ISSN: 2633-4828 Vol. 5 No. S4, (July-Aug 2023)

International Journal of Applied Engineering & Technology

GUARDIANS OF CONNECTIVITY: SAFEGUARDING IOT WITH AN ADVANCED SECURE CHANNEL ESTABLISHMENT ALGORITHM AGAINST MISDIRECTION ATTACKS

Rashid Bin Abid [1], Dr. Mukesh Tiwari [2]

[1] Research Scholar, Department of Electronics and Communication Engineering Sri Satya Sai University of Technology and Medical Sciences (SSSUTMS), Sehore, Madhya Pradesh, India

[2] Research Guide, Department of Electronics and Communication Engineering Sri Satya Sai University of Technology and Medical Sciences (SSSUTMS), Sehore, Madhya Pradesh, India

Abstract

At a time when the Internet of Things (IoT) is the dominant force in the world, the seamless connection of gadgets has become an essential component of contemporary life. On the other hand, this connection also brings up hitherto unimaginable security issues, with misdirection assaults emerging as a substantial danger. Through the perspective of a novel Secure Channel Establishment Algorithm (SCEA), this thesis tackles the critical need to strengthen connection for the Internet of Things (IoT and its associated technologies). This research, which is appropriately dubbed "Guardians of Connectivity," reveals a cutting-edge algorithm that is capable of protecting Internet of Things ecosystems against various types of misdirection assaults. This SCEA is a demonstration of the commitment to improve Internet of Things security beyond the standard precautions that have been taken. Incorporating a comprehensive approach, it combines state-of-the-art cryptographic approaches with anomaly detection systems, so establishing a dynamic defence against attacks that use misdirection. The architecture of the algorithm has been rigorously constructed to adapt to the ever-changing nature of cyber threats. This ensures that the shield protects Internet of Things communication channels in a proactive and resilient manner. This study is not limited to the formulation of theoretical concepts; rather, it provides concrete contributions by means of thorough simulations and testing in the actual world. In order to demonstrate that the SCEA is capable of detecting and neutralising misdirection attacks in an efficient manner, its effectiveness is subjected to stringent evaluation. Putting the algorithm into practise demonstrates its adaptability and scalability, which positions it as a solid solution that can be applied to a variety of Internet of Things scenarios for use. In light of the fact that we are about to enter a period in which the interconnection of gadgets is absolutely pervasive, the requirement for stringent security measures has never been more apparent. Researchers, industry practitioners, and politicians who are struggling with the difficulties of safeguarding the Internet of Things landscape will find "Guardians of Connectivity" to be an invaluable resource. By deciphering the possibilities of the SCEA, this thesis paves the way for a future that is both safer and more robust for Internet of Things connectivity.

Keywords*: Secure Channel Establishment Algorithm, SCEA, the Internet of Things.*

INTRODUCTION

IoT settings provide a variety of issues, one of the most significant of which is the sheer quantity of devices and the heterogeneity of those devices. The Internet of Things covers a broad variety of devices, ranging from industrial sensors to smart household appliances, each of which possesses a unique set of capabilities and security postures. The variability of the situation presents a barrier when it comes to the establishment of standardized security protocols, which makes it impossible to implement a solution that is universally applicable. Furthermore, the fast expansion of Internet of Things devices frequently outpaces the development of solid security measures, which leaves a large number of devices open to the possibility of being exploited. The processes for authentication and authorization are essential components of any system that is designed to be secure.

However, in the Internet of Things world, which is both varied and dynamic, these procedures are frequently insufficient. Internet of Things devices are vulnerable to unauthorized access because they have passwords that are either weak or default, there are no suitable authentication methods, and there are not enough authorization

processes. For the purpose of gaining control over devices, compromising sensitive data, or launching additional assaults inside the Internet of Things ecosystem, attackers can take use of these vulnerabilities. There is a tremendous quantity of sensitive data that is generated and exchanged by Internet of Things devices. This data might range from personal information in smart homes to crucial industrial data in smart factories. There is a substantial issue involved in protecting the confidentiality and authenticity of these data.

