An overview of RFID Based Security and Access Control System

Bhojraj Agarwal, Assistant Professor

Department of Electronics & Communication Engineering, Vivekananda Global University, Jaipur

Email Id- bhojraj_agarwal@vgu.ac.in

ABSTRACT: ***The design of an RFID-based security and access control system for use at Punjab University's dormitories is described in this article. The system accomplishes the necessary job by combining RFID technology with biometrics. When a number is detected by the RFID reader at the hostel's entry, the system takes the user's picture and searches the database for a match. Access is allowed when both cards and the recorded picture correspond to a registered user; otherwise, the system activates the alarm and sends an emergency call to the security van via GSM modem. Suspect individuals may be apprehended in this manner. To combat the security risks that many companies in Pakistan are facing these days, an automatic identity and access control system has become essential. Only authorized people will be able to enter the organization once the system is installed at the entrance.***

KEYWORDS: ***Access Control, Face Recognition, RFID, Security, System.***

1. INTRODUCTION

The device may also be placed at different locations across the company to monitor a person's movements and limit their access to critical areas[1]. Suspicious people may be detected this manner, which will undoubtedly enhance the organization's security. The access control system may be developed using radio frequency identification (RFID), a wireless technology[2]. The application of this technology to automate different operations, spanning from the industrial sector to home control, has been documented in the literature. The use of RFID technology to automate the administration of sight spot tickets has been described scholars[3]. RFID electronic tickets, RFID readers, computer terminals, optical networks, computer servers, and site controllers make up the system hardware. The S-DES encrypted data on the electronic ticket includes the scenic area number, scenic spot number, ticket type, ticket date, site number, serial number, and check bit. The data included in the e-ticket is read by the RFID reader on site and sent over the network to the computer terminal and servers[4].

At the terminal, the data is encrypted and its validity is confirmed. The site controller then lets the appropriate visitor inside the area. The selling sub-system, the decision sub-system, and the administration sub-system all participate in the system identification and authentication procedure. Through database information, all of these operations interact with one another[5].The system's hardware includes an RFID tag and reader for authentication that operate at 13.56MHz, an inductive loop for metal detection, a capacity sensor for counting vehicles, a Siemens MC 39i GPRS modem for communication between entrance and exit gates, and an FEC FC440 programmable logic controller (PLC) that serves as the system's brain. The RFID tag is scanned by the reader when the vehicle stops on the inductive loop at the entry. The unique identification number (UID), validity period, and check bit for verifying the parking status are all included in the data on the tag[6].

PLC manipulates this data, and permission to park the car is allowed if the tagged information includes the proper UID, validity term, and parking status. The parking status of the vehicle will be altered by the RFID reader/writer once it enters the parking lot to prohibit the entrance of another vehicle on the same card. When the car leaves the parking lot, the same process is followed[7]. In a ubiquitous environment, Nova Ahmed presented the Guardian Angel, an RFID-based interior guiding and monitoring system. The system's strength is its ability to create dynamic queries in real time through a user interface[8]. The system's surroundings is split into zones and is supplied with RFID tags. The system's middleware is split into two layers: the guiding layer and the monitoring layer. The guiding layer is equipped with a portable RFID reader that sends location data to the monitoring layer on a regular basis. As a result, the monitoring layer gets access to information about the whole environment. The system is almost 100 percent accurate in delivering zonal information, enabling the development of extremely strong guiding and monitoring applications, according to experimental findings. Kuo-shien Huang describes a business model-based strategy to using RFID technology to automate processes in accordance with the enterprise's strategic vision and objectives.

The author created a business plan for a bike-rental system and implemented it using RFID technology. The traditional method of renting a bike, which involves writing down customer information on a piece of paper and then typing it into a computer, is replaced by giving the customer an RFID card and attaching an RFID tag to the bike. The bike is marked so that it can be tracked from the rental shop to the return shop. Through a web interface, the information is exchanged across the shops. In this manner, an effective RFID strategy may be developed and implemented. The design of a security and access control system utilizing RFID technology is discussed in this article. Entrance monitoring, exit monitoring, and mess monitoring are the three components that make up the system. Through the primary controller, these modules interact with the computer system.

