification of the potential hazards involved in establishing and maintaining IoT devices. Because of the inherent hazards in IoT contexts and due to abnormality in the pattern according to previously used data and recently used data for login, the risk value tends to be higher. Thus, we have designed our Risk Computation Module to calculate risk value, which is as follows:

$$RiskValue(RV) = i{=}1\Sigma n(TSi{*}VSi)/n$$

Here, TSi refers to the timestamp of different packets, and it is used to calculate the total time duration of the packet inside the packet header, where the packet-IN is used to check the in-time of different packets. Packet-out is used to check the out-time of different data packets. The VSi refers to the Vulnerability Score of various protocols used for the transmission of data Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Internet Group Message Protocol (IGMP), Dynamic Host Configuration Protocol (DHCP), etc. as in the National Vulnerability Database (NVD) that gives details on known vulnerabilities in software, hardware, and other systems, as well as severity ratings, impact, impacted versions, and mitigating strategies. The n refers to the total number of data packets used for the calculation of risk value. The NVD Score of different protocols is as follows (Table 1):

Table 1: Protocols and Their Vulnerability Score

Protocols	Vulnerability Score
TCP	4.9
UDP	5.0
ICMP	5.0
IGMP	8.3
DHCP	0.0

3.6. Exposure Calculation Module

In the Internet of Things, exposure calculation modules are software components or algorithms that help measure and quantify the "level of exposure" associated with IoT devices or systems. These modules assess the potential vulnerability of IoT assets to security attacks by analyzing numerous aspects such as vulnerabilities, network setups, device features, and contextual information. Thus, we have designed our exposure calculation to calculate exposure value which is as follows:

$$ExposureValue(EV) = (LV \wedge ET \wedge PN)\int_{i=1}^{\Sigma n} TS_i$$

Here, LV represents the Log Value that we will get from the Log Monitor according to the variation recorded between the past data and the recent data. The value will be set as "0" if there is no variation in data, and it will be set as "1" if there is a variation in data. ET represents Encryption Type where the different algorithms are used for security purposes where Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivets-Shamir-Adleman Algorithm (RSA) are highly secured algorithms whose default value is set to "0," and Secure Sockets Layer (SSL), Transport Layer Securities (TLS), Blowfish Algorithm are less secured algorithm whose default value is set to "1". PN represents Port Number that ranges from 0 to 65353. It is categorized into two parts, namely closed port, whose value is set to "0," and open port, whose value is set to "1". TSi refers to the timestamp of different packets. It is used to calculate the total time duration within which the packet was inside the Packet Header, where the Packet-IN is used to check the in-time of different packets, and Packet-OUT is used to check the out-time of different data packets.

4. Experimentation and Results

Our proposed solution is implemented in SCILAB, and its performance is compared to the present model's optimal solution for checking security. The default trust value was set as 0.5. The range of trust value was [0,1], where the data packet with a trust value ranging between [0,0.25] had high security and had nearly zero risk of being exposed. The data packet with a trust value ranging between [0.26,0.50] had medium-level security but still was somewhat free from being exposed. The data packet

with a trust value ranging between [0.51,1.0] was critical and was vulnerable to being exposed. The trust value was calculated from the experimental results of Risk Value, Exposure Value, and Throughput.

4.1. Risk Value

The graph of risk value versus the number of packets depicts the link between the level of risk associated with IoT devices, the protocols, and the number of packets or network traffic generated by these devices. The graph depicts how the danger level changes as network traffic volume grows. The graph consists of two axes, namely:

4.2. Risk Value Axis

The risk value is represented by the graph's vertical axis. The axis scale was determined by the risk assessment methodology used, which is on a numerical basis numbered between 0 to 1, where the packets with average risk value tending towards "0" seemed to be more secure than the ones that tended towards "1". Factors such as vulnerability severity, chance of exploitation, possible impact, and the presence of security safeguards were all used to calculate risk value.

4.3. Number of Packets Axis

The horizontal axis depicts the number of packets used in IoT connectivity. This can refer to the number of packets transmitted per unit of time or the total number of packets transmitted over a given period. The scale of this axis was determined by the range of packet counts seen in the IoT deployment under consideration (Table 2).

Table 2: Packets vs Risk Value

No. of Packets	Risk Value
100	0.3
200	0.4
300	0.4
400	0.1
500	0.7
600	0.4
700	0.8
800	0.5
900	0.9
1000	0.4

Figure 2 states that the link between the risk value and the number of packets is context-dependent and depends on things like the unique IoT system, network architecture, security mechanisms in place, and the nature of the packets being transmitted. The graph helps us to make risk management decisions. It aids in the prioritization of resources and mitigation efforts, and there can be a point where a higher number of packets may result in a higher risk value. Extra security measures should be provided to enhance the system.

