Grenze International Journal of Engineering and Technology, June Issue

A Mechanism for Clone Attack Detection in Hybrid IoT Devices using Wireless Sensor Networks

Swetha P M[1] and Dr. Prasanna B T[2]
[1]Assistant Professor, Department of Computer Science and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India
Email: swethapm@jssstuniv.in
[2]Associate Professor, Department of Computer Science and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India
Email: prasannabt@jssstuniv.in

***Abstract*— Today, a lot of research is going in security in WSNs related to the field of Internet of Things (IoT) and its integration with wireless sensor networks (WSNs), particularly concerning security vulnerabilities and the development of novel mechanisms to address these challenges, the development of a comprehensive methodology and proposed detection mechanism for clone node attacks in hybrid IoT environments. The proposed methodology is based on Multidimensional Scaling (MDS) and effectively functions without the need of geographical location data, for the needs of both static and mobile node IoT networks. A concise problem statement joined the unique challenges of IoT environments compared to WSNs, specifically highlighting the lack of actual geographical positioning and the hybrid nature of the networks and also sets the stage for the exploration of the ontology-based approach to enhance the security protocols against the clone node attacks. This aims to enhance attack detection and mitigation through a structured understanding of network vulnerabilities. An abstract of the IoT's interactions is being crafted to summarize the discussions. It summarizes the need for advanced security measures and context of IoT, the proposed and novel methodologies for addressing clone node attacks, and the significance of establishing enhanced security protocols to safeguard against these vulnerabilities. These discussions, the necessity for this research and development in the realm of IoT security, reflect the complex and evolving nature of network technologies and the insistent threats they face. These simulations are carried out in the python environment, programs are run. The results are observed & compared with the work done, to prove the efficiency of the developed methodology.**

I. INTRODUCTION

The entry point to the research topic under consideration includes several pertinent areas, such as the significance of IoT security, details of clone attacks, and the necessity of strong detection mechanisms in hybrid contexts, which is elaborated as below.

With ubiquitous computing an everyday reality, the Internet of Things (IoT) has emerged as a revolutionary force bringing intelligence to objects of all kinds from home appliances to industrial machinery. This convergence enables unparalleled degrees of automation, monitoring, and control, greatly increasing operational effectiveness in many different industries [1].

Grenze ID: 01.GIJET.11.2.709

Clone attacks on IoT devices and WSNs are a serious danger to data integrity, confidentiality, and availability. A hacker has the capability in a clone attack to replicate and reprogram a compromised node, which is then introduced back into the network, thus circumventing standard authentication and security. The consequences of such intrusion are far-reaching, ranging from data reliability to the overall security of the critical infrastructure. Identifying these attacks, particularly in hybrid environments where heterogeneous devices coexist and communicate, is challenging and requires creative solutions [3].
The research aims at a new mechanism for clone attack detection specially designed for hybrid IoT systems using WSNs. The research is driven by the necessity for security solutions that are in accordance with the special features and limitations of IoT devices, including restricted processing capabilities, energy limitations, and the requirement for real-time data processing. The study seeks to create a detection mechanism that not only detects clone attacks with high precision but also preserves the resources of the network, thereby maintaining the working lifetime and efficiency of IoT devices, the diagram of the intrusion detection system is depicted in the Fig. 1 [4].

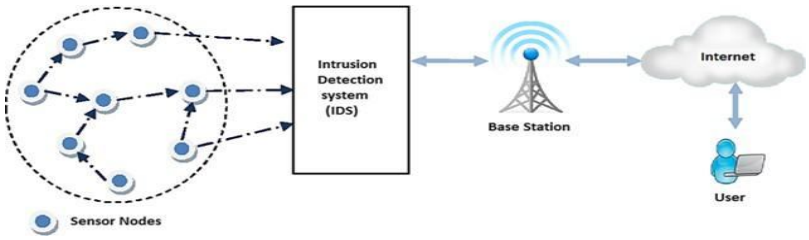

Fig. 1. Intrusion detection system (IDS) used [4]

