IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-5 E-ISSN: 2347-2693

Double Security of RFID Credit Cards

M.A.A. Khan[1*], A.A.S. Qureshi[2], M. Farooqui[3]

[1]Computer Science, College of CS and IT, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[2]Information Systems, College of CS and IT, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[3]Computer Science, College of CS and IT, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

[*]*Corresponding Author: mkhan@uod.edu.sa*

Online Available at: www.ijcseonline.org

Received: 24/Apr/2017, Revised: 30/Apr/2017, Accepted: 22/May/2017, Published: 30/May/2017

***Abstract*—** Rapid advancement in RFID systems increase the need of sufficient computing power. Nowadays, more power is required to implement the encryption and decryption for the authentication during transactions. In addition, RFID tags have enough capacity to store the corresponding information. The radio waves are used in RFID technology to read the data from RFID tags. Information about the card and its owner is embedded in a tiny microchip in the e-card. The card can be read by remote machines, therefore this paper proposed double security check by introducing mobile user for the secure transaction. In addition, to provide more security to the credit card holder when his information is processed through RFID. Proposed RFID system is based on Secure Hash Algorithm and mobile communication devices such as cellular phones. It provides a secure certificate mechanism which uses a mobile phone, RFID reader and credit card containing RFID tag. Secure Hash Algorithm is used to obtain a secure and reliable way of transmitting data. The result shows that the proposed method improves the existing RFID security issues under the premise of safety, efficiency, and compatibility with the network.

***Keywords*—** RFID, RFID Reader, RFID Tag, Secure Hash Algorithm, Credit card, Mobile security

I. INTRODUCTION

Radio frequency identification (RFID) systems use a small device (RFID tag) to receive and send remote commands. It contains two significant parts in its processing, one is RFID reader and other is RFID tag. It is passive tag as it is without power based on the job of RFID reader. It is used in many areas, for instance, security operation, identifying data etc. Due to the ability to uniquely identify the individual item at low cost, RFID tag is suited for supply chain management [1]. Previously bar code systems were widely utilized, however, these have been largely replaced by RFID systems. RFID tag will completely replace the barcode in near future [2]. Unlike barcodes, these tags have a longer range in which they can be scanned and can identify objects along several lines-of-sight simultaneously. By reducing the cost of RFID tags, they can be implemented in a wide field of applications such as entrance control, pet identification, electronic toll payments and so on [3]. RFID cards don't require swiped machines to transmit personal data like a traditional credit card. They can be read wirelessly and without line-of-sight, contain more information than barcodes. Unfortunately, Radio frequency data can be transmitted through wallets, even if it is in your pocket or purse. The operation range of RFID tags varies from few inches to several meters. RFID technology does not require line-of-sight while scanning the tagged objects. In fact, the tagged objects can be placed in a carton and packed in a box and it is not necessary to open each box to scan the objects. RFID technology supports reading of multiple tags simultaneously. On the contrary, barcodes require being in line-of-sight for perfect scanning which limits the operation range of barcodes [4].

The block diagram RFID system is shown in Figure 1. RFID reader consists of a transmitter-receiver module, a control unit, and an antenna. A tag is made up of a microchip with an antenna. The reader sends electromagnetic signals and the tag receives these signals through the antenna. The microchip modulates the signals and sends it back to the reader. This information received from the tags is then processed by sending it to the host computer [5]. RFID readers can scan tags at rates of hundreds of per second. RFID credit cards can be skimmed when an unauthorized user grabs the unencrypted data from your card using a RFID reader. With the increasing ubiquity of RFID tags, privacy became a concern.

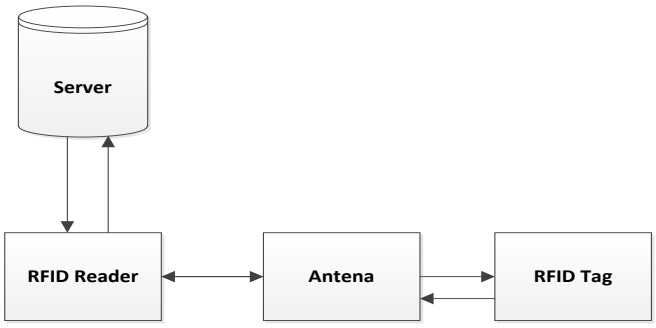

Figure 1. Block diagram of RFID system

To sum up, the basics of RFID working, power is received through mutual induction by the passive RFID tag with the help of circuits and used by RFID reader for some purpose. RFID tags contain small microchip and transmitter. They are only be activated by RFID reader to which tags returned its signals. Information of the product or the person is stored on the tag while the reader can read the data.

