



Analysis of RFID Based Vulnerable Authentication & Entrance System

Sumair Masood Khan *

Sir Syed University of Engineering and Technology

ABSTRACT

To preserve the structure or premises from any intrusion or unidentified person is now getting significance around the globe. The entrance system would help preserve the structure from intrusion, based on the Radio Frequency Identification technology, the system would recognize and allow only those who are verifiable to the system. The system would only allow entrance upon swapping the Radio Frequency Identification card and verification of Radio Frequency Identification tag number with one of the stored in a database. The identity of the person would be showed on the display screen. In this paper we are given the working of the framework and execution of Radio Frequency Identification card. The intention of this study is taking into account framework is exceptionally temperate and shoddy. In spite of the fact that the expense of the framework is low however because of minimal effort the polish is traded off. Because of restricted spending plan the gate was chosen, however glass entryways or vigorous stainless steel structure could be utilized. Moreover the framework is sufficiently solid to keep anybody from interruption.

Keywords : Radio Frequency, entrance, safeguards

*The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (IBT) or Karachi Institute of Power Engineering.

¹ Sumair Masood Khan : angelsperiod@gmail.com

© JICT is published by the Institute of Business and Technology (IBT).
Ibrahim Hydri Road, Korangi Creek, Karachi-75190, Pakistan.

1. INTRODUCTION

The decline of law and order situation in the country has raised the security concerns of residential people as well as that of commercial and business organizations, thus forcing them to opt for safety and security measures. Whether be it monitoring system powered by closed cameras, secure entrance system or else. Be it private premises or authorized access zone, there is need of a physical secure entrance system to avoid intrusion or access by an unauthorized person. The commercial offices or services centers, there are rooms that are specified for particular use, which needs to be guarded and managed by biometric identification system, card system or security guard or any other means of security barricade. Secure access systems enable only authorized workers to enter buildings or specific zones/premises, inhibiting any unwanted visitor to pop in unannounced (M. U. Chowdhury, 2007).

There are numerous levels of security in the field, from the tag or pass code securing access to the more advanced tracking device or smartcard, conservation the premises from unauthorized access. Conventional security systems need costly equipment or a guard to manage building entrance or other desired area entrance, for blocking entrance of potential intruders. Smartcards, convenient solution to the problem, hold a large volume of personal information of staff like canteen spending, entrance and exit times but is expensive. Therefore, it is desirable to have a security system to provide low cost and effective security and management system of the entrants. A security and management system which bar trespasser due to the lack of access privilege there, needs to be restricted, because of secure and private nature of the building or specific premises. Therefore, the objective of the project is to build a secure entrance system that physically bar unauthorized personal or intruder from access or intrusion in the building or specific premises. The said Secure and Authentic Entrance System (SAAES) would help barring unidentified personnel from entering the premises of the said building. Radio Frequency Identification Device (RFID) would be used to recognize the person entering the building premises (G. B. Brandao, 2008). The entry system would have mechanical support to disallow any intruder. The mechanical and physical structure would stop any trespassing as the turnstile would only allow trespassing once the identification of radio frequency is matched with the one stored in the database integrated with computer system. Frequency Identification (RFID) systems are a common and useful tool in manufacturing, supply chain management, and inventory control . The security key would be a RFID based card to identify the person wants to enter (Desmedt, Y. Major,1998). Where the signal from the RFID tag would be sent so that it could be matched, with that stored in the database in the Computer system. The system would be controlled by a Microcontroller to allow or disallow the entrant, based on the identification verification process with the identity of the authorized person resides in the database. The microcontroller used is Arduino® uno Microcontroller, programmed to

2. Literature Review

Stigall discusses a security system which he called asset sub system, the description of the system is as follow; the said authenticating system would be consisting of a controller that would ultimately help the system in triggering an alarm. The system Stigall called asset sub system is based on RFID for identification. The RFID system would also be equipped with transceiver that will help the system to communicate with RFID tag via a signal. Here the RFID tag is connected with an asset, the second signal would be accepted, sent in reply to the first signal with the help of very same transceiver. In addition, along with transceiver the said sub system would also be equipped with a controller in order to regulate if the RFID tag is unable to communicate the subsequent signal to the transceiver and activate the alarm in reaction, which shows that Radio Frequency Identification tag fails remain unsuccessful to connect the subsequent signal to the transceiver (Bringer, J., Chabanne, 2005). Gates discussed another type of security system; a redundant security system that is also Radio Frequency identification tag for identification for the transmission of security sensor data. The Gates Security system is doubled layered security system as the radio frequency identification failure to transmit the security sensor data, a backup photoelectric cell or photocell-powered transmitter, stimulated to ensure and strengthen the security, to communicate security sensor data to a monitoring station. The presence of first layer radio frequency identification tag lets surveillance from a distant location of at least one of an opened/closed and a locked/unlocked state of the door of the security safe (asset) (Gates, 2013). In this paper we discussed, out of numerous structures and means of control, their system of access control that provide access control module that is based on two parts; one they called base and the other as update. Electric coupling is used here; the update is coupled to base by the means of an electric connector. Thus with the combined methodology of the base and update, the process of access control is done efficiently (Bussard, L., Bagga, 2013). Cecil discussed the method and mechanism of determining the intrusion and intervention; the system is based over two floors; an above ground and the underground. The system is meant for the purpose of checking, watching or surveillance the intervention or intrusion into a security premises or zone. The system is equipped with one or more than one transceivers that will help in a manner that communicating a unique electromagnetic signal would take place, in return it would trigger a response from Radio frequency Identification transponders. The communication of each transponder to the transceiver would be with an exclusive code that will show that no intrusion is marked in the vicinity of the transponder. If the transponder does not receive a signal carried out by transponder, it would represent intrusion or intervention activity (Carluccio, D., Kasper, 2006). Yet another security system is being

