Secured Serverless RFID with Object Oriented Approach

Monika Sharma[1] and Dr. P. C. Agrawal[2]

***Abstract*—** In growing adoption age of RFID technology results, there are major issues and challenges. These are the security of tags, privacy of individual and cost of server and tag. As this technology is based on track and trace system, privacy of individual is suffering because a reader periodically send a query and all the vicinity respond to that reader with their id; according to that id legitimate user can access data through server.
So security from tag to reader and reader to server are major concern for solving privacy violation.

In this paper we will focus on privacy enhancing techniques which are using now a days and how object oriented approach can solve the problem of privacy violation.

***Keywords*—** *RFID*, Privacy Enhancing Techniques, Object Oriented Approach, Data on Tag

I. Introduction

ACCORDING to RFID Journal magazine an RFID tag is a microchip that is attached to an antenna that is packaged in a way that it can be applied to an object/people. RFID has three main components Tag, Reader and Antenna. A tag is a type of device that can be attached to a person or a manufactured object for the purpose of unique identification and a reader is an electronic device that broadcasts a radio signal to a tag, which then transmits its information back to the reader.

According to current scenario RFID works in six steps:

a) A RFID tag can be attached to object/people.

b) A unique id is assigned by server for each tag and the information about tag is stored in database on server.

c) Reader broadcasts a query for a tag ID.

d) Then, corresponding tagged item respond to the reader.

e) After that reader send tagged id to sever.

f). Now, the reader access all the information related to tag.

Monika Sharma[1] is Research Scholar Mewar University (Chittorgarh) Raj.,Department of Computer Science & System Studies, India. Email: monika_ 05 @rediffmail.com

Dr. P. C. Agrawal[2] is Guest Professor, Mewar University & Retired 'Scientist E' Ministry of communication & Information Technology Govt. of India, New Delhi.

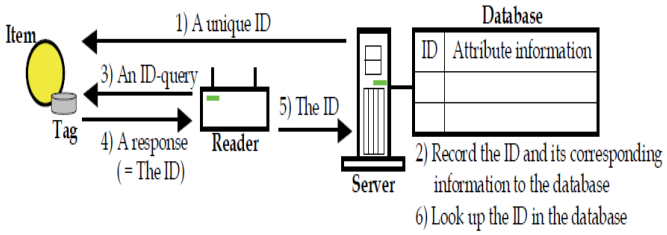

Fig. 1 A Basic RFID System [1].

II. RFID System and Privacy Enhancing Techniques

RFID tag responds to each query. Suppose a person is bearing an object containing a tag results unintentionally, that person is also tracked by adversary. To prevent tag from such situations various privacy enhancing techniques are used. These are as follows:

A. Password assigning to a Tag by reader for accessing a query

A tag responds to reader only after receiving the correct password from reader. The countermeasure is adopted in EPCglobal Class 1 Generation 2 (ISO 18000-6 Type C) and the bit length of password is 32.

B.Destroying Tag

As the tag is attached with item; after sale of item it can be destroyed so that adversary cannot track a person via object. This can be done by cutting the antenna of the Tag by scissors or burn off the logical circuits in the tag by a high voltage electrical current and so on.

C. Kill Command

After executing kill command tag will not give response permanently; as this command helps to prevent response from a tag.

D. Faraday cage

In this countermeasure tag can be prevented from id query response by covering a tag with certain type of material like foil paper etc.

E.Hash lock scheme

In this scheme a Tag authenticate a Reader before sending its ID as a response. Reader generates a password as a unique ID for each Tag and calculates a hash value for each password and stores ID for the corresponding hash values and passwords in the database. After receiving an ID-query from the Reader, the Tag sends its

hash value to the Reader and reader send the corresponding password to the tag from database. After that Tag calculates the hash value of the password and compares it with the stored one. The Tag sends it's ID if it matches.

The advantage of Hash Lock scheme over the access password scheme is that a lot of time is required in order to guess the password from the secret information in the Tag. An Adversary must analyze the hash value in the Hash Lock scheme but need not analyze it in the access password scheme. The Adversary, however, can obtain the password against both schemes only by eavesdropping upon communications between a legitimate Reader and the Tags. The Adversary can confirm the links between the responses, i.e. the hash values, because the responses are static in Hash Lock scheme.

