IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FRID cryptography and protocol

Research By **Niravkumar K Patel**

University of the Cumberlands

Abstract

The internet of Things can be categorized as one of the technologies of the 21st century. This technology has made it possible for the technology users to achieve a lot by solving the existing challenges while offering opportunities for improving how various things are being done. However, the much-hyped technology has started to get some bad reputations. Most of these negative vices have been brought about by the various security concerns within technology. Fortunately, there are various ways through which the users can improve the security of this technology. One of the techniques that can be applied to secure the internet of things is cryptography. In this research, we are going to discuss cryptography as applied in the internet of things. More specifically, we will seek to explore how RFID authentication schemes of IOT can be secured using elliptic curve cryptography.

Introduction

Business companies today have adopted recent technologies to safeguard their information. The kinds of data that are to be safeguarded within the company are customer related information, personal information, the confidential information of the organization, and employees' files among others. However, to achieve this, the encryption technique based on data should be adopted. Thus, cryptography can be defined as a process of securing information and communication within an organization by use of algorithm codes that make it difficult for the information to be deciphered (Rouse, 2018). The intended person will only get access and read the message.

The internet of things (IoT), on the other hand, is a paradigm shift in the communication environment. Communication is enhanced by the internet and the computing capabilities of the devices. In this case, the Internet of things can basically be described as the physical interconnection of devices. Such devices have the capability of detecting or sensing data collected from the environment. The transfer of the message from one device to another is achieved by the fact that, the devices are linked together. The information transferred in this case has to be secure from unauthorized access. It is noteworthy that the internet of things allows the administrator to authenticate and authorize the access or flow of data within the system.

The Internet of things is the new technology recently adopted since it has the capability of holding large amounts of data, analyzing them, and distributing them to other devices such that they can operate intelligently. It uses radio frequency identification (RFID) since it has the capability of storing sensitive information, wireless communication, and tracking of other devices.

In an ideal world, cryptography would be an essential component of IoT design. There is a rapid growth in the use of the internet of things devices in various industries, and many benefits have been accrued. Typically, the internet of things devices shares a large volume of sensitive information. This information needs to be secured from hackers or any unauthorized access. Cryptography therefore provides an encryption and decryption key for the transferred data. In this case, cryptography plays a significant role in safeguarding information and the internet of things devices. Cryptography encodes the data with a certain key, such that a specific user or device can only decode the data, hence securing the data from unauthorized access.

Cryptography techniques have been used by most companies to store and share their information using electronic methods and internet. This technique is used by businesses to secure their websites, which improves the secure transfer of information within the company (Stallings, 2017). Encryption of the website ensures the safety of shared data through the computer system from the sender to the recipient. Thus, cryptography has been used by the company to enhance secure and convenient communication within the company, since only authorized personnel will have access to the information.

Research Questions

1.To identify the security requirements for radio frequency communication (RFID) on the Internet of Things.

2. To identify and describe RFID system architecture in relation to the Internet of Things.

Architecture System of RFID

The question regarding the system architecture is necessary since it fosters understanding of how RFID works on the IoT in securing and encrypting information. The system has three entities, namely, the RFID tag, the RFID reader, and the server. Each of the entities plays a key role in the authentication of the information (Liu & Qiu, 2015). Succinctly, to authenticate the data between the tag and the server, the secret data is pre-shared after setting up the system. However, the exchange of data on the tag and the reader is wireless. Therefore, the communication channels are not secured and, on the reader and the server, the information is secured due to the presence of the secret key and other security measures.

The security requirements of RFID

This research question serves a significant role in the research report. The IoT uses cryptography to safeguard information. And in this research, the IoT uses RFID to secure information from unauthorized access. Therefore, the question creates an in-depth understanding of the fundamental principles of RFID.

RFID ensures the communication system within the internet of things devices is protected by providing access control measures. It is noteworthy that the shared information between the RFID (tag and reader) is vulnerable to attack, and therefore, the RFID should meet the following requirement for complete control of data:

RFID should have mutual authentication. It means that, the RFID tag and the RFD reader should have mutual authentication before initiating the session. Confidentiality is also essential within the system and to ensure this is achieved, encryption is done before sharing the data (Liu & Qiu, 2015). RFID should also provide information anonymity to prevent data privacy violations. Nevertheless, forward security of the information should be provided to ensure complete control of the shared information within the system.

