Emerging Trends and Challenges in Securing IoT Devices from Cyberattacks

Stuart N. Howard III

Old Dominion University

IDS300: Interdisciplinary Theory and Concepts:

Dr. Kathryn L. Lafever

30 July 2023

Abstract

The Internet of Things (IoT) has revolutionized various sectors, offering convenience and efficiency. However, this technological advancement comes with the risk of cyberattacks, making IoT security an urgent necessity. This comprehensive research draws insights into cybersecurity, sociology, and legal studies to illuminate the challenges and conflicts in securing IoT devices. Our primary objective is to answer the fundamental question: "What are the emerging trends and challenges in securing Internet of Things (IoT) devices from potential cyberattacks, and what strategies can be employed to mitigate these risks?" An interdisciplinary approach enables us to draw on the strengths of multiple disciplines, identify connections and synergies, and provides a comprehensive approach to adopting and addressing the complexities of securing IoT devices.

Keywords: *Internet of Things (IoT), cybersecurity*

Emerging Trends and Challengers in Securing IoT Devices from Cyberattacks

Introduction

The growing concern over the security of Internet of Things (IoT) devices in the face of increasing cyberattacks presents a relevant problem to explore. This research aims to answer the research question: What are the emerging trends and challenges in securing Internet of Things (IoT) devices from potential cyberattacks, and what strategies can be employed to mitigate these risks? By employing the disciplines of cybersecurity, sociology, and legal studies, this research provides a comprehensive understanding of IoT security. Through the lens of cybersecurity, we analyze the technical aspects and threat landscape of IoT security. Sociological perspectives help us explore the societal implications and ethical considerations, while legal studies allow us to investigate the regulatory frameworks and legal challenges. An interdisciplinary approach enables us to draw on multiple disciplines' strengths, identify connections and synergies, and develop effective strategies. Justification for this research holds significant importance as IoT technologies become integral to various industries. The increasing reliance on IoT devices raises concerns about cybersecurity and privacy risks. Understanding the emerging trends and challenges in securing IoT devices is essential to safeguard users, industries, and critical infrastructure.

The key terms that will be defined are *Internet of Things*, *Cybersecurity*, and Cyberattacks, are terms I will define. The *Internet of Things* is a comprehensive system that connects various computing devices, digital machines, mechanical apparatuses, animals, people, and objects that provide unique identifiers and possess the capability to generate vast amounts of information over a network that does not necessitate further human-to-human or human-to-computer engagement (Ghandour & J. Woodford, 2021).

Craigen et al. (2014) define *Cybersecurity* is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights. *Cyberattack is* malicious actions or attempts to breach the security of IoT devices with the intention of causing harm, stealing data, or gaining unauthorized access.

Cybersecurity

The Internet of Things (IoT) has become an integral part of our lives, revolutionizing how we interact with technology and enhancing efficiency across various sectors. In recent years with the advancement of technology, IoT has been incorporated into various industries, including fitness, health, agriculture, infrastructure, smart homes, smart cities, self-driving cars, drones, and others (Ghandour & J. Woodford, 2021). However, as our dependence on IoT devices grows, so does the threat of cyberattacks. Safeguarding IoT devices from these potential threats is not just a priority; it is necessary to ensure a secure and dependable future for IoT technologies. The difficulty increases as IoT devices have the option to control crucial industry infrastructure, but can the reliability and security of IoT be trusted despite not being well defined and designed, or still use parts of old architecture from the "wired" era (Radovan & Golub, 2017)? This system employs a mechanism that governs the physical environment by analyzing and processing the data generated by sensor devices (Bertino et al., 2016)—the number of device increase each year, which increases the threats. According to Bertino et al. (2016), IoT devices reached it will reach 75 billion in 2025 and 500 billion in 2030. Although IoT devices have been beneficial to the user, there are some concerns about the vulnerability of IoT to cyberattacks. In 2016, as per research conducted by H.P., it was observed that every IoT device was subjected to an attack every two minutes. Additionally, the same research reveals that nearly 70% of smart

devices are susceptible to threats. Furthermore, another study by H.P. indicates that during the testing phase, 90% of devices have accumulated personal information (Bertino et al., 2016). Analyzing common vulnerabilities and trends of IoT devices is essential for understanding the weaknesses that cybercriminals could exploit.

