




Paper Type: Original Article

## Improving IoT Security in Wireless Sensor Networks

Diptanshu Saha\* 

School of Computer Engineering, KIIT University, Bhubaneswar, India; sdiptanshu14@gmail.com.

### Citation:

Received: 17 July 2024

Revised: 01 October 2024

Accepted: 10 December 2024

Saha, D. (2024). Improving IoT security in wireless sensor networks. *Smart internet of things*, 1(4), 289-297.


### Abstract


The security of IoT-based Wireless Sensor Networks (WSNs) has emerged as a pressing issue, particularly as these networks are extensively utilized in sectors like healthcare, industrial automation, and smart cities. Given their limited computational capabilities, WSNs are especially susceptible to cyber threats, creating challenges for data integrity, confidentiality, and scalability of the network. This paper tackles these issues by examining three pivotal security algorithms: Elliptic Curve Cryptography (ECC) for effective key exchange, Advanced Encryption Standard (AES) for strong data encryption, and the Lightweight Authentication Protocol (LAP) aimed at low-resource mutual authentication. The approaches discussed involve modifying these algorithms to fit the restricted capacities of IoT devices while also introducing new security improvements to address current limitations. Specifically, the proposed initiatives encompass adaptive resource-efficient encryption, a hierarchical key management system, end-to-end protocols for data integrity, tamper-resistant hardware components, and a cross-layer security framework to safeguard communications throughout the entire network. These solutions were assessed for their ability to enhance the resilience and security efficiency of WSNs without overburdening device resources. The findings suggest that lightweight encryption techniques, hierarchical architectures, and tamper-resistant hardware can considerably strengthen IoT security in resource-limited WSNs. These outcomes contribute to building a scalable and versatile security framework, enabling safer IoT applications in essential industries, and fostering trust in IoT-enabled infrastructure moving forward.

**Keywords:** Encryption, Authentication, Wireless sensor networks.

## 1 | Introduction

The power of the Internet of Things (IoT) has revolutionized device-device and system-system communication, leading to a connected ecosystem that can address multiple domains ranging from healthcare and smart cities to industrial automation. In this ecosystem, the Wireless Sensor Networks (WSNs) are spatially distributed sensors that connect through wireless connections and send data. WSNs are designed to collect information from the real world in near-real-time, supporting various applications requiring sensing

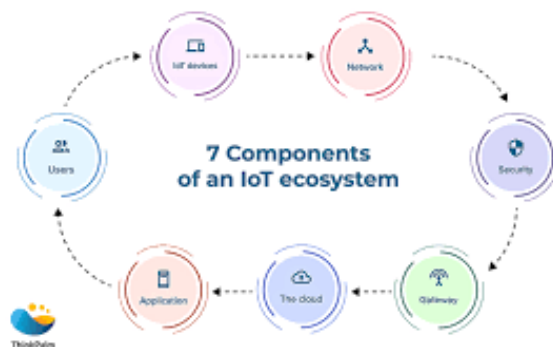
 Corresponding Author: sdiptanshu14@gmail.com

 <https://doi.org/10.22105/siot.v1i4.138>



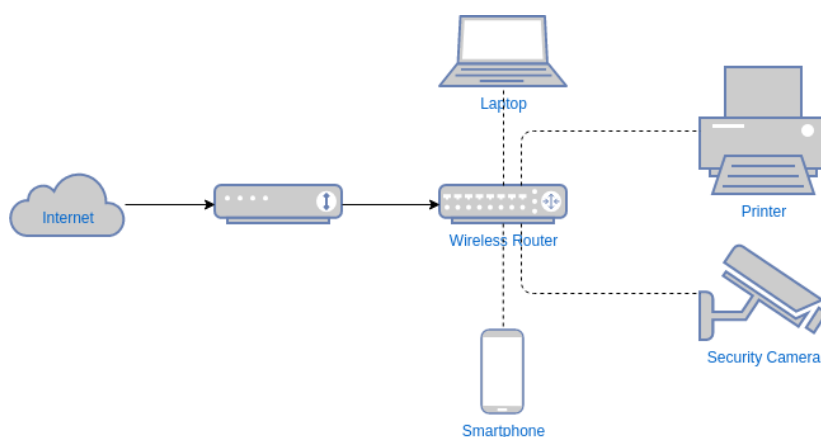
Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

and control. Nevertheless, these networks are highly prone to adversaries and face extremely challenging situations due to their constrained computational resources, power limitations, and susceptibility to cyber threats, making security a major concern for IoT seamless functionality in a safe manner. *Fig. 1* shows the seven components of an IoT Ecosystem.