Data security is an essential component of concern and, therefore, it is necessary to resolve and analyze new techniques involved in securing information. In this case, cryptography and the internet of things are the commonly used techniques for securing data. The IoT makes use of RFID, and therefore, the research questions will give a guide to the basic objectives of the research. As a result, dealing with security concerns within an organization necessitates a thorough understanding of current technology, particularly how the Internet of Things and cryptography interact to ensure data security.

Implementation and Process with Cryptography: Using RFID in Medical Field

The use of Radio Frequency Identification (RFID) in the medical field ensures the safety of the patients, efficiency in caring for patients, providing satisfaction, and tracking purposes. In the provision of security, RFID tags can give the ability to a reduction in issues of misidentification in healthcare (Paaske et al., 2017). Another benefit of using RFID in healthcare is that the RFID sensor devices can withstand high temperatures during sterilization. By using thermal data logging technologies, health centers can have real-time records of assets through use, sterilization, and reuse.

To reach the goals, there is a need to connect to a worldwide RFID system. Since The medical device industry explores IoT opportunities for medical devices and other Medicare assets, the internet is needed to contain a single network for accessing the websites across the globe. When it comes to the RFID system required to grant complete visibility and trace and track potentials from the point at which manufacturing takes place, through to the end at which delivery is done in the health centers, clinics, hospitals, or offices, some considerations should be made. To develop a successful single RFID system, healthcare facilities, hospitals, and manufacturers must implement some technology that works under some uniform and conventional operation standard.

To this day, however, there have been delays in the adoption of the standards needed to reach this goal. As organizations begin executing RFID to meet the regulatory needs and mandates and realize the advantages associated with the implementation, they are faced with synthesizing one of the two available frequencies-High Frequency (HF) or Ultrahigh Frequency (UHF) Generation 2, or both. UHF has become the de facto choice presently for tracking applications. And is well developed across industries globally.

It has been asserted that HF is a better technology for near-field (or item level) applications. Even though the HF technology has been proven to be mature, UHF is also becoming reliable and ensures better performance than HF at the device level. HF is also bound to work in the near-filed. However, UHF still grants an enterprise a single infrastructure and protocol for all applications – from the conveyer belt in the manufacturing centers where there is an item-level application to the dispatch and pallet applications in stocking stores to secure surgical suites in clinics and hospitals. The UHF-RFID protocol grants a conventional platform to enable the global and end-to-end supply chain clarity needed to smoothen transactions and reduce costs. This works better when cryptography is implemented to ensure that the operations are secure, and the data involved retains its integrity, private and crucial information belonging to the health units are safe from theft and misuse, and easy

compliance with HIPAA technical safeguards to ensure total security (Chinnasamy & Deepalakshmi, 2018). F HF

Including and assimilating into the supply chain enhances medical device distribution, performance, and delivery in various areas, including:

1. Sterilization tracking and maintenance of equipment, whereby alerts are automated so that the maintenance needs of the manufacturer can trigger notifications.
2. Billing, whereby the data gathered by RFID sensors is integrated to assist in streamlining the billing transactions.
3. Replenishment, whereby the used assets can be tracked for replenishment to ensure the availability of inventory.
4. Life cycle management, which is a crucial aspect for those with shelf life or who need calibration.
5. Asset tracking, which is done because misplaced or lost inventory can delay the process of patient care. Readily available assets and equipment boost the overall patient experience.
6. Patient tracking, which enhances the care experience and minimizes human error.
7. Inventory management- inventory can only be of use and valuable if it is readily available when needed to be used.

By incorporating RFID and Near-field communication (NFC) technology in medical devices, low-cost technology is involved, which enables all the involved technologies to operate together. According to Tim Dally, a co-founder of one of the globe's first RFID/NFC system platforms and an expert in the industry, the whole essence behind using RFID in the medical field is to make nonintelligent devices intelligent

The use of identity-oriented cryptography in the RFID networks can grant some good protection for the system's privacy and verify both the tags and reader. It can also minimize the requirements of resources on the design and enhance key management (Liang & Rong, 2008). Practitioners should, therefore, get informed and knowledgeable about the RFID system used. Suppose a patient encounters a problem with a device on the system, for instance. In that case, the practitioners should know whether the RFID caused the problem, when the issue occurred, what the patient was up to at that time, and whether the problem was solved after the patient was taken away from that environment (Health, 2019). If the problem is lying with a device, part, or whole of the system, then the necessary rectification should be done by the people charged with the same.