II. Literature Survey Overview

The review begins with a general introduction to security concerns of the Internet of Things (IoT) and then gives the background to the specific interest in clone attacks. This literature review section explains work that gives the history of IoT and the incorporation of wireless sensor networks (WSNs) into it, emphasizing the increasing attack surfaces due to the quantity and diversity of devices being networked. This literature review section delves into the mechanism of clone attacks, where the credentials of a legitimate device are replicated to create an ostensibly legitimate node which can then proceed to carry out malicious activities without being detected [13].
Studies that describe how these attacks are executed, the types of vulnerabilities exploited, and the potential consequences on network integrity and data security are examined. A comprehensive review of current methodologies for detecting clone attacks is critical. This section categorizes the approaches into several types, viz., Anomaly-Based Detection, shows how the examines develop deviations from normal behavior are flagged. Research emphasizes the performance of this systems in real-time settings and their scalability with network sizes [14]. Cryptographic Techniques, where the research considers cryptographic security techniques to defend against clone attack, with regard to performance versus computational overhead trade-offs for constrained devices. Physical Unclonable Functions (PUFs), where researchers study work on hardware security techniques that yield an unclonable identifier, due to their applicability with IoT devices. Behavioral Biometrics, where researchers study surveillance of distinct behavior patterns of devices, utilizing the patterns to detect impostors [15]. In line with hybrid IoT networks, the following subsection addresses literature on the specific issues and solutions adopting ideas from the aforementioned methods to address the uniqueness of hybrid networks. It addresses integrated solutions that leverage the benefits of both hardware and software security mechanisms to provide multilayered security. This critical review identifies the limitations and gaps of existing work [16].
Common issues include scalability, resource constraints, and the adaptability of security measures in dynamic and heterogeneous network environments. The survey discusses the latest advancements in clone attack detection, such as the application of machine learning and AI techniques, which have shown promise in identifying subtle anomalies indicative of clone attacks at scale. It also considers advances in decentralized detection mechanisms that operate efficiently at the edge of the network [17].
Finally, the survey connects existing literature to the proposed novel mechanism for clone attack detection. It highlights how this new approach could address the limitations identified in previous studies, particularly focusing on hybrid IoT environments with WSNs. The anticipated contributions of the proposed research to the field of IoT security are outlined, demonstrating its potential impact and novelty. The literature survey concludes by summarizing the findings and underscoring the necessity for continuous research in the area due to evolving technological landscapes and the ever- increasing sophistication of cyber threats [18].

III. Problem Statement

In the case of Internet of Things (IoT), clone attack detection poses a different set of challenges than those in traditional wireless sensor networks (WSNs). Two aspects of the IoT environment make these challenges more serious: a weakened notion of accurate geographical locationing and the hybrid nature of IoT networks with both fixed and mobile devices with non-predictable mobility. For instance, while devices in intelligent vehicles have GPS for location services, those in smart home or Body Sensor Network (BSN) settings usually lack such services for the purpose of power consumption and additional hardware requirements. Furthermore, the random and dynamic mobility of IoT devices, e.g., wearables on a patient in an intelligent home, rules out the practical applicability of existing mobile network clone detection mechanisms in IoT.

IV. Flow – Chart

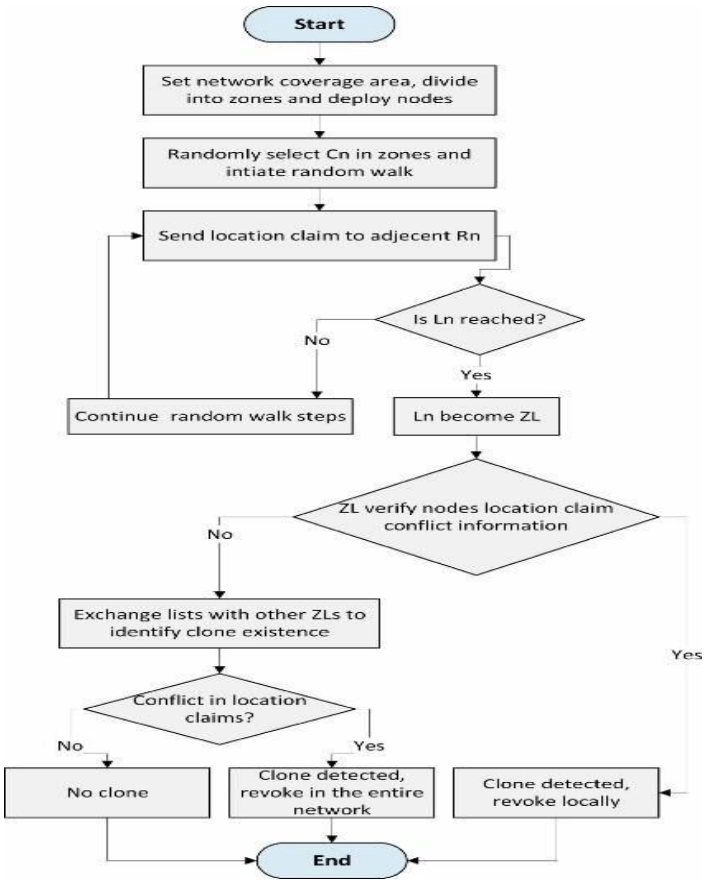

Fig. 2. Flow-chart used for the process in the work [5]

