**Technical Report on IoT Networks**

Submitted by: 100723789

Course: 5CM510 Network System Development

Instructor: Katsigiannis Christos

Date: 05/05/2025

**Abstract**  
The Internet of Things (IoT) is transforming how devices interact with each other and with the world in general. The report discusses the key aspects of IoT networks, including communication protocols, security breaches, and emerging technologies. The report covers IoT system scalability, heterogeneity, and privacy, and how conventional protocols like MQTT and CoAP address these concerns. Besides, the report also identifies how 5G, edge computing, artificial intelligence, and blockchain can ensure IoT security as well as efficiency. On that basis, the report attempts to provide an indication of the future of IoT networks and their influence on various sectors.

Table of Contents

[1. Introduction 4](#_Toc198237499)

[2. IoT Network Overview 4](#_Toc198237500)

[2.1 IoT Architecture: Layered Approach 5](#_Toc198237501)

[2.1.1 Device Layer 5](#_Toc198237502)

[2.1.2 Network Layer 5](#_Toc198237503)

[2.1.3 Service Layer 5](#_Toc198237504)

[2.1.4 Application Layer 6](#_Toc198237505)

[2.2 Key Challenges in IoT Networks 7](#_Toc198237506)

[2.2.1 Scalability 7](#_Toc198237507)

[2.2.2 Heterogeneity 8](#_Toc198237508)

[2.2.3 Security and Privacy 8](#_Toc198237509)

[3. Communication Protocols in IoT 8](#_Toc198237510)

[3.1 MQTT (Message Queuing Telemetry Transport) 8](#_Toc198237511)

[3.2 CoAP (Constrained Application Protocol) 9](#_Toc198237512)

[3.3 ZigBee 10](#_Toc198237513)

[4. Security in IoT Networks 10](#_Toc198237514)

[4.1 Common Security Threats 11](#_Toc198237515)

[4.1.1 Data Leakage 11](#_Toc198237516)

[4.1.2 Botnets 11](#_Toc198237517)

[4.1.3 Unauthorized Access 11](#_Toc198237518)

[4.1.4 Physical Attacks 11](#_Toc198237519)

[4.2 Current Security Mitigations 12](#_Toc198237520)

[4.2.1 Encryption 12](#_Toc198237521)

[4.2.2 Authentication Protocols 13](#_Toc198237522)

[4.2.3 Intrusion Detection Systems (IDS) 13](#_Toc198237523)

[5. Future Directions and Emerging Technologies 13](#_Toc198237524)

[5.1 5G and IoT 13](#_Toc198237525)

[5.2 Edge Computing in IoT 14](#_Toc198237526)

[5.3 Artificial Intelligence (AI) in IoT 15](#_Toc198237527)

[5.4 Blockchain for IoT Security 16](#_Toc198237528)

[6. Conclusion 16](#_Toc198237529)

[7. References 17](#_Toc198237530)

# 1. Introduction

A new perspective on how devices interact with other devices and the actual world is represented by the Internet of Things (IoT). The presence of sensors, actuators, and network connectivity allows for autonomous data collection and exchange. The ever-expansive ecosystem connects healthcare and smart cities, transportation, and agriculture industries. However, the expansion of IoT networks brings persistent challenges in communication protocols, security, and scalability.

This report aims to investigate the most critical components of IoT networks such as communication protocols, security gaps, and emerging IoT technologies. This report tries to address the following research questions:

* What are the most crucial communication protocols utilized in IoT networks, and how do they perform under various scenarios?
* What are the security gaps in IoT networks, and how do they overcome?
* How will the future of IoT be shaped by future technologies like 5G, edge computing, and AI?

In order to assess the present state of IoT networks and forecast future advancements, this research analyzes recent research, including a number of cases and technical assessments.

# 2. IoT Network Overview

IoT networks consist of four main layers, each playing a distinct role in ensuring seamless data flow from the physical world to the digital infrastructure. These layers are critical for understanding how IoT devices communicate, process data, and deliver services to end-users.

