The Lightweight Algorithm for Secure RFID Authentication System

V Haribaabu1, Jospeh James2, SelvakumaraSamy3, Nilesh Singh4, Aparna Upadhyay5

1,2,3,4,5. Assistant professor Department of Software Engineering, SRM - IST.
e-mail: v.haribaabu@gmail.com

Abstract. In the milieu of IOT, the entities in our habitual ex-istence have turned to be a component of the Inter-net due to their excelling communication and com-puting competencies that let them to correspond with another object. Progression in ICT i.e. Infor-mation and communication technologies, has es-corted to the surfacing of IoT. The application of IoT technologies fetches expediency to doctors and patients in Healthcare environment as they can be concerned to numerous fields of medicine. Radio-frequency Identification Devices (RFID) is the ma-jorly famous wireless communication technologies applied in the field of IoT as they could amass in-sightful data, used for wireless communication with another object, and locate and follow specific enti-ties without human interventions. In order to pro-vide enhanced security and performance to RFID authentication scheme Elliptic Curve Cryptography is being applied. An RFID has 3 entities: RFID tag, reader and server. Since the channel of communica-tion amid the RFID tag and RFID reader is unsafe since the data exchange takes place wirelessly and adversary could snare the data easily. Thus to pro-tect RFID tag data we are using data perturbation which is a form of privacy safeguarding data mining for electronic health information’s. Inside this paper, we confer the requirements of security for RFID authentication schemes with a comparative study on RSA, and in precise, we put forward an appraisal of ECC-based RFID authentication methods on the basis of security and performance.

Keywords: Internet of Things (IoT), Authentication, Elliptic curves cryptography (ECC), Healthcare environment, wireless communication, sensitive data Performance, Radio-frequency identification (RFID), Security.

1. Introduction

As IOT field Evolved Everything will be in category of smart: Smart-Phone, Smart-Refrigerator, Smart-city, Smart-car, Smart-home and Smart-Bulbs. This change is made by the technology of IoT. It has got a greater ability to gather data, store and analyze the congregated information

The levitate in expectancy of life and the resulting progressive population aging, along with a pervasiveness of unceasing diseases, trigger a vigilant considering on the role and ways that provide care to people so as to make sure an upright quality of life. The remote supervision and support has become tools that strategize to implement policies for the society over the long-standing.
The IoT could be a transformer for the healthcare industry. It is altering the medical and industry of healthcare by enhancing efficiency, running down costs and putting the aim posterior over better care of patients.

Inside the arena of Healthcare, IoT proposes different types of engross sensors that are abrasive, embedded, and environmental, and would enable senior citizens to get benefit from medical care any time and at any place. They not just cause ease for medical employees but they too increase senior citizen’s life eminency.

Radio Frequency Identification Devices (RFID) is method in WSN i.e. Wireless Communication Network technology which is used for precisely spotting specific entities.

Radio-frequency identification technology utilizes the waves for radio-frequency to relocate authenticating data among entities which are tagged and the readers without LOS, which offers an automatic identification system.

There are three components that comprise in an RFID system:

RFID Tags: It consists of an integrated circuit and a small antenna, which is put in every entity that can be recognized. Each and every tag would send its ID under request.

RFID Reader: It interacts to a centralized database and the tags. They are accountable for acting upon the tags’ queries.

Database: Provided the data and records of the tagged entities. Readers would analyze the database to track and locate a specific entity that obtains information associated with it.

RFID technology was initially implemented in the aircraft system for Identify Friend or Foe (IFF) during World War II. Contrasted to the conventional barcode, RFID can be used for objects with rough surfaces and can also give both read and write competencies, requires no LOS i.e. Line of Sight connection with RFID readers, and can identify various RFID tags at the same time. All these advantages make RFID an improved technology in comparison to the customary barcode system. As in the environment of healthcare, RFID system is applied in IoT and general applications including location tracking of medical instruments patient identification, medical treatment tracking and verification, procedure management, location of patient and at a healthcare center and process of surgical management.
2. Classification of RFID Authentication Scheme

RFID authentication is used for various applications. As per different cryptographic methods used in various methods,

- Scheme of RFID can be categorised into two types
  1) NPKC i.e. Non Public-key Crypto-system based schemes
  2) PKC i.e. Public-key crypto-system based schemes

The NPKC based RFID authentication scheme does not have complicated functions to improve better performance. In such methods basic logic gate operations, symmetric encryption technique, cyclic redundancy codes techniques are used. As stated type or schemes have been implemented for general practical applications like inventory management, verification, road traffic management etc where level of secure data is very less.

