

UNIVERSITY OF NAIROBI



**TITLE: ACCESS CONTROL NETWORK FOR A COMPLEX
BUILDING**

PROJECT NUMBER 135

BY: OPIYO ALBERT NYAMOLO

REG. NO: F17/28635/2009

SUPERVISOR: PROF. M.K. MANG'OLI

EXAMINER: DR. W.C. WEKESA

**Project submitted in partial fulfillment of the requirement for the
award of a bachelor's degree in Electrical and Electronic Engineering
at the University of Nairobi.**

Date of submission: 28th April, 2014

**DEPARTMENT OF ELECTRICAL AND INFORMATION
ENGINEERING**

DECLARATION OF ORIGINALITY

NAME OF STUDENT: OPIYO ALBERT NYAMOLO

REGISTRATION NUMBER: F17/28635/2009

COLLEGE: ARCHITECTURE AND ENGINEERING

FACULTY/ SCHOOL/ INSTITUTE: ENGINEERING

DEPARTMENT: Electrical and Information Engineering

COURSE NAME: Bachelor of Science in Electrical & Electronic Engineering

TITLE OF WORK: Access Control Network for a Complex Building

- 1) I understand what plagiarism is and I am aware of the university policy in this regard.
- 2) I declare that this final year project report is my original work and has not been submitted elsewhere for examination, award of a degree or publication. Where other people's work or my own work has been used, this has properly been acknowledged and referenced in accordance with the University of Nairobi's requirements.
- 3) I have not sought or used the services of any professional agencies to produce this work.
- 4) I have not allowed, and shall not allow anyone to copy my work with the intention of passing it off as his/her own work.
- 5) I understand that any false claim in respect of this work shall result in disciplinary action, in accordance with University anti-plagiarism policy.

Signature:

Date:

CERTIFICATION

This report has been submitted to the Department of Electrical and Information Engineering University of Nairobi with my approval as the supervisor.

.....

Prof. M.K. Mang'oli

Date:

DEDICATION

This project is dedicated to all the individuals and/or parties that will find the information contained in this report beneficial.

ACKNOWLEDGMENTS

I would like to express special thanks to my supervisor Prof. M.K. Mang'oli for giving me guidance and support throughout the project.

I do not forget to thank my family and especially my brother Nico Opiyo for the advice that has been continually offered, moral support, recommendation and suggestion of useful ideas that have been of great help and importance.

My extended gratitude goes to my fellow classmates for moral support and their continuous encouragement to continue with the work.

Finally above all, I thank the Almighty God for grace and strength.

Table of Contents

DECLARATION OF ORIGINALITY	ii
CERTIFICATION	iii
DEDICATION	iv
ACKNOWLEDGMENTS	v
Table of Contents	vi
List of Figures	viii
List of Tables	ix
List of Abbreviations	x
ABSTRACT	1
Chapter 1 INTRODUCTION	2
Chapter 2 LITERATURE REVIEW	5
2.1 Background	5
2.2 System Architecture	6
2.2.1 Head-end Computer	7
2.2.2 Field controllers	7
2.2.3 Input devices	8
2.3 Authentication Factors	8
2.3.1 Type 1	8
2.3.2 Type 2	8
2.3.3 Type 3	9
2.4 Access Control Criteria	9
2.5 Access Control Models	9
2.5.1 Discretionary Access Control (DAC)	10
2.5.2 Mandatory Access Control (MAC)	11
2.5.3 Non-discretionary Access Control	11
2.6 Access Control Technologies	12
2.6.1 Passwords	12
2.6.2 Wiegand Card Readers	13
2.6.3 Biometrics	14
2.6.4 Magnetic Cards	16
2.6.5 Smart Cards	17
2.7 Access Control Administration	19
2.7.1 Centralized Access Control	19
2.7.2 Decentralized Access Control	19
2.8 Access Control Types	19
2.9 Access Control Threats	19
2.9.1 Spoofing/Masquerading	19
2.9.2 Dictionary Attacks	19
2.9.3 Brute Force attacks	20
2.9.4 Software Malice	20
2.9.5 Emanations	20
2.9.6 Denial of Service Attack (DoS)	20
Chapter 3 DESIGN METHODOLOGY	21
3.1 Building Design	21
3.1.1 Access Control Plans	21
3.1.2 Bill of Quantities	24
3.1.3 Control Model	24
3.2 Access Control	25
3.2.1 Design Model	25

3.2.2 Access Technique.....	26
3.2.3 Access Control Devices.....	27
3.3 Database System.....	31
3.3.1 Access Control Flowchart	33
3.3.2 Pseudo code.....	34
3.3.3. Tables	36
Chapter 4 RESULTS AND ANALYSIS.....	39
4.1 Results	39
4.1.1 Access Request Cycle	39
4.1.2 Updating Database.....	42
4.1.3 Data Analysis.....	44
4.2 Analysis	46
4.2.1 Operation.....	46
4.2.2 Device Analysis	47
4.2.3 Administration	48
4.2.4 System Security	48
Chapter 5 CONCLUSION.....	50
REFERENCES	51
APPENDIX	52

List of Figures

Figure 2.1 Lock and Key

Figure 2.2 System Architecture

Figure 2.3 Flow of signal

Figure 2.4 Keypad

Figure 2.5 Wiegand

Figure 2.6 Fingerprint

Figure 2.7 Error Rate Diagram

Figure 2.8 Magnetic Card

Figure 2.9 Smart Card

Figure 2.10 Key Tag

Figure 2.11 RFID Card

Figure 3.1 Ground Floor Doors

Figure 3.2 Typical Floor Doors

Figure 3.3 ACS Diagram

Figure 3.4 RFID Tag Schematic

Figure 3.5 Bollard

Figure 3.6 Safety Loop

Figure 3.7 System Software Interconnection

List of Tables

Table 3.1 Ground Floor Doors

Table 3.2 Typical Floor Doors

Table 3.3 Privilege Levels

Table 3.4 Frequency Range Specification

Table 3.5 Tag Quantity

Table 3.6 Card Readers Breakdown

Table 3.7 REX devices Breakdown

Table 3.8 Users Table

Table 3.9 Journal Table

Table 3.10 Clearance Table

Table 3.11 DoorID Breakdown

List of Abbreviations

ACS	-	Access Control List
DAC	-	Discretionary Access Control
DFO	-	Door Forced Open
HTML	-	Hyper Text Markup Language
MAC	-	Mandatory Access Control
OTL	-	Open Too Long
PHP	-	PHP Hypertext Preprocessor
RBAC	-	Role Based Access Control
REX	-	Request-To-Exit
RFID	-	Radio Frequency Identification
RS	-	Recommended Standard

OBJECTIVE: To design and simulate an access control system for a complex building in Nairobi.

ABSTRACT

The project is aimed at designing a physical access control system(PACS) that will control entry and exit of personnel within a complex building as well as keeping a record of access events to various parts of the building by storing them in a central database.

The building is complex in that it has rental apartments as well as offices in one structure which need to be centrally managed and monitored using this control system. Optimum access control flexibility is the target so as to enhance security within the premises as well as decreasing the access time at various locations within the building. This is an improvement in efficiency in regards to ease of access.

Traditional systems have in the past used simple mechanical systems with simple key and lock mechanisms which have proven to work well but not sufficient and efficient enough. This has led to the development of complex electronic systems which enhance the security which is already provided by the mechanical systems and in addition to that, giving more security options such as logging of access information in a database to form a system journal which is key in management.

Control and monitoring of the complex structure from a central unit is the overall goal of this project and step-by-step development of this system is to result into a modern high speed access building with an incorporated high level of security.

Chapter 1 INTRODUCTION

Designing and simulating the access control system requires a co-ordination of different blocks/components to achieve the ultimate goal of high level security with minimal time of access to the desired location within the building.

Various methods used to allow external personnel to control certain essential devices located within a building. There are various methods and techniques that are used to control access and therefore theoretical as well as practical analysis is necessary to determine the method that is most suitable for a specific project which in this case is access control of a complex building. The main building blocks of the system are:

1. Identification and Authentication
2. Access Control
3. Database Management

These three blocks function independently and give individual outputs. Due to the interconnection of the blocks each output is transmitted along various paths and intelligent interaction of the blocks through the data paths results in a meaningful overall output.

IDENTIFICATION AND AUTHENTICATION

Identification is the process by which the user of the system provides specific information attached to that user to the authentication service. Authorization refers to the process of identifying and ascertaining a system user. The very first interface encountered by the user in the system is the Identification and Authentication interface. The user is required to issue credentials which are sent to a central database where all the user information is stored. The credentials that are received at the database are compared with those that already exist. The result is then issued to the control panel after which access will either be granted or denied. There are various methods employed for communication between the user and the system to give the credentials required for identification of users and hence access to the system.

ACCESS CONTROL

This block is the hub of the whole control system. It plays perhaps the most important role in the system because it is the block which sends and receives information to and from different parts of the system and makes a decision on what task should be carried out, when and how it should be carried out. It can only be compared to the central processing unit of a computer.

An access control design defines the rules for users accessing files or devices. The designs have users referred to as subjects and they access data or resources known as objects.

DATABASE MANAGEMENT SYSTEM

A database is a collection of structured and related data items organized so as to provide a consistent and controlled access to the items.

A database management system facilitates the creation, organization and maintenances of databases. It is used to manipulate, store, edit and update records and ensure continuous record keeping in a database. This enables the administrator to monitor the building more efficiently and use the generated statistics of entry and exit to make decisions on improvement of the security system as well as ease of access.

The operation of modern buildings can support a vast amount of static and real-time data. Static information such as building schematics is vital for security and rescue purposes. There is a need for first responders to be notified of designated building alerts in real-time so that actions can be performed promptly. Improvement of this system can be implemented with modern technology by introducing capability to keep the first responders updated with the latest building information during emergency situations as well as the ability to remotely control certain building devices and processes can be realized[1]. A database is necessary to store the logs/records of activities that have taken place, that are taking place and that will take place within the building in terms of access. This enables the administrator to monitor the building more efficiently and use the generated statistics of entry and exit to make decisions on improvement of the security system as well as improvement on the ease of access.

For the apartments, it is desired that the database should keep accurate records of tenant occupancy of each of the rooms as well as their account details available for reference at any given time. The records should also include logs of access points of the tenant, time of access and whether or not access has been granted.

This is necessary so that all tenants within the building operate within the specified

criteria of the building administrator. For the offices section of the building, a similar method of accurate record keeping is desired and the only major difference is that the users of a certain restricted area are generally more in number as compared to the apartment section. The records are therefore based on clearance codes because access is controlled based on predefined privileges. It is from the database that identification and authentication processes are carried out. This calls for stability and accuracy. When the database system fails, the access control block cannot function independently. The database needs to have storage capacity that is sufficient to keep records of all the users of the system as well as all the activity logs within the building.

Chapter 2 LITERATURE REVIEW

2.1 Background

Access control is a way of limiting access to a system or to physical or virtual resources.

The need to protect assets has been in existence almost since the beginning of mankind.

The early forms of protection have only involved physical barriers such as:

- Doors
- Gates
- Barriers
- Fences
- Security guards

Doors and gates are secured using locks and keys.



