JIEM : JOURNAL INFORMATIC, EDUCATION AND MANAGEMENT
Vol. 5, No. 1, February 2023, pp. 16 ~ 20
ISSN: 2716-0696, DOI: https://doi.org/10.61992/jiem.v5i1.71

Information System Security Analysis in the Internet of Things (IoT) Era

Nurrisma

STMIK Indonesia Banda Aceh

Article Info

Article history:
Received 10 February 2023
Revised 12 February 2023
Accepted 13 February 2023

Keywords:
Internet of Things (IoT), Information System Security, Security Threats, Data Encryption, Security Protocols.

ABSTRACT

The presence of the Internet of Things (IoT) has provided a new foundation in the development of information systems, but has also raised new challenges related to information security. This research aims to analyze the level of information system security in the context of the IoT era. The research methods used include an in-depth literature survey and critical analysis of security frameworks relevant to IoT. The research results show that while IoT offers great potential to increase efficiency and convenience, it also opens up new avenues for complex and serious security attacks. Security threats related to IoT include network attacks, data theft, and unauthorized access. To overcome this challenge, a holistic and layered approach is needed in securing information systems connected via IoT. The importance of implementing strong security protocols, data encryption, and continuous monitoring of IoT networks cannot be overstated. In conclusion, the success of widespread IoT implementation will be largely determined by efforts to strengthen the security of the information systems involved.

Corresponding Author:
Nurrisma | STMIK Indonesia Banda Aceh
Email: nurrisma@stmikiba.ac.id

1. INTRODUCTION

The Internet of Things (IoT) has changed the information technology landscape in significant ways, integrating physical devices into complex digital networks [1]. In this context, information systems connected via IoT present a variety of potential benefits, ranging from increased operational efficiency to the creation of innovative new services. However, along with its benefits, IoT also carries deep implications related to information security.

The advancement of IoT presents unique challenges in ensuring the security of information systems. With billions of interconnected devices, security attacks can occur from a variety of sources and with a variety of methods. These threats can include network attacks, data theft, device manipulation, and more. Therefore, an in-depth analysis of information system security in the context of IoT becomes very important.

Within this theoretical framework, this research aims to critically investigate various aspects of information system security in the IoT era [2]. Through a deep understanding of potential vulnerabilities and applicable solutions, this research effort is directed at providing valuable guidance to practitioners and decision makers in addressing this complex security challenge.

Thus, this research not only serves to improve our understanding of information systems security in the context of IoT, but also makes a meaningful contribution to the development of effective security strategies in this ever-changing digital era. By strengthening this theoretical foundation, it is hoped that this research can become a solid foundation for developing best practices in securing information systems in the Internet of Things era.

2. THEORETICAL BASIS

The Internet of Things (IoT) has expanded the scope of information systems by introducing networks consisting of interconnected physical devices. In this context, a strong understanding of information system security theories becomes crucial for identifying, analyzing and overcoming emerging threats in the IoT era [3].

One of the main relevant theories is Information Security Theory. This theory provides an understanding of the basic concepts of information security, including confidentiality, integrity, and data availability. In the context of IoT, these aspects become more complex due to the large number of interconnected devices and multiple potential entry points for attacks.

Furthermore, Computer Network Theory plays an important role in understanding the architecture and communication protocols used in IoT networks. This is important for analyzing weak points that can be exploited by attackers, as well as for designing appropriate security solutions.

Apart from that, Cryptographic Theory is also a crucial basis for securing communications and data in IoT systems. The concepts of encryption, digital signatures, and authentication protocols provide a strong foundation for protecting sensitive information from unauthorized access [4].

No less important, Risk Management Theory provides guidance in identifying, assessing, and managing security risks associated with IoT system implementation. A systematic approach to risk management will help organizations prioritize security efforts and allocate resources efficiently.

By combining a deep understanding of these theories, this research aims to provide a strong theoretical foundation for analyzing information system security in the Internet of Things era. Thus, it is hoped that this research will provide valuable insights for the development of effective security strategies in facing complex challenges in an increasingly connected world [5].

