# A MICRO-CONTROLLER BASED DOOR ACCESS CONTROL SYSTEM USING RADIO FREQUENCY IDENTIFICATION

BY

OLUFEYIMI, GBENGA OLATUNDE

CPE/12/0940

A Project Submitted to the Department of Computer Engineering,
Faculty of Engineering,

Federal University, Oye-Ekiti (FUOYE)

Ekiti, Nigeria.

In Partial Fulfillment of the Requirement for the Degree of Bachelor

of Engineering (B. Eng) in Computer Engineering,

November, 2017.

# CERTIFICATION

This project with the title

**A MICRO-CONTROLLER BASED DOOR ACCESS CONTROL SYSTEM USING RADIO FREQUENCY IDENTIFICATION (RFID)**

Submitted by

**OLUFEYIMI, GBENGA OLATUNDE (CPE/12/0940)**

Has satisfied the regulations governing the award of degree of

**BACHELOR OF ENGINEERING (B. Eng)**

Federal University Oye-Ekiti, Ekiti.

……………………………………… 20-12-2017

**Dr. (Engr.) I.A. Adeyanju** **Date**

**Supervisor**

DEPARTMENT OF COMPUTER ENGINEERING
HOD SIGN
DATE
FEDERAL UNIVERSITY OYE EKITI

……………………………………… 20-12-2017

**Dr. (Engr.) I.A. Adeyanju** **Date**

**Head of Department**

# DECLARATION

This project is a result of my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet and so on) has been acknowledged within the main report to an entry in the References list.

I agree that an electronic copy or hardcopy of this report may be stored and used for the purposes of plagiarism prevention and detection. I understand that cheating and plagiarism constitute a breach of University Regulations and will be dealt with accordingly.

## COPYRIGHT

Student's full name: OLUFEYIMI GBENGA OLATUNDE

Sign. & Date: Gbenga 15|03|2018

# DEDICATION

I dedicate this report to God, the Almighty; the All-knowing, the All sufficient, the Giver of wisdom, knowledge and understanding.

# ACKNOWLEDGEMENTS

I humbly wish to appreciate Dr. Adeyanju I.A., who stepped in as my supervisor when my former supervisor, Engr. Olayinka Adeleye, travelled outside the country to further his education. Also, many thanks to all the lecturers in the Computer Engineering department, as well as non-academic staff members of the department.

Special thanks to my parents, Mr. and Mrs. Olufeyimi, and to my friends, course mates, family members and loved ones for their relentless support and never ending love.

# ABSTRACT

There have been several cases of unwanted entries into the laboratories and offices within the school environment, and in a quest to reduce these occurrences, this project "a micro-controller based door access control system using Radio Frequency Identification" was proposed to control access to restricted areas within the school. Access control is a process by which users are granted access and certain privileges to systems, resources or information. Radio frequency identification (RFID) is a wireless communication technology that has been widely deployed in access control and security systems. The aim of this project is to develop a micro-controller based door access control system using Radio Frequency Identification.

This RFID-based system is built around a micro-controller, programmed to read in data from an RFID tag through the RFID reader. The RFID reader sends this data (ID number of the RFID tag) to the micro-controller which checks whether or not the data from the RFID reader matches with the data that is programmed into the micro-controller. The micro-controller serves as the database and contains the information of each of the RFID tags to be used to access the doors. The RFID reader which is placed at the door post will read the data of RFID tags, and only users with authorized tags will be granted access.

The developed system reads and responds to both registered and unregistered tags, but grants access to only registered tags. The developed system can't read more than one card at a time and it doesn't save tag information. The power source of the system must be powered by an AC power within the range of 110-240V AC as any power outside this range may damage the system.

The developed system can be adapted to securing various kinds of doors such as in libraries, laboratories, office equipment, etc. Further improvements can be made on this work can by incorporating concepts such as database implementation and management, alternative source of power (such as a UPS) for the entire system, addition of another security measure like biometrics, etc.

## TABLE OF CONTENTS

# LIST OF FIGURES

**FIGURES** **PAGE NUMBER**

# LIST OF TABLES

**TABLES** **PAGE**

# LIST OF ACRONYMS

| | |
|---|---|
| AC | Access Control |
| AC | Alternating Current |
| ADC | Analog to Digital Converter |
| ACL | Access Control List |
| AMC | Access Modular Control |
| BEME | Bill of Engineering Measurement and Evaluation |
| CBAC | Content-Based Access Control |
| CISC | Complex Instruction Set Computers |
| DAC | Discretionary Access Control |
| DAC | Digital to Analog Converter |
| DC | Direct Current |
| DNA | Deoxyribo-Nucleic Acid |
| EEPROM | Electrically Erasable Programmable Read Only Memory |
| GPR | General Purpose Register |
| GPS | Global Positioning System |
| ICC | Integrated Circuit Card |
| ID | Identification |
| I/O | Input and Output |
| IT. | Information Technology |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| MAC | Mandatory Access Control |

| | |
|---|---|
| OCR | Optical Character Recognition |
| ONS | Object Naming Service |
| RAM | Random Access Memory |
| ROM | Read Only Memory |
| PIC | Peripheral Interface Controller |
| QTY | Quantity |
| RBAC | Role-Based Access Control |
| RFID | Radio Frequency Identification |
| SFR | Special Function Register |
| SPR | Special Purpose Register |
| SSO | Single Sign-On |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| UNIX | Unix Operating System |
| VLSI | Very Large Scale Integrated Circuit |

# CHAPTER ONE

# INTRODUCTION

## 1.1 PREAMBLE

Access control is a technique that enables us to emphasize a selected restriction on access to data/privileges to authorized users. Therefore, identification, authentication (audit/verification against predefined policies/rules) and authorization are the three major activities that make up an access control model. Access control mechanism allow subject (user) to use their credential to identify themselves as legitimate users and help gain access to resources (Nancy et al, 2015). There are only two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access limits connections to computer networks, system files and data (Searchsecurity, 2017).

A microcontroller is a solitary chip microcomputer fabricated from VLSI fabrication. A microcontroller is also known as embedded controller. Today various types of microcontrollers are available in market with different word lengths such as 4bit, 8bit, 64bit and 128bit microcontrollers. Microcontroller is a compressed micro-computer manufactured to control the functions of embedded systems in office machines, robots, home appliances, motor vehicles, and a number of other gadgets (Garfinkel, and Juels, 2005). A microcontroller is comprises components like – memory, peripherals and most importantly a processor. Microcontrollers are basically employed in devices that need a degree of control to be applied by the user of the device. Examples of microcontrollers are PIC (Peripheral Interface Controller) microcontroller, AVR (Advanced Virtual RISC) microcontroller, 8051 microcontroller, ARM microcontroller, etc. Microcontrollers can be used in light sensing and controlling devices, temperature sensing and controlling devices, fire detection and safety devices, industrial instrumentation devices, process control devices and access control devices (Electronicshub, 2017). This project proposes a microprocessor-based door access control system using Radio Frequency Identification (RFID).

## 1.2 STATEMENT OF PROBLEM

Over the last few years, there have been several cases of unwanted entries into many laboratories and offices within the school environment. There have been several alarms raised by the members of staff in the school and there is need to address the issue. In a quest to limit these unwanted entries, this project "a micro-controller based door access control system using Radio Frequency Identification" was developed to control access to restricted areas within the school.

Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users must present credentials before they can be granted access (Juels and Rivest, 2003). In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security. In the fields of physical security and information security, Access Control (AC) is the selective restriction of access to a place or other resources. Permission to access a resource is called authorization. Locks and login credentials are two analogous mechanisms of access control (Juels, 2006; Jules and Weis, 2006).

For this project, RFID will be used to provide security and access control because it has few advantages over other listed access control systems. Some of its advantages over others are are: Unique item identification is easier to implement with RFID than with barcodes and other electronic access control systems. RFID has the ability to identify items individually rather than generically. RFID tags are less sensitive to adverse conditions (dust, chemicals, physical damage etc.) and many tags can be read simultaneously, RFID tags can be combined with sensors and they can locally store information (Garfinkel, 2002).

## 1.3 AIM AND OBJECTIVES

The aim of this project is to develop a micro-controller based door access control system using Radio Frequency Identification (RFID). The specific objectives of this project are:

1. To design a door access control system using RFID and a microcontroller
2. To implement the system design
3. To evaluate the performance of the developed system

## 1.4 SCOPE OF STUDY

This project developed a microcontroller-based door access control system using RFID. The microcontroller served as the control device, as well as the database, and it contains the information of users' RFID tags. For this project, Nuvoton W78E052D microcontroller (a member of the 8051 family of microcontrollers) was used, even though there are other microcontroller families that could have been used, such as PIC microcontrollers, Atmega microcontrollers, Atmel Microcontrollers, etc.

For this project, a prototype of a microcontroller-based door access control system, using RFID mechanism, was designed to provide security to the doors in a computer laboratory. RFID mechanism can also be used for identification or authentication in industry, agriculture, commerce, health care, public transport, electronic ticketing, access control systems, retail, animal identification, logistics, and entrance control, etc. It can be embedded into everyday items as a smart label (Ayoade, 2007).

Radio Frequency Identification (RFID) is a technology for wireless information exchange over short distances. The main parts of an RFID system are RFID Tags (with unique ID numbers) and RFID reader, for reading the RFID tags (Nancy et al, 2015). For this project, the RFID tags are passive tags. Users will be given passive RFID tags and only users whose RFID tag information are saved onto the microcontroller will have access to the doors.

## 1.5 SIGNIFICANCE OF STUDY

The use of RFID interfaced to a microcontroller to provide security at door posts in laboratories, homes and offices will be beneficial to its users in many ways, some of which are:

1. **Better Security:** The designed system will ensure the availability of security at all time, data integrity, authentication of every user and non-repudiation.
2. **Reduced Cost of Providing Security:** The system will reduce the number of physical security officers at door posts, as it has always been the custom at almost every place where security is needed. There is also no need for regular maintenance of the system.

3. **Convenience:** The designed system eliminates the aggravation and struggle associated with the opening of heavy and manual doors.
4. **Easy Usage and Maintenance:** The system is designed to ensure minimal maintenance which makes it easy to use and also eliminates the need for regular maintenance.

## 1.6 METHOD OF STUDY

1. The first stage of this project was for extensive feasibility study and adequate literature review. This is also included studying background information about the project concepts, and familiarization with the tools needed for the implementation of the project.
2. The second stage of the project was for circuit design development and code writing. Also in this stage, the software simulation was carried out.
3. The third stage was for the procurement of the tools needed for the project, as well as for the project implementation and prototyping.
4. The final broad stage was for the performance evaluation of the developed access control system.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 ACCESS CONTROL

Access Control is an important mechanism which protects system resources and also helps different applications to give specific resources/object access to subject/user. There are two main Types of Access Control:

a) Physical Access Control: Physical access control is an access control system that determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically, this was partially accomplished through keys and locks. When a door is locked, only someone with a key can enter through the door, depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door, and the keys can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed (Karjoth and Moskowitz 2005; Juels and Brainard, 2004). Physical access control system is designed to control the physical attributes like access control to room, building and campus.

b) Logical Access Control: Logical access control, also called Electronic Access Control, uses computer technology to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. There are various logical access control systems in existence, some of which are barcode systems, biometric based access control, smart cards, RFID systems, etc. (Juels et al., 2003). Logical access control system is designed to control computer network systems like local access control to number of connection to a computer, files and data.

Access Control categorizes into seven different types as shown in Figure 2.1 below:

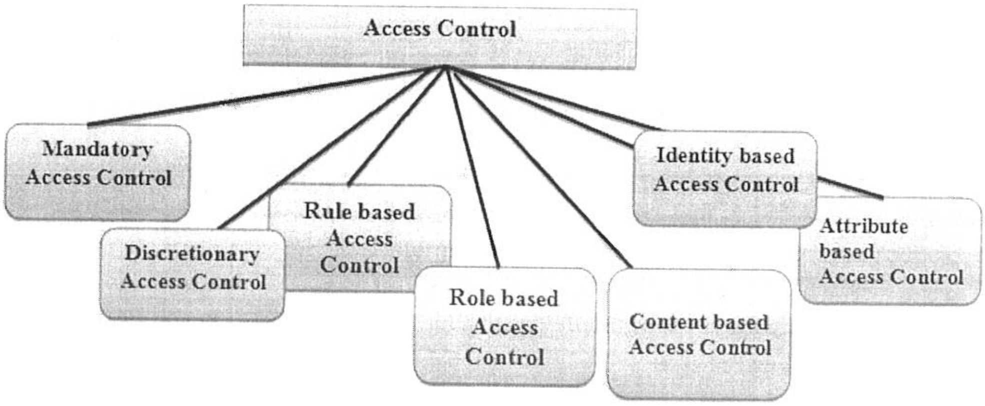
Access Control
Mandatory Access Control
Discretionary Access Control
Rule based Access Control
Role based Access Control
Content based Access Control
Identity based Access Control
Attribute based Access Control

Figure 2.1: Access Control Models (Bai and Zheng, 2011).

