IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 1)
Available online at: www.ijariit.com

Cybersecurity risks associated with the Internet of Things: A review of related literature

Davis Matovu
davismatovu@yahoo.com
Masinde Muliro University of Science and Technology, Kakamega, Kenya

Mutua Stephen
makau@gmail.com
Masinde Muliro University of Science and Technology, Kakamega, Kenya

Mugeni Gilbert
gbmugeni@gmail.com
Communication Authority of Kenya, Nairobi, Kenya

Karume Simon
smkarume@gmail.com
Laikipia University, Eldoret, Kenya

Gilbert Gilibrays Ocen
gilbertocen@gmail.com
Busitema University, Tororo, Uganda

ABSTRACT

The Internet of Things (IoT)is the network of physical objects accessed through the Internet that can identify themselves to other devices and use embedded technology to interact with internal states or external conditions. The continued growth of the internet of things phenomenon has led to an influx of a number of cybersecurity risks. This paper aimed at analyzing the most common classes of cybersecurity threats associated with IoTs and their impact on the security of the information systems. To achieve this, we examined and reviewed cybersecurity risks related literature of the IoT leading to the specification of the Internet of the Things cybersecurity landscape. Finally, this review provides insights for cybersecurity risks evolution, suggesting tools, methods and potential approaches that can help ensure a safe IoT environment.

Keywords— *Internet of things, Cybersecurity risk, Security threats*

1. INTRODUCTION

The development of information and communications technologies (ICTs) enables businesses and individuals to communicate and transact with other parties electronically, instantaneously and internationally (Marco, 2010). Among these developments has been the advent of the Internet of Things (IoT) phenomenon which represents a major transformation in a digital world that has the potential to affect everyone and every business. The Internet of Things (IoT) is the network of physical objects accessed through the Internet that can identify themselves to other devices and use embedded technology to interact with internal states or external conditions Treffyn et al, 2013). According to Somayya, Ramaswamy, & Tripathi (2015), the Internet of Things is a novel paradigm shift in IT arena and is defined as an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face of situations and changes in the environment. IoT describes a world where just about anything can be connected and communicate in a smart mode by combining data to produce usable intelligence. With the IoT, the physical world is becoming one big information system with the ultimate goal of improving the quality of life and empowering new business models. However, this also means that more personal information and business data will exist in the cloud and be passed back and forth through thousands of devices that may have vulnerabilities Cybercriminals are able to exploit the existence of a global digital world even in the presence of the necessary regulatory frameworks, laws, and related enforcement capability. In this paper, we identify and examine cybersecurity risks as enumerated in selected Information systems and from engineering research journals. We classify the papers to create taxonomies of the cybersecurity risk types in existence. Using these classifications, we observe the impacts between types of IoT cybersecurity risks and the methods used to mitigate them.

2. DATA

Secondary data was collected from selected published cybersecurity papers in major Information Systems and engineering journals. We selected ten peer-reviewed journals with specific publications on cybersecurity risk related articles (Table 1). Since computer and information security researchers in the Information Systems discipline have traditionally published at least some of their research in engineering journals, we also included those engineering journals that are most important to the Information System discipline.

Five selected journals are in the core Information Systems discipline and five are in computer science and engineering. All of them are listed in prominent positions on the SJR Journal ranking lists (2018).

An online search for cyber security risk papers using standard search engines such as Google Scholar was done. Important and relevant information from the performance reports, journals and publications on cybersecurity risks and their mitigation strategies were reviewed. From each of these journals, we identified up to 5 articles, searching up to five volumes and stopping when we had identified the five articles or completed five volumes, whichever occurred first. This resulted in a total of 50, and a corresponding sample size of 44 according to Krejcie and Morgan (1970). The final list included a total included 35 articles consisting of 15 articles in computer science and engineering journals and 20 in Information Systems journals.