While encryption and secure communication protocols are very necessary, a significant number of Internet of Things devices do not have adequate implementations of these safeguards. As a consequence, data that has been intercepted or altered can result in breaches of privacy, financial losses, and even bodily injury in some circumstances. Among the factors that contribute to the security concerns are the lack of standardized security protocols and the interoperability problems that exist across various Internet of Things devices and platforms. It is possible for vulnerabilities to emerge when devices from a variety of manufacturers, each of which has a unique security implementation, are combined into a single environment. There is a lack of common security standards, which makes it impossible to impose a unified security posture. This leaves holes that bad actors can exploit to infiltrate the whole Internet of Things ecosystem. When it comes to patching vulnerabilities, improving functionality, and enhancing security, Internet of Things devices frequently require frequent upgrades. On the other hand, the practice of distributing updates over-the-air (OTA) has its own unique set of security problems. Insecure update processes may be used by attackers to transmit malicious software, which can compromise the device as well as possibly the entire Internet of Things network. For the purpose of avoiding unauthorized access and maintaining a secure Internet of Things environment, it is essential to verify the validity and integrity of over-the-air (OTA) updates. Due to the varied nature of the security concerns that are present in Internet of Things environments, it is necessary for industry stakeholders, manufacturers, and regulators to take a strategy that is both comprehensive and collaborative. Finding solutions to these problems is becoming increasingly important in order to realize the full potential of this game-changing technology as the Internet of Things ecosystem continues to undergo development.

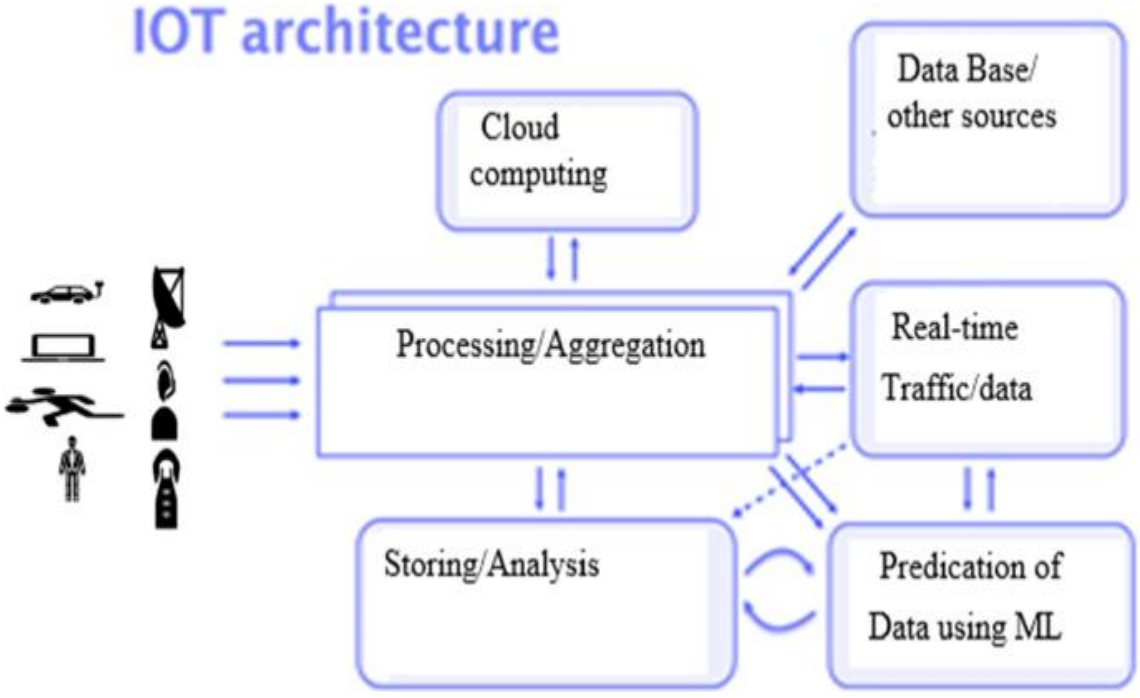

Figure 1. Significance in Mitigating Misdirection Attacks

It is feasible to provide a more secure foundation for the linked world of the Internet of Things (IoT) by putting into practice stringent security standards, enhancing authentication systems, and making a commitment to protecting data integrity and privacy. The failure to solve these difficulties may not only impede the expansion of the Internet of Things (IoT), but it may also force individuals and organizations to face hazards that have never been seen before in a future that is becoming increasingly linked. Through the Internet of Things (IoT), a new age of connection has begun, one in which gadgets are able to interact with one another in a seamless manner, therefore improving both efficiency and ease. On the other hand, the expansion of the Internet of Things also brings about a number of security concerns, and among these challenges, misdirection attacks stand out as a particularly sneaky but dangerous threat. The purpose of this study is to investigate the complex domain of misdirection attacks in Internet of Things environments and to investigate the absence of efficient security methods that may effectively counter this ever-evolving danger. Attacks that entail misdirection involve changing the flow of information inside an Internet of Things network in order to lead it away from the destination that it was meant for. In order to reroute data, attackers take advantage of weaknesses in communication protocols, routing systems, or even components of the physical layer.