### 2.1.1 Mandatory Access Control (MAC)

The MAC model for computer security allows subject access to all resource objects controlled by the operating system based on system administration configured setting. Under the MAC subject cannot change the control list designed for resources (Bai and Zheng, 2011). A subject is allowed access the object based upon security labels with policies determined by network administrator enforced by operating system. Special UNIX operating systems are based on MAC. MAC is generally applied in environments where security rules are definite and security strategy is simple. MAC is mostly used in government and military field by assigning a classical label to file system object. In MAC since users do not have the control over the access policy applications and declassify information, the system is safeguarded from the Trojan horse attacks.

### 2.1.2 Discretionary Access Control (DAC)

DAC access control type defined by Trusted Computer Evaluation Criteria. In DAC the owner of the resource objects (file and data) grant access through policy determined. Simple example of DAC in UNIX operating system, file mode like read, write and executable permissions assigned to every user, group and others. In DAC (Bai and Zheng, 2011), Access Control List (ACL) consists of a list of subjects with their permission to access the file on that operating system. Lower lever DAC in contrast with MAC, does not allow resource owner to assign access control and to prepare their own policies.

### 2.1.3 Role-Based Access Control

Most of the enterprises and organizations go with Role based access control because the privileges to objects are based on roles of employees in the organization. Computer applications are always in developing mode, computer security changes continually but DAC and MAC support only some access control demands (Bai and Zheng, 2011). Role is defined based on responsibility, authority and job within the enterprises. Subject user inherits privileges that are tied with their role hence it is called Non-discretionary Access Control. The main advantage of RBAC is that roles can be easily created and can be changed as per requirements of enterprise, thereby making management of policies easier. However, the consolidations of many users into one group prevent the ability to apply fine-grained access policies to realize a customized access control environment.

### 2.1.4 Rule-Based Access Control

The Rule based access model allow system administrator to access or deny the resources object to subject. In discretionary access control model, ACL is implemented by Network administrator for user or group. If any user or group is accessing the object, operating system checks the rule contained in ACL for that object. Example of Rule based access controls are situations in which any account or group can access the network connection at certain hours or days of the week.

### 2.1.5 Content-Based Access Control (CBAC)

It is an innovative access control model designed for content centric information sharing. It is applied where RBAC will give more access right; on top of such model CBAC is deployed (Wenrong et al 2014). The CBAC model takes access control decisions based on content similarity. In CBAC subject can use RBAC model to access all large set of objects but CBAC add additional restriction to subject where the subject could access subset of designated record. Boundary of the subset is dynamically determined by the textual content of data objects.

### 2.1.6 Identity-Based Access Control

Identity based access control is the general mechanism that exists for authenticating a device/user based on the identity or password that they possess. It provides a mechanism for identifying who the user is. A variation of this is the group identity access control that enables access to a group of users gain access to databases and the like resources. A simple example of identity based access control is the secured access to Wi-Fi networks (Milyaev et al, 2013).

### 2.1.7 Attribute-Based Access Control

Attribute based access control provides access to users by verification against access policies that are formed by combining relevant attributes to regulate access to users (Jerichosystems, 2017). This provides a mechanism to enable fine grained access to resources/data. It helps realize the most need "principle of least privilege" to ensure the security of resources and information that is contained in the system. A simple example that follows attribute based access control is where access to specific company related data are provided to employees who have completed fifteen (15) hours of training on a specified platform.

## 2.2 TECHNOLOGY BASED ACCESS CONTROL SYSTEMS

There are different kinds of technologies in existence for access control. In terms of applications, cost requirement, and functionality demands, one or a mix of solutions are adopted to fulfill the access control functionality and information collection in the applied systems.

With the cost decline in wireless and GPS technology, access control systems can integrate these high-end technologies with Information Technology (IT) systems to offer not only the identification functionality but also value-added information and service in the applied systems. It can greatly improve the information visibility in the system information flow (Rieback and Crispo, 2006). Various technology-based access control system include the following listed below:

### 2.2.1 Barcode Systems

Barcode technology is becoming an essential tool for successful companies. Barcoding will bring to the new millennium what the internet has done for us in the last decade. In order for businesses to effectively utilize this technology, however, a base level of knowledge of how barcoding works is necessary.

Barcode is a binary code comprising a field of bars and gaps arranged in a parallel configuration as shown in the Figure 2.2 below. They are arranged according to a pre-determined pattern and represent data elements that refer to an associated symbol. The sequence made up of wide and narrow bars and gaps can be interpreted numerically and alphanumerically. It is read by optical laser scanning. However, despite being identical in their physical design, there are considerable differences between the code layouts.

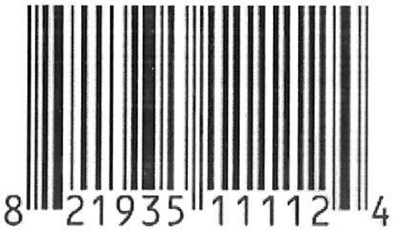

Figure 2.2: A typical barcode (Harmon and Adams, 1989).

Barcode data entry is at least 100 times faster and more accurate than traditional manual keyboard entry. The use of barcode as a means of access control has several advantages, some of which are:

1. Data Accuracy: Accurate data is the single most important resource for any company or organisation. Precise data produces accurate reports on any operational function of a company and allows for more accurate predictions about the future needs and patterns of processes. Data accuracy is the biggest benefit of barcoding. Organizations that cannot afford data entry errors, such as schools, hospitals, crime labs, professional service organizations, and many manufacturing companies, are implementing barcoding systems to achieve near 100 percent accuracy in data reporting.

2. Efficiency: Barcoding also enables users to work faster. Barcode scanning improves data entry speed. It also alleviates the need for correcting data entry errors; a costly byproduct of manual data entry. Truly beneficial efficiency occurs when processes can become automated using barcodes. A shipping/receiving dock does not need a person dedicated to counting inventory just received if it is scanned as it is unloaded. Conveyor systems can efficiently route products to the correct destination when scanners read strategically placed barcodes on product bins. Stores do not need as many Cashiers to handle customers when each register is equipped with a scanner that can quickly and accurately scan barcoded products. Barcoding ensures that the record of a package's journey will be recorded at every stop along its trip. Much of this technology exists on its own, but it is barcoding that allows for the easy tracking and transfer of this information.
3. Consistency: Consistency is becoming more important to companies not only with the type of products they create or sell, but with how these products are sent to other companies that create or sell. Large companies need to receive products in a timely and efficient manner from their suppliers. They do this by demanding that all of the companies they work with adhere to certain standard principles when using barcodes. This is called Compliance Labeling. By making sure these suppliers use a certain type of barcode placed in a certain way on the package, a dependable uniformity is established. That lets each company know what each of the different barcodes on the package represent. It also allows companies to preset their scanners to only read a certain type of barcode. This allows only the right company to read the right barcode off of the right product (Harmon and Adams, 1989).

### 2.2.2 Biometric Procedure

Biometrics refers to metrics related to human characteristics. Biometrics is defined as the science of counting and measurement procedures involving living beings. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control (Milyaev et al, 2013).

Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice (Okereafor et al, 2016). Some common biometric identifiers are discussed briefly below:

**1) Face Recognition**

Face recognition systems recognize human face using facial features (Adeyanju, Omidiora, & Oyedokun, 2015). Although face recognition has increased in reliability significantly over time, it is still not accurate all the time. The ability to correctly classify the image of the face depends the following variables which include lighting, pose, facial expressions and image quality (Anila & Devarajan, 2012). Figure 2.3 shows a face recognition system processing the image of a human face (Jain, Ross, & Prabhakar, 2004). In face recognition, the following features are important for system recognition: nose, eyes, eyebrows, mouth and nostril. Face recognition is widely accepted by users because it is not intrusive.

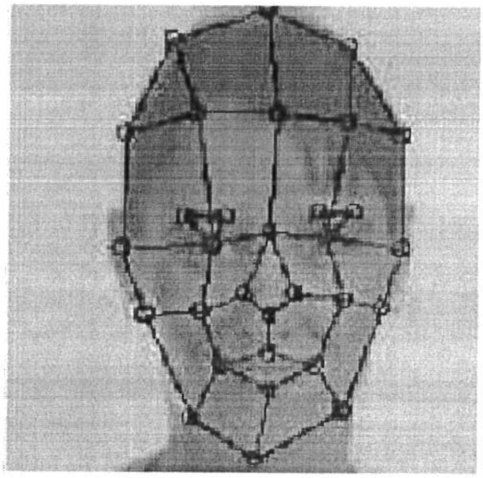

Figure 2.3: A face recognition system processing the image of a human face. (Jain, Ross, & Prabhakar, 2004)

### 2) Fingerprint Recognition

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae. The upper skin layer segments of the finger are the ridges while the lower segments are the valleys (Shoewu, Makanjuola, & Olatinwo, 2014). It is a widely accepted assumption that the minutiae pattern of each finger is unique and does not change during one's life. Figure 2.4 shows the human fingerprint and its different parts. When human fingerprint experts determine if two fingerprints are from the same finger, the matching degree between two minutiae pattern is one of the most important factors. The five basic fingerprint patterns are arch, tended arch, left loop, right loop and whorl as shown in Figure 2.5.

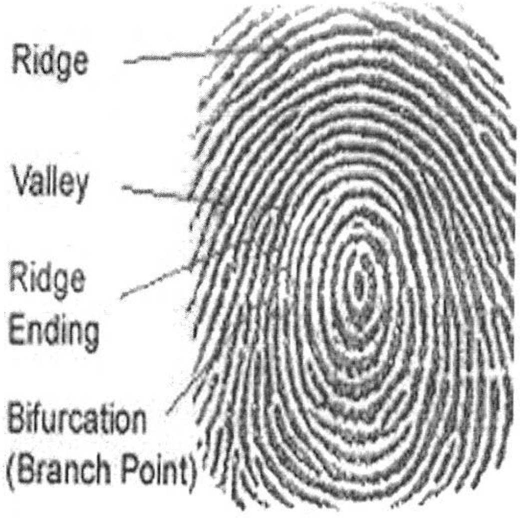

Figure 2.4: The Human Fingerprint and its different parts (Chaurasia, 2012).

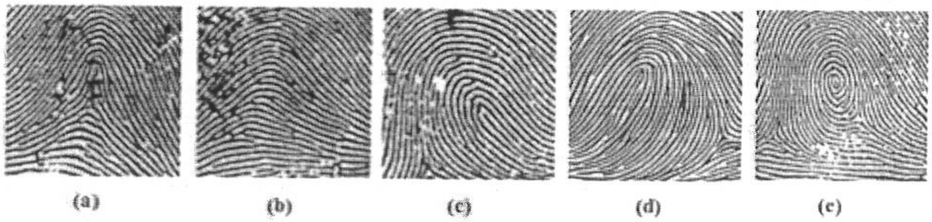

Figure 2.5: The Five Basic Fingerprint Patterns (a) Tended Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl. (Shoewu, Makanjuola, & Olatinwo, 2014)

### 3) Iris Recognition

The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. The iris is perforated close to its center by a circular aperture known as the pupil. The function of the iris is to control the amount of light entering through the pupil, and this is done by the sphincter and the dilator muscles, which adjust the size of the pupil. The iris' unique epigenetic pattern remains stable throughout adult life making a very good biometric traits for biometric systems (Masek, 2003). Figure 2.6 shows the image of an iris.

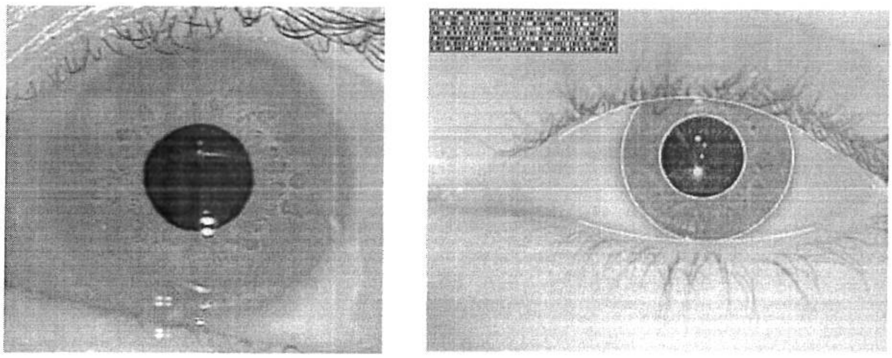

Figure 2.6 The Human Iris (Jain, Ross, & Prabhakar, 2004).

### 2.2.3 Smart Cards

A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card that has embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate. Since April 2009, a Japanese company has manufactured reusable financial smart cards made from paper. Smart cards can be either contact or contactless smart card. Smart cards can provide personal identification, authentication, data storage, and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations (Exuberantsolutions, 2016).

Figure 2.7: A smart card (Exuberantsolutions, 2016).

A smart card (see Figure 2.7) is an electronic data storage system, possibly with additional computing capacity (microprocessor card), which is incorporated into a plastic card. The first smart cards in the form of prepaid telephone smart cards were launched in 1984. Smart cards are supplied with energy and a clock pulse from the reader via the contact surface. Data transfer between the reader and the card takes place using a bidirectional serial interface (I/O port). In practice, there are two basic types of smart card based upon their internal functionality: memory card and microprocessor card.

