

**A MODEL FOR REAL ESTATE SECURITY MANAGEMENT SYSTEM: STUDY
OF COMMERCIAL BUILDINGS IN NAIROBI, KENYA**

BY

MARY NJERI KAHORA

**A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
REQUIEREMENTS FOR THEAWARD OF THE DEGREE OF MASTER
OF SCIENCE IN INFORMATION TECHNOLOGY, DEPARTMENT OF
INFORMATION TECHNOLOGY, SCHOOL OF INFORMATION
SCIENCES**

**MOI UNIVERSITY
ELDORET**

2021

DECLARATION

This research project is my original work and has not been presented for a degree in any other University.

MARY NJERI KAHORA

DATE.....

.....

IS/MPHILIT/057/12

This thesis has been submitted for examination with our approval as University Supervisors

Prof. David Gichoya

DATE.....

.....

Dept. of Information Technology

Moi University, Eldoret, Kenya

Prof. Japhet Otike

D ATE.....

.....

Dept. of Library, Records Management and Information Studies

Moi University, Eldoret, Kenya

DEDICATION

This research project is dedicated to my family (The Kahora's) for their boundless support and inspiration.

ABSTRACT

Most commercial buildings in Nairobi are vulnerable to various forms of insecurity threats, some as severe as terrorist attacks. Proprietors of these buildings have invested heavily in latest security techniques and technology. Social and technological dynamics have resulted in unforeseen security threats that demand constant upgrading of existing interventions to secure the properties. This study analyzed the current security procedures in five commercial buildings within Nairobi County and developed a Model Real Estate Security Management System. The objectives of this study were to: determine the security procedures used within the five commercial buildings; determine weaknesses and challenges associated with their current security system; determine the requirements for the security management system and develop an improved real estate security management system model. The Study adopted rapid development methodology for system modeling and development while requirements were gathered and analyzed qualitatively. The target population comprised of 50 members of staff of the buildings. A sample of 35 respondents was purposively selected. A web based model security management system was designed and developed using Unified Modeling Tools to depict the design plan. The Study findings revealed that existing security procedures are manual and they are exposed to misplacements and alterations while the systems are not integrated and do not allow sharing of information. Also, existing security technologies are expensive and do not meet the expected standards. The system that this study proposes allows collaboration and sharing of information among the various stakeholders and real estate agents to enhance security for the buildings and their occupants. The developed web based security system can be used by any real estate agency, security agencies and law enforcers, the study recommends integrating the model real estate security system to the conventional security devices such as alarms detectors, cameras, e.tc to positively identify visitors, report crime properly, collaborate, and share information with other buildings' management agents at a lower cost. Continuous study and implementation has been suggested on leveraging latest technologies to enhance security as new threats keep on emerging.

TABLE OF CONTENTS

DECLARATION.....	ii
DEDICATION	iii
ABSTRACT	iv
TABLE OF CONTENTS.....	v
LIST OF TABLES	ix
LIST OF FIGURES	x
ACKNOWLEDGEMENTS	xi
LIST OF ABBEVIATIONS.....	xii
CHAPTER ONE	1
INTRODUCTION	1
1.0 Background of the Study.....	1
1.1 Problem Statement.....	3
1.2 Aim of the Study.....	4
1.3 Specific Objectives of the Study	4
1.4 Research Questions.....	4
1.5 Significance of the Study	5
1.6 Justification of the Study.....	5
1.7 Scope of the Study	6
1.8 Limitations of the Study.....	6
1.9 Definition of Key Terms	7
1.10 Organization of Thesis Document	8
CHAPTER TWO	10
LITERATURE REVIEW.....	10
2.0 Introduction	10
2.1 Commercial Buildings that were studied	10
2.1.1 Summary of the Case Studies	16
2.2 Theoretical Framework.....	17
2.2.1 Social and Technical Theory	18
2.3 Conceptual Framework.....	20

2.4 Collaboration and Sharing of Information	21
2.5 Factors that Contribute to Security Threats in Commercial Buildings.....	22
2.6 Analysis of Security Threats and Trends for Commercial Buildings in Kenya	23
2.7 Analysis of the Global Security Threats and Trends for Commercial Buildings	24
2.8 Status of the Current Security Systems.....	26
2.9 Improved Security Systems.....	27
2.10 Innovative Security Systems	28
2.11 Challenges with the New Security Systems	31
2.12 Intelligent Buildings.....	34
2.13 Implementation Gap.....	36
2.14 Anticipated Future Threats.....	37
2.15 Chapter Summary	38
CHAPTER THREE.....	40
RESEARCH METHODOLOGY.....	40
3.0 Introduction	40
3.1 Research Methods	40
3.2 Research Design	41
3.3 Study Location.....	41
3.4 Study Population.....	41
3.5 Sampling Methods	42
3.6 Sample Size	43
3.7 Requirement Gathering Techniques	44
3.7.1 Interviews	44
3.7.2 Observation.....	45
3.8 Requirement Analysis.....	45
3.9 System Development Methodology	45
3.10 Tools Required for System Development	46
3.10.1 Software.....	47
3.10.2 Hardware	47
3.11 Chapter Summary	47

CHAPTER FOUR	48
REQUIREMENT ANALYSIS AND MODELLING	48
4.0 Introduction	48
4.1 Findings of the Study	48
4.1.1 Security Procedures:.....	48
4.1.2 Existing Technologies and Associated Challenges:.....	49
4.1.3 Crime Reporting Procedures.....	51
4.1.4 System Remote Accessibility	51
4.1.5. User System Training	52
4.2 User Requirements Interpretation.....	52
4.2.1User Interface.....	52
4.2.2Data Design Form Requirements	53
4.2.3 Non-functional requirements	53
4.2.4 Attributes for the buildings	53
4.3 Use Case Diagram	54
4.4 Class Diagram	55
4.5 Context Diagram.....	56
4.6 System Scope	57
CHAPTER FIVE	58
SYSTEM DEVELOPMENT	58
5.0 Introduction	58
5.1 System Design	58
5.1.2 The Bottom up Approach	59
5.2 Architectural Design	59
5.3 Sample Screen Shots.....	60
5.4 Login Details	60
5.4.1 Register a Person.....	61
5.4.2 Check In.....	61
5.4.3 Check Out	62
5.4.4 Incident Reporting.....	63
5.4.5 Flag A Suspicious Person at Teleposta Towers	63

5.4.6 Threat Detection at Unga House.....	64
5.4.7 Reporting Incidents	65
5.5 Sample Code.....	65
5.6 General Test Data and System Document	67
5.7 Result Table for Check in Visitors	68
CHAPTER SIX.....	69
SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS	69
6.0 Introduction	69
6.1 Summary of the Study Findings	69
6.2 Conclusion	71
6.3 Recommendations.....	72
6.4 Suggestions for Further Study	72
REFERENCES	73
APPENDICES	77
Appendix 1: Photos of the Existing Security Systems/Technologies	77
Appendix 2: Interview Guide for Security Guards	79
Appendix 3: Interview for the Security Officers.....	80
Appendix 4: Interview for Property Manager.....	81
Appendix 5: Interview for Administrative Police	83
Appendix 6: Observation Check List	84
Appendix 7: User Manual	85
Appendix 8: Sample Code	103
Appendix 9: System Evaluation Form.....	123

LIST OF TABLES

Table 1: Population and Sample Size	42
Table 2: Results for the Current Security Procedures	49
Table 3: Summary Results for the Existing Technologies.....	50
Table 4: Result Table for Login Test Data	67
Table 5: Result Table for Register Test Data.....	68
Table 6: Result Table for Check-In Test Data	68

LIST OF FIGURES

Figure 1: Social Technical Model	19
Figure 2: Conceptual Model	20
Figure 3: Structure of Face Detection Method.....	29
Figure 4: Building Automation Network.....	36
Figure 5: Rad Overview Structure.....	46
Figure 6: Use Case diagram	54
Figure 7: Class Diagram	55
Figure 8: Context Diagram	56
Figure 9: System Scope	57
Figure 10: System Architectural Design.....	60
Figure 11: Login Dialog Box	60
Figure 12: Register Dialog Box	61
Figure 13: Check in Dialog Box	61
Figure 14: Checkout Dialog Box.....	62
Figure 15: Incident Report Dialog Box	63
Figure 16: Flag Suspicious Person Dialog.....	63
Figure 17: Visitors Flagged Dialog Box.....	64
Figure 18: Threat Detection Dialog Box	64
Figure 19: Reporting Incidents Dialog Box.....	65

ACKNOWLEDGEMENTS

Special thanks go to my supervisors, Professor David Gichoya and Professor Japhet Otike for their timely, passionate support, and guidance that made this work a success. Many thanks to you my beloved mum, Hannah Wanjiru Kahora and my daughter, Shaynen Suen, for your abundant support, and love that provided me an enabling environment during this study. My brother, Samuel Maina, your abundance support took me far and I trust that success of this work brings you joy. My other siblings, Alice and John, kindly receive my gratitude for your kind support, love and standing with me.

Mr. David K. Machua, Real Estate Advisor, I appreciate your insights on real estate security structures and functions. It gave me the foundation for research into the development of sustainable real estate security management system. Special mention goes to Peter Kibera for his tremendous support. My colleagues class of 2012, I appreciate your moral support and encouragement may God bless you in all your endeavors. Dorcas Njoroge, I thank you for your understanding, and priceless support. To my friends and all others, who I may have skipped, yet you contributed towards this project, thank you too.

Above all, thanks to the Almighty God, to whom all the glory and honor of the successful completion of this Masters Project I surrender.

LIST OF ABBEVIATIONS

C.I. D	Criminal Investigation Department
CBD	Central Business District
CCTV	Closed Circuit Television
CISSP	Certified Information System Security Professional
CRISP	Connecting Research in Security Practice
CSS	Cascading Style Sheet
DBAs	Database systems administrators (DBAs)
DFD	Data flow Diagrams
ERD	Entity Relation Diagram
FOSS	Free and open source software
HTML	Hypertext Markup Language
IR	Infrared beams
IBI	Intelligent Building Institute
ICT	Information Communication Technology
IP	Internet Protocol
JAD	Joint Application Design
KNBS	Kenya National Bureau of Statistics

LSPS	local service providers (LSPs)
MVC	Management View controllers
OBS	Office security building
ORM	Object relational mapper
ORR	Optical Reader Recognition
Resp	Respondent RADRapid Application Development
STS	Security, Technology & Systems
UML	Unified Modeling Language
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network

CHAPTER ONE

INTRODUCTION

1.0 Background of the Study

Kenya is a regional economic hub that enjoys political stability. This has given growth to a rapidly growing economy manifested by among other factors, a proliferation of a wide range of prime, real estate commercial investments in most major urban centers. Kenya National Bureau of Statistics (2011) indicated that the real estate market in Kenya has been experiencing a boom in the past few years. This is evidenced by increasing number of off-plan purchases of properties, the rise in property prices, and an influx of foreigners into the local property market. It is also evidenced by the rapid development of suburbs of major towns.

Nairobi suburbs, for instance, have experienced exponential growth partially due to the Government of Kenya proposal to set up a Nairobi Metropolitan region to decongest the Central Business District and ease transaction of business in the area. Nairobi is among Kenya's towns that have experienced rapid growth. According to UN-habitat (2013), the capital city has a population of about 4 million people, which grows by 5 percent annually.

Most of the large commercial buildings in Kenya's towns and cities are a beehive of economic activities and are, therefore, vulnerable to a wide range of security threats such as theft, burglary, and terrorist attacks. UN-habitat (2013), for instance, argues Nairobi faces very high-security challenges. The report says recent terrorist activities across the world have heightened insecurity in many countries, Kenya included. The 2013 Westgate

attack in Nairobi and other terrorist attacks across the country have increased checks on visitors to various premises to ensure security in and around the buildings.

Kenya National Bureau of Statistics (2011) shows to stand out and succeed in the very competitive real estate market that is characterized by a high demand and low supply, developers have incorporated building security systems in their developments, establishing the concepts of smart and intelligent buildings to offer something that would attract and retain tenants and at the same time offer them value for their money.

According to a global research for commercial building security measures around the globe by Navigant consulting (2013), the security products and services in the globe are mature but the penetration rate of modern security technologies remains relatively low except for the largest and newest buildings.

This Study analyzed the current security systems in five commercial buildings within Nairobi County and confirmed that indeed the investment in security has been accorded priority. This was indicated by the wide range of approaches applied to guarantee security. Among these are checks conducted by guards at entrances to the building. The guards, either use metal detectors or manually check visitors for any security threat possession. They also get the visitors' identity and record it in a logbook before issuing them after confirming their destination. They in some instances accompany the visitors to the destinations in case of doubt. The guards also physically check incoming vehicles, confirm their entrance stickers if any and record details in a register. Tenants and staff of the buildings also identify themselves before entering.

The study identified gaps as; the buildings are vulnerable to various forms of insecurity ranging from normal thefts, burglary to terrorist attacks. The fact that the buildings often house valuable properties in an environment where movement is not well-controlled compounds the security challenge. Tracking of visitors entering into most commercial buildings is often manual where identification details of the visitors are recorded in log books. These records are prone to misplacements and/or alterations and therefore, may not be very reliable.

According to Ekman (2014), advance in technology today has improved security systems beyond what was previously considered possible. The technological developments, besides ensuring optimal security solutions, make it harder for criminals to conduct their activities. The following improved security systems have boosted Security of Property; Access Control and Automatic Gate Access, CCTVs, alarms, Biometric Identification System, Thermal Infrared Recognition Technology, Optical Reader Recognition Technology, and M-Secure

1.1 Problem Statement

Some buildings have advanced to use of computer-aided security. This approach normally uses standalone, unintelligent applications such as Excel worksheets, which are not linked to any central data base system. Such systems neither verify the visitor's identity nor do they alert the security personnel of any suspicious visitors entering the building. This means one can commit the same crime in several buildings separately and yet raise no suspicion nor get identified positively as there is no collaboration and sharing information platform. Hence there is need to come up with a model security management system that allows collaboration and sharing of information among shareholders, real

estate agents and security management across several buildings and at a lower cost, to offer a solution to the problem.

1.2 Aim of the Study

This study sought to analyze the current security procedures in commercial buildings within Nairobi County and develop a model real estate security management system.

1.3 Specific Objectives of the Study

The specific Research Objectives were to:

1. Determine the security procedures used within the buildings.
2. Determine the security management systems' weaknesses and challenges in commercial buildings.
3. Determine the requirements for a security management system.
4. Develop an improved web based model real estate security management system for commercial buildings

1.4 Research Questions

The Research sought to answer the following questions:

1. What are the existing security measures and procedures being used by the proprietors, property agencies and security agencies to manage and ensure security within the building?
2. What are the weaknesses and challenges experienced by the users while using the current security systems?

3. What are the requirements of a web based model real estate security management system?
4. What are the design aspects needed to improve the web based model real estate security system for commercial buildings?

1.5 Significance of the Study

The Study provides critical information to property developers and business operators regarding enhancement of security within their premises. This will in turn, enhance returns on investment thanks to reduced losses from insecurity. Increased collaboration on security among commercial buildings owners will improve security in the city and if replicated in other towns, will make the country safer and attract more foreign and local investors and tourists. This will contribute to higher national economic growth.

The insights on the security challenges, analysis of weaknesses in current security procedures and systems and the suggested mitigations will assist the Government and policymakers in planning and decision making on issues relating to security.

The study also contributes to the existing literature on Real Estate Security Management and builds a foundation for further scholarly research.

1.6 Justification of the Study

Insecurity is today a global challenge though with varying levels per country. It is a major drawback to business progress and real estate investment. Evolving trends in crime require a review of traditional approaches to maintaining security and instead adoption of more sophisticated approaches that leverage on technology and also encourage broader

stakeholder collaborations. With the ever-increasing hype of the digital age coupled with high penetration of smartphones, tablets, computers and fast internet connections, the Model Real Estate Security Management System developed through this Study will be universally accessible to allow constant stakeholder collaboration and information sharing.

1.7 Scope of the Study

The study entailed carrying out a review of security systems in five commercial buildings located in Nairobi, Kenya and are managed by Lloyd Masika Limited. The buildings were purposively selected. The study focused on property Managers, system administrators, security officers/guards and law enforcers who were also purposively selected from the five commercial buildings. The data collected during the study was analyzed and used as system requirements for a model real estate web based security management system that allows collaboration and sharing of data among security managers across commercial buildings in the County

1.8 Limitations of the Study

Due to time and financial limitations, the Study covered only five commercial buildings within Nairobi County. The buildings are all managed by Lloyd Masika Limited. The study did not extend to residential property and other commercial buildings within and without Nairobi and their environs. However, the output of this Study can be applied with or without modifications to any real estate property.

1.9 Definition of Key Terms

Building Security: This is the act of protecting buildings and their occupants from vandalism, burglary, theft and personal attacks by use of security guards, access control systems, closed circuit surveillance systems, alarm systems and so on, building security management system, Challinger (2010).

CCTV: These are Closed Circuit Television cameras, also known as video surveillance and are used for monitoring, primarily for surveillance and security purposes. It involves placement of cameras at specific places such as walkways, public halls, entrances, parking and observation of the camera's input on monitors from somewhere else. Over the years, the installation of CCTV cameras has grown tremendously around the globe particularly in the areas where terrorist threats and attacks have undermined national security, Reynald (2013).

Access Control: Means by which people are granted or denied access to specific areas. Commercial buildings often accommodate large volumes of tenants, employees, and visitors that are routed through a control area before admittance is authorized. The degree of access to the buildings varies depending on purpose, area and time. Some of the types of access control into a building are magnetic card readers, barcodes, and smart cards, Reynald (2013).

Smart and Intelligent Buildings: Buildings that incorporate the best available concepts, materials, systems, and technologies to achieve a building that is more than a mere fulfillment of shelter as a basic need, Intelligent Building Institute (IBI), (2010). It is an expression of self-investment, privacy and most of all safe havens in which, business

owners, property managers, occupants, and visitors can experience ultimate comfort, convenience, safety, and security.

Real Estate: Comprises of; land, buildings as well as natural resources such as water, minerals, crops and uncultivated flora. Real Estate is grouped into three broad categories; residential, commercial and industrial. Examples of a commercial real estate are office buildings, retail stores buildings and warehouses buildings, IBI (2010).

1.10 Organization of Thesis Document

The document is organized into seven chapters as follows: -

Chapter One: Introduces the topic of this Study and gives a brief background and situation analysis of the problem. It particularly highlights the current security approaches, gives relevant definitions of terms, and the Significance as well as Justification of the Study. It also highlights Statement of the Problem, Research Questions, study Objectives, Study Scope and Limitation and the Organization of the Study.

Chapter Two: This Chapter gives an overview of the current security procedures and factors that contribute to security threats in commercial buildings. Overview of the previous literature on the security status approaches and reviewed four case studies in commercial buildings both globally and locally. It also analyses the case studies, highlights the technologies that are used to develop an integrated real estate security management system and describes the conceptual framework of the security management system.

Chapter Three: This Chapter explains and describes the Research Methodology adopted for the Study. The Chapter begins by outlining the Research Design adopted for the Study. Through the process of rationalizations, the Chapter justified the choice of the Research Design. The Chapter also explains identification of the Study population and Sampling Design used to isolate the Study sample as well as Data Collection Methods, Data Collection Process, and System Modeling Implementation.

Chapter Four: This Chapter discusses requirements Analysis and system modelling. Requirement analysis entailed a review of data collected during the Study and analysis of the existing system to establish the requisite features for a Real Estate Security Management System Prototype projected by this Study. Design entailed defining the System Architecture, Modules, Interfaces and System Data.