In I section, RFID is introduced while in II section, related work is discussed. In III section, Methodology of the algorithm is defined. In IV section, the algorithm is explained. V section is about the improved mechanism. Finally, paper is concluded with some future directions.

II. RELATED WORK

As RFID field is very vast and advancing, previously work had been done in organizing and executing RFID Systems for monitoring products in fields like supply chain management. This contains a lot of complication, and difficulties affecting data controlling and maintenance. Therefore, Cloud computing appeared to be one of the outcomes that are used to diminish the hazards related to the execution and deployment of RFID based on the system in supply chain management. The multifaceted system for data filtering, management and maintenance are implemented in the cloud [6].

RFID-enabled credit cards are broadly used in the United States and other nations, without open study comprehensively evaluated the mechanisms that provide both security and privacy. It's been observing that using models from a variety of RFID-enabled credit cards, the information is stolen and the name of cardholder and other information from the card is disclosed to unauthenticated readers. Also, skimmed cards devices provide execution for the RF repeat attack. The information revealed by the RFID communication infects the security of RFID and non-RFID payment contexts, and RFID-enabled credit cards are vulnerable to a range of other customary RFID attacks such as skimming and relaying [7].
There are many challenges and methods for RFID-enabled credit for security and privacy in place of other RFID-based verification and proof of identity systems.

Work in the field of cloning is also found where many categories of RFID tags emit static identifiers, for easy to clone. These are inappropriately used in unauthorized building access control. A simple and inexpensive device has been validated by Westhues that can skim many types of cards at a distance and then simulate them [8]. This could be security break if no-clonability is considered as a security assumption. More use of cryptography to emit different data during different transactions is required in place of security tags. For instance, in some areas, common theft deterrent systems for automobiles are commonly used. These systems have been exposed to be susceptible because of defective cryptography [9]. The use of cryptography for increasing difficulty is contrasting the RFID credit cards without holding personally detecting information.

Another field is Read Arrays which is also related business that claims around the security of RFID devices. No read ranges are assigned to RFID tags. Short, non-standard reader or large antennas are included normally in a RFID tag that can grow the range at which an attacker can scan a RFID tag.

III. METHODOLOGY

As credit cards holder moves in the RFID Reader area, RFID Tag is detected and the query is asked automatically. Now Tag sends the Reader information to user Mobile for authentication of RFID Reader. Next mobile sends the information received from the Tag to the Server for the authentication of true mobile user and Reader. Since Server has secret keys shared with reader and tag, also it has a key which is shared with the mobile user, it has to do the following two tasks: First it verifies the true mobile user by asking the secret key which is shared between them. If it finds that it's a valid user then it performs the second task otherwise, the process will halt due to the reason that it is not in the hands of the valid user. If the user is valid then it checks the authentication of valid Reader using the shared key between them. If it finds the valid reader, then it sends the reader validation information to the tag.

As Tag has a secret key so it checks that the information comes from a valid server if tag finds that it's a valid server, then it sends credit card information to the reader. Thus, in this whole mechanism, double security is provided at each stage of the transaction. If at any stage, the unauthorized person tries to hack the information, he will fail because of the double secured method. In the end, all the secret keys are updated after each mutual authentication and prevent from replay attacks. Figure 2 shows the main working of transaction handled through RFID.

