ENHANCING SECURITY IN BANKING APPLICATION FOR LOW COST RFID TAG

A.Anny Leema[1], M.Hemalatha[2]

ABSTRACT

RFID (Radio Frequency identification) is a wireless identification technology used to identify and track objects using radio frequency waves. It has pierced into all the sectors like supply chain automation, asset tracking, manufacturing and supply chain management , retailing, Warehousing, agriculture, traffic , transportation and banking due to its increased functionality and easy-to-use capabilities. It has its own attractiveness because of no line of sight is required between the reader and the Antenna. The role of RFID in banking is of more importance to improve customer satisfaction, avoid counterfeiting, financial document management, electronic payments using contactless cards and access control to resources. RFID tag cloning is one of the common attacks found in the RFID system. Our work uses low-cost tags where cloning of tags could lead to big damage. To improve access security and privacy in banking sector this paper introduces the new authentication protocol which prevents the tag from cloning. EPC Class1 Gen2 standard is considered as a universal specification for low cost RFID tags, but assurance is not given for the security. A new lightweight authentication protocol based on Gen2 is proposed to resist the attacks tracing and cloning using the method of CRC, PRNG and BAN logic. The result shows that the enhanced protocol of GEN2 meets the Enhancing Security Standard.

Key words - RFID Protocol, CRC, PRNG and BAN logic

I. INTRODUCTION

Radio Frequency Identification (RFID) has been considered as a key infrastructure for the omnipresent society. It is currently championed and widely used in all applications. RFID system consists of a tag , reader and the antenna. The tag is used to uniquely identify the object, the antenna is used to transmit and receive signals and the reader is used to observe the RFID readings. This technology uses radio frequency waves to transmit the information between the reader and the tagged item. The tags are of two types namely passive and active tags. Passive tag has no internal power source and it depends upon the power of the reader to backscatter its Id. It has its own attractions and known for its low cost and long life. Active tag has internal power supply and it is very expensive compared to the passive tag. Data storage can typically range between 32 to 256 bits in passive tags and several megabytes in active ones [1].

The role of RFID in banking is vital to improve both operational efficiencies and data security. The banks that were previously using bar coding now moved onto RFID thinking accuracy in mind. The RFID tag is attached to

[1]Research Scholar, Karpagam University,Coimbatore.
E-mail : annyleema@gmail.com

[2]Professor, Department of Computer Science
Karpagam University, Coimbatore.
E-mail : hema.bioinf@gmail.com

the customer bank card or passbook and it is being scanned automatically when customers enter the bank. The customer information alerts the bank staff to provide services to the customer. The bank card embedded with an RFID chip is read by the reader and the payment is processed automatically. Swiping the card or entering the Pin is not required due to RFID embedded chip. RFID readers are kept strategically throughout and RFID-enabled banking cards are provided to the customers. Hence bank employees are able to identify and greet clients by name and access the available account information when they walk through the door. After banking operation is over and the customer exit the system the captured information indicates that transactions have been completed. And from the bank point of view it is evaluated how long a customer waited before being helped and how long the client spent completing individual transactions.

The important problem we are facing with low cost RFID tag is unauthorized readers can access to tag information and illegal tags can be authorized by legal readers. Tag cloning is one of the common attacks in the banking sector. It is defined as the simulation of the original tag's behavior physically or virtually. When the cloned tags come into contact with radio waves, they respond with a slightly tainted signal and the reader is not able to distinguish authentic tag from the fraud one and may prove the authenticity of the tags falsely. The response can contain encoded personal identifying information like card holder's name, address, account information, Social Security Number and phone number. Upon harvesting these sensitive information the thieves are able to program their own cards to respond in an identical fashion.