Figure 2.1 Lock and Key

In addition, security guards have been employed to man the gates to ensure that unauthorized personnel do not get access to premises which they are unwanted.

For mechanical lock and key protection scheme:

- a) The door or gate can be opened at any time as long as the correct key is available.
- b) When a key is lost, either the door has to be broken or a duplicate key used to open the door.
- c) Each door has a specific key and cannot be opened by any other key.
- d) It cannot be known who opened a door by examining the lock or key at hand.

The mechanical lock and key scheme has faced many challenges such as insecurity, inefficiency, unreliability and monitoring inability among others.

It's generally said that the roots of radio frequency identification technology can be traced back to World War II. The Germans, Japanese, Americans and British were all using radar—which had been discovered in 1935 by Scottish physicist Sir Robert

Alexander Watson-Watt—to warn of approaching planes while they were still miles away. The problem was there was no way to identify which planes belonged to the enemy and which were a country's own pilots returning from a mission.

The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back. This crude method alerted the radar crew on the ground that these were German planes and not Allied aircraft (this is, essentially, the first passive RFID system [2]. Electronic access control uses computers to solve the limitations of mechanical locks and keys. It manifested itself in the 1960s and served to reinforce the security that was already provided by the physical barriers.

The earliest systems of electronic access control basically consisted of keypads which required pin codes for access to restricted doors. After that, the swipe technology closely followed. Non-contact proximity cards replaced the swipe cards in the 1970s and were very much popular for their big advantage of the major reduction of complexity in access. The problems associated with physical keys were instantly done away with such as having many keys for different location access.

The development in technology also allowed for the generation of log reports on the entry and exit of people at different locations at different times. [3] The proximity readers have maintained their popularity up to date and only the technology of the readers have been advancing. The card readers are connected to intelligent controllers which either store information or directly communicate with a control panel and generate useful information which is necessary for routine management.

The modern systems come with extra packages such as digital telephony, video recording, among others. The advantageous disadvantage is a seemingly high initial cost of setting up with a hidden advantage of preventing advanced level theft which may result in big losses.

2.2 System Architecture

This refers to the interconnection of access control system devices or how the devices relate to each other.

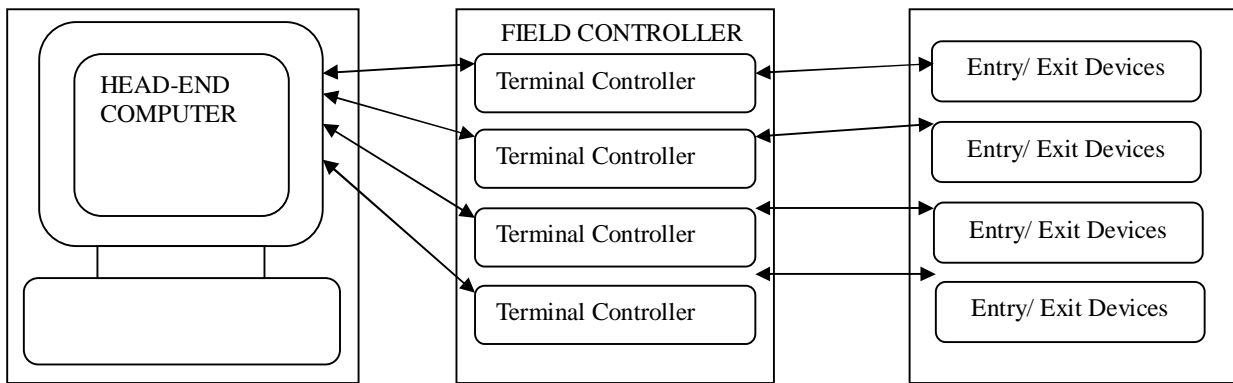


Figure 2.2 System Architecture of an Access Control System

The architecture has three levels:

2.2.1 Head-end Computer

The computer sends, receives and processes data on the access control network. It provides display for the operator to monitor system operation by interrogating the system. The computer has the ability to request for any specific information regarding the status of any of the devices within the system. And initiate specific actions at any specified location within the system. The computer also provides storage and a means for retrieving info, creating reports and backing up data.

Today security systems are networked and they feature distributed architecture. Processing is spread out at points throughout the network rather than having all processing capability residing at the head end. Field controllers provide the system with this processing capability. A field controller consists of:

- Central Processing Unit
- Input/ Output (I/O) Modules
- Card reader modules
- Network Communication capability

2.2.2 Field controllers

A field controller allows continuous functioning of the system even when the head-end temporarily shuts down. In such a case, the controllers store all event activity for uploading to the main database after it returns back to normal state. Scheduled data exchange between field controllers and head-end computer ensures that the database is up to date and that current information is available to the field controller. Security

networks are increasingly being designed to use industry standard communication protocols. E.g TCP/IP. This ensures high levels of reliability and minimum downtime in the event of a component failure.

2.2.3 Input devices

The term Input devices refers to any detectors that report their status to a computer electronically. They provide data to the processor regarding the current condition at a given location. These are:

- Door switches
- Card reader or keypad devices
- Locking devices
- REX devices

Card readers and keypads are the most sophisticated door peripherals used in operation of an access control system. An access control door must be equipped with a locking mechanism, either electric door strike or magnetic lock, which can be controlled by a field controller.

2.3 Authentication Factors

The authentication factors are based on credentials. Credentials are defined as a physical or tangible object, a piece of knowledge or a facet of a person's physical being, that enables an individual access into a physical facility or a PC-based information system.

2.3.1 Type 1

The credentials are known by the user. Eg. Pin, Password. It is the simplest form of all the methods. It involves issuing a password or a pin which may be stored in the human brain or written somewhere known by the user for quick reference. However, it is the least secure and because of this reason, it uses encryption which unfortunately can be easily hacked.

2.3.2 Type 2

The credentials are present with the user. Eg. Magnetic Cards, Smart Cards. It is a bit more complex. The authentication identity is either stored in a magnetic card, smart card, RFID chip among others. This type has proved to be very efficient and is therefore preferred by most people.

2.3.3 Type 3

The credentials are part of the user. Eg. Biometric Technology. It is the most sophisticated of them all. Verification of the user is accomplished using unique human traits or features. This is basically biometrics. Due to its sophisticated nature, it is therefore very expensive thus very prohibiting. As much as biometric identification has a high level of security due to unique entries, the analysis methods used are generally imperfect with generally poorer false rejection and acceptance rates when compared with the other types.

For a secure and effective authentication, multi-factor authentication is used where any two or more of the authentication factors are used to gain access.

2.4 Access Control Criteria

Access control is based on the following:

1. Roles played by the users of the system.
2. Groups which the users of the system are members. The groups are based on parameters set for accessing the objects of the system.
3. Location of the user of the system.
4. Transaction Type of transaction that the user is carrying out.
5. Time at which a transaction is being made.

2.5 Access Control Models

An access control model is a framework which dictates how subjects communicate with objects. There are many access control models and mechanisms, most of which are defined in terms of subjects and objects.

A subject is a computer system entity that can initiate requests to perform an operation or series of operations on objects. The subjects may be users, processes or domains. An object is a system entity on which an operation can be performed.

Within the context of an operating system, an object might represent a file while within the context of a database management system; an object might represent a table or a view. A program residing in memory or stored on disk is considered to be an object; however during its execution it becomes part of a process, and as such is treated as part of the subject.

The reference monitor is an abstract concept, whereby all accesses that subjects make to

objects are authorized based on the information contained in an access control database. It represents the hardware and software portion of an operating system that is responsible for the enforcement of the security policy of the system.

All attempts by a subject to access an object are controlled by the reference monitor in accordance with a security policy embodied in the access control database. Security relevant events are stored in the audit file [4].

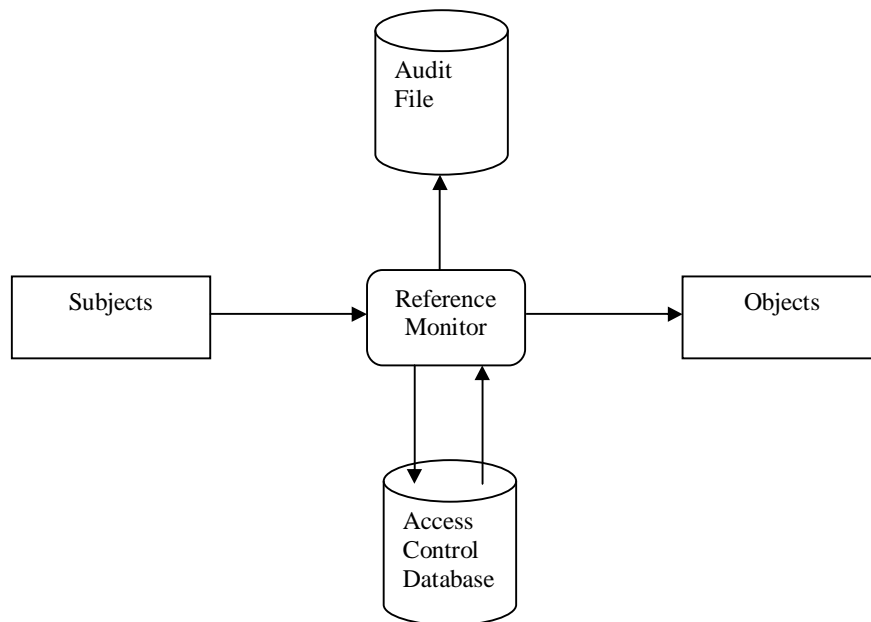


Figure 2.3 Flow of signal in an Access Control System

There are three main types of access control models:

2.5.1 Discretionary Access Control (DAC)

Discretionary access controls are implemented by ACL (Access Control List) and identity-based access control. Identity-based access control makes object access decisions based on a user ID or a user's group membership [5]. Each object has an owner. This means any access to an object is at the discretion of the object owner. It could also be described as a means of restricting access to objects based on the identity of subjects or groups, or both, to which they belong. The owner governs the method of protection by having the ability to grant or revoke access to any of the objects under their control without the intercession of the system administrator.

This model assumes that the end users own the information to which they are allowed

access. For many enterprises within industry and civilian government, this is not the case. The corporation or agency is usually the owner of the system objects. It is therefore not appropriate to allow users to give away access rights to the objects.

Allowing users to control object access permissions has a side-effect of opening the system up to Trojan horse susceptibility. Additionally maintenance of the system and verification of security principles is extremely difficult for DAC systems because users control access rights to owned objects.

2.5.2 Mandatory Access Control (MAC)

It is also known as Rule Based Access Control. Mandatory access control uses security labels to control access. A security label is assigned to each subject and object and the system governs the method of protection. It is a means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization.

The limitation is that the assignment and enforcement of security levels by the system under the MAC model places restrictions on user actions that, while adhering to security policies, prevents dynamic alteration of the underlying policies, and requires large parts of the operating system and associated utilities to be trusted and placed outside of the access control framework. Also, MAC systems are difficult and expensive to implement due to the reliance on trusted components and the necessity for applications to be rewritten to adhere to MAC labels and properties.