Chapter Five: This Chapter explains the process of System Development, Testing, and Evaluation of the Real Estate Security Management System. It involved System Construction, verifying System Construction, preparing a test data, Documents Plan and System Evaluation.

Chapter Six: This Chapter presents discussions, conclusions, and recommendations based on the analyzed results. It summarizes the study findings based on the study Objectives and gives conclusion and recommendations based on the Study findings.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The purpose of this literature review is to provide in-depth information of the similar studies that have been conducted and to provide deeper understanding of the topic. The review has assisted the researcher in determining research methodologies and identifying the research gap that sought to bridge. The literature review is based on four qualitative case studies for Commercial Buildings to gather insights into their security operations, and explore how collaboration and sharing of information occur among proprietors, property/security agencies and law enforcers.

According to Welman and Kruger (2013), case study offers an opportunity to deal with "understanding of uniqueness and peculiarity" of a particular case and also provides insights into a particular research. The chapter also discusses theories that are related to the study and developed a conceptual frame work.

2.1 Commercial Buildings that were studied

The Study undertook four case studies for Commercial Buildings to gather insights into their security operations. According to Welman and Kruger (2013), case study offers an opportunity to deal with "understanding of uniqueness and peculiarity" of a particular case and also provides insights into a particular research.

The four buildings studied and the findings are as follows;

1. Teleposta Towers

Study at Teleposta Towers – Kenya, on security procedures systems David and Erick (2015). Available at Lloyd Masika Management Department: A Documentation of Security Procedures: Unpublished

Teleposta Towers is one of the skyscrapers in Kenya with 28 floors and three basements.

It has the following security features: -

- Analog and Digital Closed-Circuit Television (CCTV) Cameras

The analog cameras relay footage to video tape recorders, which capture the analog signals as pictures. The analog tapes were found to be very slow and produced blur snapshots. The building management has replaced the analog CCTV, with digital ones. They have a digital video recorder whose digital signals are saved in a computer.

- Visitor Identification

All visitors must produce identification documents, often the national identity card while tenants and staff must produce official badges. The visitors' details are registered in a register/log book. The details include name, identity card, and phone numbers as well as purpose and destination for the visit. The information, which is entered into marked rows and columns, also includes date and check-in and check-out times. This paper-and-pen system was found to be slow and creates delays at the entrance. Should the guards suspect any visitors, they accompany them to their destinations and wait for them.

- Visitor Scanning Using Electronic Walk-Through Metal Detectors

Teleposta Towers has three entrances. All persons entering the building are required to pass through walk-through metal detectors. They first put aside any loose metal or electronic gadgets they may be having such as car keys, phones, laptops etc.

Should the metal detectors raise an alarm, security guards at the entrance scan the visitor using a mobile metal detector

- Motor Vehicle Access Control System

The building has 420 car bays in three basements. All vehicles pass through the following checks:

- Car stickers

All motor vehicles which park in the building are issued with stickers, indicating their registration number and specific parking bay. The stickers are displayed on the windscreen and only cars with stickers are can access the private road leading to the building.

- Explosive Detector Scan

Once the validity of the sticker is confirmed, the vehicle proceeds to a section where the guards scan it for explosives using an explosive detector. The guards also physically check the car for other security threats. If any security threat is discovered, information is relayed to the Central Computer, which warns deny the vehicle access into the building.

- Log Book Recording

Once the vehicle is cleared, its details are recorded in a register. These include registration number, time in, driver's name as well as national identity card and mobile phone numbers. The parking level it goes to is also recorded.

- Access Control

Though the car is by now allowed in, the driver has to swipe a card issued at the gate to open the final entrance barrier. These cards are issued to the vehicles which are allowed to access the building

2. Rahimtulla Building

The building is one of the high-rise buildings in Nairobi with 22 floors, two basements and open parking lots. The building houses major corporations with thousands of workers and visitors. After its completion in 1999, the biggest worry was how to manage it and the best possible security approaches to adopt. According to Lynn B. (2013), the building installed surveillance security systems with embedded DVRs.

Analog surveillance cameras were also installed and connected to embedded hybrid DVRs to ensure real-time recording of footage throughout. The connections ensured integrated surveillance throughout. The cameras are placed along the corridors, stairways, and lobbies.

High megapixels' cameras were also installed in the most critical areas, one camera at the front gate to monitor trespassers and another one at the entrance to the parking lot to capture vehicle registration numbers.

Besides the DVRs surveillance system, intelligent devices such as real-time alarms, notification by email, pop-up video, warning sounds, and video search by date, time and event were also incorporated.

3. Microsoft Offices

The facility, which is in Dublin, Ireland, has adopted the use of Speed Gates as an access control system. Speed Gates are entrance control systems that are used to provide security by allowing entry only to authorized persons. The technology utilizes multiple infra-red beams, typically creating a matrix linked to an advanced microprocessor with opinion-making software. The matrix of IR beams means there is more data for the processor to analyze. This allows the system to track multiple people through the lane simultaneously and make decisions about how fast people are moving. The end result of this kind of technology is an improvement in performance in three key areas - security, speed, and safety.

Roche (2013) argues the shift to Speed Gates resulted from the need to upgrade to a control system with higher efficiency and capacity to handle more people. This resulted in an upgrade of the security system to create a secure border inside the premises that ensured only authorized persons progressed further into the building. This decision considered several factors such as the amount of space available in the main entrance and speed of throughput. The Speed Gate was installed at the reception where there was a need to pay attention to the level of security.

This greatly enhanced security since the new system, with capacity for one person per second, detects more people and faster reducing the risk of unauthorized access. The

speed of throughput was also increased as there is no delay occasioned by resetting the system beam as it is automatic.

Roche adds fast throughput of the Speed Gate was crucial for Microsoft's reception, which handled about 2000 staff and visitors daily. The slim pedestal of the Speed Gate has allowed fitting of more lanes in the reception area thus, clearing hold-ups for people moving in and out.

4. Cisco Facilities

Cisco is an American multinational technology company based in the United States and has over 271 facilities in more than 50 countries. According to Jacob (2012) the biggest challenge for Cisco security initially, was to ensure only authorized people accessed the facilities and to identify unauthorized entries. To achieve this, Cisco adopted the following security technologies: Intrusion Detection, Physical Electronic Security Access Control Systems and CCTV.

However, between 1992 and 2007 Cisco embarked on attempts to upgrade these technologies to address the following attendant shortcomings: - provide a unique individual user access card; security systems integration in all Cisco facilities worldwide and management of physical access using the limited resources.

Jacob says by 1997, Cisco lacked network-based access control and relied on standalone controls at every facility. This meant employees from different facilities had to have their badges manually programmed into the local authorization database to access different facilities across countries.

Lack of connectivity – coordination, and integration of camera surveillance was still a challenge since most cameras sent their signals to a bank of videotapes that were re-used after every 30 days. A disparate database was administered and managed from a computer with some specialized software for managing access control that was inconsistent and required high-skilled personnel.

According to Roche (2013), to determine the best staff general physical access control system a real-time access control system, skilled database administrators and well-maintained equipment (servers) and software to support the system is required .

After the study, Cisco installed a centralized server architecture that connected to servers from different countries. The servers were linked to each other using IP WAN. The access control and alarm systems in every country were also standardized. Employees were issued with staff badges that bore one's photograph and an identification number. Whenever one uses the badge to open a door the photograph and badge number is copied from the regional servers to the global/centralized server. The photograph is then compared with the one in the video stream and access granted or denied depending on the results.

2.1.1 Summary of the Case Studies

According to Case Study 1: Teleposta Towers upgraded from analog to digital CCTV, which capture real-time footage and saves it in a computer. However, recording of visitors' personal details is still manual where the details are recorded in a counter book.

According to Case Study 2: Rahimtulla Towers embedded hybrid DVRs to ensure continuous recording of footage. The cameras are placed along the corridors, stair ways,

and lobbies to spot suspicious visitors or activities in the building and prevent/monitor crimes such as theft and vandalism.

According to Case Study 3: Microsoft has automated their security by using Speed Gates system. It is fast and allows passage to authorized individuals only. Microsoft installed Speed Gates at the reception to control the large volumes of employees and visitors seeking entry daily.

According to Case Study 4: Cisco installed a centralized server architecture that connected to servers from different countries. The servers were linked to each other using Wide Area Network' this helps to determine any authorized entries into their premises. All the employees' details were put into the database and badges were produced with an identification number and employee's photograph on it. The badges are used to open doors while the details on the badge would be compared with the details on the database and on the video stream to grant access. For visitors and new employees, their records would be put into the database before issuing them with a badge

2.2 Theoretical Framework

According to Abend and G. (2018), theoretical framework consists of concepts that are interrelated together to predict and explain a phenomenon and in most cases to extend knowledge of a certain research study. According to Williams, J., & Booth, C. (2017), theoretical framework is very important for any given research study as it gives direction and helps to interpret things, connect researcher to the existing knowledge, describe various aspects, specify key variables, define how the researcher analyzes and interpret

data that is to be collected and helps to address the how and why question by expressing the assumptions of the research.

The researcher studied theory that is related to the topic of this study and it informed the study accordingly. The theoretical framework that guides this study is socio technical theory. This theory was chosen because of its core idea that the design and performance of any system can only be improved if both social and technical aspects are brought together. It ensures that human and technology are coined together to enhance collaboration and sharing of information among interconnected systems.

2.2.1 Social and Technical Theory

According to Jim Smith (2010), there is need to apply some theory before taking the next step of developing any system. The defined theory is then broadened to principle of redesign, change and act as a foundation of informed actions.

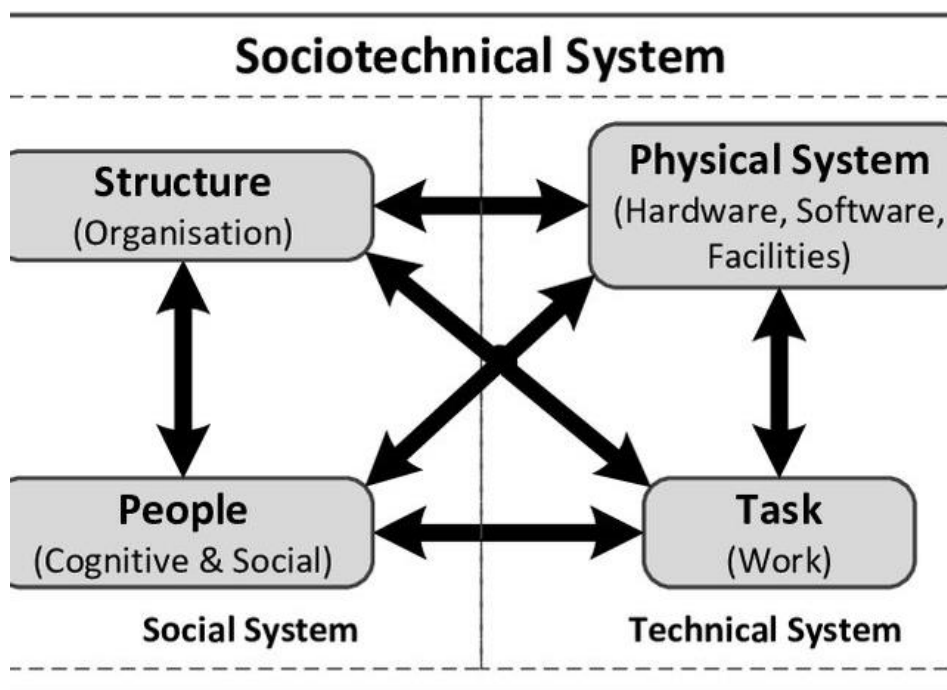
According to Mumford E. (2006) social and technical theory has the idea that design and performance of any system can only improve if social and technical aspects are put together and treated as interdependent parts of a system. He indicates that systems fail because they focus on one aspect of the system mostly technology and fail to analyse and understand interdependences that exist.

Social technical theory originates from the pioneering work at the Tavstock Institute in 1960 and is still applied to date and continued on a worldwide basis Harold Leavitt (2010). It was originally coined by Emery and Twist (1960) to define systems that involve interactions between humans, machines and environment. Benefits derived from this theory are:

- Understanding on how systems may be improved.
- Understanding and analysis of how systems work.
- Reliable and valid data on how to build understanding.
- High chance of successful improvements.
- Strong engagement.

Social technical theory draws heavily on work of Harold Leavitt (2010) who viewed organizations as comprising four key interacting variables namely; tasks, structures, technology and people (actors).

Figure 1 below represents Mumford E. (1960) model of socio technical system design.



*Mumford E. (1992) Social technical model
Figure 1: Social Technical Model*

The researcher chose the theory because it is intellectually robust and provides useful tool to help understand and address challenges. It provides a coherent vehicle for collaborations and sharing of information with other stake holders, real estate agent, law enforcers, tenants and etc.

2.3 Conceptual Framework

According to Smyth (2014), a conceptual framework is a structural set of ideas and theories that help a researcher to identify a problem and look for a suitable solution to meet the aims and goals of the research. He adds that conceptual framework can be graphically presented and used as a tool for integration and interpretation of information.

From the Case Studies analyzed above, a conceptual framework was derived as shown below:

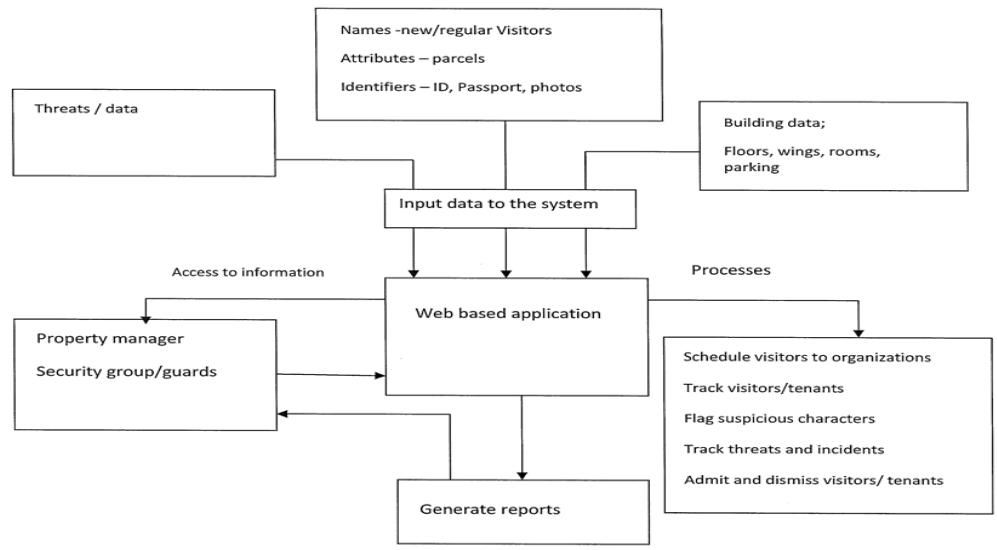


Figure 2: Conceptual Model

According to the conceptual model above, the security management system will be used to capture, store and retrieve visitor and tenant details as well as building details threats and incidents. Visitors will be registered in the system central database first. They will then be checked in if they qualify and later checked after clearing with their business in the building and the security agent. The web-based application will generate reports such as visitors to the building at specific time and date, flag out suspicious characters, track threats/incidents and enhance collaboration, sharing of information among stake holders and other users.

Property managers, security officers, CID can log into the system and view activities in real time.

2.4 Collaboration and Sharing of Information

According to Ephraim (2015), collaboration is where one or more people work together with common shared goal. Technology today has the potential to transform any service in a number of ways. It offers collaborative platforms as a means of communication, sharing information and interaction among users. According to Ephraim Freed (2018), collaboration and sharing of information applies all-engaging approach where users and stake holders are engaged in an ICT based platforms to share information and work together towards addressing a certain challenge.

According to Brindley and Blaschke (2009), collaboration platform can work in real time where more than one person communicates, review and collaborate on the same platform at once. Feedback of any raised issue is received without any delay despite the location of

the communicator. Some of the real-time collaborative tools are instant messages/alerts, emails, chat forums, video conferencing, VoIP calling etc.

2.5 Factors that Contribute to Security Threats in Commercial Buildings

Size: Commercial buildings are mostly targeted for security threats especially those that accommodate large amounts of valuable properties and have many occupants as well as a large number of visitors. According to Challinger (2011), such large sizes slow down security response.

Anonymity Within the building: This applies often in situations where one cannot tell whether people in a building should be in it or not. These are a collection of genuine occupants or visitors and among possible criminals, who may not be easily identified. Security threats are enhanced in large anonymous environments. On the contrary, a small and identifiable group of people enables better and manageable security procedures, Shaftoe (2010). He argues anonymity in a commercial building may also lead to a "not my problem" attitude, making it easier for criminals to operate unnoticed.

Building Contents: Commercial buildings generally house high volumes of valuable properties that would normally attract criminals. Clarke (2013), states that most of such buildings easily attract potential criminals. He says some occupants in commercial buildings furnish their offices with very expensive fittings and expensive properties increasing chances for possible threats.

Occupant Characteristics: Challinger (2011) describes some occupants of commercial buildings as not concerned about security within and outside the buildings. Others are very ignorant and unable to detect any security threat about to or already taking place.

Physical Features: According to Yuen (2016), physical features of a big commercial building provide high opportunities for crime. He argues that surveys indicate elevator crimes and breakdowns are among the top five concerns of big commercial buildings.

Location: This refers to the location of a building and its environment. Kitteringham (2016) says many commercial buildings are located in main urban centers and their proximity to mass shipment facilities and ease of access by the general public exposes them to a higher security threat.

2.6 Analysis of Security Threats and Trends for Commercial Buildings in Kenya

According to Ibrahim (2013), Kenya's national security is ranked among the worst in the world. He says the country is grouped among nations facing unmanageable security situations, at position 42 near the bottom and ranked as poor in personal security for its citizens and visitors. He attributes Kenya's position largely to instability among its neighbors such as Somali and argues the situation is likely to remain the same unless security in Somali is improved.

According to Ploch (2014), Kenya experienced at least 17 attacks involving grenades or explosive devices that caused many fatalities and injuries, between 2011 and 2014. The worst security incident was the 2013 Westgate Shopping Mall, in Nairobi terrorist attack where gunmen killed at least 69 people and injured over 175 others. The attack significantly increased security alertness and provoked serious concern around local commercial buildings and abroad.

Sugden (2014), reported in a survey conducted on Nairobi's security preparedness carried in the Business Daily (August 31, 2014), that most contractors and owners of buildings

are yet to come to terms with the high level of risk associated with terrorism in the city, putting human life and expensive investments at risk. It stressed that owners of commercial buildings in Nairobi must bear the additional cost of installing modern equipment, software, and features to deal with emerging security threats. The survey recommended provision of all security emergency plans to occupants of commercial buildings while owners should invest in access control systems and alarms to prevent unauthorized visitors and also install CCTVs to monitor human movement.

2.7 Analysis of the Global Security Threats and Trends for Commercial Buildings

Though security products and services for commercial buildings are mature in the globe, the penetration rate of modern security technologies remains relatively low except for the largest and newest buildings, Navigant Consulting (2013). A Research by Navigant Consulting on commercial buildings security measures conducted in 2013 found that building security measures are not often changed unless the building undergoes a significant renovation, which may be undertaken after a very long time. The report established despite the availability of new security technologies in the market, most buildings still operated on the old and manual systems, compromising security in the buildings. It also established digital technology accelerated the ability to affect real estate security systems.