II. Background Study

RFID-tags for anti-counterfeiting purposes and cloning problem have been discussed in [2]. It proposes an efficient protocol for authenticating these tags and it focuses on online authentication of RFID-tags. Considering a large deployment of RFID tags, there are many situations we need offline authentication where there is no valid reader available. In [3], RFID tags suitable for cloning attacks are discussed and therefore it should be taken into consideration during the e-banking RFID solutions. In order to prevent RFID tags from leaking messages, some improved physically and cryptographically schemes are proposed [4-8]. Cryptographic measures include reader-to-tag and tag-to-reader authentication. Several tag-to-reader authentication protocols have been proposed in [9, 10, 11] based on cryptographic primitives like bitwise operations and pseudo-random numbers.

III. EPCglobal Class 1 Gen 2 UHF RFID Protocol

The effective reading range is based upon the tag class. Generally class-0 tag reading range is 5-10 cm, and that of a class-1 tag is several meters. The Electronic product code (EPC) is a unique identification number provided to each RFID tag. EPCglobal class-1 generation-2 (Gen2) was approved as ISO18000-6C in July 2006. A Gen2 tag contains a Pseudo Random Number Generator (PRNG) and protects message integrity via Cyclic Redundancy Code. 16-bit random string is generated by the tag denoted as RN16 stored temporarily in the memory.

IV. Existing System

In GEN2 the identity of the tag (TID) is transmitted in

plaintext which makes the tag traceable and clonable. Symmetric or asymmetric ciphers are the traditional encryption methods and used in the existing solutions which are not suitable for low-cost RFID tags. To address these cloning issues, lots of works have been proposed in the existing literature but most do not conform to the EPCglobal RFID Gen2 standard. The existing system has the following disadvantages:

1) Cloning: RFID tags are usually positioned in open environments such as hospitals, schools, and offices which are exposed to all kinds of malicious tools. An opponent can read the tag and then clone the tag by writing all the obtained data into a blank tag. Unauthorized tag cloning is called as integrity attacks which succeed by capturing a tags identifying information [12].

2) Tag tracing: Communication takes place between Readers and tags by sending data. Attackers can trace the tags with the help of rogue readers called as passive attacks.[13] discusses the prospect of rogue readers and how it is controlled by hackers to monitor tags.

3) Eavesdropping: An opponent listens to all the communications through Radio Frequency (RF) and dumps them for later cracking.

V. Proposed System

The proposed system is a lightweight authentication protocol based on Gen2 to resist various attacks. The cryptographic function is not used in the proposed tag thus it is suitable for low-cost RFID. Gen2 using only PRNG and CRC-16 functions for authentication. Our work is to develop the novel authentication protocol which uses CRC, PRNG operations and BAN logic to improve the security level.

The advantages of the proposed system are :

- Cost is minimized
- Intractability
- It is not clonable
- Security and privacy

VI. Methodology

The methodology followed in this project is Top down approach. Top-down approach emphasizes planning and a complete understanding of the system. It is inherent that no coding can begin until a sufficient level of detail has been reached on the design of at least some part of the system. Then it is separated into different modules. To reduce errors, each module has to be processed separately, so programmer gets a large amount of time for processing each module. If an error occurs in the output, it is easy to identify the errors generated from which module of the entire program. The entire project is divided into five modules. The five modules include Admin, Command Detection module, CRC and Pseudo random number generator, BAN, Database management. The hierarchical diagram of the proposed system is depicted in the Figure 1 and the Architectural diagram is depicted in Figure 2.

A. Admin

Admin is the first point of interaction for anybody coming to the Bank. It has all the information about the creating employee id , creating RFID tag, delete the unwanted employee information in the banking system. Admin

Verified tags only allowed. If tags come within the specified range data is read and write operation is performed.

B. Command Detection

Command Detection focuses on RFID reader used to interrogate with an RFID tag. This module is used to read data from user tag and checks with the database. If the tag value matches it gives access to the user. This module is mainly designed for the code analysis to implement the data for authenticated person.