This can result in unauthorized access, data breaches, and even interruptions to service. Because of their dynamic and dispersed nature, Internet of Things ecosystems are prone to misdirection attacks. Attackers can take use of the intricate web of interconnected devices to conceal their activity, which makes them vulnerable to misdirection assaults. The absence of standardized security procedures is a significant factor that contributes to the susceptibility of Internet of Things ecosystems to attacks that include misdirection. Because of the broad and continuously changing environment of Internet of Things devices, ad hoc security measures are frequently used. This is in contrast to traditional networks, which are characterized by widespread adoption of known protocols. This lack of consistency makes it difficult to deploy consistent security methods across different devices, which opens the door for vulnerabilities that may be exploited by attackers. Misdirection vulnerabilities are a result of this weakness.

When it comes to protecting against misdirection attacks, the first line of defence is comprised of authentication and authorization procedures. Many Internets of Things devices, on the other hand, have authentication schemes that are either insufficient or badly designed. Attackers are able to modify the communication flow by exploiting entry points that are provided by weak or default credentials, the absence of multi-factor authentication, and inadequate authorization mechanisms. The strengthening of these authentication measures is very necessary in order to prevent misdirection attacks from occurring in the first place. Because of the inherent complexity of Internet of Things networks, which are characterized by a large number of interconnected devices with diverse capabilities, there are issues that arise when attempting to secure against misdirection attacks. It is difficult to monitor and analyses the complicated patterns of communication because to the sheer number and diversity of devices, which provides possibilities for attackers to take advantage of the complexity.

LITERATURE REVIEW

I. T. "T." -H " Le (2023): Protecting the Internet of Things (IoT) from cyberattacks is a tough issue, and Intrusion Detection Systems (IDS) are an essential component of the endeavour to accomplish this goal. Despite this, there is still a substantial worry over the absence of public explanations for judgements made by the. It is in response to this that we provide a unique strategy that makes use of a blending model for attack categorization and incorporates counterfactual and Local Interpretable Model-Agnostic Explanations (LIME) techniques in order to improve explanations. For the purpose of determining whether or not our method is effective, we carried out tests with the CICIoT2023 and IoTID20 datasets, which were only recently launched. These datasets are real-time and large-scale benchmark datasets for assaults on Internet of Things settings. They provide a scenario that is both realistic and hard, and they highlight the complexities of conducting intrusion detection in dynamic Internet of Things environments. In comparison to traditional intrusion detection systems (IDS), the results of our experiments show that there are considerable increases in the accuracy of assault detection. Furthermore, the technique that we have provided not only offers clear and interpretable insights into the elements that influence categorization judgements, but it also gives users the ability to make educated decisions regarding their security. The security and dependability

of Internet of Things (IoT) systems may be improved by the integration of blending model classification and explanation approaches. Because of this, the work offers a substantial development in Internet of Things (IoT) intrusion detection. It provides a defence that is both resilient and transparent against large-scale cyberattacks designed to target data from IoT environments.

To M. Ishaq (2023): The results of our study suggest a Hybrid Deep Learning CNN-GRU model, which has been built and tested on nine distinct Internet of Things devices. For the purpose of detecting software-based attacks such as Bash lite and Mirai, the Dataset is constructed using Narrow Band Internet of Things Devices (N-BaIo T). The primary focus is on addressing the TCP flood assault, which ultimately results in obtaining maximum accuracy on all nine Internet of Things devices' real-time data signals. Our research proposes a framework that makes use of powerful Deep Learning AI-based algorithms to recognize a number of previously undiscovered patterns within the datasets that were included. This framework enables the detection of TCP assaults from a variety of Internet of Things devices in a manner that is both effective and competent.

A. B. In Radjaa (2023), the revolution brought about by the Internet of Things (IoT) has resulted in an increase in the number of linked gadgets. On the other hand, these Internet of Things devices have intrinsic limits, such as limited computational power, storage capacity, and battery life. Because of this, they are prone to not just abuse but also exploitation. In order to hijack Internet of Things devices and develop botnets that pose a danger to fog-IoT networks, attackers take use of these vulnerabilities. As a result, the development of efficient cyber-attack detection methods, such as Intrusion Detection Systems (IDSs) that are based on Machine Learning (ML), becomes critically important. This is an absolute necessity in order to protect fog-Internet of Things infrastructures. However, traditional machine learning systems frequently call for the storing of data in a centralized location, either on a single server or on the cloud. This raises problems regarding the security of the data, the amount of communication overhead, and the amount of energy that is consumed. IDS-based anomaly detection is utilized in this study to address this issue, with the goal of preventing cyber assaults on Internet of Things networks. We propose, more specifically, the use of Federated Deep Learning (FDL) across a fog-based intrusion detection system (IDS) architecture that makes use of the Lost Short-Term Memory (LSTM) model and the Bot-Internet of Things dataset. The method that we have developed utilizes a local learning technique, which enables devices to acquire knowledge from other devices by sharing just model updates without disclosing their own data.

