An RFID Mutual Authentication Protocol using ECIES

Nidhi Soni¹, Samidha Dwivedi Sharma²

Abstract--Security of data is a major issue in RFID environment as RFID is a wireless Radio frequency devices used in the wireless network. The data reads by the tag is send to reader which is then stored at the server, but security is an important concern during the transmission of data from tag to reader. Although there are various security and authentication techniques implemented for the security of data and for the authentication of tag and reader. Here in this paper an efficient ECIES based authentication is implemented for the security of data from tag to reader.

I. INTRODUCTION

Radio Frequency Identification (RFID) system is the latest technology used for object identification in various applications in access control, manufacturing automation, maintenance, supply chain management, parking garage management, automatic payment, tracking, and inventory control. RFID offer several advantages over barcodes like in RFID system data are read automatically, it does not required the line of sight. The reader can read the contents of the tags by broadcasting RF data via antennas. The readers receive the tag’s data and then passed to a host computer, which uses middleware (API) for further uses.

1.1 Basic Working Principles

RFID system is totally a wireless network. The data is transmitted through radio waves. RFID tag: is a small radio chip that comprises a simple silicon microchip attached to a flat aerial and mounted on a substrate. The tag can be attached to an object like item, box, or pallet, and this tag is remotely read by the reader device which ascertains the tag’s identity, position, or state. The Reader device sends and receives RF data to and from the tag via antennas. Figure 1 shows the basic working of RFID devices in RFID working environment.

RFID readers and RFID tags operate in an inherently unstable and potentially noisy environment in the wireless network so the RFID tags may suffer from security and privacy risk. Unprotected tags may have vulnerabilities to eavesdropping, location privacy, spoofing, or denial of service (DoS) and also the unauthorized readers may access the tags. If the tags are protected, then also the tag may be tracked through predictable tag responses.

1.2 ECIES

ECIES (Elliptic curve integrated encryption system) is a technique which is a combination of Asymmetric key generation technique i.e. ECC (Elliptic curve cryptography) and encryption technique i.e. X-OR based encryption.

ECC

ECC (Elliptic curve cryptography) generates the public private key pairs on the basis of ECC standards. The mathematical operations of ECC is defined over the elliptic curve y² = x³ + ax + b, where 4a³ + 27b² ≠ 0. Each value of, a” and „b” gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve [17]. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve.

Domain parameters – These are such constants which sheared among all the devices i.e G generator point, n Order of elliptic curve, „a” and „b” curve parameters and few more. One main advantage of ECC is its small key size.

1.3 Asymmetric key cryptography

In public/ Asymmetric key cryptography each device/user have a pair of keys, a public key and a private key, Only the particular user knows the private key whereas the public key is distributed to all other users.

II. RELATED WORK

In 2011 Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu in [1] proposes the mutual authentication protocol based on the challenge response model. The Advanced Encryption Standard (AES) is used as a cryptographic primitive to secure the data it is a mutual authentication protocol which utilizes AES-128 as a primitive to encrypt the messages transmitted on the channel.
International Journal of Emerging Technology and Advanced Engineering

With that cipher block, the protocol can protect against many types of attacks such as information leakage, tag tracking etc.

In 2011 by Liangmin Wang, Xiaoluoy Yi, Chao LV, Yuanbo GuOn proposed the protocol which uses CRC and PRNG operations supported by Gen-2 that require very low communication and computation loads. It uses the concept of BAN logic and AVISTA for security of RFID protocol. BAN logic is gives the proof of protocol correctness, and AVISTA gives the authentication and secrecy properties. [2]

In 2010 Mike Burmester Jorge Munilla proposed a lightweight RFID authentication protocol; it supports forward and backward security. It uses is a pseudorandom (PRNG) which used in backend Server. Authentication is achieved by exchanging number generator a few numbers (3 or 5) drawn from the PRNG. The protocol can prevent online man-in-the-middle relay attacks [3].

In 2012 Tian-Fu Lee, Hsin-Chang Chen, Pei-Wen Sun introduced an efficient and secure RFID authentication protocol based on quadratic residues for multiple services. This protocol can solves the problems of user privacy and intractability and keeps an invariable response time in the backend server and also supports low computational cost in Tags.[4]

In 2009 Bongno Yoon, Man Young Sung, and Sujin Yeon, 2 Hyun S. Oh suggested the enhanced version of HB-MP and HB-MP+ protocol, called HB-MP++. It uses Ultra low-weight and concrete function to remove vulnerability of the conventional methods. HB-MP++, provides a powerful method against passive and active attacks. [5]