F. Change of operation modes

There are the various schemes related to change of operation modes. One of these schemes is LKI. In this scheme when Tag does not emit its ID and signal is called *a Silent mode*. This scheme assumes that the Tag has a non-volatile memory to record the operation mode. Then the Tag maintains its operation mode without electric power. This scheme also needs the authentication mechanism. According to Liu et al., the password- based authentication may be enough if the password is managed appropriately and legitimate Readers pay appropriate attention to eavesdropping upon communication of authentication [5].

G. Jamming

This is the additional device with the tag which prevents legitimate Reader to access the ID. But the major disadvantage is the emission of electromagnetic waves form device is restricted in some areas, e.g. hospitals. So some countries restrict the emission of jamming.

H. BLOCKER TAG

This is also an additional device with the tag which responds only when receiving queries from reader. The disadvantages of the Blocker Tag is that if an Adversary have smart Reader that can accurately identify the location of a Tag sending its ID, may obtain the ID.

I. Randomized Hash Lock scheme

In this scheme after receiving an ID-query, a Tag generates random number r and calculates hash value h of its ID and r, i.e. $h = H(ID||r)$, where ID|| r denotes concatenation between ID and r. And the Tag sends h and r as its response to the Reader and receiving h and r, the Reader calculates the hash value $H(x||r)$, where x denotes each ID of the Tags managed by the Reader. Then the Reader exhaustively searches for x such that $H(x||r)$ matches h. The Reader regards the corresponding x as Tag's ID if it matches.

It is difficult for an Adversary to identify the Tag's ID by comparing the responses mutually because the responses sent by the Tag change at each ID-query. The disadvantage of this scheme is that if the number of candidate IDs is small then the Adversary may be able to identify the ID from the response by exhaustively searching, like the Reader and the computational complexity for the Reader identifying the ID is proportional to the product of the following two factors: the number of the Tags that the Reader manages and the number of the Tags in the area where the Reader can communicate.

J. Symmetric Key Cryptography based schemes

This scheme solves the problem of random hash lock scheme. Here A Reader preliminarily records symmetric key k, which is common to the RFID system, to each Tag and after receiving an ID-query, the Tag generates random number r and encrypts r and its ID with k and SE(), where SE() denotes a symmetric key encryption function. And it sends cipher text $c = SE(k, r||ID)$ as its response to the Reader .finally after receiving c, the Reader obtains $r||ID$ by decrypting c with k and extracts the ID.

As the Tag generates random numbers at each ID query so responses sent by the same Tag are different . So it is difficult for the Adversary to identify the IDs and to confirm the links between the responses if the symmetric key cryptography adopted is secure.

K. Hash Chain scheme

In this scheme, it is difficult for the Adversary who obtains the leaked secret information to confirm the link of the responses. This scheme assumes that Tags are implemented with two one-way functions H () and G (). Its procedure is as follows:

a) A Reader preliminarily assigns a different key to each Tag and stores each ID and the corresponding key in the Reader's database. We describe the initial key of Tag-i as $k_{i,0}$ $(1 \le i \le n)$, where n is the number of Tags managed by the Reader.

b) After receiving an ID-query, Tag-i calculates hash value $h_{i,0} = H(k_{i,0})$ and sends $h_{i,0}$ as its response to the Reader. And Tag-i updates $k_{i,0}$ with G() and replaces $k_{i,0}$ by $k_{i,1} = G(k_{i,0})$. The key of Tag-i is updated when receiving the queries.

c) And after receiving the response h, the Reader calculates $h_{i,t+j} = H(G^j(k_{i,t}))$ and searches for i and j such that $h = h_{i,t+j}$, where $G^j() = G(G^{j-1}())$, $0 \le j \le s$. s denotes a range where the Reader searches for the hash value. And $k_{i,t}$ denotes the Tag-i's key recorded in the database at that time.

d) The Reader considers the sender of the response as Tag-i if matching. The key of Tag-i is $k_{i,t+j}$ at this time. The Reader replace $k_{i,t+j}$ in the database by $k_{i,t+j+1} = G(k_{i,t+j})$.