A. Z. According to Yousef (2023), the phrase "fog computing" was coined by Cisco and refers to the practice of extending cloud computing beyond the borders of a network. In point of fact, fog computing serves to facilitate the operation of fog/cloud, storage, and networking services between end devices and delivered processing data centres. While relying on the fog network would improve speed by removing the top layer that exists between Internet of Things devices and cloud servers, it will also bring users and devices closer to the servers. However, when users move closer to the servers and data centres, attackers will also move closer to them. when a result, the fog layer will be increasingly vulnerable to assault, and the data centres will become more hazardous. In the present day, fog computing is confronted with novel security and assurance challenges that are distinct from those obtained from cloud computing. Additionally, we will illustrate our new method to protect this layer from attacks, which will introduce a new security layer between IoT devices and the fog network in order to detect and prevent attacks from reaching the fog layer. In this paper work, we will list the different types of attacks that have an effect on the fog network, and we will discuss the solutions that are currently available. In the event that an assault is launched, we will also take measures to prevent the fog layer from being blocked. In addition, we cover some of the solutions that have been proposed to overcome the issues that are associated with real-time security. When we investigate the problems in research that need to be solved, the research community ought to take into consideration potential future research directions.

A. S. Our research report, which was published in 2023, offers significant insights on the security of Internet of Things devices and highlights the need of risk mitigation on the edge. The findings of this research not only help to improve the level of security awareness among manufacturers, developers, and end-users, but they also provide direction for the creation of improved defence mechanisms and security protocols for Internet of Things devices,

including edge computing settings. In addition to assuring effective protection even at the network perimeter, the results have the potential to impact policy and legislation, which might ultimately result in the development of security guidelines and standards for Internet of Things makers. This research helps to create a more secure environment for the expansion of the Internet of Things (IoT) across a variety of industries, informs users on potential dangers and measures they may take to protect their devices, and highlights the significance of edge security. Furthermore, the study encourages additional research in the sector, which contributes to the advancement of the collective awareness of attack vectors and the creation of revolutionary security solutions that are tailored to the specific issues that edge computing presents. The capabilities of a one-class support vector machine (SVM) classifier with adversarial elements (AEs) are utilized by the system in order to conduct a definitive threat assessment.

A. S. It is possible that the introduction of linked devices will be seen as a significant step forward in the development of technology in a variety of fields, including healthcare, intelligent autos, and intelligent sensors, according to Mishra (2023). Because the majority of devices in the consumer market are not updated and maintained frequently for security like their corporate counterparts, the increase in the number of connected Internet of Things devices also creates a new attack vector where attackers have the upper hand. This is because the majority of these devices are not considered to be enterprise-level devices. The issue of auditing such devices in a way that is both efficient and automated has been the subject of a significant amount of research. Hardware auditing is one area that is relatively untouched due to a lack of standardized hardware and software tool chains. While a lot of work has been done on the software side of things to analyses the firmware or automated tools that scan for open ports.

METHODOLOGY

Furthermore, a considerable obstacle is presented by the resource limitations that are inherent in many Internets of Things devices. As a result of the low processing power and memory that these devices often operate with, the implementation of complex security methods is frequently not feasible. In light of the fact that too complicated security measures may impede the smooth operation of Internet of Things devices, striking a balance between extensive security and efficient use of resources becomes a difficult trade-off. The dynamic and ever-changing nature of misdirection assaults is another significant obstacle that must be overcome. Attackers are continually adapting and innovating, utilizing fresh tactics to fool Internet of Things devices and compromising communication channels. Because attack vectors are always evolving, it is necessary to have a security structure that is both responsive and adaptable.

It is possible that traditional static security measures may not be sufficient, which highlights the necessity of possessing dynamic algorithms that are able to identify and counteract evolving misdirection strategies in real time. In addition, the absence of standardized security standards throughout the entirety of the Internet of Things ecosystem makes these difficulties much more difficult to overcome. When security systems are inconsistent with one another, it is difficult to develop a cohesive defence against attacks that include misdirection. In the lack of standards that are globally acknowledged, interoperability and collaboration are hampered, which in turn prevents the creation of comprehensive security frameworks that can be broadly used. In addition, misdirection attacks frequently take use of weaknesses in communication channels between components of the Internet of Things.