C. CRC & PRNG

Pseudo Random Number Generator (PRNG) protects message integrity via Cyclic Redundancy Code. CRC-16 is used to protect the information transmitted by both readers and tags. CRC-16 will detect burst errors of 16-bits or less,any odd number of errors less than 16, and error patterns length 2 [14] . CRCs by themselves are not suitable for protecting against intentional (malicious) alteration of data. Reserved memory, EPC memory, TID memory, and User memory are the four banks in memory space. As it gather power from readers through the antenna it cannot perform complex computations. RN16 is a 16-bit random string generated by the tag and temporarily stored in the memory.

D. BAN Logic

The BAN-logic is one of the methods for the analysis of cryptographic protocols. One of the goals is to show how the BAN-logic is best applied. Although the BAN-logic can be easily applied and gives a quick insight in the working of a protocol, attention has to be paid that the analysis is made thoroughly. The protocols CRC and PRNG are not secure and subject to replay/impersonation and synchronization attacks. Hence in addition to the CRC and PRNG, BAN logic is proposed to enhance the security. The used BAN logic notation are as follows:

□ P |≡X : P believes X ;

□ P□X : P sees X ;

□ P| ~X : P said X ;

□ P |□ X : P controls X ;

□ #(X) : X is fresh ;

□ P←□K→Q : K is the key shared by P and Q ;

□ {X}K : the ciphertext of X encrypted by the key K.

BAN logic consists of 19 logical rules and out of the only four rules Jurisdiction rule, Nonce-verification rule, Message-meaning rule and Message-meaning rule are used to enforce security.

E. Database Management

A database is an integrated collection of data records, files, and other objects. A DBMS allows different user application programs to concurrently access the same database [15]. Varieties of database models are used by the DBMS to easily describe and support applications based upon the requirements of the user. It typically supports query languages, which are in fact.

