Available online at: http://journal.uinsgd.ac.id/index.php/ks
Khazanah Sosial, Vol. 4 No.2: 235-240

DOI: 10.15575/ks.v4i2.17638

Internet of Things (IoT) Cybersecurity Challenges and Mitigation Mechanisms

Joshua Ebere Chukwuere

[1]Department of Information Systems, North-West University, South Africa
*Corresponding Author E-mail: joshchukwuere@gmail.com

Abstract

This study deployed desktop research methodology in seeking to understand the cybersecurity challenges confronting Internet of Things (IoT) and the mitigation mechanisms. Objects are no longer independent from each other; rather, connectivity through the power of the internet has connected them. IoT is no longer a new invention or innovation in the technology industry and human lives. The concept is widely used in different industries such as healthcare, food, finance, manufacturing, government, insurance, oil and gas, transportation, postal services, defence, and many more. These industries are using the ability of IoT to function optimally in facilitating different activities. Users of technology devices use IoT devices in homes, offices, and other places to increase productivity and efficiency daily. This article analyses the cybersecurity challenges of IoT and its mitigation mechanisms. The findings identified different cybersecurity challenges confronting IoT and the ways to mitigate them.

Keywords: Cybersecurity, Internet of everything, Internet of things, Internet, IoT, Security

Abstrak

Studi ini menggunakan metodologi penelitian desktop dalam upaya memahami tantangan keamanan siber yang dihadapi Internet of Things (IoT) dan mekanisme mitigasinya. Objek tidak lagi independen satu sama lain; melainkan, konektivitas melalui kekuatan internet telah menghubungkan mereka. IoT bukan lagi sebuah penemuan atau inovasi baru dalam industri teknologi dan kehidupan manusia. Konsep ini banyak digunakan di berbagai industri seperti perawatan kesehatan, makanan, keuangan, manufaktur, pemerintah, asuransi, minyak dan gas, transportasi, layanan pos, pertahanan, dan banyak lagi. Industri-industri ini menggunakan kemampuan IoT untuk berfungsi secara optimal dalam memfasilitasi berbagai aktivitas. Pengguna perangkat teknologi menggunakan perangkat IoT di rumah, kantor, dan tempat lain untuk meningkatkan produktivitas dan efisiensi setiap hari. Artikel ini menganalisis tantangan keamanan siber IoT dan mekanisme mitigasinya. Temuan ini mengidentifikasi berbagai tantangan keamanan siber yang dihadapi IoT dan cara untuk menguranginya.

Kata kunci: Keamanan siber, Internet segalanya, Internet segalanya, Internet, IoT, Keamanan

INTRODUCTION

The definition of IoT is confusing when one looks at huge interest from cross-disciplinary research and attention from researchers. Commonly, the definitions look into the connectivity of objects over the internet and many more. Internet of things (IoT) presents a new and evolving opportunity with increased connectivity of humans and objects, and object to object. IoT defines a new paradigm of connectivity and communication among things and objects (Lee, 2020). The initiative has the potential to change individuals' and organisations' processes (Maple, 2017). The interconnection of objects will continue to increase yearly because of IoT capabilities. IoT further presents the opportunity for millions and even billions of devices, things, or objects to interconnect over the internet. At the same time, robust security measures are necessary to manage different forms of threats and attacks (Abomhara & Køien, 2015). The

Received: March 6, 2022; In Revised : April 10, 2022; Accepted : April 16, 2022

invention of IoT presents initiatives such as the internet of everything (IoE), the internet of all things (IoaT), SmartThings (ST), and many others. Through this development and invention, the security of these connectivities remains a challenge for users and developers. Users are worried about their data security and their devices, while developers are worried about keeping up with the growing security challenges confronting the IoT digital space and cyberspace. The questions users keep asking are:

1. Would my IoT device be safe?
2. Would users' personal data and information be safe?
3. While developers are asking:
4. What can we do to secure IoT cyberspace?
5. Are the current mechanisms protecting against threats and attacks?

These questions and many more pose a severe concern for all stakeholders in the industry. However, the healthcare industry is playing a leading role in applying the capabilities of IoT in its function (Saad & Soomro, 2018). According to Tawalbeh, Muheidat, Tawalbeh and Quwaider (2021), security and privacy are major concerns of the IoT; while Lee (2020) believes that cybersecurity is the major concern when you think and talk about IoT and its devices. This short paper aims to provide a comprehensive analysis of the intelligent, smart things, and IoT data security challenges and the way forward.