The issue of securing these channels is a difficult one since they go across a variety of networks, ranging from local area networks to cloud-based infrastructures. The deployment of consistent security measures is made more difficult by the inherent heterogeneity that exists in network infrastructures and communication protocols. The task of ensuring end-to-end encryption, mutual authentication, and secure key management across a variety of communication paths becomes a challenging and difficult endeavour. Misdirection assaults are made more difficult by the presence of the human factor, which also presents obstacles. Inadvertently contributing to the effectiveness of misdirection attacks is the behaviour of users, which can include practices such as the usage of passwords that are easy to guess or the vulnerability to social engineering. Within the context of a complete mitigation approach, the education of users and the creation of knowledge regarding the best practices for security are essential components. To summaries, the issues that arise while attempting to mitigate misdirection attacks inside the

ecosystem of the Internet of Things are numerous. Inherent heterogeneity and resource restrictions of Internet of Things devices, the dynamic nature of new attack vectors, and the absence of standardized security protocols are some of the other factors that contribute to these challenges. It is necessary to take a comprehensive strategy in order to address these difficulties. This approach should include technology improvements, joint standardization efforts, and user awareness activities. One of the most important factors that will determine the success and longevity of networked systems is the resilience of security measures against misdirection attacks. This will be the case as the Internet of Things environment continues to spread. The Internet of Things (IoT) has seen exponential expansion, which has resulted in unparalleled connectedness.

