Volume 3, Issue 2, February – 2025 **ISSN (E):** 2938-379X

SECURITY ANALYSIS IN IOT TECHNOLOGIES

Berdimurodov Mansur 1,
1 PhD, Senior Lecturer, Department of Modern Information and Communication Technologies, International Islamic Academy of Uzbekistan, Tashkent
e-mail: m.berdimurodov@iiau.uz

Babajanov Mumin 2 ,
2PhD, Senior Lecturer, Department of Modern Information and Communication Technologies, International Islamic Academy of Uzbekistan, Tashkent
e-mail: babajanov.mumin@gmail.com

Farmonov Bobur 3
3Senior Lecturer of the Department of Information Security,
National University of Uzbekistan, Tashkent.
e-mail: boburfarmonov93@mail.ru

Abstract
Internet of Things (IoT) technologies are becoming an integral part of our daily lives. IoT systems work efficiently through interconnected devices, but these connections also lead to several security risks. This paper analyzes the specific methods and technologies used to ensure security in IoT systems. It examines how the protection of IoT devices is implemented in a changing environment, and how cryptography and authentication methods work to ensure network security and data protection. The research also explores advanced technologies aimed at reducing risks and threats in IoT systems.

Keywords: IoT, security, authentication, cryptography, network security, protection methods, device security.

Introduction

The Internet of Things (IoT) technologies are widely used not only in homes but also in industries, healthcare, and many other fields. IoT devices create the potential to transfer and analyze data, improving efficiency; however, they also give rise to new risks and threats. Specifically, IoT devices often have weak security systems, which allow cyber attackers to access the system and steal data. This paper analyzes specific methods and strategies for ensuring security in IoT technologies. These methods can provide effective results in protecting devices and networks.

Literature Review

Research in IoT security is divided into several main areas. The first area is authentication and identification systems. High-level authentication systems are crucial in ensuring the security of IoT devices (Zeldovich & Jackson, 2020). Another area is network security and the use of

encryption technologies in data transmission. The exchange of data between IoT devices is often carried out over open channels, which poses significant risks to data security. Cryptographic methods, such as AES and RSA algorithms, are widely used to enhance data security in IoT systems (He & Zhang, 2019). Furthermore, blockchain technology is also being applied in IoT systems to enhance security (Liu & Zhao, 2021). Literature also examines systemic monitoring and network management methods for protecting IoT devices.

Research Methodology

The primary method used in this study is a literature review and comparative analysis. Through literature review, advanced approaches and technologies aimed at ensuring IoT security are explored. The study analyzes security issues related to IoT devices, networks, and data transmission processes, as well as practical methods for reducing risks. The research also presents information about cryptographic methods, authentication systems, and secure network architectures used to ensure IoT security.

Analysis and Results

Several key methods for ensuring security in IoT systems can be identified:

1. **Authentication and Identification Systems:** Weak authentication systems are common in IoT devices, allowing unauthorized access to systems. Strong authentication methods, such as two-factor authentication (2FA) and biometric authentication, are effective in securing IoT systems.

2. **Cryptography:** Data between IoT devices is often transmitted over open channels, making encryption necessary. Modern cryptographic algorithms, such as AES and RSA, are widely used to ensure data security in IoT systems.

3. **Network Security:** The networked portion of IoT devices is often vulnerable. To address this, it is necessary to implement network monitoring, access control, and secure network architectures. For instance, VPNs and IDS/IPS systems are effective tools for ensuring the security of IoT systems.

4. **Blockchain Technology:** Blockchain helps provide transparency and security in data transmission within IoT systems. This technology protects the data exchange between IoT devices and ensures the security of inter-system communication.

Conclusion and Recommendations:

Ensuring security in IoT technologies is an essential and pressing issue. As data exchange between IoT devices and networks expands, security measures must be strengthened. To protect IoT systems, it is necessary to integrate advanced technologies such as authentication, cryptography, network security, and blockchain. The following recommendations are proposed:

Web of Teachers: Inderscience Research
webofjournals.com/index.php/1

1. **Implement Strong Authentication Methods:** Widely adopt two-factor authentication and biometric authentication in IoT devices.

2. **Strengthen Data Encryption:** Use modern cryptographic methods like AES and RSA widely in IoT systems.

3. **Create Secure Network Architectures:** Implement VPNs and IDS/IPS systems to protect data transmitted by IoT devices.

4. **Apply Blockchain Technology:** Use blockchain to ensure data security in IoT systems' data exchanges.

References

1. Zeldovich, N., & Jackson, M. (2020). Security in the Internet of Things: Challenges and Solutions. Journal of Cyber Security, 13(2), 45-59.
2. He, Y., & Zhang, H. (2019). IoT Security: A Survey. International Journal of Computer Networks, 7(4), 87-101.
3. Liu, Q., & Zhao, X. (2021). Blockchain and IoT Security: A Survey and Research Directions. Computers & Security, 99, 101978.
4. Ahmed, S., & Ali, M. (2022). Authentication and Privacy Challenges in the Internet of Things. Future Internet, 14(3), 112.

Web of Teachers: Inderscience Research
webofjournals.com/index.php/1