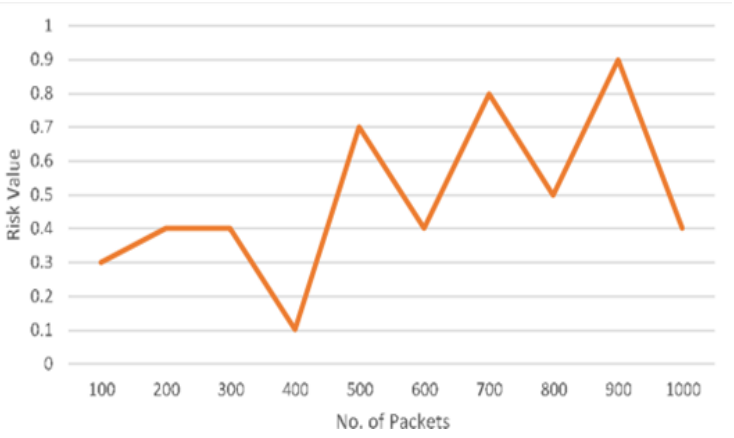

Figure 2: Packets vs Risk Value

4.4. Exposure Value

The graph of exposure value versus the number of packets depicts the level of exposure of the generated packets to incoming threats and how feasible they are to provide security.

4.5. Exposure Value Axis

The exposure value is represented by the graph's vertical axis. The axis scale was determined by the exposure assessment methodology used, which is on a numerical basis numbered between 0 and 1, where the packets with an average risk value "0" are the most secured. In contrast, the ones that are "1" are not secured.

4.6. Number of Packets Axis

The horizontal axis represents the number of packets, which indicates the amount of data being transmitted or received in the IoT system. The scale of this axis was determined by the range of packet counts seen in the IoT deployment under consideration (Table 3).

Table 3: Packets vs Exposure Value

No. of Packets	Exposure Value
100	1
200	1
300	1
400	0
500	0
600	1
700	0
800	0
900	1
1000	0

Figure 3 illustrates how the exposure value changes as the number of packets varies. It helps identify patterns and trends in the system's exposure to risks. The relationship between exposure value and the number of packets can provide insights into how the volume of packets being processed influences the exposure level.

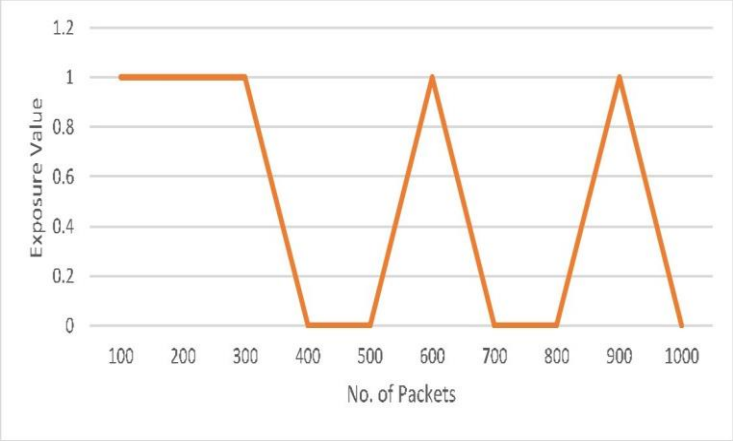

Figure 3: Packets vs Exposure Value

Throughput refers to the rate at which data is transmitted or received in an IoT system. The common units of measurement are bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps). Generally, throughput ranges between 2 to 5 Mbps. Higher throughput levels correspond to quicker data transfer rates, whereas lower values correspond to slower rates. The graph will depict how throughput fluctuates as the number of packets increases. It aids in the detection of patterns and trends

in the system's performance. The relationship between throughput and packet count can reveal information about the system's capacity, efficiency, and constraints.

4.7. Throughput Value Axis

The throughput value is represented by the graph's vertical axis, which is a measure of the data transfer rate or the amount of data that can be transmitted per unit of time.

4.8. Number of Packets Axis

The horizontal axis represents the number of Packets, which indicates the amount of data being transmitted or received In the IoT system. The scale of this axis was determined by the range of packets seen in the IoT deployment under consideration (Table 4).

Table 4: Packets vs Throughput

No. of Packets	Throughput
100	3.2
200	3.3
300	3.5
400	4.2
500	4.7
600	4.7
700	4.7
800	3.1
900	2.9
1000	2

Figure 4 can be categorized into three parts where. Firstly, the throughput kept on increasing when the number of packets was 100 till the number of packets was 400; it implied that the graph had a positive correlation, i.e., the system can handle bigger data quantities efficiently while improving the transfer rate. Secondly, with the increasing number of packets between 500 and 700, there was no longer a significant impact on the throughput. This signified the saturation point, where the system has reached its maximum capacity, and future increases in packet count will not result in proportional improvements in throughput.