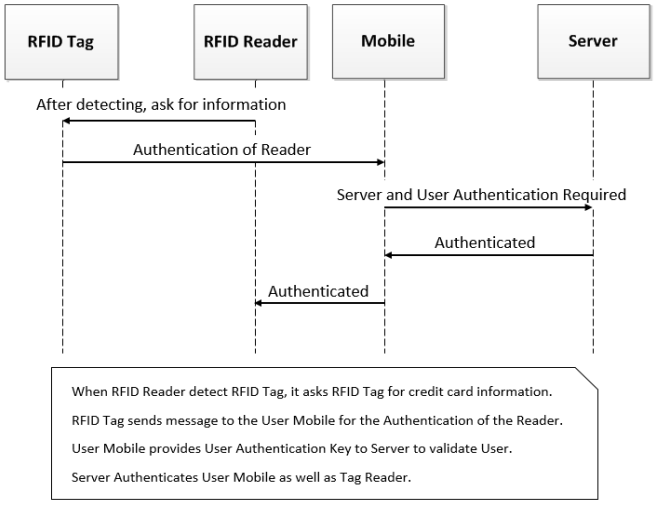

Figure 2. Transaction Process

In the security code creation, Reader generates a Random number. It is XNOR'ed with the RSK. With the help of Hash function, a value is calculated. Here XNOR function is used. XNOR is a quite simple logical operation, comparing two values. Another important function applied here is the Hash function for cryptography. The Reader then sends S, N with a query signal to Tag.

Secure Hash Algorithm encrypts the information using mathematical transformation. It is based on Hash Value which is fixed length output. A hash function is usually represented as an n-bit hash function. The competency of Hash function operation is faster as compare to other security methods. Many operating systems uses the hash function to encrypt the password to provide some measures of the integrity of information [10].

Next RFID tag receives values in the form of input from the reader. Again, a random number is generated and XNOR'ed with a secret key and the hash function is applied. Here the result of the previous hash function is compared with the new hash function result. If both are same then again, the random number is generated with a timestamp (T_i) is generated to detect the attacks. New code is generated based on these inputs and TIC then divided into three blocks to send to user mobile for authentication of Reader. The mechanism of the method proposed is shown in Figure 3.

All the information based on previous findings is sent to the Server. At this point, the server performs two tasks: First it asks the secret key of the user then Mobile generates a random number and use the hash function and send this information to the server for authentication. The second task after user authentication, it uses the secret key to verify the valid reader.

IV. ALGORITHM

Table 1. Notation

Symbol	Meaning
TIC	Tag identification code
TSK	Tag secret key between tag and server
RSK	Reader secret key shared among tag, reader and server
USK	Mobile user Secret key shared among user and server
H()	one-way hash function
ʘ	X-NOR operation
||	The function of string concatenation

Assumption:

I. This paper proposed that during the authentication process the random values and shared keys are used to achieve the mutual authentication through different signals at each timestamp.

II. The tag has shared a secret key (TSK) and security identification code (TIC). The RFID credit card and the backend server will update the secret key (TSK) synchronously after completing the transaction.

Authentication process

To identify the authorized reader, tag, mobile and server conduct the following steps as shown in Figure 3.

Step-1: (Reader to Tag)
The reader generates a random number N, perform X-NOR operation, and calculate.

$$N_{new} = RSK \text{ ʘ } N \text{ \& } S = H(N)$$

The reader then sends (S, $N_)$ with a query signal to Tag.

Step-2: (Tag to mobile)
As the tag receives the values N_{new} & S from the reader, it will verify the identity of the reader. Therefore, it will calculate,

$$N' = N_{new} \text{ ʘ } RSK \text{ \& } S' = H(N')$$

Now for verification, it compares S and S'. If both are same then it generates a random number 'n' and a time stamp Ti to compute

$$M = ((TIC_i \text{ ʘ } n \,||\, Ti) \text{ ʘ } H(n \text{ ʘ } TSK)$$

$$Code = H(n \text{ ʘ } TIC_i \text{ ʘ } TSK \text{ ʘ } T_i)$$

The message code is divided into three blocks C_1, C_2, and C_3 for comparing the results and send a message to user mobile.

Step-3: (Mobile to server)
In this stage, the mobile user sends all the information that comes from tag to the server for verification of reader and it also transmits the user information to verify the authenticate user.

I. Mobile receives a message containing (C1, M, n). it sends this value back to the server along with the values generated in step-1 as N_{new} and *S*.

II. The mobile user generates a random number K and computes the value of $K_{new.}$

$$K_{new} = K \text{ ʘ } USK \text{ \& } S_u = H(K)$$

Now send K_{new} & S_u to the server to authenticate the mobile user.