2.5.3 Non-discretionary Access Control

It is also known as RBAC. This model, access is governed by the role played by the subject. The principle motivation behind Role based access control is the ability to specify and enforce enterprise-specific access control policies and to streamline the typically burdensome process of authorization management. It is best suited for large organizations with high employee turnover and can be used in conjunction with MAC and DAC systems. [6]

Transaction based rights help ensure system integrity and availability by explicitly controlling not only which resources can be accessed but also how access can occur. In

large organizations, the consolidation of access control for many users into a single role entry allows for much easier management of the overall system and much more effective verification of security policies.

RBAC has integrated support for principle of least-privilege, separation of duties, and central administration of role memberships and access controls. Separation of duties and least-privilege are not a part of MAC while central administration is loosely supported in MAC with trusted components and impossible in DAC due to the violation of the safety principle.

While this model has greatly solved some limitations of DAC and MAC, it also has some limitations. In large systems, memberships, role inheritance, and the need for finer-grained customized privileges make administration cumbersome. It supports data abstraction through transactions, it cannot be used to ensure permissions on sequences of operations need to be controlled.[2] To do this, a less general and more sophisticated access control model must be used.

2.6 Access Control Technologies

2.6.1 Passwords

A password is a string of characters that are uniquely developed and used for authentication of different users of a system. It is the most common authentication and identification method across the world in the present day. This is because it is simple and easy to implement.

There are various types of passwords:

- a) Cognitive passwords
- b) Dynamic passwords/ One time passwords

Cognitive passwords are facts or opinion-based information used to verify an individual identity. This method employs a set of questions whose answers only the legitimate user is able to correctly answer.

One time passwords have an expiry and are generated based on time or a counter. They are used in token based systems that require a higher level of security than static password provides.

The major disadvantage of password protection scheme is that in comparison to the other methods, it is the most insecure. Because of its high level of insecurity, methods

have been developed to reduce this risk. Some of them are as follows:

- Use of long and complex passwords
- Password expiry
- Limited log-on attempts
- Record of password history
- Encryption

These methods altogether help in reducing the risk posed by using passwords and because of this, fraudsters have launched attacks on these methods. The interesting thing is that system administrators use these same attacks to improve the security of their systems by implementing them and enhancing their passwords.

Because of these challenges, systems able to detect these kind of attacks have been developed. They are known as intrusion detection systems. The most successful password system developed to counter hacking is the cognitive password system where passwords are based on fact or opinion which are related or unique to that specific user or individual who is trying to gain access.



Figure 2.4 Keypad

2.6.2 Wiegand Card Readers

The Wiegand effect was discovered by John R. Wiegand in the 1980s. Many access control system manufacturers adopted Wiegand technology, but were unhappy with the limitations of only 8 bits for site codes (0-255) and 16 bits for card numbers (0-65535). Wiegand cards use a simple LC circuit. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil which transmits it to the reader.

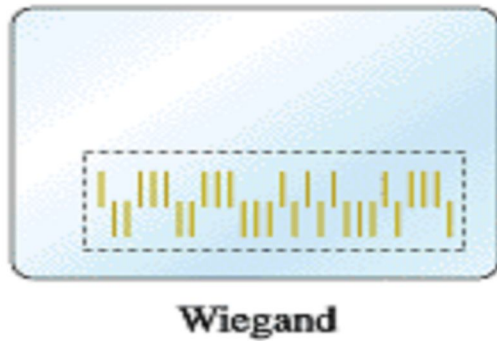


Figure 2.5 Wiegand Card

2.6.3 Biometrics

Biometrics employs characters or traits of an individual for verification. The common traits that are used in identification lead to various types of biometric authentication:

- **Hand geometry**

For hand geometry, the shape of hand and the width of fingers are analyzed and stored in the database.

- **Fingerprints**

Fingerprint scanning is divided into two sections. One is where analysis and verification is done using the ridge endings and bifurcations on a finger.



Figure 2.6 Fingerprint

Another is where selective points on the fingerprint are stored. The advantage is that it conserves space in the database as less data is stored.

- **Facial recognition**

Facial recognition takes note of bone structure, length of forehead, nose ridges, eye widths among other minute facial details.

- **Iris detection**

The iris is the colored portion of the eye. For Iris detection, the unique patterns and rings in the iris are captured as a photo and stored using a special iris detector.

- **Retinal scan**

In Retinal scanning, the patterns of the blood vessels on the backside of the eyeball have been found to be just as unique as the other methods and therefore suitable for access control.

- **Palm Scan**

Palm Scans are based on the creases, ridges, and grooves that are unique in each individual's palm.

- **Voice geometry**

Voice geometry method recognizes small differences in the speech patterns of an individual and uses the very pattern for detecting the individual.

- **Hand topography/topology**

Hand topography is also considered in some cases where the side view is analyzed in terms of height and length.

- **Signature dynamics**

Signature dynamics is based on electrical signals generated due to physical motion of the hand during signing a document.

- **Keyboard dynamics**

Keyboard Dynamics is based on electrical signals generated when each user of a system types on the keyboard.

Biometric analysis collects data which is virtually impossible to imitate. This means that they provide a high level of protection. It is the most expensive type of authentication method to implement. No two fingerprints have ever been found to be alike. They are perceived by society to be intrusive because the method unlocks personal information. This restricts the use of this method to environments or setups where a high level of security is required. The one major event that caused an influx in implementation across the world is the famous September 11, 2001 bombing.

The accuracy of different biometric systems can be gauged as:

- i. Type I error
- ii. Type II error

Type I error results when an individual is denied access to a system which he/she is entitled to. It is given a measure known as False Reject Rate (FRR). Type II error occurs when an imposter is granted access upon verification. This error is measured using what is known as false accept rate (FAR).

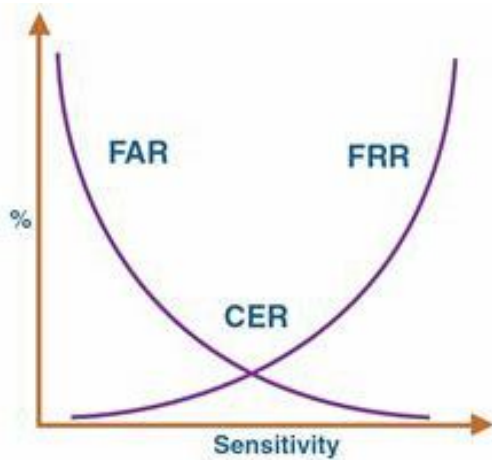


Figure 2.7 Error Rate Diagram

A balance between the two errors has been developed and analyzed resulting in crossover error rate. It is the point at which the false rejection rate equals the false acceptance rate. It is also known as Equal Error Rate (EER). This is a metric used to govern the overall protection of a system.

2.6.4 Magnetic Cards

Magnetic recording began during World War II and it was done on steel tapes for storage of audio. In the 1960s, IBM then used this idea to develop a way of securing magnetic stripes onto plastic cards. A magnetic card is a device which holds data in a magnetic stripe. The stripe is made up of tiny iron-based magnetic particles in a plastic-like film. The writing operation is carried out by aligning the dipoles of the tiny magnets in either the north or south direction.

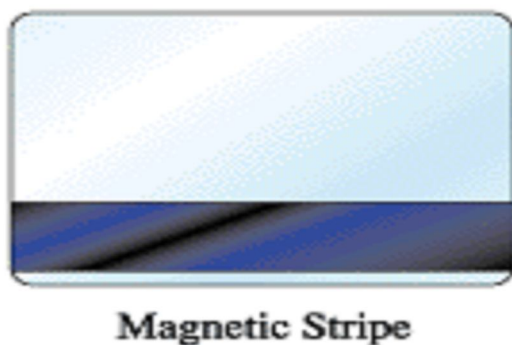


Figure 2.8 Magnetic Card

There are three tracks on the magnetic stripe on to which data is written. Usually in credit cards, only two tracks are used. The third is a read/write track that has the encrypted code, amount authorized, and country code among others. The information contained in the card is then extracted using a magnetic reader. Memory cards usually require two-factor authentication where the user is required to enter the PIN stored in

the card after swiping the card or placing it in the reader. Data in a stripe can easily be read and written.

2.6.5 Smart Cards

A smart card is pocket size card with an embedded microprocessor. This technology employs cards which have the capability of storage of data and can process the data. The microprocessor is like a replacement of the magnetic stripe in memory cards which is in form of an integrated circuit. The integrated microprocessor is an intermediary of communication between the reader and the host computer. A smart card is not self supporting and receives operation power from an external source.



Figure 2.9 Smart Card

There are two categories of smart cards:

- Contact card
- Contactless card
- Hybrid card
- Dual interface card

A contact smart card must be inserted into a smart card reader for any information to be transferred. There must be direct contact with a conductive plate.

A contactless card only requires close proximity to the reader. The reader and the card have antennas and they communicate using radio frequency signals and its application restricted to ISM bands which is a necessary measure to avoid interference with other important radio systems. The unique serial number in the RFID chip is read by an RFID card reader and the data is transmitted to the host computer for identification and authentication purposes. This is popularly known as RFID technology. The same circuit used in the contactless card may also be incorporated in a key tag.



Figure 2.10 Key Tag

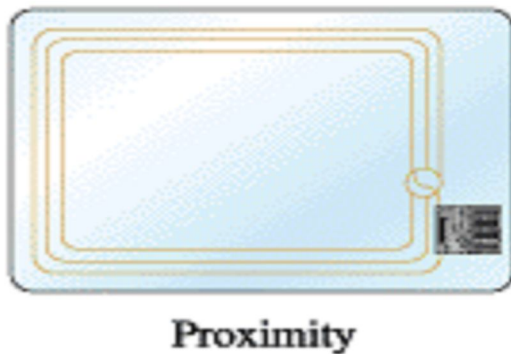


Figure 2.11 RFID Card

This technology was first used in World War II, which began in 1939, to differentiate friendly and enemy machinery such as aircrafts and tanks. Later on in the 1970s, it emerged that this technology was being used to identify railroad cars. It then significantly expanded in the 20th century in use in highway toll systems, consumer products tracking and vehicle immobilization among many others.

The hybrid type has two separate chips that can support both contact and contactless communication. The dual interface type has a single chip with both contact and contactless interfaces. It has a microprocessor that can communicate with both a contact reader and a contact terminal. This means that the chip is accessible with either a contact or contactless interface.

The chips used in the various cards above are of two categories:

- a) Microcontroller chips
- b) Memory chips

A microcontroller chip can modify data in its memory by adding, deleting or editing the data. Cards with embedded microcontroller chips are therefore comparatively more expensive. They have the ability to store large amounts of data and have their own functions. Cards that use memory chips depend on the security of the card reader. They

are less expensive because of the reduction in ability of security management.

2.7 Access Control Administration

2.7.1 Centralized Access Control

This method of administration only one entity is responsible for overseeing access to all corporate resources within a controlled system. This enables a consistent and uniform method of controlling users access rights.

2.7.2 Decentralized Access Control

Decentralized access control administration gives control of access based on proximity. Due to access control at different locations, conflicts may arise due to different access control methodologies employed by the various authorities at different locations. Due to this, the method may lack the consistency that would have otherwise been provided by the centralized control.

2.8 Access Control Types

- Preventive – Works toward goal of avoiding unwanted occurrences.
- Corrective - Rectifies errors that have already occurred.
- Detective - Determines unwanted occurrences before they happen.
- Compensative – This provides alternatives to other controls
- Deterrent - This type discourages the users of the system from violating rules.
- Recovery – Restores capabilities which have been lost.