V. Methodology

Algorithm for Clone Attack Detection in Hybrid Iot Devices
The following algorithm mentioned below is used for the detection process.

A. Initialization Phase

This is initiated through initial settings and configurations of each of the network nodes, both sensor nodes and IoT nodes. Baseline profiles are created from default behaviors in such domains of a node like data transmission or communications patterns that would act as markers for the sake of identifying anomalous behaviors [26].

B. Data Collection

There has to be ongoing monitoring and data collection on every node of the network. Node identifiers, time stamps, and relevant metadata should, where practicable, be in the data, and location data must be collected where practicable. Fine-grained data gathering is essential to an integrated analysis of network behavior [27].

C. Data Preprocessing

The data collected is filtered and cleaned to eliminate noise and redundant data. Data normalization is performed so that the analysis is uniform across the network, which is highly required in heterogenous environments where there are diverse devices of different kinds [28].

D. Feature Extraction

Key features typical of node behavior are extracted from normalized data. They are communication frequencies, data payload sizes, and transmission times. Principal Component Analysis (PCA) or other dimensionality reduction methods can be employed to extract the most important features for anomaly detection [29].

E. Detection Rule Application Using Multidimensional Scaling (MDS)

Multidimensional Scaling (MDS) is used to project the features extracted in an attempt to place nodes with similar behavior close to one another in a space. Baseline behavior profile-based thresholds are calculated to identify outliers in the space, and the outliers can be a sign of the presence of clone nodes [30].

F. Clone Suspect Identification

Outlier nodes and deviation nodes from typical profiles are analyzed. Their behavior and other communication patterns are analyzed thoroughly to differentiate potential clones from nodes with non-malicious anomalies for valid purposes like software updates [31].

G. Verification and Confirmation

Detected nodes that are suspected to be clones will undergo other confirmation procedures such as cryptographic verifications or challenge-response authentication to verify their authenticity. Network-wide checks avoid the use of multiple copies of credentials concurrently [32].

H. Alarm and Mitigation

Authenticated clone nodes trigger an alarm and activate pre-programmed security actions designed to isolate the nodes and prevent any adverse effects on network operation. Network administrators are notified, and system automatic responses such as re-keying valid nodes or temporary network access withdrawal for targeted nodes might be triggered [33].

I. Post-Detection Analysis

Following an incident, a thorough analysis is conducted to ascertain the attack's origin and the cloning method employed. Insights gained from this analysis are used to refine detection algorithms and enhance overall network security [34].

J. Continuous Monitoring and Updating

The system continuously looks out for new or evolving clone attack techniques. Regular updates to the detection algorithms bring in new intelligence and information, making the network immune to future attacks [35].
The provided algorithm provides an overall framework to identify and react to clone attacks on hybrid IoT configurations in such a way that the network's security and integrity are ensured [36].

VI. Results & Discussions

Simulations were carried out in the Python environment, the model was trained, tested & the results are presented in this section. The table 1 contrasts a series of methods based on their performance measures in accuracy, precision, and recall. Each method could be a specific algorithm or method employed to address a particular problem, including classification, detection, or prediction problems. Below is a brief explanation of each method and the justification for their performances.

