ISSN Online : 2709-5088
ISSN Print : 2709-507X
IJCST

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY (IJCST) Vol. 8 No.1 (2024)

Mitigating Cyber Security Risks in IoT: A Focus on Reliability and Efficiency

Shehr Bano,
Shoaib Saqib,
Sobia Khursheed,
Fasih us din,
Muhammad Sajjad Hussain

[1]Faculty of Computing Gomal University, Dera Ismail Khan, Khyber Pakhtunkhwa (KPK), Pakistan
[2]Faculty of Computing Gomal University, Dera Ismail Khan, Khyber Pakhtunkhwa (KPK), Pakistan
[3]Department of Computer Science, [3]Institute of Southern Punjab, Pakistan
[4]Faculty of Computing Gomal University, Dera Ismail Khan, Khyber Pakhtunkhwa (KPK), Pakistan
[5]Faculty of Computing Gomal University, Dera Ismail Khan, Khyber Pakhtunkhwa (KPK), Pakistan

[1]Shehrbano1050@gmail.com

[2]Sohaib_saqib40@yahoo.com

[3]gghss.tsha@gmail.com

[4]fasiudin@ulm.edu.pk

[5] muhammadsajjadhussain@gmail.com

Abstract:
Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Various problems such as authentication, authorization, and privacy have been highlighted in the context of cybersecurity. Previous research has addressed and mitigated these threats to a considerable extent, but the aspect of reliability in cybersecurity remains underexplored. This paper proposes a qualitative method to emphasize data security reliability and productivity on various aspects and parameters that are crucial in cybersecurity. Although these reliability measures are still in development, they aim to reduce the number of threats affecting cybersecurity performance.

Keywords:
Cyber Security, E-systems, IoT, Reliability, Data Security, Productivity

Introduction:
The Internet of Things (IoT) is a transformative technology that connects a diverse array of devices, from everyday household items to complex industrial systems. By integrating sensors, software, and connectivity, IoT enables these devices to communicate and exchange data, creating

ISSN Online : 2709-5088
ISSN Print : 2709-507X
IJCST

a more interconnected and efficient world (Oracle, n.d.). IoT devices include everything from smart home appliances like thermostats and refrigerators to advanced medical devices such as heart monitors and even vehicles equipped with sophisticated sensors (TechTarget, n.d.).

The benefits of IoT are manifold. For consumers, IoT offers increased convenience and automation, such as smart home systems that allow remote control of home environments and personalized energy management (van der Schaaf et al., 2021). For businesses, IoT can lead to significant improvements in operational efficiency, supply chain management, and customer service. Real-time data from IoT devices enables businesses to monitor system performance, optimize processes, and reduce costs (Savic et al., 2021). For instance, IoT applications in logistics and manufacturing can help in predictive maintenance, where sensors monitor equipment health and predict failures before they occur, thereby minimizing downtime and reducing maintenance costs (Djenna, Harous, & Saidouni, 2021).

Despite these advantages, the rapid proliferation of IoT devices presents substantial cybersecurity challenges. The very nature of IoT—its vast network of interconnected devices—creates multiple points of vulnerability. Many IoT devices are designed with convenience in mind rather than security, leading to potential security gaps (Mendhurwar & Mishra, 2021). The COVID-19 pandemic accelerated the adoption of IoT technologies, but this rapid expansion often came at the expense of thorough security considerations (Zaghloul et al., 2021).

IoT devices are increasingly targeted by cyber-attacks due to their widespread deployment and often inadequate security measures. These attacks can range from data breaches and unauthorized access to sophisticated distributed denial-of-service (DDoS) attacks. For example, IoT botnets have been used to orchestrate massive DDoS attacks, highlighting the risks associated with insecure IoT devices (Qureshi et al., 2021). The potential consequences of these attacks are severe, affecting not only the security of individual devices but also the integrity and reliability of the entire IoT ecosystem.