discussed by Cecil; an Intrusion detection system. The system is a little bit complex with power transmission cable establishing an electromagnetic field that will let each Radio Frequency Identification tags transmit a signal in normal circumstances. If any intervention or intrusion occurs, it would be find out by the system because of disconnection of either power transmission cable or data transmission cable (Carluccio, D., Kasper, 2006). To discussed the mechanism in this research paper for the assembling of the security system for security of premises or building. The system comprises of Radio Frequency Identification reader and a Radio Frequency Identification transponder and controller synchronized with an alarm system automatically triggered when needed. There is being placed an intrusion-detecting sensor for finding any interruption. A battery may be used with the transponder whereas the power may also be acquired by Radio Frequency Identification reader. One or more than one controller may be attached with the system (W. Zhang, 2009). Kim and Jun discussed a more reliable system with additional safety of Radio Frequency Identification System with the 2-step authentication process for the tightening of the security of common Radio Frequency Identification system. The system is enhanced by the camera, for surveillance, at the ingress. The system starts with general Radio Frequency Identification tag verification, once the RFID verification is done the system drew out the identification information of the incomer so that further verification may be done, with the help of camera. This remains as the second layer of the security system. The system helps maintaining the security with (1) the cognitive features of Radio Frequency Identification tag and (2) and the physiognomies of the user with the help of camera. The Radio Frequency Identification reader is capable of recognition of RFID in numerous output means. Therefore, if, in the radio frequency system, any error occurs, the second layer of matching the physiognomies of the user with the one stored in the database. Thus, the system would be more efficient in the purpose of ensuring the security of the premises due to its 2- layered operations (X. Zhang and B. King, 2008).

Yet another paper discussed a mechanism of the ingress and egress security and surveillance system. The system would be capable of switching in between modes of operation in accordance with the state or level of security desired of the surveillance area/zone. The surveillance system is installed in the ingress location. The system comprises of RFID based authentication terminal for the incomer at the ingress and server for observing the total number of people passing through the ingress (Drimer, S., Murdoch, 2007). The switching mode function would be done by the server, with the said capacity, in the light of observing the people and the quantity of people passing through the ingress. This paper, we are discussed a model security system; radio frequency identification based digital access-control. The security and surveillance system is remote based that functions through network visual access, network visual telephone, home information broadcasting

and surveillance alarm mounted at home. Along with the following; the access machine, door machine and a machine for management is also required. The access machine is placed in the home location. All the parts are connected with one another through LAN network. The feature of the model system is that it combines radio frequency identification technology with the intelligent networking (X. Liu, 2010). With a unique idea of effective security and surveillance, K., Markantonakis and G., Mayes discussed specifications of a novel face recognition system. It has unique structure comprising of radio frequency identification tag for the purpose of storing Eigen features and face recognition unit. After long and thorough evaluation, the algorithm for face recognition was designed and hardware was built. Experimentations were carried out for the purpose of research on the process of verification and validation so as to achieve accurateness and low response time. Redundant evaluation and experiment of the verification system and database structure help achieving reduced time response and analogous verification precision (K., Markantonakis and G., Mayes, 2010).

3. Methodology

The project we opt for is an authenticating and a management system for safeguarding entrance for premises. The project is very practical and readily applicable. The option of Safe and Authentic Entrance System was made final due to the fact that Institute of Business and Technology (IBT) had the room for improvement for secure and authorized entrance in the campus as well as for selective premises in the campus like faculty room etc. The different structural designs that were studied moved us toward optimum solution of SAAES. The system is based on very economical and user-friendly RFID (Radio Frequency Identification) system; a RFID reader and RFID card to be used as RFID tag. The electronics tools gathered for authorization are the best suited for the basis of current process. The study for the mechanical design and structure help in finding out the most economical as well as robust structure. The best found microcontroller was Arduino UNO, that was thoroughly studied and thus selected for the system to be used as a processor. The display mechanism and sensors were identified. In the last, the materials for mechanical structure were selected.