After the computer has analyzed the data from these modules, control instructions are sent to the modules giving or refusing the user's access[9]. RFID technology has been used by many researchers in the development of access control systems. Filipe created an RFID-based monitoring and access control system that includes an RFID terminal, a camera, a server, and an alert device. When a transponder is detected, the terminal takes a photo and sends the data, including the UID and photo, to the server via a TCP/IP connection. The server searches the database for this query and returns the results to the terminal, allowing or disallowing access. The system also monitors illegal activities, such as when a person tries to enter while the door is open without completing the authentication process, and uses web services to activate the alert device. Installation of RFID kits with antennas covering a 10cm range is used to test the system's performance, and satisfactory results are obtained.

An RFID-based embedded security authentication system with a novel face recognition structure was described by Xiang-Lei Meng. Registration and recognition are the two phases of the system. Ten pictures of the user's face with various emotions are collected during the registration phase, and eigen information is extracted using an extraction algorithm. On an RFID tag, this information is written along with a UID. A camera tracks the face in the recognition phase, and an extraction algorithm returns the eigen information of the face in the image. For authentication, this data is compared to the data already stored on the tag. Instead of using a digital device or server, the entire processing is done on an embedded ARM11 processor, S3C6410. This results in a faster response time of about 57ms and verification accuracy of up to 86.5 percent. When the system's performance is compared to that of existing database systems, it is discovered that the system has a significantly faster response time while maintaining the same level of authentication accuracy[10].

Scholars describes an RFID-based access control system that includes neural network-based face recognition. If the individual carrying the RFID card is discovered to be unauthorized, the system identifies their face and refuses entry. The face of authorized people was learned using a radial basis function neural network (RBFNN). The picture characteristics were extracted using principal component analysis (PCA), and the features were refined using classification techniques (LDA). To improve its generalization capabilities, the network is trained using the localized generalization error model (L-GEM). The suggested solution may enhance the security of RFID access control, according to experimental findings.

1.1 System Component :

- RFID Tags: The user is given an RFID Tag IPC80 passive RFID tag with a 125KHz frequency. The reader receives information from the tag in the ASK format.
- RFID Reader: IP10 is a proximity card reader with a 125KHz operating frequency and a reading distance of up to 4 inches. The reader is simple to install on metal doors, delivers tag information serially in RS232 format, and may be used both inside and outdoors. For hostel security, three readers have been installed: a hostel entry gate, a hostel exit gate, and a mess entrance gate.
- Camera: The pictures are captured with a Logitech C500 webcam. The camera features 1.3 mega pixel sensors and can record video at a resolution of up to 1280x1024 pixels. For hostel security, two similar cameras have been installed: one at the entrance and the other at the exit. To minimize the overall complexity, no cameras are utilized to access the mess hall.
- GSM Modem: The Nokia 12i GSM modem is used to contact the security van in an emergency. Nokia 12i has advanced GSM connectivity and supports EDGE/GPRS and HSCSD with automatic GSM connection creation. It also comes with application level watchdogs, integrated self-check mechanisms, and a dependable Virtual Machine (VM) for JAVATM. TCP/IP for reliable data transmission, UDP/IP for music and video streaming, and HTTP for accessing web sites are all supported by the Nokia 12i's inbuilt internet protocols. An external GPS device that supports the National Marine Electronics Association (NMEA) standard may also be attached to the module. The GPS device's output can be parsed by the inbuilt NMEA parser, which can parse the location data.

External microcontrollers can interact with Nokia 12i via AT instructions, and basic remote I/O applications can be simply controlled using text messages. The AT89C52 microcontroller was chosen because it is a powerful microcomputer with low power consumption that offers a highly versatile and cost-effective solution for many embedded control applications. It features an inbuilt flash memory of 8K bytes, 256 bytes of RAM, 32 programmable I/O lines, three 16 bit timers/counters, eight interrupt sources, and a programmable serial channel.

- Nonvolatile RAM: The 256K Nonvolatile RAM (NV-Ram) DS1230Y-85 is used to store passwords for RFID numbers that have been registered. The best of RAM and ROM are combined in NV-RAM, which has the read and write capabilities of RAM and the non-volatility of ROM. The DS1230 Nonvolatile SRAM has a capacity of 262,144 bits and is organized into 32,768 words by 8 bits. Each NV SRAM is equipped with a self-contained lithium energy source as well as control circuitry that constantly monitors VCC for out-of-tolerance conditions. When this happens, the lithium energy source is turned on automatically, and write protection is enabled unconditionally to prevent data corruption.
- Locks on Doors: Hostel entrance, exit, and mess gates all have solenoid-operated door locks. To open the gate, a relay is used to energize the solenoid.
- Alarms: There are two alarms in place, one at the entrance and the other at the exit gate. If an unauthorized person tries to enter the hostel, these alarms will sound.