2.9 Access Control Threats

2.9.1 Spoofing/Masquerading

This is the situation where an intruder falsifies the real user of a system and thereby gains unwarranted access.

2.9.2 Dictionary Attacks

Dictionary attack method has predefined words commonly used as passwords. Special software is used to cross-reference the password and the words in the software program until a match is obtained.

To counter this, dictionary tools are used to detect weak passwords and make them stronger.

2.9.3 Brute Force attacks

Brute force method just as the name suggests is an untiring process of going through all possible sequence of characters until the exact combination is arrived at.

To curb these kind of attacks passwords are rotated frequently or one time passwords are effected.

2.9.4 Software Malice

This method is implemented by using software that is capable of extracting important information from other programs such as passwords and using the same to gain access where it is otherwise not supposed to be granted.

2.9.5 Emanations

This involves tapping of signals or waves sent from electronic devices over the air interface such as signals using special dedicated devices and acquiring the vital data or information that is contained in those signals.

2.9.6 Denial of Service Attack (DoS)

This attack is aimed at disabling an access control system by making the relevant resources of the system unavailable to the users. This obstruction of resources can be implemented in various ways:

- Interference with the physical devices of the network.
- Bugging up of the communication channel between the user and the system so as to disrupt communication.
- Distortion of configuration settings of the network.
- Slowing down of processing speed by eating up of disk space and bandwidth.

Chapter 3 DESIGN METHODOLOGY

3.1 Building Design

3.1.1 Access Control Plans

The complex building has 6 floors. In this project, 4 floors are considered for design.

The building is divided into two main sections:

- Office Section
- Apartment section

All of the floors have a form of access control present. The exterior of the building has two access controlled zones at the points of entry and exit.

Ground Floor

<u>ACCESS CONTROLLED UTILITIES</u>	<u>NO.</u>
Apartments	5
Restaurant	1
Bank Space	1
Shop	1
Staircase	1
Main Entrance	1
Main Exit	1
TOTAL	12

Table 3.1 Ground Floor Doors

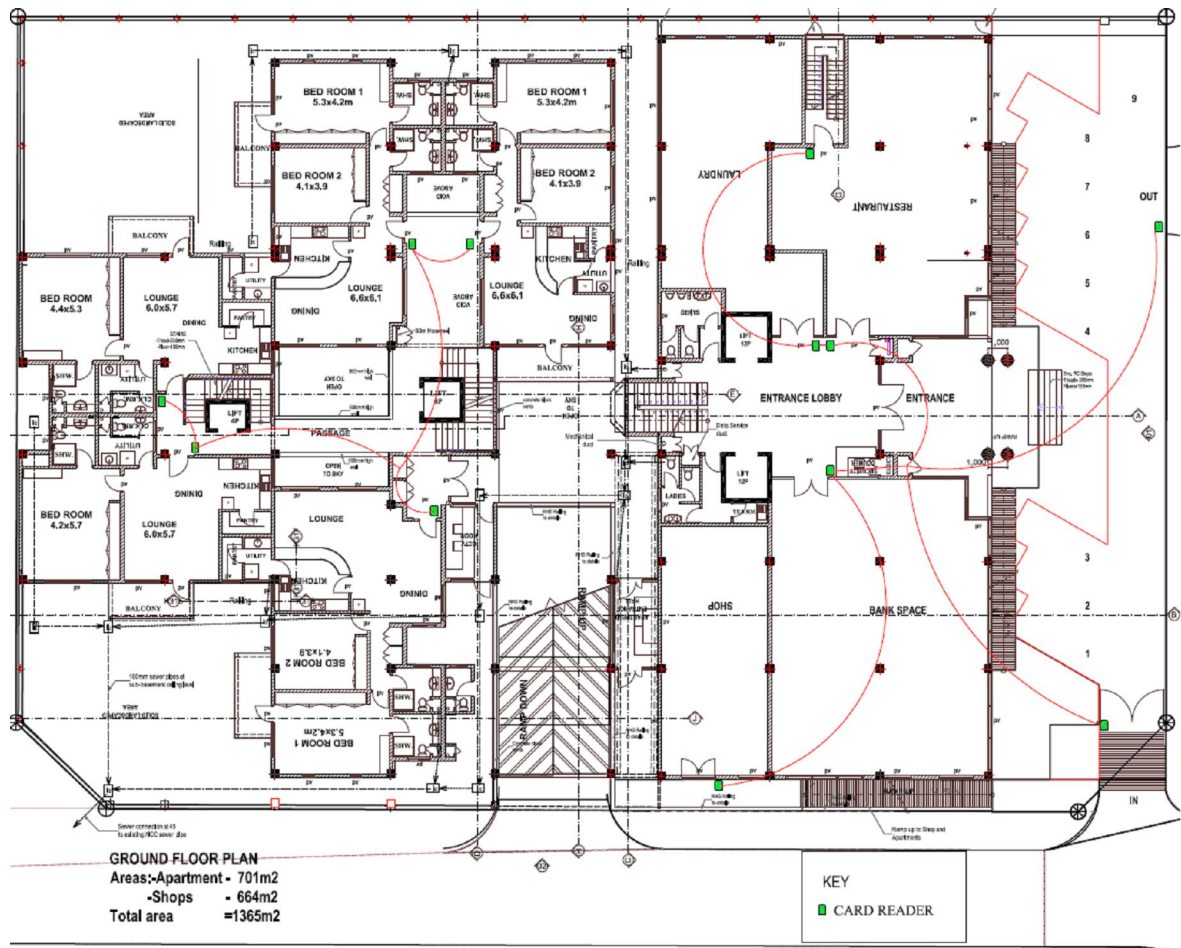
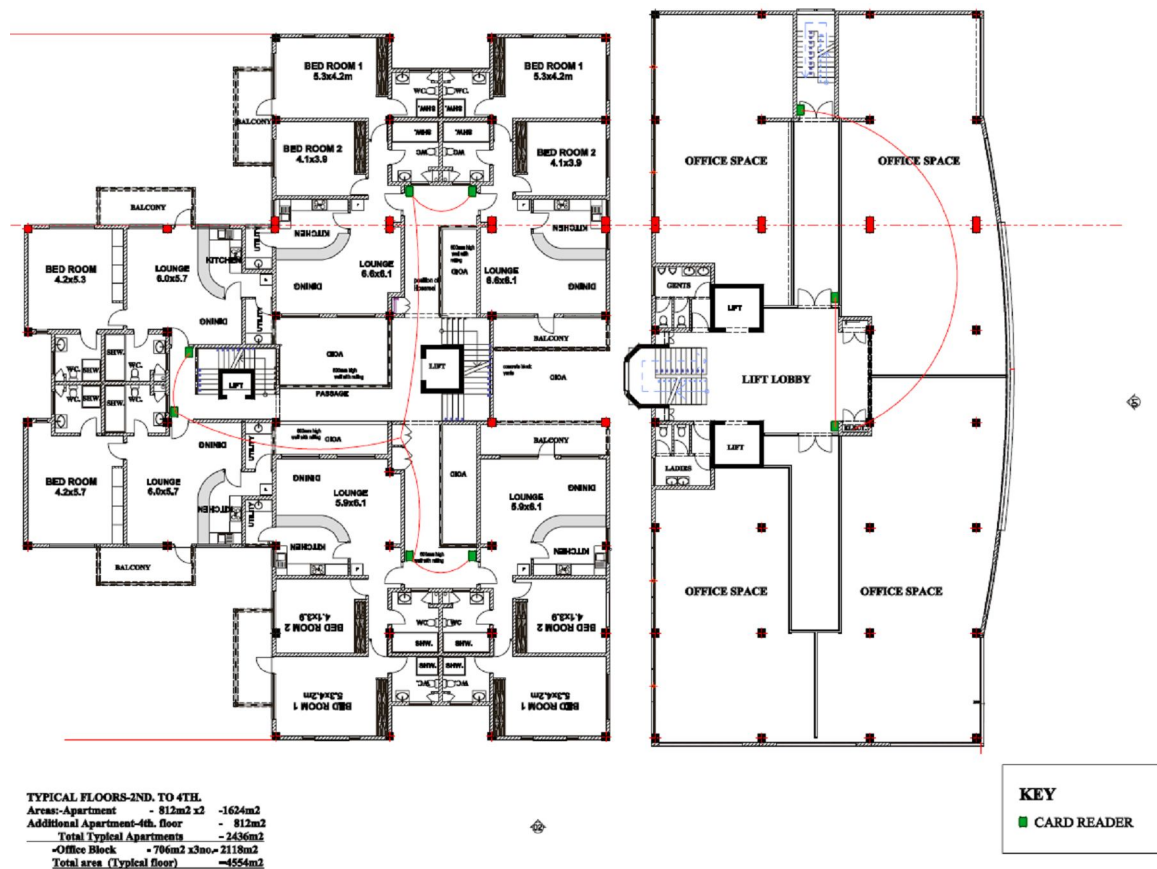


Figure 3.1 Ground Floor Plan

Typical Floors(2ND to 4TH floor)

<u>ACCESS CONROLLED UTILITIES</u>	<u>NO.</u>
Apartments	6
Office Section	2
Staircase	1
TOTAL	9(3 floors) = 27

Table 3.2 Typical Floor Doors*Figure 3.2 Typical Floors Plan*

3.1.2 Bill of Quantities

The BoQ for the complex building:

BILL OF QUANTITIES					
ACCESS CONTROL NETWORK					
No.	Description	Unit	QTY	Rate	Amount (Kshs.)
1	Card Readers	No.	37	1,500.00	55,500.00
2	Electromagnetic locks(Single leaf)	No.	37	12,500.00	462,500.00
3	Intelligent Access Controller(IAC)	No.	7	106,000.00	742,000.00
4	RFID Cards/Badges	No.	145	450.00	65,250.00
5	Request-to-Exit(RTE) push buttons	No.	36	2,000.00	72,000.00
6	Break Glasses	No.	15	3,000.00	45,000.00
7	Door Contacts	No.	37	1,500.00	55,500.00
8	IAC Power supplies, Backup battery & Castings	Piece	37	11,000.00	407,000.00
9	Access Control Software and Server	Item	1	40,000.00	40,000.00
	Sub-total				1944,750.00
	Labour	%	30%		583,425.00
	Sub-total				2528,175.00
	Contingency	%	10%		252,817.50
	Sub-total				2780,992.50
	VAT (16%)	%	16%		444,958.80
	Grand Total				3225,951.30
	Total (SAY)				3400,000.00

3.1.3 Control Model

The access control model is the framework that dictates how subjects access objects. It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.

The model employed in this building is Role Based Access control. Role Based Access Control on the other hand is based on the role that the user plays/or is assigned in the building.[7] Security policies are maintained in RBAC through the granting of rights to roles rather than individuals. Access is based on predefined rules such as payment of rent and validity of user after crosschecking from the database. This applies to both the apartment and office section as long as the owner of the subject, which in this case is the controlled doors, is not the tenant. Clearance codes are used to control access within the building. These are predefined sets of access privileges. Once created, can be assigned to any number of access cards.