Table 1: Information systems and engineering journals included in the study

Journal Name	Acronym
Journal of Management Information Systems	JMIS
Communications of the Association for Information Systems	CAIS
Internet Research	INTR
Journal of Computer and Communications	JCC
Journal of Cyber Security	JCSM
Journal of strategic information systems	DR
International Journal of Communication networks & information security	IJCNIS
IEEE Internet of Things Journal	IoTjnl
IEEE Transactions on Information Forensics & Security	TIFS
IEEE Transactions on Industrial Informatics	TII

3. ANALYSIS

We classified the papers by IoT cyber security risk, threats, and mitigation methods. The researchers independently evaluated the content of each paper for these three characteristics and established item categories in the three dimensions, in order to develop sets of cyber security risk types and mitigation strategy. We used an open coding approach. Different category names with the same meaning were consolidated into one category name without counting that as a difference. To resolve the remaining classification differences, the researchers reread the respective articles and obtaining consensus. Differences were resolved in an iteration of this process and the codes were consolidated into twelve cyber security risk types and respective mitigation method types.

4. RESULTS

4.1 Clusters of IoT security threats and mitigation methods

Clusters of IoT cyber security risks and mitigation methods are presented in Table 2 and Table 3 respectively. Table 2 shows the results of our analysis, in terms of the count of the number of papers at the intersection of each cyber security threats. From this review, it is found out that organizations and their information systems are subject to security threats from different sources majority including computer frauds, espionage, sabotage, vandalism, fires, computer bugs, hacker attacks, and denial-of-service attacks, are more frequent and their hazardousness and sophistication are increasing. To differentiate between Information Systems journals and computer science and engineering journals, we split the results as seen in table 2 below;

Table 2: IoT Cyber security threats

IoT Security threats	Information Systems journals	Percentage	computer science & engineering journals	Percentage
Cyber / network attacks	3	15	3	20
Computer frauds	2	10	1	6.7
Espionage	2	10	1	6.7
Sabotage	2	10	2	13.2
Vandalism	1	5	1	6.7
Fires	3	15	2	13.2
denial-of-service attacks	2	10	1	6.7
computer bugs	1	5	1	6.7
Spoofing	1	5	1	6.7
message falsification/injection	1	5	1	6.7
malicious attack	2	10	1	6.7
TOTAL	**20**	**100**	**15**	**100**

Table 3: Mitigation of IoT cyber security threats and risks

Threat mitigation strategy	Frequency	Percentage
Develop Initiatives supporting the creation of international legal standards	1	2.8
Enforce Human security	2	5.7
Secure the physical locations of installed devices	2	5.7
Employ access controls measures	3	8.6
Disaster control and recovery	3	8.6
Empowerment of users to manage their data and avoid anonymous usage.	2	5.6

Create manpower with better qualification/training and skills on cyber security matters through public-private partnerships	1	2.9
Use an intrusion detection system (IDS) / intrusion prevention system (IPS)	2	5.7
Privacy policy for applications on IoT	1	2.9
Increased awareness on issues of security, risks and cyber incidents to form a healthy base for use.	3	8.6
Employ security specialists	2	5.7
Implement multi-factor authentication	1	2.9
Use a secure communication channel by utilizing a secure Virtual Private Network (VPN)	2	5.7
Limit network traffic such that it is accessible only to authorized users	2	5.7
Use encryption mechanisms for security data transmission	2	5.7
Perform frequent data backups to keep copies of sensitive data	2	5.7
Avoid infrastructure outsourcing to a third-party service provider	1	2.9
Track system behavior to identify any suspicious privacy leakage	2	5.7
Use only trusted providers to receive technical support for hardware failures in organisations	1	2.9
TOTAL	**35**	**100**

4.2 IoT risks

Securing cyberspace entails a number of considerations to mitigate risks and threats while encouraging accessibility and openness across various types of interconnected networks and devices (NATO,2016). In this study, we established several IoT risks and mitigation measures as presented in table 3 and table 4 respectively;

Table 4: Cyber security IoT risks

IoT risks	Frequency	Percentage
Lack of control and asymmetry of the information	3	8.6
Limitations in the possibility of maintaining anonymity when using services	3	8.6
Web Application Vulnerabilities	5	14.3
Complexed ecosystem	2	5.7
Sharing of data with the third party	5	14.3
Security failures in the device's design and its exploitation	2	5.7
The lack of clearly assigning responsibilities	2	5.7
User privacy violation	4	11.4
Misuse of organizational information systems with the possibility of malfunction	2	5.7
Possibility of injecting new security vulnerabilities into the system	3	8.6
The attacker changes the system configuration and adding back doors	2	5.7
Possibility of bringing the system down, making it ultimately unusable	2	5.7
TOTAL	**35**	**100**

5. DISCUSSIONS

IoT-based organizations are highly vulnerable to attacks via the Internet. If the entire or part of an organization’s information system is compromised, the adversary will be able to invade the privacy of organizational inhabitants, steal personal or sensitive information, control the organizational information system, and even monitor residents inside the organizational environment. Pursuing security IoT threats and risk assessment, as well as mitigation, is essential (Babate et al, 2015).