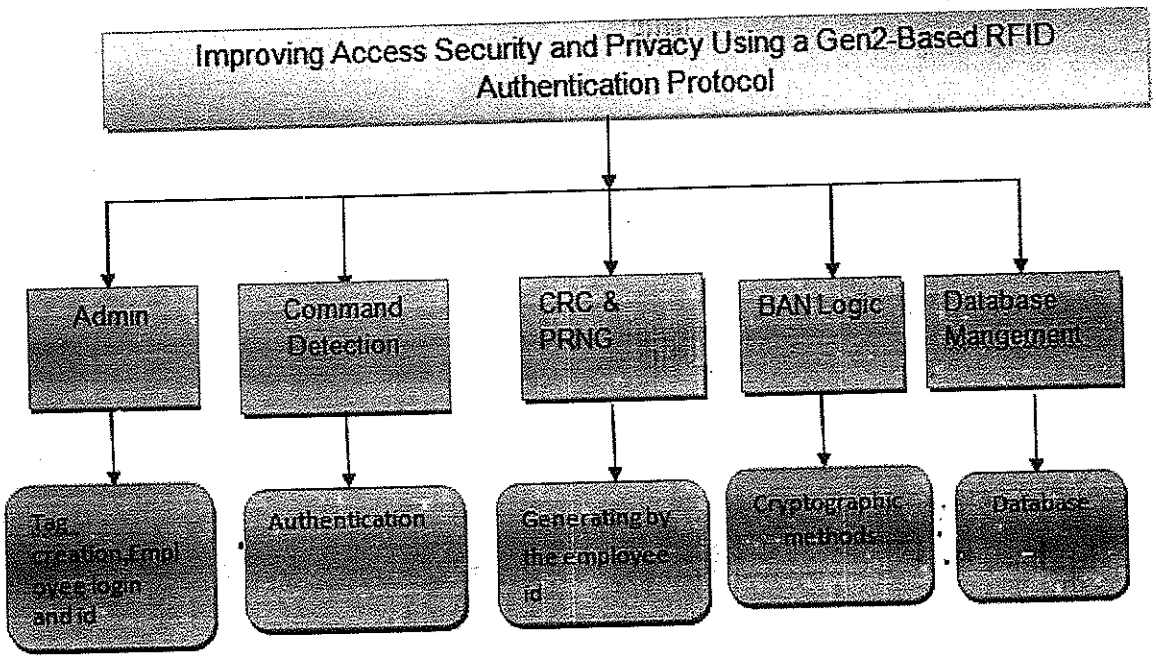

Figure 1 : Hierarchical Diagram of the System

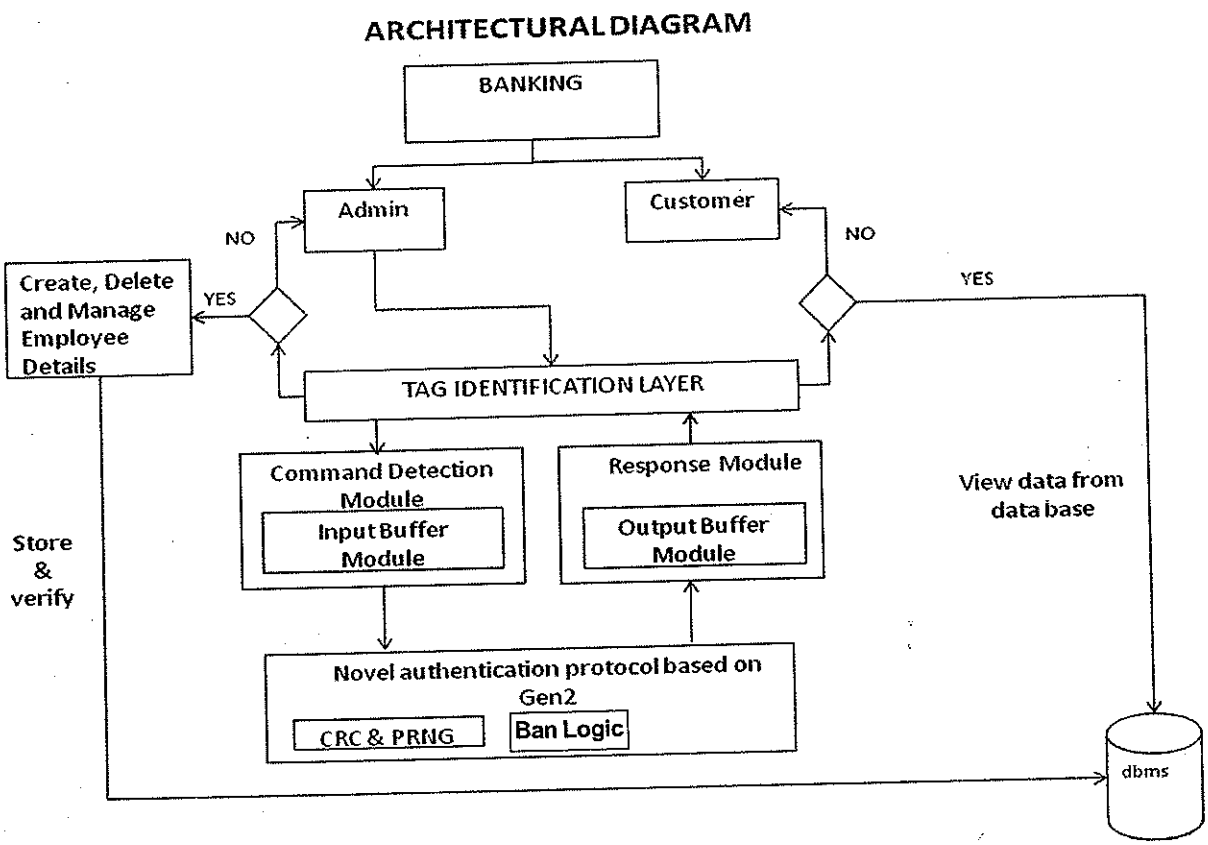

Figure 2 : Architectural Diagram of the system

VII. Our Contribution

The new authentication protocol is proposed here which avoids traceability and tag cloning. It also prevent queries by unauthorized readers. The proposed protocol also uses 16-bit CRC and 16- bit PRNG like GEN 2 but it do not use them directly. It constructs new functions in order to generate 96-bit random nonce and 96 bit CRC result. CRC() (Cyclic Redundancy Check) is used to encrypt0decrypt and implement authentication between readers and tags. The protocol does not send the plain text and it is send in the encypted form so that the information is not leaked to the attackers. BAN logic is used to prove the correctness of the protocol and find major security loopholes. BAN logic has been an important tool for reasoning about protocols. Figure 3 shows the User interface to enter the new employee. The sample screenshot for enforcing tag security in banking application is depicted in the Figure 4 and Figure 5 depicts the generation of account number for the customer.