In 2011 Ramzi Bassil Wissam El-Beaino Ayman Kayssi Ali Chehab proposed a protocol which uses Physically Unclonable Functions (PUFs) to achieve mutual authentication for ultra lightweight tags is. The proposed approach provides robust security properties as well as good performance. The technique uses light operations and a PUF circuit that only requires minimal logic and storage circuitry. [6]

In 2012 Jeremy Gummeson, Pengyu Zhang, Deepak Ganesan proposed RFID-scale sensors for distributed sensing. RFID-scale uses harvested energy. It sense and store data when not in contact with a reader. It use backscatter communication to upload data when a reader is in range. [8]

In 2011 Imran Erguler and Emin Anarim introduced RFID deligation protocol which provides a centralized back-e end server to delegate the right to identify and authenticate a tag to specified readers, they also discover a subtle flaw by which a delegated entity can still keep its delegation rights after the expire of them. It improves the SMD protocol. [9]

In 2012 Kai Bu, Xuan Liu, Bin Xiao [10] suggested a Fast Cloned-Tag Identification Protocols for Large-Scale RFID Systems. It proposes broadcast and collisions techniques to identify cloned tags. This approach reduces the efforts from complex cryptography techniques and transmission of tag IDs which consumes much time.

In Paolo D’Arco and Alfredo De Santis proposed a protocol SASI, It is a RFID authentication protocol, it provides Strong Authentication and Strong Integrity. It is an Ultralightweight RFID authentication protocol. It is suitable for passive Tags and uses limited computational power, limited storage and involves simple bitwise operations such as and, or, exclusive or, modular addition, and cyclic shift operations. [12]

In 2012 Ye Li and Fumio Teraoka [13] proposed mutual authentication protocol which is based on hash-function based for low-cost RFID-tags. It needs very limited calculation resources. The protocol prevents eavesdropping tag’s ID by randomly-picked nicknames which shared between the RFID-tag and the back-end systems are transmitted in the air. This protocol consumes less time than Gossamer protocol for mutual authentication.

In 2012 Florian Kerschaubam and Leonardo Weiss Ferreira Chaves presented an encryption scheme for enforcing access control in a Discovery Service allows the data owner to enforce access control on an item-level by managing the corresponding keys. Data remains confidential even against the provider of the Discovery Service. We present three ways of querying data and evaluate them with databases containing up to 50 million tuples. [14]

In 2012 A. Anny Leema1, Dr. Hemalatha. M [15] proposed a technique to improve the quality of data. This approach is a hybrid approach of middleware and deferred because it is not always possible to remove all anomalies and redundancies in middleware. It performs the cleaning in an effective manner.

In 2012 Kaoutar Elhifiouati, Erik-Oliver Blass, Refik Molva introduces a new protocol CHECKER, which used for counterfeit detection in RFID-based supply chains through on-site checking.

---

![Diagram](image.png)

In 2012 Matthew Butler, Peter J. Hawrylak and John Hale proposed Dynamic Risk Assessment Access Control (DRAAC) protocol for intrusion detection, it reduces access privileges in RFID access control system. by using This method enables one to secure the most sensitive areas of a facility while minimizing the extent to which legitimate users are restricted. [7]
By the help of this protocol RFID readers check the validity of the product’s path and after it verifies the product genuineness, CHECKER uses a polynomial based encoding to represent paths in the supply chain. Each tag T in CHECKER stores an IND-CCA encryption of T’s identifier ID and a signature of ID using the polynomial encoding of T’s path as secret key. [16]

III. PROPOSED METHODOLOGY

Assumption

IDR- Reader’s Identity
ID- Tag’s Identity
s- Tag’s seed value
E-Encryption function(x-or based)
D-Decryption function(x-or based)
Ks-Reader’s/Server’s private key
Kp- Reader’s/Server’s public key
Ks1-Tag’s private key
Kp1-Tag’s public key

Query phase: Initially, the server generates Ekp(s⊕IDR) (by using its kp public key) and sends to the reader. The reader will decrypt this value Dks(s⊕IDR) (by using Server’s Private key ks) and obtain the seed s by performing s=IDR⊕(IDR⊕s). Afterward, reader encrypts the seed Ekp1(s) (by using Tag’s Public key) and forward to the queried tag.

Tag to Reader Authentication: On receiving EKp1(s), then the tag performs it’s on board x-or encryption on its stored seed value Ekp1(s)(by using its public key) then the tag match the received encrypted seed value to its own encrypted seed value if they get match then reader get authenticate and if not, the tag keeps quiet. If reader get authenticate after that the tag updates it’s the seed value s by s*=Kp1⊕Ekp1(s) and again performs XOR encryption to compute Ekp (s*⊕ID) (by using public key kp of Server/ Reader) in order to convey to the reader.