Public key cryptography based methods are essential where security of data is important concern. As such attributes can never be implemented by Non Public-key cryptosystem based scheme. Development in micro electric technology many complex algorithms have been put into operation on RFID chips.

In many methods ECC authentication system can be better suited for the system as it provides same security but using shorter key size and low computational requirement so it limit the computing power.

In Public Key algorithms it uses a mechanism in which there are participants are very large to share keys in information system. When analyzed with respect to RSA algorithm or other algorithm, ECC which uses shorter key length. To authorize and authenticate a RFID is the most necessary steps to establish a communication which is highly secure to RFID system. We are using multiple authentication schemes for this purpose, As RFID tags and readers are vulnerable to various kinds of security threats.

3. Related Works

The research work had carried out in Elliptic Curve Cryptography and IOT was started in 2005 by Wolkerstorfer [6]. Wolkerstorfer gave the idea of RFID authentication scheme which was based on ECC, in 2005. But, he failed in proposing any precise authentication scheme. Tuyls and Batina [2] gave acceptance to the Schnorr’s identification protocol [3] and came up with the first RFID authentication scheme based on ECC, in 2006. Later, Batina et al. [3] applied Okamoto’s identification protocol [4] and adopted another RFID authentication scheme based on ECC, in 2007.

Conversely, Lee et al. [5] indicated that both Tuyls and Batina’s scheme [3] and Batina et al.’s scheme [3] failed in providing anonymity. Thus, for improving security and ensuring anonymity, Lee et al. [5] came up with an unarguably RFID authentication scheme based on ECC.
Nevertheless, Bringer et al. [7] showed that Lee et al.’s scheme lack endurance to tracking attack and the tag impersonation attack. Thus, for endurance to above said two attacks, Bringer et al. [7] came up with a new authentication scheme for RFID called randomized Schnorr scheme.

Later, Lee et al. [7] also put forward an ECC-based RFID authentication method to cope up with the tracking attack and the tag impersonation attack against their previous schemes [8]. But he did not succeed in developing an authentication protocol. Many research were conducted on later period for achieving all the essential security features into their work. Attacks like Man in the middle, tag cloning, tag spoofing hinders the way in standardizing an authentication protocols. In scheme of authentication for IoT and cloud servers’ security, they have put forward that the schema mainly depends on algorithms based on Elliptic Curve Cryptography (ECC) that lets more security for Public Key Cryptography (PKC) algorithms due to its smaller size of key.

Problem Statement
In domain of IoT, the data were collected from various things in the network is highly sensitive. Data collected in medical field were the personal and medical details of a patient. Digitized healthcare records have turned out to be very valuable to people with criminal records. Privacy of patient and user data is highly required. The patient should be in a state of control of what is being checked by whom and the platform will allow him to view and maintaining anonymity and masking of data wherever possible.

So data should be in encrypted form. Also the IoT consist of many cheap sensors and RFID tags with low computational power, therefore the technique of encryption should be light weight and also provide higher level of security.

The RFID tags are much admired due to easiness to use. RFID will be resilient for attack, cloning attack is very easy attack in RFID Tag. It is easy job for to retrieve data which is stored in a RFID Card’s memory.

4. Elliptical Curve Cryptography

Cryptography is an electronic technique that is used to preserve important data over transmission. Mainly cryptography is science to provide security to information. To preserve our records by using multiple authentication methods is the main objective of cryptography. When authentication of data is main consider that should be less cost than the value of original information.

Two major terms that we used for the cryptography technique are Encryption and Decryption.

Encryption technique is used to send confidential data over communication. The process of encryption require two things (1) an encryption algorithm and (2) key. Encryption is done at the side of sender. An encrypted algorithm can be applied to make data undetectable by all multiple authorized receivers.

\[
\text{Cipher text} = \text{Encrypt (plaintext, key)} \\
\text{Plaintext} = \text{Decrypt (cipher text, key)}
\]

The process of Decryption is to convert the cipher text to its original data. Decryption technique need separate Decryption algorithm and a key.

Elliptical curve cryptography (ECC) is a public key encryption scheme based cryptosystem as like RSA (Rivest-Shamir-Adleman) though different from RSA because of its faster capacity to evolve, providing lucrative and different way for the researchers to create algorithm for cryptography according to their requirement that means how much security they want to provide to the system.