## 2.1 IoT Architecture: Layered Approach

All four layers work together to move data from the physical world to digital systems. Each layer depends relies on the functionality of the one below it. One big challenge is scalability, making sure the network can handle a growing number of devices without slowdowns.

### 2.1.1 Device Layer

The device layer consists of sensors, actuators, and other end-user devices that generate, collect, and sometimes process information. Devices in this layer are usually low-power, low-cost, and resource-constrained. IoT devices are likely to be of the form of smart thermostats, wearable health devices, and industrial sensors. While these devices are part of the functionality of the network, they are likely to have limited processing power and memory, which is difficult to offer strong security (Bayılmış et al., 2022).

### 2.1.2 Network Layer

The devices and cloud systems are interconnected at the network layer. This system is in charge of forwarding the data gathered from IoT gadgets efficiently through various networks including cellular, WiFi, ZigBee, and Low Power Wide Area Networks (LPWAN). Being a network layer, the network is expected to handle a high data traffic in lower latency to provide high quality communications, as the existing number of IoT devices, is rapidly increasing. The rapid expansion of IoT networks brings challenges related to network traffic and bandwidth management (Lee et al., 2017). With the expansion of IoT devices, scalability becomes a major concern. Gupta et al. (2017) point out that IoT networks must support horizontal scaling (increasing number of devices) and vertical scaling (increasing capacity of existing infrastructure), to avoid performance bottlenecks and system re-designs.

### 2.1.3 Service Layer

It conceals the underlying hardware and provides fundamental services like data management, processing, and storage. It can include cloud platforms that perform computationally complex operations and store amounts of data generated by IoT devices. The service layer is responsible for processing such data, pulling out insights, and providing actionable information to users through interfaces such as dashboards or automated systems. With increasing IoT devices, service layer platforms must scale up to handle bulk amounts of data without impacting performance (Meneghello et al., 2022).

### 2.1.4 Application Layer

The application layer is where end-users interact with the IoT network. It includes the software applications that make use of data from IoT devices to deliver value-added services. Smart home apps (e.g., lighting, heating), industrial IoT (IIoT) apps for predictive maintenance, and healthcare IoT for real-time patient monitoring are some examples. Such apps typically integrate several data sources and provide real-time decision-making capabilities (Gerodimos et al., 2023).

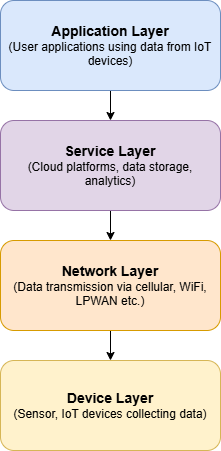


Figure 1 - 2.1.4 Application Layer

## 2.2 Key Challenges in IoT Networks

As the IoT landscape evolves, several challenges must be addressed to ensure its effective implementation and scalability.

### 2.2.1 Scalability

IoT networks will have to handle billions of connected devices, producing huge streams of data to be processed in real-time. The network infrastructure must scale cost-effectively to handle this large volume of data, with no latency or service degradation. Some more advanced network protocols and infrastructure, e.g., 5G networks, will be required by future IoT networks to scale (Albouq et al., 2022). Scalability for an IoT network must ensure that working performance remains the same or increases when data loads increase. The better an IoT network is scaled, the better it is implemented in terms of resource usage, energy efficiency, and the entire system's flexibility (Gupta et al., 2017).

### 2.2.2 Heterogeneity

One of the unique features of IoT networks is that devices connected are diversified. The devices are very different in terms of processing capability, power consumption, and communication needs. This diversity creates a difficulty in making devices compatible and enabling communication between devices with variable capabilities (Bayılmış et al., 2022).