There are 6 Group Privilege Levels for this system:

<u>USER GROUP</u>	<u>CLEARANCE CODE</u>
Administrators	Super-user
Tenants	Apartment
Visitors	Visitor
Employees	Office
General Staff	Low
Miscellaneous	Custom

Table 3.3 Privilege Levels

The access privilege levels are based on the following parameters:

- Day of the week
- Time of the day
- Location within the building

The principle of least privilege has been described as important for meeting integrity objectives. [8]The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Principle of least privilege is employed as all the users of this building are given no more privilege than they require.

3.2 Access Control

3.2.1 Design Model

The Access Control System (ACS) has four blocks:

- a) Head-end system
- b) Control panel
- c) Access Devices
- d) User interface

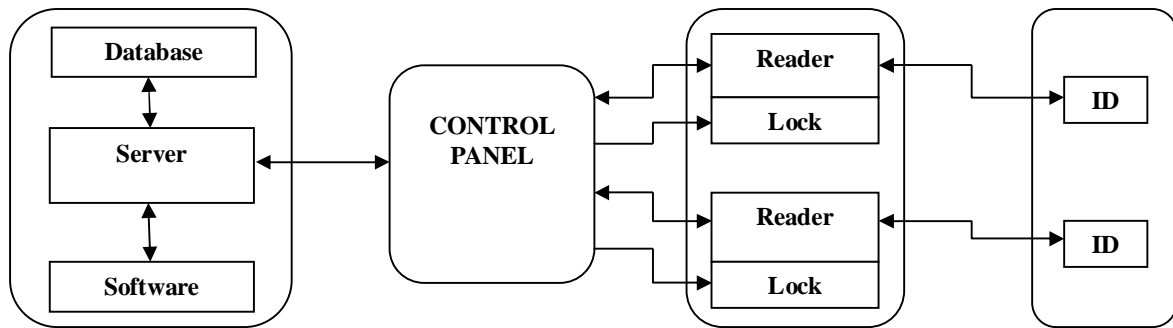


Figure 3.3 Access Control System Diagram

It is designed to integrate multiple building functions including alarm management and intrusion detection. The head-end system consists of a database, server and software. It receives, processes and sends data in the access control network. The control panel is the interface between the head-end system and the user involved in the control of the access devices. It basically houses a microcontroller or a series of microcontrollers. Access controlled devices are the devices which receive signal from the control panel and respond to the commands. They include locks and readers.

3.2.2 Access Technique

The contactless approach of Radio Frequency Identification has proved to be the most convenient for the building because it is easy to use, flexible and well suited for automatic operation. It is a system of technologies used by an object to identify another object. The fact that it does not require line-of-sight makes it a more superior system than all the other access techniques. It also provides a high level of data integrity and security because it is difficult to forge the unique serial numbers embedded in a tag.

The RFID Technology combines advantages not available with other identification technologies as it gives an optimum balance between types 1 and 3 techniques. Type 1 techniques are the easiest to implement and are at the same time the least secure. They give a chance to the users to search for loopholes which degrades the security of the system. Also, accessing various locations of the building will take a significantly longer time. Type 3 techniques are very expensive and they are generally considered by the users to be invading their privacy.

Every apartment is to have a proximity reader installed at the entrance. The tenants will each be issued with an RFID tag which will be used to access the main door of the

apartment through the readers installed at each apartment.

For the office section, readers will be installed at every access controlled door. Employees will be issued with user specific tags and access privileges granted according to the role of the user. Each employee can have a maximum of only one tag. All the readers within the building are connected to the host computer through access controllers to facilitate the back and forth access of the server.

3.2.3 Access Control Devices

3.2.1.1 Access Controller: PC-Based

This is the device which handles signal exchange between the host computer and the system components such as the door locking system and the readers. It is used to process access control activities for all doors connected to it and is situated in a secured area to prevent tampering, preferably in a locked cabinet with space for a power supply and backup battery to ensure an uninterruptible supply of power. Controllers are usually mounted in telephone, electrical, or communications closets.

7 Intelligent access controllers are used for this building, each with a capability of handling 6 doors.

Maximum capability = $7 \times 6 = 42$ Access Controlled Doors.

3.2.1.2 Tags

High frequency Passive RFID Tags of 13.56MHz are used. The maximum read distance for this frequency is 1.5m.

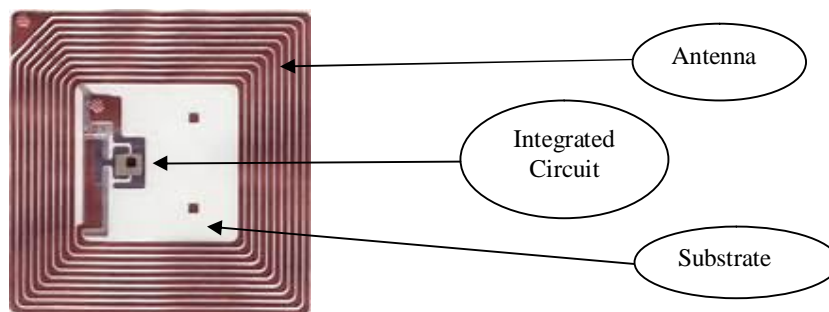


Figure 3.4 RFID TAG Schematic

The tags to be used are read only devices meaning information that is in the memory

can't be changed by RF command once it has been written. Each tag has a unique 10 digit serial number embedded within them.

Contactless smart card readers are offered for technologies including, but not limited to: iCLASS, MIFARE and LEGIC.

FREQUENCY RANGE	DESCRIPTION	TRANSMISSION POWER
13.553 ~ 13.567 MHz	<p>High Frequency 13.56 MHz. ISM</p> <p>Inductive coupling.</p> <p>Proximity smartcard (ISO 14443, MIFARE®, Legic, etc)</p> <p>Vicinity smartcard (ISO 15693, Tag-It, I-Code)</p> <p>Item management (ISO 18000-3)</p>	60 dBμA/m

Table 3.4 Frequency Range Specification

Implementing an RFID system requires that all the hardware used meet the local regulations.

USERS	NO. OF TAGS
Administrators	5
Tenants	30
General Staff	20
Employees	60
Visitors	30
ESTIMATED TOTAL	145

Table 3.5 Tag Quantity

Temporary cards are issued to visitors at the main entrance reception and the tags are configured according to their requirements:

- a) Location to be accessed
- b) Time Period

The tag will automatically be deactivated after a certain period of time configured by the security officer or administrator of the building. This prevents the visitors from becoming intruders.

3.2.1.3 Card Readers

The 13.56 MHz close range tags are used for every controlled door and that requires a reader of the same frequency.

Semi-intelligent Card Readers are used.

LOCATION	NO. OF READERS
Office section	27
Apartments	10
TOTAL	37

Table 3.6 Card Readers Breakdown

3.2.1.4 Magnetic Locks

Single-leaf electromagnetic locks are used. The electromagnet locks uses the magnetic force generated from the electromagnet to secure the doors. They allow swing of doors in only a single direction.

The lock has a built-in safety feature which disables the lock during emergencies.

The number of locks required is same as that of readers.

NO. OF ELECTROMAGNETIC LOCKS = 37

3.2.1.5 Door Contacts

The door contacts are used for two types of monitoring:

- DFO monitoring

- OTL monitoring

NO. OF DOOR CONTACTS = 37

3.2.1.6 Request-to-exit device

There are two types of REX devices that may be employed in this building. The primary device is an exit motion sensor that uses infrared technology to initiate door release. The secondary device is hand operated and is activated by pressing a switch. Activating the device releases a magnetic door lock and sends a request-to-exit signal through a relay output. The magnetic lock is released by breaking 12V DC power.

LOCATION	NO.OF BUTTONS
Office Section	9(3floors) =18
Ground Floor	4
Apartment Section	23
TOTAL	36

Table 3.7 Request-to-exit devices Breakdown

NO. OF REQUEST-TO-EXIT PUSH BUTTONS = 36

3.2.1.7 Break Glasses

Ground Floor = 5

Office Section = 9(3 for 3 floors)

NO. OF BREAK GLASSES = 14

3.2.1.8 Access Control Barriers/Bollards

For the main entrance to a building, heavy duty Impact Rated Electro-hydraulic Rising bollards are used in combination with a Boom barrier. When not activated, the bollards lie flush with the road surface.



Height: 800mm

Diameter: 273mm

Rise Speed: 6 seconds

Operations: 3000/day

Figure 3.5 Bollard

Electrical Requirements: 240 V, 1-phase, Neutral supply rated 13A at each location.

One control panel operates 4 bollards. We require 6 bollards; 3 for entry and 3 for exit. This means that 2 control panels will be in use. The control panels are local to the bollards with a maximum allowable length of 10m.

The low voltage control cable from the control panel to the gate house can be as long as required.

3.2.1.9 Safety Loops

Vehicle induction loops are used to prevent the bollards or the boom barrier from rising or lowering on vehicles.

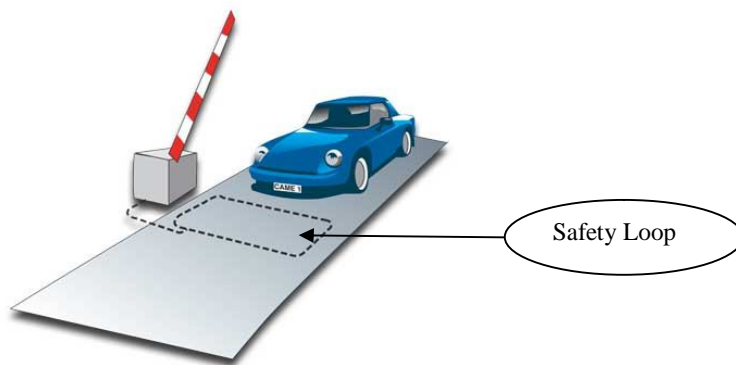


Figure 3.6 Induction Safety Loop

Two induction loops are required for the entrance and exit. Single channel loop detectors are used to identify the presence of vehicles by means of an inductive loop buried under the road. The loops are cut into road surface after surface has been laid.

