Intra Debit Card System using RFID Technology

Senthil Kumar Mathi
Amrita School of Engineering
Amrita Vishwa Vidyapeetham
Coimbatore, Tamil Nadu, India

M. L. Valarmathi
Department of CSE
Government College of Technology
Coimbatore, Tamil Nadu, India

T Dhivya
Amrita School of Engineering
Amrita Vishwa Vidyapeetham
Coimbatore, Tamil Nadu, India

ABSTRACT

RFID - Radio-Frequency IDentification is one of the technologies that is used for the past few decades for tracking and identification of an object. RFID tag contains unique information wirelessly with computer databases and network for tracking the objects easily. Prior to performing the read/write operation on RFID card, the reader has to make an authentication check. Usually a default key supplied by the manufacturer is used to do the above. This poses a security threat; anyone can now access the contents of the RFID tag. For handling this security threat, we propose a mechanism involving where the RFID reader tag communication has been enhanced by making use of an identity based authentication technology which involves a third party's authentication. We intend to deploy this security mechanism of the RFID reader and tag access in the scenario of educational institutions; an internal debit card system could be set up. This is particularly beneficial for students of small age to be able to carry out transactions involving the purchase of their uniforms, bags, stationary and other requirements at school. Parents wouldn't have to worry about going in person to take care of their ward's monetary needs.

General Terms

RFID, Cryptography, Debit card system.

Keywords

Advanced Encryption Standard, Tag content access control, Identity based authenticated key exchange, Electronic Product Code.

1. INTRODUCTION

RFID has been employed for an object tracking and detection [1]. The RFID device provides the same function as a bar code or a magnetic strip on the backside of a debit card or ATM card; it gives a unique identifier for that object. And, just as a bar code or magnetic strip, the RFID device should be scanned to obtain the information about identification of the object. RFID devices have three major parts: a chip, an antenna, and a reader. The tag [2] is usually a chip attached to a product and restrains a unique identification number referred an Electronic Product Code (EPC). It includes application of concern to manufacturers, healthcare institutes, military applications, logistics suppliers, and retailers, or others that need to follow the physical position of wares or equipment. Every bit of details stored in RFID tags go together with items as they trek through a supply chain or erstwhile business process. The details on RFID tags, such as product features, physical measurements, charges, or laundering constraints, can be scanned wirelessly by a reader at high speed and from a distance of several meters. The reader of RFID is a piece of equipment with an antenna through which it communes with the tag. The different types of RFID readers are SL101, SL102, SL 801, SL500 etc. There are three main frequency bands are being used for RFID and they are as follows: 1) Low Frequency with 125/134 KHz - used for access control, animal tracking, and asset tracking. 2) High-Frequency with 13.56 MHz - applied for average data rate and read ranges up to about 1.5 meters. This frequency also has the advantage of not being prone to interference from the presence of water or metals. 3) Ultra High-Frequency with 850 MHz to 950 MHz – recommended for the longest read ranges of up to roughly 3 meters and high reading speeds.

Based on their power, RFIDs are classified as active, passive and semi-active [3]. Active RFID tags have their own internal power supply and hence the range of communication between the tag and reader increases. The range is about 8-10 meters. Passive RFID tags do not have their own internal power supply and hence the range of communication between the reader and tag is less. RFID device is no-contact, non-line-of-vision and hidden identification, which is dissimilar from omnipresent barcode identification system. Thus, it is hard to completely prevent the signals from being emitted from the tags. Tags [4] are put on pallets, cases, and individual items and they can be scanned between inches to meters for disclosing the EPC number. The following are the security threats related with RFID tag that has to be addressed while designing the system against any type of assails and threats:

Spoofing identity - It occurs while an assailant successfully poses as an authorized user of a system.

Tampering with data - Tampering of date happens when an attacker is trying for modifying, adding, deleting, or reordering the data.

Repudiation - Repudiation happens when users refuse a deed and no proof exists to prove that the deed was performed.

Information disclosure - Information disclosure arises when information is exposed to an unauthorized person.

Denial of service - Denial-of-service denies communication service to legitimate users. Denial-of-service attacks are easy to achieve and formidable to guard against.

Elevation of privilege - Elevation of privilege transpires when an unprivileged person or attacker gets higher privileges in the system than what they are authorized.