One of the primary advantages of the smart card is the fact that the data stored on it can be protected against undesired access and manipulation. Smart cards make all service that relate to information or financial transactions simpler, safer and cheaper. One disadvantage of contact-based smart card is the vulnerability of the contacts to wear, corrosion and dirt. Readers that are used frequently are expensive to maintain due to their tendency to malfunction. In addition, readers that are accessible to the public cannot be protected against vandalism.

### 2.2.4 Radio Frequency Identification (RFID) Systems

RFID systems are closely similar to the smart cards. Data is stored on an electronic data carrying device. However, unlike the smart card, the power supply to the data carrying device and the data exchange are achieved without the use of galvanic contacts, but using magnetic or electromagnetic fields. A typical RFID system is shown in Figure 2.8 below. The technical procedure is drawn from the field of radio and radar engineering. Due to the numerous advantages of RFID systems compared with other identification systems, RFID systems are beginning to conquer new mass market, and hence have been chosen for this project (Piramuthu, 2007).

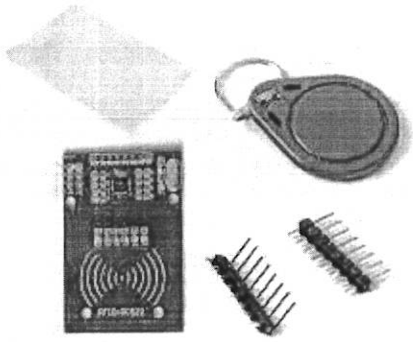

Figure 2.8: RFID kit (Piramuthu, 2007).

### 2.2.5 Comparison of Different Technology Based Access Control Systems

A comparison of these different identification and access control technologies is shown in Table 2.1 below, to demonstrate their parameter characteristics and the impact of influence factors against the data reading.

Table 2.1: Comparison of technology-based access control systems (Adapted from: Rieback and Crispo, 2006).

| Parameters | Barcode | Biometric | Smart card | RFID |
|---|---|---|---|---|
| Data density | Low | High | Very high | Very high |
| Reading speed | Low | Very low | Low | Fast |
| Reading Distance | 0~50 cm | 0~2m | Contact | 0~30m |
| Cost of readers | Very low | Very high | Low | Medium |
| Unauthorized copying / modification | Slight | Impossible | Difficult | Difficult |
| Influence of dirt | Very high | Low | Possible | No influence |

In the table above, it can be easily concluded that RFID technology is the best among all. Hence, RFID has been adopted in this project.

The cost of the technology with active sources is generally higher than those using passive or none sources. However, with the active source to power the electronics devices, they can offer more functions to achieve automation level in the systems. For RFID technology, the system can adopt the tags from passive, semi-active to active ones.

It can meet wider customer demands and offer the advantages covering both active and passive technologies. Meanwhile, with the advance of semiconductor technology and the volume used, RFID technology is gradually being implemented in a variety of devices, products and applications.

## 2.3 RFID SECURITY SYSTEM

Radio frequency identification security is composed of the following components; confidentiality or message content security, integrity of message content, authentication of sender and recipient non-repudiation by the sender, and availability (Ranasinghe and Engels, 2004).

Radio frequency identification has security concerns that must be addressed pertaining to vulnerabilities and making sure that confidential data remains secure. In the article The Evolution of RFID Security, Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum list the following as vulnerabilities to RFID system: replay-attack, man-in-the-middle attack, denial-of-service attack, and spoofing (Rieback et al., 2006). Additional vulnerabilities include tag-to-reader eavesdropping, reader-to-tag eavesdropping, rouge scanning, and counterfeiting (Juels, 2006).

Security concerns for RFID are similar in nature to those posed for computer networks. Similar to the TCP/IP networking model used for computer networks, the RFID communication model consists of the following layers for both the RFID reader and RFID tag; Application Layer, Data Link Layer, and the Physical Layer (Knospe and Pohl, 2004). The RFID model just like the TCP/IP model uses protocols to negotiate the transfer of data from the identification tag to the reader. Even though a single round protocol such as the Weise, Sarma, Rivest, and Engels uses a lock calculation, it is still susceptible to a replay attack (Piramuthu 2007) and is also vulnerable to a man-in-the-middle attack. However, the model purposed in the paper Security and Privacy Analysis of RFID Authentication Protocol for Ubiquitous Computing, utilizing a modified security protocol, is not vulnerable to a man-in-the-middle attack (Kim and Choi, 2007). The RFID communication model utilizes protocols to facilitate the transfer of information between component devices. In order to resolve the vulnerability posed by unauthorized access, Martin Feldhofer developed the Simple Authentication and Security Layer protocol (Feldhofer, 2004).

Cryptography is used to increase security and reduce the vulnerabilities that RFID tags experience. However, with the low cost of passive RFID tags being utilized, it is difficult to develop an algorithm that can fit the storage capacity (Robshaw 2006). Leonid Bolotnyy and Gabriel Robins, in their paper Physically Unclonable Function-Based Security and Privacy in RFID Systems, they discussed the use of a PUF based tag protocol instead of a cryptographic algorithm (Bolotnyy and Robins, 2007).

### 2.3.1 The Evolution of RFID

Radio Frequency Identification is a growing technology that has been around since early 1900's and was used in World War II. An early research paper had explored RFID work where the author of this paper stated that "Evidently, considerable research and development work has to be done before the field of useful applications is explored". Then, the electromagnetic theory related to RFID was studied in 1960's. Apart from that, inventions like Robert Richardson's "Remotely activated radio frequency powered devices" took place in that era. By this time, the wheels of RFID development had started turning. 1960's was the start of the adoption of RFID in commercial activities. A noticeable development work in this area had taken place in 1970's where vehicle tracking, factory automation etc. were the prime intentions.

By 1980's, RFID technology had taken shape in terms of the full implementation of the technology. The deployment of applications using this technology was noticed in 1990's.

The pace of developments in RFID is as well apparent in the 21st century where even the modest of item like cloth is bearing a small sticky patch of RFID and human implantation of RFID tag and that too of rice sized grain is the reality of the day.

The first use of radio wave to transmit the signals as similar to the RFID technology can date back to World War II when transponder (tags) were put on airplane and used to identify an approaching plane. Interrogators (readers) sent a signal to the transponder on the plane and the signal that is sent back could be used to distinguish between friendly and hostile aircraft. The history of RFID technology development is listed in the Table 2.1 below.

Table 2.2: The history of RFID technology development (Rieback and Crispo, 2006).

| **DECADE** | **EVENT** |
|---|---|
| 1940 – 1950 | Radar refined and used, major World War II development effort.<br>RFID invented in 1948. |

| | |
|---|---|
| 1950 – 1960 | Early explorations of RFID technology, laboratory experiments. |
| 1960 – 1970 | Development of the theory of RFID.<br>Start of applications field trials. |
| 1970 – 1980 | Explosion of RFID development.<br>Tests of RFID accelerate.<br>Very early adopter implementations of RFID. |
| 1980 – 1990 | Commercial applications of RFID enter mainstream. |
| 1990 – 2000 | Emergence of standards.<br>RFID widely deployed.<br>RFID becomes a part of everyday life. |

### 2.3.2 RFID Technology Development

Radio frequency identification is a developing technology that uses several basic components in order to satisfy the needs of the implementing organization. Radio frequency identification (RFID) is not a new technology. It has been around since the early 1900's and was utilized during World War II (Domdouzis et al., 2007). Radio frequency identification is a technology that uses a few simple components. The RFID tag system (see Figure 2.9 below), is composed of an antenna, integrated circuit, a reader that gathers information from the ID tag, and a database system that is used to store the information gained through interrogating the ID tag (Roberts, 2006).

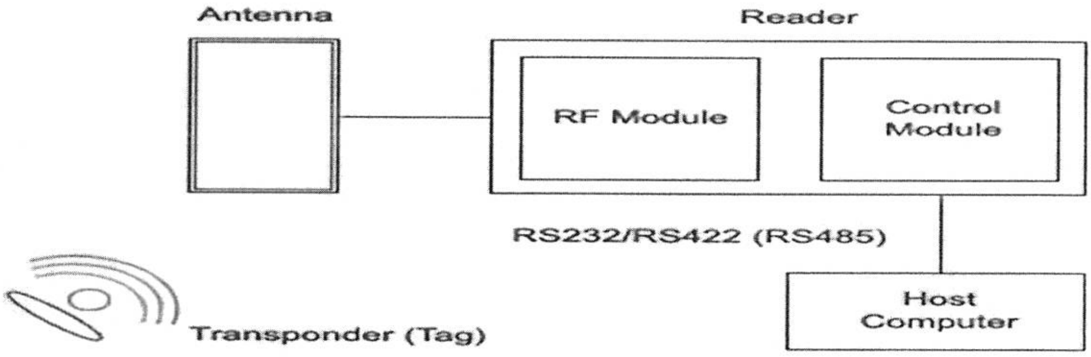

Figure 2.9: RFID tag system (Roberts, 2006).

Based upon the application, the identification tag can be active or passive. Active tags in addition to the circuit and antenna have a battery that powers the circuit and allows the tag to broadcast information that will be picked up by a reader (Roberts, 2006). Passive tags collect and store power from the reader through the use of a capacitor located within the circuit. The circuit then utilizes the energy collected to transmit tag information to the reader (Weinstein, 2005). Low cost passive tags are the predominantly used form of identification tag. The differences between active and passive tags are briefly discussed in the Table 2.2 below:

Table 2.3: Difference between active and passive tags (Roberts, 2006).

| **Active tags** | **Passive tags** |
|---|---|
| Active tags have a transmitter and their own power source (typically a battery) which is used to run the microchip's circuitry and to broadcast signal to the reader. | Passive tags have no battery, instead they draw power from the reader which sends out electromagnetic waves that induce a current in the tag's antenna |

| | |
|---|---|
| Active tags have a longer reading distance than passive tags | Passive tags have a short reading distance |
| Active tags are expensive and they have large sizes | Passive tags are cheaper and they have smaller sizes |

Deciding whether to use active or passive tags is an important component of the architectural design process. Architectural design of the RFID network is imperative when developing a RFID system. In their article Architecture design and performance evaluation of RFID object tracking systems, Chen et al., (2007) discussed the development of an RFID/IP gateway that uses the Object Naming Service (ONS) protocol to improve the performance of an RFID network. It is important to design a network that has the ability to scale in size and maintain data privacy (Solanas and Domingo-Ferrer, 2007). To meet application requirements, autonomous RFID systems have been developed that have the ability to read tags from greater distances (Jedermann and Behrens, 2006). Developing RFID technology to support data privacy and the utilization of secret-key, public-key, symmetric and asymmetric cryptographic algorithms to protect the data transmitted via the id tag during interrogation by the reader is critical to the protection and integrity of the system (Robshaw 2006). Additionally, design systems that are interoperable with other technologies such as global positioning satellite technology will allow the deployment of RFID systems designed for unique situations (Song and Haas, 2007).

## 2.4 MICROCONTROLLERS

A microcontroller is a solitary chip microcomputer fabricated from VLSI fabrication. A micro controller is also known as embedded controller. Today various types of microcontrollers are available in market with different word lengths such as 4 bits, 8 bits, 64 bits and 128 bits microcontrollers (Garfinkel, and Juels, 2005). Microcontroller is a compressed micro-computer manufactured to control the functions of embedded systems in office machines, robots, home appliances, motor vehicles, and a number of other gadgets. A microcontroller is comprises components like – memory, peripherals and most importantly a processor. Microcontrollers are basically employed in devices that need a degree of control to be applied by the user of the device (Electronicshub, 2017).

### 2.4.1 Features of a Microcontroller

Any electric appliance that stores, measures, displays information or calculates comprise of a microcontroller chip inside it. The basic structure of a microcontroller (See Figure 2.10 below) comprise of:

1. **CPU** – Microcontrollers brain is named as CPU. CPU is the device which is employed to fetch data, decode it and at the end complete the assigned task successfully. With the help of CPU all the components of microcontroller is connected into a single system. Instruction fetched by the programmable memory is decoded by the CPU.
2. **Memory** – In a microcontroller memory chip works same as microprocessor. Memory chip stores all programs & data. Microcontrollers are built with certain amount of ROM or RAM (EPROM, EEPROM, etc.) or flash memory for the storage of program source codes.

3. **Input/output ports** – I/O ports are basically employed to interface or drive different appliances such as- printers, LCD's, LED's, etc.
4. **Serial Ports** – These ports give serial interfaces amid microcontroller & various other peripherals such as parallel port.
5. **Timers** – A microcontroller may be in-built with one or more timer or counters. The timers & counters control all counting & timing operations within a microcontroller. Timers are employed to count external pulses. The main operations performed by timers' are- pulse generations, clock functions, frequency measuring, modulations, making oscillations, etc.
6. **ADC (Analog to digital converter)** – ADC is employed to convert analog signals to digital ones. The input signals need to be analog for ADC. The digital signal production can be employed for different digital applications (such as- measurement gadgets).
7. **DAC (digital to analog converter)** – this converter executes opposite functions that ADC perform. This device is generally employed to supervise analog appliances like- DC motors, etc.
8. **Interpret Control -** This controller is employed for giving delayed control for a working program. The interpret controller can be internal or external.
9. **Special Functioning Block** – Some special microcontrollers manufactured for special appliances like- space systems, robots, etc., comprise of this special function block. This special block has additional ports so as to carry out some special operations.