Radio Frequency Identification authentication work on the protocols. RFID contains several algorithms to track the record, connect to the device, identify the person from the scanned barcode in the hospitals. It should reduce the efforts of the doctors and nurses to monitor the patient's medications, Wheelchair, contact details, schedule doctor visits.

RFID authentication schemes working on the ECC-based RFID authentications scheme. There is a tag to scan the bar code and authenticate to the person identifications. The RFID device reads the label from the barcode and transmits it to the database thru the radio frequency. The device has algorithm chips to transfer the data to the database. There is high security on the level of the algorithm to steal the data from the data and receivers. The data is fully encrypted for each patient and stored in a database. For security purposes, the algorithm is designed in the high computational formula to make a secure system. It has a hash function. Several operations are involved in this design, such as tag cost, gate area, power consumptions, and small operations to make a better scheme. As explained earlier, RFID authentication schemes have been proposed for different applications recently. Few plans use only curve operations; other methods involve in cryptography operations illustrate hash function. It has private and public key pair of the server where Y=yp, secret information of the tag where Xi=XiP, I=1,2 and secure hash function mapping [0,1] to Zn.

The use of public-key infrastructure is assumed in the scheme; In the initialization phase, the server generates system params={F (q),E (F(q)), n, P, Y} and stores [m, X1] and [X1,Y] database. It has a separate database and tag memory to store.

Server to the Tag: The server is used for private critical y to compute a signature of the random number generated by the reader and send the message to the tag.

Tag to server: Tag receives the message from the server, and it's used the server public to check validations of the title. If it's not valid, then the tag terminates the session. Otherwise, the tag generated the rando number and computed the formula and signature. The title sends a message to the reader.

Server: when the server receives the message, it uses the private key to compute and looks on the tag public key according to m. If there is no tuple in the database, the server terminates the session, or the server uses X1 to check the validity of the signature. If it's not valid, the server rejects the session, or the tag is authenticated. These operations are a bit complex to verify the algorithms, multiplications, hardware needed with curve point operations. The title sends identify ID to the server. The server checks the identity of the tag.

I am explaining the performance and security of the ECC-based RFID authentications schemes, evaluating the security requirements, and comparing the communications and computing cost. We could determine whether an ECC-based RFAID authentication is well for the application in life. The tag computing capability and memory are minimal. Therefore, the computation cost, communications cost, and storage requirements are critical factors. RSA algorithms with 1024 bits key size, and it's used in many implementations. We also used such a curve to discuss the different schemes' computation cost, communications, and security requirements.

RFID authentication is used everywhere in the healthcare environment. Security of the requirements authentication scheme should satisfy. Its communication costs are associated with ECC-based RFID schemes. In the recent cryptography trade, the cryptography scheme is provable secure using a secure model. RFID systems are safe from various malicious attacks. To ensure secure communication in RFID systems. This protocol is divided into periods. In the beginning, the user tries to use the protected device, a temporary secret key used to decrypt the message sent in the time durations. The secure algorithms are managed in plain text and cipher text mechanisms to handle the security and vulnerability of the applications. The algorithm is working on the notation based to make the logical calculations and transmit the data to the server. It will try to calculate the logical operations, and as per the formula, the data comes from the database with secure authentications. This algorithm has been tested in many ways as per the security of the vulnerability to use at the application level. It's tight coupled algorithms. Many healthcare organizations are using this technology to maintain their inventory in the hospitals.

Challenges

Remote RFID sensors (both advanced and straightforward) have not yet become unavoidable in the home and individual gadgets market, with the benefits of RFID for following and overseeing regular articles promptly evident. A few principle hindrances forestall RFID detecting from becoming unavoidable. This audit distinguishes six principle challenges. Shows an outline of the fundamental difficulties of RFID, which are arranged by the RFID part or parts (peruser, aloof sensor, correspondence convention) which they influence.