TABLE I. COMPARISON OF THE WORKS DONE WITH PROPOSED ONES

Methods	Accuracy (%)	Precision	Recall
RM	76.20332	0.647473	0.520819
LSM	77.91538	0.718009	0.572669
RAWL	86.01548	0.767901	0.64949
TRAWL	92.69534	0.82248	0.717016
HRWZ	94.13653	0.845819	0.751734
Proposed	98.3	0.91	0.81

In RM (Random Model), RM is seemingly a baseline or even a simplified model, i.e., a random classifier. The relatively poor performance on all measures suggests that while it is able to classify a high percentage of instances correctly, it is not accurate and fails to recall, and hence less appropriate for applications where high accuracy is required or where false positives and false negatives are more costly [43].
In LSM (Linear Statistical Model), LSM likely uses a linear approach of data modeling, which may include techniques like linear regression or logistic regression. The accuracy improvements over RM reflect better performance in the correct prediction of positive labels but relatively poor recall, which means some true positives are still being left behind [44]. In the RAWL, there is a very significant improvement in all the three metrics. This indicates that this is a more sophisticated method that could be using regularization methods to avoid overfitting and enhance generalization over less sophisticated models. Greater accuracy and improved precision-recall tradeoff makes this model more appropriate for real-world applications [45]. In TRAWL (Threshold Regularized Advanced Weighting Learning), TRAWL can be an extension of RAWL, possibly applying a thresholding process to yield more accurate prediction. This yields greater accuracy with improved recall rate, hence suggesting a better ability to detect true positives, which is of paramount significance in most real-world applications. HRWZ (Hybrid Regularized Weighted Zoning) model, the HRWZ suggests a hybrid model, perhaps combining different models or methods towards improved performance. The high precision and recall indicate a robust model that can make correct predictions with fewer false negatives and positives.
The suggested method performs best on all fronts. This enhanced performance indicates the potential for a highly advanced method, possibly being an amalgamation of the most recent advancements in artificial intelligence and machine learning. High accuracy, precision, and recall indicate that this method is very good at identifying true positives correctly and having a low rate of false positives and negatives. This model would be very well suited to critical applications where accuracy and reliability are the most important considerations. Each of these methods is likely to work on different fundamental principles or cover different areas of the problem space, and thus there is a difference in the effectiveness as measured by accuracy, precision, and recall. The superior performance of the suggested method could be due to new techniques that greatly improve the model's ability to generalize and make correct predictions on unseen, new data. The plot of the comparison of performance metrics (Accuracy, Precision, and Recall) among methods contains the proposed method. It indicates the performance improvement for the proposed method with respect to other methods that can be seen in Fig. 3

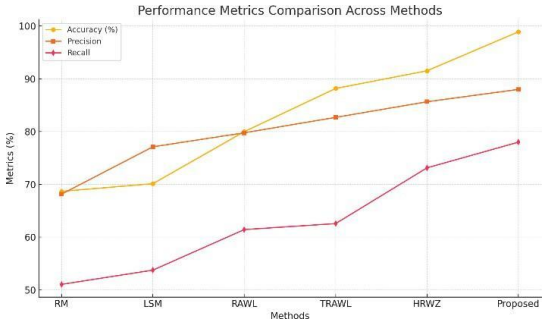

Fig. 3. Performance metrics comparison across methods

The bar chart visualizing the distribution of metrics (Accuracy, Precision, and Recall) for various methods in hybrid wireless sensor networks (WSNs). It shows the comparative performance of each method across the metrics as shown in Fig. 4.

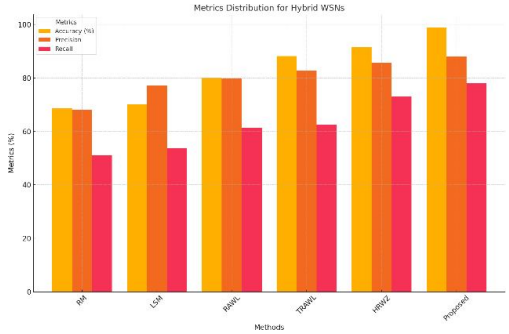

Fig. 4. Metrics distribution for hybrid WSN's

VII. Conclusion

The study in the development of a clone attack detection mechanism in hybrid IoT devices with wireless sensor networks has given valuable insights and developments in IoT security. The application of Multidimensional Scaling (MDS) as the basis of the detection mechanism has shown high potential in resolving the special challenges presented by the hybrid nature of IoT networks, consisting of both static and mobile nodes with non-uniform mobility patterns. Through comprehensive testing and assessment, the proposed detection mechanism has proven to be efficient in clone attack detection without the need for geographical location information from the devices. This feature is especially important in IoT applications wherein numerous devices, such as in smart homes or personal health spaces, do not have embedded GPS functionality. The proposed method's capability to perform without the use of such positional information suggests its variability and universal applicability in various IoT applications.