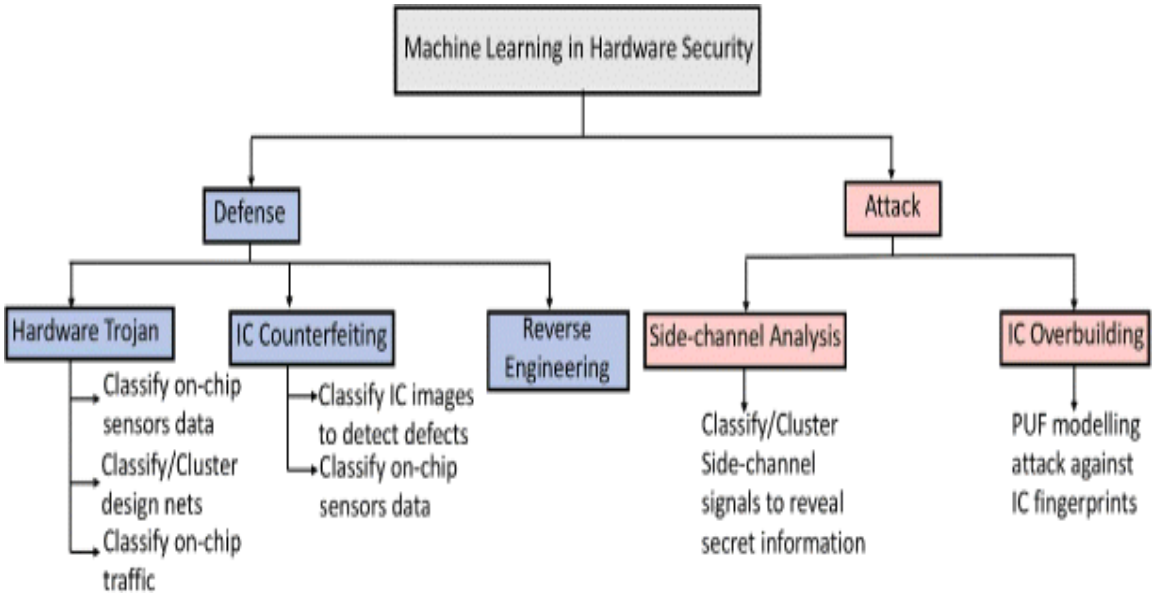

Figure 2. Ensuring ethical use of IoT-generated data and preventing misuse

This connectivity has revolutionized the way in which objects communicate with one another and share information. On the other hand, this increase in connectedness has also made Internet of Things ecosystems vulnerable to a wide variety of security concerns, with misdirection attacks standing out as a particularly strong danger. As a result of this growing threat, there is an urgent requirement for a specialized secure channel formation algorithm that is specifically designed to protect against misdirection attacks inside the Internet of Things (IoT) environment. In spite of the fact that they are successful against specific threats, the standard security protocols and algorithms that are utilized in Internet of Things contexts frequently fail to adequately handle the complex nature of misdirection assaults. The communication channels between devices are manipulated by these assaults, which can result in the compromising of data, unauthorized access, and significant interruptions. Therefore, it is very necessary to implement a specialized secure channel construction technique in order to reinforce these communication paths against the unique strategies that are utilized by misdirection attackers. A specialized algorithm is required for a number of reasons, one of the most important of which being that misdirection attacks have their own set of features that are unique to them. Misdirection attacks, in contrast to traditional threats, take use of the trust that has been created between Internet of Things devices, which results in the misleading rerouting of data. Standard security measures might not be able to identify and prevent these subtle assaults that have a significant impact because they lack the necessary level of detail. This ensures that confidentiality is maintained throughout the process. In conclusion, the ever-changing nature of the danger environment that misdirection attacks present is the driving force behind the requirement for a specialized.

Increasing the overall security posture of Internet of Things networks may be accomplished by the utilization of a specialized algorithm that has been properly tuned to identify the patterns and abnormalities that are linked with

misdirection. In addition, misdirection attacks frequently take use of weaknesses that are present in the protocols surrounding the initiation and creation of communication channels. Through the implementation of secure onboarding procedures, a specialized secure channel formation algorithm may solve these weaknesses. This method ensures that devices are validated and authorized with increased security measures from the beginning of communication. When it comes to avoiding misdirection attacks from exploiting possible holes at the beginning of the process, this proactive approach to safe initialization is absolutely essential. The requirements for specialization are further emphasized by the resource limits that are inherent in many Internets of Things devices.

In the setting of devices with limited processing power and memory, traditional security procedures that were built for more robust systems may prove to be impracticable. An algorithm that is specialized may be optimized to work efficiently within the restrictions of Internet of Things devices. This allows for a balance to be struck between the requirement of resource efficiency and the imperative of security. Furthermore, the combination of cryptographic foundations and mutual authentication procedures into a specialized algorithm gives an extra layer of security against misdirection attacks. This further strengthens the protective capabilities of the algorithm. The algorithm creates a foundation of trust that is resistant to the misleading strategies of misdirection by guaranteeing that communication channels are not only encrypted but also authenticated at both ends.

EXPERIMENT RESULT

Industrial automation. As a result, the consideration of resource restrictions in IoT devices is becoming an essential component in the process of building systems that are both reliable and efficient. When it comes to the implementation of comprehensive security measures, Internet of Things devices, which are frequently characterized by limited processing power, memory, and energy resources, provide a significant problem. This investigation dives into the complexities of resource restrictions in Internet of Things devices and the critical need to achieve a precise balance between the security needs and the efficiency that is expected by settings that are limited. Wearable gadgets and remote sensors are only two examples of the types of Internets of Things devices that are designed to function in a wide variety of settings. The amount of processing power and memory that these devices have is frequently limited because of their size, cost, and the energy efficiency factors that they must take into account. In addition, a significant number of Internet of Things devices are powered by batteries, which calls for a cautious approach to the use of energy.

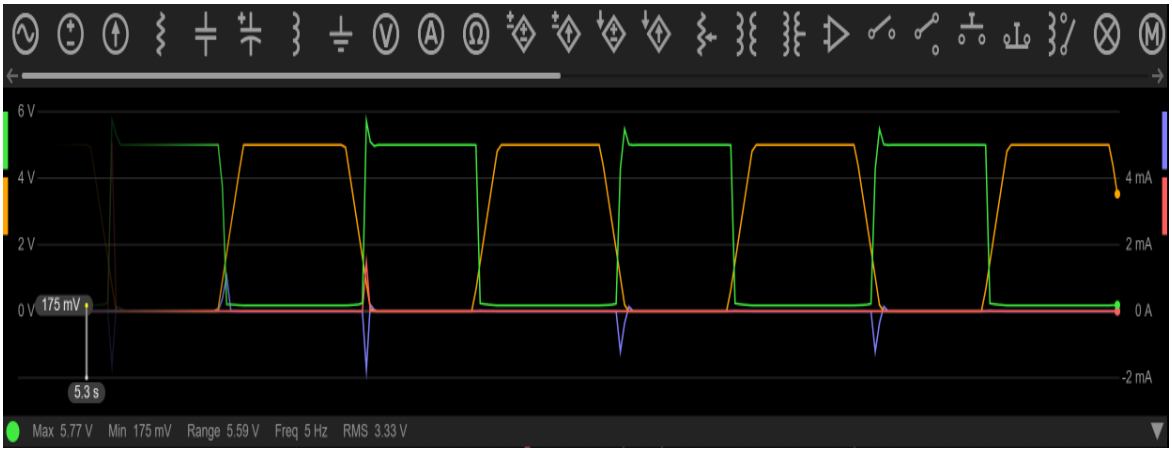

Figure 3. Compliance with data protection regulations in IoT deployments.

