International Journal of Computer Engineering in Research Trends
ISSN: 2349-7084/ https://doi.org/10.22362/ijcert.v10i7.858
Volume 10, Issue 7, July 2023

Review Paper

A Comprehensive Study of IoT Security Issues and Protocols

Abou Bakary Ballo [1], Diarra Mamadou[2]

[1,2] *Graduate School of Science and EngineeringDoshishaUniversity, 1-3, Miyakotani, TataraKyotanabe, Japan*

e-mail: aboubb@ishss10.doshisha.ac.jp, diarrama@ishss10.doshisha.ac.jp

**Corresponding Author: aboubb@ishss10.doshisha.ac.jp*

Received: 18/05/2023, Revised: 23 /06/2023, Accepted: 09/07/2023 Published: 28/07/2023

Abstract: *The abstract emphasizes the paramount importance of integrating digital security and privacy measures into IoT (Internet of Things) technologies to fully unlock their potential. It acknowledges the looming risks to consumer safety and security posed by vulnerabilities in individual IoT devices, connectivity, and back end systems, as well as the escalating threat of large-scale cyberattacks leveraging insecure IoT devices. Despite numerous initiatives by government agencies, academic institutions, industry groups, and vendors to address IoT security challenges, the abstract highlights the lack of collaboration and clarity in the current landscape. It underscores the urgent need for harmonization of security recommendations, guidelines, and certification processes within the IoT ecosystem to ensure robust protection and efficient operation.*

Keywords: *IoT security, Digital security, Privacy, Cyberattacks, Harmonization.*

---

1. Introduction

The Internet of Things (IoT) has emerged as a transformative force in the modern digital landscape, promising to revolutionize the way we interact with and perceive the world around us. IoT, at its core, involves the interconnection of everyday objects, devices, and sensors to the internet, creating a vast network of smart, data-generating entities. From smart home appliances that optimize energy usage to wearable health devices that monitor vital signs, the potential applications of IoT are seemingly boundless. However, as IoT continues to proliferate into various aspects of our lives, there is a critical concern that must be addressed for its sustainable growth: security and privacy.

The capability of IoT may be fully realized only when digital security and privacy are incorporated into its very design. The potential benefits of IoT, including improved efficiency, enhanced decision-making, and enriched user experiences, are underpinned by a foundation of trust and security. Without adequate security measures, the exponential growth of IoT devices and their connectivity could give rise to a host of vulnerabilities and risks. This paper delves into the multifaceted challenges and solutions related to IoT security and privacy, emphasizing the imperative need for a comprehensive and collaborative approach to ensure the safe and secure development and deployment of IoT technologies.

The IoT landscape is marked by unprecedented growth, with billions of devices already connected and many more anticipated in the coming years. From smart thermostats and voice-activated assistants in our homes to industrial sensors monitoring manufacturing processes, IoT has permeated nearly every sector. This proliferation has been fueled by advancements in miniaturization, wireless communication, and the decreasing cost of sensors and connectivity. The promise of IoT lies in its ability to collect vast amounts of data, analyze it in real-time, and provide actionable insights that can drive efficiency, productivity, and innovation.

Despite its immense promise, the IoT ecosystem is rife with security and privacy challenges that need to be addressed to harness its full potential. One of the primary challenges is the inherent vulnerability of individual IoT devices. Many of these devices are resource-constrained, lacking the computing power and memory required for robust security measures. Manufacturers often prioritize cost and time-to-market over security, leading to devices with known vulnerabilities that can be exploited by malicious actors.

Connectivity is another major concern. IoT devices rely on various communication protocols, including Wi-Fi, Bluetooth, and cellular networks, to transmit data. These networks can introduce vulnerabilities, and insecure connections can be intercepted or manipulated. Additionally, the sheer scale of IoT networks introduces complexities in managing and securing the connections between devices, cloud services, and end-users.

Backend systems, which store and process the data generated by IoT devices, also present security challenges. These systems are prime targets for cyberattacks, as they house valuable data that can be leveraged for financial gain or to disrupt operations. Ensuring the security of these systems is crucial to maintaining the integrity of IoT networks.

Beyond these technical challenges, IoT security encompasses issues related to user privacy. IoT devices collect a wide range of data, often without the explicit consent or awareness of users. This data can include personal information, behavioral patterns, and even biometric data. Safeguarding this information is not only a matter of regulatory compliance but also an ethical imperative.