According to Homeland Security and Emergency Management Agency (HSEMA), (2012) commercial buildings in the United States of America range in size. However, they share the following vulnerabilities: lack of security measures; designs without security considerations; inadequate vehicular control; lack of security in loading dock and open access by the tenants and visitors. The survey recommended that protective

measures to be taken to reduce common threats facing commercial buildings and protective measures such as planning and preparedness; personal checks at the entrance; access control; barriers; communication and notifications; as well as monitoring and surveillance. It also recommended incidence response and reporting of suspicious activities.

According to Sugden (2014) comparing the 2008 bombing of TajHahal Palace and Towers in Mumbai, India that killed at least 166 people with theft and burglary within commercial premises, concluded theft, burglary, and other undesirable activities remain the largest security challenge for commercial buildings.

Guidry (2010) states that the attack on the Murrah Building in Oklahoma City in 1995 brought monumental changes in security for Federal buildings and their leased spaces. Guidry observes security enhancements on commercial buildings are on the cutting edge and have since steered to the implementation of security measures such as CCTV cameras, biometrics, access control, vehicular entry/exits, lighting, Anti-Ram devices and ventilation safeguards. Other measures include balanced magnetic switches, sensors lighting, optical turnstiles, elevator lockouts, and motion sensors. Some of the security services derived from these security measures are admittance monitoring and control; visitor processing; alarm response and monitoring parking. Others are documentation of conditions and incidents; maintaining logs; tracking incidents; exterior after hours/special events and interior patrol.

Guidry relates security response to threats for commercial buildings to their location, and type of buildings, for example, buildings in populated areas such as New York, Boston,

Washington, D.C, and San Francisco are viewed as prime targets and their security responses have been given attention accordingly.

2.8 Status of the Current Security Systems

- CCTV Manning

CCTV footage is stored in the same building what poses a risk of loss of the data if anything happened to the storage computer. Further, if the building was destroyed, it would be impossible to establish what happened using the CCTV. The guards manning the building also control the CCTV room exposing the data and the cameras to possible manipulation especially should the guards be linked to the crime under investigation. The CCTV cameras in some locations are visible what means one can cover them to avoid being monitored.

- Visitor / Staff Identification and Vehicle Control

Visitor / Staff Identification access control approach focuses on the two categories and fails to recognize the possibility of guards themselves posing a security threat as they are not subjected to any checks when they report for duty. There is also the risk of guards developing familiarity and rapport with regular visitors and staff to the extent of compromising their security responsibilities by allowing them in unchecked. A familiar staff may continue accessing the building even long after ceasing to be a client or staff courtesy of the rapport. Use of badges may also compromise security when an ex-staff retains the badge even after discontinuation of service. Use of car stickers can also be subject to manipulation through the creation of counterfeits. These cases undermine the efficacy of Visitor / Staff Identification and Vehicle Control as access control measures.

- Manual Log Book

The indicated security systems above have proved to be laborious and time-consuming especially for busy buildings. It presents challenges especially for the illiterate. The system is also prone to abuse especially in case of unverifiable details such as phone numbers, which may be deliberately recorded wrongly. The records sometimes get lost or fade especially when not properly handled. The logbook can also be abused by users should the guards deliberately decide not to take details of some people or the register gets stolen or is misplaced.

2.9 Improved Security Systems

Advance in technology today has improved security systems beyond what was previously considered possible. The technological developments, besides ensuring optimal security solutions, make it harder for criminals to conduct their activities. The following improved systems have boosted Security of Property.

- Access Control and Automatic Gate Access

Modern Access Control Systems designed for commercial and residential buildings are more complex today. They are designed to grant and deny access during certain hours. The system can also send emails in case some doors are left open. Automatic Gate Access can be operated through key fob, security code or car recognition. These intelligent systems ensure every access to the buildings is monitored effectively.

- CCTVs

Improved CCTV camera technology makes it harder for criminals to avoid being recognized as the pictures are more clear and flexible. Technological advancements have allowed for smaller cameras, which are perfect for users who prefer the covert use of the gadgets. Footage is also accessible through the internet. This has made cameras more deterrent.

- Alarms

Technological advancement has made alarms more effective especially when used in combination with other security solutions such as sensors. Detective alarm systems have become more effective in monitoring building access points. Unlike the loud traditional alarms that alerted the neighborhood to destruct criminals, modern alarms alert the manned receiving centers and enable operators to contact security personnel without rousing the neighborhood.

2.10 Innovative Security Systems

Technology around security systems has evolved tremendously over the years. As a result, Property Developers and Owners, as well as Real Estate Agencies, have come up with innovative ways to ensure efficient security management for their buildings. Some of the latest technologies implemented to achieve include: -

- Capture of Facial Features Through Biometric Identification System

According to Ekman (2014), continuous technology advances have significantly hastened image processing and facial expression recognition. Real-time facial expression

recognition has been a technology development used to identify people. It is known as Face Tracking Procedure and includes procedures such as Image Processing, Skin Color Detection, Lip and Eye Detection.

Multimodal biometric recognition system that incorporates facial recognition, iris and fingerprints are also incorporated to uncover false and double identity cases in real-time.

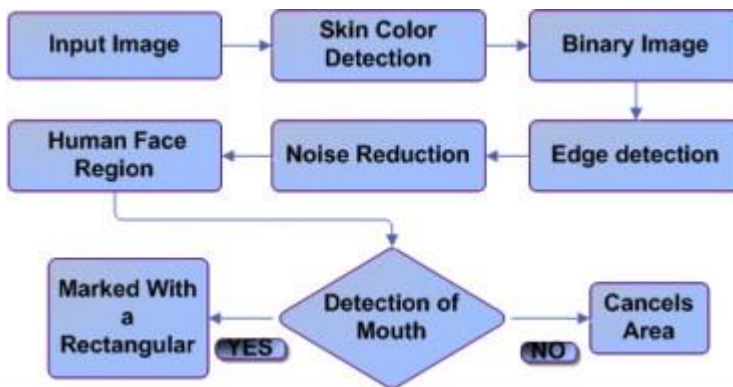


Figure 3: Structure of Face Detection Method

The face detection method by Ekman (2014) above, shows facial expression recognition process. The facial region is detected and segmented using feature approaches. Facial expressions are classified by assessing the relationship functions among numerous lip types and positions of the corners of the mouth. Additionally, the algorithm is implemented in order to achieve real-time recognition for various facial expressions. Experimental results show that the proposed scheme can recognize facial expressions exactly and proficiently.

- Thermal Infrared Recognition Technology

The Facial Recognition Expression model by Ekman (2015) is dependent on clear and well-lit environment. Heseltine (2016) argues this model may be limited if the object is

not well-lit. Heseltine developed a facial recognition technology that uses thermal infrared technology to read person's thermal signature. This technology can recognize and identify a person's face even in poorly lit environments or total darkness. The technology uses deep neural network systems to analyze infrared images and match them with ordinary photos. Thermal infrared recognition technology provides images based on the heat energy (infra-Red) emitted by the object photos

According to Mensik (2016), the thermal infrared technology uses Detection, Recognition, and Identification (DRI) criteria known as Johnson Criteria. The criteria are defined as: -

- Detection: Ability to detect and distinguish an object (target) from the background
- Recognition: Ability to classify the object into a class such as human beings, animals, vehicle etc.
- Identification: Ability to describe the object into details, for instance, two people walking wearing black and white clothes.

Heseltine (2016) argues, though his model has the challenge of reliability in case of body temperature variations, the technology is superior as it can work in the dark without active infrared illuminations.

- Optical Reader Recognition Technology

Hounsel (2015) argues that one of the main solutions to security challenges is the installation of identity data solutions such as optical reader recognition. It enables mining and processing in real time visitor's identification data from an identification card, driving

license, passport or business card. The optical reader recognition Technology besides being faster and more accurate, it reduces human errors related to the manual recording of visitors' details. The data mined through optical reader recognition can also auto-populate fields depending on security requirements that's enables a facility to create accurate reports on visitors entering and exiting the building.

- M-Secure

M-Secure is a security solution which comes as a Small device with a control panel and several panic buttons, Alvis (2017). It is designed to control thefts at M-Pesa and other outlets that handle bulk money by transmitting information to control panels. For instance, in case of a security threat at an M-Pesa shop, the attendant would press the M-Secure panic buttons, which immediately send an alert to the control rooms, nearest police station, and any other designated persons. According to Alvis (2017), other M-secure solutions are; M-secure for home, M-secure for health, M-secure for children, and M-secure for house helps.

2.11 Challenges with the New Security Systems

Despite advancement in security systems, the transition to new technologies has several challenges as they are open to various vulnerabilities such as: - and pose the following challenges: -

- System Hacking:

Hacking is a way of gaining access to a computer system by unauthorized personnel commonly known as hackers, Lisa B. (2016). Hackers use their technical skills to gain

access to computer systems for either malicious or criminal purposes, and others would do it just for fun. According to Lisa B. (2016), some of the hacking methods are password cracking, privileges escalations, spyware installations and key loggings among others.

Recent global reports of cybercrime indicate technologies such as biometrics are also vulnerable if stored and accessed online. Fang (2015) says in late 2014, a European hacker group managed to generate fingerprints of Germany defense secretary Ursula von der Leyen from a press event and recreate photos of the fingerprints which they used to get access to other events. To mitigate against hacking, there is need to carefully consider the type of biometric that is more appropriate and also combine more innovative technologies and robust information security practices.

- Privacy

The common challenge for building owners and property management companies especially when installing CCTV cameras is striking the right balance between property and occupants' security and upholding privacy rights of visitors and the occupants. Article 31 of the Constitution of Kenya, for instance, specifically protects the right to privacy. It states:

"Every person has the right to privacy, which includes the right not to have—

- (a) Their person, home or property searched;
- (b) Their possessions seized;

(c) Information relating to their family or private affairs unnecessarily required or revealed; or

(d) The privacy of their communications infringed."

CCTV cameras and facial recognition systems infringe on this right since they record every person and activity within their reach. Individuals within premises under surveillance may be engaged in private business but this too is considered public activity for surveillance.

- Lack of Legal Clarity

According to U.S. Government Accountability Office (2015), there is a concern in the US that due to lack of legal clarity information collected from facial technology and surveillance cameras could be used, shared or sold in ways that customers do not understand, anticipate or consent to. The institution adds Federal Law does not expressly state the circumstances under which commercial entities can use facial recognition or surveillance cameras to identify or track individuals or when customer knowledge or consent should be required for the technology's use. Further, in most contexts, Federal Law does not define how personal data from the technology may be used or shared.

The situation is the same in Kenya. This leaves businesses without guidance on how to properly employ facial recognition and what protections are required for data gathered through the biometrics. For example, while it's necessary for a business to prominently post that the premises are under surveillance, management is not under any obligation to notify occupants that facial recognition technology is in use. This eliminates the ability for individuals to "opt in" or consent to be identified.

2.12 Intelligent Buildings

According to Intelligent Building Institute (IBI), (2010), Intelligent Buildings is house constructions that incorporate the best available concepts, materials, systems, and technologies to achieve property that is more than a mere fulfillment of shelter as a basic need. IBI stresses comfort, privacy, as well as property and human safety as key elements of an Intelligent Building.

Intelligent buildings have building management systems that control, monitor and optimize building services such as security - CCTV and alarm systems, access control, time and attendance control and reporting (notably visitor's movement). It does the same for lighting, heating, entertainment system, ventilation, filtration and climate control among others to create comfort.

The essence of Building Management Systems is in the control technologies, which allow integration, automation, and optimization of all the services and equipment that provide services and manages the environment of the buildings. According to According to Kastner (2015), the main application areas for Building Automation services are Security critical (intrusion alarm and control system), Safety critical (fire and control alarms systems) and Environmental control (heating, ventilation, and air conditioning) normally provided by proprietary stand-alone systems. The automation of security and safety-critical services reduces operational costs and increases efficiency and functionality through the possibility of sharing data originating from one control system. Therefore, an integrated building automated system can be installed to substitute different single systems.

The use of these technologies allows the optimization of various site and building services, often yielding significant cost reductions. There are numerous methods by which building services within buildings can be controlled. These broadly fall into two types – Access Control- Based and Time-Based. Access Control- Based provides services that restrict entry into the building such as visitor registration and surveillance, while Time-Based provide heating or lighting services, etc. and only when required.

Access control is an integral part of the safety and security of any building. Access control systems work to keep building occupants and properties safe with an integrated Building Management System.

According to Kastner (2015), the main application areas for Building Automation services are Security critical (intrusion alarm and control system), Safety critical (fire and control alarms systems) and Environmental control (heating, ventilation, and air conditioning) normally provided by proprietary stand-alone systems. The automation of security and safety-critical services reduces operational costs and increases efficiency and functionality through the possibility of sharing data originating from one control system. Therefore, an integrated building automated system can be installed to substitute different single systems.

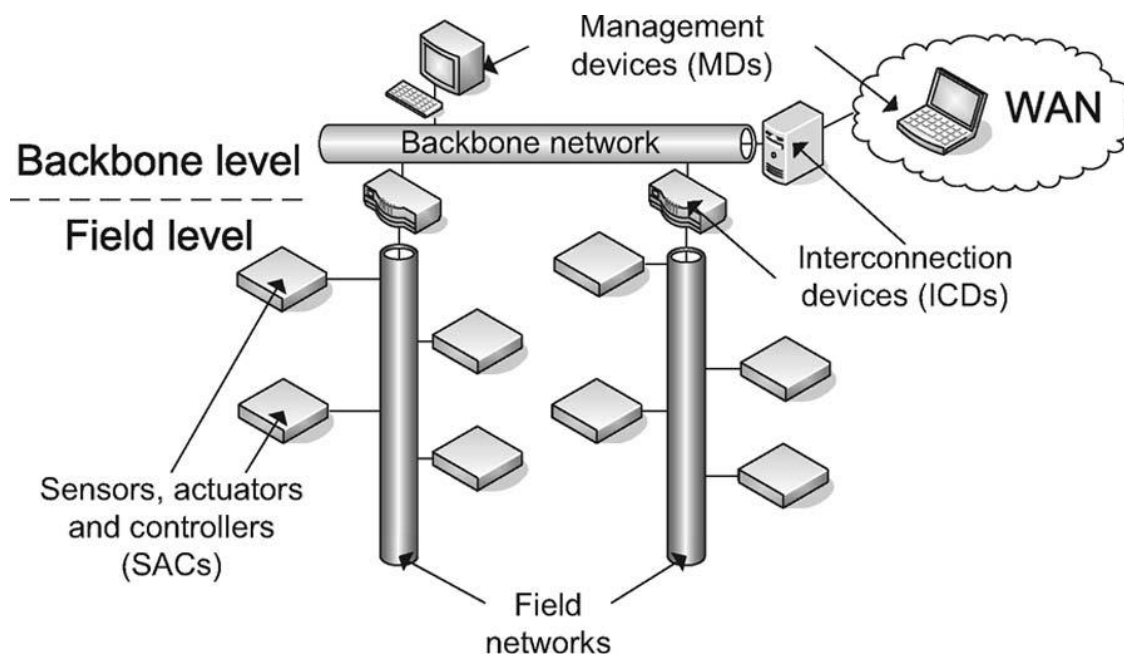


Figure 4: Building Automation Network

The figure above shows a building automation network by Wolfgang Kastner (2015)

2.13 Implementation Gap

The above challenges indicate that a gap exists between the security procedures and the expected security standards. The Study identified the gap as Inefficiency of the current systems and the enormous cost of hiring guards and procuring registers, which with time get filled up, tattered, altered and/or misplaced leading to loss of information. Retrieving information and generating reports from log book is also a challenge. There is also a risk of replication of information due to lack of intelligent systems while the manual systems lack the capability to eliminate, monitor or deter undesirable characters.

There is, therefore, need to develop a Real Estate Security Management System that ensures automation of manual systems, elimination of inefficiencies and the attendant enormous costs, while providing for easy retrieval of data, better monitoring visitors and

sharing of information across buildings through collaboration. This study developed a Model Real Estate Security Management System for this purpose.

2.14 Anticipated Future Threats

Despite all efforts, Security threats in commercial buildings are unlikely to be completely eliminated. There are some threats that are anticipated in the future such as;

Technological Advancements pose a significant challenge in future to commercial buildings. Advancements such as satellite images, hidden cameras and even hacking of CCTV footage that is meant to assist in securing commercial buildings, will most likely pose a significant threat to the same buildings. As a result, the gathering of intelligence regarding a building will not necessarily require one's physical presence in it.

Building's design also poses a security challenge to commercial buildings. As buildings embrace modern building technology such as green buildings, some of these designs may expose the building to new avenues of attack and thereby compromise their security.

Building use is changing with times. Institutional use of commercial buildings resulting in high human traffic will continue posing security threats to the buildings. Nairobi CBD has experienced commercial buildings being turned into universities that handle thousands of students and other clients daily. This is likely to continue in the future. Managing such high human traffic may pose a challenge and create security threat especially if the trend continues and we have a building hosting several institutions.

Eliminating these threats lies in the flexibility of security approaches and adjusting fast. It will also be important to include security experts at the design stage to incorporate security considerations early enough.

2.15 Chapter Summary

The Literature Review started by noting that commercial buildings today face security challenges that are raising concern among owners and occupants.

On analysis of the global security threats and trends for commercial buildings, the Review established that though security products and services in the globe are mature, the penetration rate of modern security technologies remains relatively low except for the largest and newest buildings.

The Review also noted that despite the availability of new security technologies in the market, most buildings still operate on the old and manual systems and as a result, security in the commercial building remains compromised. It was found out that security measures in-built into the structures are often not changed unless the building undergoes significant renovation.

The Literature Review also identified some of the security services derived from the security approaches found to be in operation. These include admittance monitoring and control, visitor processing, alarm response, monitoring parking lots, documentation of conditions and incidents, maintaining logs, tracking incidents, exterior, and interior patrol after hours/special events.

For the Kenyan situation, the Literature analyzed security threats and trends for commercial buildings in Nairobi. It was noted that Kenya's national security is ranked

among the worst in the world and is grouped as one of the nation's major challenge. This, and especially terrorism in Nairobi City, has put human life and expensive investments at risk. Further interrogation of security procedures in Nairobi buildings identified key challenges with the existing systems. These include storage of CCTV footage in the same buildings, Lack of

proper security protocol where guards could be security threats in themselves, replicable car stickers and potential of laxity and over familiarity of the guards with tenants and visitors.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This Chapter explains the research design used for the study, area of study, population and sampling methods. It also discusses the methodology used to develop the Model Real Estate Security System.

Greg (2015) describes Research Methodology is a systematic process used to collect data within which facts are placed so that their meaning may be clearly seen. Greg (2015) says that research methodology is determined by research design, data collection methods, sampling methods and data analysis methods.

3.1 Research Methods

According to Herbst and Coldwell (2004), research methods are strategies used to implement a plan to answer research questions.

This Study adopted qualitative research Methodology. The methodology was adopted for this Study because of its ability to provide a detailed description of how the respondents feel about the security issues in the buildings. It was effective in identifying tangible facts such as how the security is managed and systems used to manage the same. This was achieved by having open-ended interview questions to the respondents. Observations alongside the interviews and studying existing documents that are related to real estate security management.

3.2 Research Design

According to Labaree (2013), research design describes how research will take place including how data will be collected, what tools will be used and the intended means of analyzing the data.

The study adopted case study design for gathering and analyzing requirements while Rapid Application Methodology approach was used for system development. The case study gave an insight of security measures used in commercial buildings both globally and locally (Kenya), and challenges experienced. Also, the case studies assisted in identifying the research gap and came up with recommendations to fill the gap.