Despite the growing body of research on IoT security, the focus has predominantly been on privacy, authentication, and threat detection, with less emphasis on reliability. Reliability in cybersecurity refers to the system's ability to consistently perform its intended functions under predefined conditions. For IoT systems, this means ensuring that devices and networks are not only protected from attacks but also maintain their performance and functionality under various scenarios (Corallo et al., 2021). Addressing reliability issues is crucial for ensuring the long-term stability and trustworthiness of IoT systems.

Literature Review:

The IoT security landscape is complex and multifaceted, encompassing a range of methodologies designed to protect internet-connected devices from a variety of cyber threats. A comprehensive understanding of IoT security involves examining several key areas: API security, public key infrastructure (PKI) authentication, network security, and data privacy (Djenna, Harous, & Saidouni, 2021).

API Security: Application Programming Interfaces (APIs) are integral to IoT systems, allowing different devices and services to communicate. However, APIs can also be a significant security vulnerability if not properly secured. Weak API security can lead to unauthorized access and data breaches (Zaghloul et al., 2021). Researchers have proposed various methods to enhance API security, including the use of strong authentication mechanisms and encryption to protect data in transit (Mendhurwar & Mishra, 2021).

ISSN Online : 2709-5088
ISSN Print : 2709-507X
IJCST

PKI Authentication: Public Key Infrastructure (PKI) plays a crucial role in ensuring secure communications between IoT devices. PKI uses asymmetric cryptography to provide authentication and encryption services, which are essential for maintaining the integrity and confidentiality of data exchanged between devices (van der Schaaf et al., 2021). Effective PKI implementation involves the use of digital certificates and robust key management practices to prevent unauthorized access and tampering.

Network Security: The security of the network infrastructure is critical for IoT systems, as the network serves as the backbone for data transmission between devices. Network security measures include firewalls, intrusion detection systems (IDS), and secure network protocols to prevent and detect unauthorized access and attacks (Qureshi et al., 2021). As IoT networks often involve diverse and heterogeneous devices, ensuring compatibility and security across different network layers can be challenging.

Data Privacy: Ensuring the privacy of data collected and transmitted by IoT devices is a major concern. Data privacy involves protecting sensitive information from unauthorized access and ensuring that data is collected, stored, and processed in compliance with relevant privacy regulations (Savic et al., 2021). Techniques such as data anonymization and secure data storage are employed to safeguard user information and maintain privacy.

Despite significant advances in these areas, the reliability of IoT systems remains a relatively underexplored aspect of IoT security. Reliability encompasses not only the resilience of IoT devices to attacks but also their ability to consistently perform their intended functions under various conditions. This includes maintaining operational performance, data accuracy, and system stability even in the face of potential disruptions or attacks (Corallo et al., 2021).

Research Methodology:

Methodological Approach: This study adopts a qualitative approach to address the cybersecurity challenges related to reliability in IoT systems. The qualitative approach is well-suited for exploring complex issues and gaining a deeper understanding of expert perspectives on reliability and cybersecurity. Surveys, interviews, and focus groups with industry experts and stakeholders are used to gather insights and highlight the importance of reliability in IoT cybersecurity (Scribbr, n.d.).

Methods of Data Collection: Data for this study is collected through various qualitative methods, including:

- Observational Surveys: Surveys are conducted to gather opinions and experiences from cybersecurity professionals regarding the importance of reliability in IoT systems. The surveys aim to identify key reliability concerns and assess the current state of reliability measures in IoT cybersecurity (van der Schaaf et al., 2021).
- Interviews: Semi-structured interviews with experts in IoT security provide detailed insights into specific reliability challenges and best practices. Interviews allow for a deeper exploration of expert opinions and experiences, offering valuable perspectives on how to enhance reliability in IoT systems (Djenna, Harous, & Saidouni, 2021).
- Focus Groups: Focus groups are organized to facilitate discussions among multiple experts, enabling the identification of common themes and consensus on reliability issues. This collaborative approach helps in understanding the collective viewpoint on the significance of reliability in IoT cybersecurity (TechTarget, n.d.).

