Evaluation of Current Standards for IoT Security Protocols

Aqsa Sayed

aqsa.sayed89@gmail.com

Abstract

The Internet of Things (IoT) is rapidly expanding, connecting millions of devices across various sectors. However, the proliferation of IoT devices has raised significant security concerns, making the evaluation of current security protocols essential. This paper reviews existing standards for IoT security protocols, assessing their effectiveness, applicability, and challenges. By analyzing various frameworks, this paper aims to provide insights into the current landscape and identify potential areas for improvement.

Keywords: **Internet of Things (IoT), Cybersecurity,National Institute of Standard & Technology (NIST),IoT Security Foundation (IoTSF)**

I. Introduction

The improvements in wireless standards from 3G to 4G/LTE & now with the ongoing deployment of 5G, IoT is becoming one of the highlights or the main feature accompanying the technology.IoT offers applications in a variety of fields, including healthcare, transportation, industry automation, V2X, home sensing and many more. With these applications that provide ease with automation,they present multiple levels of cybersecurity threat regarding the data being collected on these devices, not only the sensitive data, such as personal information, financial transactions, butalso operational data required to read patterns &provide continued enhanced service. This integration of millions of devices into essential infrastructure increases the risks involved, as a successful breach could lead to significant disruptions, data loss, and even threats to public safety.Every device connected is subjected to malware, viruses & cyber threat which brings us to the need & enforcement of security systems in IoT environments.[10]

The unique characteristics of IoT devices—such as their limited processing power, varying communication protocols, and diverse operational environments propose significant challenges for implementing robust security measures. Many devices are resource-constrained, making it difficult to deploy traditional security solutions without affecting performance. Additionally, the rapid growth of IoT has outpaced the development of standardized security protocols, leading to a fragmented landscape where inconsistent implementations leave gaps that malicious actors can exploit.[9]

Given these challenges, this paper evaluates current IoT security protocolsin safeguarding IoT ecosystems. By analyzing established standards such as IEEE 802.15.4, MQTT-SN, and CoAP, this study aims to provide a comprehensive understanding of how these protocols address security vulnerabilities and where improvements are necessary. Ultimately, the goal is to highlight best practices and recommend strategies for enhancing the security framework surrounding IoT, ensuring that as the ecosystem grows, it remains resilient against emerging threats.

.

II. IoT Overview

The term IoT was first coined by Kevin Ashton in 1999 with reference to the supply chain management

[6,7]. The concept of IoT relies on the system or device being able to reciprocate output by applying itself & the data available, making an inanimate object "smart", hence the term Internet of Things[7]

At its core, IoT are devices & sensors that collect data from the environment& once the data is collected it requires data processing capabilities which can either be done using edge computing on the device or using the cloud depending on the use & processing capacity of the device. The processed data is stored in databases for analysis, reporting, and future references. Cloud storage solutions are commonly used for scalability and accessibility, At the topmost layer is the User Application where the user interacts with IoT using the interface such as web or mobile applications, dashboards.

Figure.1 is a general idea of how IoT Layers would look like, the other form of naming these would include data link, network, transport ,session layers. These layers include specialized protocols for routing/messaging, initiation of sessions,security &management.Different standards were proposed by organizations like IEEE, ITU. Below is a description of a few of these standard IoT protocols that are commonly used.

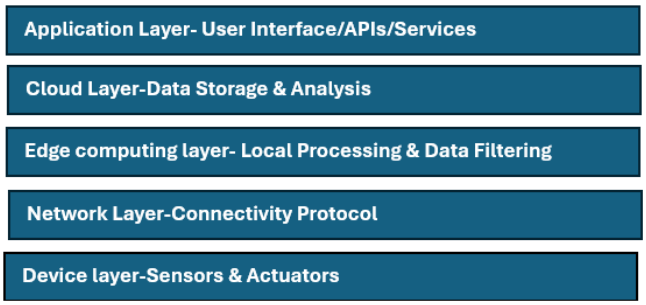

Figure 1: IoT Architecture

1. IEEE 802.15.4

This standard specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is foundational for many IoT applications, particularly in home automation and sensor networks.

Designed for devices that require long battery life, making it ideal for sensor applications.

System can maintain low power consumption due to the slot frame structure, which is defined by IEEE802.15.4 frame structure for scheduling of data. It basically means when a node is transmitting, it's awake & waits for acknowledgment. Once received it sends the data to the upper layer & sleeps.

Includes support for security services such as encryption, access control, and data integrity, essential for protecting communications between devices.

Supports various network topologies, including star and mesh networks, which are beneficial for scalable IoT applications.

2.Network Layer Routing Protocols.

This layer mainly discusses standard created for how the data is to be transferred from Source to destination & what is it encapsulated with.