3.3 Study Location

The Study was conducted in Nairobi City. It offered an ideal location for the Study because it is Kenya's capital city and more vulnerable to insecurity. It also has experienced serious incidences of insecurity and threats in the recent past. As the face of Kenya, the city can set standards for national and international urban centers and property developers on security for buildings.

3.4 Study Population

Cooper and Schindler (2016), defined the term Population as; the total collection of elements about which, we wish to make inferences. All buildings within the City composed the Population for this Study. The selected five buildings have total population of 50. However, the researcher targeted those respondents that are directly involved in security management.

Table 1: Population and Sample Size

No	Buildings	Sample category	Population	Sample Size
1	Teleposta Towers	Property manager	1	1
		System admin/vendors	4	1
		Senior security officers	1	1
		Security guards	4	4
2	Unga House	Property manager	1	1
		System admin/vendors	3	1
		Senior security officers	1	1
		Security guards	4	4
3	View Park Towers	Property manager	1	1
		System admin/vendors	5	1
		Senior security officers	1	1
		Security guards	4	4
4	Hazina Towers	Property manager	1	1
		System admin/vendors	5	1
		Senior security officers	1	1
		Security guards	4	4
5	Standard chartered building	Property manager	1	1
		System admin/vendors	5	1
		Senior security officers	1	1
		Security guards	2	2
6	Administration police Service	Police officers		2
	Total		50	35

3.5 Sampling Methods

According to Singaravelu (2015), Sampling is a means of selecting a subset of units from a target population for the purpose of collecting information. The information collected is used to draw inferences about the population as a whole. The subset of units selected through the acceptable Sampling Design for the specific Study is called a Sample.

Purposive Sampling was again used to pick a sample from the Population of fifty employees of the five buildings selected. However, Cluster Sampling applied first where

the fifty employees were clustered into seven categories: Property Managers, Supervisors, Senior Security Officers, System Administrators, Vendors, and Security Guards.

According to Tongco (2013), a Purposive Sample, also commonly called a Judgmental Sample is selected based on the knowledge of a Population and the purpose of the study. Purposive Sampling can be very useful for situations where you need to reach a targeted sample quickly and where sampling for proportionality is not the main concern.

The selected were: Teleposta Towers, Hazina Towers, Unga House, View park Towers, and Standard Chartered Building.

3.6 Sample Size

According to Denscombe (2010), a sample size is the representatives selected for the study whose characteristics represent the larger group from which they were selected. A sample size is made to gather data about the population in order to make an inference that can be generalized to the population

The sample size was arrived by sampling staff in the five buildings and from the target population, the researcher was able to arrive at accessible population by selecting those involved in security management only. Out of the total population, 35 employees were selected for this Study in equal proportions with reference to numbers for each category for every building.

3.7 Requirement Gathering Techniques

Lawton (2015) defines requirement gathering techniques as a process of determining what users and stakeholders want, what they require, and how to fulfill their interests. It involves understanding what the users know, what they do, and the context in which they want to use the system, and expectations for a new or upgraded system. It requires frequent communication with the users and stakeholders to ensure functional specification. Lawton (2015) says that requirements can be gathered through interviews, questionnaires, observation, census, experiments, documents, and archival records.

This Study used Interviews and Observation as techniques for requirement gathering. While a review of literature such as Reports, Newspapers, and Journals was used to collect Secondary Data.

3.7.1 Interviews

The respondents were; security Guards, Security Officer, System administrators/Vendors, Property Managers and the Kenya Police Officers. According to Prasad M.S (2009), Interview is a two-way systematic conversation between an investigator and informant initiated for obtaining information for the relevant study. Prasad classifies interviews into five categories: Structured, Unstructured, Focused, Clinical and in-depth. For this Study, Structured Interviews were used where the Researcher talked to the respondents directly and filled the responses in the Interview Form (appendix 2). The data collected was subsequently analyzed and interpreted later in Chapter Four.

3.7.2 Observation

Powell (2008) defines Observation as a way of gathering data by watching behavior, events or noting physical characteristics. He says Observation can be open - performed while the subject is aware or confidential – undertaken without the subject’s knowledge. The subject is likely to behave normally under confidential Observation.

For this Study Observation and Interview ran concurrently with photographs taken (as shown in Appendix 8) to identify the building security systems that are in place. Observation check list (appendix 6) that had a list of items the researcher was to observe was used.

3.8 Requirement Analysis

The data collected from the interviews and observation was analyzed and used to come up with the user requirements which guided the design of the model system. The analysis was done to understand the problem and come up with the solution the system sought to solve. The researcher was able to achieve this by coming up with user and system requirements, the researcher then adopted Rapid Application Methodology for the system development and modelling.

3.9 System Development Methodology

The Study adopted Rapid Application Development (RAD) Methodology for System Design and Development. RAD uses minimal planning and therefore, allows much faster writing of software. The Researcher used the following specific RAD phases to develop the Real Estate Security Management System: -

- Requirements Planning
- User Design
- Rapid Construction
- Transition stage

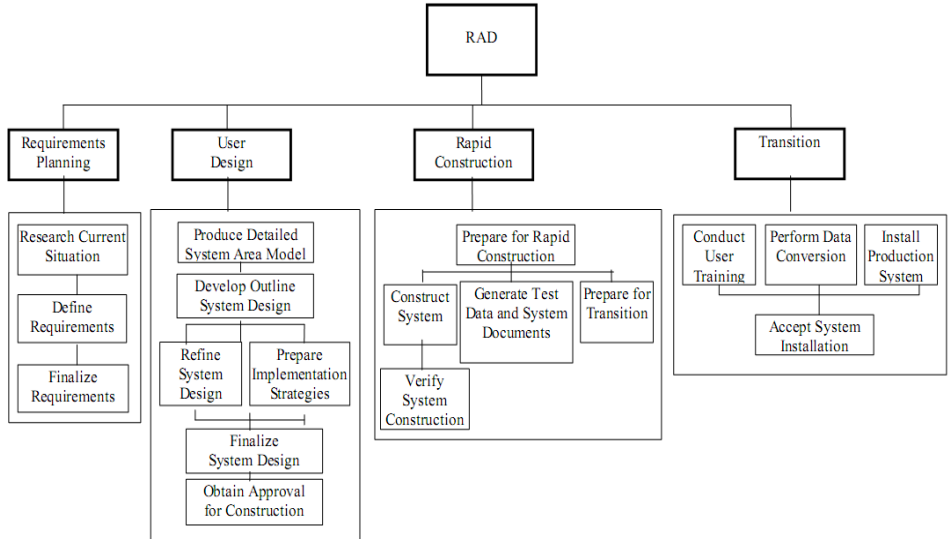


Figure 5: Rad Overview Structure

The figure above depicts RAD Overview Structure by Abert Ronnell (2010)

The Rad overview structure above describes the phases that were followed in developing the Real Estate Security Management System.

3.10 Tools Required for System Development

Below is a complete description of hardware and software components used to develop the Real Estate Security Management System and their use: -

3.10.1 Software

- **Php 7.0:** For server side scripting
- **Apache 3.2.2:** For receiving requests to access web pages and run security checks.
- **MySQL 5.7:** For database modelling
- **Text editor** (subline text): Source code editing with application programming language (API)

3.10.2 Hardware

1. **Test server:** - Core i7 Desktop computer with 2TB HDD, 8 GB RAM

3.11 Chapter Summary

This Chapter discusses all the techniques applied in conducting the Study. It Highlights the Research Methodology, Design, and Population, Sample and Sampling methods applied. It also discusses the study Location and Data Collection. In the end, the Chapter discusses the System Development Methodology used for this Study and also outlines the System Requirements.

CHAPTER FOUR

REQUIREMENT ANALYSIS AND MODELLING

4.0 Introduction

This Chapter discusses two major components: Analysis and Design. Analysis entailed studying and interpreting requirements gathered from primary and secondary sources during the study. Design on the other hand consisted of, the System Architecture, Modules, Interfaces and System Data.

4.1 Findings of the Study

Requirements gathered were organized and documented by creating categories based on each Objective to ensure optimal solution of the system. Below are the interview questions and their answers summarized;

4.1.1 Security Procedures:

These refer to the security procedures carried to ensure security. It is in line with the first objective that is; to determine the security procedures used within the buildings. The actors involved in security procedures are the security guards.

From the interview conducted, it is obvious that the current security procedures are still manual, where visitors are checked manually and their details recorded in a physical log book.

The following are the analysis in table 2, of the security procedures that formed the bases for the requirements.

Table 2: Results for the Current Security Procedures

No	Interview question	Response	Text analysis
1	What are the types of security system to manage security in the building?	-Use of a log book and a pen to register any visitor that is checking in and any incident -Use of CCTV cameras to monitor any activities in the building -Use of alarm, metal detectors	misplacement, tattered and loss of the log book digitization integration
2	How are the security checks carried out?	-Physically checking the visitors - use of metal detectors	Digitization Integration
3	What are the systems for regular visitors' check?	-Physically identifying the visitors	digitization

Source: *Field study January 2015*

Based on the analysis above, it could be seen that different questions could lead to more than one text analysis from one respondent; document loss, misplacement, tattered, digitization, integration and training. This analysis shows that there is need to digitize and integrate the current systems to ensure collaboration and sharing of information.

4.1.2 Existing Technologies and Associated Challenges:

The study sought to find out what are the security management systems' weaknesses and challenges in commercial buildings. This was in line with objective 2 and 3 of the study of; Refers to the existing security technologies.

Table 3: Summary Results for the Existing Technologies

No.	Questions	Response	Text analysis
1	What challenges do you experience with the existing security systems?	<ul style="list-style-type: none"> -Difficult in retrieving data since it is stored manually - Lot of time taken to register visitors and to check in and out, since the visitors are registered every time they visit the building. - Information not accessible remotely - Stake holders and agents are not able to access information in real time and from any location and at any time 	<ul style="list-style-type: none"> Integration Digitization Sharing
2	What kind of desirable features or functionalities that are missing in the current system?	<ul style="list-style-type: none"> -Positively identifying visitors who have visited and registered within the building or from another building. -A system that is able to be accessed from anywhere and at any time. - System that can allow collaboration and information sharing. 	<ul style="list-style-type: none"> Digitizing Integrating Visitor tracking
4	what are the major challenges to adoption of Information Technology	<ul style="list-style-type: none"> -High costs of acquiring technology -Lack of user proficiency. 	<ul style="list-style-type: none"> Training

Source: Field study January 2015

Based on the text analysis above, the respondents indicated that the existing technologies are not able to identify visitors positively, use a lot of time to register visitors since the process is manual, difficult in retrieving the information. While users of the system are

not able to collaborate and share information across different buildings which the proposed system sought to solve.

4.1.3 Crime Reporting Procedures

This is a very important procedure as it indicates how crimes in the buildings are reported to the authority. It is in line with the main aim of this study which is to analyze the current security procedures in commercial buildings.

One of the respondents (Resp. 5) said *“Crimes in commercial buildings are reported to the authority but the process is very long as it takes making calls which most of the time goes unattended or visiting the authority offices where one has to queue for long before being attended to. ICT based platform would help in reporting any crime to the authority promptly. On the other hand, crimes are replicated to other buildings and a collaborative platform would go in handy to communicating and reporting issues promptly with other users and stake holder.”*

This indicates that there is a problem on how the crimes are reported to the authority and it was supported by respondent Resp 3 who indicated that the procedures are very casual and requires a platform where users and the authority could interact for prompt action.

4.1.4 System Remote Accessibility

Research findings showed that most of the current security systems are not accessible remotely hence making it impossible to know what is happening in the buildings at a glance and slowing down decision making. Respondent Resp 6 said *“Security systems mostly for tracking visitors, reporting suspicious persons and flagging threats are manual and cannot be accessed remotely since they are reported in a log book manually.”*

Hence the stake holders and agents are not informed promptly as to what is happening leading to some issues go an attended and slowing decision making process.” This was also supported by respondent Resp 8 who also confirmed that some CCTV footages can be accessed remotely but there is no ICT based system to collaborate and share information on the same. This calls for a system that can be accessed remotely to enhance prompt decision making.

4.1.5. User System Training

On the user system training, respondent Resp 12 who is the ICT vendor said *“Training the users on the system use is very paramount since it would help the users in adopting to the system quickly.”*

Training the users will enhance system adoption and it is critical during implementation as it helps in identifying challenges experienced by the users.

4.2 User Requirements Interpretation

4.2.1 User Interface

1. Must have a log-in dialog box with unique username and password to enhance authentication.
2. Must have access levels e.g. for standard user, administrator e.t.c.
3. Search visitors’ records by using key words such as name, car registration number.
4. Generate reports where the user would key in the date of the required reports.
5. Enable data input validation.
6. Centralized data base where the user operates on a server environment

As indicated by respondent Resp. 6, Resp., 11 and Resp. 12 in table 11

4.2.2 Data Design Form Requirements

1. Names of the visitors, tenants, vendors e.t.c as indicated
2. Identifiers – Identification card number, passport, job card, photo
3. Destination, time in, date.
4. Capture attributes from table.

As indicated by respondents Resp 6, Resp 10 and Resp 12. Table 12.

4.2.3 Non-functional requirements

5. Accessibility: The system should be available at all times and easily accessed to the any time and from any location as indicated by respondent Resp. 19.
6. Reliability: The system should have accurate outputs and available all the time.
Suggested by respondent Resp. 20
7. Secure: The system should be secure and safe from virus attacks, intruders, hackers as indicated by respondent Resp. 3
8. Compatibility: The system should be compatible with other existing system. This was indicated by respondent Resp. 9
9. Centralization. The system should have a central database that ensure server environment. Respondent Resp. 9.

4.2.4 Attributes for the buildings

- Names
- Organizations/tenants
- Floors

- Wings
- Rooms

The above requirements are necessary for monitoring visitor/vendor movements in terms of their exact destination i.e. the building, organization, floor, wing and room they visited. This creates a record of tenants in the building indicating the specific floors, wings and rooms they occupy, which makes management of the building easier. This was indicated by respondent Resp.9 table.

4.3 Use Case Diagram

Use Case Design scenario showing the main processes

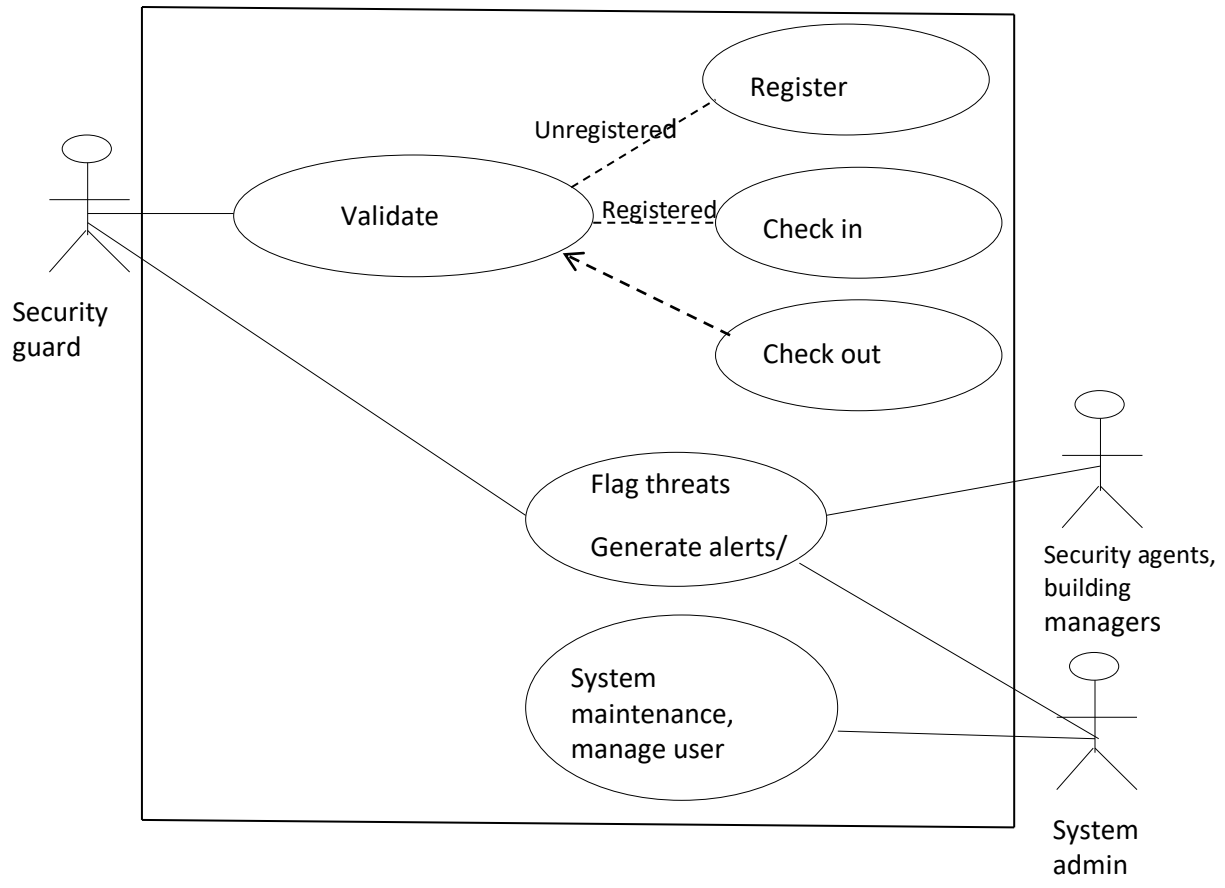


Figure 6: Use Case diagram

Figure 8 above demonstrates the main System processes and system users' interaction with the system. The main processes are register, check in/out people, flag threats and generate reports. While checkout is indicated with an arrow to show that it is a must to complete the process..The System Users are; Security Guards/Officers, Building Agents and System Administrator. The Security Guard register, check in/ out people and record threats. Building Agents and Security Officer will access reports, while the System Administrator maintains the System.

4.4 Class Diagram

Class diagram was used to show the system class, attributes and relationships.

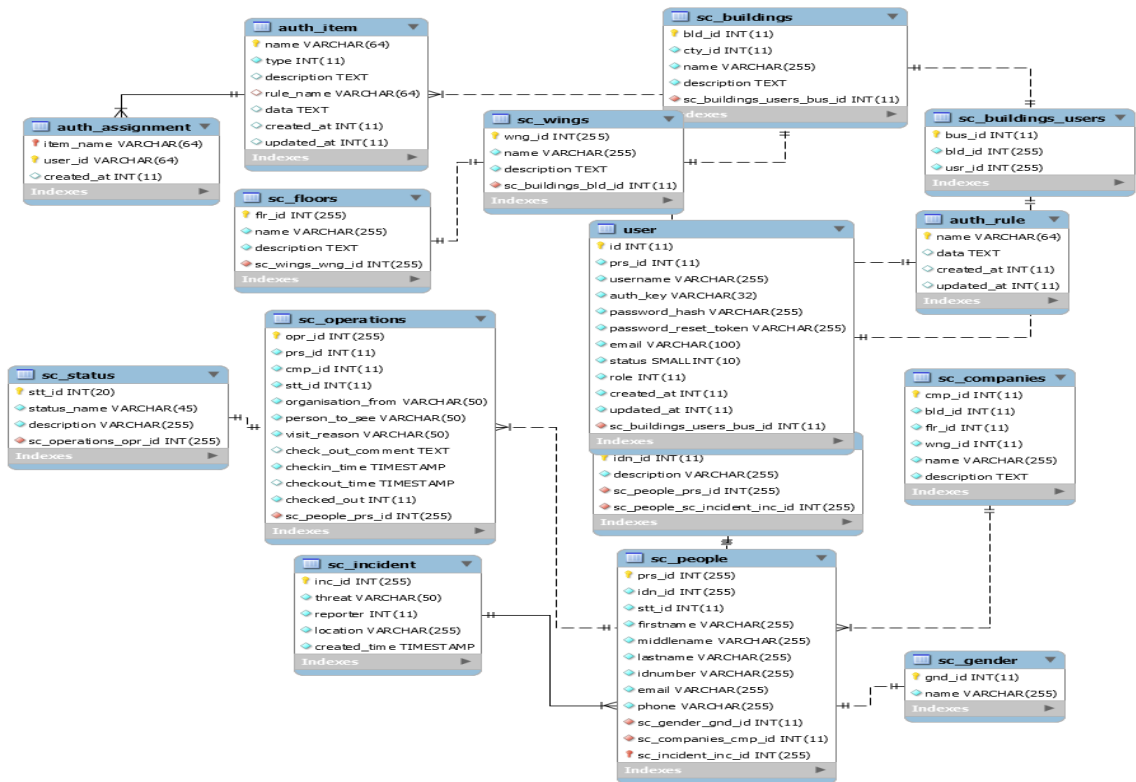


Figure 7: Class Diagram

The figure above depicts the structure of the System. It shows the System's entities / classes, their attributes, operations (or methods), and the relationships among them. For instance, it shows how a registered person relates to each checking, how each checking relates to the building, office and eventual company. It also shows that one person can check-in into more than one building while one office can be in one specific building.