The following are the spoofing threats [5-6]. A robber carry outs an unauthorized record of a store by scanning RFID EPC tags with an unauthorized reader to determine the types and quantities of items. An unauthorized reader can query the tag

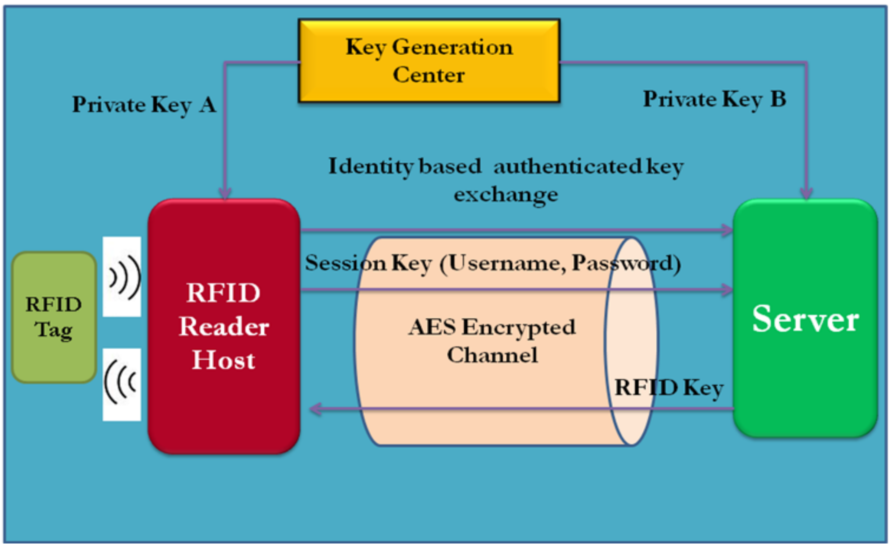


Fig 1: System Architecture

for the EPC number to use the RFID system since the majority tags used in the supply chain respond to any reader.

Nevertheless, the assailant can determine the manufacturer and possibly the product number since he knows the standard way of creating an EPC number. It is possible that the number allotted to all manufacturers will turn out to be public knowledge as well as the product number after some short period of time. The attacker determines which individual is allotted an EPC number by posing as an authorized EPC's. RFID presents a number of technology challenges. First, the organizations must deal with enormous quantities of data that is produced by reading tags on individual pallets, cartons, or high-value items. Additionally, they should employ fully-integrated software structural design that enables this data to be analyzed and made available to internal and external systems in near real time.

In this paper, we propose a framework to provide security in RFID based on identity based authenticated scheme which can be used to deploy an intra debit card system in educational institutions. In boarding schools, students leave the campus only during long holidays and vacations; they purchase all their stationary, snacks, household items etc from the stores within the campus itself. Our application's framework aids such an environment. It is built from a set of concepts linked to existing cryptographic methods and primitives.

2. ARCHITECTURE

2.1 System Architecture

Fig. 1 shows the overall design of the system architecture of our proposed method. It consists of RFID Reader Host which is the host system onto which the RFID reader is attached. It scans the contents stored on the RFID card. Authentication Server is responsible for storing all the RFID keys [14]. Corresponding to various RFID Cards which are read at the RFID Reader Host end, it also maintains the details of all the authenticated users of the RFID reader. Key Generation Centre (KGC) is a server which behaves like is a third party that authenticates the RFID Reader host and the Server for communications. Initially when the servers are up and running, both the RFID reader host and the server will send some unique detail of theirs to the KGC. The KGC verifies if the server and RFID reader host are authorized. If yes, it supplies private keys to each of them. Using Identity based authentication mechanism both the RFID Reader host system and the server will generate identical session keys. Using these keys, the RFID reader host will encrypt its username and password with Advanced Encryption Standard (AES) Encryption [7] and send it over to the server. The server will perform AES decryption on these using the same session keys, check in its database to validate the user. Once validated, the server will further encrypt its respective RFID key and send it to the host. At the host end, if the tag's key and the RFID key matches, the card contents will get unlocked and then can be read by the RFID reader. The hardware requirements includes SL 500 RFID readers of 13.56 MHz which are used for reading the cards, Mifare 1K RFID cards, two servers; one behaves as the KGC and the other as the Authentication Server. RFID reader host systems need to be set up at all locations within the school campus where the debit card system needs to be used.

2.2 Application Architecture

According to our application, we propose to build an intra debit card system in an educational institution which has the environment of a boarding school. Students leave the campus only during long holidays and vacations; they purchase all their stationary, snacks, household items etc from the stores within the campus itself. For such an environment, it would be very beneficial if we installed an intra debit card system. Our application software provides one such solution where we make use of RFID Reader-tag technology to ensure security in carrying out money transactions for all the purchases that the students were to make. Every student can be provided with an RFID card which can be debited and used for making purchases. Our security system ensures that no two people can use the same card. The cards will be laminated with the student's photo to ensure the identity. In case, the card is lost, a new card can be assigned and the old balance can be transferred into the newly assigned card.

3. IMPLEMENTATION

The system is implemented as an integrated form of the following modules:

3.1 RFID Reader Software Interface

The RFID Reader software interface is the process of requesting the tag id; each card has a unique Identification key called Tag id which is given by the manufacturer. This cannot be changed. The process involved in recognizing the tag id is by selecting the Com Port and Baud Rate.