3.3 Database System

The Database system makes up a large part of the head-end system. It is the entirely non-physical part of the system comprising of:

- Database – MySQL Database
- Server – Apache Server
- Software – PHP and HTML

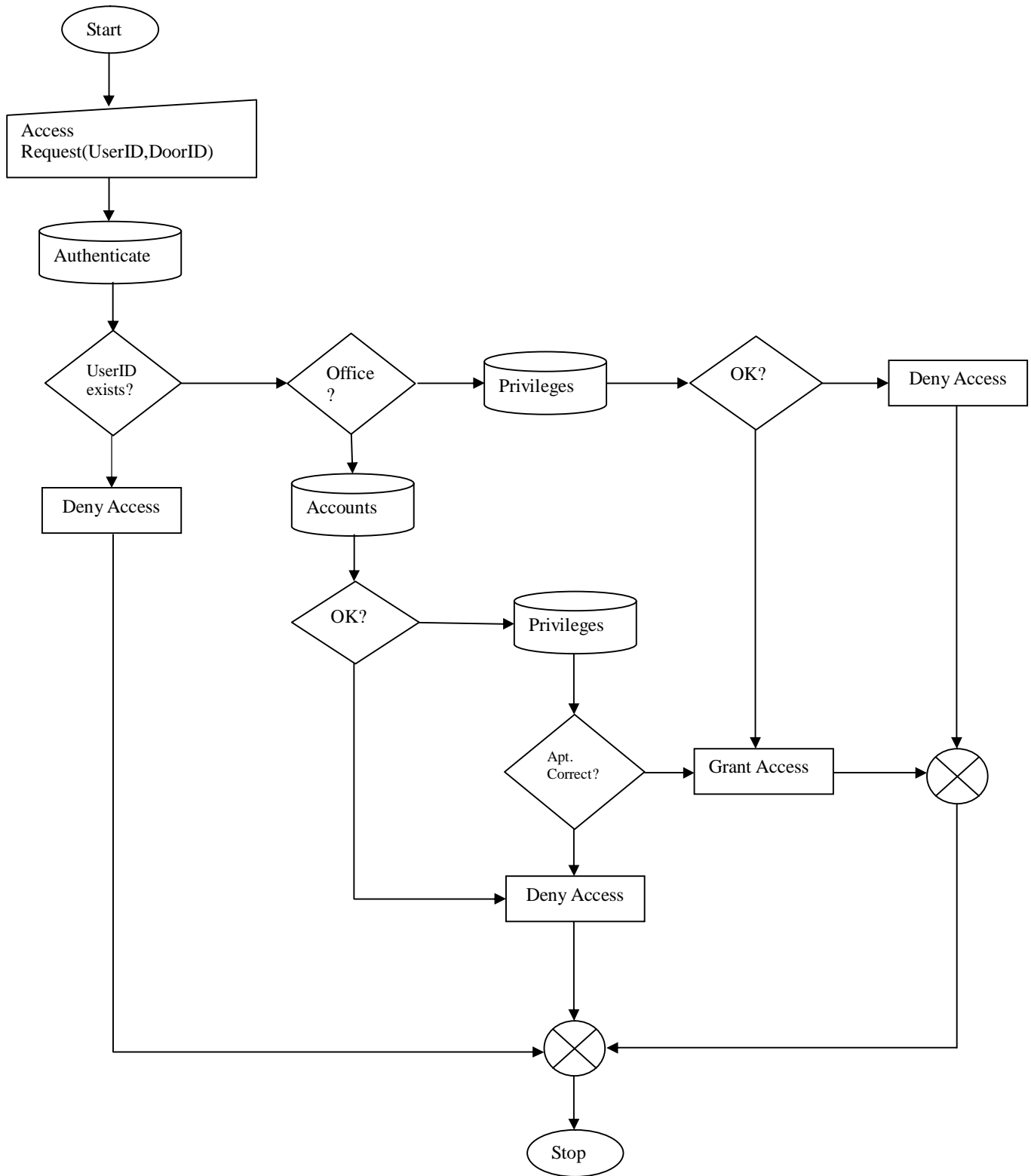


Figure 3.7 System Software Interconnection

The server computer is the central database of the system. It manages all the activities of the whole system. Distributes info to the control panels and receives info from the panels. A single server is capable of controlling many doors such as in a building. The system is designed to store all records in a MySQL database.

The access control software is written and developed using PHP and HTML. The user interface of the software is designed using HTML and the necessary validations implemented using PHP. Data is obtained from the user through HTML interface and the data is forwarded to PHP which handles the data and then it finally ends up in the database.

3.3.1 Access Control Flowchart



3.3.2 Pseudo code

Get the TagID of the user trying to Access the system and the DoorID of the place trying to be accessed

Connect to database

Check if TagID exists

If the TagID does not exist

 Deny Access

 Log details

Else

 Get the section the user is trying to access using DoorId

 If the user is trying to Access an Apartment

 Get clearance of the user from database

 If clearance is apartment

 Check if apartment he is trying to access

belongs to him/her

 If the apartment belongs to him/her

 Check if Account is ok using

TagID

 If Account is ok

 Grant Access

 Log details

 Else

 Deny Access

 Log details

 End If

 Else

 Deny Access

 Log details

 End If

 Else

 Deny Access

 Log details

 End If

```

Else if the user is trying to Access an Office
    Get clearance of the user from database
    Get the number of the door that is to be accessed using
the DoorID

    Get the floor which the door is from the DoorID

    Check if the time and date of Access is Valid for that
clearance

        If time and date is valid for that clearance
            Check if floor is valid for that
clearance

                If the floor is valid
                    Check if the doorno
is valid

                        If the doorno
is valid

                            Grant Access

                                Log
details

                                    Else

                                        Deny Access

                                            Log
details

                                                End if

                                                    Else

                                                        Deny Access

                                                            Log details

                                                                End If

                                                                    Else

                                                                        Deny Access

                                                                            Log details

                                                                                End If

```

End If

End If

3.3.3. Tables

The database has four tables:

i. Users

The users table stores the records of all the users of the system. It includes their names, the tags they hold, their privilege levels, apartment numbers if any, the date that they got onto the system list and their account status. The fields in the table are:

FIELD	DATATYPE
UserID	INT(AutoNumber)
TagID	VARCHAR
Name	VARCHAR
Clearance	VARCHAR
CreateDate	DATE
AccountStatus	BOOLEAN
ApaNo	INT

Table 3.8 Users Table

ii. Journal

The journal table keeps a record of all access attempts within the building regardless of whether access is granted or denied. The fields are:

FIELD	DATATYPE
JournalID	INT(AutoNumber)
TagID	VARCHAR
DoorID	VARCHAR
AccessTime	TIME
AccessDate	DATE
AccessResult	VARCHAR

Table 3.9 Journal Table

iii. Clearance

The clearance table stores the list of privilege levels that are available to users of the system. The fields are:

FIELD	DATATYPE
ClearID	INT(AutoNumber)
ClearName	VARCHAR
StartDate	DATE
EndDate	DATE
StartTime	TIME
EndTime	TIME

Table 3.10 Clearance Table

iv. Administrators

This table stores a list of the administrators of the system.

FIELD	DATATYPE
ID	INT(AutoNumber)
UserName	VARCHAR
Password	VARCHAR

The physical system which comprises of tags and readers is emulated in this project by a system which prompts the user to give the TagID and DoorID. In the real system, the TagID would be passed to the system from the tag to the database through the access card reader and microcontroller. The DoorID would automatically be passed to the database by the specific card reader which has been requested of access by the user.

The program developed is to capture the DoorID and TagID, crosscheck with the records in the database whether the particular tag requesting access exists. If yes, the privileges of the specific user is compared to the DoorID which gives details of the:

- a) Section of the building
- b) Floor to be accessed
- c) Door number

The DoorID has 8digits which is divided into three parts to represent:

- i. Section
- ii. Floor
- iii. Door Number

DOORID	SECTION	FLOOR	DOOR NUMBER
OFF04309	OFF	04	309
APA03200	APA	03	200

Table 3.11 DoorID Breakdown

OFF - Office 04 – Floor 309 – Door Number

APA - Apartment 03 – Floor 200 – Door Number

If the user's credentials are varied, access is granted. Otherwise, access is denied. All the access attempts are stored in the system journal at the host computer's database which is a collection of access requests to the system.

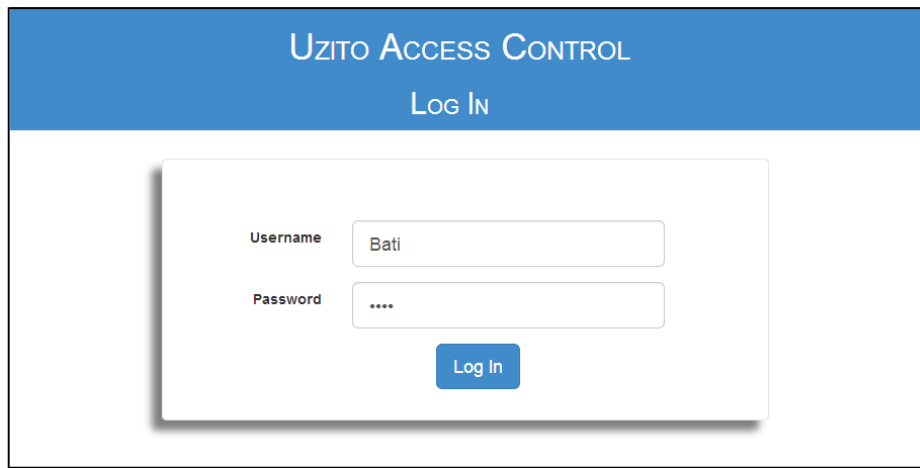
Chapter 4 RESULTS AND ANALYSIS

4.1 Results

4.1.1 Access Request Cycle

Log In Form

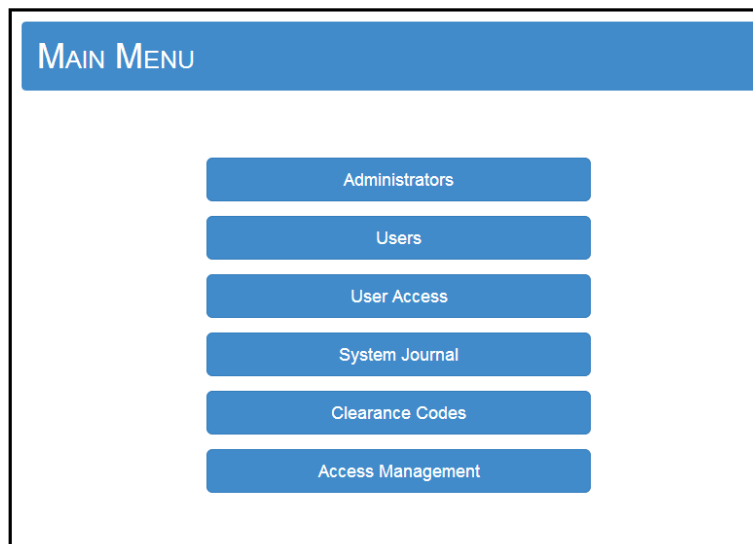
This form ensures security of the intangible information of the system. Only authorized administrator or system operator is allowed to Log in.



The image shows a web interface for 'UZITO ACCESS CONTROL'. At the top, there is a blue header bar with the text 'UZITO ACCESS CONTROL' and 'LOG IN' below it. The main content area is white and contains a login form. The form has two input fields: 'Username' with the value 'Bati' and 'Password' with four asterisks '****'. Below these fields is a blue button labeled 'Log In'.

Main Form

This is the interface through which all the forms of the access control program are accessed.



The image shows a web interface for the 'MAIN MENU'. At the top, there is a blue header bar with the text 'MAIN MENU'. The main content area is white and contains a vertical list of six blue buttons: 'Administrators', 'Users', 'User Access', 'System Journal', 'Clearance Codes', and 'Access Management'.

User Access Form

This form is simulating the action that the passive tag would do in the real-world system. It passes the details of the user access request to the system.

The form contains two input fields and a submit button. The first field is labeled 'Tag ID' and contains the value '4001002301'. The second field is labeled 'Door ID' and contains the value 'OFF02202'. Below these fields is a blue button labeled 'Submit'.

TagID: **4001002301**

DoorNo: **202**

Building Section: **Office**

Floor: **2**

Users List

The system checks whether the user's record is in the database.

