Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 07 July-2024, Page No.- 4439-4442

DOI: 10.47191/etj/v9i07.13, I.F. – 8.227

Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices

Rohith Vallabhaneni

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands, USA

ORCID: 0009-0003-3719-2704

ABSTRACT: IoT has revolutionized life around us very quickly. All houses, offices, and even most of the cities in turn are a blanket or mosaic figured out by inter-woven devices keeping to each other; this shows how life was finally distracted. It is presented as a technological marvel that will make life simpler, more efficient, and connected more than it has ever been. However, beneath this gleaming surface lurks a growing threat: the widespread nature of vulnerabilities in IoT devices. The systematic review method is the basis of this study, using Google Scholar and keywords such as "IoT security and consequences", to retrieve scholarly articles pertaining between 2015 – 2023. Research articles that had strict inclusion criteria were considered to evaluate their applicability in the relationship between IoT security vulnerabilities and ordinary lives.

These consequences include from information leakage to denial-of-service attacks and unauthorized access. The risks and scale differences from economic losses to life safety hazards that threaten public security due to an intensifying interdependency of IoT applications. The repercussions impact the key segments such as health care and military applications, where more stringent security measures can be highlighted.

KEYWORDS: IoT, Security Vulnerabilities, Cyber-attacks, Privacy Violations, Mission-Critical Infrastructure.

1. INTRODUCTION

The potential of the Internet of Things (IoT) to change our everyday lives is quickly manifested in private and commercial web-based interactions, knitting itself into even the most mundane aspects of home offices. From smart thermostats and connected refrigerators to fitness trackers, self-driving cars promise convenience, efficiency, and a seamless, interconnected world [1]. The global Internet of Things market is forecasted to reach $11 trillion by 2025 [2]. More than thirty billion connected devices will have been installed on various continents by then. This rapid growth highlights the rise of vulnerable devices in our lives. Research by Schiller et al. [3] also suggests that the number of active IoT devices will swell to 75 billion a year from now. The rapid growth of IoT devices results from the ability to gather, process, and exchange data autonomously. These not only ensure smooth communication but also automate processes easily. Meneghello et al. [4] highlighted how these devices are everywhere now, which calls for an urgent examination of their security weaknesses. Threats related to IoT security also go beyond the digital sphere, encompassing physical risks, as Sivaraman et al. [5] exemplified in their study examining smart IoT devices installed in homes. As IoT technology advances, the possible outcomes of security breaches are more and more intricate.

According to Chen et al., the rapid development of IoT applications has led to the emergence of critical threats that significantly demand strong security measures. Since critical applications are interconnected, the risks arising from unauthorized access to data, breaches, and service disruptions could affect economic well-being, lifesaving, and public security [6]. In addition, Butun et al. [7] draw attention to security issues in mission-critical applications such as military and medical missions, where compromising IoT systems could lead to severe consequences. With IoT devices penetrating all areas of life, be it healthcare and industry or smart homes, one has to realize how vulnerable these can become regarding security implications.

II. MATERIALS AND METHODS

A. Search Strategy

A comprehensive search strategy was used to collect a set of scholarly articles discussing the effects of IoT security vulnerabilities on everyday lives. The leading search engine used for this study was Google Scholar, which is popular due to its broad scope of scholarly literature. The search was

conducted using a combination of relevant keywords and phrases to locate articles specifically targeting "IoT security and its consequences". These selected search terms were created not only to cast the widest net possible but also to ensure relevance concerning what the research is focusing on.

B. Search Terms

The search terms employed in Google Scholar included variations and combinations of key phrases such as:
"IoT security vulnerabilities"
"Consequences of IoT security breaches"
"Impact of IoT security on daily life"
"Security risks in Internet of Things"
"IoT threats and consequences"

C. Inclusion and Exclusion Criteria

The inclusion criteria were specified as limited to scholarly articles, conference proceedings, and books that have been published in reputed journals with an emphasis on the impact of IoT security vulnerabilities. The literature review included only articles published in English. The eligibility criteria included removing articles that did not specifically address how IoT security weaknesses translated into daily life implications. Further exclusion criteria considered grey literature, non-peer-reviewed sources, and articles that did not provide adequate information on consequences to ensure the scholarly nature of this review.

D. Article Selection

Searching concerned a systematic review of the search outcomes derived from Google Scholar. The relevance of each article to the research question was based on its title, abstract, and keywords. Subsequently, full-text versions of potentially relevant articles were accessed for further evaluation.

E. Data Extraction

The review of selected articles was conducted with a high level of thoroughness to generate the required information on possible effects caused by IoT security vulnerabilities. During data extraction, the following key aspects were taken into consideration: types of vulnerabilities investigated, methodologies used in research, and findings made on everyday activities.

