Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

A Detailed Investigation of Threats in RF-Enabled IoT Systems

[1]Omar Sherif Farouk, [2]Tamer Salah Ezzat, [3]Amr Nour Abdelrahman

[1,2]Electrical Power and Control Engineering, Pyramids Higher Institute for Engineering and Technology, Egypt
[3]Department of Computer Engineering, University of Basra, Iraq

Abstract: The rapid adoption of Internet of Things (IoT) systems has led to widespread deployment of devices communicating over Radio Frequency (RF) channels, enabling applications ranging from smart homes to industrial automation. While RF-based communication provides flexibility and scalability, it also introduces significant security vulnerabilities that can be exploited by malicious actors. This research presents a detailed investigation of the security threats associated with RF-enabled IoT systems, including eavesdropping, signal jamming, spoofing, replay attacks, and unauthorized access. The study categorizes these threats based on their impact on confidentiality, integrity, and availability of IoT data and services. Additionally, the research analyzes the effectiveness of existing mitigation techniques, such as encryption, authentication protocols, frequency hopping, and intrusion detection mechanisms. Simulation results and literature-based analysis highlight critical vulnerabilities and demonstrate the need for comprehensive security frameworks tailored for RF-enabled IoT environments. The findings provide valuable insights for designers, developers, and security analysts aiming to enhance the resilience and trustworthiness of IoT networks against evolving cyber threats.

Keywords: RF, Radio frequency, Threats, Wireless communication, IoT networks, Security challenges, IoT security solutions, Wireless communication security.

I. Introduction

The Internet of Things (IoT) has transformed how devices communicate and share information, enabling applications in smart homes, healthcare, industrial automation, and environmental monitoring. A significant portion of IoT systems relies on Radio Frequency (RF) communication due to its wireless nature, low cost, and ability to connect devices over long distances. However, the very characteristics that make RF communication attractive also expose IoT networks to numerous security vulnerabilities. These vulnerabilities can compromise data confidentiality, integrity, and system availability, making RF-enabled IoT systems an attractive target for malicious attacks. This study aims to provide a comprehensive investigation into the various security threats in RF IoT networks and evaluate strategies for mitigating these risks.

Radio frequency (RF)-based Internet of Things (IoT) networks have transformed connectivity by enabling devices to communicate wirelessly over radio frequencies. These networks are critical to various sectors, such as smart homes, industrial automation, healthcare, agriculture, and environmental monitoring [1]. These networks consist of sensors, actuators, and smart devices that communicate using technologies such as Zigbee, Bluetooth Low Energy (BLE), Wi-Fi, and LoRaWAN. Each technology serves different purposes depending on factors such as range, power consumption, data speed, and application suitability. For example, Zigbee and BLE are used in low-power, short-range applications, while Wi-Fi is preferred for higher data rates in multimedia and real-time monitoring. The IoT network architecture is shown in Figure 1.

However, the rapid growth of RF-based IoT networks presents significant security challenges. These include risks such as unauthorized access, data interception, device tampering, and denial-of-service attacks [2]. Many IoT devices have limited resources and may prioritize functionality over security, making them prime targets for cyberattacks.

Securing RF-based IoT networks is complex due to their distributed configuration, diverse environments, and large number of connected devices. Protecting data integrity, confidentiality, and availability requires robust security protocols tailored to the unique characteristics and constraints of IoT environments [3]. RF-based IoT networks often operate in unlicensed frequency bands, such as 2.4 GHz, which are susceptible to interference, signal interception, and unauthorized access. As IoT adoption grows, the scale and complexity of RF networks increase, making traditional security measures inadequate. While encryption and authentication provide a

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

degree of protection, attackers continue to exploit protocol weaknesses, device misconfigurations, and physical vulnerabilities. Understanding these threats and developing mitigation strategies is crucial for ensuring the reliability and safety of IoT applications, especially those involving sensitive data or mission-critical operations.