4.5 Context Diagram

.Context diagram is a tool used to show how the system interact logically. The researcher therefore used the diagram during the system design to show the interaction between the system and actors.

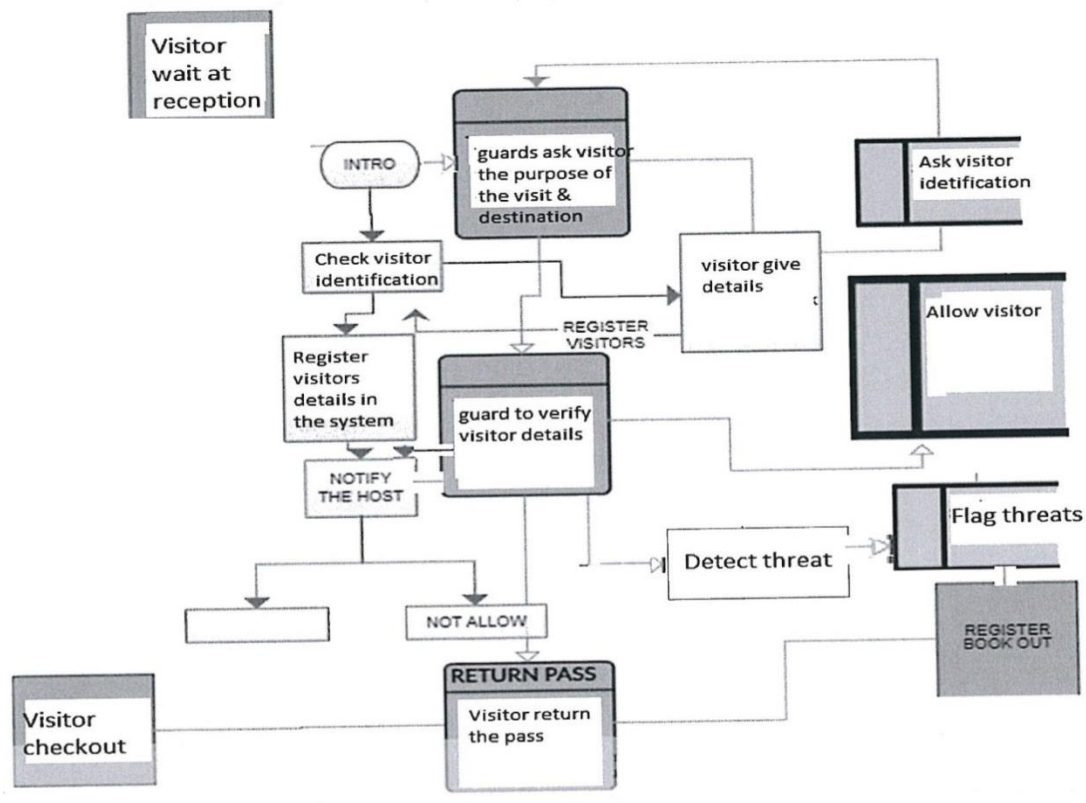


Figure 8: Context Diagram

4.6 System Scope

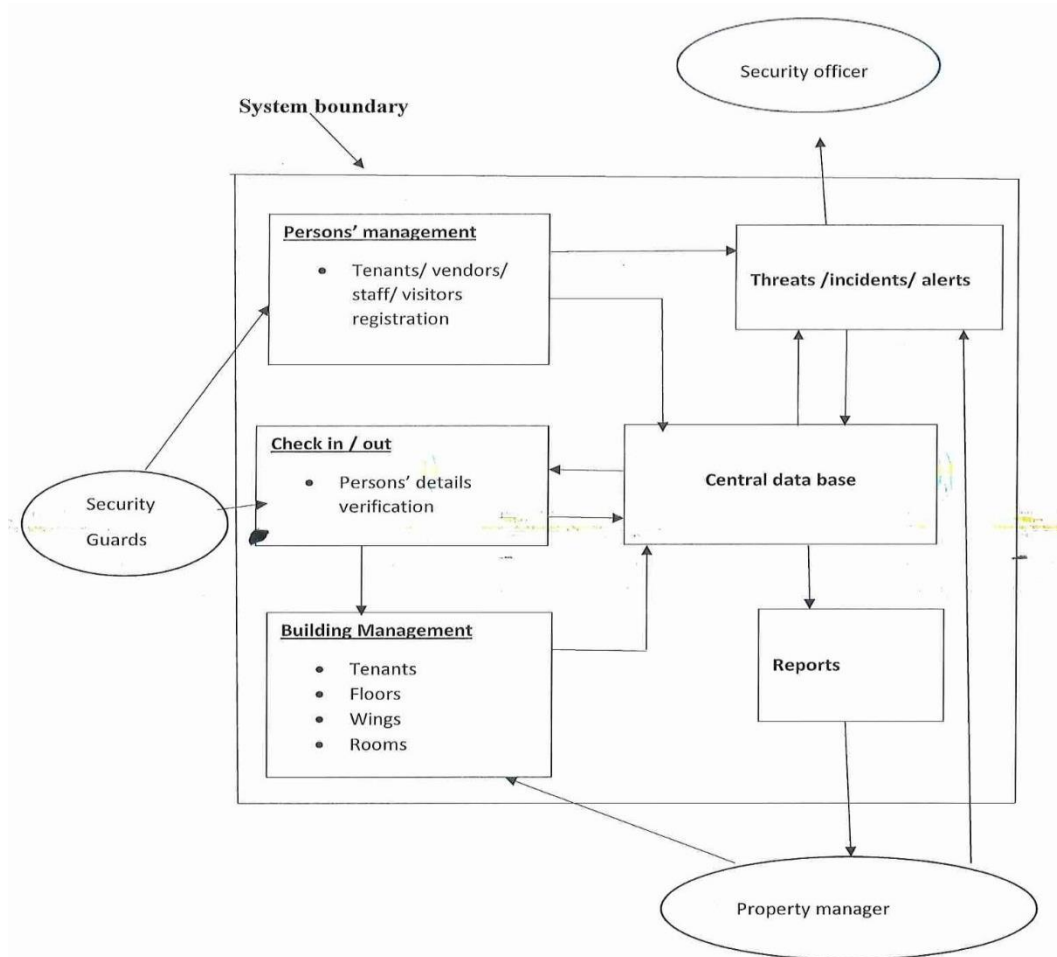


Figure9: System Scope

The System Scope shown in Figure 6 above illustrates the extent of the system's functionality. The functionality includes: - visitor, staff/tenant, and vendor registration; buildings and tenant management; check-in and check-out and threat reporting. Visitors, staff and vendors getting into the buildings are registered and the details stored in the central data base. They are then checked into the buildings, floors and rooms. Any threats identified are recorded for security attention. Visitors are then checked out once they are cleared by their host.

CHAPTER FIVE

SYSTEM DEVELOPMENT

5.0 Introduction

This Chapter explains the process used in coding, testing and evaluation of the Real Estate Security Management System. It involved System Construction, Verifying System Construction, preparing a Test Data, Documents Plan and System Evaluation.

5.1 System Design

The system design was converted into a working Real Estate Security Management System that addressed all documented System requirements. At this stage, the Researcher undertook actual creation of the System by dividing the System scope into modules and then produced actual code.

Modules were defined as follows;

- **Registration Module:** This captures visitors' details such as identification type/number, names, telephone number, email address and photo.
- **Check-In and Out Module:** This is for capturing details such as visitors' destination, person to be seen, reason for the visit, approval status as well as check in and checkout time. This would help in identifying who is in the building and for how long and protecting outside threats from gaining access. This is crucial for many reasons such as emergency situations, access control and monitoring to know who is in the building at any given time
- **Manage Buildings Module:** This capture building details such as floors, wings, rooms and occupants in terms of organizations.

- **Report Module:** This generates reports such as visitors in the building at any given time, incidents, and occupants.

5.1.2 The Bottom up Approach

The researcher used the bottom up approach in developing the system. In this approach, the modules were designed individually and then integrated together to form a complete system. Each and every module was built, tested individually (unit testing) prior to integrating them.

The researcher used the following tools to develop the system;

- **Php 7.0:** For server side scripting
- **Apache 3.2.2:** For receiving requests to access web pages and run security checks.
- **MySQL 5.7:** For database modelling
- **Text editor** (sublime text): Source code editing with application programming language (API)

5.2 Architectural Design

Architectural design is a formal representation of the structure, behaviour and other views of a system.

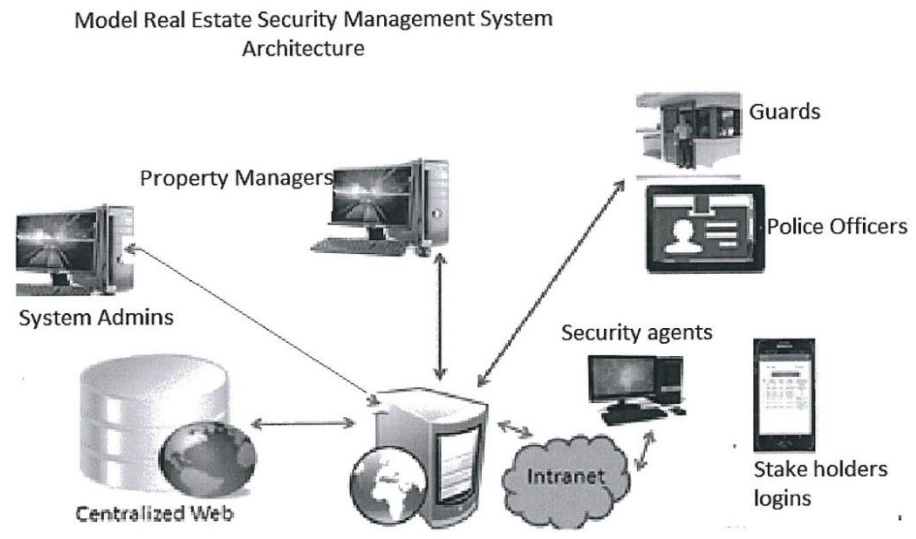


Figure 10: System Architectural Design

5.3 Sample Screen Shots

The following sample screen shots present the system modules

5.4 Login Details

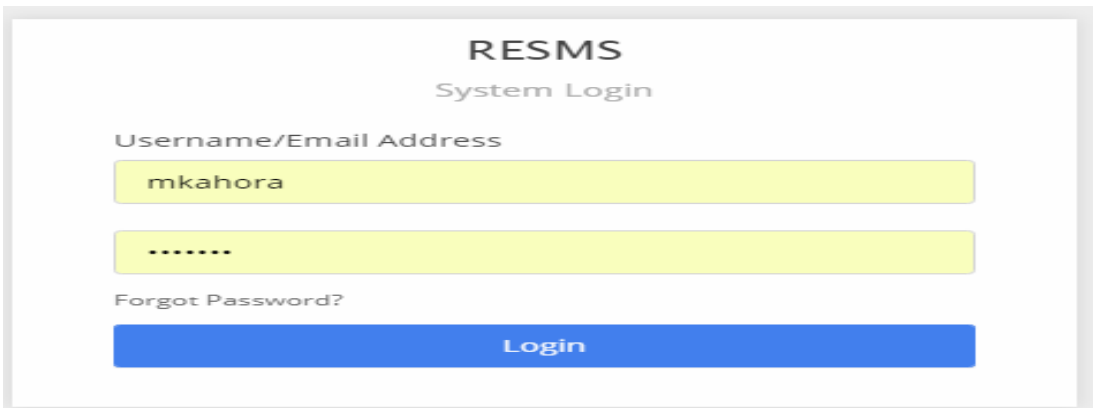


Figure 11: Login Dialog Box

The figure above is the first System Page that is displayed when one attempts to connect to the Real Estate Security Management System model. It contains the following: -

1. **Username and Password:** These ensure security of the System by allowing access to only the authorized users.

5.4.1 Register a Person

Figure 12: Register Dialog Box

Figure 10 above, facilitates in registering visitors' details to control access. This page allows capture of peoples' names, photo, identification card number, phone, and status. Registration of people entering into the building ensures security and accountability.

5.4.2 Check In

Figure 13: Check in Dialog Box

The above dialog box allows verification and recording of various critical pieces of information upon peoples' registration.

5.4.3 Check Out

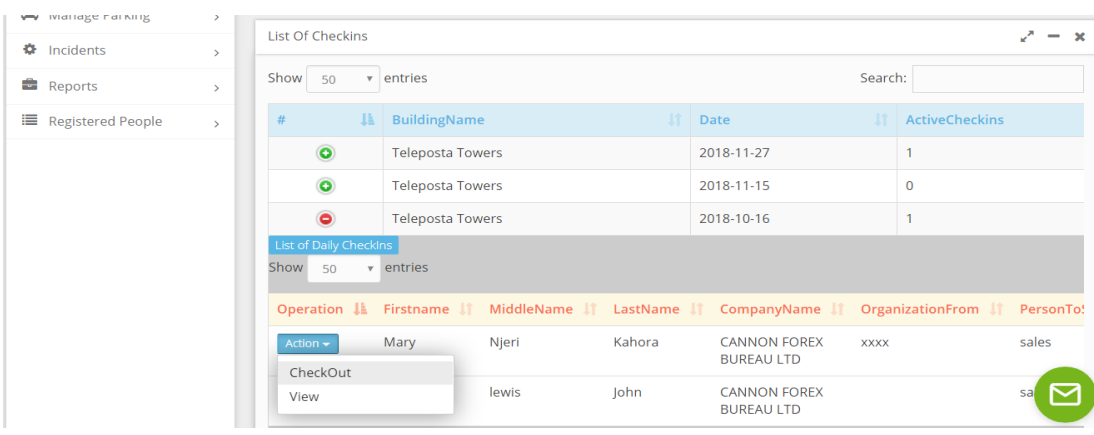


Figure 14: Checkout Dialog Box

Figure 12 above, allows signing off the visitors from the building. Just as all people undergo checked-in procedures, they should also go through check-out procedures before leaving the building.

5.4.4 Incident Reporting

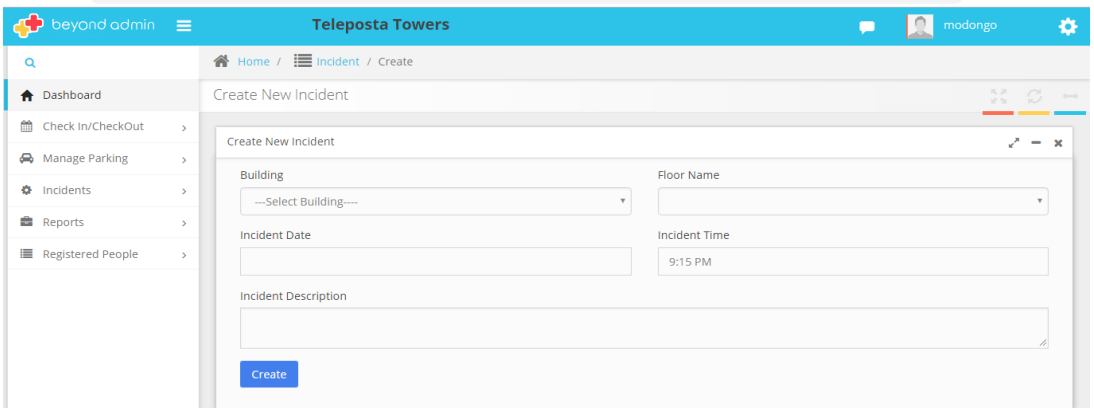


Figure 15: Incident Report Dialog Box

Figure 13 shown above, allows incidents' reporting platform where all incidents occurring in any building are reported. This allows proper analysis of events and implementing actions that would prevent repeat incidents.

5.4.5 Flag A Suspicious Person at Teleposta Towers

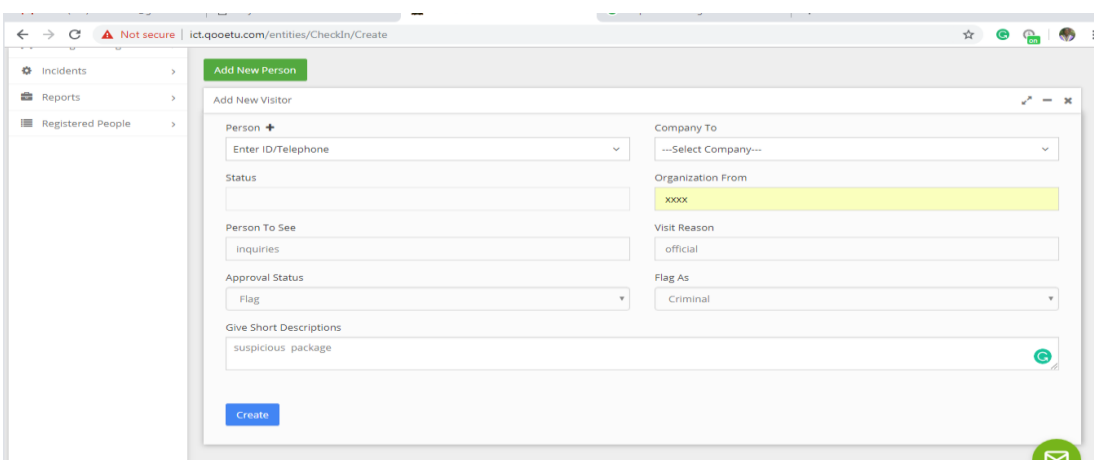


Figure 16: Flag Suspicious Person Dialog

The above figure shows the process of flagging a person upon detecting any threat.

