Enhancement of Security with Dynamic Auditing

A. Arthi[1]
Department of Computer science and Engineering
Anand Institute of Higher Technology, Chennai,

P. Deekshitha[2]
Department of Computer science and Engineering
Anand Institute of Higher Technology, Chennai,

R. Elakiya[3]
Department of Computer science and Engineering
Anand Institute of Higher Technology, Chennai,

***Abstract*—RFID is a wireless device which is used for identifying objects, data and people in an effective way. In number of applications Radio Frequency Identification have been used for past few decades and have been implemented in various environment, but it is very challenging to fight against access control system due to reasons such as stolen or unauthorized duplications of the Smart cards. Other techniques to overcome this is to use bar code detection but bar code readers are sensitive device which are not capable of detecting barcodes with stains and scratches and it is not foolproof. Our proposed system overcomes this problem by generating One Time Password every time when the Radio Frequency Identification card is detected. When the radio frequency identification card is encountered within the radiation, one time password generates for every micro electrical mechanical system axis rotation by reading the IMSI (international mobile equipment identity) number. In the proposed system 97 percent high accuracy rate among users is obtained.**

Keywords: Radio frequency identification, smart card authentication, one time password, micro electrical mechanical (MEMS) sensor.

I. INTRODUCTION

Network security consists of provisions and policies adopted by a network administrator to prevent from unauthorized user or unauthorized access to data. Involves the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password or other authentication information this allows them access to their information andwithin their authority. Network security covers large variety of computer networks,both public and private, that are used in everyday life conducting transactions and communications among businesses, and individuals. Networks can be used in private, such as within a company, and others which might be open to public access. Network security is involved in organizations, and other types of institutions. It secures the network, as well as protecting operations being done. The most common and simple way of protecting a network resource is by assigning the unique name and corresponding password.

In modern era automatic teller machine is essential part of our life. Automatic teller machine is a currency dispenser it includes smart card reader and transaction details through message to mobile phone. The smart card reader can read data from a radio frequency identification card [1]. The card reader, such as radio frequency, can be located so as to provide additional space for another transaction component. The smart card includes housing for the RFID tag reader that is adapted to prevent interception of radio signals and a Global System for Mobile Communication modem which helps to send text message for every transaction. In this project, when consumers usages their card for the transaction, after the transaction a corresponding message about the transaction will sent to the mobile no which was registered by the consumer. In existing system it reads user details by magnetic tapes or bar. In proposed system we introduced radio frequency identification card. It automatically reads the data and information of authorized user.

In general, authentication methods in a smart card systems can be divided into two broad categories. The first category is based on mechanical matching, such as keys and combination locks. Individuals are authenticated in these access control systems if and only if the blade of the key matches the key of the lock or the correct numerical sequence for combination lock has been dialed. Due to the physical constraints of mechanical matching systems, they are insufficient to meet the demanding requirements of access control authentication for critical infrastructures. On the other hand, it is also very hard to frequently change the interior structure of such matching mechanisms for security enhancement. The other category of authentication for access control systems is electronic authentication including barcode [2], magnetic stripe, biometrics, and so on. Compared with mechanical matching authentications, the electronic authentications such as radio frequency identification-based smart card offer much more convenience and flexibility for both administrators and users of access control systems.

II. RELATED WORKS

A. Global system for mobile communication

GSM, which stands for Global System for Mobile Communications, the world’s most widely used cell phone technology. Cell phones use a cell phone service carrier’s global system mobile communication network by searching for cell phone towers in the nearby area. Global system for mobile communication is a globally accepted standard for digital cellular communication

The mobile station consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and a smart card called the Subscriber Identity Module. The SIM provides personal mobility, so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. By inserting the SIM card into another Global System for Mobile communication cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity. The SIM card contains the International Mobile Subscriber Identity, identifying the subscriber, a secret key for authentication, and other user information. The details inside SIM card may be protected against unauthorized user by setting a secret password or personal identity number. The central component of the Network Subsystem is the Mobile services Switching Center [3]. It acts like a normal switching node of the Public Switched Telephone Network provides all the functionality needed to handle a mobile updating, handover.