Step-4: (Server-Tag)
Now the server receives the values to verify the true user and authenticate reader. So, this process is divided into two steps again. First, it verifies the user information by using Secret key (USK) which is shared between mobile user and server.

If it verifies the true mobile user then server authenticates the reader. In case server finds that user is false then it terminates the whole process.

I. First, it checks the user information to verify that it is a true user or not. So, it calculates
$$K' = K_{new} \odot USK \ \& \ S_u' = H(K')$$ and
verify that $S_u = S_u'$. If both are identical then it moves to the next step.

II. It calculates N" and S", to verify the reader. N" is given as,
$$N'' = N_{new} \odot RSK \ \& \ S'' = H(N'')$$

compare S'' and S, if same then search for tag information from common key (TSK).

Recomputed TICi = $M \odot H(n \odot TSK_{db}) \odot n$ and timestamp Ti

Now compare $TIC_i = TSK_{db}$ if true then recalculate code
$Code' = H(n \odot TIC_i \odot TSK_{db} \odot T_i)$ Divide into 3 blocks C_1', C_2' and C_3'
Now compare $C_1 = C_1'$ is true then the server generates r, calculate
$T=C_2' \odot H(r \odot TSK_{db})$ and send the authentication of the reader to tag.

Step-5:
The tag use (T, r) to verify the server's identity by comparing C_2' *with* C_2
Where $C_2' = T \odot H(r \odot TSK)$
If $C_2' = C_2$, then it shows the successful authentication. At last, it updates the TIC for the next session by setting
$$TIC_{i+1} = TIC_i \odot C_3$$

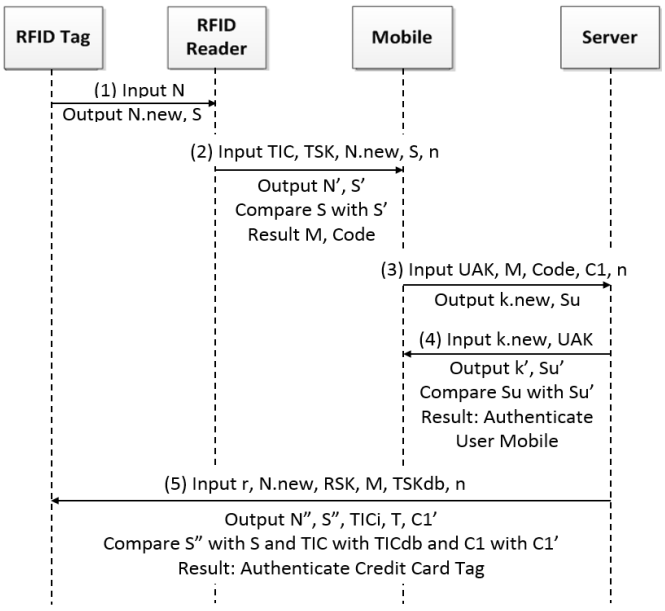

Figure 3. Proposed Scheme

V. IMPROVED MECHANISM

The improved version of algorithm provides double security. The technique used here is providing security to the mobile user and credit cards as well. Now even if mobile is stolen or credit card is stolen, key blocked the transactions by preventing from unauthorized access. Use of more random numbers helps in updating the keys.

The previous research used mobile as a reader but in proposed mechanism, the mobile is in between tag and reader to provide the security. If there is no valid user, there will be no transaction held.

Using the proposed technique, it prevents the various attacks such as Snooping, replay attacks, Cloning, Tag Tracing, User Privacy Violation, Data Imitating, Denial of services and Man in the middle attacks.

VI. CONCLUSION AND FUTURE SCOPE

Despite progressive and advanced security measures, fraud remains an important risk. Thus, in this paper, more secure methods for credit card transactions are introduced. Secure Hash Algorithm and XNOR function are used for protecting the transaction in RFID credit cards. The server manages the private key.
The key management can be done using clouds. To provide more facilities to users and customer, multifunction cards with the ability of debit and credit account on the same card can be used having similar cryptography approaches. Companies are working to reduce the cost and more advanced ways to use RFID technology in future. Nowadays RFID tag is required in medical field for record keeping of the patients. Similarly, RFID can also be used to keep track of expiry dates of products so more work can be done in the field of Virtual Smart Stores to meet customers' demands and needs. List of items and products bought are easy to maintain.