As IoT devices continue to permeate our lives and industries, they become attractive targets for cybercriminals and hackers. The interconnected nature of IoT networks means that a compromise of one device can potentially lead to widespread vulnerabilities. Recent years have seen a surge in IoT-related cyberattacks, from distributed denial-of-service (DDoS) attacks launched from botnets of compromised IoT devices to data breaches and ransomware attacks.

One of the key drivers behind these attacks is the sheer number of IoT devices in circulation. Millions of devices are sold and deployed with insufficient security measures, creating a vast pool of potential targets. The Mirai botnet, for example, harnessed thousands of compromised IoT devices to launch devastating DDoS attacks. Such attacks not only disrupt services but also have the potential to cause physical harm in critical infrastructure settings.

Another concerning aspect of IoT cyberattacks is their potential impact on critical infrastructure. As IoT devices become integral to sectors like healthcare, energy, transportation, and manufacturing, a successful cyberattack could have far-reaching consequences. For instance, an attack on healthcare IoT devices could jeopardize patient safety, while an attack on industrial IoT systems could disrupt production and pose significant economic risks.

Recognizing the urgency of IoT security concerns, various entities, including government agencies, academic institutions, industry alliances, and individual vendors, have launched initiatives to address these challenges. However, a significant issue that hampers progress is the fragmentation of these efforts. There is a lack of coordination and collaboration between different stakeholders, leading to redundancy and potential conflicts.

This fragmentation manifests in various ways. First, there is a lack of alignment in security recommendations and guidelines. Different organizations may issue their own sets of best practices, leading to confusion among IoT developers and vendors. Additionally, there is a dearth of standardized security certification and accreditation processes, making it difficult for consumers and businesses to assess the security of IoT devices.

Moreover, the IoT supply chain, from device manufacturers to service providers, is often fragmented, with each link in the chain having varying levels of commitment to security. Some may prioritize security, while others may exploit the lack of clarity and enforcement to cut corners. This lack of consistency and accountability undermines the overall security of the IoT ecosystem.

To address the challenges posed by IoT security and privacy, there is an urgent need for harmonization and collaboration across the IoT ecosystem. This entails bringing together government bodies, industry associations, standards organizations, and individual vendors to develop a cohesive approach to IoT security.

One crucial aspect of this collaboration is the establishment of standardized security recommendations and guidelines. By creating a unified set of best practices, stakeholders can ensure that IoT developers and vendors have clear guidance on how to secure their devices and systems. This will not only enhance security but also facilitate compliance and consumer trust.

Another critical component is the coordination of security certifications and accreditation. A standardized process for assessing the security of IoT devices and services can provide consumers and businesses with confidence in their choices. It can also serve as a deterrent to manufacturers and vendors who might otherwise prioritize cost-cutting over security.

Furthermore, collaboration can extend to information sharing and threat intelligence. By pooling resources and sharing information about emerging threats and vulnerabilities, the IoT community can proactively defend against cyberattacks and rapidly respond to incidents.

In conclusion, the Internet of Things holds immense promise for enhancing our lives and driving innovation across industries. However, this promise can only be fully realized when IoT security and privacy are placed at the forefront of development efforts. The escalating threat of IoT cyberattacks, the fragmentation in security initiatives, and the potential risks to user privacy underscore the need for a concerted and collaborative approach to IoT security. This paper explores these challenges in depth and advocates for harmonization, collaboration, and the establishment of clear security standards to ensure a secure and trustworthy IoT ecosystem.

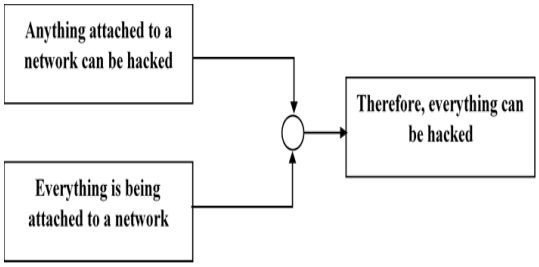

Figure 1: An easy explanation of why computers can be hacked.