The security of this scheme is based on the difficulty of inversion of the hash functions. It is difficult for the Adversary to guess the former keys from the key obtained by the Adversary at a certain time because the keys are updated with G(). Then the scheme satisfies forward security if G() is sufficiently secure. Moreover, it is also difficult for the Adversary to confirm the link of the responses because the responses are generated by calculating the hash value of the keys with H(). However, the computational complexity for the Reader identifying the ID is proportional to the product of the following three factors: the number of the Tags managed by the Reader, the number of the Tags in the area where the Reader can communicate, and the number of

the key updates which are not comprehended by the Reader. Moreover, the Tag updates its key even if a malicious Reader sends an ID-query to the Tag. The Tag's key goes out of the range in which the Reader searches if the malicious Reader sends ID-queries *s* times. That is, the legitimate Reader cannot identify the ID in this case.

L. Public Key

We can construct a scheme which contains the following two features if Tags are implemented with a pseudo-random generator and a public key encrypting function: a) the scheme satisfies forward security, b) the Reader need not search for IDs exhaustively. The procedure of the scheme, hereafter called *a PKC-based scheme*, is as follows:

a) The Reader preliminarily writes its public key and a Tag's ID into the Tag.

b) After receiving an ID-query, the Tag generates a random number and encrypts the number and its ID with the public key. And the Tag sends the ciphertext as its response to the Reader.

c) After receiving the ciphertext, the Reader decrypts it with the Reader's secret key and extracts the ID.

In this scheme Adversary needs a Tag's ID, the Reader's public key, the responses and the random numbers used for generating the responses in order to confirm the link between the responses. so this scheme satisfies forward security if the pseudo-random generator adopted is secure. Moreover, the Reader need not search for IDs exhaustively because the Reader can obtain the IDs only by decrypting the responses. The other schemes like RSA and elliptic curve cryptography are not suitable for low performance RFID tags because of the computational complexities of such cryptosystems. Then, lightweight PKC [9] is suitable for Tags because its encryption can be performed only with exclusive-OR in the parallel processing [1][6].

M.Re-encryption schemes

In this scheme a Tag is updated with a pseudo-random generator and the PKC. A Reader preliminarily writes a cipher text of a Tag's ID and the public key of the Reader into the Tag. After receiving an ID-query, the Tag sends its cipher text as its response to reader and updates the cipher text. The Reader can identify the ID in the same way as a Reader in a PKC-based scheme does.

The advantage of the Re-encryption scheme over the PKC-based scheme is that it does not store the plaintext of the ID in the Tag. On the other hand, the Tag cannot flexibly execute the reactions which correspond with its ID because the Tag does not know its ID. Moreover, the computational complexity of the updating is not low because the complexity is equal to that of encryption with ElGamal PKC. However, the Tag in the scheme needs to authenticate the Reader in order to prevent a malicious Reader from forging it.

Above all schemes have limitations in terms of tag security, computational complexity as well as cost.

III. RFID TAG WITH OBJECT ORIENTED APPROACH

RFID tag is of three types: Active, Passive and Semi Passive tag. Active Tags has an on-board power source, whereas Passive Tags have no power source of their own and therefore must rely on the EM field created by a reader. Passive labels normally communicate information to a reader by modulating the reader's RF signal. Semi-passive tags which have a battery but use the power of the reader to transmit messages results in good reliability but limited range.

As discussed in section '2' about various schemes of privacy protection, it is difficult to protect accessing of tag information on server. So we proposed an object oriented approach, where information of tag will be stored only in the tag memory as tag has its own memory and it can store more than just a tag ID [2]. So this memory can be used to store and hide tag id from unauthorized access.

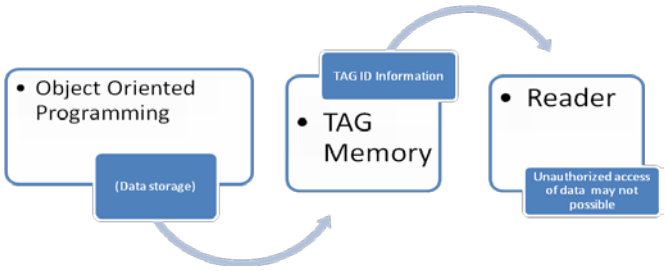

Fig. 2 Object Oriented Approach on RFID Tag Memory

In this approach the tag memory size needed for this operation is considerably larger than the memory size available on current tags. Since the template structure is memorized directly on the tag, additional memory space is required for the definitions of classes and field types. This information is necessary in order to ensure the independence of tags. Furthermore, the classes and field types could be used by a low-resources embedded device (station) to interpret and modify the tags read. If a tag template is unknown, its content cannot be interpreted and thus data privacy is ensured. The evolution of the tag market and the demand for RFID-based applications will dictate the appropriate choice [3].

