International Journal of Science, Technology and Management (IJSTM) ISSN (online): 2321-774X
Volume 11, Issue 1, 2024

Enhancing Security in IoT Networks: Advanced Communication Protocols for Robust Data Protection

[1]Shivpal Singh, [2]Ms. Jyoti

[1]M.Tech. CSE Scholar, [2]Assistant Professor

Department Of CSE, BRCM CET, Bahal, Bhiwani, Haryana

[1]Shivpalsheoran99@gmail.com

[2]jyoti@brcm.edu.in

ABSTRACT

In this study, we examine the basics of IoT architecture and provide a comprehensive overview of the communication protocols specifically designed for IoT technology. Additionally, we explore security threats and general implementation challenges, highlighting various sectors that stand to gain the most from IoT advancements. Our discussion of the findings identifies unresolved issues and challenges, outlining the necessary steps to enhance and secure IoT systems in the future.

Keywords: IoT , Security Protocols Threats.

INTRODUCTION

A few decades ago, the Internet revolutionized global connectivity in real-time. Today, the Internet of Things (IoT), also known as the Internet of Everything or the Industrial Internet, is transforming the technology landscape by connecting machines and devices globally, enabling them to interact autonomously within the existing Internet infrastructure. IoT encompasses countless tangible devices that collect and share data without the need for human interaction. Advances in affordable computer chips, ubiquitous wireless networks, and technologies like machine learning, big data, smart sensors, and 5G have made it possible to integrate almost anything into the IoT, from small pills to large ships. IoT devices, distinct from conventional Internet-enabled devices like laptops and smartphones, include home appliances and health monitors that can communicate without human intervention. This connectivity transforms these objects into intelligent devices, enhancing efficiency and responsiveness. The widespread application of IoT has the potential to significantly improve various industries and overall welfare. However, it also introduces security threats, especially when connected to critical systems. By 2030, the number of IoT devices is expected to grow by 300%, reaching over 25 billion, with China leading in IoT applications as of 2020.

This article makes significant contributions and is innovative. This article covers a generic IoT architecture, communication protocols for the application, transport, network, and physical layers, current security threats, challenges, solutions, and future directions.

Vulnerabilities and Security Threats on IoT System:

IoT systems are vulnerable to various weaknesses in hardware, software, user practices, and policies, which can be exploited by attackers to execute commands, access unauthorized data, and perform denial-of-service attacks. Threats include hardware and software attacks, radio communication breaches, personal data violations, and privacy invasions. Notable IoT malware includes Mirai, which hijacks devices for DDoS

attacks, Torii, which exfiltrates sensitive information using encrypted communications, BrickerBot, which destroys data through brute-force attacks, Reaper, which targets disclosed vulnerabilities, and Persirai, which exploits network protocols like UPnP in IP cameras. These attacks exploit poor configurations, firmware vulnerabilities, and weak network protocols. IoT devices are also susceptible to physical tampering and eavesdropping due to their unattended nature and limited security capabilities.

Security Challenges in IoT Systems:

IoT systems face numerous and varied security challenges:

- Data Privacy and Industrial Secrets: Ensuring the security and privacy of personal data and industrial secrets is critical.

- Confidentiality and Data Integrity: Maintaining confidentiality, access controls, and data integrity within IoT systems is essential.

- Critical Infrastructure Security: Protecting critical infrastructure to ensure its availability is a major concern.

- Authentication: Securely verifying the identity of entities (individuals, programs, processes, or machines) in a network is crucial. Effective authentication underpins confidentiality, integrity, and non-repudiation.

- Monitoring: Continuously monitoring the status of IoT devices to detect whether they are online or offline and alerting users or systems if there is a disruption.

- Minimizing Attack Surface: Reducing the attack surface is challenging due to the widespread and remote accessibility of IoT devices, which increases the risk of attacks.

- End-to-End Encryption: Providing encryption for communications between IoT devices and servers, ensuring mutual authentication.

- Access Control: Implementing secure access control to manage who can transmit and receive data on the network.

- Battery Life Preservation: Balancing robust security measures with the need to conserve battery life, especially in resource-constrained IoT devices.

Implementing robust security mechanisms is challenging due to the limited computational power, memory, and battery life of IoT devices. Ensuring privacy in data collection, sharing, and management remains an ongoing research issue. Therefore, designing and implementing secure protocols for IoT systems is essential to preserve privacy and ensure data security.