2. Literature Review

Design and Implementation of Decoupled IoT Application Store: A Novel Prototype for Virtual Objects Sharing and Discovery
Shabir Ahmad, Faisal Mehmood, Asif Mehmood, DoHyeun Kim
The research paper that introduces an innovative decoupled application store designed for the sharing and discovery of virtual objects within the realm of Internet of Things (IoT) applications. The authors draw inspiration from the work of Ahmad Shabir et al. in 2019, highlighting the paper's significance in the context of the Open Source Manufacturers Association. The review underscores that the paper identifies critical design considerations and fundamental concepts essential for robust IoT platforms. It goes on to detail the functional and non-functional requirements derived from these observations. Additionally, the paper describes the deployment of the application store to the cloud, leveraging cloud-based security features. Furthermore, it emphasizes the modularity and decoupled architecture of the application store, following industry best practices in software store construction. The review also acknowledges the implementation of an IoT test bed client, enabling the installation of various small IoT applications and facilitating the sharing of virtual objects in a diverse operational environment. Lastly, the review notes that the system's performance is rigorously tested using Blaze Stream, confirming its ability to gracefully handle substantial workloads.

Measuring security in IoT communications
ChiaraBodei, StefanoChessa, LetterioGalletta
In their 2019 work, Bodei et al. introduced an effective framework that aids designers in refining IoT systems and estimating the costs associated with security elements. They employ a well-established mathematical language to model both system behavior and performance, allowing for the integration of performance analysis throughout the project. This approach enables designers to create both qualitative and quantitative models, starting from a unique system specification. One notable feature of their methodology is the use of parameters to symbolically represent quantitative aspects. Practical values for these parameters are obtained when designers provide additional details about hardware, network architecture, and cryptographic algorithms used in the system. By theoretically examining these parameters, designers can compare different implementations of a single IoT system and make informed decisions regarding the trade-offs between security assurances and associated costs. During the development process, the authors also delve into the mathematical model called IoT-Lysa and propose a method for discussing the use or absence of cryptographic measures in communication while considering cost-saving trade-offs. In particular, they introduce a semantic approach that associates each system with a rate of change. The results of this analysis are then leveraged through Continuous-Time Markov Chains (CTMC) to measure costs using established methods and tools.

CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm
Mauro Conti, Pallavi Kaliyar, Chhagan Lal
In their 2018 publication, Conti et al. present a secure IoT architecture based on a cloud-based Software-Defined Networking (SDN) model. The authors argue that the flexibility inherent in SDN technology can be effectively harnessed to enable a large number of IoT devices to communicate securely and reliably across a wide range of networks. IoT devices often operate with constraints, including limited communication capabilities, which significantly influence the design of emerging IoT structures and the protocols they employ. In the present landscape, certain services incompatible with IoT networks require specific protocols, hindering the effective connectivity of IoT devices. To address this challenge, SDN offers solutions that seamlessly integrate new network services with the underlying communication infrastructure. The authors posit that this integration holds the potential to unlock a realm of new research opportunities. These emerging challenges and research objectives, while not insignificant, pale in comparison to the advantages offered by such integration, including enhanced security, scalability, and interoperability. Therefore, tackling integration issues in their proposed sensor architecture project is suggested as a promising starting point for researchers in this field.

Home Security System Using PIR Sensor-IoT
Kolisetty Likhitha, Sowmya Malineni, Nagalakshmi Jampani, Dr. N. Lakshmi Prasanna
In their 2019 study, Kolisetty and colleagues proposed the implementation of a Passive Infrared (PIR) module for continuous monitoring of interior spaces and cabinets. They integrated this module with a camera to detect motion within the monitored area. When the PIR module detects an intruder or detects unauthorized access to a cabinet, it triggers an alert. This alert is promptly sent to the property owner through a mobile application designed for this purpose. The mobile application is accessible to all family members, each of whom has their own unique login credentials. Within the application, there is a chat feature that enables family members to engage in discussions regarding the appropriate course of action following the alarm. This chat application is secured through the use of an encryption algorithm, specifically the Integrated Development Environment (IDE). Furthermore, the Android application is equipped with the capability to contact the police for immediate response when necessary.