REFERENCES

[1] L. Castro, S.F. Wamba, "*An Inside Look at RFID technology*", Journal of Technology Management & Innovation, Vol.2, Issue 1, pp.1-14, 2007.
[2] A. Sharma, D. Thomas, "*Looking Backwards to Look Ahead: Lessons from Barcode Adoption for RFID Adoption and Implementation*", Journal of Information Systems Applied Research (JISAR), Vol. 7, Issue 4, pp. 1-13, 2014.
[3] K. Ahsan, H. Shah, P. Kingston "*RFID Applications: An Introductory and Exploratory Study*", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, pp. 1-7, 2010.
[4] W. Zhang, D. Li, "*Research on barcode Image Binarization in Barcode Positioning*", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, pp. 1-5, 2012.
[5] M. Kaur, M. Sandhu, N. Mohan, P.S. Sandhu, "*RFID Technology Principles Advantages Limitations & Its Applications*", International Journal of Computer and Electrical Engineering, Vol. 3, No. 1, pp. 1-7, 2011.

[6] S. Jamal, A. Omer, A.S. Qureshi, "*Cloud Computing Solution and Services for RFID Based Supply Chain Management*", Advances in Internet of Things, Vol. 3 No. 4, pp. 1-7, 2013.
[7] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, T.O. Hare. "*Financial Cryptography and Data Security",* IFCA/Springer-Verlag Berlin Heidelberg, USA, pp.2-14 2007.
[8] J. Westhues "*Hacking the prox card*", Springer, USA, pp.291-300. (2005)
[9] A. Juels, "*RFID Security and Privacy: A Research Survey*", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.
[10] B. Preneel, "*Cryptographic HASH Functions: An Overview*", In the Proceedings of the 6th International Computer Security and Virus Conference (ICSVC), Belgium, pp.1-9, 1993.

Authors Profile

Mr. Mohammad Aftab Alam Khan pursued B.Tech in Electronics & Communication Engineering and M.Tech in Electronics & Telecommunication Engineering in 2005 and 2009 respectively from India. He is currently working in College of Computer Science & Information Technology, Imam Abdulrahman Bin Faisal University (previously known as University of Dammam), Saudi Arabia since 2011. He is a member of Member of Computer Science Teachers Association (CSTA) and International Association of Computer Science and Information Technology (IACSIT) since 2012. His main research work focuses on Wireless Communication, Microstrip Patch Antenna, and Machine Learning. He has 12 years of teaching experience and 8 years of research experience.

Ms. Asiya Abdus Salam Qureshi pursued Bachelor and Master of Computer Science and Master of Business Admisntration from University of Karachi, Pakistan in the year 2006 and 2009 respectively. She is currently working in College of Computer Science & Information Technology, Imam Abdulrahman Bin Faisal University (previously known as University of Dammam), Saudi Arabia since 2014. She is a member of International Association of Computer Science and Information Technology (IACSIT) & International Association of Engineers (IAENG) since 2014, a Computer Science Teachers Association (CSTA) & European Alliance for Innovation (EAI) since 2015. She is a Reviewer at Journal of Big Data. She has published more than 7 research papers in reputed international journals and conference. Her main research work focuses on Cryptography Algorithms, Database, Cloud Security and Privacy, Big Data Analytics, and Computational Intelligence. She has 10 years of teaching experience and 6 years of research experience.

Mrs. Mehwash Farooqui pursued B.Tech in Electronics & Communication Engineering from India in 2005 and M.Tech in Communication Engineering from India in the year 2011. She is currently working in College of Computer Science & Information Technology, Imam Abdulrahman Bin Faisal University (previously known as University of Dammam), Saudi Arabia since 2011. She is a member of Member of Computer Science Teachers Association (CSTA) and International Association of Computer Science and Information Technology (IACSIT) since 2012. Her main research work focuses on Cryptography Algorithms, Network Security, OFDM, Microstrip Patch Antenna and Wireless communication. She has 12 years of teaching experience and 7 years of research experience.