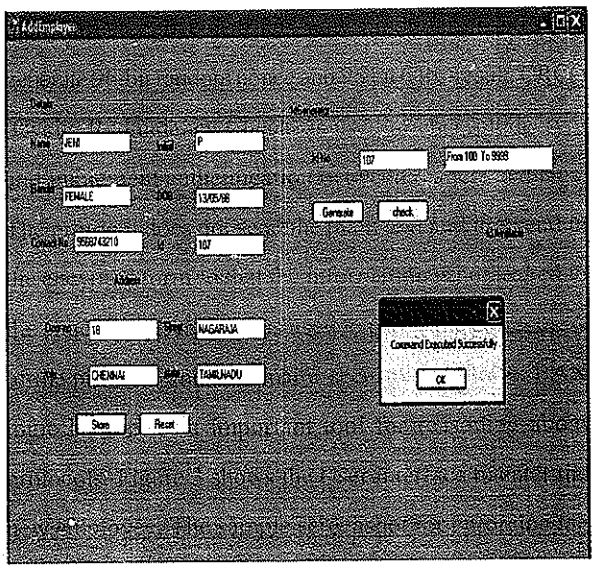

Figure 3 : Screenshot to add new employee

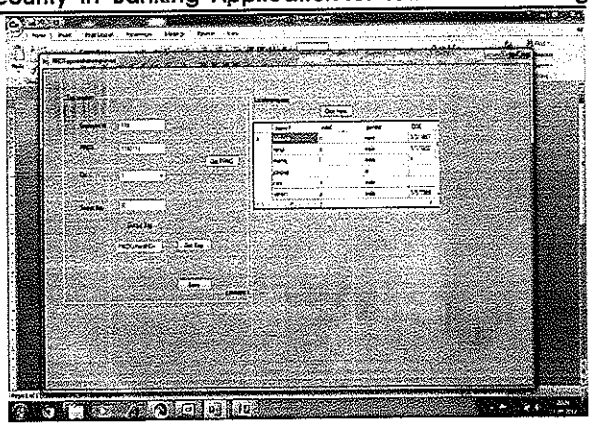

Figure 4 : Screenshot to generate tag which prevents cloning

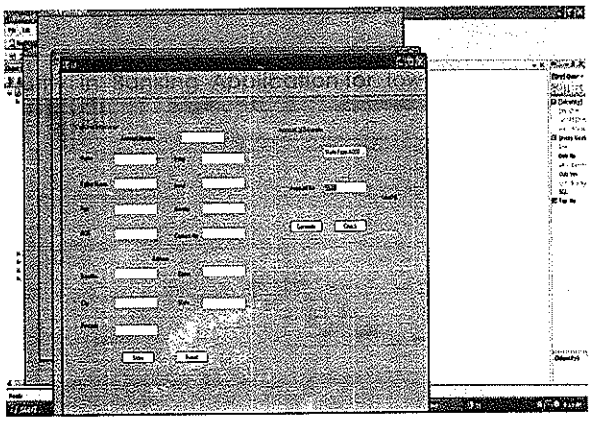

Figure 5 : Screenshot to generate account number for the customer

VIII. Conclusion

The level of security is less in EPC Gen 2 protocol and it is subjected to masquerade attacks and organization attacks. As a kind of formal analysis methods, BAN logic is used to discover the current attacks in cryptographic protocols and also to find out flaws expansively and intensely. There are four phases in BAN logic and they are Establishment of Idealized Model, Initiative Assumptions, Establishment of Security Goals and Protocol. It consists of rules like Message-meaning rule, Jurisdiction rule, Belief rule and

freshness rule. In this paper, we have designed a tag authentication protocol and shown that the proposed protocol do handle the identified threats (i.e., tag cloning).