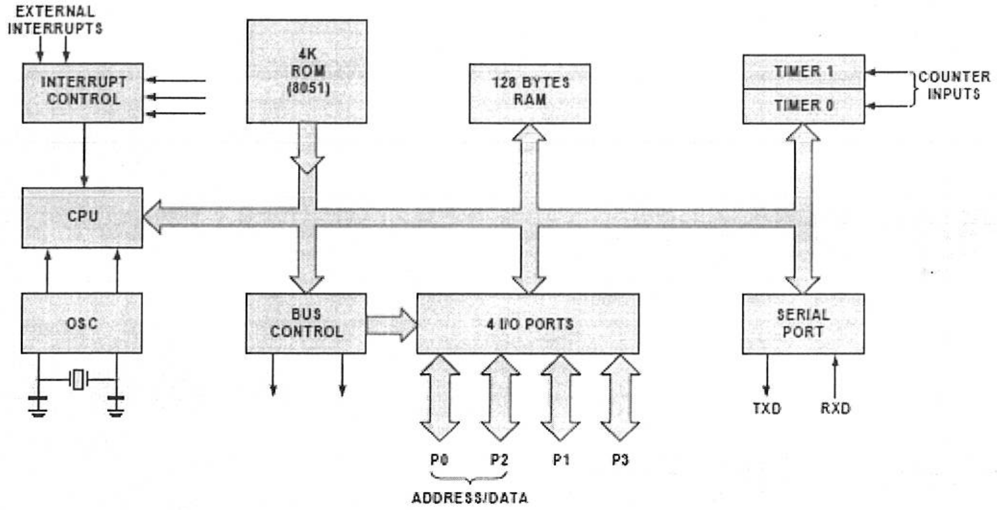

Figure 2.10: Block Diagram of a microcontroller (Domdouzis et al., 2007).

### 2.4.2 Categories of Microcontrollers

Microcontrollers are divided into categories according to their bits, memory, instruction sets, and memory architecture.

1. **Bits:**

- 8 bits microcontroller executes logic & arithmetic operations. Examples of 8 bits micro controller is Intel 8031/8051.
- 16 bits microcontroller executes with greater accuracy and performance in contrast to 8-bit. Example of 16 bit microcontroller is Intel 8096.
- 32 bits microcontroller is employed mainly in automatically controlled appliances such as office machines, implantable medical appliances, etc. It requires 32-bit instructions to carry out any logical or arithmetic function.

2. **Memory:**

- External Memory Microcontroller – When an embedded structure is built with a microcontroller which does not comprise of all the functioning blocks existing on a chip it is named as external memory microcontroller. For illustration- 8031 microcontroller does not have program memory on the chip.

- Embedded Memory Microcontroller – When an embedded structure is built with a microcontroller which comprise of all the functioning blocks existing on a chip it is named as embedded memory microcontroller. For illustration- 8051 microcontroller has all program & data memory, counters & timers, interrupts, I/O ports and therefore its embedded memory microcontroller (Harmon and Adams, 1989).

3. **Instruction Set:**
   - CISC- CISC means complex instruction set computer, it allows the user to apply one instruction as an alternative to many simple instructions.
   - RISC- RISC means Reduced Instruction Set Computers. RISC reduces the operation time by shortening the clock cycle per instruction.

4. **Memory Architecture:**
   - Harvard Memory Architecture Microcontroller
   - Princeton Memory Architecture Microcontroller

### 2.4.3 Families of Microcontroller

#### 1. 8051 Microcontroller

The most universally employed set of microcontrollers come from the 8051 family. 8051 Microcontrollers persist to be an ideal choice for a huge group of hobbyists and experts. In the course of 8051, the humankind became eyewitness to the most ground-breaking set of microcontrollers. The original 8051 microcontroller was initially invented by Intel. The two other members of this 8051 family are:

- 8052 – This microcontroller has 3 timers & 256 bytes of RAM. Additionally it has all the features of the traditional 8051 microcontroller. 8051 microcontroller is a subset of 8052 microcontroller.
- 8031 – This microcontroller is ROM less, other than that it has all the features of a traditional 8051 microcontroller. For execution an external ROM of size 64K bytes can be added to its chip.

8051 microcontroller brings into play 2 different sorts of memory such as- NV-RAM, UV-EPROM and Flash.

8051 microcontroller is an eight bit microcontroller launched in the year 1981 by Intel Corporation. It is available in 40 pin DIP (dual inline package). It has 4kb of ROM (on-chip programmable space) and 128 bytes of RAM space which is inbuilt, if desired 64KB of external memory can be interfaced with the microcontroller. There are four parallel 8 bits ports which are easily programmable as well as addressable. An on-chip crystal oscillator is integrated in the microcontroller which has crystal frequency of 12MHz. In the microcontroller there is a serial input/output port which has 2 pins. Two timers of 16 bits are also incorporated in it; these timers can be employed as timer for internal functioning as well as counter for external functioning. The microcontroller comprise of 5 interrupt sources namely- Serial Port Interrupt, Timer Interrupt 1, External Interrupt 0, Timer Interrupt 0, External Interrupt 1. The programming mode of this micro-controller includes GPRs (general purpose registers), SFRs (special function registers) and SPRs (special purpose registers).

## 2. PIC Microcontroller

Peripheral Interface Controller (PIC) provided by Micro-chip Technology to categorize its solitary chip microcontrollers. These appliances have been extremely successful in 8 bit micro-controllers. The foremost cause behind it is that Micro-chip Technology has been constantly upgrading the appliance architecture and included much required peripherals to the micro-controller to go well with clientele necessities. PIC microcontrollers are very popular amid hobbyists and industrialists; this is only cause of wide availability, low cost, large user base & serial programming capability (Juels, 2006).

The architecture of the 8 bit PIC microcontrollers can be categorized as below :

I. **Base Line Architecture** – In the base-line architecture PIC microcontrollers of PIC10F family is included, other than that a fraction of PIC12 & PIC16 families are also included. These gadgets make use of 12 bit program word architecture with six to twenty-eight pin package alternatives. Briefly defined attribute set of baseline architecture allows the most lucrative product solutions. This architecture is perfect for battery enabled gadgets. The PIC10F200 series is another reasonably priced 8 bit flash micro-controller with a 6 pin package.

II. **Mid-Range Architecture** – In this midline member of PIC12 & PIC16 families are added that attribute 14 bit program word architecture. The midrange PIC16 gadgets proffer a broad variety of package alternatives (from 8 to 64 package), with low to high levels of peripheral incorporation. This PIC16 appliance attributes a variety of analog, digital & serial peripherals, like- SPI, USART, I2C, USB, LCD & A/D converters. The mid-range PIC16 micro-controllers have suspended controlling ability with an eight level hardware load.

III. **High Performance Architecture** – The high performance architecture included the PIC18 family of appliances. These micro-controllers make use of 16 bit program word architecture along with 18 to 100 pin package alternatives. The PIC18 appliances are high performance micro-controllers with incorporated Analog to Digital converters. All PIC18 micro-controllers integrate a highly developed RISC architecture that supports flash appliances. The PIC18 has improved foundation attributes, 32 level deep load and several inner and exterior interrupts.

### 3. AVR Microcontroller

AVR also known as Advanced Virtual RISC, is a customized Harvard architecture 8 bit RISC solitary chip micro-controller. It was invented in the year 1966 by Atmel. Harvard architecture signifies that program & data are amassed in different spaces and are used simultaneously. It was one of the foremost micro-controller families to employ on-chip flash memory basically for storing program, as contrasting to one time programmable EPROM, EEPROM or ROM, utilized by other micro-controllers at the same time. Flash memory is a non-volatile (constant on power down) programmable memory.

AVR microcontrollers' architecture was developed by Alf-Egil Bogen and Vegard Wollan. The name AVR is derived from the names of the architecture developers of the microcontroller. The AT90S8515 was the foremost micro-controller which was AVR architecture based; on the other hand the foremost micro-controller to strike the commercial marketplace was AT90S1200 which was launched in the year 1997 (Domdouzis et al., 2007).

The SRAM, Flash and EEPROM all are incorporated on a single chip, thereby eliminating the requirement of any other external memory in maximum devices. Several appliances comprise of parallel external bus alternative, so as to add extra data memory gadgets. Approximately all appliances, except TinyAVR chips comprise serial interface, which is used to link large serial Flash & EEPROMs chips.

### 4. ARM Microcontroller

ARM is the name of a company that designs micro-processors architecture. It is also engaged in licensing them to the producers who fabricate genuine chips. In actuality ARM is a 32 bit genuine RISC architecture. It was initially developed in the year 1980 by Acorn Computers Ltd. This ARM base microprocessor does not have on-board flash memory. ARM is particularly designed for micro-controller devices, it is simple to be trained and make use of, however powerful enough for the most challenging embedded devices.

The ARM architecture is a 32 bit RISC processor developed by ARM Ltd. Owing to its power-saving attributes, ARM central processing units are prevailing in the mobile electronics marketplace, where less power expenditure is a vital design aim. ARM architecture comprise of the underneath RISC elements:-

- Maximum single cycle functioning
- Constant 16×32 bit register file.
- Load or store architecture.
- Preset instruction width of 32 bits so as to simplify pipe-lining and decoding, at minimized code density.
- For misaligned memory access there is no support.

### 2.4.4 Microcontroller Applications

Microcontrollers are intended for embedded devices, in comparison to the micro-processors which are used in PCs or other all-purpose devices. Microcontrollers are employed in automatically managed inventions and appliances like- power tools, implantable medical devices, automobile engine control systems, , office machines, remote controls appliances, toys and many more embedded systems. By dipping the size and expenditure in comparison to a design that make use of a different micro-processor, I/O devices and memory, micro-controllers formulate it inexpensive to digitally control more & more appliances and operations. Mixed signal micro-controllers are general; putting together analog constituents required controlling non-digital electronic structures (Domdouzis et al., 2007).

Microcontrollers can be applied in our day to day life devices. Some of the devices which they can be used are: Light sensing & controlling devices, temperature sensing and controlling devices, fire detection & safety devices, industrial instrumentation devices, process control devices and access control devices. Microcontrollers can also be used in making industrial control devices such as industrial instrumentation devices, Process control devices and also, access control devices (Electronicshub, 2017).

## 2.5 RELATED WORKS

It is becoming increasingly difficult to ignore the importance of security and privacy aspects in research and industrial appliance of RFID (Sarma et al, 2002). Juels' survey (Juels, 2005) gives a good introduction and overview on some of the central topics in RFID security. Lehtonen et al (2006) limited the scope of their examination to product authentication and a discussion of the trade-off between complexity and security in different RFID authentication methods.

Moreover, there are publications on state-of-the art in RFID privacy preservation (Simson et al, 2005), as well as numerous reviews on security and privacy concerning health care, e-commerce and data mining. The latter two are especially interesting, as essential privacy questions in these fields, like "What data is collected?" and "How is data secured during transmission?" apply to RFID as well. The central factor underlying these topics in e-commerce is trust (Avizienis et al., 2004; Belanger et al, 2002), a topic that can easily be anticipated in an RFID context. When RFID tagged objects hit the end-user market at a large scale, consumers' willingness to provide data will likely depend on individual perceptions of trustworthiness.

Deciding whether to use active or passive tags is an important component of the architectural design process. Architectural design of the RFID network is imperative when developing a RFID system. In their article Architecture design and performance evaluation of RFID object tracking systems, Chen et al. (2007) discussed the development of an RFID/IP gateway that uses the Object Naming Service (ONS) protocol to improve the performance of an RFID network.

In their paper, Yashi et al (2015) proposed a secure system that provides information about authorized and unauthorized persons. In that system, when a card brought is near to the RFID module it reads the card information and it compare with the data in the program memory and displays authorized or unauthorized entry. The door opens for authorized entry and marked the attendance corresponding to that code id and save in excel sheet format in SD card and after that display it's all information on the LCD like name and employee code number that link with authorize entry and welcome message with audio greetings by taking their name which is already saved into SD card and for unmatched entry the gate remain closed and alerts the security person through speakers by playing the separate audio file saying entry is unauthorized.

According to Solanas and Domingo-Ferrer, it is important to design a network that has the ability to scale in size and maintain data privacy (Solanas and Domingo-Ferrer, 2007). A quantitative analysis on a cell based network simulation was performed and the results were gathered for three different conditions to test the scalability of a private network. To meet application requirements autonomous RFID systems have been developed that have the ability to read tags from greater distances (Jedermann and Behrens, 2006). Developing RFID technology to support data privacy and the utilization of secret-key, public-key, symmetric and asymmetric cryptographic algorithms to protect the data transmitted via the id tag during interrogation by the reader is critical to the protection and integrity of the system (Robshaw, 2006). Additionally, design systems that are interoperable with other technologies such as global positioning satellite technology will allow the deployment of RFID systems designed for unique situations (Song and Haas, 2007).