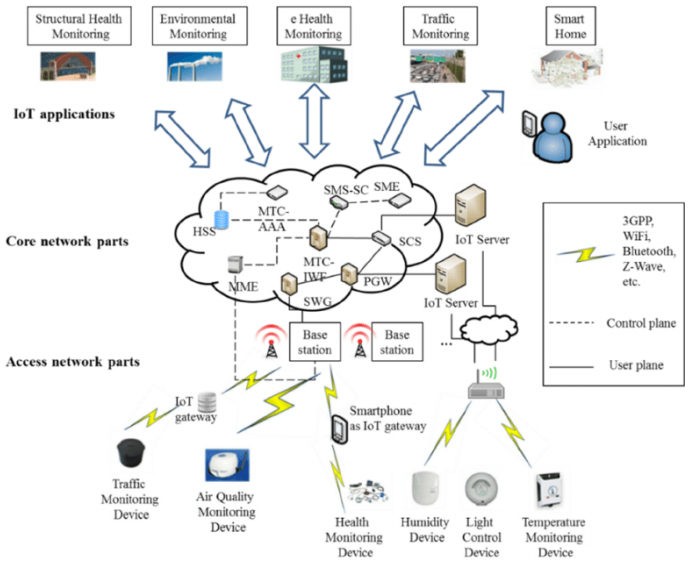

Figure 1: IoT network architecture

Furthermore, the dynamic nature of IoT ecosystems, characterized by device mobility, network changes, and varying communication patterns, makes maintaining consistent security measures difficult.

Despite these challenges, continuous advances in sensor technology, communication protocols, and data analytics continue to drive the development of RF-based IoT networks. These advances promise greater operational efficiency, cost savings, and an optimized user experience across all industries. However, to ensure the long-term security and sustainability of these networks, vulnerabilities must be addressed and proactive security strategies implemented.

Threat Analysis in RF IoT Systems:

RF-enabled IoT networks face multiple categories of security threats:

Eavesdropping: Attackers can intercept RF signals to gain access to sensitive data transmitted between IoT devices, such as sensor readings, authentication credentials, or control commands.

Signal Jamming and Denial-of-Service (DoS): Adversaries can intentionally interfere with RF channels, causing network disruptions, data loss, and system unavailability.

Spoofing and Replay Attacks: Malicious actors can impersonate legitimate devices or replay captured RF signals to manipulate IoT devices or inject unauthorized commands.

Unauthorized Access: Weak authentication mechanisms and default credentials can allow attackers to gain control over IoT devices.

Physical Layer Vulnerabilities: Devices that use RF communication are often deployed in unsecured locations, making them susceptible to tampering, hardware attacks, or signal manipulation.

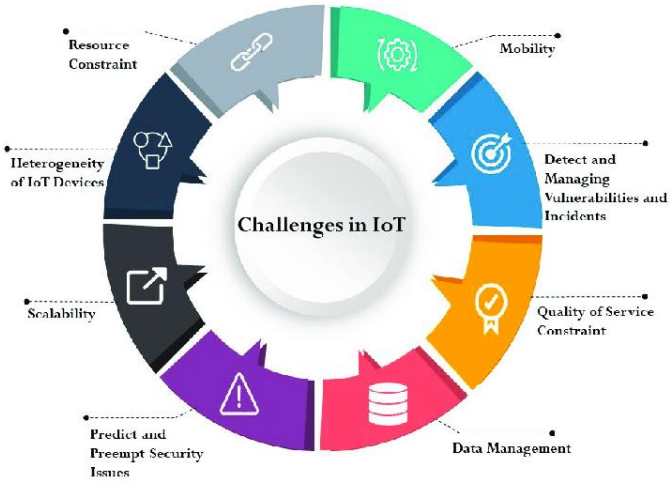

Figure 2: Challenges in IoT

This article aims to provide a comprehensive overview of security issues and solutions in RF-based IoT networks. By examining current vulnerabilities, evaluating existing security measures, and exploring new technologies such as advanced encryption, secure authentication, and anomaly detection, the paper aims to improve the resilience and security of RF-based IoT deployments. Practical examples and case studies illustrate effective security strategies and highlight the importance of collaboration to protect RF-based IoT networks from growing cybersecurity threats.