### 2.2.3 Security and Privacy

IoT devices are vulnerable to all sorts of security attacks, such as unauthorized access, data theft, and physical manipulation. Moreover, the majority of IoT devices operate in the periphery of the network, out of reach of conventional security defenses. With billions of devices sharing sensitive data, robust security and privacy controls take center stage (Meneghello et al., 2022; Gopalsamy, 2020).

# 3. Communication Protocols in IoT

The communication protocol plays a key part in enabling devices in an IoT network to communicate with each other. The choice of the right protocol is important in delivering optimal performance, power efficiency, and reliability. Most used protocols in IoT networks are as follows:

## 3.1 MQTT (Message Queuing Telemetry Transport)

MQTT is also among the most popular messaging protocols found in IoT networks. MQTT follows a publish-subscribe paradigm in which devices subscribe to topics of interest and receive messages whenever there are new data published on these topics. MQTT is light, and therefore apt for low-power, low-bandwidth IoT devices. MQTT has a widespread use in use cases such as smart home automation and industrial monitoring (Gerodimos et al., 2023; Bayılmış et al., 2022).

Advantages

* Low Overhead: MQTT supports low bandwidth consumption, which is a requirement for low-resource devices.
* Real-Time Messaging: Offers real-time message delivery.
* Scalability: Allows for a high number of devices due to its efficient message delivery mechanism.

Drawbacks:

* Limited Security: MQTT does not provide inbuilt encryption or authentication and thus other security levels must be used to preserve data confidentiality (Meneghello et al., 2022).

## 3.2 CoAP (Constrained Application Protocol)

CoAP is another lightweight protocol designed for resource-constrained environments. It employs UDP (User Datagram Protocol) rather than TCP/IP, which consumes less power and allows messages to travel more quickly. CoAP finds extensive application in machine-to-machine communication among constrained IoT devices (Bayılmış et al., 2022).

Benefits:

* Low Power Usage: Best suited for devices with scarce resources.
* Simple Design: Involves low overhead, thus best suited for applications where the requirement is for fast response time.

Limitations:

* No Built-In Security: Like MQTT, CoAP does not have inherent mechanisms to ensure data integrity and confidentiality (Meneghello et al., 2022).

## 3.3 ZigBee

ZigBee is among the most used protocols to implement wireless mesh networks in IoT environments, notably smart homes. ZigBee is used to facilitate short-range communications and possesses the low power feature ideal for use on devices like lightbulbs, motion sensors, and locks. ZigBee works very well in creating robust self-healing networks with the capacity to send messages from one node to another (Gerodimos et al., 2023).

Pros

* Mesh Networking: Facilitates long-range communication through relaying messages through other devices.
* Low Power: Designed for devices powered with batteries.

Limitations:

* Low Data Throughput: It is not suitable for applications with high-speed data transfer requirements (Bayılmış et al., 2022).

# 4. Security in IoT Networks

Security is one of the largest challenges in IoT networks. With an increasing number of devices connected and the combination of sensors and actuators, IoT networks are highly susceptible to all types of security threats. The security landscape for IoT devices is multifaceted and encompasses issues pertaining to data confidentiality, device integrity, and access control.

## 4.1 Common Security Threats

IoT devices are hard to protect because they are often small, use different systems, and are placed in locations where they can be easily attacked.

### 4.1.1 Data Leakage

Sensitive data are transmitted via IoT devices and, if intercepted, results in a privacy violation. Devices with poor encryption schemes or operating on old software are prime candidates for data breaches (Gopalsamy, 2020). The authors Abdulghani et al. (2019) argue that weak encryption to no encryption in data storage results in unauthorized accesses, thereby making "data at rest" a common target of attack in IoT. Owing to having a larger surface to attack, IoT systems are thus subject to a variety of threats that include vulnerabilities on both software and hardware. These threats exploit weak authentications, insecure interfaces, and limited protections for devices (Kumar et al., 2019).