RESEARCH METHOD

Academic research papers can be considered using primary or secondary data. In this case, secondary data was used through desktop research methodology. The study allows the researcher to carry out the study through the desktop research methodology. The methodology allows the researcher to search for existing literature documents that discuss the topic. No primary data source/s will be used because of no human involvement in the study.

RESULT AND DISCUSSION

INTERNET OF THINGS (IOT) AND INTERNET OF EVERYTHING (IOE)

Digital age inventions are interchangeable in some cases. However, the difference is discussed below :

IoT: IoT connects everything, i.e. entities, things and objects over the internet through a wired or wireless mechanism (Tawalbeh et al., 2020). According to Langley, van Doorn, Ng, Stieglitz, Lazovik and Boonstra (2021), IoT has the ability to change everything about human and organisational functions. The authors define IoT as the connectivity of objects (things) through internet-connected constituents. Boeckl, Boeckl, Fagan, Fisher, Lefkovitz, Megas and Scarfone (2019) suggest that IoT devices can interact with real-life objects, things and the physical world. The ability of objects, things and smart devices to interact with each other made IoT the fastest growing technology in recent years, with many potentials to increase in developing countries. The connectivity is remote, like objects (things) locating sensors and working in real-time. The changes will alter the organisational business model and flow of activities and information between individuals and organisations. The innovation of smart things is changing objects' connectivity, such as car and house doors, alarms, home, office bells, TV, fridges, and many more. These objects are beginning to connect and speak with each other through sensor connectivity on the internet.

The ability of objects or smart things to interconnect in a real-world setting made IoT the current and future technology. According to Abombara and Koien (2015), IoT involves smart things such as home appliances, smartphones, cars, healthcare devices, buildings, factories, and many objects connected

 ISSN 2715-8071 (online)

through network sensors to share connectivity and resources. The ability of the IoT made it possible for everything in a physical environment to communicate with a connected device in a real-life setting. The ability of IoT is a function of cellular systems, smartphones, remotes, and other technologies that are controlled through wireless connectivity.

IoE: Internet of Everything (IoE) is a branch of IoT (Raj & Prakash, 2018) with the ability to provide connectivity for people, smart things, and organisations that have changed organisations and human lives (Langley et al., 2021). Business models are beginning to adopt the internet of smart things innovations. According to Banafa (2017), IoE brings individuals, objects, and things together to make connection and resource sharing easy and efficient. As a subset of IoT, organisations and individual lives are made better and are enriched (Farias da Costa et al., 2021). The two concepts make connectivity and access to internet connections effortless.

SECURITY CHALLENGES

The security of IoT devices involves protecting the device and the users from any unauthorised access within and outside the network. Security challenges affect the device and the service, the user's information, and identity (Lu & Da Xu, 2018). IoT devices are facing similar security challenges to other internet-enabled devices. In this case, security is regarded as protection against unauthorised access, usage, theft, and loss of physical damage or attack. Unauthorised access and breach of confidentiality and integrity of users' information are critical to be maintained (Abombara & Koien, 2015). According to Boeckl et al. (2019), some organisations are unaware of the amount of connectivity between devices and the security risk associated with these connectivities. The increase in attacks and threats on IoT devices is increasing (Abombara & Koien, 2015). IoT security challenges can be mitigated in three ways (Boeckl et al., 2019):

1. **Protect device security:** Protect online or IoT devices from being used to attack other devices on the internet, carrying out distributed denial of service (DDoS), eavesdropping on the network, and causing traffic delays and compromises.
2. **Protect data security:** Confidential data and information on the internet should be protected using different mechanisms. The protection should involve identity protection, procession, and storage protection.
3. **Protect individual or personal privacy:** All personally identifiable information (PII) on IoT devices should be protected.

SOURCES OF SECURITY RISK AND MITIGATION MEASURES

Sources of security risks

As conventional information technology devices are faced with cybersecurity threats, so are IoT devices. Cybersecurity discussions are aimed at protecting users and organisations against IoT security threats (Lee, 2020). Cybersecurity threats come through sources such as IoT sensor data, IoT devices, ubiquity IoT sensors, network interfacing with IoT, and many more (Kimani et al., 2019). These security sources are caused by different incidents such as lack of security architecture, different software to manage, difficulty to manage growing expectations, legacy hardware, and lack of investment in capacity and capabilities. According to Abombara and Koien (2015), IoT security risks and th reats are sourced from lack of human intervention in connectivity, wireless connection, and lack of computing resources and low-power capabilities. At the same time, Tawalbeh et al. (2020) suggest that IoT is challenging due to

numerous devices connecting and sharing similar resources and sensor interference. The growing attack on IoT devices has made it necessary to step up interventions and mitigation measures in managing and controlling these attacks and threats.