REFERENCES

[1] Saeed Mehmandoust1 and Reza Ebrahimi Atani, 2010. APPLICATION OF PUF-ENABLED RFID TAGS IN ELECTRONIC BANKING International Journal of Computer Science & Information Technology (IJCSIT), 3(2).

[2] A. Juels, 2005. Strenthening EPC Tag against Cloning. ACM Workshop on Wireless Security (WiSe) .pp.67-76.

[3] P. Tuyls, L. Batina,2006. RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, Topics in Cryptology - CT-RSA 2006. Lecture Notes in Computer Science, San Jose, USA,February 13-17 2006. Springer Verlag.

[4] M Ohkubo, K Suzki, S Kinoshita. Cryptographic approach to *"Privacy-Friendly"* Tags. In RFID Privacy Workshop, MIT, MA, USA, 2003.http:// www.rfidprivacy. us/2003 /agenda. php.

[5] A Henrici, P Muller,2004. Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. 149–153.

[6] B Song, C Mitchell,2008. RFID Authentication Protocol for Low-cost Tags. In Proceedings of the First ACM Conference on Wireless Network Security .140-147

[7] S Weis, S Sarma, R Rivest, D W Engels, 2003. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C], In Proceedings of the First Security in Pervasive Computing. Berlin: Springer: 454-469.

[8] Datasheet Helion Technology, 2005. MD5, SHA-1, SHA-256 Hash core for Asic.http:// www.heliontech.com .

[9] Juels,2004. A.: Minimalist cryptography for low-cost RFID tag. In: Blundo, C., Cimato,S. (eds.) International Conference on Security in Communication Networks –SCN LNCS, vol. 3352, pp. 149-164, Springer, Heidelberg .

[10] Vajda, I., Buttyn,2003. L.: Lightweight authentication protocols for low-cost RFID tags.In: Workshop on Security in Ubiquitous Computing, Ubicomp.

[11] Tsudik, G,2004.Yet another trivial RFID authentication protocol. In: IEEE International Conference on Pervasive Computing and Communications, pp. 640-643.

[12] Mike Burmester and Breno de Medeiros, 2007.RFID Security: Attacks, Countermeasures and Challenges. http://www.cs.fsu.edu.

[13] Christian Floerkemeier, Roland Schneider, and Marc Langheinrich, Scanning with apurpose - supporting the fair information principles in RFID protocols, UCS, 2004, pp.214–231.

[14] EPC Global. EPC Tag Data Standards, vs. 1.3. http:/ /www.epcglobalinc.org/standards/EPCglobal Tag Data Standard TDS Version 1.3.pdf.

[15] Paul syverson,1991.The Use of Logic in the Analysis of Cryptographic Protocols. IEEE explore, pp. 156-170.

Author's Biography

A.Anny Leema, completed MCA., MPhil., PhD in Computer Science and working as an Assistant professor (Sr.Gr) in the department of Computer Applications in B.S.Abdur Rahman University, Vandalur, Chennai. She has 13 years of experience in teaching and has presented 12 papers in National Conferences and 9 papers in International Conferences. She has published twelve papers in the International Journals. Her area of interest is Data Mining, RFID-Wireless Identification Technology, Web Mining and E-learning.

Dr. M. Hemalatha, Completed M.C.A M.Phil., Ph.D., in Computer Science and currently working in Department of Computer Science, Karpagam University. Twelve years of Experience in teaching and published more than hundred papers in International Journals and also presented more than hundred papers in various National and international conferences. Area of research is Data mining, Software Engineering, bioinformatics, Neural Network. Also reviewer in several National and International journals.