1.2 System Operation :

There are two stages to the security and access control system: registration and recognition. During the registration process, 10 pictures of the hostel user are taken while an RFID tag is issued. These pictures are utilized to train a feed forward neural network using a back propagation training method, and the converged weights for each user are saved. When the user wishes to join the hostel, the user enters the recognition phase. After receiving the RFID user number, a picture of the user is taken and sent to the neural network for identification. If a match is discovered, the user is given access. The identity of the user is verified at three locations: the hostel entry, hostel exit, and mess entrance. RFID and facial recognition are used in the entry and exit modules, while RFID plus a password are used in the mess module to give access. A primary controller connects these components to the computer system. The information from the modules is sent to the computer system via the main controller. After processing these interruptions, the computer system sends instructions to the modules through the main controller. The serial port is used for data transmission between the main controller and the computer system, whereas the parallel port data and control lines are utilized for handshaking. Figure 2 depicts the system's block diagram.

- *Entrance Monitoring Controlle:* The Entrance Monitoring Controller is a device that monitors the entrance to a building. The entrance monitoring controller includes an RFID reader, a GSM modem, NVRAM, door lock, alarm, scroll keys, and a 16x4 LCD, all of which are connected to an AT89C52 microcontroller. The microcontroller searches the NV-RAM for this number after detecting and receiving RFID tag data through a serial interrupt function. If no match is discovered, the microcontroller uses a GSM modem to make an emergency call to the security van. Simultaneously, it sends a request to the computer system through the main controller to capture the user's picture and activates the alert signal. If a match is discovered, however, the microcontroller verifies the user's entry status by reading NV-RAM. The controller makes a request to the computer system to collect and process the user picture if the user has not yet entered the hostel.
- The computer system has two purposes. It examines whether the user is a defaulter or not after verifying the person against the received RFID number using a facial recognition technique. Following processing, the computer system produces one of three messages: "access allowed" for a registered and clear user, "access refused" for a non-registered user, and "user is a defaulter" for a registered and defaulter user. In the event of a non-registered user who uses another user's RFID tag, a hefty fine is added to the user's hostel fees. The message from the computer system is received by the entry controller and shown on a 164 LCD. The scroll keys may be used to read the information on the LCD. The controller unlocks the entry gate by switching the relay if the message "access granted" is received. The user's entry status is updated in the non-volatile RAM at the same time.
- Exit Monitoring Controller: the exit monitoring module consists of an RFID reader, an alarm, and a door lock, all of which are connected to an AT89C52 microprocessor. When the microcontroller receives RFID tag information from the reader, it sends a request to the entry monitoring controller to look up the user and their entrance status in NV-RAM. The exit controller disables the RFID tag and sends a request to the computer system to capture the user picture after receiving a "no" signal

from the entry controller. Simultaneously, it makes an emergency call using a GSM modem connected to the entry controller and activates the alarm system. If a "yes" signal is received, on the other hand, the exit controller sends a request to the computer system to collect and process the user picture. To validate the user, the computer system employs a facial recognition algorithm. If a match is discovered, the computer system requests that the exit controller give the user access to depart the hostel.

- Exit controller makes a request to the entrance controller through main controller after the user has left the hostel to update the user's entry status. In the event of a non-registered user, a hefty fine is added to the user's hostel fees for using another person's card. As a result of the exit monitoring controller, the system is able to allow a legitimate individual to depart the hostel.
- Controller for Mess Monitoring: Mess monitoring controllers automate the mess attendance system, while entry and exit monitoring controllers assist track users. the mess monitoring module includes an RFID reader, 4x3 keypad, 16x4 LCD, NV-RAM, door lock, and alarm indication, all of which are connected to an AT89C52 microprocessor. The controller looks for the RFID tag number in a list of registered numbers stored in NV-RAM when it receives it. If a match is discovered, the controller will prompt the user for their password. In addition, NV-RAM stores a password list for registered users that corresponds to RFID tag numbers. If the password provided is accurate, the controller allows the user entry to the mess hall. Simultaneously, the controller transmits user data as well as mess attendance to the computer system through the main controller. The computer system changes the database and gives the mess controller a "attendance recorded" notification. The precise mess costs are kept in an online database in this manner.