**Fig. 1. Components of an IoT ecosystem.**

Ensuring IoT security in WSNs involves implementing robust mechanisms safeguarding data integrity, authenticity, and confidentiality within these interconnected networks. Advanced security measures, such as encryption techniques, authentication protocols, and anomaly detection systems, are now essential to protect WSNs against malicious activities. Despite the innovations, vulnerabilities persist due to the open nature of IoT environments, where data must be shielded against unauthorized access and tampering. WSNs have emerged as a transformative technology in modern communication and data acquisition. These networks are an integral part of the IoT ecosystem and play a pivotal role in various domains, including environmental monitoring, industrial automation, healthcare, smart cities, and more [1]. *Fig. 2* shows the security of a network through a data flow diagram.



**Fig. 2. Network security data flow diagram.**

## 2 | Literature Review

Various algorithms have been applied to secure IoT-based WSNs, each addressing specific security needs within these resource-limited environments. Elliptic Curve Cryptography (ECC) offers robust protection with low computational requirements, making it ideal for secure key exchanges in WSNs. Advanced Encryption Standard (AES), a high-security block cipher, encrypts data efficiently, safeguarding it against unauthorized access. Additionally, the Lightweight Authentication Protocol (LAP) provides mutual authentication between

devices and servers with minimal resource use, ensuring trusted communication. ECC, AES, and LAP form a strong security foundation for WSNs by enhancing data confidentiality, integrity, and authentication.

## 2.1 | Elliptic Curve Cryptography Algorithm

### Description

An ECC algorithm is a public key encryption method based on the mathematics of elliptic curves over finite fields. It tempts a high-security level, creating an elliptic curve data key that safeguards the transmission and optimizes computational efficiency. EC cryptography is used extensively in the vast network of IoT to help support secure communication, establishment of keys, and data integrity. ECC is a public key cryptography algorithm, and this model detects several kinds of attacks, including man in the middle, denial of service, and weak authentication. The ECC model utilizes two keys: the public key and the private key. The public key encrypts the real information; the private key decrypts the original information [2].

**Step 1.** Select an elliptic curve: initialize a curve equation elliptic curve over a finite field), which is used to encrypt the messages. The curve is designed to have parameters  $a$  and  $b$  that meet security requirements.

**Step 2.** Generate key pairs: 1) Private Key: choose a large random number for that private key. 2) ECC functions have properties that range from private keys to public Keys. — Public Key => Compute the public key and multiply it with your Private Quadratic Residue  $Q$  on the Elliptic Curve. It is a predefined and shared base point that provides an initial key generation starting point.

**Step 3.** Encrypt the data: the sender creates a new temporary private key and derives the corresponding temporary public key.

This data message is then encoded using the sender's temporary public key, combined with a public uplink secure layer enterprise PK and eventually the recipient's private enterprise key, to ensure that only this specific person can decrypt it.

**Step 4.** Transmit encrypted data: Sender: the sender sends back encrypted data and a temporary public key. The recipient decrypts the message using this temporary public key and their private key.

**Step 5.** Decrypt the data: with some math help from ECC, the recipient rebuilds the original message using her private key in combination with the sender's public key.