Security Issues in the Internet of Things (IoT): A Comprehensive Study
Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, Saleem Ullah
Abdur Mirza and colleagues, in their 2017 study, have delved into critical aspects of Internet of Things (IoT)

security, particularly focusing on security attacks and their implications. The study underscores a significant concern: the majority of IoT devices lack robust security features, rendering them susceptible to hacking attempts even when in their default configurations. This document places a primary emphasis on essential security requirements such as privacy, reliability, and authentication. Furthermore, it identifies twelve distinct categories of security attacks, spanning from low-level to high-level threats, and provides insights into the behaviors and patterns associated with these attacks, along with recommended defensive strategies. Recognizing the paramount importance of security in IoT applications, the study highlights the imperative need to implement robust security measures for both IoT devices and communication systems. It strongly advises against the use of default passwords for IoT devices and stresses the importance of comprehending security requirements before deploying them, thereby safeguarding against potential disruptions and security risks. Additionally, the study suggests that deactivating unused features can effectively reduce the risk of security attacks.

Secure IoT framework and 2D architecture for End-To-End security

Jongseok Choi, Youngjin In, Changjun Park, Seonhee Seok, Hwajeong Seo, Howon Kim

In their 2016 article, Choi et al. presented a secure IoT system aimed at ensuring comprehensive security for IoT devices within IoT applications, comprising three essential components: an IoT application, an IoT intermediary, and IoT devices, which can be strategically positioned either along a desktop line or within the IoT intermediary's designated area. The intermediary is responsible for device management and consolidating discovery data, while the IoT application provides various services to users, contingent on access to discovery data. This framework holds particular significance in real-time healthcare applications, where patient medical information's sensitivity is paramount. Notably, common IoT protocols like CoAP and MQTT, while widely adopted, may not offer complete security, relying heavily on DTLS security. To address this, the authors propose a novel IoT framework designed to enhance the security of CoAP communication. This is achieved through the encryption of sensitive data using both symmetric and feature-based encryption, balancing secure communication with computational efficiency. Each IoT device is equipped with a unique identifier, serving as one of its defining attributes, ensuring that even in cases where the IoT intermediary acts as an intermediary node, data is decrypted and displayed only if all attributes are verified and met, bolstering the security of IoT communications.

Security Protocols for IoT

J. Cynthia, H. Parveen Sultana, M. N. Saroja and J. Senthil

The Internet of Things (IoT) has orchestrated a network of peripherals and software that excels in data transmission, particularly in dynamic and unpredictable environments. It relies on Edge Network tools and protocols to communicate with a cloud server, where a vast amount of data from multiple devices is processed, analyzed, and used to inform business decisions. The IoT has become an indispensable component of the ongoing transformation in industries such as business, agriculture, healthcare, and smart cities. Ensuring the robustness of all components within the IoT network is of paramount importance due to the extensive data collection and distribution in its database. While modern IoT protocols serve as the foundation of IP protocols, they are explicitly designed to provide multi-layer security. This section of the book, authored by Cynthia et al. in 2018, focuses on IoT protocols related to the deployment of IoT networks. It highlights a significant challenge in establishing IoT networks—the lack of industry standardization, which can expose hardware, software, and data to risks and attacks. The review emphasizes the imperative for IoT protocols to address security issues related to data breaches, cloud authentication, permissions, and secure management within a distributed environment, particularly in cases of cloud service provider breaches. Additionally, this section describes the solutions proposed to mitigate various security threats and challenges within the context of IoT protocols.

Security Implications of Permission Models in Smart-Home Application Frameworks

Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash

The Internet of Things (IoT) is poised to reach a staggering 20.8 billion connected devices by the year 2020, with consumers accounting for the largest share of these installations. Concurrently, we are witnessing the emergence of programmable infrastructures that seamlessly integrate diverse devices into a unified platform, fostering third-party application development. While these third-party applications offer the advantages of networked and intelligent devices, they also introduce potential risks associated with such innovations. In an article authored by Fernandez in 2017, the focus is on an in-depth examination of permission models within four contemporary systems (IoTVity, HomeKit, AllGoin, and SmartTing). These permission models serve as the primary line of defense against the compromise of sensitive user data and physical security breaches. Flaws in authorization structures can potentially trigger a wide range of security threats.