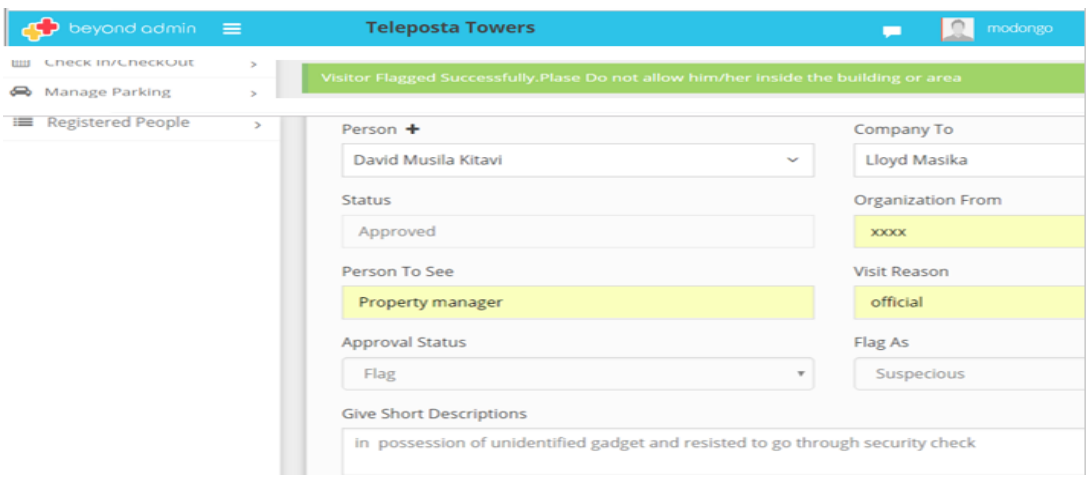


Figure 17: Visitors Flagged Dialog Box

Figure 15 shown above, shows that a person has been flagged successfully at Teleposta Towers Building. This helps in threat prevention by disallowing the person from entering the building.

Note: If a person is flagged in one building, he or she would be detected when trying to check-in in another building.

5.4.6 Threat Detection at UngaHouse



Figure 18: Threat Detection Dialog Box

The figure above shows how the system automatically detect threat by pulling details of suspects, wanted, criminals etc. from the central data base.

Note: The person was flagged at Teleposta Towers and detected at unga house.

5.4.7 Reporting Incidents

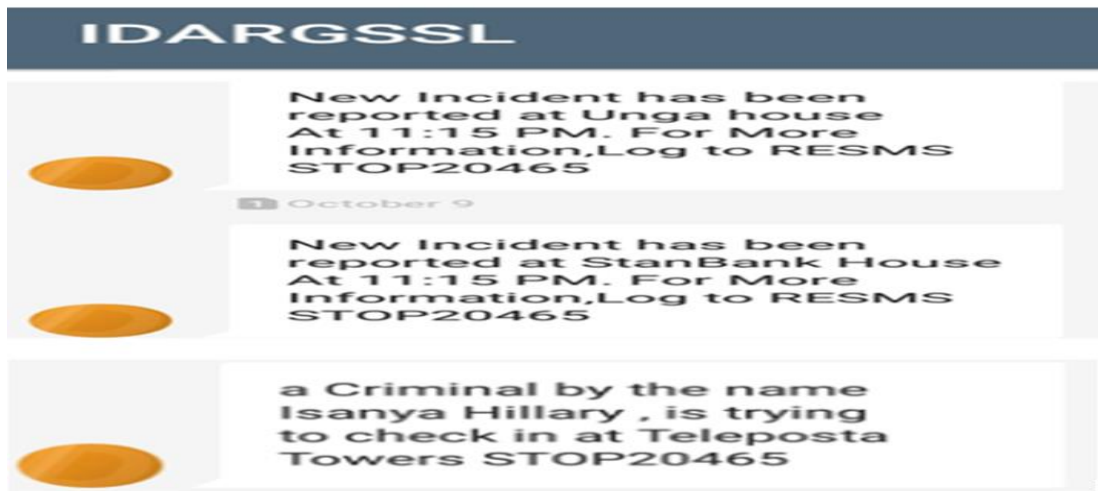


Figure 19: Reporting Incidents Dialog Box

Figure 17 shown above shows how the system automatically sends notifications to the relevant personnel via mobile phones' sms. This enhances prompt reporting and action.

5.5 Sample Code

- **Send sms and get wanted person code**

The following is a sample code sending sms and get wanted persons.

Other codes are found in appendix 8

Send Sms and Get Wanted Person code

```

public static function sends SMS ($phone, $message2)
{

$key="bNtzIr3j0nw7abhS4fPhPD4RoZspFjERpYsZI2uQrpuSfDHFJxfbnN9QzeDFR93Y";
    $phone=$phone;

    $post = [
        'key' => $key,
        'numbers' => $phone,
        'text' => $message2,
        'sender_id' => 'IDARGSSL'
    ];

    $ch = curl_init('http://bulksms.orbit.co.ke/api/message/bulk/send');
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
    $response = curl_exec($ch);
    curl_close($ch);
    $return_message=json_decode($response);
    return $return_message;

return true;
}

public static function getWantedPerson($number)
{

    $post = [
        'id_number' => $number,
    ];

    $url1="http://connected.goetu.com/Api/getPerson";
    $ch = curl_init($url1);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
    $response = curl_exec($ch);
    curl_close($ch);
    $return_message=json_decode($response);
}

```

```

return $return_message;

}

```

5.6 General Test Data and System Document

These tasks involved developing Test Data and verifying the System functionality. All the modules were tested to ensure that they corresponded to functional requirements. The test started with Registration Module, then Check-In / Check-Out Module, and finally Report Generating Module. Any problem with the modules was diagnosed to ensure they all meet their respective usability features. This was done taking into consideration the Requirements Specification and Conceptual Design. A User Manual explaining how the System is to be operated by the Users and Administrators was also produced.

Below is a sample of Unit Testing the Researcher carried out on a few of the interfaces developed by the Study. It outlines Test Procedure, Test Data, Results Expected and the Actual Results Obtained.

User login

Table 4: Result Table for Login Test Data

Test No	Test procedure	Test data	Expected results	Actual results
1.	User login and password	Password and username omitted	Reject	Rejected
2.	User name and password	Correct username and password	Accept	Accepted

Table 5: Result Table for Register Test Data

Test No	Test procedure	Test data	Expected results	Actual results
1.	Integer for telephone number	Ffyhtk78900	Reject	Rejected
2.	Insert mandatory fields	Some fields omitted	Reject	Rejected

5.7 Result Table for Check in Visitors**Table 6: Result Table for Check-In Test Data**

Test No	Test procedure	Test data	Expected results	Actual results
1.	Pick unregistered user	Valentine	Reject	Rejected
2.	Automatically enter the current date/time	13 th /06/2016	Accept	Accepted

CHAPTER SIX

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

6.0 Introduction

This Chapter presents Discussions, Conclusions, and Recommendations based on the analyzed results. The overall objective of this Study was to analyze current security systems in commercial buildings in Nairobi County with a view to develop an integrated web-based Real Estate Security Management System. This was achieved by first analyzing the current systems in the buildings to gather system requirements. The Researcher later developed integrated web-based Model Real Estate Management System.

6.1 Summary of the Study Findings

The main findings of the study, based on the objectives are as follows;

1. Security procedures used within the buildings.

It was established that most security procedures consisted of manual registers where every visitor's details such as official names, Identification number, date, time and destination are recorded manually in a log book. The log book is exposed to alterations and misplacement as it is presented from the findings section 4.1.2, table 2. This also demonstrated that the procedures take a lot of time since they are done manually. and there was no ICT based system to facilitate in registering people. This was solved by developing an integrated web-based Real Estate Security Management System.

2. weaknesses and challenges associated with the current security system in the buildings

In line with this objective, the users experience weaknesses and challenges associated with current security as follows: Difficult in retrieving data since it is stored manually, registers exposed to regular misplacements besides not being confidential., lot of time taken to register visitors and to check in and out, since the visitors are registered every time they visit the building, Information not accessible remotely, Stake holders and agents are not able to access information in real time and from any location and at any time, difficult in tracking visitors, not able to identify and track visitors, lack of a platform that would allow collaboration and sharing of information with Property Managers, Security Officers and other relevant parties as discussed in section 4.1.2, table 3.

3. Requirements for a security management system

In line with objective 3, the study sought to establish requirements that would go to designing the proposed security management system. The requirements were gathered and analyzed to determine what and how the system would function as far as the users were concerned. The requirements provided a basis of design in terms of what the users expected from the system given the current scenario as discussed in section 4.2, section 4.3 and section 4.4 respectfully.

4. Improved Model Real Estate Security Management System for commercial buildings

The System was successfully developed using bottom up approach, where each and every module was built, tested individually (unit testing) prior to integrating them. The system was able to link the five buildings together by having several modules so that each building has a subsystem to manage. The modules are then linked to the core system and each building can access the system through the web.

The system has addressed most of the requirements as proposed by the users. The system has been able to address areas such as; Collaborating and sharing of information, tracking visitors and notifications, positively identify visitors, flagging and reporting threats, reporting incidents, and retrieving information faster.

6.2 Conclusion

The study examined the current security systems procedures, challenges and weaknesses in five commercial buildings with a view to developing a model real estate security system. Analysis of the security management and procedures was done, based on the objectives.

From the findings, it was established that the process of registering, tracking, checking visitors is manual. Registering of visitors is majorly manual where visitors are registered in a log book. Tracking of visitors from one building to the other is also manual and searching and retrieving information is also manual.

The findings revealed some limitations with the current systems and based on the user requirements, there was need for digitized security systems. A web based system was

developed in line with objective four – that is to develop an improved web based model real estate security management system for commercial buildings.

6.3 Recommendations

The findings as presented in the analysis in table 2 & 3 in section 4.1.1 and 4.1.2 showed that the current system lack collaborative security management feature for managing security. The developed system is integrated but to realize the full benefits that comes with integrated systems it could be integrated with optical character reader devices and software to ensure maximum efficiency and effectiveness also be integrated with the CCTV camera footage or images to synchronize visitor's identification details with the visitors' images. This would ensure that if a visitor is searched, his/her details should reflect in the footage/images and vice versa.

6.4 Suggestions for Further Study

1. Continuous study and implementation should be carried out as new security threats keep on emerging.
2. The new digital identity card platform can be studied to find out the possibilities of integrating the digital identity cards with the Real Estate Security System. The integration would enhance security as the card will provide details of the visitor once presented to allow access into any building. The System will retrieve the history of the visitor and help verify his/her identity. It would also identify criminals from the digital cards database.

REFERENCES

- Abend, & G. (2018). *Meaning of theory* (5th ed., Vol. 3). William K. *Theory Building in Applied Disciplines*. <https://doi.org/10.1016/S0005-7894>
- Alvis. (Ed.). (2017, May 11). *M-secure as a security solution*. Retrieved June 10, 2018, from <https://kenyayote.com/m-secure-website-secure-mpesa-shop-business-register-msecure/pdf>
- A., Onwuegbuzie, & N, L. (2017). *Sampling design in qualitative research* (1st ed., pp. 35-40). Colorado: University of Colorado. Retrieved from <http://www.citeseerx.ist.psu.edu/viewdoc/download>
- Bacon, T. (2013). *Impact of crime in high-rise buildings*. Retrieved 24 March 2016, from <https://www.welivehere.net/media-coverage/121-owners-corporation-law>
- Brindley, & Blaschke, (2009). *Creating Effective Collaborative platforms in an online Environment*. *International Review of Research in open Distance Learning*, 10(3) Retrieved June 27, 2018 from <http://www.uh.cu/static/documents/AL/Creating%20Effective%20Collaborative%20L>.
- Building security management. (2017) (1st ed. p. 1). Colorado. Retrieved from <http://www.navigantresearch.com/research/commercial-buildings-automation-systems>
- Challinger, D. (2010). *Security in tall buildings* (1st Ed.). Asis Foundation Research Council. Retrieved from <http://www.asisonline.org>
- Clarke. (2013). *Factors that contribute to security threats in commercial buildings*. Retrieved June 10, 2015, from www.cowellclarke.com.au
- Cisco IT case Study-Enterprise access Control*. (2011). *Corporate security Technology & systems*. Retrieved 11 June 2014, from <http://www.cisco/web/about/ciscoitwork/downloads/ciscoitwork.pdf>
- Commercial building automation systems. (2013). *Intelligent management building*. Retrieved 15 March 2015, from <https://www.navigantresearch.com/research/building-innovations/intelligent-building-management-systems>
- Cooper, D. (2015). Research Methods. *Journal of Business & Economic Research*, 5(3).
- CR, Kothari (2009). Research methodology. *Methods and Techniques*, 2(2), 2-10. Retrieved from <http://www.modares.ac.ir/uploads/Agr.Oth.Lib.17.pdf>

- David. & Erick.(2015). *Security procedures- Teleposta Towers*. Accessed on August 10, 2016, from LloydMasika Ltd, Management department: Unpublished document.
- Ekman.(2015, May). *Facial detection*. Retrieved. March 19, 2018, from <https://www.paulekman.com/tag/facial-recognition-technology-2/>
- Electric, Schneider.(2013). *Future of commercial building security* (1st ed., pp. 2-11).TAC. Retrieved from http://www.schneiderlectric.lv/documents/buildings/office_building_security.pdf
- Ephraim Fred. (2015). *A metrics tool set for communication* (4th ed., pp. 6).
- Fang.(2015). *Cybercrime technologies*. Retrieved July 2, 2017, from <https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime>
- Homeland security and emergency management.(2012). *Commercial Buildings' Vulnerabilities in the United States*. Retrieved November 17, 2016, from <https://www.arrowpreparedness.com>
- Heseltine.(2016). *Facial recognition*. Retrieved April 11, 2018, from https://www.researchgate.net/publication/266049847_Three-Dimensional_Face_Recognition_Using_Surface_Space_Combinations
- Hounsel.(2015). *Optical reader recognition*. Retrieved March 6, 2018, from <https://searchcontentmanagement.techtarget.com/definition/OCR-optical-character-recognition>
- Ibrahim. (2013). *Kenya national security ranked among the worst in the world*. Nairobi: Ibrahim. Retrieved June 12, 2015, from <https://www.nation.co.ke/news/Kenya-security-ranked-among-the-worst-in-Africa>.
- Intelligent building Institute. (2010). *The concept of buildings' technologies*. https://web.itu.edu.tr/~onaygil/eht614e/IB_Definition.pdf.
- Jacob. (2012). *Cisco IT Control access building over the Enterprise WAN centrally managed IP-based building*. Retrieved January 17, 2014, from http://www.cisco.com/web/about/ciscoitwork/downloads/ciscoitwork/pdf/Cisco_IT_Case_Study_Enterprise-Access_Control.pdf
- Kastner.(n.d.).*Building automation systems*. Retrieved November 11, 2017, from https://www.researchgate.net/publication/284131458_Building_Automation_Systems_Concepts_and_Technology_Review
- Kitteringham. (2016). *Building location as security threats* (1st ed., Vol. 2). Retrieved March 12, 2017, from www.researchgate.net/publication.

- Krisandra, G. (2010). Anti-terrorism measures in commercial buildings. *Appraisal Journal*, Volume: 75(4). Retrieved from <http://www.freepatentsonline.com/article/Appraisal-Journal/171851339.html>
- Kumar, A. (2013). *Qualitative research process*. *International Journal*, 2(1), 16-18. Retrieved from <http://www.journals.cluteonline.com/index.php/jber/article/viewfile/2532/2578>
- Labaree (2013). Types of Research Design. 5th ed. U.K: Introduction to research design. Retrieved 21 June 2008, from <http://www.libguides.usc.edu/writingguide/qualitative>
- Lincoln, D. (2007). *Data collectors field guide* (1st Ed.). Retrieved from <http://www.personal.psu/wx139/quality.thm>
- Lisa, B. (2016). *System hacking*. Retrieved. May 5, 2018, from <https://www.industry-era.com/SecuringtheInternetofThings10044.php>
- Lynn, B. (2013). *Towers on surveillance security systems with embedded DVRs*. Retrieved September 6, 2015, from <http://fr.surveillance.aver.com/case-study/AVer-provides-a-safe-working-environment-with-a-solid-security-system-to-Rahimtulla-Tower>
- Mensik.(2016). Technics for robust security. *Thermal Infrared Technology*, 2(1), 6–12. <https://doi.org/10.5772/18986>
- National Bureau Statistics.(2010). *Growth in real estate*. Retrieved July/August, 2015, from www.knbs.or.ke/download/economic-survey
- National Security Council.(2015). *safety security in high-rise buildings*. Retrieved 21 August 2015, from <http://www.asisonline.org/council/documents>
- Navigant Consultant. (2013). *Commercial Buildings Security Measures*. Retrieved October 19, 2015, from <https://www.navigant.com/>
- Ongiri, I. (2013). *Kenya national security*. *Daily Nation*, p. 1. Retrieved from <http://www.nation.co.ke/news/Kenya-security-among-Africa-s-worst/1056-2032444-mjf9t3/index.html>
- Ploch. (2014). *Kenya experiences several attacks*. Retrieved 2nd March 2015, from <http://www.ke.undp.org/content/dam/kenya/docs>
- Reynald, D. (2013). *Crime prevention in high-rise building* (1st Ed.). USA. Retrieved from <http://www.popcenter.org/library/crisps/security-tall-buildings.pdf>

- Roche, T. (2013). *Case study- speed gates at Microsoft site. Speed gates*. Retrieved 17 January 2014, from <http://www.microsoft.co./casestudies>
- Security Council.(2016). *high-rise building safety procedures*. Retrieved 9 January 2016, from <http://www.asisonline.org/councils/documents>
- Security for business.Access control. Retrieved 13 April 2015, from <http://www.American alarm.com/business security/access control system>
- Shankardass, s. (2013). *Security prevention* (1st ed., pp. 1-4). Nairobi: UN Habitat. Retrieved from http://www.preventionweb.net/files/1700_462551419GC202120.pdf
- Surveillance cameras.Surveillance.aver.com. Retrieved 26 April 2010, from <http://www.surveillance.aver.com/case-study-Tower>
- Security Procedures Systems. Nairobi: Lloyd Masika Limited, 2017. Print. *A Documentation of Security Procedures*.
- Sugden. (Ed.). (2014, August 31). *Nairobi Buildings exposed to security threats*. Business Daily. Retrieved November 10, 2015, from <http://www.businessdailyafrica.com/corporate/Nairobi-buildings-exposed-to-security-threats--says-survey-1>
- Understanding Research Methodology. (2013). Eldoret: Utafiti Foundation.
- Welman,&Kluger. (2013). *Case study in research methodology* (3rd ed.). Retrieved October 19, 2015, from www.welman-research-methodology.com
- Williams, J., & Booth, C. (2017). *The Craft of Research* (4th ed., Vol. 1). John Crewel.
- Yuen. (2016). *Building occupants' characteristics*. Retrieved 26 September 2017, from Www.thirdway.org/talking-points/talking-points-for-the-top-national-security (1st ed., Vol. 1, Ser. 2).

APPENDICES

Appendix 1: Photos of the Existing Security Systems/Technologies

The photos were taken during field survey on January 2015.

Security systems incorporated include CCTV cameras with centralized control and monitoring screens, while access control systems include bar code reader cards, finger prints readers, biometric or gate barriers.

Figures 1, 2, 3, 4 illustrate CCTV cameras that are used while figures 5,6,7,8 illustrate access control systems.