The rapid increase of IoT devices brings a host of cybersecurity trends and challenges that demand attention. Radovan and Golub (2017) have identified several trends regarding IoT security, including the absence of established or demonstrated security standards, the rapid expansion of electronic devices, communication protocols, protection against cyber threats, safeguarding user privacy, and establishing consumer trust. IoT faces numerous security challenges from different aspects, like communication protocols and hardware, less memory, and short batteries cause low computational power devices, gateways connect may cause security issues, nodes may cause an information breach, and an intruder can cause issues by manipulating a device physically (Bertino et al., 2016). As IoT technology becomes more prevalent in infrastructure, industries, and healthcare, the potential impact of successful attacks grows significantly.

We must adopt a proactive approach to cybersecurity to address these challenges and safeguard the expanding IoT landscape. Radovan & Golub (2017) recommended the importance of using existing security technologies in IoT and the need for a more systematic approach to IoT security. Additionally, the development and deployment of IoT services without adequate security measures expose them to cyber threats, and as IoT becomes more prevalent in daily life, the risks associated with cyber exploitation and malicious threats increase (Bertino et al., 2016). While the IoT has brought unprecedented convenience and efficiency to various aspects of our lives, the escalating number of IoT devices also gives rise to significant cybersecurity concerns.

However, this is not a challenge that can be tackled in isolation. Understanding the latest trends and challenges in IoT security is crucial in devising effective strategies to protect users, industries, and critical infrastructure from the ever-evolving threats posed by cybercriminals.

Sociology

The societal implications of IoT security cannot be overlooked. Users must be empowered with knowledge and awareness of IoT devices to ensure their participation in the security process. IoT has impacted society, and a sociological perspective is essential in exploring the societal implications and ethical considerations associated with securing IoT devices. Bertino et al. (2016) have asserted that the domain of smart homes has become essential due to the rapid growth of IoT. While it is highly advantageous for users as it offers numerous amenities, it is concurrently plagued by several security concerns that necessitate resolution. The difficulty arises when one considers that many end users are not furnished with sufficient direction and instruction to accomplish this task, and manufacturers have little motivation to assist them in their endeavors. This challenge can be attributed to the insufficiency of IoT security documentation that bolsters the creation of secure IoT devices (Sereda & Jaskolka, 2022). Sereda and Jaskolka (2022) provide significant insight toward comprehending the societal effects of IoT devices, underscoring the importance of involving end-users in the documentation process at a level comparable to that of manufacturers. Ensuring the end-user has a comprehensive knowledge of IoT devices will aid in security enhancements. This could build consumer trust, considering that deploying IoT devices raises concerns about privacy, data protection, and the potential impact on human behavior.

Legal

The rapidly evolving IoT landscape poses legal questions regarding data protection and compliance with existing laws. The existence of disparate parties, each adhering to distinct legal and regulatory frameworks and possessing divergent incentives, engenders a heightened level of intricacy regarding the legal, privacy, and cybersecurity challenges confronting innovative energy technology (Mylrea, 2017). The current trends and challenges of IoT devices could lead to a breach of users' data which could have legal considerations surrounding IoT security, including the role of governmental agencies, regulatory frameworks, and the development of appropriate legal standards.

Users are unaware of the nature and extent of data collected and how it is employed. Notably, small-print end-user license agreements are frequently disregarded. Users of smart energy technology are familiar with sharing information yet unaware of the data being collected and its use. End-user license agreements are ignored, and the scope of data collection and use of private information is not always understood (Mylrea, 2017). Several privacy laws, including the Privacy Protection Act of 1974, the Federal Trade Commission Act, and State consumer protection laws, are outdated and have not adapted to new technology (Mylrea, 2017).