II. Security Threats in RF-Based IoT Networks

Despite their numerous advantages and application possibilities, RF-based Internet of Things (IoT) networks are subject to numerous security threats that compromise data integrity, user privacy, and system reliability [4]. Due to the use

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

of wireless technologies such as Zigbee, Bluetooth Low Energy (BLE), Wi-Fi, and LoRaWAN, these networks have certain vulnerabilities that attackers can exploit.

One of the biggest security concerns in RF-based IoT networks is unauthorized access. The wireless communication framework allows attackers to intercept and tamper with data packets, gaining unauthorized access to the network. This unauthorized access can lead to control of IoT devices, data leaks, or the injection of malicious commands that disrupt normal operations.

Another major threat is data interception. Without appropriate security measures, radio frequency (RF) signals can be intercepted by intruders who can steal sensitive information such as personal data, financial transactions, or operational details. This intercepted data can be used for identity theft, industrial espionage, or other malicious activities.

RF-based IoT networks are also at risk of device tampering. Attackers can exploit vulnerabilities in IoT devices to gain physical access or compromise their firmware, which can lead to unauthorized modifications, data manipulation, or the introduction of malware. These compromised devices can serve as entry points for broader network attacks.

Denial-of-Service (DoS) attacks are another serious concern. Attackers can overload the network with excessive requests or exploit vulnerabilities in IoT protocols to disrupt legitimate communications and services. These attacks can cause business disruption, financial loss, and reputational damage to organizations that rely on these networks.

Furthermore, poor authentication and authorization mechanisms pose significant risks. Many IoT devices and networks use default or easily guessed credentials, making them vulnerable to brute-force attacks. Inadequate authentication allows unauthorized access to devices or network resources, compromising overall network security.

Mitigating these security threats requires a comprehensive approach. Crucial steps include implementing strong encryption protocols for data transmission, ensuring robust authentication mechanisms to verify device identity, and regularly updating device firmware to address vulnerabilities. Implementing intrusion detection systems and network monitoring tools can also help detect and prevent potential attacks in real time.

Mitigation Techniques:

To counteract these threats, several security measures can be employed:

Encryption and Secure Communication Protocols: Implementing strong encryption (e.g., AES) ensures data confidentiality during RF transmission.

Authentication Mechanisms: Multi-factor and certificate-based authentication prevent unauthorized device access.

Frequency Hopping and Spread Spectrum Techniques: Randomizing transmission frequencies reduces the effectiveness of jamming and interception attacks.

Intrusion Detection Systems (IDS): Monitoring network traffic for unusual patterns allows early detection of malicious activities.

Physical Security Measures: Securing device hardware and deploying tamper-resistant modules protects against physical attacks.

Combining these approaches in a layered security framework enhances the overall resilience of RF-enabled IoT networks.

III. Existing Security Solutions and Their Limitations

Various security solutions have been developed to address the growing threats and vulnerabilities of RF-based IoT networks. These solutions aim to protect the integrity, confidentiality, and availability of data, but they have their own limitations [5].

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

Figure 3: IoT-Challenges and Opportunities

Encryption protocols: Encryption is widely used to protect data transmitted over RF-based IoT networks. Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are popular options for ensuring secure communication. Although encryption effectively prevents unauthorized access to data, it can be resource-intensive for IoT devices with limited computing power. This can lead to higher power consumption and latency, critical aspects in IoT environments.

Authentication mechanisms: Strong authentication mechanisms such as public key infrastructure (PKI) and digital certificates are essential for verifying the identities of devices and users in IoT networks. However, implementing PKI in IoT environments can be challenging due to the overhead of key management and the need for a secure infrastructure for certificate distribution and verification. Furthermore, many IoT devices lack the necessary computing power and storage capacity to efficiently handle complex authentication protocols.

Access Control: These models are effective at managing permissions, as the number of devices and users on an IoT network increases, management can become complex and difficult. Furthermore, the dynamic nature of IoT environments requires flexible and adaptive access control mechanisms, which traditional models often lack.