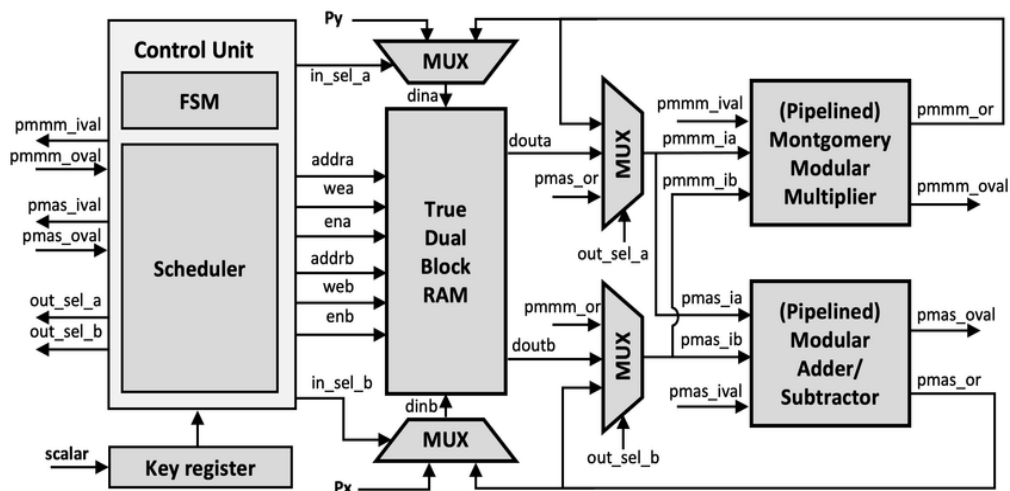


Fig. 3. Working of AES algorithm.

### Benefits of ECC in IoT Security for WSNs

**Fast Computation:** the lesser the key sizes are, the easier it is for computation to save CPU resources on devices

Strong encryption: secure data transmission across WSNs, combatting potential attacks.

Scalability: facilitates seamless integration through multiple IoT applications with minimal overheads on network resources.

## 2.2 | Advanced Encryption Standard Algorithm

### Description

The AES is a symmetric encryption algorithm widely used for securing data in WSNs and IoT applications. Due to its balance of security and efficiency, AES is ideal for IoT devices with constrained resources. It uses a block cipher approach, dividing data into fixed-size blocks (typically 128-bit) and encrypted in rounds. One of the most widely studied encryption algorithms is the AES, which offers robust security and efficiency in securing digital communications. AES, developed by Daemen and Rijmen, supports key lengths of 128, 192, and 256 bits, with AES 256-bit encryption providing the highest level of security [3]. The AES Algorithm, adopted by the U.S. government in 2001, is a block cipher that transforms 128-bit data blocks under a 128-bit, 192-bit or 256-bit secret key by means of permutation and substitution [4].

**Step 6.** Key expansion: through key expansion, a 128-bit secret key creates a series of round keys. These round keys are used in each encryption round to ensure the data's secure transformation.

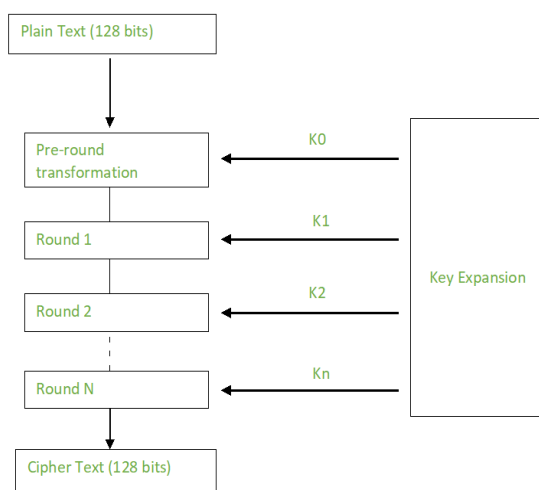
**Step 7.** Initial round: add round key: the initial plaintext block is XORed with the initial round key, creating the first transformation of the data.

**Step 8.** Encryption rounds (typically 10 rounds for 128-bit AES).

- I. SubBytes: each byte in the block is substituted using a predefined substitution table (S-Box).
- II. ShiftRows: rows of the block are shifted cyclically to the left to create data diffusion.
- III. MixColumns: columns of the block are mixed by applying a mathematical transformation to increase diffusion.
- IV. Add round key: the current state is XORed with the round key for each round.

**Step 10.** Final round: the final round involves SubBytes, ShiftRows, and Add Round Key steps but omits MixColumns. The output after this round is the encrypted ciphertext.

**Step 11.** Data decryption: the decryption process is the reverse of encryption, where each step (Add Round Key, MixColumns, ShiftRows, SubBytes) is applied in reverse order. *Fig. 4* below shows the algorithm's entire workings.



**Fig. 4.** Working of AES algorithm.

### Advantages of AES in IoT Security for WSNs

- I. High Security: AES is resistant to most known cryptographic attacks and is the standard for secure data encryption.
- II. Efficiency: With small block sizes, AES operates efficiently on low-power IoT devices, making it suitable for WSNs.
- III. Versatility: AES can support multiple key lengths (128, 192, 256 bits), allowing for adaptable levels of security based on application needs.