Adeyanju et al. (2017) carried out a research work, titled, RFID based anti-theft and monitoring system for small objects. Their system was built around a microcontroller, programmed to read in data from RFID reader and send the data to a designated host. The host served as the database containing the information of each of the RFID tags embedded in the items to be secured. The reader can read data, which are kept in tags of each item and also reads the status of each item whether it is permitted to be taken out or not. Any unauthorized possession of item triggers the anti-theft alarm. Their system provided an automated and user-friendly method of tracking and monitoring small objects which could be adapted to securing various kinds of small items such as library books, laboratory and office equipment.

Adeyanju et al. (2017) also argued that the common anti-theft systems which were in place for monitoring small objects in places such as library, supermarkets, shopping malls, etc. were the watchful security guards and as CCTV (Closed Circuit Television) cameras. However, while the use of security guards has been proven inefficient and labor intensive

(Jinapon et al, 2008), the use of CCTV is far too expensive for most businesses or organizations in countries like Nigeria (as the cost of the goods shoplifted were often less than the cost of installing and maintaining the expensive security systems), hence, they made use of RFID technology which provides a convenient, efficient, and affordable technique to develop automated security systems and access control mechanisms. RFID allows automatic identification of tagged objects and data collection using radio waves.

In their paper, Okomba et al. (2015) discussed the design and prototype implementation of an Arduino microcontroller based liquid crystal display (LCD) system that uses a light dependent resistor (LDR). The Arduino microcontroller was connected (hard-wired) to the pins of an LCD programmed to display a list of names continuously but one at a time. The system designed in this work was carried out using an Arduino microcontroller and not any other microcontroller because, Arduino microcontroller is a tool for making computers that can sense and control more of the physical world than the desktop computer. It's also an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board. Their system was designed using four main components including power supply unit, sensing unit, controller unit (Microcontroller) and display unit (LCD), and it works by the sensory unit triggering the circuit on changes in light intensity. On high light intensity, the sensor is at logic one and the microcontroller executes its programmed instructions by enabling the LCD to display the specified data in a continuous and an attached LED indicator illustrates the status of the sensor. The sensor status is reconfirmed for consistency until the sensor is in an inactive state which leads to the shutting down (switching off) of the system.

Oluwole et al. (2015) carried out a research work on the design details and implementation of a security lock system using card and code combination. Their system was fully controlled by an 8 bit microcontroller PIC16F876A which has a 2kbytes of ROM for the program memory. Their design concept of the prototype was an access control system that allows only authorized persons to access a restricted area. The code and card pattern was stored in the EEPROM so that we can change the code at any time. The system has a card slot which the card will be inserted into, if the card pattern matches with the one stored in the memory then it allows the code to be entered and if the code entered equals with the code stored in the memory then the relay gets on and then the door opens.

# CHAPTER THREE

# DESIGN METHODOLOGY

## 3.1 OVERVIEW OF THE ACCESS CONTROL SYSTEM

The access control system using RFID is built around a microcontroller, and it is programmed to read in data from an RFID tag through the RFID reader. The RFID reader sends this data (ID number of the RFID tag) to the microcontroller which checks whether or not the data from the RFID reader matches with the data that is programmed into the microcontroller. Figure 3.1 below shows the block diagram of the access control system.

The system is made up of hardware and software components which makes it an embedded system. The hardware components are RFID reader and tags, connecting cables, Nuvoton W78E052D microcontroller, keypad, power source and buzzer. In addition to these, an electromagnetic door lock is used as the actuator to perform the door lock.

The RFID reader is placed on the door and the data (ID numbers) of the tags (which is the data carrying device for radio frequency system) are registered as a part of the program into the microcontroller to automatically identify each tag. The power source will power the RFID reader, the actuators and the microcontroller. The door lock opens automatically when the tag of a registered user is read by the reader.

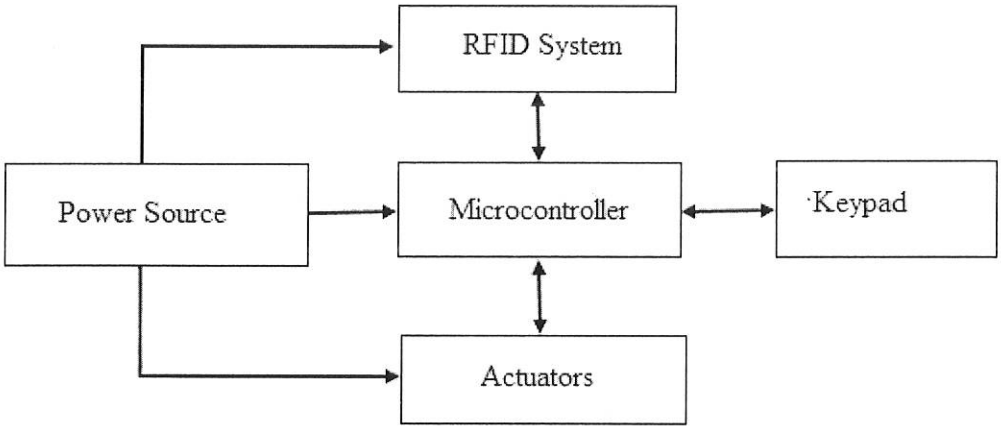

Figure 3.1: A block diagram of the access control system.

## 3.2 COMPLETE SYSTEM DESIGN

Proteus simulation application was used for the circuit design (see Figure 3.2 below). Proteus simulation application does not have Nuvoton microcontroller packages on it, hence, I used Atmel 89C52 microcontroller (because it has similar properties as that of Nuvoton W78E052D) to represent it. As seen in Figure 3.2 below, the electromagnetic door was represented with a DC motor; a 3×4 keypad is connected to the port 0 of the microcontroller to serve as an alternative means of unlocking the access control system in case a user is unable to find his tag. The RFID reader (Modulo Rx) and the RFID tag (Modulo Tx) are connected to the pins 3.0 and 3.1 respectively. The buzzer is also connected to the port 3 of the microcontroller; the function of the buzzer is to make a loud sound to alert the people around whenever an unauthorized personnel tries to use an unregistered RFIG tag to access the access control system (See Figure 3.2 below).

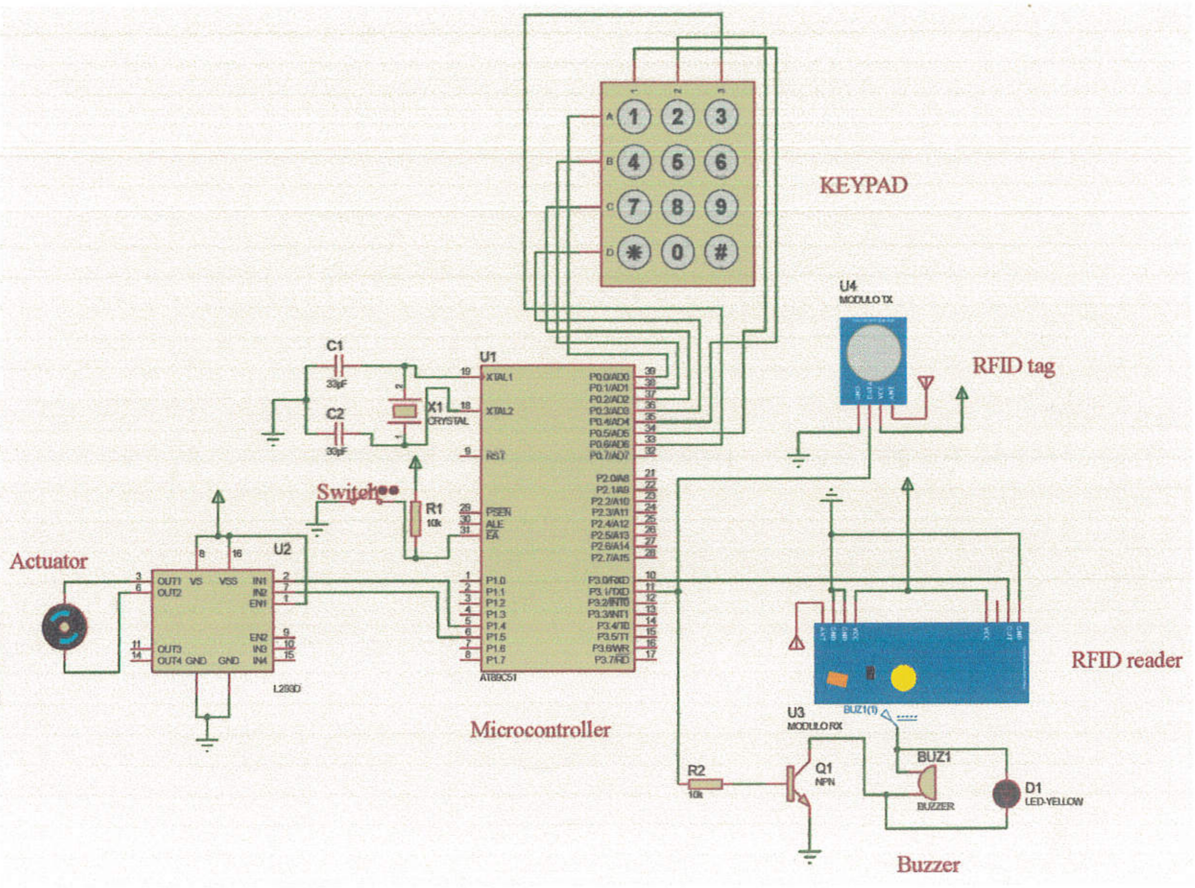

Figure 3.2: Circuit diagram of the access control system

## 3.3 POWER SOURCE

A power source is a device which delivers an exact voltage to another device as per its needs. Power sources, which are sometimes called power adapters, are available in various voltages, and they have varying current capacities, which is the maximum capacity of a power supply to deliver current to a load. For this project, a 12V power source will be required to power the RFID, as the RFID requires a 12V DC to work (Instructables, 2017). The power source as seen in Figure 3.3 below will convert a 110/240V AC into 12V DC. Here, the power supply employs the use of voltage regulator IC 7812. Herein, a regulated DC voltage is obtained from the mains 220VAC. A step down transformer is used to step down the 220V AC to 12V AC. The 12V AC is rectified to obtain a 12V DC voltage required to power the digital circuitry of the RFID reader.

The microcontroller, Nuvoton W78E052D, requires a 5-volt supply. For this system (as seen in Figure 3.3 below), the power supply employs the use of voltage regulator IC 7805. Herein, a regulated DC voltage is obtained from the mains 220VAC. A step down transformer is used to step down the 220V AC to 5V AC. The 5V AC is rectified to obtain a DC voltage required to power the digital circuitry.

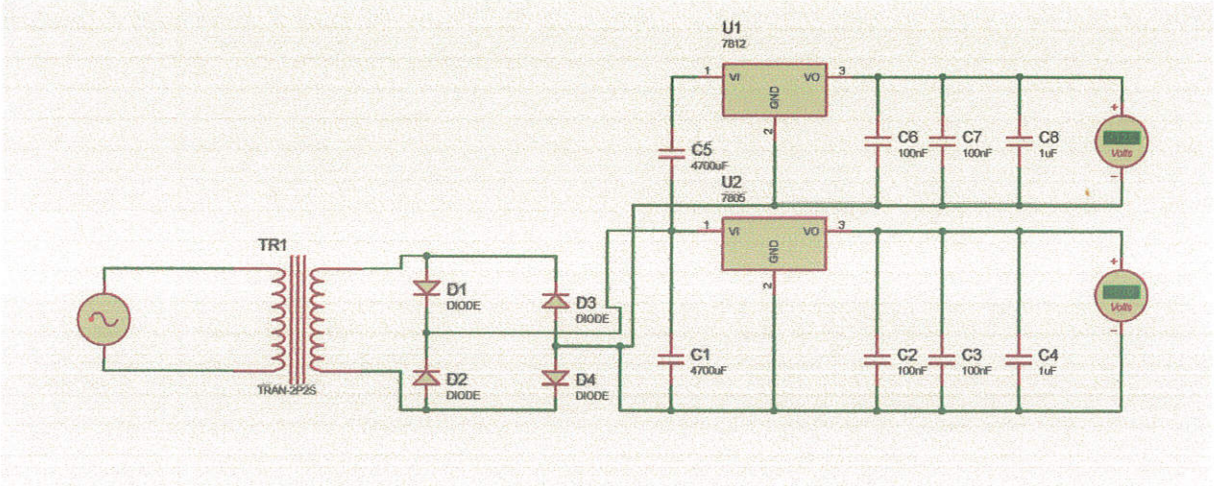

Figure 3.3: Schematic diagram of a 5/12V power source.

## 3.4 RFID SYSTEM

RFID systems are a reliable and maintenance-free option to control access rights. An authorized person gains access to an area by passing an RFID tag over a reader. The RFID system contains the RFID tag and the RFID reader.

### 3.4.1 RFID Tag

An RFID tag can either be passive, active or battery assisted. For this access control system, the RFID tag used is IPC80 passive RFID tag operating at a frequency of 125 KHz. The tags (Figure 3.4 below) have been pre-programmed with unique ID numbers which is printed on them. The RFID tags transmit information to the reader in Amplitude Shift Keying format.