Qualitative Methods:

ISSN Online : 2709-5088
ISSN Print : 2709-507X
IJCST

- Surveys: Survey-based questions are designed to assess the perceptions of reliability and cybersecurity concerns among professionals. The survey results highlight the importance of incorporating reliability measures in IoT systems to address emerging cybersecurity challenges (Mendhurwar & Mishra, 2021).
- Experiments: Post-survey analysis involves using techniques such as Principal Component Analysis (PCA) and factor analysis to evaluate the impact of reliability on IoT device performance. These statistical methods help in identifying key factors affecting reliability and their relationship with overall cybersecurity performance (Savic et al., 2021).
- Existing Data: A comprehensive review of existing literature and journals is conducted to identify gaps in the current research on reliability measures in IoT cybersecurity. This review helps in understanding the state of the art and the need for further research on reliability issues (Corallo et al., 2021).

Results: The analysis of survey responses, interview transcripts, and focus group discussions provides valuable insights into the importance of reliability in IoT cybersecurity. Key findings include:

- Perceived Importance of Reliability: The majority of experts agree that reliability is a critical factor in ensuring the security and performance of IoT systems. Reliable systems are essential for maintaining operational continuity and minimizing the impact of potential disruptions or attacks (Qureshi et al., 2021).
- Reliability Challenges: Experts identify several challenges related to reliability, including the need for robust error detection and recovery mechanisms, consistent performance under varying conditions, and effective handling of system failures (Zaghloul et al., 2021).
- Best Practices: Recommendations for improving reliability in IoT systems include implementing redundancy, regular testing and validation, and adopting best practices for system design and maintenance (Djenna, Harous, & Saidouni, 2021).

Conclusion: IoT connects a diverse array of computing devices, enhancing both personal and business environments through automation and real-time data insights. While significant advancements have been made in securing IoT systems, the focus on reliability remains limited. This paper proposes a qualitative approach to addressing data security reliability and productivity in IoT cybersecurity. The results underscore the importance of integrating reliability measures into IoT systems to improve their performance and resilience against cyber threats (van der Schaaf et al., 2021).

Reliability in IoT cybersecurity is crucial for ensuring the long-term stability and trustworthiness of interconnected systems. By addressing reliability concerns, organizations can enhance the effectiveness of their IoT deployments and safeguard against potential cybersecurity risks. Future research should continue to explore and develop strategies for improving reliability in IoT systems, ensuring that they can meet the demands of an increasingly connected world (Mendhurwar & Mishra, 2021).

References:

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2021). Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2021.3086230

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meet Internet of Threats: New concern cybersecurity issues of critical cyber infrastructure. *Applied Sciences, 11*(10), 4580. https://doi.org/10.3390/app11104580

Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: Architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems, 15*(4), 565-584. https://doi.org/10.1080/17517575.2021.1870287

Oracle. (n.d.). What is IoT? Retrieved from https://www.oracle.com/internet-of-things/what-is-iot/

Qureshi, S., He, J., Tunio, S., Zhu, N., Akhtar, F., Ullah, F., ... & Wajahat, A. (2021). A hybrid DL-based detection mechanism for cyber threats in secure networks. *IEEE Access, 9*, 73938-73947. https://doi.org/10.1109/ACCESS.2021.3071352

Savic, M., Lukic, M., Danilovic, D., Bodroski, Z., Bajović, D., Mezei, I., ... & Jakovetić, D. (2021). Deep learning anomaly detection for cellular IoT with applications in smart logistics. *IEEE Access, 9*, 59406-59419. https://doi.org/10.1109/ACCESS.2021.3076068

Scribbr. (n.d.). Methodology. Retrieved from https://www.scribbr.com/dissertation/methodology/

TechTarget. (n.d.). IoT security (Internet of Things security). Retrieved from https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

van der Schaaf, K., Tekinerdogan, B., & Catal, C. (2021). A feature-based approach for guiding the selection of Internet of Things cybersecurity standards using text mining. *Concurrency and Computation: Practice and Experience*, e6385. https://doi.org/10.1002/cpe.6385

Zaghloul, Z. S., Elsayed, N., Li, C., & Bayoumi, M. (2021). Green IoT system architecture for applied autonomous network cybersecurity monitoring. *arXiv preprint arXiv:2106.00834*. Retrieved from https://arxiv.org/abs/2106.00834