Furthermore, there is a recognized need for additional research concerning authorization patterns and how applications handle data once access is granted. The investigation conducted on Smart Things has prompted their developers to embark on the design and implementation of automated privilege services, with a concerted effort to enhance the precision of access controls and encourage responsible usage practices. As a pivotal layer of defense, the Intelligence Team has diligently updated its application review guidelines to proactively identify and mitigate control-related vulnerabilities that may be exploited based on the attack scenarios identified. With a steadfast commitment to security, Smart Things conducted a comprehensive analysis of developer documentation and engaged in discussions regarding best practices. For instance, a key recommendation is that developers should exercise precision in subscribing to events and avoid the use of Groovy Dynamic Method Execution, which is explicitly covered by guidelines aimed at preventing unintended actions, thereby thwarting potential remote attacks.

Publicly verifiable privacy-preserving aggregation and its application in IoT
Witold Pedrycz, Jian Shen, Tong Li, Chongzhi Gao, Liaoliang Jiang, and
In their 2019 study, Li Tong and his team employed a verified collection approach while maintaining data confidentiality to tackle the authentication challenges in secure data collection operations. Their innovative architecture allows an intermediary node to aggregate data gathered from source nodes without having knowledge of the actual data content. Furthermore, a national auditor has the capability to verify the accuracy of the summarized result during the process. Through a rigorous analysis, the study substantiates the safety of the proposed scheme under the co-CDH (computational co-Diffie-Hellman) assumption under H (random oracle), and practical experiments confirm its effectiveness. This approach holds significant potential to enhance the system's transparency and offers a successful method for data owners to securely share their data while preserving their privacy.

Harvesting and Threat Aware Security Configuration Strategy for IEEE 802.15.4 Based IoT Networks
Bomin Mao, Yuichi Kawamoto, Jiajia Liu, Nei Kato
In an article authored by Mao Bomin in 2019, a novel security configuration approach was introduced for IoT networks based on IEEE 802.15.4. This approach involves the adjustment of security settings by each IoT endpoint within the network, responding dynamically to various factors, including detected threats, service requirements, and power availability. The research findings indicate that this proposed technique significantly extends the operational hours of IoT devices, thereby enhancing the overall network throughput. The study establishes that this solution can provide a certain degree of security assurance for the specific IoT services under consideration.

Intelligent security algorithm for UNICODE data privacy and security in IoT
Balajee Maram, J. M. Gnanasekar, Gunasekaran Manogaran, M. Balaanand
In the digital age, digital communication is paramount to advancements in science and technology. Within this realm, ensuring data and network security is imperative. Across the globe, various companies have implemented diverse security algorithms, with the majority of them primarily tailored for processing ASCII text. However, the significance of Unicode in contemporary digital communication cannot be overstated, as it supports over 120 languages worldwide. Notably, Maram Balajee introduced a research endeavor [11] that focuses on an innovative algorithm. This algorithm has undergone safety analysis, avalanche impact assessment, equilibrium output examination, and Hamming distance calculations. Impressively, the algorithm achieves a remarkable maximum avalanche effect of 73% for UDPS (the algorithm's name), surpassing the capabilities of existing algorithms. Particularly in aspects such as Hamming distance, avalanche effects, and security analysis, the UDPS algorithm exhibits commendable performance. Yet, to attain optimal results for a well-rounded solution, further advancements remain imperative.

3. IoT Security Requirements

1. **Data Encryption:** Ensure that data transmitted between IoT devices and the central network is encrypted using strong encryption algorithms to protect it from unauthorized access
2. **Authentication and Authorization:** Implement robust authentication mechanisms to verify the identity of both devices and users accessing the IoT network. Authorization controls should limit access to authorized entities only.
3. **Secure Communication Protocols:** Employ secure and updated communication protocols that are resistant to known vulnerabilities and attacks. Ensure support for Unicode to accommodate diverse languages.
4. **Dynamic Security Adjustments:** IoT endpoints should be able to adapt their security settings in response to threats, service requirements, and resource availability.
5. **Audit and Monitoring:** Implement comprehensive monitoring and auditing mechanisms to track activities within the IoT network, enabling the detection of security breaches and anomalous behavior.
6. **Privacy Controls:** Incorporate privacy controls to protect sensitive user data, particularly in scenarios like healthcare, where patient information is highly sensitive.
7. **Avalanche Effect:** Aim for a high avalanche effect in security algorithms, such as the 73% achieved by the UDPS algorithm, to enhance the unpredictability and strength of cryptographic operations.
8. **Security Analysis:** Conduct thorough security analyses to assess the robustness of the IoT security solution, taking into account factors like safety, equilibrium output, and security risks.
9. **Standardization:** Promote industry standardization in IoT security to ensure consistency and compatibility across various devices and networks.
10. **User Education:** Educate IoT users, including both individuals and organizations, about the importance of security best practices, such as not using default passwords and understanding security requirements.