- Limited energy reaper and read range: These are viewed as two of the most fundamental constraints because both sensor hubs and RFID labels are made of scant assets. Existing RFID stages executed in the IoT are essentially uninvolved. That is, they can't work or detect information without being set inside the peruser's understanding zone. The coordinated circuit (IC), the microcontroller unit, and the detecting module on an aloof tag is fueled by collecting the RF energy sent by the peruser and conveying by backscattering the occurrence signal. This execution diminishes the assembling cost by keeping IC costs low. Be that as it may, the force accessible at the label will restrict long-reach correspondence and force-hungry detecting capacities.

Moreover, the most significant force sent by the peruser is obliged by the Federal Communications Commission (FCC) (or comparable local association) at 1 W (30 dBm), expecting a receiving wire with a most extreme addition of 6 dBi. A small amount of this sent RF power is gotten at the IC after misfortunes and polarization befuddles.

Albeit every one of the parts is commonly intended to be power adequate, the sensors' rationale is more perplexing and tedious. In this manner, it is a test to control every one of the parts and cover the tasks of the explanation with just reaped RF energy. This test is more striking when the sensors are embedded in the materials under test because the encompassing materials lessen the RF signal. The got RF energy can scarcely control every one of the activities, which genuinely influences the read/to compose scope of the RFID sensor.

- Sensor reactions crash: A RFID detecting application is made out of around one peruser and a few RFID sensors, including one sensor. The label crash issue secures the center while investigating these labels. The correspondence channel is divided between them, and, like this, their reactions should be mediated to keep away from synchronous responses that will prompt crashes. This issue is one of the primary sources of fuel wastage, recognizable proof time increments, and the read rate diminishes. Because of the expanding number of sensor labels in a joint peruser cross examination region, this issue is the subject of expanding concern. The productive enemy of crash conventions for streaming sensor information is expected to limit the effect of impacts.

- Lack of adaptability: Current sensor RFID labels, for the most part, accompany a solitary sensor or, sometimes, with different inherent sensors. Yet, they can't be supplanted or reconfigured whenever they are produced without an exorbitant upgrade and multiplication. Since the IoT is an open, dynamic, and adaptable worldwide systems administration and detecting framework, the over-simplification, measured

quality, and reconfigurability of the detecting hubs/stage are fundamental for their reception later on IoT engineering. Moreover, business RFID perusers are, for the most part, discovery frameworks that just permit restricted arrangement and are just fit for executing the current UHF RFID correspondence standard named EPCglobal Class 1 Generation 2 (EPC C1G2) (ISO/IEC 18000-63). Subsequently, it is difficult to execute new correspondence conventions past the EPC C1G2 that satisfy the needs of novel and arising RFID-based sensors. Albeit a few distributions in writing propose an adaptable RFID peruser dependent on a product characterized radio, there is a great deal of opportunity to get better in such a manner

One more constraint is identified with the current absence of a UHF RFID versatile detecting stage. Presently, convenient business RFID perusers shouldn't be connected to work. Yet, there is an absence of a cellphone-based location that empowers the utilization of unmodified cell phones to peruse information from UHF RFID sensors. It would be gainful and down-to-earth to peruse RFID sensor labels utilizing a commonplace cell phone with some extra equipment parts (like a UHF radio wire).

- Cost: The expense of business RFID perusers is generally high contrasted with sensors and labels.

Conclusion

RFID verification is one of the most basic security administrations for IoT executions in the medical services climate. We have introduced a top-to-the-bottom study of proposed ECC-based RFID verification plans as of late. We distinguished a portion of the security necessities that an RFID validation the Framework to fulfil. We have examined the calculation and correspondence costs related to past proposed ECC-based RFID plans, which meet a few or all

References

Liu, C., & Qiu, J. (2015). Study on a secure wireless data communication in internet of things applications. International Journal of Computer Science and Network Security (IJCSNS), 15(2), 18.

Rouse, M. (2018). Identity and Access Management; Cryptography. Techtarget Network. Retrieved from: https://searchsecurity.techtarget.com/definition/cryptography

Stallings, W. (2017). Cryptography and network security: principles and practice (p. 743). Upper Saddle River, NJ: Pearson.

D. He, N. Kumar and N. Chilamkurti, et al., Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol, Journal of Medical Systems, 38 (2014)116.

M. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography,"J. Supercomput., 2014, DOI: 10.1007/s11227-014-1272–0.