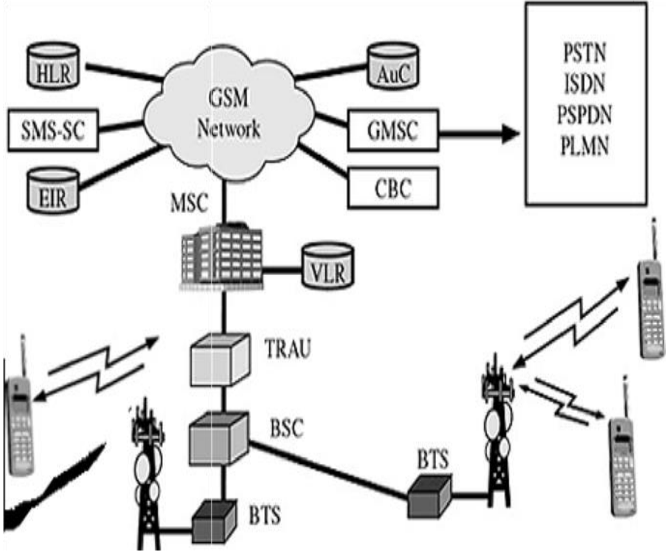

Fig1: diagram for Global System for Mobile Communication

SIM card contains International Mobile Subscriber Identity is used to identify where the user is exactly with the help of Subscriber Identity Module card. And it is used to send text messages to the authorized user.

B. Radio frequency identification

It is used for identifying and tracking the details using radio signals. Radio Frequency Identification system consists of Radio Frequency Identification cards, a means of reading or interrogating and a means of communicating the data to computer or information managing system[3].

This system will sends the radio signals from radio transmitter and radio frequency receivers receives these signals and checks the details whether the authorized user is using the smart card with radio frequency. There may also be present antennas for communication between the smart card and the reader.

C. Radio frequency identification reader

Radio Frequency Identification reads data with the help Radio Frequency antennas at a certain frequency range. The reader is electronic devices which transmits and receives a radio signals. The antennas has a reader which is attached, the reader translates the smart card radio signals through antenna. The antenna within a reader generates an electromagnetic field, when smart card with radio frequency is present near this electromagnetic field the data or information stored on the chip in the smart card is get transfer to reader[3]. Radio frequency Identification card comes in different ranges of forms and vary in radio frequency and storage capacity. Here low-frequency 125 KHZ RFID cards are used to identify a user, which is fast and does not require contact between reader and the tagged. It is used to provide unique identification that allows for wide range of applications RFID cards can be read very quickly also they can be read in all types of environment[6].

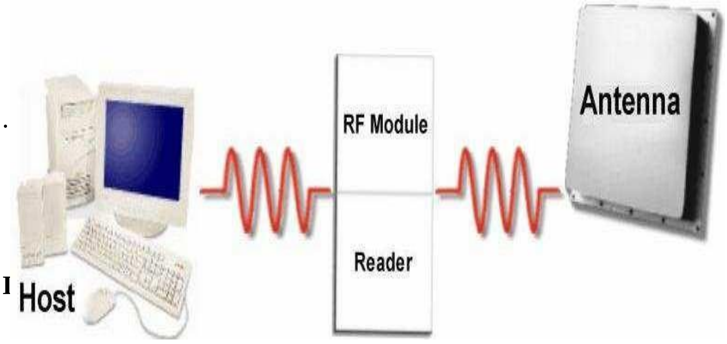

Fig2: Radio frequency identification

III. EXISTING SYSTEM

Magnetic stripsor barcode technology is most commonly used in existing smart cards. In magnetic stripe, when the person swipes his card into the Automatic teller Machine, the Automatic teller machine captures the card information which is placed upon the readers. Once the customer swipe the smart card the system automatically and continuously collect information.

In existing system first a user needs to swipe the card after swiping the card it will ask for password then the user needs to type the password, if only the password matches it will proceed further transaction. The password which has been entered by user will displayed in encrypted form.

In existing system Advanced Encrypted algorithms used for encryption [2]. It encrypts the password entered in keyboard. It verifies the details of the user and performs transaction.

Drawback:

The main drawback is that the user comes to know the balance amount in the card only at the time of swiping the card in the machine. If the barcode in smart card damaged user cannot access the transaction [5].

If the user does not punch the PIN (Personal Identity Number) properly he is given three tries utmost. If he fails in all of the four attempts, the card is locked [7]. If the user succeeds in any of the attempts he is allowed to access the system. This makes the system more secure and less prone to anonymous usage. In existing system the password can be easily hacked or it can be used by unauthorized user. The main drawback in existing system, barcode or magnetic strips are sensitive electronic device which are not capable of detecting barcode with strains or scratches. If barcode damaged it cannot proceed for next transaction.