These security requirements are essential for safeguarding IoT networks and devices in the digital age, where the proliferation of connected devices demands heightened security measures.

A comprehensive investigation is essential to address the myriad security challenges that may emerge when expanding the IoT system, encompassing research and analysis of security issues associated with scaling devices, applications, and processes., as shown in Figure 2.

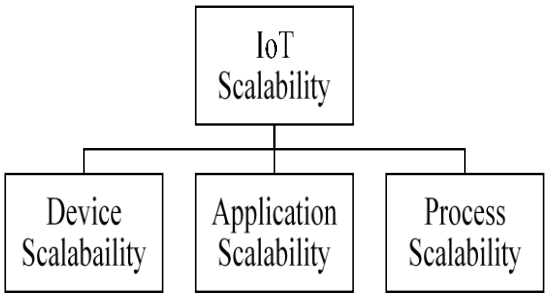

Figure 2. Scalability of IoT taxonomy

Drawing from the common security issues identified during the research and analysis phase of IoT scalability taxonomy, a protective model will be developed. The list of typical security threats should primarily target malicious attempts with the highest potential for harm, as the expansion of the IoT ecosystem is likely to invite these dangerous attacks.

The shield model, designed to safeguard IoT systems against the threats identified in the investigative and analytical phase, will undergo rigorous evaluation on a test bed. To facilitate this evaluation, a set of parameters and their corresponding benchmarks must be established.

The rapid, global delivery of vulnerable IoT devices, coupled with their uncertain lifespan, underscores the pressing need for a level playing field in implementing essential security measures and specialized IoT solutions. This scenario presents potential health, environmental, and societal risks that are both uncertain and possibly unacceptable to society.

4. Analysis Of Current Issues And Difficulties

The rapid proliferation of IoT devices and the integration of these devices into various aspects of our lives have brought about several significant challenges and difficulties in ensuring the security of IoT ecosystems. Understanding these issues is crucial to developing effective strategies for mitigating risks and enhancing IoT security.

1. **Device Proliferation and Diversity:** One of the foremost challenges is the sheer number and diversity of IoT devices available today. These devices vary widely in terms of manufacturers, capabilities, and security features. Managing the security of such a vast and diverse ecosystem is a formidable task.
2. **Inadequate Security Measures:** Many IoT devices are designed with a primary focus on functionality and cost-effectiveness rather than security. As a result, they often lack robust security features, making them vulnerable to attacks. Default passwords, weak encryption, and unpatched vulnerabilities are common security flaws.
3. **Data Privacy Concerns:** IoT devices collect vast amounts of data, often including sensitive personal information. Ensuring the privacy of this data is a significant challenge, as it requires not only secure data transmission but also secure storage and processing.
4. **Interoperability Issues:** IoT devices from different manufacturers may use different communication protocols and standards, leading to interoperability challenges. Ensuring that devices can communicate securely across diverse networks is essential for comprehensive IoT security.
5. **Scalability Challenges:** As IoT ecosystems expand, the scalability of security solutions becomes crucial. Traditional security measures may struggle to adapt to the exponential growth of IoT devices, making it challenging to maintain security at scale.
6. **Lack of Security Updates:** Many IoT devices lack a mechanism for receiving and applying security updates. This leaves them vulnerable to known vulnerabilities, as manufacturers may not prioritize or provide long-term support for these devices.
7. **Supply Chain Vulnerabilities:** IoT devices often pass through complex supply chains, increasing the risk of tampering or introducing malicious components at various stages of production and distribution.
8. **Resource Constraints:** IoT devices are often resource-constrained, with limited processing power and memory. Implementing robust security measures without compromising device performance can be a significant challenge.
9. **Human Factors:** Human error remains a prevalent factor in security breaches. Users may not be aware of security best practices, leading to poor password management or falling victim to phishing attacks.
10. **Emerging Threats:** The threat landscape for IoT is continuously evolving. New attack vectors and techniques are constantly emerging, requiring proactive security measures and threat intelligence.