3.2 Key Assignment To The Card

The Request Tag id has to be called again. Prompt the user to enter the old key (default) and the new key. Confirm the new key by re- entering it. Append the new key value with 'FF078069' and 'FFFFFFFFFFFF' in order to store the access bits and the key B value. Call the function 'rf_M1_authentication2 ()' with the old key. Once authenticated, write the newly assigned key into block 4 of all 16 sectors Now that the key of the Card has successfully been changed, store this value in the database.

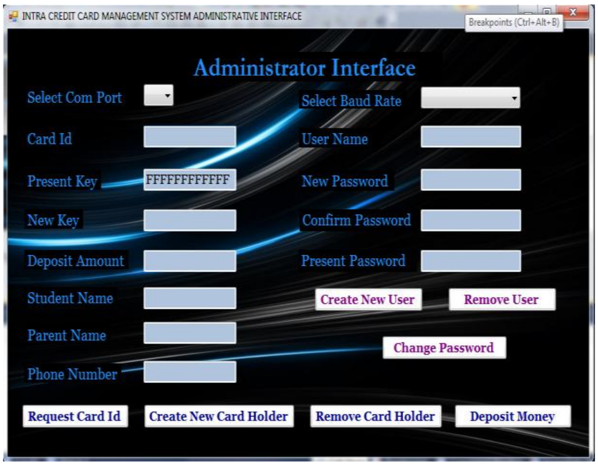
3.3 Adoption of encryption algorithm

In this module, AES encryption and decryption algorithm has been implemented for sending username and password between reader and server.

3.4 Interface Design For Administrator Responsibilities

There are different responsibilities for the Administrator (refer Fig. 2) each of which are explained below:

Create New User: This is to allow a new individual to use the Intra Debit Card application software. The admin will have to first enter the new user's name and a password for his account. This password has to be re-entered for confirmation. All the details are updated in the shopkeeper table.



Present Key FFFFFFFFFFFF

Fig 2: Admin interface

Remove User: This responsibility is to revoke a user from further using the application software. All the details are removed from the shopkeeper table.

Change User Password: This is to change the password of an existing user of the software. The username, old password and new password have to be entered. The confirmation is made for given password. All the details are updated in the shopkeeper table.

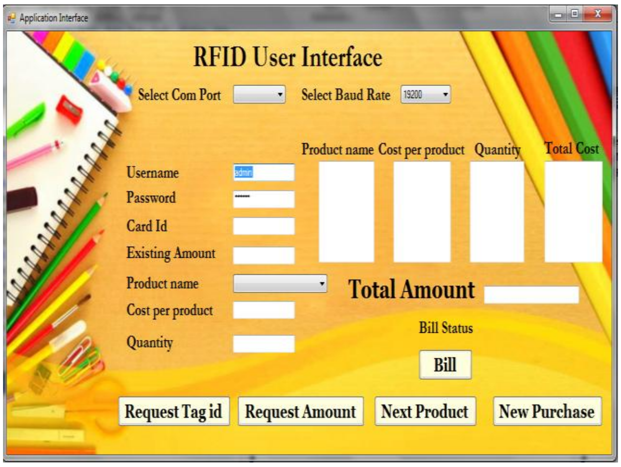
Create New Card Holder: This option allows you to create an account for a student to use a card. For this first you must enter his details into the textboxes provided for Student Name, his Parent's Name, and Phone Number. At the back end, key change occurs as explained in section 3.2. Also, all the details are updated in the student table.

Remove Card Holder: This is to remove a card holder from the intra debit card system. You need to enter the card holder's name. At the back end, key is changes to the default key. Also, all the details are updated in the student table.

Deposit Money: This is to deposit money into the account. Parents or guardians will have to deposit the money at the school administration department and give the username. The Admin will enter the Student's name and the amount in 'Enter Deposit Amount'. The amount is written into the card. Also, all the details are updated in the student database.

3.5 Application Interface Design

The RFID user interface design is shown in Fig.3. The user has to enter the username and password. Once the amount is requested, the following background processes occur. The RFID Reader host system and the server separately send their MAC addresses to the KGC for receiving their unique private keys for further key exchange [8-11]. Upon receiving the private key, the host and the server exchange keys as described in section 3.4. At the end of the key exchange based on identity based method [12], both the host and server obtain the same session key. This key is used to perform AES encryption to send the RFID Reader user's username and password and the card id to the server. At the server end, these credentials are decrypted and the user is authenticated.