Data confidentiality is a major source of security challenges for IoT devices and services (Abombara & Koien, 2015). The users of IoT devices and confidential data should be protected against unauthorised access (Abombara & Koien, 2015). Improper updating, lack of security protocol, lack of user awareness, and active monitoring are among the sources of security concerns and risks (Tawalbeh et al., 2020).

Mitigation measures

According to Boeckl et al. (2019), asset, vulnerability, and access management is necessary to manage growing security challenges. The authors further suggest that data protection, discontinuing data management, and incident and privacy breach detection are important in mitigating security challenges in IoT cyberspace.

1. **Monitoring and control:** This process involves a physical guide of hardware and software monitoring against any possible threats and vulnerabilities that might develop (Ali & Awad, 2018). This process assists in the prevention and detection of threats.
2. **Risk identification and quantification:** IoT security threats, vulnerabilities, and assets must be identified, and the impact and frequency probability should be identified beforehand (Lee, 2020). This process allows for proper mechanisms to be put in place to mitigate and control it.
3. **Continuous improvement:** Organisations should endeavor to continuously improve the software and hardware to accommodate changes and enhance possible vulnerability threats points.
4. **Proper software updating:** Users of IoT devices should always update the software application timely (Poyner & Sherratt, 2018). This will increase the security features and minimise vulnerabilities.
5. **Vulnerability and access management:** Detect known and unknown potential vulnerabilities using firmware and other software and manage access to the network and devices.
6. **Data protection:** Every object connected to the IoT network is exposed to vulnerability; therefore, protection against unauthorised access and manipulation must be detected and controlled.
7. **Protect user privacy and access to data:** Provide authentication and identifiable access to confidential data and information (Abombara & Koien, 2015). Every object connected to IoT must be encrypted in the communication and exchange of data over the internet.
8. **Discontinue data management:** Detect any unauthorised personal identifiable information (PII) and minimise the link with network and IoT devices.
9. **Incident detection:** This involves early detection of cybersecurity threats through proper and continuous analysis of the network (Tuor et al., 2017).
10. **Privacy breach detection:** IoT cyberspace and cybersecurity should be monitored to detect any sign of security breaches from external hackers aimed at compromising users' privacy (Boeckl et al., 2019).

Against these growing security and privacy threats, the privacy and confidentiality of users should be respected and protected from all forms of unauthorised access (Abouelmehdi et al., 2017). Increased awareness for the users to understand the threats in the IoT device connectivity should be increased. Different protection mechanisms should be put in places, such as end-to-end encryption channels, periodic

 ISSN 2715-8071 (online)

updating, authentication, embedded password, pattern, and other forms of protection should be embedded on IoT devices to protect users' identity and the service.

CONCLUSION

Our world is becoming more interconnected between humans and objects and objects to objects in sharing resources and communication. IoT and its devices are making lives better and easier. However, different challenges listed above always oppose the application and adoption of IoT devices in real life. Physical object connectivity will be accelerated in the future, making it easier for humans to interact with objects from different locations. Furthermore, human-to-human connectivity will be a norm. Humans will be able to share and communicate wirelessly and wired using the power of the internet. This connectivity will be made possible through humans having embedded chips in their bodies for accessible communication and access to internet capabilities. At the same time, security and privacy threats will increase on IoT networks.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65–88.

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73–80.

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, *18*(3), 817.

Banafa, A. (2017). *The Internet of Everything (IoE)*. Dostupno Na.

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. US Department of Commerce, National Institute of Standards and Technology ….

Farias da Costa, V. C., Oliveira, L., & de Souza, J. (2021). Internet of everything (IoE) taxonomies: A survey and a novel knowledge-based taxonomy. *Sensors*, *21*(2), 568.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49.

Langley, D. J., van Doorn, J., Ng, I. C. L., Stieglitz, S., Lazovik, A., & Boonstra, A. (2021). The Internet of Everything: Smart things and their impact on business models. *Journal of Business Research*, *122*, 853–863.

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157.

Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184.

Poyner, I. K., & Sherratt, R. S. (2018). Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people. *Living in the Internet of Things: Cybersecurity of the IoT-2018*, 1–5.

Raj, A., & Prakash, S. (2018). Internet of Everything: A survey based on Architecture, Issues and Challenges. *2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 1–6.

Saad, M., & Soomro, T. R. (2018). Cyber Security and Internet of Things. *Pakistan Journal of Engineering, Technology & Science*, *7*(1).

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*.

 ISSN 2715-8071 (online)