LITERATURE REVIEW

The rapid growth of connected objects raises concerns due to a lack of standards, security considerations, and the prevalence of cyber attacks. Significant efforts are being made to enhance the security of IoT systems, including data confidentiality, integrity, and privacy.

Jayaraman et al.[1] proposed a method for end-to-end IoT privacy using random data decomposition and homomorphic encryption for secure data retrieval.

Ukil Arijit et al.[2] introduced a privacy preservation framework incorporating data masking, demonstrated in medical and energy use cases.

Kalra et al.[3] suggested encrypting IoT communications, with agreed-upon encryption keys, to ensure secure interactions. Vucinic proposed object security for end-to-end IoT communication.

Mooassi[4] introduced a secure authentication and authorization architecture for IoT-based healthcare using smart gateways.

Types of Secure Communication Protocols

1. MQTT (Message Queuing Telemetry Transport):

- Lightweight messaging protocol ideal for low-bandwidth, high-latency networks.

- Uses TLS/SSL for secure communication.

2. CoAP (Constrained Application Protocol):

- Designed for low-power, low-bandwidth devices.

- Uses DTLS (Datagram Transport Layer Security) for secure communication.[5]

3. HTTPS (Hypertext Transfer Protocol Secure):

- Secure version of HTTP, widely used for secure web communication.

- Uses TLS/SSL for encryption.[6]

4. DTLS (Datagram Transport Layer Security):

- Provides security for datagram-based applications, similar to TLS but for UDP.

- Ensures data privacy and integrity.[7]

5. AMQP (Advanced Message Queuing Protocol):

- Messaging protocol for business messaging.

- Supports TLS/SSL for secure communication.

6. DDS (Data Distribution Service):

- Middleware protocol for real-time systems.

- Uses TLS/SSL and other security plugins to ensure secure data distribution.

7. Zigbee:

- Low-power, low-data rate wireless protocol.

- Uses AES-128 for encryption to ensure secure communication.

8. Bluetooth Low Energy (BLE):

- Wireless personal area network technology.

- Uses AES-128 for encryption and various authentication mechanisms.

9. 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks):

- Adaptation layer for IPv6 packets over IEEE 802.15.4 networks.

- Uses IPsec for secure communication.[8]

10. LoRaWAN (Long Range Wide Area Network):

- Protocol for low-power, wide-area networks.

- Uses AES encryption for secure communication.

These protocols provide various levels of security tailored to the constraints and requirements of different IoT applications.

CONCLUSION

As the Internet of Things (IoT) expands, the diversity and complexity of its applications increase, making them vulnerable to various attacks aimed at stealing information, controlling devices, and disrupting services. This paper analyzed the security requirements specific to IoT, focusing on network security, identity management, privacy, trust, and resilience. Standardized protocols and networking stacks from bodies like IETF, IEEE, and industry alliances were examined for their mechanisms to ensure data confidentiality, integrity, origin authentication, and freshness. A wide range of IoT technologies, from single-layer protocols like 6LoWPAN to full stacks like Thread, were evaluated, and their security capabilities summarized.

The study highlighted the existing mechanisms in IoT technologies that address core security needs but noted areas for future research, including solutions for trust and resilience and

the practical implementation of security properties in IoT devices given their limitations.

REFERENCES

[1] Biggs John “Hackers release source code for a powerful DDoS app called Mirai”, October 10, 2016. https://techcrunch.com/2016/10/10/hackers-release-source-code-fora-powerful-ddos-app-called-mirai/

[2] Ukil, Arijit, et al. “Negotiation-based privacy preservation scheme in internet of things platform.” Proceedings of the First International Conference on Security of Internet of Things. ACM, 2012. p. 75-84

[3] Kalra, Sheetal, and Sandeep K. Sood. “Secure authentication scheme for IoT and cloud servers.” Pervasive and Mobile Computing 24 (2015): 210-223.

[4] Moosavi, Sanaz Rahimi, et al. “SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways.” Procedia Computer Science 52 (2015): 452-459

[5] Shelby, Z., Hartke, K., Bormann, C., & Frank, B. (2014). "The Constrained Application Protocol (CoAP)." IETF RFC 7252.

[6] Rescorla, E. (2000). "HTTP Over TLS." IETF RFC 2818.

[7] Rescorla, E., & Modadugu, N. (2012). "Datagram Transport Layer Security Version 1.2." IETF RFC 6347.

[8] Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). "Transmission of IPv6 Packets over IEEE 802.15.4 Networks." IETF RFC 4944.