ECC is Public Key Cryptography a encryption method which is based on elliptic curve theory which can be used to improve faster in speed, smaller in size, and more efficient Cryptographic keys to provide authentication scheme to RFID system.

In previous finding it shows that the security level stated by RSA algorithm, which uses same as in ECC that can be generated using smaller key size. Researches depict that by using RSA algorithm that same security level can be achieved using 1024 bits key size but when ECC algorithm requires 160 bits key size.

ECC scheme can be used on small and compact size of RFID tags. So ECC authentication scheme is well suits with communications which are wireless such as mobile phones and smart cards. ECC
point of multiplication operation appears to be more efficient computationally than RSA using fast and effective computational time.

Active-Attack: An intruder will try to get access by attacking the vulnerabilities of the system to directly send data used in the past operations or manipulated messages with a slight change in the original message.

Passive-Attack: The intruder can exchange and develop information about the communication in passive attacks. The goal is to prevent the attacks since their uncovering is complicated. The attacker can send manipulated data and delete messages in case of active attacks.

5. System Architecture & Requirements For Security Of An Rfid Authentication System

A. System Architecture

In Fig. 1 the fundamental architecture of the scheme for authentication of RFID systems include three basic elements: the RFID reader and tag, and a server. The tag and the server authentication mechanism is achieved by passing some furtive data among them after setting up the system. The channel of communication amongst the tag and the reader is unsecure since the data is exchanged wirelessly and data interception by an intruder could be easy. The channel of communication between the reader and the server is protected because of establishment of a channel of security amid using a pre shared key which is secret and a mechanism for security.

Tag for RFID: It comprises of a microchip, an antenna, and a dedicated hardware for cryptographic processes. The tag interacts with the RFID reader and preserves confidential information for authentication. Generally, the computing capacity and memory storage for a RFID tag is limited.

Reader for RFID: A reader comprises of a control and memory unit along with a radio transmitter and a receiver. RFID reader allows interchange of data or message amid the RFID tag and server with achieving mutual authentication. Generally, computational capacity of a RFID reader is higher in comparison to that of the tag.

Server for RFID: In order to get an aim of inter mutual authentication, it preserves all the identification data records of RFID tag’s in its database when the system is built. By using the preserved data identification information, the server can deduce tag’s validity. Generally, the computing capability and memory capacity of the server is high.

6. Security Requirements

RFID security requirements are satisfied when they fulfill following requirements to make effective authentication scheme.

1) Mutual authentication: the Tag and reader need to be linked to each other before starting any session. In system we suppose that the passage of data message through the communication channel between server and tag is secured only mutual authentication is required.

2) Confidentiality: It is very important to provide security to secret data /record information such as identity, user id, passwords financial transaction at different times when communicated using the communication channel. The information can be hacked during transmission so it must be encrypted before transmission.

3) Anonyms Behavior: In this RFID authentication scheme it must give enhanced anonymity which shows it can track and trace the owner’s activity, its location and privacy if the identity of the tag is known, thus the tag should be encrypted.

4) Availability: When the information is executed the Authentication mechanism must give an update to the secret data stored. The authentication methods for RFID can be implemented during the life cycle period of Tag. If it fails to synchronization of any update, then authentication mechanism will become vague.

5) Forward security: It is very compulsory to provide forward security to authentication scheme. As provided in various authentications scheme we can locate the past location of the tag. It can be very problematic for owner’s privacy and security.
6) Scalability: To give proper authentication to RFID Tag the system has to get the records from the data base. If the computational work on algorithm increases the number of tags increases so no longer the system will remain scalable.

7) Attack resistance: To provide guaranteed authentication this scheme should be secured against various attacks as man in the middle attack, reply attack, modification attack, server spoofing attack etc.

7. Comparative Study Between RSA And ECC

Since the inception of elliptic curve cryptography (ECC) it has acquired wide acceptance because of its smaller key size and higher security. Cryptography generally is mathematically very thorough, and in order to let resource restrained devices such as embedded systems so as to encrypt information which gets send across the network, the type of cryptography that can apply, and to optimize the algorithms applied to constrain the power consumption and computing cycles required.