Intrusion Detection Systems (IDS): IDS to improve the effectiveness of IDS, machine learning and anomaly detection techniques have been integrated into IDS. However, IDS can generate false positives that can trigger unnecessary alerts and overwhelm network administrators. Furthermore, the limited resources of IoT devices can limit the implementation of sophisticated IDS solutions.

Firmware updates and patches: Regular firmware updates and patches are essential to address security vulnerabilities in IoT devices. However, the heterogeneous nature of IoT ecosystems, with devices from different manufacturers and varying capabilities, makes it difficult to implement uniform update mechanisms. Furthermore, some IoT devices may be installed in remote or hard-to-reach locations, complicating the upgrade process.

IV. New Trends and Technologies in RF-Based IoT Security

With the growth of RF-based IoT networks, the demand for advanced security measures is increasing. New trends and technologies are shaping the future of IoT security and offering innovative solutions to address constantly evolving threats and challenges [6].

Blockchain Technology: Blockchain is emerging as a valuable tool for improving IoT security. Its decentralized and immutable ledgers ensure secure and transparent transaction records, protect data integrity, and prevent unauthorized modification. Smart contracts within blockchain frameworks can automate and enforce security protocols, minimizing human error and increasing trust between IoT devices.

Artificial Intelligence and Machine Learning: Machine learning algorithms can adapt to new threats, improving the accuracy and effectiveness of intrusion detection systems (IDS) and other security measures.

Quantum cryptography: Quantum cryptography introduces a new layer of security for RF-based IoT networks. By relying on the principles of quantum mechanics, quantum cryptography can theoretically create unbreakable encryption keys. This technology can significantly improve the protection of sensitive data transmitted over IoT networks, making it virtually immune to interception and decryption by malicious actors.

Edge computing: Edge computing is becoming a critical trend in IoT security. By processing data closer to its source (at the network edge), you reduce the risk of interception and tampering in transit. Furthermore, it enables faster detection and response to security threats, as the data does not need to be transferred to a central location for analysis.

V. Real-World Cases and Practical Implementations

Reviewing case studies and practical implementations provides valuable insights into the application of RF-based IoT security solutions in real-world scenarios, demonstrating their effectiveness and the associated challenges.

Smart Cities: A good example is the use of IoT networks in smart cities. Barcelona has implemented IoT devices throughout its urban infrastructure to manage resources such as water, electricity, and waste. The city uses secure communication protocols and strong encryption to protect data transmitted between sensors and control systems [7]. However, managing a large number of devices and ensuring consistent security updates remains a challenge.

Healthcare Monitoring Systems: In healthcare, RF-based IoT devices are used to remotely monitor patients. Hospitals use devices to monitor vital signs and transmit the data to medical

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

professionals in real time [8]. The University of Pittsburgh Medical Center (UPMC) has implemented such a system and uses strong encryption and authentication mechanisms to protect patient data. Despite these measures, maintaining the security of these devices against potential security breaches remains a significant challenge, as they involve sensitive health data and require continuous monitoring. Industrial IoT (IIoT): In the manufacturing sector, companies such as Siemens have adopted industrial IoT to improve operational efficiency. They implement radio frequency (RF)-based sensors and actuators to monitor and control manufacturing processes [9]. Siemens uses edge computing for local data processing, thus reducing the risk of data interception in transit. They also implement robust access control measures to ensure that only authorized personnel can access critical systems. However, protecting large industrial networks remains a complex task.

Agriculture: Precision agriculture uses RF-based IoT networks to improve agricultural practices. John Deere, for example, uses IoT devices to collect data on soil moisture, weather conditions, and crop health. These devices communicate securely with cloud platforms for data analysis and decision-making [10]. While this data is protected by encryption and secure communication protocols, ensuring the security of IoT devices in large, remote agricultural areas remains a challenge.

Challenges and Limitations:

Despite mitigation efforts, RF IoT networks face persistent challenges due to resource constraints of IoT devices, such as limited processing power, memory, and energy. Implementing advanced security protocols may increase latency or energy consumption, affecting network performance. Additionally, evolving attack vectors and sophisticated adversaries require continuous updates to security strategies. Therefore, research in adaptive, lightweight, and context-aware security solutions remains critical.