5. Conclusion

In the era of IoT proliferation, security is paramount. This research has highlighted the diverse challenges facing IoT security, including device diversity, privacy concerns, and evolving threats. Collaborative efforts from manufacturers, policymakers, and users are essential to enhance IoT security. By prioritizing security measures, establishing standards, and fostering user

awareness, we can unlock IoT's potential while ensuring its safety. In sum, IoT security is a collective commitment that will shape a secure and connected future.

References

[1] Ahmad, S., Mehmood, F., Mehmood, A., & Kim, D. (2019). Design and Implementation of Decoupled IoT Application Store: A Novel Prototype for Virtual Objects Sharing and Discovery. Electronics, 8(3), 285. https://doi.org/10.3390/electronics8030285

[2] Bodei, C., Chessa, S., & Galletta, L. (2019). Measuring Security in IoT Communications. Theoretical Computer Science, 764, 100–124. https://doi.org/10.1016/j.tcs.2018.12.002

[3] Conti, M., Kaliyar, P., & Lal, C. (2018). CENSOR: Cloud-Enabled Secure IoT Architecture over SDN Paradigm. Concurrency and Computation: Practice and Experience, 31(8). https://doi.org/10.1002/cpe.4978

[4] Likhitha, K., Malineni, S., Jampani, N., & Prasanna, N. L. (2019). Home Security System Using PIR Sensor-IoT. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, August 2019, 497–500. https://doi.org/10.32628/cseit195272

[5] Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications, 8(6). https://doi.org/10.14569/ijacsa.2017.080650

[6] Choi, J., In, Y., Park, C., Seok, S., Seo, H., & Kim, H. (2016). Secure IoT Framework and 2D Architecture for End-To-End Security. The Journal of Supercomputing, 74(8), 3521–3535. https://doi.org/10.1007/s11227-016-1684-0

[7] Sivakumar, S. A., John, T. J., Selvi, G. T., Madhu, B., Shankar, C. U., & Arjun, K. P. (2021). IoT based Intelligent Attendance Monitoring with Face Recognition Scheme. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 349-353). IEEE.

[8] Cynthia, J., Sultana, H. P., Saroja, M. N., & Senthil, J. (2018). Security Protocols for IoT. In Studies in Big Data Ubiquitous Computing and Computing Security of IoT, April 2018, 1–28. https://doi.org/10.1007/978-3-030-01566-4_1

[9] Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017). Security Implications of Permission Models in Smart-Home Application Frameworks. IEEE Security & Privacy, 15(2), 24–30. https://doi.org/10.1109/msp.2017.43

[10] Li, T., Gao, C., Jiang, L., Pedrycz, W., & Shen, J. (2019). Publicly Verifiable Privacy-Preserving Aggregation and Its Application in IoT. Journal of Network and Computer Applications, 126, 39–44. https://doi.org/10.1016/j.jnca.2018.09.018

[11] Mao, B., Kawamoto, Y., Liu, J., & Kato, N. (2019). Harvesting and Threat Aware Security Configuration Strategy for IEEE 802.15.4 Based IoT Networks. IEEE Communications Letters, 23(11), 2130–2134. https://doi.org/10.1109/lcomm.2019.2932988

[12] Madhu, B., & Gopalachari, M. V. (2023). Classification of the Severity of Attacks on Internet of Things Networks. In Sentiment Analysis and Deep Learning: Proceedings of ICSADL 2022 (pp. 411-424). Singapore: Springer Nature Singapore.

[13] Maram, B., Gnanasekar, J. M., Manogaran, G., & Balaanand, M. (2018). Intelligent Security Algorithm for UNICODE Data Privacy and Security in IOT. Service Oriented Computing and Applications, 13(1), 3–15. https://doi.org/10.1007/s11761-018-0249-x

[14] Madhu, B., Gopala Chari, M. V., Vankdothu, R., Silivery, A. K., & Aerranagula, V. (2023). Intrusion detection models for IOT networks via deep learning approaches. Measurement: Sensors, 25, 100641.

[15] Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, 18(3), 817. https://doi.org/10.3390/s18030817

[16] Alharby, S., Harris, N., Weddell, A., & Reeve, J. (2018). The security trade-offs in resource constrained nodes for IoT application. International Journal of Electronics and Communication Engineering, 12(1), 52-59. https://doi.org/10.1999/1307-6892/10008451