While there is a lack of legal regulation for the IoT, there are several modules that could be a source of guidance to establish a legal framework. Mylrea (2017) claims that the European Union (EU) has more advanced privacy laws than the USA, especially in the Digital Age. Recently, the Council of the European Union approved new data protection and privacy laws for all 28 Member States and established a pan-European framework. The New European law requires companies to seek approval from pan-European authorities to operate in any European Member State. Moreover, despite numerous nations globally adopting a strategic approach towards enhancing their Internet of Things (IoT) proficiency, the United Arab Emirates (UAE)

persistently exhibits indications of bold and daring modifications in their legal framework to facilitate innovation and investment in IoT, they pushed the Telecommunications Regulatory Authority (TRA) to issue the IoT regulatory Policy (Ghandour & J. Woodford, 2021). “Although UAE has no data protection law, the newly regulations of the IoT Policy and Procedures put forward by the TRA may be acted upon as such (Ghandour & J. Woodford, 2021).”

It is difficult to overstate both the importance as well as the complexity of IoT; however, there is an importance to ensuring that there is a legal, ethical, and regulatory framework. A legal analysis the opportunities and challenges of innovative energy technology from a legal perspective, focusing on privacy laws, cybersecurity regulations, and recent legislation in Europe and the USA (Mylrea, 2017). Additionally, the UAE has given TRA control and oversight of the entire IoT services in the country (Ghandour & J. Woodford, 2021). There is a need to implement an IoT legal framework for the U.S., and countries like the EU and UAE are setting the example and establishing policies and procedures that the US can follow their example.

Creating Common Ground

This interdisciplinary research discloses three significant findings. First, it is evident from the contributions of cybersecurity and sociology that secure communication protocols play a critical role in enhancing IoT security. Cybersecurity analyzes trends in IoT standards regarding security, which will mostly depend on developing security standards, user behavior, and education in the next few years (Bertino et al., 2016). Second, the analysis from cybersecurity and legal disciplines reveals the challenges in securing IoT devices. Cybersecurity research emphasizes the need for research and coordinated efforts to address these concerns and identify potential research topics to enhance the security and reliability of IoT services (Bertino et al., 2016). Finally, the insights from sociology and legal disciplines highlight the significance of

collaboration for IoT security standards. Sociological and legal research emphasizes the need for legal frameworks and providing users with a better understanding of IoT to prevent cyberattacks (Mylrea, 2017; Sereda & Jaskolka, 2022). These points of common ground demonstrate the shared concerns and objectives among cybersecurity, sociology, and legal studies in addressing the challenges of securing IoT devices from cyberattacks. Specific insights and connections might not have been discovered without interdisciplinary research due to each discipline's limited scope and perspective. Each discipline brings its unique lens to examine the research question. By solely focusing on one discipline, researchers may miss the broader picture and fail to identify critical aspects that contribute to the understanding of securing IoT devices from cyberattacks.

Disciplinary Conflicts

While interdisciplinary research enriches the analysis of IoT security, it may also give rise to inevitable conflicts between the disciplines involved. Cybersecurity, sociology, and legal studies each have methodologies, terminologies, and approaches to problem-solving. These differences can lead to challenges in communication and collaboration, especially when researchers from different disciplines have varying interpretations of the data and its implications. One potential conflict could arise between cybersecurity's technical focus and sociology's social focus. Cybersecurity researchers may emphasize the implementation of technical solutions to address vulnerabilities in IoT devices, while sociologists may highlight the importance of considering the human factor in securing these devices. Finding a balance between technical measures and user awareness is essential to tackle IoT security issues effectively.