VI. Conclusion

This study provides a detailed investigation of the security threats inherent to RF-enabled IoT networks and evaluates mitigation strategies for protecting data and system integrity. RF communication offers flexibility and scalability but introduces vulnerabilities that must be addressed through encryption, authentication, intrusion detection, and physical security measures. The findings emphasize the importance of a comprehensive, layered security approach to safeguard IoT devices against emerging threats. By understanding the nature of RF-specific attacks and applying appropriate countermeasures, designers and security analysts can significantly enhance the resilience and trustworthiness of IoT networks. The increasing proliferation of radio frequency (RF)-based IoT networks, addressing their security challenges is becoming increasingly important. By leveraging these technologies, IoT networks can better defend against constantly evolving cyber threats and protect sensitive data. To achieve these goals, collaboration among stakeholders is critical. This includes creating and enforcing strict regulations, promoting secure design principles, and encouraging regular security assessments and updates. In short, the future of RF-based IoT security depends on a multifaceted approach that combines advanced technologies, collaborative efforts, and continuous education. By prioritizing security at every stage of IoT development and deployment, stakeholders can create a more secure environment for IoT networks. This proactive approach not only protects against current threats but also anticipates and mitigates future risks, ensuring the sustainability and long-term success of IoT innovations.

As radio frequency (RF)-based Internet of Things (IoT) networks become more widespread, addressing their security vulnerabilities is increasingly critical. The dynamic nature of the IoT environment demands ongoing innovation and future strategies should emphasize the incorporation of advanced technologies, including blockchain, artificial intelligence, quantum cryptography, and edge computing, to establish security frameworks that are both resilient and flexible. Utilizing these technologies will enable IoT networks to better counteract the ever-evolving cyber threats and safeguard sensitive data. The growing prevalence of radio frequency (RF)-based Internet of Things (IoT) networks underscores the urgent need to tackle their security challenges. The continuously changing IoT landscape requires persistent innovation and the establishment to formulate security frameworks that are resilient and adaptable. By leveraging these technologies, IoT networks can enhance their defenses against evolving cyber threats and secure sensitive information effectively.

REFERENCES

[1] C. Morimoto, R. Chellappa, ”Fast electronic digitl image stabilization” Proc. 13th International Conference on Pattern Recognition, vol. 3, pages .284-288, 25-29 August 1996.

[2] M. Papageorgiou, Video sensors, Papageorgiou Markos (Ed.), Concise Encyclopedia of traffic and transportation systems, pp. 610–615.

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

[3] W. Enkelmann, Obstacle detection by evaluation of optical flow field from image sequences, Proceedings of European Conference on Computer Vision, Antibes, France 427 (1990) 134–138.

[4] Mishra, Nivedita, and Sharnil Pandya. "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review." IEEE Access 9 (2021): 59353-59377.

[5] Liu, Qingzhi, et al. "Safe and secure wireless power transfer networks: Challenges and opportunities in RF-based systems." IEEE Communications Magazine 54.9 (2016): 74-79.

[6] Wu, Weiwei, et al. "Reliable resource allocation with RF fingerprinting authentication in secure IoT networks." Science China Information Sciences 65.7 (2022): 170304.

[7] Mojail, N. Disages K., et al. "Understanding Capacitance and Inductance in Antennas." National Journal of Antennas and Propagation 4.2 (2022): 41-48.

[8] N. Hoose, Computer vision as a traffic surveillance tool, IFAC Transportation systems, Tianjin, Proceedings (1994).

[9] X. Li, Z.-Q. Liu, K.-M. Leung, Detection of vehicles from traffic scenes using fuzzy integrals, Pattern Recognition 35 (2002) 967–980.

[10] H. Moon, R. Chellapa, A. Rosenfeld, Performance analysis of a simple vehicle detection algorithm, Image and Vision Computing 20(2002) 1–13.

[11] Multimedia, “Use Image Stabiliza. For Gyroscopic Stabilizer”, [online], URLhttp://www.websiteoptimization.com/speed/tweak/stabilizer. Access 13-January- 2009].