Fig 1 Dome CCTV Camera



Fig 2 Bullet CCTV Camera



Fig 3: Analogue CCTV

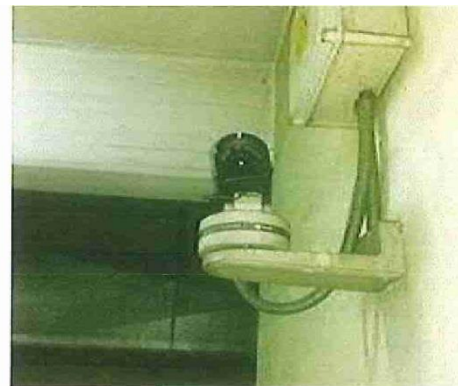


Fig 4: Infrared CCTV camera



Fig 5: Card reader



Fig 6: Access control System



Fig 7: Automated gate barrier



Fig 8: Automated gate sensor



Fig 9: card reader

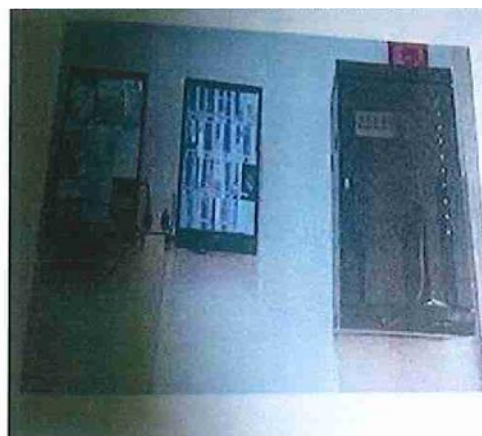


Fig 10: Access control system.

Appendix 2: Interview Guide for Security Guards

Dear Sir/Madam,

My name is MARY NJERI KAHORA, a student pursuing Master of Science in Information Technology in the Department of Information Technology at Moi University. My Registration number is IS/MPHILIT/057/12. I am carrying out a research in partial fulfillment of the requirement for the program. Part of the research requires gathering information from select personnel through interviews. Your assistance in answering the interview questions will be highly appreciated. All information provided will be treated with utmost confidentiality and will be used strictly for academic purpose.

PART A: BUILDING DETAILS

a) Name of the building _____

b) Location of the Building _____

PART B: SECURITY PROCEDURES**Respondent: Security Guard**

a) What type of security systems in place for managing security?

b) How security checks for visitors are carried out?

c) What are the systems that cater for regular visitors?

Appendix 3: Interview for the Security Officers

PART A: BUILDING DETAILS

a) Name of the building _____

b) Location of the Building _____

PART B: SHORT COMINGS OF THE CURRENT SYSTEM

NB: The interview is going to take approximately 40 minutes

- a) What challenges do you experience with the existing security systems?
- b) How would acquisition of a security management system dress the shortcomings?
- c) What kind of desirable features or functionalities that are missing in the current system?
- d) What has been the level of demand for adoption of Information Technology in in your opinion, what are the major challenges to adoption of Information Technology in managing security procedures?

Appendix 4: Interview for Property Manager

PART A: BUILDING DETAILS

- a) Name of the building _____
- b) Location of the Building _____

PART B: EFFECTIVENESS AND RELIABILITY OF THE CURRENT SYSTEMS

NB: The interview is going to take approximately 40 minutes

- a) How does the existing security system allow for remote and centralized control and monitoring of the security procedures?
- b) How would you describe the current state of security management procedures?
- c) How would you rate the effectiveness of the current system?
- d) How would implementation of online security system improve security in commercial buildings?
- e) What role do you think an online security system would play in enhancing security?
- f) How is the current security system linked to another building or to any security offices?
- g) What suggestions would you make for successful implementation of an online security portal?
- h) What are the weaknesses and challenges associated with the current system?
- i) How would you rate the degree of reliability of the existing security system?
- j) What type of training you and other staff require?

PART A: BUILDING DETAILS

- a) Name of the building _____

- b) Location of the Building _____

PART B: KIND OF ICT SYSTEMS/TECHNOLOGIES CURENTLY IN PLACE

Instructions: Please tick (√) as appropriate. Where there are no choices, kindly fill in the blank spaces provided.

- a) What kind of ICT security systems or Technologies are in use currently? (*tick as appropriate*)

- b) What is the success level of these technologies in meeting the objectives of the system?

- c) What modification do you think would make the system more effective?

- d) How would an alternative technology or system be more appropriate?

Appendix 5: Interview for Administrative Police

PART A: BUILDING DETAILS

- a) Name of the building

- b) Location of the Building

PART B: CRIMES EXPERINCED IN THE BUILDING AND REPORTING PROCEDURES

NB: The interview is going to take approximately 40 minutes

- a) What types of crimes are mostly experienced in commercial buildings?
- b) What crimes are reported to the authority
- c) How are these crimes reported?
- d) How are these crimes replicated in other buildings?
- e) How the security management ICT systems are integrated with police systems?
- f) How would integrating the online security portal with police systems enhance security?
- g) What is the trend in insecurity in commercial building in Nairobi currently?
- h) What are the challenges experienced when investigating a certain crime committed in a commercial building?

Appendix 6: Observation Check List

This entailed a list of things that the observer is going to look at alongside the interview.

The researcher is going to observe the following;

- a) Security devices and software in place.
- b) Approximate number of visitors received in one particular time.
- c) visitor check-in queues on a normal day
- d) Average time taken to check-in/clear a visitor?
- e) Integration level

Appendix 7: User Manual

System overview

The proposed real estate security management system is an online security system that helps real estate agents to capture visitors' details, record any incidence, detect threats, prevent threats and report threats in real time. The system integrates five commercial buildings within Nairobi County, hence allowing sharing of information and collaboration.

User manual organization

The user manual consists of system overview, system configurations, system users, system users access levels, and getting started.

System Configurations

The proposed real estate security management system operates on devices such as computers, mobile phones, iPad with operating systems such as windows, Android and IOS (iPhone operating system). The system requires connection to the internet in order to save and share data from the central database. It is accessible through any web browser.

System users

- i. The system has the following users;
- ii. System admin
- iii. Property manager
- iv. Security guard

Users access levels

System admin:

The system admin can perform the following;

- Add, edit and delete users
- Add, edit and delete a building, floor, wing, and company
- View and print reports

Property manager

The property manager can perform the following;

- Add, edit, delete floor, wing, and company
- Register, check in, check out visitors, record incidences
- view and print report

The security guard

The security guard can only perform the following;

- Register, check in, check out visitors
- Record incidences
- View and print reports.

Note: The users can only login to the building assigned.

User accounts login credentials

System admin

- User name: mkahora
- Password: 123qwe

Property manager

Teleposta Towers

- User name: joel
- Password: joel@18

Unga House

- User name: Richard
- Password: Richard@18

Stanchart House

- User name: Kimoite
- Password: kimoite@18

1. Hazina Towers

- User name: Kenneth
- Password: kenneth@18

2. View park Towers

- User name: Sarah
- Password: sarah@18

Security officers

1. Teleposta Towers

- User name: joel
- Password: joel@18

2. Unga House

- User name: Richard
- Password: Richard@18

3. Stanchart House

- User name: Kimoite
- Password: kimoite@18

4. Hazina Towers

- User name: Kenneth
- Password: kenneth@18

5. View park Towers

- User name: Sarah
- Password: sarah@18

Getting started

This section explains how to connect to the system and how to perform specific tasks.

Connect to the system

To access the system, use any web browser

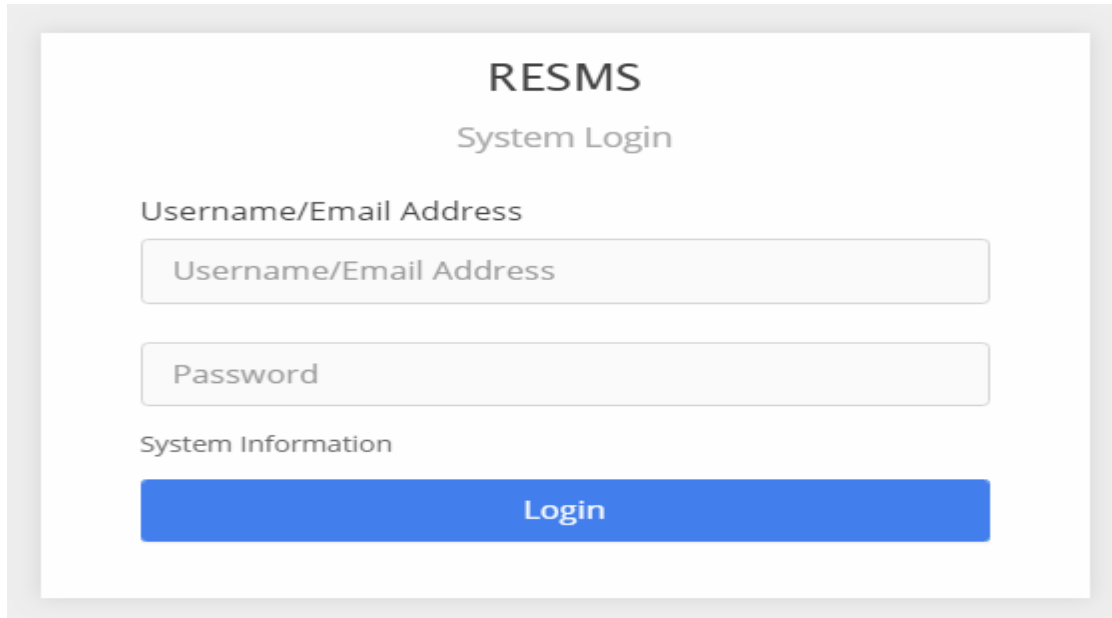
Type the following URL: [http://www. Real estate security/](http://www.Real estate security/)

login page opens once you open the link.

1.0 Login

Login dialog box shown below would allow you to login into the system using the credentials provided.

Note: If you are logging in for the first time, you will be prompted to change the password.



The image shows a login dialog box for the RESMS system. It has a white background with a light gray border. At the top, the text "RESMS" is centered in a bold, black font, with "System Login" centered below it in a smaller, regular black font. There are two input fields: the first is labeled "Username/Email Address" and contains the placeholder text "Username/Email Address"; the second is labeled "Password" and contains the placeholder text "Password". Below the input fields, the text "System Information" is centered. At the bottom, there is a prominent blue button with the white text "Login".

Change password login dialog .

If you are login for the first time, you will be prompted to change the password as shown below. Please change the password and continue.

USER PASSWORD RESET

You Are Required To Change Your account Password before start using this portal. Kindly reset to a more secure and memorable password.

Email Address
jacob@ymail.com

Account Username
2267190

Old Password

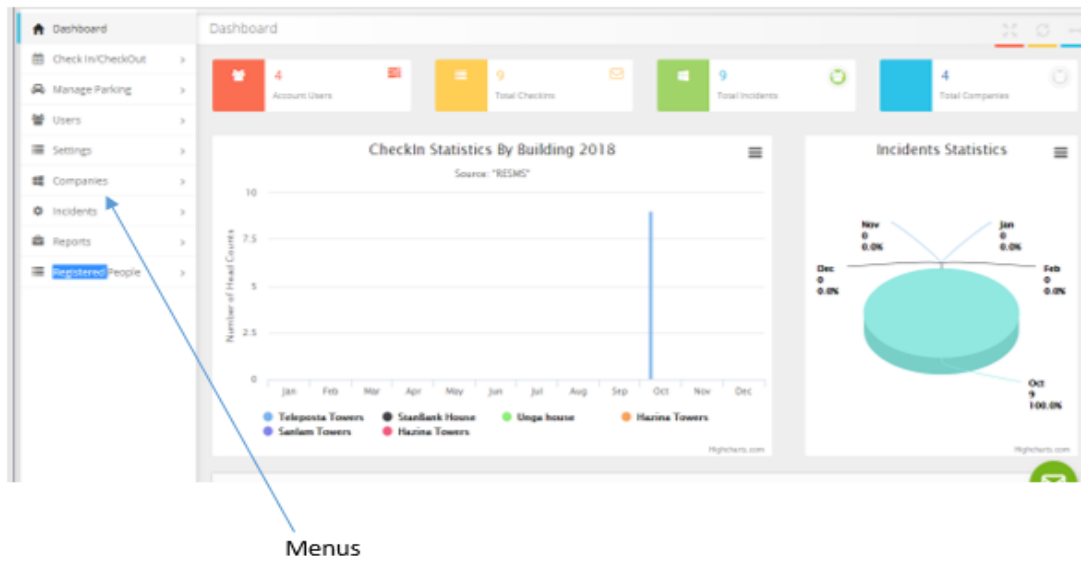
New Password

Confirm Password

Rest Password

Dash board

This is the first page that appears first, after login to the system. It is the interface that presents information in a simple way to help the user visualize the information at a glance by the help of graphs and charts. The dash board below displays the main functions and current status of the building in terms accounts users, check-in, incidents, companies and main menu that are used to perform specific tasks.



1.1 Add, edit and delete user accounts

Login as a system admin, click add new user under users at the left side of the main panel /dash board and fill in the details form the add new user fields and click create as shown below;

The 'Add New User' form contains the following fields and controls:

- Name: Text input field
- Building: Dropdown menu with '---Select Building Name---
- Identification: Dropdown menu with '---Select Identification---
- Mobile Number: Text input field
- Password: Text input field
- Department: Dropdown menu with '---Select Department---
- Email: Text input field
- Identification Number: Text input field
- Access Level: Dropdown menu with '---Select User Role---
- Confirm Password: Text input field
- Create: Blue button
- Green envelope icon: Located at the bottom right of the form.

Edit and delete users

Still under users, click on user accounts, a dialog box with a list of users opens as below;

Name	Username	Mobile	Email	Access Level	Department	Action
Jacob	jacob@ymail.com	+254705843672	jacob@ymail.com	Property Manager	Operation	[Edit] [Delete]
Irine	2727896	+254712524521	inaisenya@gmail.com	Security Officers	Operation	[Edit] [Delete]
Joel	joel		joel@tps.com	Property Manager	Operation	[Edit] [Delete]
John Kitavi	14978456	+2547846732	kitavi@yahoo.com	Security Officers	Operation	[Edit] [Delete]
Michael Odongo	modongo	+25474245689	modongo@gmail.com	Security Officers	Operation	[Edit] [Delete]

Showing 1 to 5 of 5 entries

Previous 1

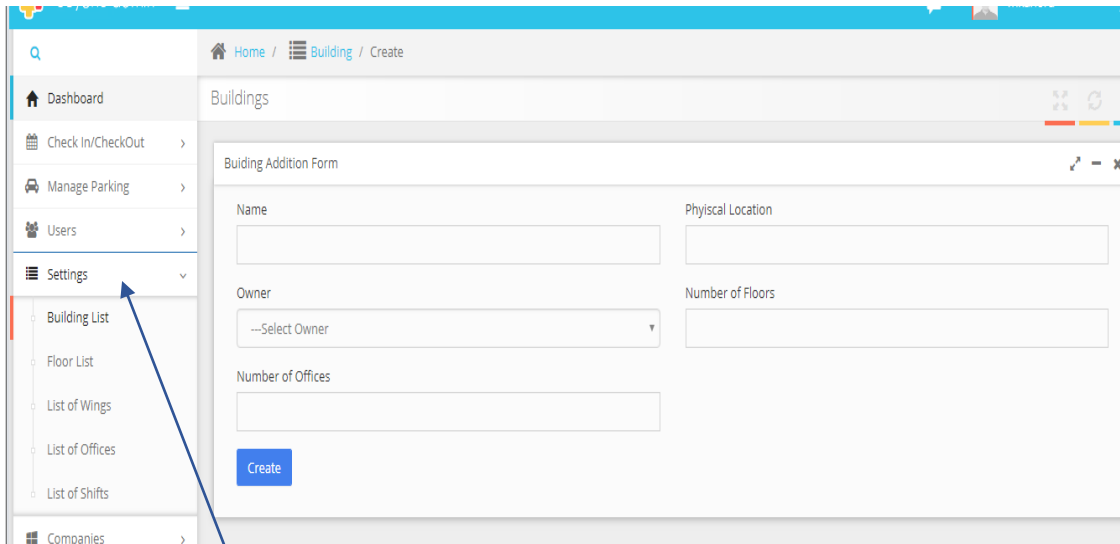
Edit Delete

- To edit, click on edit icon next to the user account that is to be edited, at the right hand side, an editable dialog box opens, edit and click submit changes for the changes to take effect.
- To delete click on delete icon next to the user account that is to be deleted, at the right hand side. You will be prompted to confirm the user and click 'OK'.

1.2 Add a building

Login as a system admin,

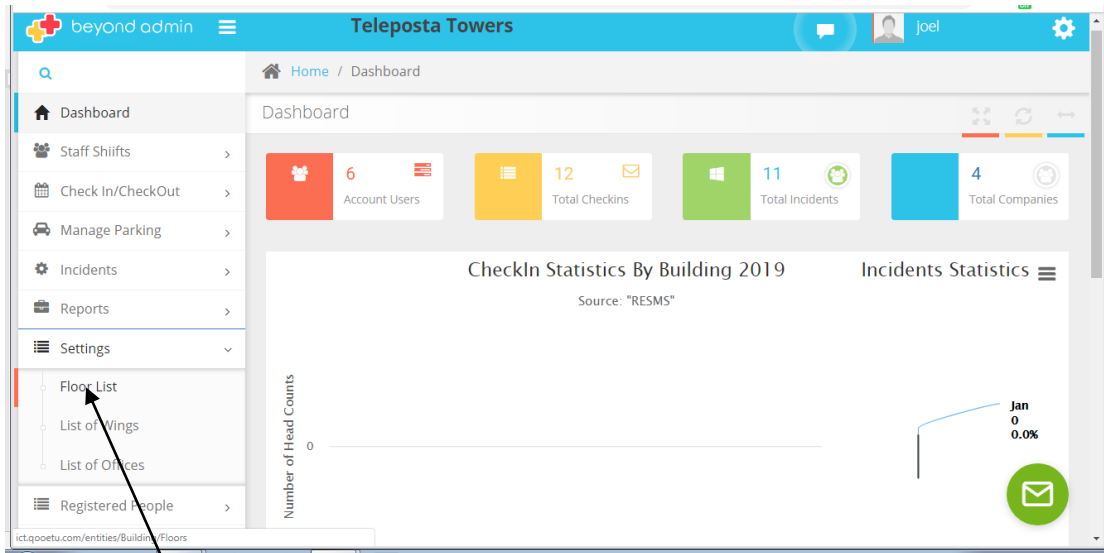
Note: A building has to be added first before adding floor, wing, company, shift and visitors.



- Click “**SETTING +**” at the left pane (main function pane- dash board) to expand the menu.
- Choose “**BUILDINGS list**”
- Click on “**Add new**” at the right
- Fill in the details as required
- Create

1.3 Add floor, wings, offices, companies and shifts

Login as property manager – Teleposta Towers



- Click “**SETTING +**” at the left pane (main function pane- dash board) to expand the menu.
- Choose “**floor list**”
- Click on “**Add new**” at the right
- Fill in the details as required
- Create

Add a wing

- Click “**SETTING +**” at the left pane (main function pane- dash board) to expand the menu.
- Choose “**wing list**”
- Click on “**Add new**” at the right
- Fill in the details as required

- Create

Add offices

- Click “**SETTING +**” at the left pane (main function pane- dash board) to expand the menu.
- Choose “**office list**”
- Click on “**Add new**” at the right
- Fill in the details as required
- Create

Add company

- Click “**SETTING +**” at the left pane (main function pane- dash board) to expand the menu.
- Choose “**company list**”
- Click on “**Add new**” at the right
- Fill in the details as required
- Create

Add shifts

- Click “**SETTING +**” at the left pane (main function pane- dash board) to expand the menu.

- Choose “**shift list**”
- Click on “**Add new**” at the right
- Fill in the details as required
- Create

1.4 Edit/delete floor, wings, offices, companies and shifts

Login as a property manager,

Go to setting, double click on floor list. The following dialog box opens

The screenshot shows the 'beyond admin' interface for 'Teleposta Towers'. The main content area is titled 'Manage Floors' and features a '+ Add New' button. Below this is a 'List Of Floors' dialog box with a search field and a table. The table has columns for 'FloorName', 'FloorTelephone', and 'Action'. The data rows are as follows:

FloorName	FloorTelephone	Action
Basement 3	103	[Edit] [Delete]
Basement 2	102	[Edit] [Delete]
Basement 1	101	[Edit] [Delete]
Mezzanine	100	[Edit] [Delete]
28th	028	[Edit] [Delete]
	026	[Edit] [Delete]

Arrows point from the labels 'Edit' and 'Delete' to the respective icons in the table.

