RFID AND GSM synthesis for authenticated ATM transaction

Deveshree Zawar ECE/SAOE PUNE University

Shruti Ranjalkar ECE/SAOE PUNE University

Zain-ul-Abedin ECE/SAOE PUNE University

V.A .More Professor/ECE/SAOE PUNE University

ABSTRACT:

The main objective of this project is to develop an embedded system, which is used for security applications. In this security system we give access to the authorized people through the RFID tags and mobiles using GSM technology. The system is programmable we can change the data of the authorized people in the data base of the embedded system. This paper suggests for a technical innovation which aims at preventing all the financial fraud. Today, we are living in the 21st century. Money and internet have become the primary needs of a human being. The existence of cards mobile/net banking has made our work easy and convenient. Every coin has two sides, and there lies an inertial threat, security. Today, we deal with a transaction in hardly few seconds. It is just that we need the related account information. But there are frauds existing which can hamper an individual's life. Hence, our tech innovation –"**RFID & GSM SYNTHESIS FOR AUTHENTICATED ATM TRANSACTION",** will prove fruitful to avoid such financial frauds.

1. INTRODUCTION:-

The aim of this project is to revolutionize the ATM security system in developing countries like India where the existing system is already stressed and prone to frauds. In present scenario Internet is playing very essential role in the online business. Today, E-commerce application is widely used in E-business and various kinds of service industry where all kind of transaction of data is made possible through internet. It is one of the best, cheapest and convenient processes for online business. Privacy and security is the basic concern in this kind of transaction. Privacy is handled by cryptography but for security we have to apply techniques which are necessary to secure our transaction and the digitized data present in these transactions. In the consideration of ATM, there are different aspects that should be considered. First, one has to have an idea about the communication within ATMs. Second, the issue of security is of paramount importance because all over the world, there is an increasing use of ATMs and so the risks of hacking turns to be a reality more than ever before. The Personal Identification Number (PIN) has been of very great importance in the overall operation.

RFID and GSM module form the core technology with an ability to deliver embedded information in a tag without any physical contact. The various transactions in logistic companies and banking institutions contain sensitive information in the form of data. Hence, there must be a unique technique to be applied on these financial transactions. With this we

IJSER

achieve the primary goals of security. SIM 900 is a quad band GSM/GPRS module which is very useful for data transactions applications. It integrates TCP/IP protocol and provides all hardware interfaces between the module and the boards.

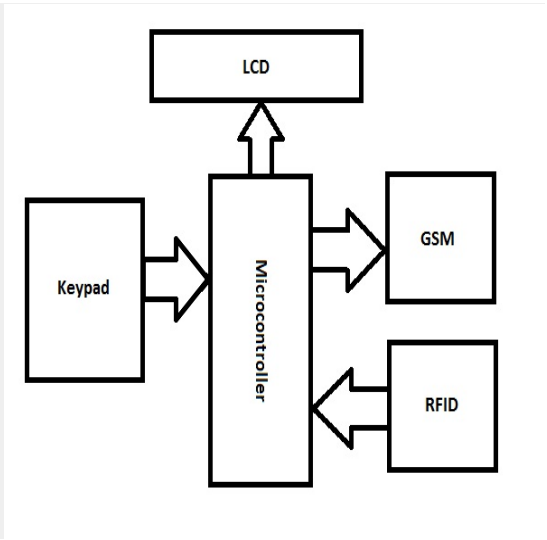
2. BODY:

The function of ATMs is to deliver cash in the form of bank notes and to debit a corresponding bank account. Cards were used to identify the user. As for the withdrawal of money, different methods were used. For instance, punched cards were used. By the use of such cards, only one payment was authorized. Thereby, a user had to get a supply of cards from his/her bank because the punched cards were not returned to the user. Another example was the use of a magnetic card which had a limited life. The use of such cards allowed; for instance, twenty withdrawals of money.

3. METHODS AND RESULTS:

In the modern transaction scheme, there is no way to identify the owner of credit/debit card. We face this most common issue to recognize the true owner of the card. Any stolen card can be used to make purchases using online system (swipe system). This proves to be a threat & potentially affects the user. It has also become easy for the fraudsters to successfully tap ATM card inserts, capture owners PIN using micro-cameras or mock keyboards. The main objective of our novel invention is to safeguard security of ATM transactions. The main purpose of this scheme is to provide a database for RFID card, & to identify the RFID reader & provide a dynamic password for secured transactions.

The basic block diagram of proposed methodology is given in fig.



The working principle is as follows:

When RFID card is brought into vicinity of ATM, the card reader verifies the details of card holder with the database. Then the information like (account no.) is sent to microcontroller. With this verification the uniqueness is checked & a message is sent to card holder whether to proceed the transaction or not. This is done with the aid of RT system, i.e. GSM module.