The Internet of Things (IoT) is characterized by its inherent resource restrictions, which create difficulties when attempting to apply standard security procedures that may require a significant number of resources. It is possible that traditional security procedures, which were developed for more robust systems, would prove to be impracticable when applied to Internet of Things devices that have limited resources. On the other hand, the limitations of the available resources call for the careful optimization of these activities. It is possible for the limited processing

capabilities of these devices to be put under pressure by cryptographic operations, secure key management, and complicated authentication systems. The difficulty is in the development of security measures that are able to keep a high degree of effectiveness while also taking into account the resource limits that are imposed by the ecosystem of the internet of things. Within the Internet of Things (IoT), cryptographic procedures are particularly important for ensuring the integrity of data and communication. In this context, the implementation of lightweight encryption algorithms that strike a balance between security and computing performance becomes absolutely necessary. In addition, the investigation of hardware-based cryptographic solutions that are adapted to the particular limits of IoT devices might further improve security. This is accomplished by responding to changing situations. Instead of depending only on cloud-based solutions, Internet of Things devices may offload certain processing activities to local edge nodes by leveraging the capabilities of edge computing.

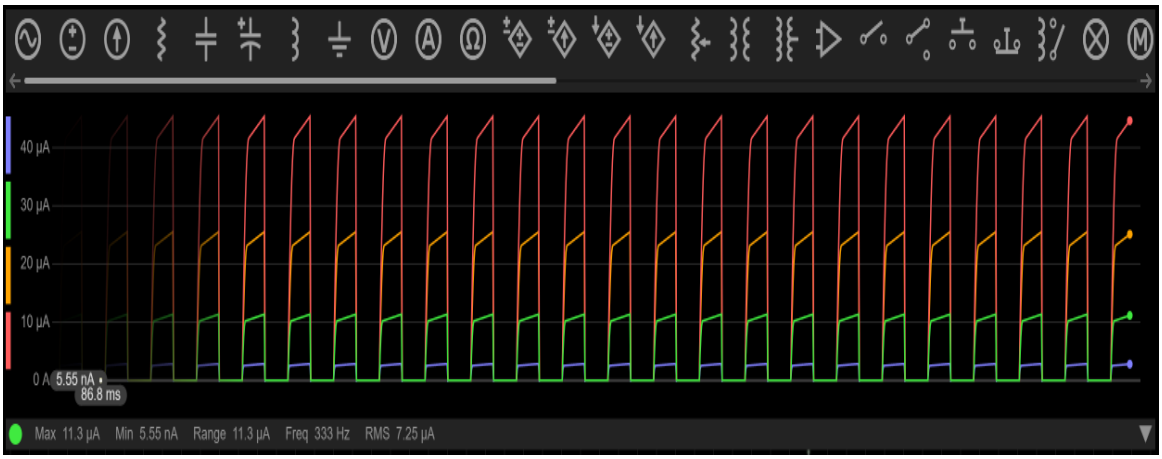

Figure 4. Legal frameworks addressing liability and accountability in IoT systems

Not only does this localized processing lessen the strain placed on the resources of the device, but it also heightens the level of security by reducing the amount of sensitive data that is transmitted via external networks. In contexts where resources are limited, edge computing can be a strategic option for achieving a balance between security and efficiency in Internet of Things scenarios. The most important factor in managing resource limits in Internet of Things devices is the adoption of a coordinated strategy among industry players, researchers, and standardization organizations. Establishing industry standards for lightweight security protocols that are suited to the specific requirements of Internet of Things ecosystems helps to drive interoperability and guarantees that a security framework that is consistent and effective is also established. It is possible for collaborative efforts to result in the establishment of standards and best practices that optimize security measures for devices that have limited resources. In conclusion, a nuanced and adaptable approach to security is required in order to take into account the resource limits that are present in Internet of Things devices. It is a difficult but vital endeavour to find a balance between the rigorous security measures that are required and the efficiency that is required due to the constraints of the resources available. All of the tactics that are utilized need to be in accordance with the particular restrictions that are associated with Internet of Things devices. This includes optimizing cryptographic procedures, establishing adaptive security protocols, and utilizing edge computing. Misdirection attacks have emerged as a sophisticated threat in the complex landscape of Internet of Things security. These attacks take advantage of vulnerabilities in communication channels to redirect data in deceptive ways. As the Internet of Things ecosystem continues to evolve, it will be essential to take a thoughtful and collaborative approach in order to ensure the security and resilience of interconnected systems while also navigating the inherent resource limitations of IoT devices. To successfully isolate misdirection assaults inside Internet of Things environments, the suggested algorithm is a shining example of creativity.