The screenshot shows a database query result for the 'uzito.users' table. The table has 7 columns: UserID, TagID, Name, Clearance, CreateDate, AccountStatus, and ApaNo. The results are displayed in a table with alternating row colors. The second row, corresponding to the user 'Betty Kel', is highlighted in blue.

UserID	TagID	Name	Clearance	CreateDate	AccountStatus	ApaNo
1	4001002300	Albert Opiyo	SuperUser	2012-04-22	on	(NULL)
2	4001002301	Betty Kel	Office2	2014-01-10	on	(NULL)
3	4001002302	Duncan Maina	Apartment	2012-04-03	off	600
4	4001002303	Pete Owen	Limited	2012-07-06	on	(NULL)
5	4001002304	Scholastica Weng'	Low	2013-04-30	off	(NULL)
6	4001002305	Kevin Ndeti	Custom	2013-04-27	on	(NULL)

User: **Betty Kel**

Clearance: **Office2**

Clearance of user

This form shows a list of all the privilege levels that are available. The privileges of the particular user above are highlighted.

Clearances					
ClearName	StartTime	EndTime	StartDate	EndDate	DoorVal
SuperUser	00:00:00	23:59:00	2009-04-28	2030-12-31	
Low	11:00:00	16:00:00	2014-04-03	2014-10-03	
Limited	13:00:00	14:00:00	2014-04-24	2015-06-24	303
Apartment	00:00:00	23:59:00	2014-04-27	2020-05-27	
Office1	08:00:00	18:00:00	2013-01-03	2015-04-20	101
Visitor	08:00:00	09:30:00	2014-04-04	2014-04-15	220
Office4	08:00:00	18:00:00	2013-04-12	2017-04-20	401
Office2	08:00:00	18:00:00	2013-05-07	2016-04-27	202
Office3	08:00:00	18:00:00	2013-11-03	2016-04-18	303
Custom	08:20:00	09:30:00	2014-07-07	2014-07-22	500

StartTime: **08:00:00**

EndTime: **18:00:00**

StartDate: **2013-05-07**

EndDate: **2016-04-27**

DoorVal: **202**

Verdict

The final decision of whether to deny or grant access is made after comparing the privileges allowed with the given parameters.

Tag ID

Door ID

Access Granted!

Access Status: Granted

Journal Form

The record of this activity is updated into the database and can be viewed from the journal form.

System Journal					
Tag Id	Door Id	Floor	Access Time	Access Date	Access Status
4001002300	OFF02220	2	11:03:14	2014-04-13	Granted
4001002306	APA02458	2	00:09:38	2012-04-27	Granted
4002003507	OFF02741	2	22:48:40	2013-07-06	Granted
4004006578	OFF03401	3	23:09:42	2014-03-04	Granted
4001002305	OFF03500	3	08:45:43	2014-06-24	Granted
4001002306	OFF02101	2	08:09:45	2012-08-15	Denied
4004006578	OFF01202	1	06:36:47	2013-11-24	Granted
4001002309	OFF04303	4	09:09:48	2014-05-15	Granted
4002003404	APA04458	4	12:07:28	2014-03-18	Denied
4009009002	APA02600	2	07:11:12	2014-10-01	Granted
4001002307	OFF01202	1	18:27:04	2014-04-28	Denied

4.1.2 Updating Database

New User

A new user is entered into the system by filling the necessary data in the New User Form.

NEW USER

Tag ID

Name

Apartment No.

Clearance

Create Date

Add User

User updated in database:

21	4001002001	Fred Jakochia	Visitor	2014-04-27	on	(NULL)
22	4001002000	Rita	Visitor	2014-06-20	on	(NULL)
23	4001002002	Jackson Shebesh	Visitor	2014-02-06	on	(NULL)
24	4001002003	Stephen Boi	Visitor	2014-03-07	on	(NULL)
25	4001003035	Michael Kimemia	Apartment	2014-04-10	on	453

New Clearance

A new clearance code is entered in the New Clearance Form.

NEW CLEARANCE

Clear Name

Start Time

End Time

Start Date

End Date

Door Value

Updated Clearance Code:

10	Visitor	08:00:00	09:30:00	2014-04-04	2014-04-15	220
12	Office4	08:00:00	18:00:00	2013-04-12	2017-04-20	401
13	Office2	08:00:00	18:00:00	2013-05-07	2016-04-27	202
14	Office3	08:00:00	18:00:00	2013-11-03	2016-04-18	303
16	Custom	08:20:00	09:30:00	2014-07-07	2014-07-22	500
17	Office5	08:30:00	10:30:00	2014-06-16	2014-11-05	450

New Administrator

NEW ADMINISTRATOR

Username

Password

Updated Administrator table:

SQL 8.1.0.4545

Host: localhost Database: uzito Table: administrators

uzito.administrators: 3 rows total (approximately)

ID	Username	Password
1	Bati	da974f5eba1948690c83e9c3b43ffd87
2	Edu	f3ac63c91272f19ce97c7397825cc15f
3	Seska	2c4189a6213986088de094a5623ec98b

4.1.3 Data Analysis

Data Analysis is done from the system journal.

Granted Entry records

Returns records of all access requests that have been granted permission.

Granted Entries						
JournalID	TagID	Floor	DoorID	AccessTime	AccessStatus	AccessDate
25	4001002300	2	OFF02220	11:03:14	Granted	2014-04-13
26	4001002306	2	APA02458	00:09:38	Granted	2012-04-27
27	4002003507	2	OFF02741	22:48:40	Granted	2013-07-06
28	4004006578	3	OFF03401	23:09:42	Granted	2014-03-04
29	4001002305	3	OFF03500	08:45:43	Granted	2014-06-24
31	4004006578	1	OFF01202	06:36:47	Granted	2013-11-24
32	4001002309	4	OFF04303	09:09:48	Granted	2014-05-15
34	4009009002	2	APA02600	07:11:12	Granted	2014-10-01
38	4001002303	4	OFF04678	13:15:44	Granted	2014-08-20

Denied Entry records

Denied Entries						
JournalID	TagID	Floor	DoorID	AccessTime	AccessStatus	AccessDate
30	4001002306	2	OFF02101	08:09:45	Denied	2012-08-15
33	4002003404	4	APA04458	12:07:28	Denied	2014-03-18
35	4001002307	1	OFF01202	18:27:04	Denied	2014-04-28
36	4001002306	2	OFF02202	05:50:25	Denied	2014-03-28
37	4003003455	2	OFF02220	16:52:48	Denied	2014-06-23

Visitors

Returns information on the number of visitors that have accessed the building and the locations that they have accessed.

Visitors					
TagID	Floor	DoorID	AccessTime	AccessStatus	AccessDate
4001002000	3	OFF03220	01:44:18	Granted	2014-06-20
4001002003	2	OFF02220	08:00:00	Granted	2014-03-07

Door Access

A particular Door Number is given to the system and it returns the records of access of that particular door.

System Journal - Filter By Door Number

Please Enter the Door Number Of the Door You want To View

Tag Id	Door Id	Floor	Access Time	Access Date	Access Status
4004006578	OFF01202	1	06:36:47	2013-11-24	Granted
4001002307	OFF01202	1	18:27:04	2014-04-28	Denied
4001002306	OFF02202	2	05:50:25	2014-03-28	Denied

User Access

Returns access information of a particular TagID holder.

System Journal - Filter By TagID

Please Enter the TagID of the User You want To View

Tag Id	Door Id	Floor	Access Time	Access Date	Access Status
4001002306	APA02458	2	00:09:38	2012-04-27	Granted
4001002306	OFF02101	2	08:09:45	2012-08-15	Denied
4001002306	OFF02202	2	05:50:25	2014-03-28	Denied

Section Access

Returns information of access based on section.

Offices Filter:

System Journal - Offices

Tag Id	Door Id	Floor	Access Time	Access Date	Access Status
4001002300	OFF02220	2	11:03:14	2014-04-13	Granted
4002003507	OFF02741	2	22:48:40	2013-07-06	Granted
4004006578	OFF03401	3	23:09:42	2014-03-04	Granted
4001002305	OFF03500	3	08:45:43	2014-06-24	Granted
4001002306	OFF02101	2	08:09:45	2012-08-15	Denied
4004006578	OFF01202	1	06:36:47	2013-11-24	Granted
4001002309	OFF04303	4	09:09:48	2014-05-15	Granted
4001002307	OFF01202	1	18:27:04	2014-04-28	Denied
4001002306	OFF02202	2	05:50:25	2014-03-28	Denied

Apartments Filter:

System Journal-Apartments					
					Office Apartment
Tag Id	Door Id	Floor	Access Time	Access Date	Access Status
4001002306	APA02458	2	00:09:38	2012-04-27	Granted
4002003404	APA04458	4	12:07:28	2014-03-18	Denied
4009009002	APA02600	2	07:11:12	2014-10-01	Granted

4.2 Analysis

4.2.1 Operation

This technology uses radio frequency which refers to waves that are suited for use in radio communication. It uses frequencies within the range of 50 kHz to 2.5 GHz. Increasing frequency involves an improvement in the read range as well as the speed of data transfer. It is implemented using the following devices:

- Transponder or tag that contains data about an item.
- An antenna used to transmit the RF signals between the reader and the tag.
- An RF transceiver that generates the RF signals.
- A reader that receives RF transmissions from the tag and passes the data to the host computer for processing.

The tags used are read only devices. Each tag has an antenna coil and an integrated circuit which is a silicon chip that includes basic modulation circuitry and non-volatile memory. The information that is in the memory can't be changed by RF command once it has been written. The tag is presented to the reader to initiate an authentication transaction and to request access authorization.[9]

The reader is used to activate the tag. It continuously transmits an RF signal and watches for modulated backscattering signal from the tag. The data stored in the tag is obtained by the reader using backscattering where an ac voltage is generated in the tag coil and rectified to a dc voltage of a certain level.

The information obtained by the reader is passed to the controller of that specific reader which then relays the information to the host computer for cross-checking with the reference database. If the access request is valid, access is granted and the event is logged. Otherwise, access is denied. The controller is responsible for the issuance of

signal to the magnetic lock of the doors based on response from the host computer as to whether access has been granted or denied.

4.2.2 Device Analysis

Access Controller

The access controllers are interconnected through PC-based on-line access control system as opposed to a stand alone. This method is suitable because it reduces the initial overlay costs and the continuous running costs.

Passive Tag

The passive tags consume less power than the active tags which are self powered. It is however more economical and practical to use passive tags in the complex building. Having active tags would mean that the power source of every user of the system be changed after a certain period of time.

The 13.56MHz tags have a faster reading speed, providing faster data capturing with an improved bandwidth as compared to the 125 KHz. It has substantially longer read distance (about 2-5times) than the 125 KHz tag with the same size of physical form-factors. For the same card size form-factor, more than 100 loops are needed to produce the tag for 125 KHz in contrast to the 5-7 loops for the tag operating at 13.56 MHz. This is a significant reduction in cost and hence the use of this particular frequency.[10]

Reader

The system for this building uses simple readers which read data and forward to the control panel as opposed to intelligent readers which have processing power and the ability to make decisions.

Electromagnetic Door Lock

The designs and type of electromagnetic locking systems varies with the type and usage of the doors on which they are installed.