## 2.3 | Lightweight Authentication Protocol

### Description

The LAP is designed for resource-constrained IoT devices, providing mutual authentication between devices and servers with minimal computational and memory requirements. LAP is widely used in WSNs to prevent unauthorized access and secure data exchange. In LAP-IoHT, the gateway authenticates all participants, including the users and wearable sensors. Subsequently, a shared session key is established for each communication session. LAP-IoHT encrypts the biometric features of the users to ensure anonymity [5].

**Step 12.** Initialize parameters: the device and server establish shared parameters, including a secret key and unique device identifiers.

**Step 13.** Device sends authentication request: the device initiates an authentication request by generating a unique nonce (random number) and combining it with the device's identifier, creating a message sent to the server.

**Step 14.** Server authentication: the server verifies the device's identifier and generates a response by encrypting the device's nonce with the shared key. This encrypted response is then sent back to the device.

**Step 15.** Device verification: the device decrypts the server's response using the shared key and confirms its authenticity by comparing the decrypted nonce with its original nonce.

**Step 16.** Mutual authentication success: if the device's verification is successful, both entities can securely exchange data, as mutual authentication has been established.

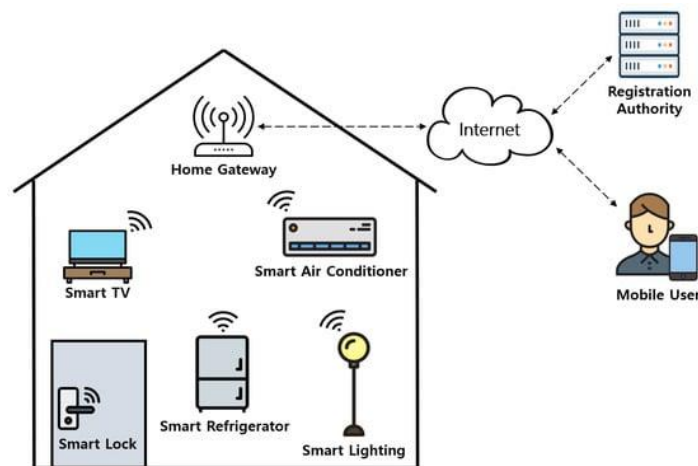


Fig. 5. LAP algorithm in IoT.

### Advantages of LAP in IoT Security for WSNs

- I. Low Computational Overhead: The protocol requires minimal computation, ideal for WSNs with limited processing capabilities.

- II. Mutual Authentication: Ensures server and device authenticate each other before data exchange, enhancing security.
- III. Efficient Resource Usage: A lightweight protocol design minimizes power and memory usage, which is crucial for IoT networks with constrained devices.

## 3 | Limitations and Challenges in IoT Security for WSNs

As IoT-based WSNs expand across various applications, securing these networks faces unique limitations and challenges. Limited device resources, potential scalability issues, and vulnerability to diverse attack vectors present significant hurdles to implementing comprehensive security solutions. Understanding these challenges is essential for developing effective, resilient strategies for IoT security.

### 3.1 | Resource Constraints

IoT-based WSNs often consist of small, low-power devices with limited processing capabilities, memory, and battery life. This restricts the implementation of complex security protocols and robust encryption algorithms, making it challenging to achieve strong security without compromising performance or efficiency.

### 3.2 | Scalability Issues

As the number of devices in IoT networks grows, scalability becomes a concern. Adding new devices requires the security system to handle increased authentication requests, key management complexities, and data integrity checks, which can overload networks and lead to security vulnerabilities.

### 3.3 | Data Integrity and Privacy Risks

IoT-based WSNs are vulnerable to attacks like eavesdropping and data interception, compromising data integrity and privacy. Ensuring data protection in transit and at rest, particularly within low-power sensors, is challenging due to their limited storage and processing capabilities.

### 3.4 | Vulnerability to Physical Attacks

IoT sensors are often deployed in remote or unsecured areas, making them vulnerable to physical tampering and node capture attacks. Attackers can gain direct access to devices, extract encryption keys, or tamper with data, creating significant security risks for the network.