This study has conducted a comprehensive IoT security threat and risk assessment using a literature review and identified 12 critical IoT security risks from the cyber and physical perspectives, as reported in Table 4, originating from both inside and outside organizations. Intuitively, there are other risks that have not been identified due to time limitations. Suitable countermeasures for mitigating the risks to an acceptable level (since 100% security is never attainable) are proposed in Table 3. Physical security risks correspond to devices such as hardware concerns the theft, defect, manipulation, and sabotage
of the various devices inside or outside the organization environment.

The threats to organizational information systems may include Cyber/network, attacks, Computer, frauds, Espionage, Sabotage, Vandalism, Fires, denial-of-service attacks, computer bugs, Spoofing, message falsification/injection malicious attack and can result in harm to the confidentiality, availability, and integrity of data. The highest-ranking threats, Cyber/network attacks at a percentage of 20%. Therefore, it is imperative that all the actors at all levels in an organization understand their responsibilities and are held accountable for managing cyber security risks associated with IoT in order to support the mission and business functions of the organization (Faris et al,2014).

The cyber security IoT risk assessment outcomes demonstrate that Sharing of data with third party and Web Application Vulnerabilities are the highest risk exposure that organizations are vulnerable to in case of attacks to their information systems. Other identified risks are Lack of control and asymmetry of the information, Limitations in the possibility of maintaining anonymity when using services, Complexed ecosystem, Security failures in the device's design and its exploitation, lack of clearly assigning responsibilities, User privacy violation, Misuse of organizational information systems with the possibility of malfunction, Possibility of injecting new security vulnerabilities into the system, Attacker changes the system configuration and adding back doors and possibility of bringing the system down, making it ultimately unusable(Faris et al,2014; Kamrani et al(2016); García,2017; Fenz et al(2011); Ebru,2016).

The proposed mitigation approaches should be used to reduce the IoT cyber security threats and hence to alleviate the potential risks. Increasing organizational information system security by applying more security solutions will impact the overall system usability. Therefore, when using some of the proposed countermeasures, both system security and usability should be balanced. In addition, other factors that influence organizational information system security, such as access control measures, Disaster control and recovery, Empowerment of the user to manage their data and avoid anonymous usage should be encouraged.

Other measures to curb cyber security threats and risks of IoT include; develop manpower with better qualification, conduct training and skills on cyber security matters through public-private partnerships, usage of an intrusion detection system (IDS) or intrusion prevention system (IPS), consider Privacy policy for applications on IoT, Increase awareness on issues of security of IoT based organizations, document the risks and cyber incidents to form a healthy base for use, employ security specialists and usage of a secure communication channel through utilization of a secure virtual private network (VPN).

Roozbahani and Azad (2015) argued that communication networks must be secured and protected against intentional and unintentional attacks as this will improve response time, availability or high readiness, reliability or high reputation, integrity and be flawless thus providing scalability as well as accurate information. Limiting network traffic such that it is accessible only to authorized users is key when employing security countermeasures in IoT-based organizational information systems. Although this paper proposed precautions for mitigating cyber security IoT threats and risks, the precautions considererd the end-user side. The governmental authorities also need to become more involved by offering legal support, security standards, and law enforcement policies. The study findings and the proposed mitigation approaches can enable all stakeholders, especially end users, to be aware of various cyber security threats and risks of IoT and to take appropriate security mitigation measures to improve security in IoT-based organisations. Furthermore, the research findings establish useful contributions that can be used as a foundation for updating the security requirements in IoT-based organisations and for improving the existing security policies.

6. CONCLUSION

This paper has outlined the different types of threats to IoT cyber security risks and threats. The aim of this survey was to assess the state of IoT Cyber security emerging risks and threats and the best approach needed to mitigate Cyber security breaches. This paper has focused solely on the identification of cyber security threats, risk and suitable countermeasures for the IoT based organizations. As a research outcome, approximately 12 cybersecurity risks of IoT originating from both inside and outside smart organizations have been identified. Suitable countermeasures for mitigating the risks to an acceptable level have been proposed. Further research must be conducted on the ranking of the cyber security risk of IoT using different methodologies.