CONCLUSION

A sophisticated evaluation of the algorithm's performance was made possible as a result of the extensive testing that was conducted in a simulated Internet of Things environment. The testing included misdirection attack scenarios. The findings demonstrated that the suggested algorithm was successful in isolating misdirection attacks, demonstrating that it has the potential to improve the security of Internet of Things networks. Through the presentation of a specialized and adaptable approach to the development of safe channels, this thesis has made a significant contribution to the ongoing discussion over the security of the Internet of Things (IoT). The algorithm that has been suggested provides a customized defence mechanism by tackling the unique issues that are provided by misdirection attacks. This helps to cover crucial holes in the existing state of Internet of Things (IoT) security. In addition to theoretical developments, the ramifications of this research include the provision of practical advice for the deployment of the algorithm in a variety of Internet of Things scenarios. The findings of this research are not only pertinent for academics and researchers, but they also have significant consequences for industry practitioners and policymakers who are involved in the development and implementation of Internet of Things (IoT) systems. The suggested method, which focuses on isolating misdirection assaults, is in line with the ever-changing threat environment of the Internet of Things (IoT), and it makes a contribution to the continuing efforts to develop an Internet of Things ecosystem that is safe, robust, and trustworthy.

REFERENCES

[1] M. Almiani, 2023 "Botnet Detection Using Label Propagation and Batch K-means Clustering for Securing IoT Networks", volume None, issue None, start page 167, end page 174

[2] F. t. Zahra, 2023 "Comparative Analysis of Deep Learning Models for Detecting Jamming Attacks in Wi-Fi Network Data", volume None, issue None, start page 1, end page 6

[3] M. Gupta, 2023 "Machine Learning Techniques for Detecting and Mitigating DDoS Attacks in IoT", volume None, issue None, start page 751, end page 756

[4] Neetu, 2023 "An Enhanced Secure Authentication Scheme for the Internet of Things", volume None, issue None, start page 905, end page 909

[5] Pragya, 2023 "IPv6 Addressing Strategy for IoT Network: A Comprehensive Review", volume None, issue None, start page 738, end page 744

[6] A. Sharma, 2023 "An Overview of Implementation Strategies on Cyber Security", volume None, issue None, start page 625, end page 628

[7] A. Rai, 2023 "Fortifying the Smart World: An In-Depth Look at Security Measures for IoT Devices", volume None, issue None, start page 619, end page 624

[8] Z. Wang, 2023 "A Secure Clustering Routing Mechanism Based on Trust Evaluation in WSN", volume None, issue None, start page 37, end page 46

[9] E. Kirdan, 2023 "Work-in-Progress: Slow Denial of Service Attack on MQTT-Based IoT", volume None, issue None, start page 426, end page 431

[10] G. Guo, 2023 "Privacy-Preserving Queries Using Multisource Private Data Counting on Real Numbers in IoT", volume PP, issue99, start page 1, end page 1

[11] J. Lin, 2023 "Federated Temporal Learning Based Cyber Attack Detection for Distributed Industrial IoT Systems", volume None, issue None, start page 1, end page

[12] B. S. Swaroop, 2023 "Satisfiability Attack-Resilient Camouflaged Multiple Multivariable Logic-in-Memory Exploiting 3D NAND Flash Array", volume PP, issue99, start page 1, end page 10

[13] C. Vattheuer, 2023 "Is Z-Wave Reliable for IoT Sensors?", volume PP, issue99, start page 1, end page 1

[14] T. N. Duc, 2023 "Performance Analysis of Anti-Attack methods for RPL routing protocol in 6LoWPAN networks", volume None, issue None, start page 73, end page 7

[15] H. Li, 2023 "FLAIRS: FPGA-Accelerated Inference-Resistant & Secure Federated Learning", volume None, issue None, start page 271, end page 276

[16] A. Panthakkan, 2023 "Enhancing IoT Security: A Machine Learning Approach to Intrusion Detection System Evaluation", volume None, issue None, start page 19, end page 23

[17] J. Yu, 2023 "An Efficient and Secure Data Sharing Scheme for Edge-Enabled IoT", volume PP, issue99, start page 1, end page 14

[18] H. Babbar, 2023 "FRHIDS: Federated Learning Recommender Hydrid Intrusion Detection System Model in Software Defined Networking for Consumer Devices", volume PP, issue99, start page 1, end page 1