### 3.5 | Complexity of Multi-Layered Security

IoT security for WSNs often requires a multi-layered approach, encompassing device-level, network-level, and application-level security. Implementing cohesive security measures across these layers is challenging due to device diversity and varying communication protocols, which may lead to gaps in protection.

IoT in smart manufacturing has led to a major improvement in product quality and efficiency of the manufacturing process. However, enormous uncertainty issues can still arise during its implementation. Some of the main challenges include the uncertainty of machine designers, builders, and even the end users to contrive this technology, as each enterprise has its own design requirements and process. This also creates the need for a customized design, which is usually expensive and requires experts in the related domain [6].

## 4 | Future Directions and Emerging Solutions in IoT Security for WSNs

Addressing the security challenges posed by IoT requires a multifaceted approach, including developing secure firmware and software, implementing robust authentication and access control mechanisms, and deploying IoT-specific security solutions that can monitor and detect anomalous behavior in these resource-constrained devices [7].

With the continuous evolution of IoT technology, new solutions are emerging to address the security challenges within WSNs. Cutting-edge advancements, such as lightweight cryptography, AI-driven intrusion detection, and blockchain, promise to enhance network security. Exploring these solutions can pave the way for innovative, resource-efficient approaches to safeguarding IoT-enabled WSNs.

#### **4.1 | Lightweight Cryptography Advances**

Lightweight cryptographic algorithms designed for IoT devices aim to provide strong security with minimal resource consumption. Research into these algorithms, such as ChaCha20 and SPECK, continues to evolve, making it possible to balance security and efficiency for resource-limited WSNs.

#### **4.2 | AI-Driven Intrusion Detection Systems**

Artificial Intelligence (AI) and Machine Learning (ML) are becoming integral to identifying unusual patterns and detecting security breaches in real-time. Emerging AI-driven intrusion detection systems can help WSNs identify threats early and respond autonomously, enhancing network resilience without constant human intervention.

#### **4.3 | Blockchain for Decentralized Security**

Blockchain technology can address IoT security issues through decentralized data storage, making it difficult for attackers to compromise the network. Using blockchain, each sensor's data can be securely verified across the network, enhancing trust and data integrity without relying on a central authority.

#### **4.4 | Quantum Cryptography**

Although still emerging, quantum cryptography holds promise for secure communication in IoT networks by enabling unbreakable encryption techniques. Quantum key distribution (QKD) is a potential solution for future IoT and WSN security, providing theoretically unbreakable encryption for data transmitted across networks. The field of quantum cryptocurrency encompasses the implementation of quantum cryptography protocols, which are designed to ensure secure transactions that can withstand potential threats posed by quantum computing technology [8].

#### **4.5 | Context-Aware Security Protocols**

Context-aware security protocols adapt security measures based on device location, data sensitivity, and environmental conditions. This approach allows WSNs to apply stricter security for more sensitive data while minimizing resource use for less critical applications, making security more adaptable and efficient.

### **5 | Proposed Work**

This proposed work outlines innovative approaches tailored to the constraints and vulnerabilities of IoT-based WSNs to address the critical limitations. By focusing on resource efficiency, scalability, data integrity, and adaptive security, these strategies aim to improve security without overburdening the network [9], [10].

#### **5.1 | Adaptive Resource-Efficient Encryption**

To counter resource constraints, this approach introduces adaptive encryption methods that adjust encryption strength based on data sensitivity and network load. Lightweight encryption techniques, such as ECC-based variations and optimized AES, will be used to achieve secure data transmission without overwhelming device resources.

## 5.2 | Hierarchical Key Management for Scalability

This proposal includes a hierarchical key management system where cluster heads manage encryption keys for their nodes to manage scalability. This structure reduces the need for individual devices to handle complex key exchanges, improving security scalability while distributing computational load across the network.

## 5.3 | End-to-End Data Integrity Protocols

To ensure data integrity and privacy, this solution proposes an end-to-end protocol that validates data at both source and destination points. Combining digital signatures and hash-based data verification can create a secure path, enabling strong integrity without continuous encryption at each node.

## 5.4 | Tamper-Resistant Hardware Modules

For physical security, tamper-resistant hardware modules in IoT sensors are proposed. These modules can store encryption keys securely, making it harder for attackers to extract data through physical attacks. In conjunction, these modules would trigger alarms upon physical tampering, adding a layer of security to network nodes.