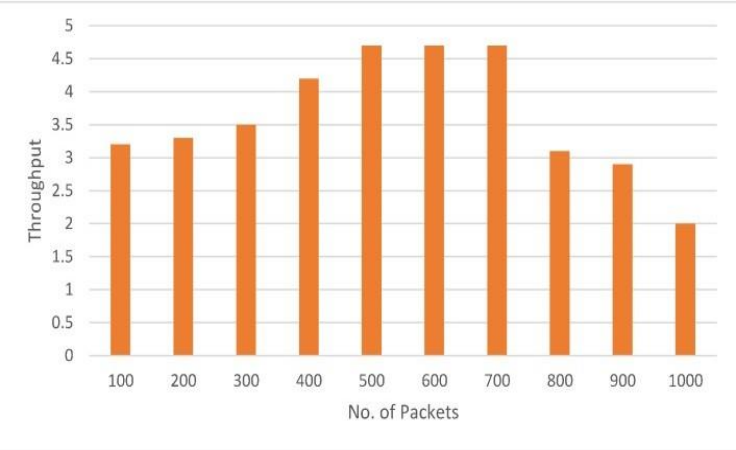

Figure 4: Packets vs Throughput

Thirdly, despite the increase in the number of packets, i.e., between 800 and 1000, A plateau or reduction in throughput was observed. It Indicates the presence of bottlenecks in performance. Bottlenecks may cause by network congestion, hardware restrictions, or inefficient processing.

5. Conclusion

A secure architecture for the Internet of Things (IoT) communication and network layer protocols is essential for safeguarding sensitive data and ensuring the integrity of operations. This architecture incorporates key features such as data encryption, secure communication protocols, intrusion detection and prevention systems, and network segmentation. Implementing these measures lays a strong foundation for protecting IoT systems from potential threats and vulnerabilities that could compromise user data and system functionality. The proactive approach to IoT security emphasizes the importance of pre-emptively addressing security challenges before they can be exploited. By safeguarding sensitive information and maintaining the operational integrity of IoT devices, organizations can foster trust among users and stakeholders. This trust is critical in an increasingly interconnected world where IoT devices are becoming ubiquitous in both personal and professional environments. As the IoT landscape continues to evolve, it is crucial to explore future directions for enhancing security frameworks.

Addressing emerging threats and vulnerabilities will require the development of resilient architectures that can adapt to changing technologies and attack vectors. Innovative solutions, such as artificial intelligence and machine learning, can play a significant role in enhancing the security posture of IoT systems. By continuously improving these frameworks and embracing new technologies, organizations can ensure the long-term security and reliability of their IoT communications and protocols, ultimately leading to a safer digital ecosystem. A secure architecture for IoT communication and network layer protocols provides data encryption secure protocols, intrusion detection and prevention, network segmentation, etc. It lays the groundwork for protecting IoT systems from potential threats. This proactive approach to IoT security aids in the protection of sensitive threats. This proactive approach to IoT security aids in the protection of sensitive data, the integrity of operations, and the overall trustworthiness of IoT systems. As the IoT landscape evolves, addressing the areas of future scope will contribute to the creation of resilient and secure frameworks for IoT communication and network layer protocols that will improve the security posture, respond to emerging threats, and utilize innovative solutions.

Acknowledgment: We are deeply grateful to the SRM Institute of Science and Technology, Ramapuram, Dhaanish Ahmed College of Engineering, Chennai, and St. Peter's Institute of Higher Education and Research, Chennai, Tamil Nadu, India.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding

Conflicts of Interest Statement: The authors have no conflicts of interest to declare. This work represents a new contribution by the authors and all citations.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants.

References

1. G. Gan, Z. Lu, and J. Jiang, "Internet of things security analysis," in 2011 International Conference on Internet Technology and Applications, Wuhan, China, 2011.
2. J. Zhang, H. Chen, L. Gong, J. Cao, and Z. Gu, "The current research of IoT security," in 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), Hangzhou, China, 2019.
3. L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," Appl. Sci. (Basel), vol. 10, no. 12, p. 4102, 2020.
4. M. Husnain et al., "Preventing MQTT vulnerabilities using IoT-enabled intrusion detection system," Sensors (Basel), vol. 22, no. 2, p. 567, 2022.
5. Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 2014.
6. P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 2013.
7. S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT-flock: An open-source framework for IoT traffic generation," in 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), Karachi, Pakistan, 2020.
8. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017.

9. S. Lata, S. Mehfuz, and S. Urooj, “Secure and reliable WSN for internet of things: Challenges and enabling technologies,” IEEE Access, vol. 9, no.11, pp. 161103–161128, 2021.
10. R.P. Prawin, R.P. Pravin, S. Rajavel, “Performance evaluation and comparative analysis of several machine learning classification techniques using a data-driven approach in predicting renal failure,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 11, no. 6, pp. 3522–3530, 2023.
11. K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, “A review paper on wireless sensor network techniques in Internet of Things (IoT),” Mater. Today, vol. 51, no.1, pp. 161–165, 2022.
12. S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” J. Big Data, vol. 6, no. 1, pp. 1-21, 2019.
13. A. H. Hussein, “Internet of things (IoT): Research challenges and future applications,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 6, pp. 77-82, 2019.