IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

RFID WIRELESS SECURITY SYSTEM

Ms. Vijayalakshmi N, Anand Kumar Jaiswal C, John Samuel Raj J, Joshua Virgil J, Karthick Rajavel S,

Assistant Professor, Department of Computer Science and Engineering,

"IV'th year, Department of Computer Science and Engineering, SNS College Of Technology, Coimbatore, Tamil Nadu, India

Abstract: *A common automatic identification and data capture (AIDC) technology is radio frequency identification (RFID). It has applications in many different fields, including access control, asset tracking, and inventory management. However, security has grown to be a significant issue because of the widespread use of RFID technology. RFID transmission is wireless, making it susceptible to different forms of attacks, such as eavesdropping, spoofing, and denial of service. The goal of this project is to develop and deploy a secure RFID wireless security system to guarantee the privacy, availability, and integrity of data sent across RFID communication channels. The suggested system will protect communication between RFID tags and readers using cryptographic methods such symmetric and asymmetric encryption, digital signatures, and message authentication codes. To ensure that only authoriszed users may access the RFID system, the system will also have access control methods. The proposed system will be judged on its performance, usability, and security. The evaluation's findings will be applied to verify the suggested system's efficacy.*

Keywords: ***RFID, AIDC***

1. INTRODUCTION

The automated identification and data capture (AIDC) technology known as radio frequency identification (RFID) allows for the wireless transfer of data between RFID tags and readers. Numerous industries, including asset tracking, access control, and inventory management, have found extensive use for RFID technology. RFID transmission is wireless, though, which leaves it open to many forms of attacks like eavesdropping, spoofing, and denial of service. As a result, there is now a lot of anxiety about the security of RFID systems.

The use of RFID systems has significantly expanded in recent years, which has raised the potential of security risks. In order to guarantee the confidentiality, integrity, and availability of data exchanged across RFID communication channels, a secure RFID wireless security system is required.

The proposed project intends to develop and deploy a secure RFID wireless security system that will protect communication between RFID tags and readers using cryptographic methods. To ensure that only authorised users may access the RFID system, the system will also have access control methods.

In conclusion, this project will help to design a safe RFID wireless security system that will support maintaining privacy, accuracy, and accessibility.

2. METHODOLOGY

2.1 System Requirements

To make sure that only authorised users can use the system, the system should authenticate the identity of the RFID reader and the RFID tag before permitting data exchange. To guarantee that only authorised users may access the RFID system, the system needs to incorporate access control measures. To protect the privacy of the data exchanged between the RFID reader and the RFID tag, the system should employ encryption techniques.

A high number of RFID tags and readers should be able to be supported by the system. The system should be capable of sending large amounts of data quickly and efficiently. The system needs to be dependable and able to function in challenging environmental circumstances.

2.2 System Design

Three primary parts make up the proposed RFID wireless security system: RFID tags, RFID readers, and a backend server. To protect the connection between RFID tags and readers, the system architecture integrates cryptographic techniques such symmetric and asymmetric encryption, digital signatures, and message authentication codes. Access control methods are also incorporated into the system architecture to guarantee that only authorised users can access the RFID system.

Each RFID tag in the system has a unique identifier programmed into it, and it can store data like location or product details. Both a battery and energy from the RFID reader are used to power the wireless communication between RFID tags and RFID readers.

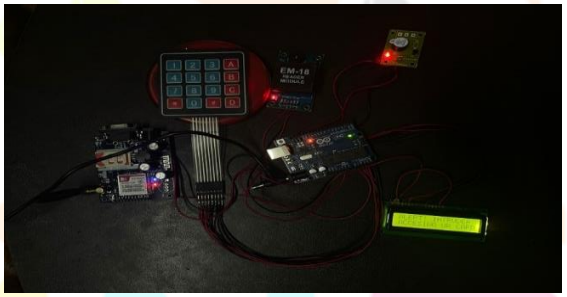
The system's RFID readers are in charge of decoding the information contained on the RFID tags. The RFID readers, which can be either fixed or portable, connect wirelessly with the RFID tags. The antenna on the RFID readers makes it possible for them to communicate with the RFID tags.

In charge of controlling the data transmission between RFID tags and readers is the backend server. The server maintains the information gathered by the RFID readers and grants authorised users access to it. The access control systems, which guarantee that only authorised users may access the RFID system, are likewise managed by the backend server.

The system uses cryptographic techniques like symmetric and asymmetric encryption, digital signatures, and message authentication codes to protect the communication between RFID tags and readers. Asymmetric encryption algorithms like Advanced Encryption Standard (AES) are used to encrypt the data sent between RFID tags and readers. To guarantee data authenticity and integrity, the system also employs digital signatures and message authentication codes.

3. IMPLEMENTATION

Install and set up the backend server software as the first step is to store and handle the data sent between RFID tags and readers, install the backend server software on a server computer. Only authorised users should be able to access the server. Configure the network infrastructure in step two. Connect the network switch or router to the backend server and RFID readers. To enable communication between the RFID readers and the backend server, configure the network settings for both devices.



Installing and setting up the RFID reader software is step three. Install the RFID reader software on the RFID readers, then set up the backend server as the communication destination. Set up the RFID readers so that they symmetrically encrypt data sent between RFID tags and readers using a technique like AES. Program the RFID tags. Each RFID tag should be programmed with a special identification number and any extra data that needs to be kept. Set up the RFID tags so they can communicate wirelessly with the RFID readers and encrypt the data sent between them.

Use an authentication system that is password- and username-based to implement the access control methods. Set up the backend server so that authorised users' login information is stored. Check that the data is safely delivered to the backend server by scanning RFID tags using RFID readers to test the system. To make sure that only authorised users can access the system, test the access control methods.

4. CONCLUSION

In conclusion, implementing an RFID wireless security system can offer a dependable and effective solution for a variety of applications, including access control, asset tracking, and inventory management. The system may include symmetric encryption, access control via a username and password-based authentication system, and other security measures in order to be both safe and user-friendly.

Overall, businesses and organizations can profit significantly from the adoption of an RFID wireless security system utilizing either conventional or IoT-based solutions, which can assist improve their operations, productivity, and security.