Magnetic locks are chose as opposed to electric door strike or drop bolt. This is because such locks require very little or no maintenance and the costs incurred are minimal. The magnetic lock system is also easy to install and can be easily replaced allowing for flexibility and future expansion as well as development.

Break Glasses

The emergency break-glass switch is provided to enable the indoor users to release the locking mechanism to ensure that there are no unnecessary lock-ins occurrences.

4.2.3 Administration

Centralized administration is employed in this building. The rental apartments and the offices are all to be managed from a central point. It requires that all access requests go through a central authority that grants or denies access.

An employee in the office section may require to access more than one floor hence the doors make the group of objects while the employee is the subject. If there is more than one administrator, they will need to access the control room therefore the door is managed using a group of subjects for an object.

Access control lists are therefore employed to allow groups of objects or group of subjects to be controlled together. These will be used to determine which access rights each user has to a particular system object. To simplify administration, access control groups are used.

The limitation of central administration is single point failure and slow down in processing of requests in the case when the system is overloaded. However in this specific case, the building has inherently controlled population flow due to the nature of activity within the building. This means that a system will be developed to adequately handle the capacity in question. Centralized administration brings about reduction in complexity and ease of management.

4.2.4 System Security

Alarm Management

A magnetic door sensor may be added to monitor the door position, so that an alarm can be raised if the door is left open too long or opened illegally.

The alarm management system is set to operate for the following transactions:

- Door Forced Open(DFO) monitoring
- OTL(Open Too Long) monitoring
- Valid access
- Invalid attempt

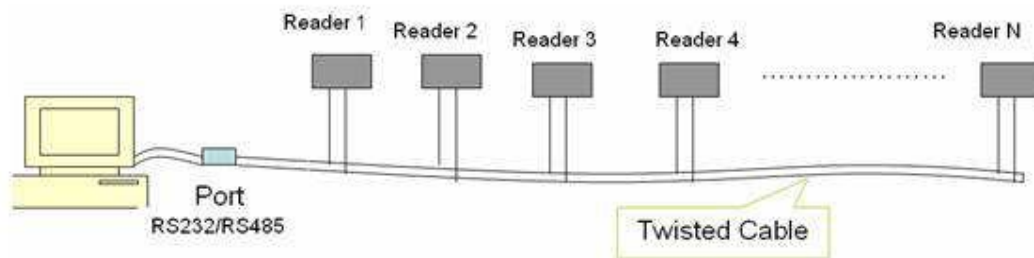
- Equipment Failure
- Power Failure

Intrusion Detection

In this control system, there is no method employed for ensuring that only the authorized user accesses the controlled door when it is unlocked. Rules therefore must be enforced to deter unauthorized access.

Network:

The readers are connected to the host computer using RS-485 or RS-232 cable. It is more flexible than RS-232 as it allows for bus network topology.



RS-485 supports longer distances than RS-232 or Ethernet. The RS-485 standard only defines the electrical characteristics of the transmitter and the receiver and not the digital communication protocols. [11]

The limitation of the RS-485 cable is length. If the length goes more than 1.5km, there is attenuation. RS-485 networks can achieve reliable data transmissions in electrically noisy environments. By considering the tradeoff between data rate and cable length, you can design a system that achieves data rates in excess of 50Mbps over cable lengths of hundreds of meters, and without repeaters. Adding shielding to the cable enhances noise immunity, and thereby increases the data rate for a given distance. Data is usually transmitted to the central unit using a serial connection usually RS-485. RS-485 enables the configuration of inexpensive local networks and multidrop communications links. It offers data transmission speeds of 35 Mbit/s up to 10 m and 100 kbit/s at 1200m.

Chapter 5 CONCLUSION

Electronic Physical Access Control Systems have widely been incorporated in large organizations significantly eliminating the inconvenience of mechanical locks and keys. In RFID systems, the bulkiness of keys is eliminated by use of light weight cards/ tags. Theft related issues such as key cutting and breaking in are totally eradicated. The DFO monitoring helps in curbing break-in instances. For an intruder to access a certain door, he/she has to have possession of the tag as opposed to the former schemes of making duplicate keys. Making a duplicate tag, though possible, is extremely difficult and this makes the RFID system a major security enhancement. There is much time saving in accessing any controlled area within the building. Access involves only two things; being close enough to the controlled access point and having the correct credentials.

There is improved efficiency with ability to control many doors from a central operating point. This eases the management of the building and makes it an enhanced security zone. Keeping a comprehensive record of all the individuals who have accessed the building electronically has an upper hand over the former manual systems because of the capability of critical analysis of data that is stored in the database using dynamic queries. The information obtained from the analysis is useful in improvement of the security system.

The designed access control network is deemed to be successful because it can perform all the main basic functions:

- Allowing & Denying access
- Limiting access & Revoking access

The major drawback of this system is its inability to capture tailgating. Ensuring that only an authorized user gains access to a controlled access point without allowing others to gain access is a significant problem. This challenge can be eliminated by using equipment with ability to incorporate other security mechanisms such as video surveillance and sophisticated alarm systems to aid in monitoring and capturing of suspicious activity such occurrences. Video surveillance helps in investigating attacks, crimes and other security issues when need arises.

REFERENCES

- [1] Holmberg, David G., Davis, William D., Treado, Stephen J., Reed, Kent A., “*Building Tactical Information System for Public Safety Officials, Intelligent Building Response (iBR)*”, NIST Internal Report 7314, January 2006.
- [2] Mark Roberti, (2005, Jan 16) “*The History of RFID Technology*”, Available: <http://www.rfidjournal.com/articles/view?1338>
- [3] Peter H. Gregory, *Advanced Physical Access Control for Dummies*, New Jersey, USA: John Wiley & Sons, Inc., 2011.
- [4] Michael V. Mannino, *Database Design, Application Development & Administration*, McGraw-Hill Education - Europe, 2005.
- [5] Gansen Zhao, Ziliu Li, Wenjun Li, Hao Zhang, Yong Tang, “*Privacy Enhancing Framework on PaaS*”, 2012 International Conference on Cloud Computing and Service Computing, pp. 131-137.
- [6] David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli, *Role-Based Access Control*, Artech House, 2003, pp.27-36.
- [7] D. D. Clark, D. R. Wilson. “*A comparison of commercial and military computer security policies.*” IEEE Symposium on Security and Privacy, pp 184–194, April 1987.
- [8] T. Mayfield, “*Integrity in Automated Information Systems*”, National Computer Security Center, September 1991.
- [9] A smart card alliance Physical Access Council White Paper “*An overview of the impact of FIPS 201 on Federal Physical Access Control Systems*” September 2005 PAC-05001.
- [10] Kevin Chung,(2004, Jan 10) “*Is 13.56 MHz RFID technology equally or more effective than 125 KHz for livestock identification and tracking?*” Avante International Technology, Inc. [Online] Available: <https://www.avantetech.com/uploads>
- [11] Thomas L. Norman, *Electronic Access Control*, Butterworth Heinemann, October 2011.

APPENDIX

Users

```

<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Uzito | User Records</title>
    <link rel="stylesheet" href="css/bootstrap-3.1.1-dist/css/bootstrap.min.css">
    <link rel="stylesheet" href="css/main.css">
</head>
<body>
    <p><h1>Users</h1></p>
    <?php
    require_once('connect.php');
    $query = "SELECT * FROM users";
    $data = mysqli_query($connect,$query);
    ?>
    <table class="table table-striped" border="1px" width="100%" height="10px">
        <tr>
            <th>TagID</th>
            <th>Name</th>
            <th>Clearance</th>
            <th>Create Date</th>
            <th>Account Status</th>
            <th>Apartment No</th>
        </tr>
        <?php while($viewallrecords = mysqli_fetch_array($data)){ ?>
            <tr>
                <td><?php echo $viewallrecords['TagID'];?></td>
                <td><?php echo $viewallrecords['Name'];?></td>
                <td><?php echo $viewallrecords['Clearance'];?></td>
                <td><?php echo $viewallrecords['CreateDate'];?></td>
                <td><?php echo $viewallrecords['AccountStatus'];?></td>
                <td><?php echo $viewallrecords['ApaNo'];?></td>
            </tr>
        <?php } ?>
    </table>

</body>
</html>

```

Administrators

```

<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Uzito | Administrators</title>
    <link rel="stylesheet" href="css/bootstrap-3.1.1-dist/css/bootstrap.min.css">
    <link rel="stylesheet" href="css/main.css">
</head>
<body>
    <p><h1>Clearances</h1></p>

    <?php

    require('connect.php');
    $query = "SELECT * FROM administrators";
    $result = mysqli_query($connect,$query);

    ?>

    <table class="table table-striped" border="1px" width="100%" height="10px">

        <tr>
            <th>Username</th>
            <th>Password</th>

        </tr>

        <?php while($viewallrecords = mysqli_fetch_array($result)){ ?>

            <tr>
                <td><?php echo $viewallrecords['Username'];?></td>
                <td><?php echo $viewallrecords['Password'];?></td>

            </tr>

        <?php } ?>
    </table>

</body>
</html>

```

Imposters

```

<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Uzito | Imposters</title>
    <link rel="stylesheet" href="css/bootstrap-3.1.1-dist/css/bootstrap.min.css">
    <link rel="stylesheet" href="css/main.css">
</head>
<body class="container col-sm-12">
    <p><h1>Imposters</h1></p>
    <?php
        require('connect.php');
        $query = "SELECT * FROM journal WHERE TagID NOT IN
        (SELECT TagID FROM users)";
        $data = mysqli_query($connect,$query);
        ?>

        <table class="table table-striped table-hover col-sm-12" border="1px"
width="100%" height="10px">

            <tr>

                <th>Tag Id</th>
                <th>Door Id</th>
                <th>Floor</th>
                <!-- <th>Door No</th> -->
                <th>Access Time</th>
                <th>Access Date</th>
                <th>Access Status</th>

            </tr>

            <?php while($viewallrecords = mysqli_fetch_array($data)){ ?>
                <tr>
                    <td><?php echo $viewallrecords['TagID'];?></td>
                    <td><?php echo $viewallrecords['DoorID'];?></td>
                    <td><?php echo $viewallrecords['Floor'];?></td>
                    <!-- <td><?php echo $viewallrecords['DoorNo'];?></td> -->
                    <td><?php echo $viewallrecords['AccessTime'];?></td>
                    <td><?php echo $viewallrecords['AccessDate'];?></td>
                    <td><?php echo $viewallrecords['AccessStatus'];?></td>

                </tr>
            <?php } ?>
        </table>
    </body>
</html>

```


NewUser

```

<?php
require('connect.php');
$tagid = $POST['tagid'];
$name = $POST['name'];
$clearance = $POST['clearance'];
$createdate = $POST['createdate'];
$apano=$POST['apartmentNo'];
$query = "INSERT INTO users(TagID,Name,Clearance,CreateDate,ApaNo)
VALUES('$tagid','$name','$clearance','$createdate','$apano')";
//Connect to database

if(!connect){
    echo("Database connection failed!");
}
$result = mysqli_query($connect,$query);
if($result){
    print("User has been added.");
}else{
    print("User addition failed!");
}
?>

```

Connect

```

<?php
$database="Uzito";
// Connect to the database
$connect = mysqli_connect("localhost","root","1234",$database);
if(!$connect)
{
    echo("Database connection failed!");
}
?>

```