### 4.1.2 Botnets

The greatest threat to IoT networks is, perhaps, the creation of botnets. These infected systems may be enticed into botnets, where they are employed in carrying out extremely large-scale distributed denial-of-service (DDoS) attacks. An example in point was the Mirai botnet that executed one of the largest-ever DDoS attacks (Sha et al., 2020).

### 4.1.3 Unauthorized Access

The majority of IoT devices lack proper authentication and authorization mechanisms, whereby hackers can remotely access and commandeer devices. This is particularly common with devices that use default passwords or lack firmware updates (Meneghello et al., 2022). Many devices lack proper privacy safeguards for stored data, creating risk for linkage attacks and data misuse (Abdulghani et al., 2019).

### 4.1.4 Physical Attacks

Since IoT devices are also deployed in unmanned or remote locations, they can be physically tampered with. Physical alterations of devices to retrieve data or disable their functions would constitute attacks (Sha et al., 2020).

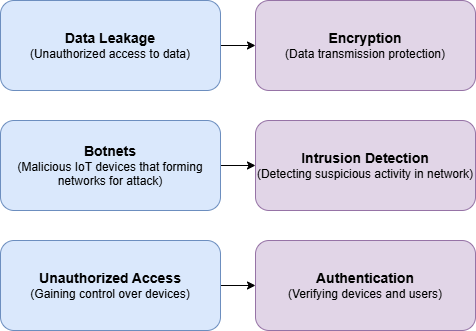


Figure 3 - 4.1 Common Security Threats

## 4.2 Current Security Mitigations

Efforts to secure IoT networks have given rise to a number of countermeasures at any rate the prevalence of many challenges. Among the popular security features include:

### 4.2.1 Encryption

Sophisticated encryption methods like AES (Advanced Encryption Standard) are typically used to encrypt data transmission. However, the majority of IoT devices have limited resources, making the application of high-level encryption infeasible (Sha et al., 2020).

### 4.2.2 Authentication Protocols

Certain IoT systems employ token-based or public-key infrastructure (PKI) systems for device authentication. However, the majority of devices still utilize weak or default credentials, which can be prone to usage (Gopalsamy, 2020).

### 4.2.3 Intrusion Detection Systems (IDS)

IDS systems scan network traffic to detect unusual activity, supporting detection of potential intrusions in real-time. Machine learning-based intrusion detection systems are progressively applied to detect and identify previously unknown threats (Sha et al., 2020).

IoT security remains problematic, particularly due to the extensive use of a great variety of devices. The absence of a standard of security that applies to all IoT devices further complicates the issue. Zaman et al. (2021) also highlight the effectiveness of multi-layered AI models, such as fuzzy logic and SVMs, in detecting complex IoT security threats in real time.

# 5. Future Directions and Emerging Technologies

With the evolution of IoT networks, several emerging technologies are likely to address the challenges faced by such networks. These include 5G/6G, edge computing, and artificial intelligence (AI).

## 5.1 5G and IoT

The functioning of IoT networks could be significantly improved by 5G networks. 5G will meet the demands of bulk IoT deployments to ensure reliability for real-time applications such as autonomous vehicles and remote healthcare monitoring with very low latency and high bandwidth. The advent of 5G will bring forth the presence of dense IoT ecosystems, allowing smart city and industrial IoT (IIoT) applications that require rapid, reliable communication (Albouq et al., 2022).

Another aspect of 5G that will increase efficiency and reliability is Network Slicing, whereby IoT networks may be tuned for special circumstances, e.g., prioritizing critical health or emergency service applications (Albouq et al., 2022). And clearly in smart cities, this is good since real-time monitoring and optimized use of infrastructure are key (Kasznar et al., 2021).