Figure.1 Arduino UNO Microcontroller

The Part modeling of mechanical structure took place. Then the interfacing of the sensors and display unit took place. Then Finite Element Analysis (FEA) of the mechanical system was conducted. Whilst the modeling of the mechanical structure was done, the integration of all of the electronics components into a modular circuitry was also done simultaneously. There was a need of total attention towards the mechanical structure. Therefore, the manufacturing, fabrication and welding of the mechanical components took place. Once fabricated, the disintegrated mechanical components were assembled. At this stage, the electronics system was finalized as well as the mechanical structure was also established, there was a need of final integration of both the system so that a fully working system could be established. Therefore, at this stage the integration of mechanical and the electronics system took place into a single mechatronics entity.

4. ALGORITHM

The circuit LCD is as follow:

- * LCD 16 BLACK GND
- * LCD 15 RED 5V
- * LCD 14 PURPLE TO A5
- * LCD 13 BLUE TO A4
- * LCD 12 GREEN TO A3
- * LCD 11 ORANGE TO A2
- * LCD 6 YELLOW TO A1
- * LCD 4 WHITE TO A0

Typical pin layout used for rc522:

* Signal	Pin	Arduino Uno	Arduino Mega	Arduino Nano v3	Arduino Leonardo/Micro	Arduino Pro Micro
* RST/Reset	RST	9		5	D9 RESET/ICSP-5	RST
* SPI SS	SDA (SS)	10		53	D10	10
* SPI MOSI	MOSI	11 / ICSP-4		51	D11	ICSP-4
* SPI MISO	MISO	12 / ICSP-1		50	D12	ICSP-1
* SPI SCK	SCK	13 / ICSP-3		52	D13	ICSP-3

5. ARDUNIO UNO

The following is the code been burned in the Arduino uno Microcontroller so as to run the program.

```
#include <SPI.h>
```

```
#include <MFRC522.h>
#include <LiquidCrystal.h>
LiquidCrystal lcd(A0, A1, A2, A3, A4, A5);
#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfc522 (SS_PIN, RST_PIN);
String uID_prev="hjh";
Void setup ()
{
  Serial.begin (9600);
  SPI.begin ();
  mfc522.PCD_Init ();
}
void loop ()
{
  String(mfc522.uid.uidByte[0],HEX)+String(mfc522.uid.uidByte[1],
  HEX)+String(mfc522.uid.uidByte[2],HEX)+String(mfc522.uid.uid
  Byte[3],HEX);
  delay (250);
  if (mfc522.PICC_IsNewCardPresent ())
  {
    delay (250);
    mfc522.PICC_ReadCardSerial ();
    StringuID =
    String(mfc522.uid.uidByte[0],HEX)+String(mfc522.uid.uidByte[1],
    HEX)+String(mfc522.uid.uidByte[2],HEX)+String(mfc522.uid.uid
    Byte[3],HEX);
    bytepiccType = mfc522.PICC_GetType (mfc522.uid.sak);
    if(uID_prev != uID)
    {
      if(uID == "d5cdd5e5")
      {
        Serial.print ("\n\nSyed Ozair Asim \nBB-25266 \nInstitute of Business
        & Technology");
        lcd.print("Syed Uzair");
        digitalWrite(4, HIGH);
        delay(1000);
        digitalWrite(4, LOW);
        delay(1000);
```

```
    }  
else  
{  
Serial.print ("\n\nAccess Denied \nUnauthorized Card");  
lcd.print("chorrchorrchorr");  
}  
}  
if(uID_prev != uID)  
{  
if ( piccType != MFRC522::PICC_TYPE_MIFARE_MINI && piccType  
!= MFRC522::PICC_TYPE_MIFARE_1K&&piccType !=  
MFRC522::PICC_TYPE_MIFARE_1K) {  
Serial.println ("This tech demo requires the MIFARE Classic card.");  
return;  
}  
if (uID == "myUIDforStuff") {  
Serial.println ("Access granted");  
}  
}  
Digital Write (4, HIGH);  
delay(1000)  
digitalWrite(4, LOW);  
delay(1000);  
lcd.clear();  
}
```

RESULT

The mechanical structure of Secure and Authentic Entrance System is shown below: The image before swapping of RFID as given by the said system; Safe and Authentic Entrance System is as follow, the system initially, with main interface, no activity.



The image shows a registration form titled "SASES" on a light blue background. The form contains six input fields for the following fields: REGISTRATION ID, NAME, BARCODE, CAMPUS, DEPARTMENT, and GENDER. At the bottom of the form, there are two buttons labeled "First" and "Next".