Reader to Tag Authentication: Upon obtaining EKp(s⊕ID), the will pass it to the backend database to decrypt it. The decrypted value DKs(s*⊕ID)(by using its private key Ks)is used to extract the tag’s ID by carrying out the simple operation ID = Kp1⊕EKP1(s⊕(s*⊕ ID)). Then this ID is verified by comparing with the ID existing in database to check whether this tag is legally acceptable or not. If the mismatch occurs, the server discards any data it has received and declines the authentication of the tag. Oppositely, the server update the seed value of reader by s*=Kp1⊕EKP1(s).

Figure No.2 Mutual authentication between tag and reader.

IV. SECURITY ISSUES

1. Security of the tag, reader and the server: In RFID data travel in a wireless network so the security of data is an important factor to achieve better Communication and better efficiency of the data in the network.

2. The original data stored at the receiver: The original data from the tag get stored at the server, and it is possible that the server can be accessed in an unauthorized manner and also the server can get damage so the data will get lost so it also need fault tolerance.

3. Low computational and storage cost: There are various functions are existing for the better working so when this functions get implemented the tag and the reader should not increase the computational and the storage cost.

4. Chances of eavesdropping: The security of the data from tag to reader should be authenticated so that the chance of eavesdropping has been reduced.

5. Proper synchronization between tag and the reader: It is the flow of control from tag to the reader. The data moved from tag to the reader should be synchronized so that the data can’t be lost and the chance of congestion has been reduced.

V. RESULT ANALYSIS

5.1 Security Analysis

Information leakage

Here the proposed protocol implemented using ECIES prevents the plain text from accessing the outsider in the air, since the technique implemented uses the Tag and Reader side authentication separately and the chances of accessing the key is not possible and also even if he gets the key he can’t decrypt the text. The encryption and decryption is done on the tag and reader and server side hence the chances of information leakage are minimum.

Tag Tracing and Tracking

FID tag is designed to have a unique number which can be tracked in range of any readers. However, this protocol provides the mechanism that whenever the counterfeit reader queries the tag; the tag does not send any response back. Consequently, the tracking and tracing privacy is secure in this protocol.

Tag Cloning

In theory, there is no tag which has similar unique identifier number to another one. However, adversaries can replicate the forged tag without much effort and expense. To conduct the tag clone attack, the attackers have to obtain the key K, seed s and the ID of the tag.
However, these shared data are kept safely and privately in the backend database and inside the tag; the attackers have no information to perform the same encryption block to acquire the authentication.

**Man-in-the-middle attack**

The adversative readers can impersonate the valid one in order to intercept, change and obtain the messages going between the parties which they need. In the proposed protocol, before querying the tag, the server sends the message $EKP(s \oplus IDR)$ to the reader. Because only valid reader has the key $K$ to decrypt this cipher text, there is no possibility for attackers’ readers to achieve the seed $s$ in order to communicate with the tag. Thus the man-in-the-middle attack can be avoided.

**Denial of service attack**

Let us assume the scenario in which the response $EKP(s \oplus ID)$ from tag to reader is intercepted by the adversary. Because the reader has not got the response from the tag, it does not update its seed value. In the next authentication, reader sends $EK(s)$ to challenge the tag. But the seed in tag now is $s^* \neq K \oplus EK(s)$, therefore, $EK(s) = EK(s^*)$ is not satisfied and the tag keeps quiet.

**Replay Attack**

In replay attack, the adversaries stand in the middle of communication channel to duplicate the valid transmission which will be fraudulently repeated later. However, the seed $s$ is automatically updated after each successful authentication session. This leads to the fact that the cipher text $EK(s)$ changes in every authentication cycle. Thus, the attackers cannot utilize the former data in order to deceive the authorized reader or tag to overcome the authentication process.

**Password Impersonation attack**

The password impersonation attack is possible when the attacker get any parameter through which he can access the data, but here due to the hard logarithmic problem of ECC and update of seed value in each authentication phase phase to attempt the password impersonation attack gets impossible.

5.2 Performance Analysis

The AES is symmetric key encryption technique works on key size of 56 to 256 bit and takes 37 for encryption and 42 micro seconds for decryption whereas ECIES is asymmetric encryption technique works on key size of 16-112 bit and takes 30 microseconds for encryption and 12 microseconds for decryption.

**VI. CONCLUSION**

The proposed technique provides more secure mutual authentication between tag and reader because it uses the concept of asymmetric key cryptography which is more secure than symmetric key cryptography, this technique also prevents various types of attacks and also by updating of seed value in every authentication session the replay attack, tag tracing and denial of service attack gets impossible.

REFERENCES