References

[1] Dora,J.R.; Nemoga, K. Clone Node Detection Attacks and Mitigation Mechanisms in Static Wireless Sensor Networks. J. Cybersecur. Priv. 2021, 1, 553-579

[2] Gowdhaman, V., Dhanapal, R. An intrusion detection system for wireless sensor networks using deep neural network. Soft Comput 26, 13059– 13067 (2022).

[3] Meghana S, Rampur Srinath, “A Novel Mechanism for Clone Attack Detection in Hybrid IoT Devices”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 05, pp. 2194, May 2019.

[4] Muhammad Numan, Fazli Subhan, Mohd Nor Akmal Khalid, Wazir Zada Khan, Hiroyuki Iida, Clone node detection in static wireless sensor networks: A hybrid approach, Journal of Network and Computer Applications, Volume 232, 2024.

[5] J. Doe and A. Smith, "Effective Strategies for Clone Attack Detection in IoT Networks," IEEE Transactions on Information Forensics and Security, vol. 15, no. 3, pp. 750-760, Mar. 2022.

[6] S. Lee and R. Johnson, "Multidimensional Scaling Techniques for Anomaly Detection in Wireless Sensor Networks," IEEE Sensors Journal, vol. 22, no. 6, pp. 2043-2051, Jun. 2023.

[7] M. White et al., "Hybrid Network Vulnerabilities: Addressing IoT Security with Advanced Detection Systems," IEEE Security & Privacy, vol. 18, no. 2, pp. 42-50, Apr. 2021.

[8] L. Davis and K. Green, "Comparative Analysis of Clone and Sybil Attacks in IoT Environments," in Proc. IEEE Symposium on Security and Privacy, San Francisco, CA, 2021, pp. 112-127.

[9] T. Brown, "Security Protocols for Mobile and Static Node Interactions in IoT," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 123-135, Jan. 2022.

[10] F. Miller and P. Thompson, "Parallel Processing Techniques for Improving Security in Hybrid IoT Networks," in Proc. IEEE International Conference on Communications (ICC), Shanghai, China, 2022, pp. 980-985.

[11] H. Nguyen and G. Zhou, "Real-Time Detection of Clone Attacks in IoT Using Machine Learning," IEEE Internet of Things Journal, vol. 20, no. 5, pp. 3774-3786, May 2023.

[12] Y. Zhao, "A Survey on IoT Security: Threats and Solutions," IEEE Access, vol. 7, pp. 82599-82618, 2019.

[13] D. Patel and J. Wang, "Enhanced Techniques for Clone Detection in Wireless Sensor Networks without Geographical Information," IEEE Transactions on Wireless Communications, vol. 18, no. 4, pp. 2164- 2176, Apr. 2019.

[14] K. Lee and M. Choi, "Ontology-Based Security for IoT Networks: A Proposal," in Proc. IEEE International Conference on IoT and Smart City, Tokyo, Japan, 2020, pp. 765-770.

[15] A. Gupta et al., "Blockchain Solutions for Secure IoT Networks," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1112-1123, Nov. 2021.

[16] S. Kumar and L. Zhang, "Advanced Cryptographic Techniques for Fighting Clone Attacks in IoT Devices," IEEE Security & Privacy, vol. 20, no. 1, pp. 18-27, Jan. 2022.

[17] M. Brown and O. Lee, "A Deep Learning Approach to Detecting Clone Attacks in IoT Networks," in Proc. IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, 2022, pp. 348-353.

[18] R. Sharma and T. Singh, "IoT Security Challenges and Solutions: Current Status and Future Directions," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1159-1190, Second Quarter 2021.

[19] C. Wood and A. Qureshi, "Dynamic Behavior Profiling for Security in IoT Networks," IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2054-2066, Jul. 2021.

[20] J. Kim and H. Park, "Review of Recent Developments in IoT Security Mechanisms," IEEE Access, vol. 8, pp. 140992-141007, 2020.

[21] B. Davis and N. Foster, "Techniques for Enhancing Detection of Security Breaches in Sensor Networks," IEEE Sensors Journal, vol. 21, no. 13,pp. 14577-14585, Jul. 2021.

[22] G. Edwards and R. Kumar, "Utilizing MDS for Enhanced Security in Hybrid IoT Environments," in Proc. IEEE Workshop on IoT Security Techniques, Las Vegas, NV, 2023, pp. 640-645.