This paper has noted that organizations at the moment are influenced by the principal attacks. This is based on the fact that mobile devices and web-based applications usage continues to increase hence an increase in the volume of attacks targeting these devices and applications. The study findings suggest a role for the government to take absolute countermeasures against cyber Security threats and risks of IoT. Unless governments adopt this measure to mitigate threats, security threats will continue to manifest unabated.

7. REFERENCES

[1] Treffyn L, K., Toni, R., Tuck W, L. (2013) Internet of Things: a review of literature and products. Conference Paper · ACM 978-1-4503-2525-7/13.DOI: 10.1145/2541016.2541048.

[2] Krejcie, R.V., & Morgan, D. W (1970). Determining Sample Sizes for Research Activities, Educational and Psychological Measurements, 30,608.

[3] SJR (2018). Scimago Journal & Country Rank.Journal rankings. Available at https://www.scimagojr.com/journalrank.php?category=1710.Accessed on 20th May 2018.

[4] Podhorec, M. (2012) Cyber Security Within the Globalization Process. Journal of defense resource management. Vol 3, issue 1(4).

[5] Guarinielloa, C. and De Laurentisa, D. (2014) Communications, information, and cybersecurity in Systems-of-Systems: Assessing the impact of attacks through interdependency analysis. Conference on Systems Engineering Research. Procedia Computer Science 28 (2014) 720 – 727

[6] Chulki, J and Sungjin, A. (2014) A Study on the Improvements of the Information Security Management System for Environment Education Institutes. International Journal of Security and Its Applications.Vol.8, No.4, pp.247-252

[7] EBRU, Y, Y. (2016)THE IMPORTANCE OF RISK MANAGEMENT IN INFORMATION SECURITY. Proceedings of The IIER International Conference.

[8] Fenz, S., Ekelhart, A., and Neubauer, T. (2011) "Information Security Risk Management: In Which Security Solutions Is It Worth Investing?," Communications of the Association for Information Systems: Vol. 28, Article 22.

[9] Francesco, R., Salvatore, D and Tommaso, M (2018) Securing the Internet of Things: New Perspectives and Research Challenges. IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1.

[10] Bisong., A and Rahman, S, M (2011) An Overview of The Security Concerns In Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1.

[11] Alhaji Idi Babate, Maryam Abdullahi Musa, Aliyu Musa Kida, Musa Kalla Saidu. (2015)State of Cyber Security: Emerging Threats Landscape. International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015). Vol. 3, Issue 1

[12] Roozbahani, F, S and Azad, R(2015)Security Solutions against Computer Networks Threats. Int. J. Advanced Networking and Applications. Volume: 07 Issue: 01 Pages: 2576-2581

[13] Suchitra.C, Vandana C.P(2016) Internet of Things and Security Issues. International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1, pg. 133-139

[14] T. Murakami, K. Takahashi, K. Matsuura (2014) Toward Optimal Fusion Algorithms with Security against Wolves and Lambs in Biometrics, IEEE Transactions on Information Forensics and Security, Vol.9, No.2, pp.259-271.
[15] T. Murakami, H. Watanabe, (2016). Localization Attacks Using Matrix and Tensor Factorization, IEEE Transactions on Information Forensics and Security, Vol.11, No.8, pp.1647-1660.
[16] Faris, S., Iguer, H., Medromi, H, E. L. Hasnaoui, S. and Sayouti, A. (2014) Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi-Agent Systems, Itil, Iso 27002, Iso 27005. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 6.
[17] Farzad Kamrani, Mikael Wedlin, and Ioana Rodhe, Internet of Things: Security and Privacy Issues, 2016. FOI-R--4362--SE.
[18] OWASP, Top 10 Privacy Risks Project. (n.d.). Retrieved from https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
[19] García, M., P.(2017) Cybersecurity and IoT Privacy Risks and Challenges.,. Available at https://www.certsi.es/en/blog/cybersecurity-and-iot-privacy-risks-and-challenges accessed on 10th June 2018
[20] EY(2015)Insights on governance, risk, and compliance. Cybersecurity and the Internet of Things