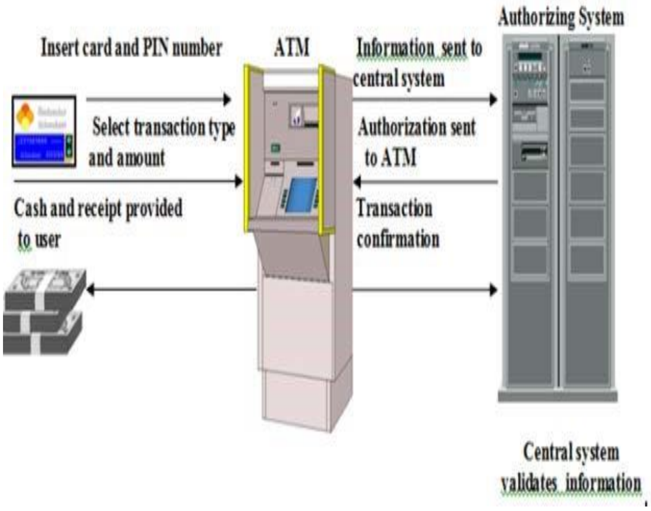
Insert card and PIN number
ATM
Information sent to central system
Authorizing System
Select transaction type and amount
Authorization sent to ATM
Cash and receipt provided to user
Transaction confirmation
Central system validates information

Fig3: Block diagram for existing transaction

IV. PROPOSED SYSTEM

Proposed system we have created the new generation machine which can be accessed by Radio Frequency enabled smart card with 3D position based key generation[1]. Working of RFID card with gyroscopic sensor. When a smart card is rotating in 3 dimensional position it automatically sensed by gyroscopic sensor and generates the password to mobile.

When we rotates Radio Frequency Identification smart card in the reader unit of the machine it transfers the unique ID with position based generated key to the server. In server we can collect the related information of the unique ID with position key and verifies the users account details, their photo etc.

If it get verified One Time Password will generate and using MAC implementation. One Time Password will be sent to requested user as Short Messaging System. It will provide Integrity checking option to check the integrity of One Time Password received only then user can use this one time password for selecting bank from multiple list of banks provided over there.

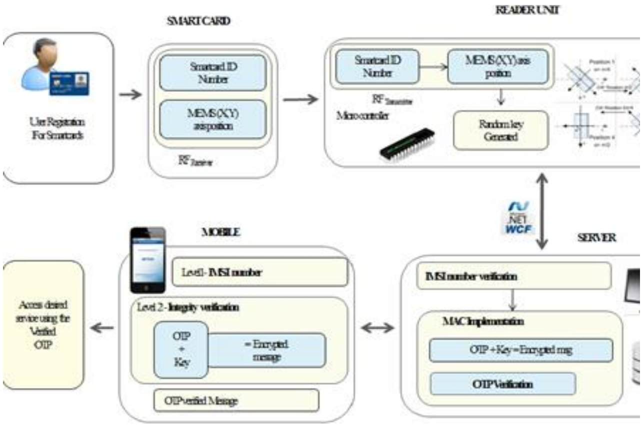

Fig 4: Block diagram for proposed system

The major advantage in this is that the same card can be used for all types of transport for fare deduction, provided the card reader is installed. Some features of smart card:

1. **Security**: Security is provided by using various encryption Algorithms and the information which is stored on the card can be accessed only by using a PIN (Personal Identification Number).

2. **Intelligence**: The smart card is not only used for storing data but for processing data also. Communication with the devices can be done through a smart card reader. Also the information and applications can be updated easily without using a new card.

3. **Convenience**: Smart card provides a portable and easy to use platform in such a way that most of the people are familiar in using the card.

V. IMPLEMENTATION

A. Smart card access

The User can register with server then user can login with Smart card ID which has to be generated number by server. Radio frequency transmitter can verified with radio frequency receiver that has to be generated Smart card ID or not apply for authentication. Once Smart card ID is Verified then receiver can check and radio frequency Reader can perform read operation. Both should be verified, smart card ID number and Position also checked by server.

B. Position based key generation

The position based rotation can be generated by server this can verify the position of smartcard. The Micro Electrical Mechanical Sensor will sense the position based on the x axis and y axis. If the position of the card is correct then a Random key is generated using random key generation algorithms like Advanced Encrypted System.The Random key also verified with server.

C. Key verification

After the position can be checked by server the random key generated which can request by user that should be sent by Short message service. The one time password can request once the key can be verified Encrypted message should match with server's encrypted message .