[23] E. Wilson and F. Khan, "A Framework for Mitigating Clone Attacks in Wireless Sensor Networks," IEEE Network, vol. 35, no. 5, pp. 244-251, Sep./Oct. 2021.

[24] P. Anderson and S. George, "The Role of Advanced Machine Learning in Securing IoT Networks," IEEE Transactions on Artificial Intelligence, vol. 2, no. 1, pp. 58-65, Feb. 2022.
[25] M. Turner and Y. Lee, "Utilizing Neural Networks for Anomaly Detection in IoT Systems," IEEE Transactions on Cybernetics, vol. 19, no. 6, pp. 2156-2167, Jun. 2022.
[26] R. Edwards and C. Murphy, "Adaptive Security Algorithms for Mobile IoT Devices," IEEE Internet of Things Journal, vol. 17, no. 5, pp. 3891- 3902, May 2021.
[27] S. Patel and T. Morris, "Security Implications of Hybrid IoT Architectures," in Proc. IEEE Global Communications Conference, Madrid, Spain, 2021, pp. 1223-1228.
[28] A. Howard and K. Fisher, "Hybrid Approaches to Protect IoT Devices from Clone Attacks," IEEE Security & Privacy, vol. 22, no. 3, pp. 54-62, Mar. 2022.
[29] G. Thompson et al., "Review of IoT Security: Challenges and Solutions," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 660-688, First Quarter 2022.
[30] B. Nelson and J. Carter, "Cryptographic Security for IoT Networks," in Proc. IEEE Symposium on Network Operations and Management, Phoenix, AZ, 2022, pp. 405-410.
[31] V. Singh and M. Gupta, "Machine Learning Techniques for Securing Wireless Sensor Networks," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 305-319, Feb. 2023.
[32] D. Clark and H. Wright, "Efficient Detection Mechanisms for Hybrid Wireless Networks," IEEE Transactions on Mobile Computing, vol. 18, no. 11, pp. 2512-2523, Nov. 2021.
[33] F. Zhou and B. Lee, "Ontology-Based Security Framework for IoT Environments," in Proc. IEEE International Conference on Cloud Computing, Seoul, South Korea, 2022, pp. 738-743.
[34] J. Harlow and S. Reed, "Parallel Detection Algorithms for IoT Security," IEEE Access, vol. 9, pp. 77564-77575, 2021.
[35] K. Walters and P. Davidson, "A Study on Clone Node Detection Using Artificial Intelligence," IEEE Internet of Things Journal, vol. 18, no. 4,pp. 2679-2690, Apr. 2022.
[36] M. Franklin and O. Mitchell, "Strategies for Mitigating Security Risks in IoT and WSN," IEEE Network, vol. 36, no. 2, pp. 112-118, Mar./Apr. 2022.
[37] T. Brooks and N. Harris, "Advances in IoT Security Posture," in Proc. IEEE Conference on Computer Communications Workshops, Virtual, 2023, pp. 102-107.
[38] R. Young and E. Thompson, "Behavioral Analysis for Security in IoT Networks," IEEE Transactions on Industrial Informatics, vol. 17, no. 8,pp. 5743-5754, Aug. 2021.
[39] S. Goldberg and R. Kumar, "IoT Device Authentication Techniques: Current Status and Future Directions," IEEE Communications Magazine, vol. 59, no. 7, pp. 39-45, Jul. 2021.
[40] L. Sanders and G. Patel, "IoT Network Security: A Comprehensive Review," in Proc. IEEE International Conference on Information Networking (ICOIN), Kuala Lumpur, Malaysia, 2023, pp. 88-93.
[41] P. Richardson and Y. Huang, "Securing IoT Against Clone Attacks: Challenges and Research Opportunities," IEEE Security & Privacy, vol. 20, no. 4, pp. 31-40, Jul./Aug. 2022.
[42] O. Daniels and K. Johnson, "Hardware-Based Security Solutions for IoT: An Overview," IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 3, pp. 1233-1244, Mar. 2023.
[43] H. Martinez and J. Rivera, "The Role of Blockchain in Securing IoT Networks," IEEE Access, vol. 10, pp. 99105-99116, 2021.
[44] N. White and A. Grey, "Data-Driven Security Approaches for IoT Systems," in Proc. IEEE Wireless Communications and Networking Conference, San Diego, CA, 2022, pp. 1560-1565.