2. DISCUSSION

RFID (radio-frequency identification) is a technology that utilizes magnetic waves to identify and track tags attached to items. A radio transponder, a radio receiver, and an emitter make up an RFID system. The tag sends digital data, typically an identifying inventory number, back to the reader when activated by an electromagnetic interrogation pulse from a nearby RFID reader device. This number may be used to keep track of your inventory. The RFID reader's probing radio waves provide energy to passive tags. Because active tags are battery-powered, they can be read from a longer distance from the RFID scanner, up to hundreds of meters. The tag, unlike a barcode, does not need to be in the reader's line of sight, thus it may be embedded in the monitored item. RFID is a kind of automated data collection and identification system (AIDC). RFID tags are widely utilized in a variety of sectors. For example, an RFID tag affixed to a car during manufacturing may be used to monitor its progress through the assembly line, RFID-tagged medicines can be tracked via warehouses, and RFID microchips implanted in cattle and pets can be used to positively identify animals. In stores, tags may be used to speed up checkout and prevent theft by consumers and staff. RFID tags may be affixed to real money, clothes, and belongings, as well as implanted in animals and humans, raising significant privacy issues. As a consequence of these concerns, standard standards addressing privacy and security problems have been developed.

3. CONCLUSION

A security and access control system for usage in Punjab University dormitories is described in this article. To distinguish between legitimate and invalid users, the system employs radio frequency identification and biometrics technologies. The system processes data from sub-controllers to complete the security and access control job. Entry monitoring controllers, exit monitoring controllers, and mess monitoring controllers are placed at the appropriate entrance gate, exit gate, and mess gate. These controllers scan the user's RFID tag and look up the number in non-volatile RAM. The controllers ask the computer terminal to capture the user picture after a successful match. The computer system verifies the user's identity using a neural network trained facial recognition module and replies to the controllers by sending them a "access allowed" or "access refused" message. Controllers either give the user access or make an emergency call as needed. A web server is used to make this system centralized. The web server collects data from hostel computer terminals and maintains track of individual users. Although the created system is effective in minimizing security risks to dormitories, the reaction time of the system might be improved. Dedicated processors, rather than computer systems capable of processing pictures in real time, may increase reaction time.

REFERENCES

[1] N. Chilamkurti, S. Zeadally, and H. Chaouchi, *Next-Generation Wireless Technologies (4G and beyond)*. 2013.

[2] A. Abuarqoub *et al.*, “Sinalgo,” *Ad Hoc Networks*, 2010, doi: 10.1049/ip-gtd:19981578.

[3] M. Aazam *et al.*, “‘Estudio de dos tipos de fertilizantes químicos y orgánicos en dos híbridos comerciales de pimiento (Capsicum annun

L.) en la parte alta de la Cuenca del Río Guayas,'" *Univ. TÉCNICA ESTATAL QUEVEDO Fac. CIENCIAS Agrar. Esc. Ing. AGRONÓMICA*, 2015.

[4] H. Jialiang, O. Dantong, and X. Youjun, "A BRS-based approach for modeling RFID untraceability," *Int. J. Adv. Comput. Technol.*, 2011, doi: 10.4156/ijact.vol3.issue11.13.

[5] A. Yee-Loong Chong, M. J. Liu, J. Luo, and O. Keng-Boon, "Predicting RFID adoption in healthcare supply chain from the perspectives of users," *Int. J. Prod. Econ.*, 2015, doi: 10.1016/j.ijpe.2014.09.034.

[6] S. Committee, *IEEE Standard for Software Verification and Validation IEEE Standard for Software Verification and Validation*. 1998.

[7] S. D. Verifier and A. H. Drive, "Simulink ® Verification and Validation ™ Reference," *ReVision*, 2015.

[8] H. Rimminen *et al.*, "MIT OpenCourseWare http://ocw.mit.edu Haus, Hermann A., and James R. Melcher.," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2012.

[9] E. Valero, A. Adán, and C. Cerrada, "Evolution of RFID applications in construction: A literature review," *Sensors (Switzerland)*, 2015, doi: 10.3390/s150715988.

[10] A. Alwadi, A. Gawanmeh, S. Parvin, and J. N. Al-Karaki, "Smart solutions for RFID based inventory management systems: A survey," *Scalable Comput.*, 2017, doi: 10.12694/scpe.v18i4.1333.