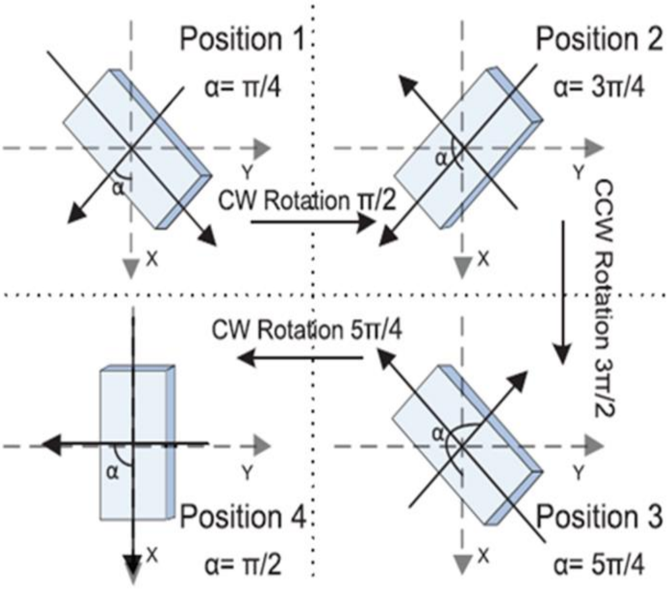

Fig4: smart card position

The user will receive one time password and Key through Short Messaging System to mobile. The one time password should be verified before it is used by the user to avail the desired service. So the user will encrypt the one time password with the key, which received in Short Messaging System. If the encrypted message is same as in server then one time password is authenticated to use it.

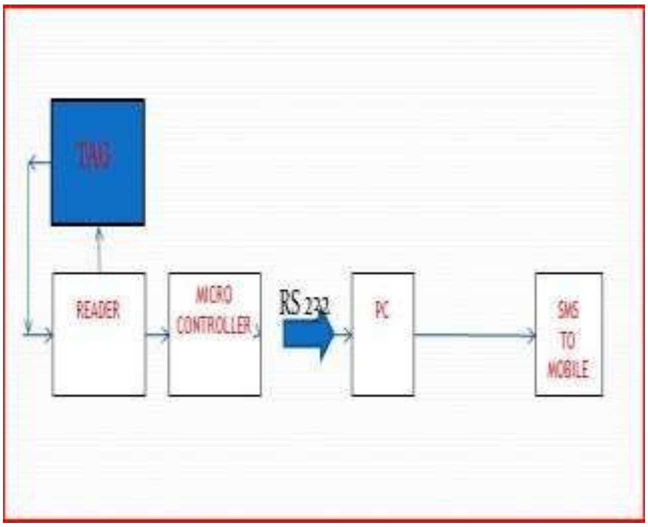

Fig 5: Key generation to mobile

V. CONCLUSION AND FUTURE WORK

In this system we are integrating both RFID and smart card to provide wider boundaries and effective solutions in secured authentication. The features of RFID tag such as security, intelligence and convenience provides users a highly secured transaction. The smart card system for secured transaction system can be used to improve the security by reducing the cumbersome efforts spent in mechanical authentication. The system can be improved by increasing the range of reader in which the tag can be read is a very large scope for future work in our system. This system can be further enhanced by using Biometric Techniques such as finger print authentication that provides user more secured access.

REFERENCES

1.Dynamic Authentication with Sensory Information for the Access Control Systems Yuanchao Shu, Student Member, IEEE, Yu (Jason) Gy , Member, IEEE, and Jiming Chen, Senior Member, IEEE.

2. An Energy Efficient ATM System Using AES Processor Ali Nawaz*1, Fakir Sharif Hossain2, Khan Md. Grihan3 1Department of Electrical and Electronic Engineering International Islamic University Chittagong, Dhaka, Bangladesh

3.RFID & Mobile Fusion for Authenticated ATM Transaction Kopparapu Srivatsa ECE/SEEE SASTRA University Madamshetti Yashwanth ECE/SEEE SASTRA University

4.RFID Based Security System K.Srinivasa Ravi, G.H.Varun, T.Vamsi,P.Pratyusha

5. Universally Composable RFID Identification and Authentication Protocols MIKE BURMESTER Florida State University, Tallahassee TRI VAN LE and BRENO DE MEDEIROS Google, Inc. 1600 Amphitheatre, Parkway Mountain View

6. Karamdeep Singh Gurmeet Kaur ‘Radio Frequency Identification: Applications and Security Issues’ IEEE Second International Conference on Advanced Computing & Communication Technologies 2012

7. Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, Senior Member, IEEE, and Li Xu, Member, IEEE