There are different types of Routing protocols

- **IPv4 and IPv6**: While IPv4 is still prevalent, IPv6 is increasingly important for IoT due to its vast address space, accommodating the billions of devices in the ecosystem.6LoWPAN adaptation layer allows IPv6 packets to be transmitted over low-power wireless personal area networks (LoWPANs). It optimizes header compression and fragmentation, making it suitable for constrained devices.

- **RPL (Routing Protocol for Low-Power and Lossy Networks)**: Designed for low-power and lossy networks, RPL enables efficient routing by creating a destination-oriented directed acyclic graph (DODAG) to facilitate data transmission while minimizing energy consumption.
- **NB-IoT (Narrowband IoT)**: This cellular technology focuses on providing wide-area coverage for IoT devices. It uses existing mobile networks, ensuring reliable connectivity for low-bandwidth applications.

3.MQTT-SN (MQTT for Sensor Networks)

MQTT-SN is a lightweight messaging protocol tailored for sensor networks and other constrained environments. It takes place on the session layer It extends the standard MQTT protocol, allowing devices with limited processing power and bandwidth to communicate efficiently.

MQTT-SN minimizes the amount of data transmitted, making it suitable for devices with limited resources. It includes mechanisms for broadcasting messages to multiple devices, which is useful in sensor networks.

MQTT-SN facilitates communication between devices from different manufacturers, enhancing compatibility in IoT ecosystems. Commonly used in applications like home automation, environmental monitoring, and industrial IoT, where lightweight communication is essential.

4. CoAP (Constrained Application Protocol)

CoAP is a specialized web transfer protocol designed for constrained devices and networks. It operates over UDP, making it efficient for low-power devices that require minimal bandwidth.

CoAP supports RESTful interactions like HTTP, allowing devices to create, read, update, and delete resources.

This layer is responsible for the reliability of data received. It has four messaging types namely confirmable, which sends an acknowledgement back to server, non-confirmable, where acknowledgment is not received and then piggyback where acknowledgment is sent with the message, lastly separate where the message and acknowledgement are sent separately.CoAP can send messages to multiple devices simultaneously, which is advantageous in group communication scenarios.

Frequently used in smart home systems, industrial automation, and sensor networks, CoAP facilitates communication between constrained devices and the cloud or other services.

IoT devices require reliable connection & stable network to transmit data which can be employed in different networks like Wifi, LTE,5G, Bluetooth Low Energy, Zigbee.

Bluetooth is used for low energy & short range like in vehicle device connection. Basically, devices communicate when Bluetooth is active on both sides else are dormant. Zigbee has one of the most common applications of IoT, like in smart homes or healthcare systems forming a private area network. They work in a star topology, with the network administrator located at the center of the star.

LTE & 5G: Below Table1 shows the difference in how IoT is employed in LTE vs 5G.

Data Rates and Latency: 5G offers significantly higher data rates and a lower latency compared to LTE, making it suitable for more demanding IoT applications.

Connection Density: 5G dramatically increases the number of devices that can be connected simultaneously, essential for massive IoT deployments.

Network Architecture: The shift to service-based architecture in 5G provides more flexibility and efficiency compared to the traditional LTE architecture. While LTE supports various IoT applications, 5G enables advanced use cases like autonomous vehicles and smart cities due to its enhanced capabilities.[12][13]

Feature/Aspect	LTE (Long Term Evolution)	5G (Fifth Generation)
Data Rate	Up to 300 Mbps (theoretical peak)	Up to 10 Gbps (theoretical peak)
Latency	Around 30-50 ms	As low as 1 ms
Connection Density	Supports up to 100,000 devices per square kilometer	Supports over 1 million devices per square kilometer
Network Architecture	Primarily based on traditional cellular architecture	Utilizes a service-based architecture (SBA) for flexibility
Device Types	Mainly mobile devices, sensors, and wearables	Supports a wider variety, including autonomous vehicles, smart cities, and industrial IoT
Energy Efficiency	Moderate energy efficiency	Enhanced energy efficiency with features like NR (New Radio)
Quality of Service (QoS)	Basic QoS features available	Advanced QoS capabilities for diverse applications
Security Features	Standard security protocols (e.g., LTE security)	Enhanced security measures with improved authentication
Use Cases	Smart homes, basic smart cities, wearables	Smart factories, augmented reality, mission-critical applications
Backward Compatibility	Compatible with 2G, 3G, and 4G	Backward compatible with 4G

Table 1: Use of IoT in LTE vs 5G[12][13]

III.Current Security Standards for IoT

IoT is susceptible to cybersecurity threats at all layers discussed above. IoT devices become inoperable if they are compromised by cyber threat.