F. Analysis

The data was analyzed using a qualitative synthesis approach. Results from each article were arranged by shared themes and patterns, allowing an overall sense of the varied impact that security vulnerabilities in IoT can have on people's everyday lives.

III. FINDINGS

A. Key Consequences

Data Leakage and Privacy Risks

Data leakage and privacy risks emerged as the major themes in terms of the consequences of IoT security breaches. Meneghello et al. [4] shed light on how risky issues like data leakage can be. In the event of data leakage, information that might have sensitive aspects goes out of IoT devices and presents itself as ominous or harmful regarding people's privacy and other confidential matters. Risks of compromise of sensitive information occur when there is a possibility to tamper with the IOT devices to gather cryptographic secrets or modify software. Similarly, Arias et al. [8]and Sivaraman et al. [5] focused on privacy and security concerns associated with home IoT devices. Although IoT technology provides many advantages like energy conservation and convenience, many Internet-connected devices do not have built-in security measures, making them ideal for potential cyberattacks. Compromised webcams or health monitoring devices could give unauthorized access to others who can harm or embarrass their users. Chen et al.[9] analyzed emerging and crucial threats to security privacy in IoT applications They argued that applications of such a large scale and variety create an environment where adversaries can more easily take advantage – either rendering the application useless or stealing what is sensitive information. Chen et al. [9] stressed that security procedures for IoT applications should be strong enough to counteract these new threats. As Neshenko et al. [10] mentioned, trust and confidence issues are some of the major effects caused by security incidents related to IoT technology. Individual privacy and crucial infrastructure such as businesses are also among high-profile cases of leaking information that is considered confidential or Denial of Service attacks.

Compromised Critical Infrastructure

The second theme is that security breaches on IoT may lead to critical infrastructure being compromised. The risk of DoS attacks on IoT devices reported by Meneghello et al. [4] is significant, negatively affecting the operation capability within such interdependent components. The usability of these devices can also get hidden by illegitimate packets, conditions for routing attacks, and eavesdropping which often raises questions about their reliability as well as the availability of services. Breach results in illicit penetration into the networks of IoT systems where they are apt to breaches, thereby rendering another threat risking their security and integrity as stemming from weak-security mechanisms steered by rogue players who may access accumulate or command these devices. As Meneghello et al. [4] stated, the scenario is worrying because IoT devices could be used to infiltrate more extensive networks. Security risk refers to the fact that vulnerabilities of IoT devices

would provide an opportunity for attackers to gain a foothold to penetrate and compromise more extensive networks. Industrial Disruption in the IoT Business was explored by Chen et al. This vulnerability might be significant in critical systems, which cannot rest and require uninterrupted operation, such as healthcare equipment or industrial control software. Zhou et al. [6]identified public and national security risks, including cyber-attacks on IoT devices in critical sectors such as industry, military, etc. A 2023 report by the World Economic Forum warns that cyberattacks on critical infrastructure are one of the top five global risks facing the world in the coming decade. This underscores the urgent need to address security vulnerabilities in IoT devices used in crucial systems.

Safety and security risks

Safety and security risk is another theme that emerged from the analysis. Butun et al. [7]pointed out that the security of Wireless Sensor Networks WSNs and IoT is a matter to be reckoned with. For instance, security breaches could lead to more severe consequences in tactical military applications or healthcare systems, such as casualties and exposure to confidential health data. Security issues include the overall IoT ecosystem rather than just specific devices. Ling et al. [11] and Li, et al. [12]. As security risk implications of demand response, it would be especially devastating in sensitive environments such as healthcare due to compromised smart plugs, which can wreak havoc on its operation series, a case that is witnessed when dealing with commercial or industrial buildings. In 2020, a cyberattack targeting a water treatment plant in Florida involved exploiting vulnerabilities in an IoT-enabled system. This incident highlights the potential for attackers to disrupt critical infrastructure with potentially life-threatening consequences.

Table 1: Major themes

Author(s)	Major themes
Meneghello, et al. (2019); Arias, et al. (2015); Sivaraman, et al. (2018); Li, et al. (2016); Neshenko, et al. (2019) and Chen, et al. (2018)	Data and Privacy Vulnerabilities
Zhou, et al. (2018); Neshenko, et al. (2019), and Tankard, (2015)	Compromised critical infrastructure
Butun, et al. (2019); Zhou, et al. (2018); Ling et al. (2017); Neshenko, et al. (2019) and Tankard, (2015)	Safety and security risk

B. Internet of Things Vulnerabilities

Weak security mechanism

Although the threats to IoT security are mainly digital, they also include physical risks – particularly concerning smart homes and industrial uses. Sivaraman et al. [5] examined intelligent IoT devices in homes and their privacy concerns about security. However, the downside of automation and efficiency gained through IoT devices is due to their ineffective built-in security that results in unlawful access. Hacking into webcams or health monitoring devices may affect privacy, from simple spying to disclosing private medical information. One of the most essential vulnerabilities that undermine security and integrity in Smart systems is unauthorized, illegal network access. Meneghello et al. [4]noted that some IoT devices have weak security policies as a result of unauthorized access, which could allow malicious actors to manipulate or remotely control connected appliances. It is not only related to the equipment but the whole IoT landscape where hackers manage unauthorized access that can compromise bigger networks.