Select Baud Rate 19200

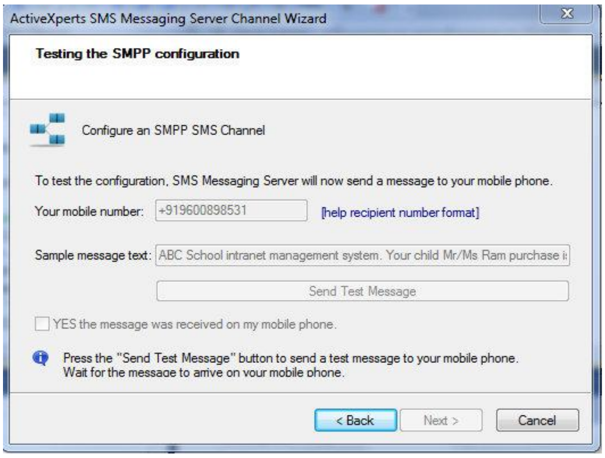
Username admin

Fig 3: Application Interface

The RFID key corresponding to the card is retrieved from the database then encrypted message sent back to the RFID Reader Host. This RFID key is decrypted at the host and is used for authenticating the card for reading purpose. The balance amount which is present in the card can be read and displayed on the GUI. The name of the product that is being purchased is given as input. Its cost is picked internally. If there are more items being purchased after entering the quantity of purchase, then they are given as inputs. At the end, the following background processes occur after requesting for a bill as shown in Fig. 4. The total bill falls within the balance present in the card, the bill status will appear as 'Bill produced'. The bill amount will be deducted from the card balance. The latest balance amount is written into the card.

4. CONCLUSION AND FUTURE ENHANCEMENTS

Our framework is an Intra Debit Card System using RFID technology which can be used in educational institutions. It allows students to pay for their daily supplies using a security enhanced RFID card. Unlike the existing, RFID encrypted using AES encryption and sent to the server where it is decrypted and updated in the database. Also from the server, the message and the email are sent to the child's parent's mobile number and email id respectively.



ActiveXperts SMS Messaging Server Channel Wizard

Testing the SMPP configuration

Configure an SMPP SMS Channel

To test the configuration, SMS Messaging Server will now send a message to your mobile phone.

Your mobile number: +919600898531

Sample message text: ABC School intranet management system. Your child Mr/Ms Ram purchase i:

□ YES the message was received on my mobile phone.

Press the "Send Test Message" button to send a test message to your mobile phone.
Wait for the message to arrive on your mobile phone.

Fig 4: Successfully sent message's interface

If the bill amount exceeds the card balance, the bill status will show 'Bill failed'. Thus the purchase cannot be made. In this work, we have employed identity based authenticated key exchange mechanism involving third party authentication; hence providing enhanced security such as resilience to man-in-the-middle attack and ephermal key compromise, perfect forward secrecy, and known session key. This system provides an advantage for children; they are not required to keep money with them. Their needs can be taken care of in a safer manner. Sending a message to the child's parents after every purchase that they make at the school store is another added advantage. Thus, the parents are well informed of the card balance and purchases made. As part of future work, we need to address the issue of transferring the balance in a lost card into a newly replaced card. In this way, in case of misplacing a card, the money in it can be retrieved.

5. REFERENCES

[1] A. Juels, RFID Security and Privacy: A research Survey, IEEE Journal on Selected Areas in Communication, Vol.24, No.2, February.

[2] Liang Yan and Chunming Rong, Tag Content Access Control with Identity-based Key Exchange, ICNAAM Numerical Analysis and Applied Mathematics, International Conference, pp297-300, 2010.

[3] Jatin A Kanzaria, Maulik J Kapuria, Niket D Shah, Rahul A Tibrewal, Project report on Smart Office - A Complete RFID Solution, 2006.

[4] Vogt, H. Efficient Object Identification with Passive RFID Tags' International Conference on Pervasive Computing, LNCS, Springer-Verlag 2002.

[5] Raza N, Bradshaw V, Hague M, Applications of RFID technology, IEEE Colloquium RFID Technology, Page(s): 1-5. 1999.

[6] A book on Attacking RFID Systems by Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Auerbach Publications, 2009.

[7] A publication on Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information, Processing Standards Publication, November 26, 2001.

[8] W. Diffie and M. Hellman, New Directions in Cryptography' IEEE transactions on Information Theory, pp.644-654, 1976

[9] Christoph G Gunther, and Asea Brown Boveri, An Identity-based key exchange protocol, Springer-Verlag, 1998.

[10] V. Cakulev, G. Sundaram, and Alcatel Lucent, IBAKE: Identity-Based Authenticated Key Exchange, draft-cakulev-ibake-04.txt, April 20, 2011.

[11] Vaibhaw Dixit, Harsh K.Verma, and Akhil K. Singh, Comparison of various Security Protocols in RFID, International Journal of Computer Applications (0975-8887), volume 24- No.7, June 2011.

[12] Li Xiaoyong and Zhang Hui, Identity-based Authenticated Key Exchange Protocols, IEEE pp.V3.85-87, 2010.