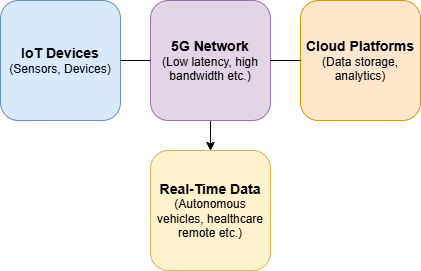


Figure 4 - 5.1 5G and IoT

## 5.2 Edge Computing in IoT

Edge computing is one of the most important paradigms shifts in the management of IoT device data. Data in the traditional cloud-hosted Internet of Things networks is sent to centralized cloud servers for processing. Edge computing, by bringing processing near the source, at the "edge" of the network, removes latency and bandwidth for data transmission to the cloud (Sha et al., 2020).

This computer model critical for time-sensitive IoT applications such as autonomous driving and health monitoring allows for faster response and more efficient use of resources. Local processing of data (Sha et al., 2020) can also enhance security and limit sensitive data subject to cyber-attacks. Low-power edge device design is what dictates the duration that devices employed over a long period of time such as radiofrequency or vibration energy-harvesting devices will survive(Jayakumar et al., 2016). In addition to performance and latency, environmental sustainability ought to inform IoT large-scale applications' decisions. Green IoT system design using solar-powered equipment and life-cycle impact modeling will mitigate energy consumption as well as electronic pollution (Baldini et al., 2023).

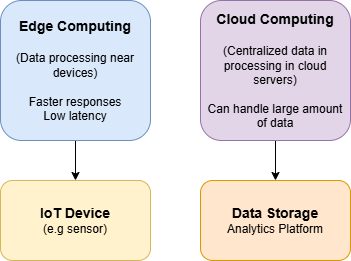


Figure 5 - 5.2 Edge Computing in IoT

## 5.3 Artificial Intelligence (AI) in IoT

Artificial Intelligence (AI) and machine learning (ML) are becoming more and more a component of IoT security and functionality. AI can identify in real time anomalies whose behavior patterns are suspicious, indicating a security attack or malicious attack. For instance, AI algorithms learn the usual behavior of networks and devices, and then it is simple to recognize the deviations that could indicate a cyberattack (Gopalsamy, 2020).  
AI is also used for IoT network management optimization. With predictive analytics, AI can optimize resource allocation, reduce power consumption, and improve the performance of IoT networks (Gopalsamy, 2020).

5.4 Blockchain for IoT Security

One of the most promising latest techniques in IoT security today is constructing security systems with the use of blockchain. A decentralized, transparent and tamper-proof ledger system can be offer by blockchain, which shows a greatest potential to secure data transactions for IoT networks. The technology can assist in solving the problem of device authentication, for example, only a device that is authenticated can be connected to the network. Blockchain technology can also improve data integrity such that data generated from IoT devices are preserved as tamperproof (Wheelus & Zhu, 2020).

# 6. Conclusion

In conclusion, IoT networks are a pillar of modern technology expansion, enabling automation in industries. Although IoT networks are faced with pressing issues, most commonly communication, security, as well as scalability, various current protocols like MQTT and CoAP try to achieve specific goals. New technologies like 5G, edge computing, and AI have promising outlooks toward the future of IoT. Future research should also focus on advanced AI models that support real-time security, as proposed by Zaman et al. (2021), including layered detection strategies tailored for IoT vulnerabilities. Ensuring security against vulnerabilities and devising sound protocols will be important as the IoT ecosystem continues to develop.