Figure 3.4: Passive RFID tags

### 3.4.2 RFID Card Reader

An RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and then responds with its identification and other information (Mazidi et al, 2006). The IP10 RFID proximity card reader as seen in Figure 3.5 below works at an operating frequency of 125 KHz and reading distance up to 4 inches is used for this project. The reader can be easily installed on metal doors, as well as wooden doors, and it provides the tag information serially in RS232 format and is suitable for indoor as well as outdoor operations.

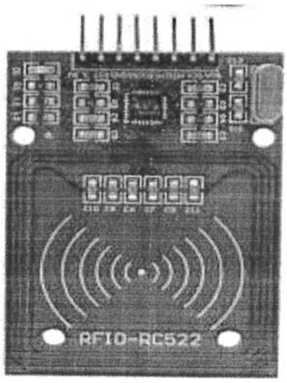

Figure 3.5: RFID reader.

## 3.5 MICROCONTROLLER

For effective development and usage, the Nuvoton W78E052D microcontroller was selected to be used for the development of this access control system. The program controlling the entire access control system is saved onto the memory of the microcontroller

### 3.5.1 Microcontroller Specifications

The Nuvoton W78E052D is an 8-bit microcontroller which can accommodate a wide frequency range with low power consumption. The instruction set for the W78E052D series is fully compatible with the standard 8052.

The W78E052D series contains 8Kbytes Flash EPROM programmable by hardware writer; a 256 bytes RAM; four 8-bit bi-directional (P0, P1, P2, P3) and bit-addressable I/O ports; an additional 4-bit I/O port P4; three 16-bit timer/counters; a hardware watchdog timer and a serial port. These peripherals are supported by 8 sources 4-level interrupt capability. To facilitate programming and verification, the Flash EPROM inside the W78E052D series allows the program memory to be programmed and read electronically. Once the code is confirmed, the user can protect the code for security.

The W78E052D microcontroller has two power reduction modes, idle mode and power-down mode, both of which are software selectable. The idle mode turns off the processor clock but allows for continued peripheral operation. The power-down mode stops the crystal oscillator for minimum power consumption. The external clock can be stopped at any time and in any state without affecting the processor. TheW78E052D series contains In-System Programmable (ISP) 2KB LD Flash EPROM for loader program, operating voltage from 3.3V to 5.5V (see Figure 3.6 below).

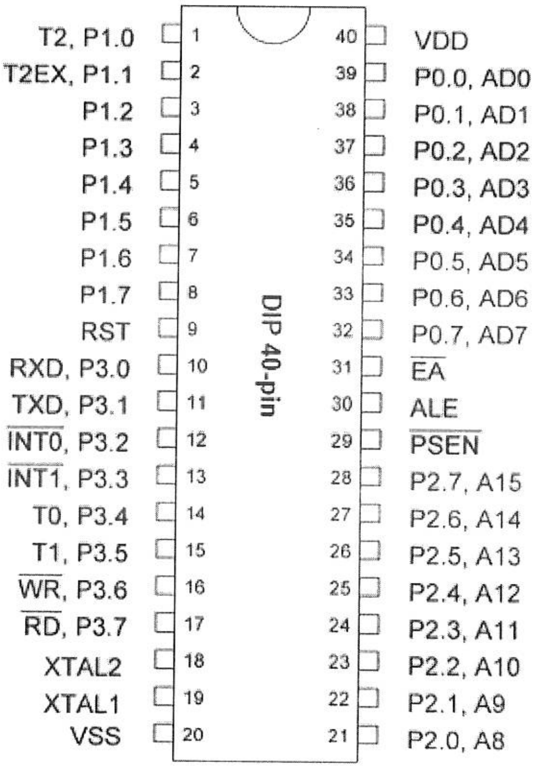

Figure 3.6: The schematic diagram of Nuvoton W78E052D Microcontroller

### 3.5.2 Microcontroller Programming

To program the microcontroller, the universal Programmer was used. The programmer has 40 pins ZIF sockets that are used for holding the pins of the microcontroller, and programming of a microcontroller is done using USB cables. The programmer supports only 5V devices and it has current protection that effectively protects the programmer and the devices (Graylogix, 2017).

The microcontroller was programmed with a code written in mikro C language and translated to assembly language (hex file) using Keil uVision software, before it was inserted into the development board. The loading of the hex file into the microcontroller was done using the Universal Programmer as shown in the Figure 3.7 below, with the aid of MikroProg software and a USB cable. AVR programmer software can also be used as an alternative for MikroProg software.

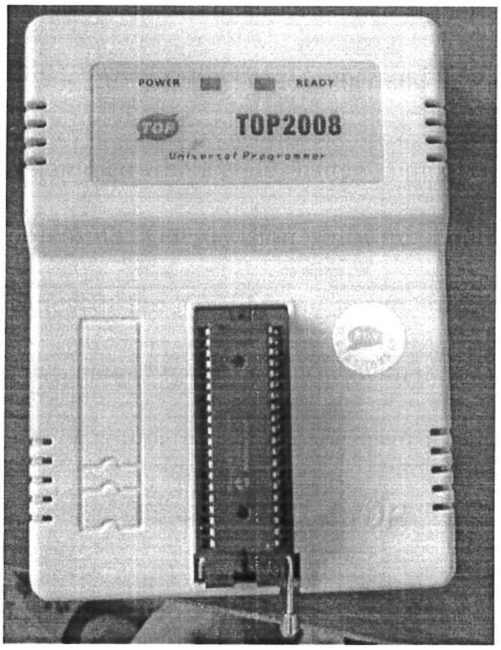

Figure 3.7: Universal Programmer for 8051 microcontroller

## 3.6 ACTUATOR

The actuator used is an electromagnetic lock, or magnetic lock, and it is a locking device that consists of an electromagnet and an armature plate (see Figure 3.8 below). Typically the electromagnetic portion of the lock is attached to the door frame and a mating armature plate is attached to the door. The two components are in contact when the door is closed. When the electromagnet is energized, a current passing through the electromagnet creates a magnetic flux that causes the armature plate to attract to the electromagnet, creating a locking action.

There are two main types of electric locking devices. Locking devices can be either "fail safe" or "fail secure". A fail-secure locking device remains locked when power is lost. Fail-safe locking devices are unlocked when de-energized. Direct pull electromagnetic locks are inherently fail-safe. The electromagnetic lock is equipped with a buzzer that allows someone outside the door to hear when the door is open.

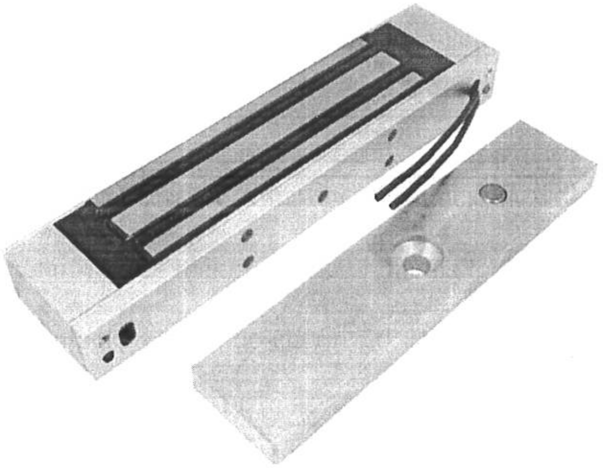

Figure 3.8: Electromagnetic lock.

## 3.7 KEYPAD

For the design of this system, I have used a 3x4 matrix keypad (See Figure 3.9 below). The function of the keypad is to alternatively enter a password to the system whenever a user can't find his RFID tag. The matrix keypad consists of a set of push buttons or switches which are arranged in a matrix format of rows and columns. The matrix is connected to the microcontroller which detects the key buttons pressed from the keypad. If the keypad input matches with the stored ID number in the microcontroller, the door opens, else, it remains locked.

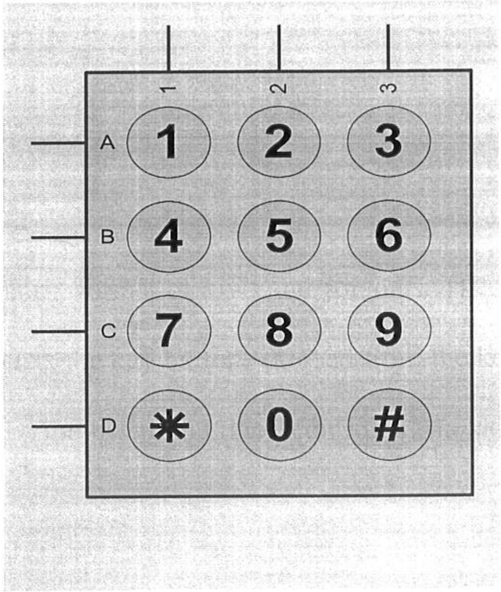

Figure 3.9: Keypad

## 3.8 THE WORK FLOW OF THE DEVELOPED ACCESS CONTROL SYSTEM

The designed access control system works according to the process flow below:

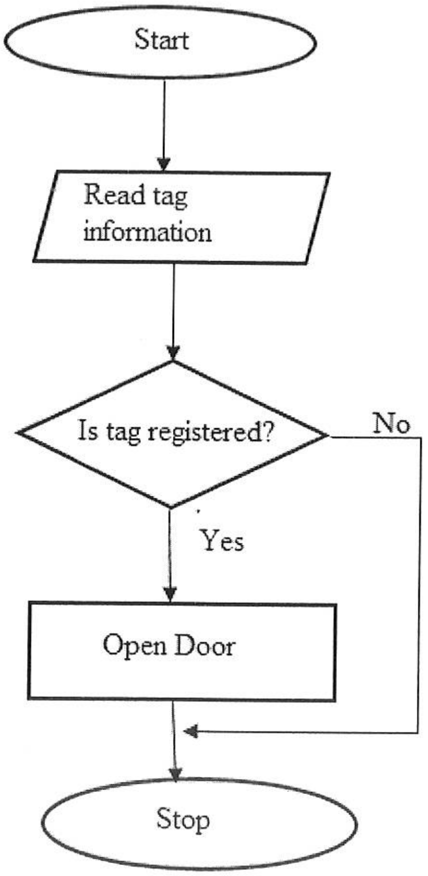

Figure 3.10: Process flow of the access control system.

The Figure 3.10 above shows the flow chart of the access control system. The details of the system is highlighted below:

- Step 1: A user approaches the door with his RFID tag, and places the RFID tag at a short distance from the RFID reader
- Step 2: The RFID reader reads the information contained in the tag as it comes in a range of few millimeters from reader.
- Step 3: after receiving the tag information, reader send this information to microcontroller for confirmation.

- Step 4: The microcontroller queries the program embedded in it and retrieves corresponding information after receiving the query from the reader.
- Step 5: Once the tag information is verified, the system generates a control signal through parallel port which controls the opening and closing of the electromagnetic door strike.

The signal information coming from RFID reader is matched with the stored program in the microcontroller. When the information which contains the ID number of the RFID tag matches with the stored information, the system grants access to the user.

## 3.9 PERFORMANCE EVALUATION

In order to ensure that all the necessary specifications and requirements are met, the performance of the system was evaluated in real life situations. Both the software and hardware will be tested by several users. The three major metrics used for the performance evaluation are Simulation parameters, Hardware testing and functional requirements.

### 3.9.1 Simulation Parameters

In order to ensure that the written program will be compatible with the system design, it is necessary that the system design should be simulated. To carry out the simulation, Proteus simulation tool was used to test the system design. The hex file of the written program is to be loaded onto the microcontroller in the system design and then the "play" button of Proteus is tapped. When the "play" button is tapped, if the written program is compatible with the system design, the actuator in the system design will move in an anti-clockwise direction indicating door opening, else, the actuator will not move to any direction.

### 3.9.2 Hardware Testing

Under this section, the system hardware components were tested independently to ensure that every component was in good working condition. For example, the voltage of the power source must be 12V, as any voltage that is less than or greater than 12V will have an effect on the system. Also, the AC current to be used to power the power source must be within the range of 110-240V; any voltage greater than 240V will damage the power source.

### 3.9.3 Functional Requirements

The system was evaluated by different users (using both registered tags and unregistered tags), based on its response to registered and unregistered tags, whether or not it saves tag information after reading the tag, whether or not it grants access to registered tags, whether or not it reads more than one tag information at a time, data management, theft tolerance, etc.

# CHAPTER FOUR

# IMPLEMENTATION AND RESULTS

## 4.1 SIMULATION RESULTS

When the simulation of the design of the RFID-based system was carried out using Proteus simulation tool, the actuator in the system design rotated in an anti-clockwise direction after three seconds (see Figure 4.1), indicating that the program is compatible with the system design and that the door will grant access to a registered RFID tag. The actuator remains opened for five seconds before it rotates back to its original lock position (See Figure 4.2).