The asymmetric primitives require a broad analysis of implementation aspects till it show up their ultimate competency, is shown by emergence of RSA and then ECC. One of the features that has been beyond the scope of scientific researches on numerous of these alternative primitives is the efficiency with respect to implementation on embedded systems. It is not only desirable to have alternatives ready for the case RSA and ECC which might get broken. As few of the different schemes can be more efficient than working schemes, possibly possessing better implementation properties than existing ones. The alternative public key crypto- systems can sway the cost, performance, and security of future embedded security applications.

A. Elliptic Curve Cryptography

A finite field is basically a field where the set has a fixed number of components. For instance, the set of integers could not be taken as the prime for a finite field since there are an infinite number of them. Nevertheless, the set of integers from 0 to 100 could figure the basis of a finite field. So now we can structure an Elliptic Curve.

Generally, an Elliptic Curve is of the form: $y^2 = x^3 + mx + n$, where $x, y, m$ and $n$ is components of some Field. In Elliptic Curve Cryptography, we abstain such that $x, y, m$ and $n$ are components of a finite field.

A group over elliptic curves can be defined specifically as:

- the group’s components are the points of an elliptic curve;
- an identity component is the point at infinity $0$;
- inverse of a point $J$ is the one symmetric about the x-axis;
- addition is given by the rule: given where three aligned, non-zero points $J$, $K$ and $L$, their sum is $J+K+L=0$

We can write $J+K+L=0$ as $J+K=−L$. This equation, to derive lets deduce a geometric process to calculate the addition between points $J$ and $K$

When a line is drawn crossing both $J$ and $K$, the line intersects a third point on the curve, $L$ proving that $J$, $K$ and $L$ are aligned. On taking the inverse of $L$, the result is $J+K$. 


Advantages and Disadvantages of ECC algorithm

ECC has evolved as a main challenger to RSA.

Some advantages of ECC are:
- Increase in speed.
- Lesser requirement of memory.
- Small key size

Some disadvantages of ECC:
- Much less explored and known about.

On execution of ECC algorithm in Cooja simulator which is a network based simulator particularly designed for Wireless Sensor Networks, the Network graph generated showed rate of algorithm execution.

The sensor map generated showed the signal processing between two devices.
A. RSA

The algorithm is applicable on two of the large prime numbers which are large enough in terms of mathematics and calculations, and whose factorization of products seems difficult than finding those numbers.

**Algorithm:**
1. Taking a and b as two prime numbers.
2. Exercise \( x = a \times b \). \( x \) which is called the modulus of both public and private keys.
3. Compute, \( \varphi(x) = (a - 1)(b - 1) = x - (a + b - 1) \), where \( \varphi \) is Euler's quotient function and its value is kept secret.
4. Select an integer \( y, 1 < y < \varphi(x) \) and \( \gcd(y, \varphi(x)) = 1 \). \( y \) and \( \varphi(x) \) are co-prime. \( y \) is called the public key exponent.
5. Calculate, \( w \equiv y^{-1} \mod \varphi(x) \). \( w \) is the private key exponent.

Some pros of RSA:
- The major advantage can be seen as increase in the security.
- The application of Digital Signature makes it secure from repudiation.
- Secret Key Cryptography can be used.

Some cons of RSA:
- The major problem is that the encryption process speed is slow.

On execution of RSA algorithm in Cooja simulator, the Network graph generated showed rate of algorithm.

The sensor map generated showed the signal processing between two devices.
8. Performance Analysis

The performance of both the algorithms was analyzed using Contiki, an open source, lightweight, highly portable and multitasking operating system which is used for embedded systems that are very much efficient in memory. Contiki has a memory usage of about 2KB of RAM and 40KB of ROM. Contiki is currently used in many microcontrollers like MSP430, AVR, HC 12 and Z80 and is developed in C. Contiki is the best operating system for sensor networks to implement asymmetric cryptography since it combines multi-threading and event driven kernel.

Performance of RSA and ECC is assessed considering the following parameters:
1. Bits as the key size unit.
2. Signature generation and verification time.

In ECC, the basic function is point multiplication, that is assumed to be quite expensive. Few efficient scalar multiplication algorithm over comes this. At the same time, RSA already has identified sub-exponential attack. Therefore the required bits for RSA generated key pair are supposed to increase much faster than that for ECC generated one. Also, for a same level of security, the ECC involve smaller numbers as compared to RSA.