The system with Radio Frequency Identification card (tag) swapped shows the identification characteristics of the identified person.

CONCLUSION

The aim is to create a authenticating and managing, reliable, entrance system to ensure security and safety of the premises. The system was based on RFID. The system was opting for it is readily applicable and practical. The system Safe and Authentic Entrance System was opting with the idea behind that the system could be installed in the campus vicinity. Thorough study was made so as to finalize the design and the mechanical structure. The mechanical structure that we opt is turnstile. The system is very economical and cheap. Although the cost of the system is low but due to low cost the elegance is compromised. Due to limited budget the turnstile was selected, however glass doors or robust stainless steel structure could be used. The system is strong enough to prevent anyone from intrusion. The system is half the size of average human body so that in case of emergency the turnstile could be step over.

ACKNOWLEDGEMENT:

I would like to thank God who made it possible for me to work on this Research paper. This research paper was written at Sirsyed University of engineering & technology, Pakistan, Karachi and I am glad, that there I got a chance to complete this useful and informative research work. I would like to extend my sincere gratitude to my organization, for their assistance and guidance towards the progress of this paper.

I would like to extend my sincere gratitude and acknowledge the selfless cooperation Sirsyed University of engineering & technology (SSUET), Pakistan, Karachi and other library staff of Engineering University.

I am deeply indebted to my family, thanks to my family members for supporting me. Their constant inspiration and guidance kept me focused and motivated.

At the end, I am deeply indebted to all my family members whose patience and understanding have played a great role in my success by sacrificing the valuable family time and supporting me throughout the research work.

REFERENCE

- [1]B. Chowdhury and M. U. Chowdhury, 2007, "RFID- Based real-time smart waste management system," Telecommunication Networks and Applications Conference , pp. 175-180, Australasian, Dec. p.p:2-5.

- [2] G. H. P. Florentino, C. A. P. de Araujo, H. U. Bezerra, H. B. de A. Junior, M. A. Xavier, V. S. V. de Souza, R. A. de M. Valentim, A. H. F. Morais, A. M. G. Guerreiro, and G. B. Brandao, Aug. 2008, "Hospital automation system RFID-based: Technology embedded in smart devices (cards, tags and bracelets)," 30th Annual International IEEE EMBS Conference, pp. 1455-1458, pp. 20-25
- [3] Brands, S., Chaum, 1993, "Distance-bounding protocols: Advances in Cryptology, Eurocrypt'93", Springer-Verlag, p.p: 344-348.
- [4] Bringer, J., Chabanne, 2008, "H.: Trusted-HB: A low-cost version of hb+se- cure against man-in-the-middle attacks", Transactions on Information Theory 54(9), pp.4339-4342 .
- [5] Bussard, L., Bagga, 2013, "W: Distance-bounding proof of knowledge to avoid real- time attacks", Springer, p.p:232-236.
- [6].Carluccio, D., Kasper, T., Paar, (July 2006), "Implementation details of a multipurpose ISO 14443 RFID tool. In: Printed handout of Workshop on RFID Security", IEEE Conference proceeding, p.p:658-662.
- [7] K. Wu, E. Bai, and W. Zhang, 2009, "A hash-based authentication protocol for secure mobile RFID systems", First International Conference on Information Science and Engineering, pp. 2440-2443.
- [8]X. Zhang and B. King, , 2008, "Security requirements for RFID computing systems", "International Journal of Network Security, vol. 6, no. 2, pp. 214-226.
- [9] N. Li, Z. L. Deng, F. Wan, S. Zhu, and X. Liu ,Oct.2010, "RFID-based information sharing platform" ,IEEE International Conference on Communications Technology and Applications, pp. 1-4, pp. 16-18.
- [10] Francillon, A., Danev, B., Capkun, S., 2010, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars", IEEE conference proceeding, John & Wiley son, p.p:78-84.
- [11] Francis, L., Hancke, G., Mayes, K., Markantonakis, 2010, "K.: Practical NFC peer- to-peer relay attack using mobile phones", in: RFIDSec'10 Proceedings of the 6th international conference on Radio frequency Identification: security and privacy issues, Springer-Verlag, p.p: 47-56.
- [12] Desmedt, Y., 1988, "Major security problems with the 'unforgivable' (feige)- at- shamir proofs of identity and how to overcome them. In: Securicor", SEDEP Paris, France, p.p.:15 -17
- [13] Drimer, S., Murdoch, S.J., 2007, "Keep your enemies close: distances bounding against smartcard relay attacks", In: Proc. of the 16th USENIX Security Symposium on USENIX Security Symposium, article no. 7, ACM Press, p.p:23-29.