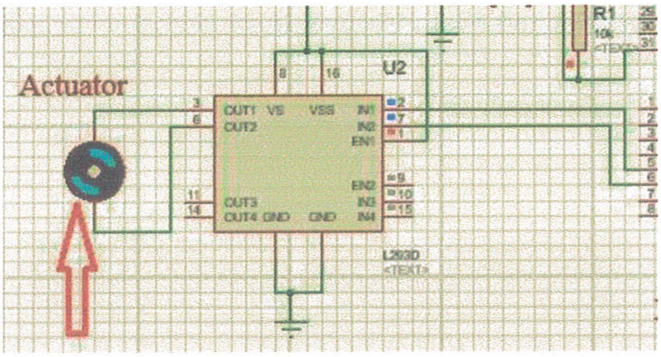

Figure 4.1: The position of the actuator after correct simulation

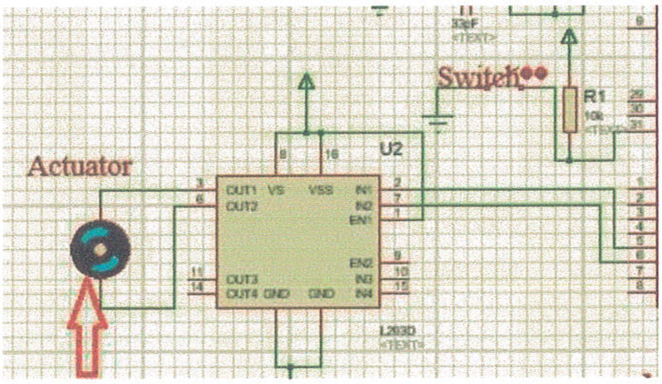

Figure 4.2: The position of the actuator before simulation

## 4.2 SYSTEM IMPLEMENTATION

The construction of this project was done in four different stages: Firstly, the implementation of the components in the system design onto a solderless experiment board (breadboard). Next is the transfer of components from the solderless experiment board to the development board, and then soldering the components permanently on the development board. Thirdly, the development board was connected to both the power source and the electromagnetic door lock. Finally, the entire project was coupled together into a casing. The Bill of Engineering Measurement and Evaluation (BEME) which highlights all the components used for the system implementation are listed in the Appendix section of this report.

## 4.3 COMPONENTS IMPLEMENTATION ON SOLDERLESS EXPERIMENT BOARD (BREADBOARD)

Firstly, the microcontroller (after it has been programmed using the universal programmer), the buzzer, the RFID reader, and the keypad were all setup on a breadboard and interconnected with each other as seen in the circuit diagram in section 3.2 of this report. Interconnections were done using jumper wires and a Multimeter was used to test every component to verify whether or not they are in good conditions. The Multimeter was also used to measure the voltage and current that gets to every component present in the connection.

## 4.4 COMPONENTS IMPLEMENTATION ON DEVELOPMENT BOARD

After a successful components layout and testing on the breadboard, the components were then transferred to the development board and were permanently soldered to the development board as seen in Figure 4.3 below. The microcontroller was placed on an IC holder before soldering it to the development board. Connection ports (12V and GND) are used to connect the development board to the power source.

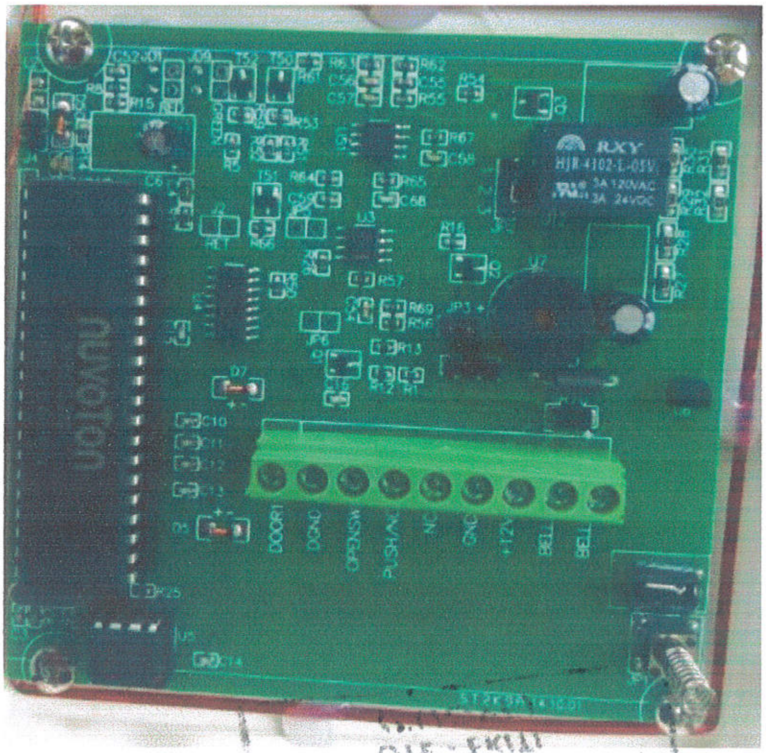

Figure 4.3: Development board after components installation

## 4.5 COMPONENTS INTERCONNECTION

After a successful layout of components on the development board, there is need to interconnect the development board with the electromagnetic door lock and the power source using connecting cables. The interconnection of the components is shown in the Figures 4.4 and 4.5 below. The electromagnetic door lock requires a 12V power supply, and this power is supplied by the power source. The live cable of the door lock is connected to the positive terminal of the power source and the ground cable is connected to the negative terminal of the power source. The development board is also connected to the power source through its ports 12V and GND.

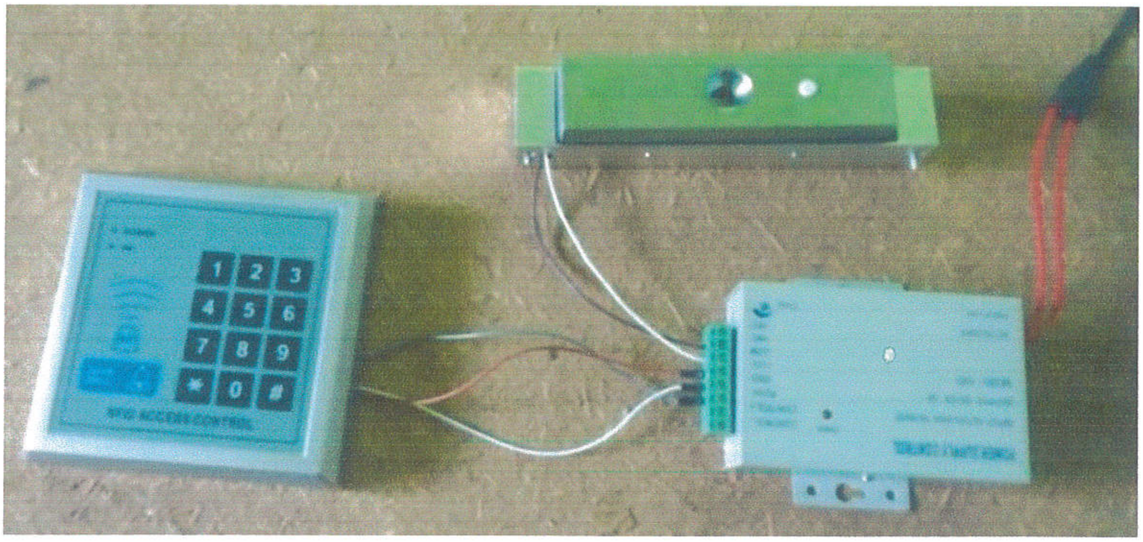

Figure 4.4: Interconnection of components (External view)

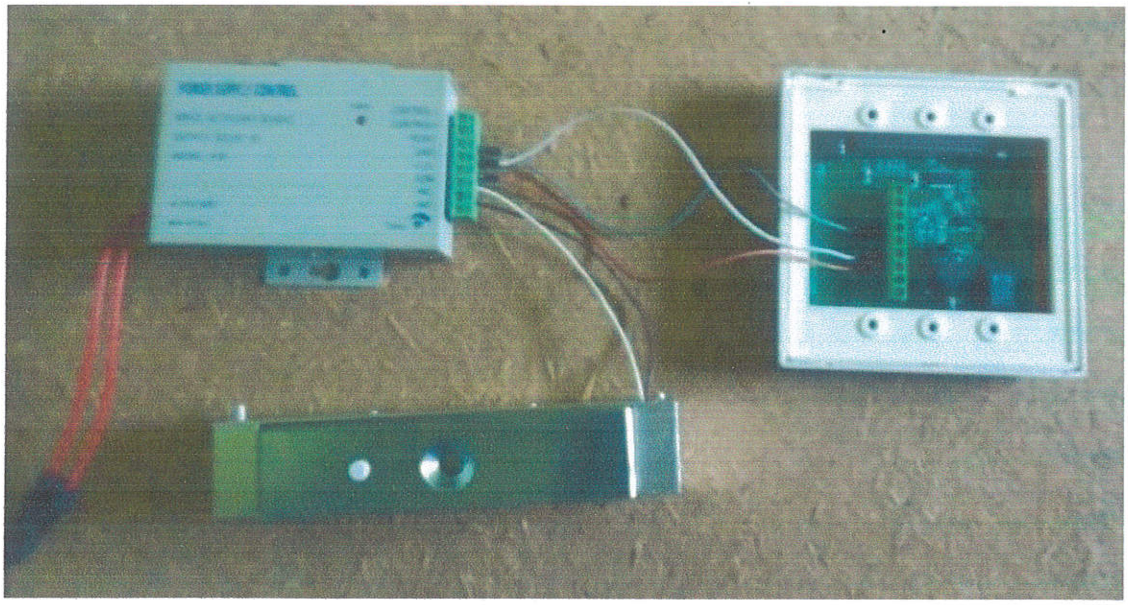

Figure 4.5: Interconnection of components (Internal view)

## 4.6 COUPLING OF PROTOTYPE COMPONENTS

After a successful components interconnection, the whole connection is tested to check whether or not it is in good working condition. If the connections perform the desired operation, then there is need to couple the components together into a casing. For this project, the casing used is a wooden box, and the components are well laid and screwed to the box. The development board which contains the RFID reader is placed in front of the box so as to be the first point of contact whenever a user tries to use the access control system. The power source is well housed inside the box and the electromagnetic door lock is attached to the door and door frame. The Figure 4.6 below shows the developed prototype of the access control system.

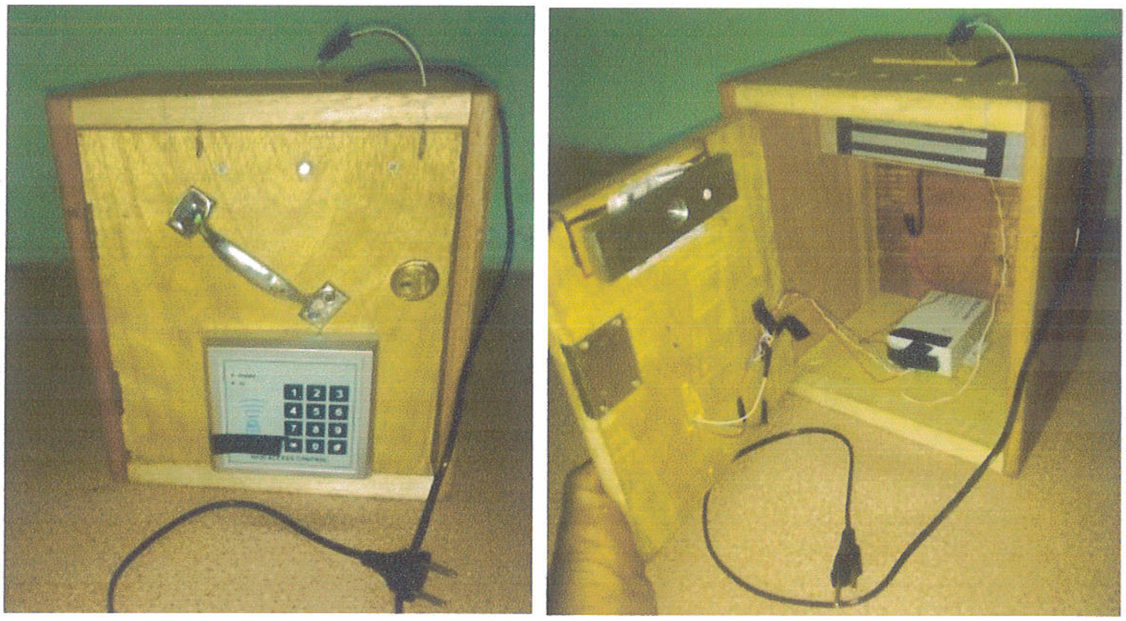

Figure 4.6: The prototype of the microcontroller based door access control using radio frequency identification

## 4.7 SYSTEM EVALUATION

In order to ensure that all the necessary specifications and requirements are met, the performance of the system has been evaluated according to real life situations. Both the simulation program and the hardware have been tested in real scenarios by many users. The two major metrics that have been used are Hardware testing and functional requirements.

### 4.7.1 HARDWARE TESTING

Under this section, all system hardware were tested independently using a Multimeter to ensure that every component is in good working condition. The system hardware components that were tested are the electromagnetic door lock and the power source.

**1. Testing the Power Source**

It is important that the power source must be tested since it provides power to the entire system. Any damage that results from the power source may damage the entire system. The result of testing the power source shows us that, the voltage of the power source must be 12V, as any voltage that is less than or greater than 12V will not make the system work or will damage the system respectively. Also, the AC current to be used to power the power source must be within the range of 110-240V; any voltage greater than 240V will damage the power source itself.