Different forms of security standards are required at each layer. We have network security standards that maintain secure communications between network and devices.This also monitors the network data to identify any threats or suspicious information.

Next form of security is required at the devices itself, embedded security. This is required to make sure we have secure hardware & software for the device. If the device can storedata, correct form of authenticationis required to access the data.

Below we discuss the different standards set by organizations to meet security needs of IoT.

1.NIST Special Publication 800-183:

The National Institute of Standards and Technology (NIST) outlines a framework to secure the emerging networks of IoT devices. It emphasizes the importance of a risk-based approach to security, acknowledging the diverse environments in which IoT devices operate. There are five key elements for NIST-identify,protect,detect, respond and recover.[16][21]

The NIST uses the above five elements to help organizations with critical infrastructure identify any risk to their network & deploy frameworks to protect them against these threats. Incase of a breach provide standards to respond to such events &help recover from the same.

Another subcategory of NIST is Risk Management Framework(RMF): Incorporates risk assessment, control selection, and monitoring. The RMF is much more flexible to fit into an existing framework for any organization. Encourages alignment with other NIST publications, enhancing security comprehensively.
Stresses the need for ongoing assessment of security posture, particularly in dynamic environments where devices frequently connect and disconnect.[21]

2.IoT Security Foundation (IoTSF) Framework

The IoT Security Foundation (IoTSF) was created to promote the best practices for securing Internet of Things (IoT) devices and systems. Its framework serves as a comprehensive guide for organizations to develop and implement secure IoT products and services. Here are the key components of the IoTSF Framework:[26][27]
The framework advocates for a "security-by-design" philosophy, which means that security should be integrated at every stage of product development. This includes considerations for device design, secure communication, data management, and user interaction.[28]
Effective governance structures are essential for managing security risks in IoT. IoTSF emphasizes the need to identify potential threats and vulnerabilities, assess their impact, and establish clear policies for security governance.
Security Controls: The framework outlines critical security measures that should be implemented in IoT devices, such as:

- Strong authentication methods to verify users and devices
- Secure communication protocols to protect data in transit
- Regular updates and patches to address security vulnerabilities
- Data protection strategies, including encryption and access controls

IoTSF encourages organizations to align their practices with established standards and regulations, such as ISO/IEC 27001 and NIST guidelines, to enhance security and build consumer trust.
Given the rapidly changing security landscape, the framework highlights the importance of ongoing assessment and improvement of security practices. This includes regular vulnerability assessments and penetration testing to ensure devices remain secure over time.[26][27][28]

3. ISO/IEC 27001:

This is a globally recognized standard that provides a systematic approach to managing sensitive information, including data processed by IoT devices. ISO/IEC 27001 sets out the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).[22]
Risk Assessment and Treatment: Involves identifying potential risks to information security and determining appropriate measures to mitigate them.
ManagementCommitment: Requires top management to be involved in establishing and maintaining security practices.
Audit and Improvement: Encourages regular audits and continual improvement processes to adapt to changing security landscapes, particularly as new IoT vulnerabilities emerge.[2]

4. OWASP IoT Top Ten

The Open Web Application Security Project (OWASP) provides a list of the most critical security vulnerabilities specific to IoT devices. This resource is aimed at helping developers, manufacturers, and organizations understand and mitigate common risks associated with IoT.[23]

Weak, Guessable, or Hardcoded Passwords: Many devices ship with default passwords that users fail to change, making them vulnerable to attacks.
Insecure Network Services: Poorly secured network interfaces can expose devices to remote attacks.
Privacy Concerns: Inadequate protection of personal data collected by devices can lead to privacy breaches.
Lack of Secure Update Mechanisms: Devices often lack the ability to securely update their software, leaving them vulnerable to exploitation.[23]
Insufficient Data Protection: Inadequate encryption and data storage practices can lead to data leaks.

5. ETSI EN 303 645

This European Telecommunications Standards Institute (ETSI) standard sets a baseline for the security of consumer IoT devices. It aims to ensure that manufacturers implement essential security measures to protect users from potential threats.[24]
No Default Passwords: Manufacturers must ensure that devices do not have hardcoded or default passwords.
Secure Software Updates: Devices should support secure mechanisms for software updates to address vulnerabilities post-deployment.
Data Protection: The standard emphasizes the importance of protecting user data, both in transit and at rest.
Vulnerability Reporting: Encourages manufacturers to provide mechanisms for reporting vulnerabilities, fostering a more proactive security posture.[24]

6. IETF RFC 8576 (SASL)

This document from the Internet Engineering Task Force (IETF) discusses the Simple Authentication and Security Layer (SASL), which is a framework for adding authentication support to connection-based protocols. It plays a crucial role in securing communications for IoT devices.[25]
Modularity: SASL allows for the integration of various authentication mechanisms, making it versatile for different use cases.
Integrity and Privacy: Supports mechanisms that ensure data integrity and confidentiality during communication.
Extensibility: New authentication methods can be added without changing the underlying protocols, facilitating the adoption of emerging security techniques.[25]