# 7. References

1. Abdulghani, H.A., Nijdam, N.A., Collen, A. and Konstantas, D., 2019. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. *Symmetry*, 11(6), 774. DOI: 10.3390/sym11060774 [Accessed 5 May 2025].
2. Albouq, S.S., Abi Sen, A.A., Almashf, N., Yamin, M. and Bahbouh, N.M., 2022. A Survey of Interoperability Challenges and Solutions for Dealing with Them in IoT Environment. *IEEE Access*, 10, pp. 36416-36429. DOI: 10.1109/ACCESS.2022.3162219 [Accessed 5 May 2025].
3. Baldini, E., Chessa, S. and Brogi, A., 2023. Estimating the Environmental Impact of Green IoT Deployments. *Sensors*, 23(3), 1537. DOI: 10.3390/s23031537 [Accessed 5 May 2025].
4. Bayılmış, C., Ebleme, M.A., Çavuşoğlu, Ü., Küçük, K. and Sevin, A., 2022. A survey on communication protocols and performance evaluations for Internet of Things. *Digital Communications and Networks*, 8(3), pp. 1094-1104. DOI: 10.1016/j.dcan.2022.03.013 [Accessed 5 May 2025].
5. Gerodimos, V., Lygeros, J. and Vasilenko, P., 2023. IoT Communication Protocols and Security Threats. *Journal of IoT Security*, 14(2), pp. 103-115. DOI: 10.1016/j.iotcps.2022.12.003 [Accessed 5 May 2025].
6. Gopalsamy, M., 2020. Artificial Intelligence (AI) Based Internet-of-Things (IoT)-Botnet Attacks Identification Techniques to Enhance Cybersecurity. *International Journal of Research and Analytical Reviews*, 7(4), pp. 24-32. [Accessed 5 May 2025].
7. Gupta, A., Christie, R. and Manjula, R., 2017. Scalability in Internet of Things: Features, Techniques and Research Challenges. *International Journal of Computational Intelligence Research*, 13(7), pp.1617–1627. Available at: http://www.ripublication.com/ijcir17/ijcirv13n7\_06.pdf [Accessed 5 May 2025].
8. Jayakumar, H., Raha, A., Kim, Y., Sutar, S., Lee, W.S. and Raghunathan, V., 2016. Energy-efficient system design for IoT devices. In: *2016 Asia and South Pacific Design Automation Conference (ASP-DAC)*. Macao, China, 2016. IEEE, pp.298–301. DOI: 10.1109/ASPDAC.2016.7428027. [Accessed 5 May 2025].
9. Kasznar, A.P.P., Hammad, A.W.A., Najjar, M., Linhares Qualharini, E., Figueiredo, K., Soares, C.A.P. and Haddad, A.N., 2021. Multiple Dimensions of Smart Cities’ Infrastructure: A Review. *Buildings*, 11(2), 73. DOI: 10.3390/buildings11020073 [Accessed 5 May 2025].
10. Kumar, P., Tiwari, P. and Mishra, A., 2019. A Survey on Security for Internet of Things: Security Requirements, Attacks, and Countermeasures. *Journal of Network and Computer Applications*, 143, pp. 102–121. DOI: 10.1016/j.jnca.2019.06.014 [Accessed 5 May 2025].
11. Lee, S.K., Bae, M. and Kim, H., 2017. Future of IoT Networks: A Survey. *Applied Sciences*, 7(10), 1072. Available at: https://doi.org/10.3390/app7101072. [Accessed 5 May 2025].
12. Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A., 2022. A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journa, 6(5)* pp.8182–8201. DOI: 10.1109/JIOT.2019.2935189. [Accessed 5 May 2025].
13. Sha, K., Yang, T.A., Wei, W. and Davari, S., 2020. A survey of edge computing-based designs for IoT security. *Digital Communications and Networks*, 6(4), pp. 195-202. DOI: 10.1016/j.dcan.2019.08.006 [Accessed 5 May 2025].
14. Wheelus, T. and Zhu, Z., 2020. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. *IEEE Transactions on Network and Service Management*, 17(1), pp. 56-70. DOI: 10.3390/iot1020016 [Accessed 5 May 2025].
15. Zaman, A., Hussain, M. and Iqbal, S., 2021. Security Threats and Artificial Intelligence-based Countermeasures for IoT Networks. *International Journal of Computer Applications*, 175(5), pp. 24-32. DOI: 10.1109/ACCESS.2021.3089681 [Accessed 5 May 2025].