## 5.5 | Cross-Layer Security Framework

This proposal advocates for a cross-layer security framework to address the complexity of multi-layered security requirements. By integrating security protocols across the physical, network, and application layers, this framework can reduce security gaps and offer a unified approach to effectively handle diverse WSN protocols and device types.

## 6 | Conclusion

In conclusion, securing IoT-based WSNs is crucial to advancing IoT applications in diverse fields despite resource constraints, scalability, and data vulnerability challenges. This research underscores the need for foundational and innovative security mechanisms in IoT networks by reviewing effective algorithms- ECC, AES, and LAP. The proposed adaptive encryption techniques, hierarchical key management, and tamper-resistant hardware modules offer practical solutions to address these limitations while enhancing network resilience. By implementing these strategies, WSNs can achieve a higher security standard, protecting data integrity and ensuring trust in IoT-driven operations. This work contributes valuable approaches that can guide the development of robust, scalable security frameworks for the future of IoT-based WSNs.

## Author Contribution

Diptanshu Saha: The author conducted all aspects of the research, including the conceptualization, methodology design, analysis of security algorithms, and proposal of innovative solutions to enhance IoT security in WSNs.

## Funding

This research received no external funding.

## Data Availability

The data used during the current study are available from the author upon reasonable request.

## Conflicts of Interest

The author declares no conflict of interest.

If necessary, these sections should be tailored to reflect the specific details and contributions.



## References

- [1] Chaudhary, P., & Wao, A. A. (n.d.). Wireless sensor network. [https://www.researchgate.net/profile/Akhilesh-Wao-2/publication/378736551\\_Wireless\\_Sensor\\_Network/links/65e722a8adf2362b63782126/Wireless-Sensor-Network.pdf](https://www.researchgate.net/profile/Akhilesh-Wao-2/publication/378736551_Wireless_Sensor_Network/links/65e722a8adf2362b63782126/Wireless-Sensor-Network.pdf)
- [2] Arunkumar, J. R., Velmurugan, S., Chinnaiyah, B., Charulatha, G., Prabhu, M. R., & Chakkaravarthy, A. P. (2023). Logistic regression with elliptical curve cryptography to establish secure IoT. *Computer systems science & engineering*, 46(1). <https://www.researchgate.net>
- [3] Goel, A., Baliyan, H., Tyagi, S., & Bansal, N. (2024). End to end encryption of chat using advanced encryption standard-256. *International journal of science and research archive*, 12(1), 2018–2025.
- [4] Patil, P., & Patil, A. R. (2018). Implementation of data encryption standard algorithm using verilog. *International journal of wireless network security*, 4(1), 37–44. <https://doi.org/10.37628/ijownsv4i1.372>
- [5] Chen, C.-M., Chen, Z., Kumari, S., & Lin, M.-C. (2022). LAP-IoHT: A lightweight authentication protocol for the internet of health things. *Sensors*, 22(14), 5401. <https://doi.org/10.3390/s22145401>
- [6] Zahra, F. T., Bostanci, Y. S., & Soyuturk, M. (2024). Security of wireless IoT in smart manufacturing: vulnerabilities and countermeasures. *Intelligent secure trustable things*, 419. <https://library.oapen.org/bitstream/handle/20.500.12657/92309/978-3-031-54049-3.pdf?sequence=1#page=424>
- [7] Alabi, M. (2024). Security challenges and solutions in wireless networks: a computer science perspective. <https://www.researchgate.net>
- [8] Imran, M., Altamimi, A. B., Khan, W., Hussain, S., Alsaffar, M., & others. (2024). Quantum cryptography for future networks security: A systematic review. *IEEE access*. <https://doi.org/10.1109/ACCESS.2024.3504815>
- [9] Dhanraj, T., Kumar, M., Singh, S., Kumar, R., Jaiswal, P., & Mohapatra, H. (2024). A review on mitigating privacy risks in IoT-enabled smart homes. *Computer networks and communications*, 146–163. <https://ojs.wiserpub.com/index.php/CNC/article/download/4736/2296>
- [10] Mohapatra, H. (2025). The role of 6G in empowering smart cities enabling ubiquitous connectivity and intelligent infrastructure. *RFID, microwave circuit, and wireless power transfer enabling 5/6g communication* (pp. 231–254). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-8799-3.ch008>