3. RESEARCH METHODOLOGY

This research adopts an in-depth qualitative approach to analyze information system security in the Internet of Things (IoT) era. A qualitative approach was chosen to enable a comprehensive understanding of various security aspects related to IoT, including challenges, solutions, and best practices.

The development of this research methodology involved the following stages:

1. Data Collection:
Data will be collected through an in-depth literature survey from primary and secondary sources relevant to information systems security and IoT. The literature analyzed will include scientific journals, books, research reports and technical documentation.

2. Data Analysis:
The collected data will be analyzed using a qualitative analysis approach. This involves identifying patterns, key findings, and relationships between various aspects of information system security in the IoT context.

3. Data Verification:
The validity of the data will be verified through the use of verified and trusted sources. In addition, the analysis carried out will go through verification and validation stages by experts in the fields of information security and IoT.

4. Interpretation of Results:
The analysis results will be interpreted to extract valuable insights about information system security in the IoT era. These findings will be linked to the theoretical framework discussed previously to develop a deeper understanding.

5. Conclusion:
Research conclusions will be prepared based on the analysis that has been carried out, presenting the main findings, implications and recommendations for the development of effective security strategies in the IoT context.

By following this methodology, it is hoped that this research can make a significant contribution to the understanding and development of best practices in securing information systems in the Internet of Things era.

4. RESULTS AND DISCUSSION

The results of the Information Systems Security Analysis in the Internet of Things (IoT) Era highlight several key findings relevant to the complexity and challenges associated with security in the IoT context.

1. Vulnerability to Attack
Analysis reveals that information systems connected via IoT are vulnerable to various security attacks, including network attacks, data theft, and device manipulation. This is due to the large number of connected devices and vulnerabilities in the implementation of appropriate security protocols [6].

2. Lack of Perfect Security Standards
The findings show that currently available security standards do not fully cover the unique security needs in the IoT context. Existing security protocols are often inadequate to protect IoT devices from complex, coordinated attacks.

3. The Role of Cryptography and Encryption
Cryptography and encryption techniques are proven to be key elements in improving the security of information systems in IoT. However, challenges remain in effectively deploying this technology across IoT devices that are often resource-constrained.

4. The Importance of Risk Management
The discussion also highlights the importance of a proactive risk management approach in dealing with security threats in the IoT era. Organizations need to comprehensively identify, assess, and manage security risks associated with implementing IoT systems.

The discussion of these findings underscores the importance of a holistic approach in securing information systems in the Internet of Things era. Effective security solutions require a combination of technical strategy, strong organizational policies, and a systematic risk management approach. Thus, this research confirms that to achieve optimal security in this increasingly connected environment, there needs to be a joint effort from various stakeholders, including developers, government and society at large.

5. CLOSURE

In this research, various findings have been revealed that provide a deep understanding of the challenges and solutions related to information system security in the Internet of Things (IoT) era. The analysis conducted highlights the complexities associated with developing security in this increasingly connected environment. From the analysis results, it can be concluded that information system security in the IoT context requires a holistic and integrated approach. This includes implementing strong security protocols, effective implementation of cryptography and encryption technologies, and proactive risk management.

Additionally, it is important to recognize that existing security standards do not fully cover the unique needs in the IoT context. Therefore, efforts to develop more comprehensive and up-to-date security standards must continue to be encouraged.
In addition, this research also highlights the need for collaboration between various stakeholders, including technology developers, government, standardization institutions, and the general public, to create a safe and trustworthy environment for IoT use.

REFERENCES

[1] Al-Fuqaha, A., M. Guizani, M. Mohammadi, M. Aledhari, & M. Ayyash (2015). The Internet of Things: A Survey of Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[2] Gauravaram, P., Hutter, D., Meder, S., Rijmen, V., & Schläffer, M. (2007). Cryptographic engineering in a nutshell. Journal of Cryptographic Engineering, 1(3), 189-204.

[3] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[4] Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

[5] Sookhak, M., Talebian, H., Gani, A., & Talebian, A. (2017). A survey on internet of things architectures. Journal of Network and Computer Applications, 85, 121-134.

[6] Yaqoob, I., Ahmed, E., Gani, A., Imran, M., Guizani, M., & Shuja, J. (2017). Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE Wireless Communications, 24(3), 10-16.