With this approach we have no need to store tag information on server. Tag details will be in tag memory only so that they can work independently on reader query. For this Java language can be used as in java newly created objects are initialized to null, automatic garbage collection results no memory leakage. And one more thing is that as tag has less memory; Java compiler compile to byte code which the JVM interprets or JIT compile it to machine code cause less memory is required in comparison of C++; as C++ code is compiled directly to machine readable code [4].

A Advantage of Object Oriented Approach

In this approach there is the flexibility to add the data on the tag without change in an applications; user can encode the sensitive information on the tag itself.

In object oriented approach: As all the data is on tag. And tag respond to a reader in comparatively in less time as authentication will be at tag level only. Because, in other

approach a reader broadcast a query to object tag, according to tag id information is accessed through the server using various privacy preserving query encryption techniques which requires more efficient work on complex queries. [7], [8].

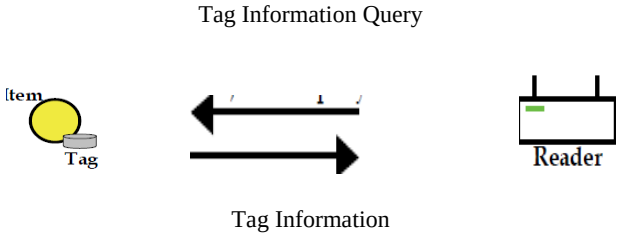

Fig. 3 A Server less RFID System after storing data on tag

One more thing is that there is no need to modify the software of the embedded system to allow the same device can be used in different applications for example supplies chain, car parking control etc.

B Disadvantage of Object Oriented Approach

Major disadvantages have that the higher the amount of data on the tag, the longer the data reading time. Nevertheless new solutions have already been found: a high capacity, high-speed LSI for RFID tag complying with ISO/IEC15693 [3].

IV. Conclusion

RFID need growing in today's trace and track world; results privacy and security also in demands. We have discussed various security solutions that are currently used to protect privacy from unauthorized access but they are not the complete solution. While storing the information on server require more security in comparison of storing data itself in a tag using object oriented approach.

In future work can be done on compressed data encryption so that tag may store more secured data.

References

[1] Masataka Suzuki and Kazukuni Kobara (2009) "Privacy Enhancing Techniques on RFID systems", Development and Implementation of RFID Technology.

[2] Sarita Pais and Judith Symonds(2011), "Data storage On RFID tag for a distributed system" International Journal of UbiComp (IJU), Vol.2.

[3] Cristina Turcu, Remus Prodan, Marius Cerlinca and Tudor Cerlinca (2009) "Object-Oriented Solutions for Information Storage on RFID Tags" Development and Implementation of RFID Technology.

[4] Ali A Altalbe and Abulrahman H Altalhi, (2013), "Performance comparison between Java and C++", Conference proceeding ICRITO 2013.

[5] Liu, D., Kobara, K. & Imai, H. (2004). Pretty-Simple Privacy Enhanced RFID and Its Application, *The Seventh International Symposium on Wireless Personal Multimedia Communications (WPMC 2004).*

[6] Niederreiter, N. Knapsack-type Cryptosystems and Algebraic Coding Theory (1986),*Problems of Control and Information Theory*, Vol. 15, No. 2, pp. 159-166.

[7] Chiu C. Tan,Qun Li,and Lei Xie "Privacy Protection for RFID-based Tracking System(2010)" IEEE RFID.

[8] Zhiqiang Yang, Sheng Zhong and Rebecca N. Wright,(2011) "Privacy-Preserving Queries on Encrypted Data". http://www.cs. rutger s.edu/ ~rwright1/Publications/esorics06.pdf

[9] M. Aikawa, K. Takaragi, S. Furuya, and M. Sasamoto (1998), "A Lightweight Encryption Method Suitable for Copyright Protection," IEEE Trans. On Consumer Electronics, Vol. 44, No.3, pp. 902-910.

[10] Ari Juels, RFID Security and Privacy :A Research Survey (2005), IEEE Journal on Selected Areas in Communications.