A typical RFID sys is made up of 3 components:

i) Tags

ii) Readers

iii) Host computer system.

An RFID tag referred to as a smart tag consist of a transmitter & responder. It comprises of a simple silicon chip mounted on substrate. The responder memory is used for data storage & response via communication. These tags can be active or passive depending on presence of battery. These tags identify the

IJSER

customer details. The readers called as “scanner” send & receive RF data to & from the tag via antenna. These provides the means of communicating with tag & facilitating data transfer using Command Response Protocol the readers help in verifying the genuineness of the details.

The contactless card reader can read data from an RFID tag of a customer's ATM card. The contactless card reader, such as an RFID tag reader, can be located so as to provide additional space for another transaction component. It can also be used in conjunction with a magnetic stripe card reader. The ATM includes housing for the RFID tag reader that is adapted to prevent interception of radio signals. The ATM is able to prevent dispensing of currency in situations where unauthorized detection of signals is sensed. Security password is entered through the keypad. When you enter the correct password then further transaction is proceeded otherwise it will be terminated. In this project, when consumers use their card for the transaction, a corresponding message about the transaction will be sent to the mobile number which is registered by the consumer.

The prime requirement is the ability to uniquely identify things & entities. This purpose is served by the RFID technology along with maintaining user’s confidentiality under any situation. The GSM module functions as a network that consists of several functional entities whose functions & interfaces are defined. This network comprises of various subsystems, stations, and registers necessary for communication. This module helps us in providing the customer the corresponding dynamic password which is generated. This provides an additional level of security.

3.1 RFID

The RFID works at different frequencies each determining the range of its operation. The card can be of active type, passive type or Battery Assisted Passive (BAP) type. This classification is according to the type of energizing the card employs. Reader on the other hand is classified based on its source of energy either AC or DC. For the implementation transmitter and receiver circuit is used to resemble the operation of the card and reader pair.

The RFID reader has the following modules:

1. Transmitter module consisting of a transmitting antenna.

2. Receiver module consisting of a receiver antenna. Distance of separation between the transmitting and receiving module depends upon the type of antenna used.

3. Microcontroller to get the count of the RFID tags used.

4. It has a RS232 interface to communicate with external devices

3.2 AT commands

AT commands are also known as Hayes AT commands. There are different views to understand the meanings of "AT". Some call it "attention telephone", whereas others interpret it as "attention terminal" commands. AT commands allows giving instructions to both mobile devices and ordinary landline telephones. The commands are sent to the phone's modem, which can be a GSM modem or PC modem. AT commands can be used for

operations that are usually done from the keypad, for instance calling a number, sending, reading, or deleting an SMS, setting the SMSC number, looking for a GPRS access point, reading and deleting phonebook data, reading the battery status, reading the signal strength, and so on. AT commands allow giving instructions to both mobile devices and ordinary landline telephones. The commands are sent to the phone's modem, which can be a GSM modem or PC modem. When you want to make a pc-based application to interface a mobile phone using USB, IR or Bluetooth, these commands are needed to communicate with mobile phones. Basically AT commands work on devices that have a built-in GSM modem.

3.3 GSM Module

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit random number (RAND) is sent to the MS. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber. The individual subscriber authentication key (Ki) is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases as previously described. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure indicated to the MS. The calculation of the signed response is processed within the SIM. This provides enhanced security, because the confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

4. CONCLUSION:

The overall implementation outputs us a secured and authentic transaction achieving goals of privacy. The only investment is in the RFID & GSM system which is one time and with less maintenance. This proposed system is suitable for several practical applications which are used in financial transactions for application of user identity and prevention from ATM frauds. Hence, our innovation ensures to solve the aspect of ATM security to a large extent. In addition to this the project can be expanded for future scope using more parameters like fingerprint, face recognition. The system can be enhanced using watermarking, card cloning and wireless technology.

5. REFERENCES:

1) Divya Singh, Pratima kushwaha, priyanka chaubey, abhishek vaish & utkarsh goel, ” A Proposed frame work to prevent financial fraud through ATM card cloning”, World Congress On Engineering (Vol1), London, UK.
2) Yiannis Hatzopoulos,” Teller Pass”, Scientific Engineering Services, GR57400, Greece.
3) Devinaga Rasiah,” ATM management and risk controls”, European journals of Economics, Finances and

Administrative services, Issue 21, 2010.

4) Antonella De Angeli, Lyne Coventry and Graham I. Johnson, "ATMs adoption in developing countries: Déjà vu or not?" Advanced Technology and Research, NCR Financial Solutions Division, UK.

IJSER