Constructing a More Comprehensive Understanding or Theory

Drawing upon insights from cybersecurity, sociology, and legal studies, this interdisciplinary research paper endeavors to construct a more comprehensive understanding of securing IoT devices from cyberattacks. By integrating knowledge from these disciplines, we aim to form a unified framework considering IoT security challenges' multifaceted nature. Our analysis reveals common ground in recognizing the critical importance of IoT security and the need to involve end-users in the security process. The technical focus of cybersecurity complements the social perspective of sociology, underscoring the significance of both technical measures and user awareness in securing IoT devices. Understanding these shared vulnerabilities allows us to develop targeted strategies for mitigating risks and enhancing IoT security. By constructing this holistic understanding of IoT security, we aim to pave the way for proactive measures that anticipate and prevent potential cyber threats. Through interdisciplinary collaboration and effective communication of our findings, we seek to influence policymakers, industries, and end-users to prioritize IoT security, thus ensuring a secure and dependable future for IoT technologies.

Reflecting On, Testing, and Communicating the Understanding or Theory

This interdisciplinary research aims to construct a comprehensive understanding of securing IoT devices from cyberattacks by integrating cybersecurity, sociology, and legal studies insights. It recognizes the critical importance of involving end-users in the process. The technical focus of cybersecurity complements the social perspective of sociology, highlighting the significance of both technical measures and user awareness. Identifying common vulnerabilities and threats in IoT devices, such as communication protocol issues and inadequate security standards, guides the development of targeted strategies for risk mitigation.

Moreover, the research emphasizes the societal implications of IoT security, advocating for empowering users with comprehensive knowledge to foster security awareness and build consumer trust. Legal considerations explore the regulatory landscape and the balance between compliance and technological innovation. Rigorous reflection on methodologies and biases enhances the robustness of the research, while real-world testing involving industry stakeholders and end-users validates the proposed IoT security measures.

Conclusion

In conclusion, this research paper delves into the emerging trends and challenges in securing IoT devices from cyberattacks, drawing upon insights from cybersecurity, sociology, and legal studies. The comprehensive understanding constructed through interdisciplinary collaboration emphasizes the critical importance of IoT security and the need to involve end-users in the process. By recognizing common vulnerabilities and threats, such as communication protocol issues and inadequate security standards, targeted strategies for risk mitigation can be developed. Moreover, the research highlights the societal implications of IoT security, advocating for user empowerment and knowledge dissemination to foster security awareness and build consumer trust. Legal considerations shed light on the regulatory landscape and the delicate balance between compliance and technological innovation. Practical communication efforts disseminate knowledge widely, engaging policymakers, industries, and end-users, to promote a collective sense of responsibility in safeguarding IoT devices.

By fostering a proactive and unified approach, this interdisciplinary effort aims to protect users, industries, and critical infrastructure from the ever-evolving threats posed by cybercriminals, securing a dependable and trustworthy future for IoT technologies. Emphasizing the importance of interdisciplinary collaboration, this research demonstrates the value of

integrating diverse perspectives to comprehensively address IoT security's complexities. As IoT devices continue to revolutionize various sectors of our lives, the insights presented in this paper provide a foundation for creating resilient and secure IoT ecosystems that can thrive in the face of emerging challenges and trends.

References

Bertino, E., Choo, K.-K. R., Georgakopolous, D., & Nepal, S. (2016). Internet of Things (IoT). *ACM Transactions on Internet Technology*, *16*(4), 1–7. https://doi.org/10.1145/3013520

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/defining-cybersecurity/docview/1638205509/se-2

Ghandour, A., & J. Woodford, B. (2021). Regulating internet of things: The case of the United Arab Emirates. *TEM Journal*, 1031–1038. https://doi.org/10.18421/tem103-04

Mylrea, M. (2017). Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges. *The Journal of World Energy Law & Business*, *10*(2), 147–158. https://doi.org/10.1093/jwelb/jwx001

Radovan, M., & Golub, B. (2017). Trends in IOT security. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. https://doi.org/10.23919/mipro.2017.7973624

Sereda, B., & Jaskolka, J. (2022). An evaluation of IOT security guidance documents: A shared responsibility perspective. *Procedia Computer Science, 201,* 281–288. https://doi.org/10.1016/j.procs.2022.03.038