**2. Testing the Electromagnetic Door Lock**

The electromagnetic door lock requires a 12V DC power supply and a current of 800mA. It works best within the temperature range of 10°C to 55°C and within a humidity range of 0 to 95%. After testing the electromagnetic door lock, it was discovered that the door lock provides a holding force of as high as 180Kg, and a lock surface temperature of 20°C. The degree of alignment between the armature plate and the mounting plate determines how strong the holding force will be. Under high temperature (above 55°C), the electromagnetic door lock will not function properly.

### 4.7.2 FUNCTIONAL REQUIREMENTS

The system has been evaluated by different users (using three registered tags and two unregistered tags), based on its response to registered and unregistered tags, whether or not it saves tag information after reading the tag, whether or not it grants access to registered tags, whether or not it reads more than one tag information at a time, data management, and theft tolerance. See Table 4.1 below:

Table 4.1: Performance evaluation of the access control system

| **Functional Requirements** | **Yes** | **No** |
|---|---|---|
| Read registered tags | Yes | |
| Read unregistered tags | Yes | |
| Grant access to registered tags | Yes | |
| Grant access to unregistered tags | | No |
| Read more than one tag at a time | | No |
| Save tag information | | No |
| Data management | | No |
| Theft tolerance | | No |

Generally, according to the various users, the system performance is excellent; it has zero tolerance to theft and it cannot be easily manipulated. The system is user friendly and it can easily be used by those who have little or no knowledge about the use of electronics.

However, it should be noted that some environmental factors such as temperature would affect the accuracy of the system. The system will perform better at room temperature than when the temperature is higher than room temperature. Also, after a user has been granted access, there is a delay of five seconds after which the electromagnetic door lock will relock automatically. The system is a good anti-theft mechanism and it can be adopted in any organisation.

# CHAPTER FIVE

# CONCLUSION

## 5.1 CONCLUSION

In this project, a prototype of a microcontroller-based door access control system that is safe, accurate, user-friendly, independent, easy to manage, and efficient was designed and implemented using radio frequency identification technology. The system is implemented to perform access control on doors for both personal and public usage. A radio frequency identification reader is placed at the entrance of the door and it reads the status of an RFID tag which is to be presented by every person that wants to pass through the door. The RFID reader reads the information in the RFID tag and sends this read information to the microcontroller which serves as the database where tags details are stored. If the information of the presented tag matches with the information in the microcontroller, the door opens, else, it remains shut.

The system is user friendly and can easily be employed by those who have little knowledge about computers and electronics, thus, it can be implemented in either an academic institution or in organizations. Further improvements can also be made in order to make the access control system safer and better.

## 5.2 RECOMMENDATIONS

Several improvements can be made on the system to make it a better access control system. Some of the improvements are highlighted below:

1. An alternative source of power (such as a UPS) should be provided as a backup so as to ensure that the power supply to the entire system doesn't go off at any time.
2. Another security measure (e.g. biometric) can be added so as to further strengthen the security of the access control system.
3. A way to add more tags to the microcontroller of the access control system should can be provided.

# REFERENCES

Avizienis A., Laprie J.C., Randell B., and Landwehr C. (2004). Basic concepts and taxonomy of dependable and secure computing. Dependable and Secure Computing, IEEE Transactions 1(1): 11–33.

Adeyanju, I. A., Omidiora, E. O., & Oyedokun, O. F. (2015). Performance Evaluation of Different Support Vector Machine Kernels for Face Emotion Recognition. SAI Intelligent Systems Conference (pp. 804-806). London: SAI Intelligent Systems.

Adeyanju I.A., Omodunbi B.A., Adeleye O, Odeyinka C and Odiase P.O. (2017): RFID Based Anti-Theft and Monitoring System for Small Objects, In Proceedings of the 2017 Future Technologies Conference, to appear.

Anila, S., & Devarajan, N. (2012). Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions. Global Journal of Computer Science and Technology Graphics & Vision, Vol. 12, No.11, 13-18.

Arduino (2017). Retrieved from https://www.arduino.cc/en/Main/Software. Accessed on 2017/05/02.

Ari Juels (2005). RFID security and privacy: A research survey.

Ayoade, J. (2007). "Roadmap to solving security and privacy concerns in RFID systems." Computer Law & Security Report 23(6): 555-561.

Bai Qing-hai and Zheng Ying (2011). "Study on the Access Control Model in Information Security", Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, IEEE: 830-834.

Belanger F., Hiller J.S., and Smith W.J., (2002). “Trustworthiness in electronic commerce: the role of privacy, security, and site attributes”, Journal of Strategic Information Systems, Vol. 11, pages 245–270.

Bolotnyy, L. and G. Robins (2007). Physically unclonable Function-Based Security and Privacy in RFID Pervasive Computing and Communications.

Chaurasia, O. P. (2012). An Approach to Fingerprint Image PreProcessing . I.J. Image, Graphics and Signal Processing, No.5, Vol.6, 29-35.

Chen J. L., Chen M.C., Chien W.C. and Chang Y.C. (2007). "Architecture design and performance evaluation of RFID object tracking systems." Computer Communications 30(9): 2070-2086.

Domdouzis, K., B. Kumar, et al. (2007). "Radio-Frequency Identification (RFID) applications: A brief introduction." Advanced Engineering Informatics 21(4): 350-355.

Electronicshub (2017). Retrieved from http://www.electronicshub.org/microcontrollers/ Accessed on 2017/05/05.

Exuberantsolutions (2016). Retrieved from http://www.exuberantsolutions.com/smartcard-training.htm. Accessed on 2016/12/28.

Feldhofer M. (2004). “An Authentication Protocol in a Security Layer for RFID Smart Tags”. Electrotechnical Conference.

Garfinkel, S. and Juels A. (2005). "RFID privacy: an overview of problems and proposed solutions." IEEE Security & Privacy Magazine 3(3): 9.

Graylogix (2017). Retrieved from https://www.graylogix.com/index.php?main_page=product_info&products_id=74 Accessed on 2017/11/12

Harmon F. and Adams R. (1989). Reading between the Lines, p.13. Helmers Publishing, Inc, Peterborough, New Hampshire, USA

Instructables (2017). Retrieved from http://www.instructables.com/id/Make-a-simple-12-volt-power-supply/. Accessed on 2017/04/22.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technologies, vol. 14, no. 1, 1-66.

Jedermann R. and Behrens C. (2006). "Applying autonomous sensor systems in logistics--Combining sensor networks, RFIDs and software agents." Sensors and Actuators A: Physical 132(1): 370-375.

Jerichosystems (2017). Retrieved from https://www.jerichosystems.com/technology/abac.html. Accessed on 2017/04/28.

Jinaporn, N., Wisadsud, S., Nakonrat, P., & Suriya, A. (2008). Security system against asset theft by using radio frequency identification technology. In Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology 5(2): 761-764)

Juels, A. (2006). "RFID Security and Privacy: A Research Survey." IEEE Journal on Selected Areas in Communications 24(2): 13.

Juels, A. and J. Brainard (2004). "Soft Blocking: Flexible Blocker Tags on the Cheap". WEPS'04. Washington, DC, USA.

Juels, A. and Rivest R.L. (2003). "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". CCS'03. Washington, DC, USA: 9.

Jules A. and Weis S. A. (2006). "Defining Strong Privacy for RFID."

Karjoth G. and Moskowitz P.A. (2005). "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced". WPES'05 Alexandria, Virginia, USA: 4.

Kim H.S. and Choi J.Y., (2007). "Security and Privacy Analysis of RFID Authentication Protocol for Ubiquitous Computing, Computer Communications and Networks".

Knospe H. and Pohl H., (2004). "RFID security". Information Security Technical Report 9(4): 39-50.

Lehtonen M., Staake T., Michahelles F., and Fleisch E. (2006) "From identification to authentication - a review of RFID product authentication techniques". Printed handout of Workshop on RFID Security – RFID.

Masek, L. (2003). Recognition of Human Iris Patterns for Biometric Identification. The University of Western Australia.

Maxembedded (2016). Retrieved from http://maxembedded.com/2013/02/how-to-build-your-own-power-supply/. Accessed on 2016/12/29.

Mazidi M.A., Mazidi J.C., and Mckinaly R.D., 2006. "The 8051 Microcontroller and Embedded Systems".

Milyaev, Sergey, Barinova, Olga, Novikova, Tatiana, Kohli, Pushmeet, Lempitsky, Victor (2013). "Image binarisation for end-to-end text understanding in natural images".

Nancy A., Yogita S. and Santosh A. (2015). "A Survey on Access Control Models and Applications", International Conference on Internet of Things, Next Generation Networks and Cloud Computing.

Okereafor K.U, Onime C. and Osuagwu O.E. (2016) "Multi-biometric Liveness Detection - A New Perspective", West African Journal of Industrial and Academic Research, 16(1): 26 – 37.

Okomba N., Adeyanju I., Adeleye O., Omodunbi B. & Okwor C. (2015): Prototyping of an Arduino Micro-Controlled Digital Display System, African Journal of Computing and Information & Communication Technologies (AJOCICT), 8(1): 61-66.

Oluwole Jola, Zakka B. and Maijama'a L. (2015). "Microcontroller Based Security Lock System Using Card and Code Combination".

Piramuthu, S. (2007). "Protocols for RFID tag/reader authentication." Decision Support Systems 43(3): 897-914.

Ranasinghe, D. C. and Engels D.W. (2004). Low-cost RFID systems: confronting security and privacy. Proceedings of MIT Auto-ID Labs Research Workshop.

Rieback, M. R. and Crispo B. (2006). "The Evolution of RFID Security." IEEE Pervasive Computing 5(1): 7.

Roberts, C. M. (2006). "Radio frequency identification (RFID)." Computers & Security 25(1): 18-26.

Robshaw, M. J. B. (2006). "An overview of RFID tags and new cryptographic developments." Information Security Technical Report 11(2): 82-88.

Sarma, S. W. and Engels D. (2002). “RFID systems and security and privacy implications”. In Cryptographic Hardware and Embedded Systems, volume 2523 of Lecture Notes in Computer Science (LNCS), Redwood Shores, CA, USA: 454–469.

Searchsecurity (2017). Retrieved from http://Searchsecurity.techtarget.com/definition/access-control. Accessed on 2017/04/05

Simson L. G., Juels A., and Pappu R. (2005). RFID privacy: An overview of problems and proposed solutions. IEEE Security and Privacy, 3(3): 34–43.

Shoewu, O., Makanjuola, N., & Olatinwo, S. (2014). Biometric-based Attendance System: LASU Epe Campus as Case Study. American Journal of Computing Research Repository, Vol. 2, No. 1, 8-14.

Smith A. D. (2005). "Exploring radio frequency identification technology and its impact on business systems." Information Management & Computer Security 13(1): 12.

Sparkful (2017). Retrieved from https://learn.sparkful.com/tutorials/what-is-a-breadboard. Accessed on 2017/04/22.

Solanas, A. and Domingo-Ferrer J. (2007). "A distributed architecture for scalable private RFID tag identification." Computer Networks 51(9): 2268-2279.

Song J. and Haas C.T. (2007). "A proximity-based method for locating RFID tagged objects." Advanced Engineering Informatics 21(4): 367-376.

Tappert C. C., Suen, C. Y., Wakahara, T. (1990). "The state of the art in online handwriting recognition". IEEE Transactions on Pattern Analysis and Machine Intelligence.

Weinstein R. (2005). "RFID: A Technical Overview and Its Application to the Enterprise." IEEE IT Professional 7(3): 6.

Wenrong Z., Yuhao Y., and Bo L. (2014) "Content-Based Access Control: Use Data Content to Assist Access Control for Large-Scale Content-Centric Databases," IEEE International Conference on Big Data, IEEE: 701-710.

Yashi Mishra, Gaganpreet Kaur Marwah and Shekhar Verma (2015). "Arduino Based Smart RFID Security and Attendance System with Audio Acknowledgement".

# APPENDIX

## APPENDIX A: Bill of Engineering Measurement and Evaluation (BEME)

For the complete development of the microcontroller-based door access control system using Radio Frequency Identification, the items used are highlighted in the Table A below:

Table A: BEME for the entire access control system

| S/N | ITEM | QTY | RATE (IN NAIRA) | AMOUNT (IN NAIRA) |
|---|---|---|---|---|
| 1 | RFID Reader module | 1 | 5,000.00 | 5,000.00 |
| 2 | RFID tag | 5 | 150.00 | 750.00 |
| 3 | EM lock | 1 | 9,700.00 | 9,700.00 |
| 4 | Jumper wires | 20 | 20.00 | 400.00 |
| 5 | Buzzer | 1 | 100.00 | 100.00 |
| 6 | LED | 2 | 15.00 | 30.00 |
| 7 | Microcontroller | 1 | 450.00 | 450.00 |
| 8 | Keypad | 1 | 550.00 | 550.00 |
| 9 | Power Source | 1 | 4000.00 | 4,000.00 |
| 10 | Development Board | 1 | 1,200.00 | 1,200.00 |
| 11 | Soldering Iron and Drilling Machine | | | 4,700.00 |
| 12 | Wooden Prototype box | | 1,200.00 | 1,200.00 |
| | **TOTAL** | | | **28,080.00** |