Scale and diversity

The widespread IoT is deeply intertwined with sizable vulnerabilities that could lead users to different threats. Scale and diversity make IoT more vulnerable to security breaches. However, as Butun et al. [7]stated WSNs do not have any alternative physical way of defending against cyber threats. With such characteristics, the integration of WSNs into IoT also makes them more vulnerable. In security-critical application areas, WSNs and the new IoT technology are vulnerable. WSNs and IoT constitute specific platforms not to mention that they are used in critical areas such as military applications or healthcare systems representing an ideal environment for security risks. According to Chen et al. [9], one of the reasons for this is that with fast deployment, there are new and critical threats emerging towards IoT security as well IoT systems becoming more vulnerable, adversaries can get into them and use those holes. Additionally, the breadth and variation in these applications ensure easy illegitimate access as attackers can disable an application's functionality, steal sensitive information, or render that function useless. This can be attributed to the weaknesses and vulnerabilities in underlying architectures that are a part of IoT.

Lack of standards for resource-limited devices

Secondly, there are no established standards when implementing and managing IoTs which leaves them exposed to security breaches. According to Frustaci et al. [13], one of the major weaknesses is that there are no general security protocols for IoT devices with limited resources and heterogeneous technologies. The Internet of Things is vulnerable to cyber threats, as IoT devices are not powered by unlimited processing power, memory space, and

communication capacity. The lack of specific standards for such devices leaves IoT ecosystems vulnerable to exploitation, making ensuring robust security more complicated.

IV. CONCLUSION

As can be seen from the results, it is necessary to work with the security vulnerabilities of IoT devices because they are increasingly being used and firmly entered into everyday life. Identified consequences include data leakage and denial of service attacks as well as unauthorized access. IoTs are interdependent and create unprecedented threats that fall outside consideration of cost or privacy alone. But they can also be able to influence wider issues in public safety. According to the reviewed literature, this calls for proactive and vigorous security measures.

In addition, the discussion of different areas like health care infrastructure, military applications-based approaches as well as convenient homes brings forth a requirement for individualized security measures to protect sensitive data and frail infrastructures. With the advancement in IoT technology, addressing these vulnerabilities becomes paramount to enable seamless and proper integration with enabling instruments. This synthesis lastly gives priceless observations to policymakers and business professionals for understanding the subtle consequences of IoT security vulnerabilities. It also guides future initiatives aimed at enhancing resilience within an IoT ecosystem.

ACKNOWLEDGEMENT

We would like to thank anonymous reviewers for their helpful feedback

REFERENCES

1. A. Thierer and A. Castillo, "*Economic perspectives projecting the growth and economic impact of the internet of things*." George Mason University, Mercatus Center, June 15.
2. B. B. Rad Babak and H. A. Ahmada, "Internet of things: trends, opportunities, and challenges," *IJCSNS International Journal of Computer Science and Network Security*, vol. 17, no. 7, pp. 89–95.
3. E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," *Computer Science Review*, vol. 44. Elsevier Ireland Ltd, May 01, 2022. doi: 10.1016/j.cosrev.2022.100467.
4. [4] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet Things J*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.
5. V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT Devices in the Home: Security and Privacy Implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, Jun. 2018, doi: 10.1109/MTS.2018.2826079.
6. W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019, doi: 10.1109/JIOT.2018.2847733.
7. I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 616–644, Jan. 2020, doi: 10.1109/COMST.2019.2953364.
8. O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, Jun. 2015, doi: 10.1109/TMSCS.2015.2498605.
9. S. Z. Z. L. Y. Z. Q. D. S. R. & Y. J. Chen Kejun, "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice.," *Journal of Hardware and Systems Security*, vol. 2, pp. 97–110, 2018.
10. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.
11. Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System," *IEEE Internet Things J*, vol. 4, no. 6, pp. 1899–1909, Dec. 2017, doi: 10.1109/JIOT.2017.2707465.
12. S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Research*, vol. 26, no. 2, pp. 337–359, Apr. 2016, doi: 10.1108/IntR-07-2014-0173.
13. M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J*, vol. 5, no. 4, pp. 2483–2495, 2018, doi: 10.1109/JIOT.2017.2767291.