[12] B. Ross, A practical stereo vision system, Proceedings of International Conference on Computer Vision and Pattern Recognition, Seattle, WA (1993) 148–153.

[13] M. Bertozzi, A. Broggi, S. Castelluccio, A real-time oriented system for vehicle detection, Journal of System Architecture 43 (1997) 317–325.

[14] F. Thomanek, E.D. Dickmanns, D. Dickmanns, Multiple object recognition and scene interpretation for autonomous road vehicle guidance, Proceedings of IEEE Intelligent Vehicles 94, Paris, France (1994) 231–236.

[15] A.Kuehnel, Symmetry based recognition of the vehicle rears, Pattern Recognition Letters 12 (1991) 249–258. North Holland, Amsterdam.

[16] M. Fathy, M.Y. Siyal, A window-based image processing technique for quantitative and qualitative analysis of road traffic parameters, IEEE Transactions on Vehicular Technology 47 (4) (1998).

[17] D.C. Hogg, G.D. Sullivan, K.D. Baker, D.H. Mott, Recognition of vehicles in traffic scenes using geometric models, IEE, Proceedings of the International Conference on Road Traffic Data Collection, London (1984) 115–119.

[18] Saxena, Vishal Narain, Juhi Gupta, and Vivek K. Dwivedi. "On the security of RF-based IoT network with randomly located eavesdropper." Proceedings of Second International Conference on Computational Electronics for Wireless Communications: ICCWC 2022. Singapore: Springer Nature Singapore, 2023.

[19] G.L. Foresti, V. Murino, C. Regazzoni, Vehicle recognition and tracking from road image sequences, IEEE Transactions on Vehicular Technology 48 (1) (1999) 301–317.

[20] G.L. Foresti, V. Murino, C.S. Regazzoni, G. Vernazza, A distributed approach to 3D road scene recognition, IEEE Transactions on Vehicular Technology 43 (2) (1994).

[21] K. Shimizu, N. Shigehara, Image processing system used cameras for vehicle surveillance, IEE Second International Conference on Road Traffic Monitoring, Conference Publication Number 299 February (1989) 61–65.

[22] M. Fathy, M.Y. Siyal, An image detection technique based on morphological edge detection and background differencing for realtime traffic analysis, Pattern Recognition Letters 16 (1995) 1321–1330.

[23] Benkhelifa, Elhadj, Thomas Welsh, and Walaa Hamouda. "A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems." IEEE communications surveys & tutorials 20.4 (2018): 3496-3509.

[24] Abhishek Bhattacharjee, Tanmoy Majumder, & Sabarni Bhowmik.(2023). A Low Power Adiabatic Approach for Scaled VLSI Circuits. Journal of VLSI Circuits and Systems, 6(1), 1–6. https://doi.org/10.31838/jvcs/06.01.01.

[25] Kornaros, Georgios. "Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective." IEEE Access 10 (2022): 58603-58622.

[26] Zeb, Hassan, et al. "Zero energy IoT devices in smart cities using RF energy harvesting." Electronics 12.1 (2022): 148.

[27] Gibson, Katharine, And Y. Salamonson. "Image processing application: Overlapping of Images for faster video processing devices." International Journal of communication and computer Technologies 11.1 (2023):

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 28-34, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211005
Available Online at https://www.jaiet.com

10-18.

[28] Yew, Hoe Tung, et al. "Iot based real-time remote patient monitoring system." 2020 16th IEEE international colloquium on signal processing & its applications (CSPA). IEEE, 2020.

[29] Zhang, Tiantian, et al. "Intelligent radio frequency identification for URLLC in industrial IoT networks." Symmetry 14.4 (2022): 801.

Citation of this Article:

Omar Sherif Farouk, Tamer Salah Ezzat, & Amr Nour Abdelrahman. (2025). A Detailed Investigation of Threats in RF-Enabled IoT Systems. *Journal of Artificial Intelligence and Emerging Technologies.* 2(11), 28-34. Article DOI: https://doi.org/10.47001/JAIET/2025.211005

***** End of the Article *****