Using the tool the execution duration for both the algorithms was estimated.
9. **Result Analysis**

Through the given comparison tables it can be found that the RSA has around 10 time’s computational overheads than ECC and the key pairs and system’s parameters are shorter for ECC. ECC presents substantial bandwidth saving over RSA as for same altitude of security; RSA requires much larger size of key. ECC has rapid key generation than RSA. Encryption is rapid in ECC but decryption is slower than RSA. The findings presented by us shows that ECC key generation is significantly faster than RSA key generation for RSA key of sizes 1024 bits and greater.

The node performance for both the algorithms was recorded using the Cooja Simulator in Contiki OS. The performance efficiency for the ECC algorithm was recorded higher which showed it to be a better alternative over RSA.

Keeping in mind that RSA keys smaller than 1024 bits can be broken by many affordable devices which can be very easy. The disparity in key sizes rises exponentially to keep up the same relative power as contrasted to the average computing power available. In fact, the rise in demand for ECC algorithm has been acknowledged by the RSA security in its website. So we can say ECC will be more competent in terms of security.

| ECC KEY SIZE (bits) | RSA KEY SIZE (bits) | KEY SIZE RATIO (bits) |
|--------------------|---------------------|-----------------------|
| 163                | 1024                | 1/6                   |
| 256                | 3072                | 1/12                  |
| 384                | 7680                | 1/20                  |
| 512                | 15360               | 1/30                  |
10. Conclusion

In IoT implementations for healthcare environment, RFID based authentication comes up to be one of the significantly crucial security services. In this paper, we aimed at putting forward an in-depth review of currently proposed RFID authentication schemes based on ECC.

The study of the costs deployed for computation and communication related to already proposed RFID schemes based on ECC has been carried out, which convene some or all of these requirements. Recently, three RFID authentication schemes are put forward which are based on ECC and are able to fulfill all the requirements for security. These proposed authentication schemes are customary for use in applications of IoT when applied in Healthcare based systems.

The latest advancements in contemporary cryptography has lead to the familiarity to schemes of cryptography which are insightfully secure when applied a model of security. Most of these schemes still appear to be prone to various attacks that can be harmful. A protected communication can be guaranteed by the use of techniques which are based on ECC algorithm in an RFID environment.
through the vital construction of a desirable security model for RFID schemes based on ECC firstly. After that, we have to design RFID authentication schemes based on ECC that secures communication.

References

[1] Debiao He and Sherali Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, FEBRUARY 2015

[2] Behzad Malek, Ali Miri, Luis Orozco-Barbosa, “Backward Link Authentication For RFID Tags,” 2011 IEEE International Conference on RFID Technologies and Applications

[3] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[4] D. Ranasinghe, Q. Sheng, and S. Zeadally, Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks. New York, NY, USA: Springer, 2010.

[5] Qamar Toheed, Hassan Razi, “Asymmetric-Key Cryptography for Contiki,” Chalmers University of Technology, Gothenburg Department of Computer Science and Engineering, Göteborg, Sweden, July 2010

[6] Himja Agrawal, Prof. P. R. Badadapure, “Authentication Scheme for Secured RFID”, IJSTE - International Journal of Science Technology & Engineering Volume 2, Issue 10, April 2016

[7] Tarun Kumar Goyal, Vineet Sahula, “Lightweight Security Algorithm for Low Power IoT Devices”, 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India

[8] Jisha S, Mintu Philip, “RFID Based Security Platform For Internet Of Things In Health Care Environment”, 2016 Online International Conference on Green Engineering and Technologies (IC-GET)

[9] Effy Raja Naru, Dr. Hemraj Saini, Mukesh Sharma, “A Recent Review on Lightweight Cryptography in IoT”, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC 2017)

[10] J. Chou, “An efficient mutual authentication RFID scheme based on elliptic curve cryptography,” J. Supercomput., vol. 70, no. 1, pp. 75–94, 2014.

[11] S. Balasubramaniam and V. Kavitha, “Geometric Data Perturbation-Based Personal Health Record Transactions in Cloud Computing” The Scientific World Journal Volume 2015 (2015), Article ID 927867

[12] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, “RFID technology for IoT-based personal healthcare in smart spaces,” IEEE Internet Things J., vol. 1, no. 2, pp. 144–152, Apr. 2014.

[13] Chatterjee, A. K. Das, and J. K. Sing, “An enhanced access control scheme in wireless sensor networks,” Ad Hoc Sens. Wireless Netw., vol. 21, no. 1–2, pp. 121–149, 2014.