IV. IoT Security Challenges

- **Diverse Device Ecosystem**: Devices vary widely in terms of hardware capabilities, operating systems, and communication protocols, complicating the implementation of uniform security measures.
- **Scalability:** As the number of devices being connected to the system/network increases exponentially, scalability becomes a challenge for IoT, so does keeping the operational data & user information for so many users is daunting and needs to be addressed.
- **Data Privacy**:[18] The sheer volume of data generated by IoT devices raises privacy concerns. Sensitive information, if intercepted or improperly accessed, can lead to serious privacy violations. Ensuring data encryption and secure transmission is critical to mitigate these risks.
- **Interoperability:**[19] The IoT ecosystem lacks uniform security standards, leading to inconsistent security measures across devices. Conglomerates usually prioritize functionality over security measures.
- **Network Security**:[20] IoT devices often use unprotected networks like using public Wi-Fi to access a secure network, making them susceptible to various attacks, including Distributed Denial of Service (DDoS) attacks. Using open networks makes the device susceptible to attacks which can access the network via the device, compromising the entire network.

- **Processing Power**: Many IoT devices have limited processing power, memory, and battery life, making it challenging to implement robust security protocols without affecting performance.
- **Vulnerabilities: Common** vulnerabilities in IoT include weak authentication mechanisms, insecure communication channels, and lack of regular updates, exposing devices to various threats such as data breaches and unauthorized access.

V. Conclusion

The evaluation of current IoT security protocols reveals a landscape of strengths and weaknesses. While several standards provide a solid foundation for securing IoT devices, challenges related to adoption, complexity, and ongoing maintenance remain. Future efforts must focus on simplifying security implementations, ensuring regular updates, and fostering collaboration among stakeholders to enhance the overall security of IoT ecosystems.

VI.References

1. "Internet of Things Security Foundation: Best Practice Guidelines." IoTSF, 2019.
2. "IEEE 802.15.4 Standard for Low-Rate Wireless Personal Area Networks." IEEE, 2016.
3. "MQTT Version 3.1.1 Specification." OASIS, 2014.
4. "The Constrained Application Protocol (CoAP)." IETF RFC 7252, 2014.
5. K. Ashton, "Internet of Things", *RFID J.*, vol. 22, no. 7, pp. 97-114, 2009.
6. K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," in IEEE Access, vol. 8, pp. 23022-23040, 2020, doi:10.1109/ACCESS.2020.2970118.
7. E. Ahmed, I. Yaqoob, A. Gani, M. Imran and M. Guizani, "Internet-of-Things-based smart environments: State of the art taxonomy and open research challenges", *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 10-16, Oct. 2016.
8. Dahlberg, J., and Pärssinen, M. "A Survey of IoT Security Frameworks and Their Capabilities." *arXiv preprint arXiv:1903.11549* (2019).
9. **S. M. M. Rahman, M. T. Iqbal, & N. F. M. Noor. (2019)**. "A Survey on Internet of Things (IoT) Security: Threats and Countermeasures." *International Journal of Computer Applications*, 975, 8887.
10. **Cisco. (2017)**. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*
11. **ITU. (2012)**. *The Internet of Things*. ITU Internet Reports.
12. **R. R. Hossain, & M. H. Reaz. (2018)**. "Internet of Things (IoT) Architecture: A Survey." In *Internet of Things: Architecture and Applications*. Springer, pp. 15-35
13. **S. K. Gupta, K. P. Shukla, & A. Kumar. (2020)**. *Internet of Things: Concepts and Applications*. Springer
14. Zhang, Y., et al. (2019). Privacy Protection in IoT: A Review. *IEEE Access*, 7, 31796-31806
15. Bertino, E., & Islam, N. (2017). Botnets and Internet of Things Security. *Computer & Security*, 67, 199-206.
16. Xu, L. D., et al. (2018). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, 14(7), 3076-3085.
17. NIST. (2017). *NIST Special Publication 800-183: Networks of 'Things'*.
18. ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.
19. OWASP. (2018). *OWASP IoT Top Ten*.
20. ETSI. (2020). *ETSI EN 303 645: Cyber Security for Consumer Internet of Things*.
21. IETF. (2019). *RFC 8576: SASL: Simple Authentication and Security Layer*

22. IoT Security Foundation. (2019). *Best Practice Guidelines*.
23. IoT Security Foundation. (2020). *Compliance Framework*.
24. IoT Security Foundation. (2016). *Security Compliance Framework*