Navigate the field you want to edit or delete and click on edit /delete icon.

1.0 Register, check-in/out, edit and delete visitors

Login as a security guard

1.1 Register visitors

To register a visitor, follow the steps below:

- Click on “**check-in/checkout**” to expand the menu
- Click on “**add new check-in**”
- Click “**Add a new person**”
- Fill in all the details as required
- Click on the “**save**” button

The screenshot shows a web application interface for 'Teleposta Towers'. A modal window titled 'Register a person' is open, displaying a form with the following fields:

- First Name:
- Middle Name:
- Last Name:
- Email Address:
- Mobile:
- Identification Type:
- Identification Number:
- Visitor Avatar: No file chosen

A blue 'Save' button is located at the bottom left of the modal. The background shows a sidebar menu with options like Dashboard, Staff Shifts, Check In/CheckOut, and Registered People.

The figure above shows “**Register a person**” page.

1.2 Check in/out visitors

Note: To check-in a person, that person must be registered first.

- Click on the Check-in/out menu

Check-in

- Click on “**CHECK-IN/OUT**” at the left pane

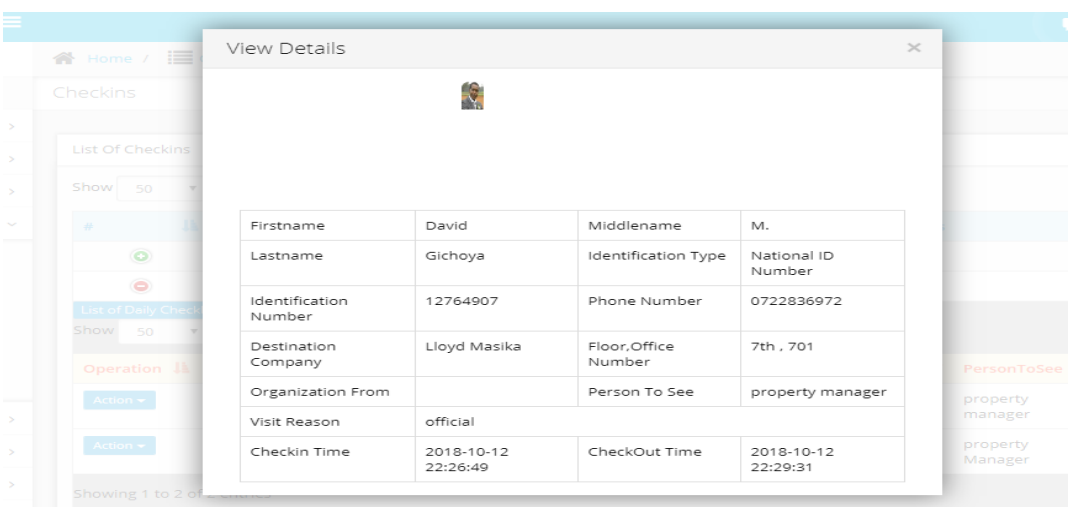
- Click “**Add new check-in**” menu under check-in /out
- Use the form below to populate a persons’ data database.

The screenshot shows a web browser window with the URL `ict.qooetu.com/entities/CheckIn/Create`. The page title is "Teleposta Towers" and the user is logged in as "modongo". The left sidebar contains a navigation menu with items like "Dashboard", "Check In/CheckOut", "Add New CheckIn", "Active CheckIns", "Manage Parking", "Incidents", "Reports", and "Registered People". The main content area is titled "Checkin" and features a green "Add New Person" button. Below this is the "Add New Visitor" form, which includes the following fields:

- Person +**: A dropdown menu with the placeholder text "Enter ID/Telephone".
- Company To**: A dropdown menu with the placeholder text "---Select Company---".
- Status**: A text input field.
- Organization From**: A text input field.
- Person To See**: A text input field.
- Visit Reason**: A text input field.
- Approval Status**: A label at the bottom of the form.

- Enter the person’s name by searching the name, select it
- Search the company to be visited, and select.
- Select status
- Fill in the other required fields e.g. organization from, person to see and reason for visit.
- Add vehicle, luggage’s or any other property if any and click on the save in button.

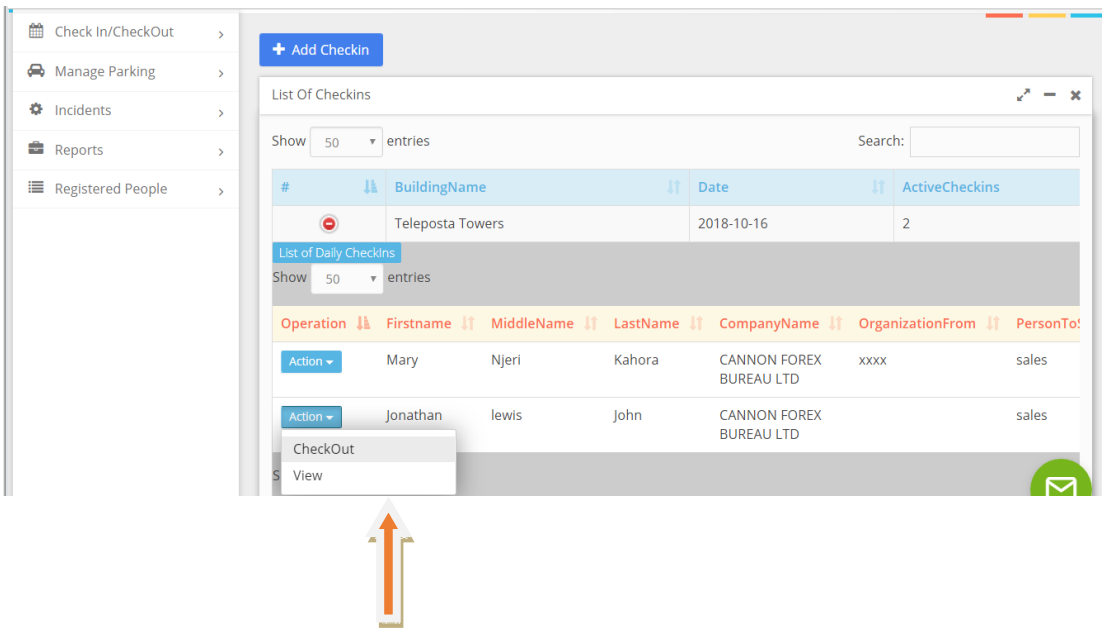
Sample of check in person



1.3 Check out visitors

- Go to “CHECK IN/OUT menu
- Click on active check in

The following pane (for the checked in persons) appears



- Navigate to the person to be checked out.
- At the extreme left, there is a “Action” button

- Click on the action drop down arrow. select **Check-Out**
- You will be prompted to select checkout action i.e. approved or flag then click on complete

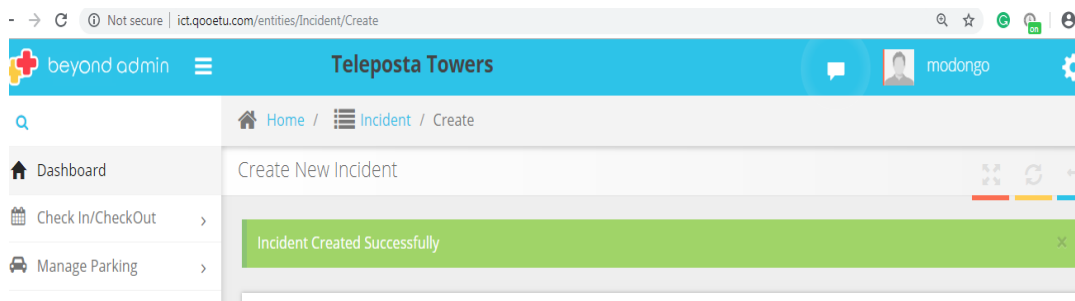
5.0 Record Incident

- Click on the “**INCIDENT**” button at the left pane to expand the menu.
- Click on “**List of incidents**”
- Click on add incidents
- Record incidents
- Click create

The screenshot shows a web application interface for creating a new incident. On the left is a navigation menu with items like Dashboard, Check In/Check Out, Manage Parking, Users, Settings, Companies, Incidents, Reports, and Registered People. The main content area is titled 'Create New Incident' and contains the following form fields:

- Building:** A dropdown menu with the placeholder text "--Select Building--".
- Floor Name:** A dropdown menu.
- Incident Date:** A text input field.
- Incident Time:** A text input field with the value "3:15 PM".
- Incident Description:** A large text area for entering details.
- Create:** A blue button to submit the form.

Upon flagging, the following message appears



5.1 Flagging a person

To flag a person, use the “check in a new person” dialog box as illustrated in number 5 above, under approval status, select flag as shown below

After flagging a person successfully, the following message would appear

5.2 Reports

- To view reports, click on the “**REPORTS**” menu at the left pane to expand the menu and view either incident or visitors’ report.
- You can filter the report by entering the dates
- Click **Generate**
- To print report, click “**Export to Excel**”

👁️ CHECK OUT / IN

📄 INCIDENTS

⚙️ SETTINGS +

📊 REPORTS +

- ↳ Visitors Reports
- ↳ Incidents Reports

Visitors Report

Generate
Export Excel

#	Name	From	Destination	Check Time	Check Out	Lapsed Time
1	Zablon Maina Macharia	Uber Taxis	Kimani Computers	07-Sep-2016 20:29:11	07-Sep-2016 21:32:11	1 hour
1	Simon Kimani Mwaura	Software Technologies Ltd	SPL Enterprises	01-Oct-2016 22:17:04	08-Oct-2016 06:34:55	6 days
1	Jeremiah Mugo Muchatha	jkl	Kimani Computers	08-Oct-2016 05:00:50	08-Oct-2016 05:03:03	2 minutes
1	Hezilon makacha chilonge	Xxxx	citizenship services	08-Oct-2016 05:52:12	10-Oct-2016 01:59:34	1 day
1	Jackie Wanjiru Maribe	Xxxx	citizenship services	08-Oct-2016 05:57:20	12-Oct-2016 06:26:45	4 days
1	Zablon Maina Macharia	Xxxx	citizenship services	08-Oct-2016 06:04:13	19-Nov-2016 13:21:15	1 month
1	Habilbu Aisha Juma	XXXX	Training school	10-Oct-2016 03:33:07	15-Oct-2016 01:00:56	4 days
1	Ezekiel Mutua Mwasi	XXXX	citizenship services	10-Oct-2016 07:38:17	06-Jan-2017 03:32:14	2 months
1	Nelly Makachia makoha	KAC	Training school	12-Oct-2016 03:30:43	10-Jan-2017 08:28:01	2 months
1	Wibronda Atieno Onyango		citizenship services	12-Oct-2016 04:42:55	11-Jan-2017 09:23:33	2 months
1	Jackson Mbabu Kirimi	XXXX	citizenship services	06-Jan-2017 03:23:25	06-Jan-2017 03:32:48	9 minutes

Appendix 8: Sample Code

- Database connection and email configuration

```
APP_ENV=local
APP_KEY=base64:gcffEf3ap81G77tLqQ0ra/3vdVhT40D9u/rsKa21rfQ=
APP_DEBUG=true
APP_LOG_LEVEL=debug
APP_URL=http://localhost
```

```
DB_CONNECTION=mysql
DB_HOST=127. 0. 0. 1
DB_PORT=3306
DB_DATABASE=property
DB_USERNAME=root
DB_PASSWORD=isanyad
```

```
DB_EXT_CONNECTION=mysql
DB_EXT_HOST=174. 138. 55. 234
DB_EXT_PORT=3306
DB_EXT_DATABASE=zadmin_pprp
DB_EXT_USERNAME=transport
DB_EXT_PASSWORD=za5asy2yg
```

```
DDB_EXT_CONNECTION=mysql
DDB_EXT_HOST=127. 0. 0. 1
DDB_EXT_PORT=3306
DDB_EXT_DATABASE=ppip
DDB_EXT_USERNAME=root
DDB_EXT_PASSWORD=isanyad
```

```
DB_EXTT_CONNECTION=mysql
DB_EXTT_HOST=174. 138. 55. 234
DB_EXTT_PORT=3306
DB_EXTT_DATABASE=zadmin_pprp
DB_EXTT_USERNAME=transport
DB_EXTT_PASSWORD=za5asy2yg
```

```
BROADCAST_DRIVER=log
CACHE_DRIVER=array
SESSION_DRIVER=file
```

```
QUEUE_DRIVER=sync
```

```
REDIS_HOST=127. 0. 0. 1
```

```
REDIS_PASSWORD=null
```

```
REDIS_PORT=6379
```

```
MAIL_DRIVER=smtp
```

```
MAIL_HOST=smtp. gmail. com
```

```
MAIL_PORT=587
```

```
MAIL_USERNAME=systemtesting209@gmail. com
```

```
MAIL_PASSWORD=eucwtmzplpnugkql
```

```
MAIL_ENCRYPTION=tls
```

```
PUSHER_APP_ID=
```

```
PUSHER_KEY=
```

```
PUSHER_SECRET=
```

- **Send Sms and Get Wanted Person code**

```
public static function sendSMS($phone, $message2)
{
```

```
    $key="bNtzIr3j0nw7abhS4fPhPD4RoZspFjERpYsZI2uQrpuSfDHFJxfbnN9QzeDFR93Y";
    $phone=$phone;
```

```
    $post = [
        'key' => $key,
        'numbers' => $phone,
        'text' => $message2,
        'sender_id' => 'IDARGSSL'
    ];
```

```
    $ch = curl_init('http://bulksms.orbit.co.ke/api/message/bulk/send');
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
```

```

curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
    $response = curl_exec($ch);
curl_close($ch);
    $return_message=json_decode($response);
return $return_message;

return true;
}

public static function getWantedPerson($number)
{

    $post = [
        'id_number' => $number,
    ];

    $url1="http://connected.qooetu.com/Api/getPerson";
    $ch = curl_init($url1);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
    $response = curl_exec($ch);
curl_close($ch);
    $return_message=json_decode($response);
return $return_message;

}

```

- **LOGIN**

```
<?php
```

```

/* @var $this yii\web\View */

/* @var $form yii\bootstrap\ActiveForm */

/* @var $model \common\models\LoginForm */

use yii\helpers\Html;

use yii\bootstrap\ActiveForm;

```

```

use yii\helpers\ArrayHelper;

use common\models\Buildings;

$this->title = 'Login';

$this->params['breadcrumbs'][] = $this->title;

?>

<?php $form = ActiveForm::begin(['id' => 'login-form']); ?>

<div class="row">

    <div class="col-sm-10 text-left">

        <?= $form->field($model, 'username')->textInput(["class"=>"form-
control", "placeholder"=>"Username"])->label(false) ?>

    </div>

</div>

<div class="row">

    <div class="col-sm-10 text-left">

        <?= $form->field($model, 'password')->passwordInput(["class"=>"form-
control", "placeholder"=>"Password"])->label(false) ?>

    </div>

</div>

<div class="row">

    <div class="col-sm-10 text-left">

        <?= $form->field($model, 'building')->dropDownList(ArrayHelper::map(Buildings::find()-
>all(), 'bld_id', 'name'), ["class"=>"form-control", "prompt"=>"--select--"])->label(false) ?>

    </div>

</div>

<div class="row">

```

```

<div class="col-sm-10 text-left">
<?= $form->field($model, 'rememberMe')->checkbox() ?>
</div>
</div>
<div class="row">
<div class="col-sm-10 text-left">
<?= Html::submitButton('Login', ['class' => 'btn btn-primary', 'name' => 'login-button']) ?>
    </div>
</div>
<?php ActiveForm::end(); ?>
<br/>
<div class="row" style="border-top: 1px #262A33 solid;">
<div class="col-sm-6 text-left">
<p>SuperAdmin User username: admin <br> password: 123qwe</p>
    </div>
    <div class="col-sm-6 text-left">
<p>Normal User username :mkahora<br> password : 123qwe</p>
    </div>
</div>

```

- **REGISTER**

```

<?php
namespace common\models;

use Yii;

/**

```



```
* This is the model class for table "sc_people".
*
* @property integer $prs_id
* @property string $firstname
* @property string $middlename
* @property string $lastname
* @property string $idnumber
* @property string $email
* @property string $phone
*/
class People extends ParentModel
{
public $role;
public $username;
public $password;
/**
 * @inheritdoc
 */
public static function tableName()
{
return 'sc_people';
}

/**
 * @inheritdoc
```

```

*/
public function rules()
{
return [
    [['firstname', 'lastname', 'idnumber', 'phone', 'stt_id', 'idn_id'], 'required'],
    //[['image'], 'required', 'message'=>"Please Take a snapshot"],
    [['firstname', 'middlename', 'lastname', 'idnumber', 'email', 'phone'], 'string', 'max' =>
255],
    [['idnumber', 'email'], 'unique'],
    [['email'], 'email'],
    [['image', 'role'], 'safe']
];
}

/**
 * @inheritdoc
 */
public function attributeLabels()
{
return [
    'prs_id' => 'Prs ID',
    'firstname' => 'First Name',
    'middlename' => 'Middle Name',
    'lastname' => 'Last Name',
    'idnumber' => 'ID Number',
    'stt_id' => 'Status',

```

```
        'idn_id' => 'Identity',
        'email' => 'Email',
        'phone' => 'Phone',
    ];
}

public function getUser(){
    return $this->hasOne(User::className(), ['prs_id'=>'prs_id']);
}
}
<?php

namespace backend\modules\settings\controllers;

use Yii;

use common\models\People;
use common\models\PeopleSearch;
use backend\controllers\BaseController;
use yii\web\NotFoundHttpException;
use yii\filters\VerbFilter;
use yii\widgets\ActiveForm;
use yii\web\Response;

/**
 * PeopleController implements the CRUD actions for People model.
 */
```

```
class PeopleController extends BaseController
{

public function actionValidate(){
    $model = new People();
    if (Yii::$app->request->isAjax&& $model->load(Yii::$app->request->post())) {
        Yii::$app->response->format = Response::FORMAT_JSON;
        return ActiveForm::validate($model);
    }
    //}
}
/**
 * Lists all People models.
 * @return mixed
 */
public function actionIndex()
{
    $searchModel = new PeopleSearch();
    $dataProvider = $searchModel->search(Yii::$app->request->queryParams);

return $this->render('index', [
    'searchModel' => $searchModel,
    'dataProvider' => $dataProvider,
]);
}
```

```

/**
 * Displays a single People model.
 * @param integer $id
 * @return mixed
 */
public function actionView($id)
{
return $this->render('view', [
    'model' => $this->findModel($id),
]);
}

/**
 * Creates a new People model.
 * If creation is successful, the browser will be redirected to the 'view' page.
 * @return mixed
 */
public function actionCreate()
{
    $model = new People();

if ($model->load(Yii::$app->request->post()) && $model->validate()) {
    //define("UPLOAD_DIR",
'C:\xampp\htdocs\securex\backend\web\ultimo\images\test');
    $img = $model->image; //Attribute to INPUT name = textimage

```

```

        $img = str_replace('data:image/png;base64,', '', $img);
        //$img = str_replace(' ', '+', $img);
        $model->image = $img;
        $model->save(false);
return $this->redirect(['index']);

    } else {
return $this->render('create', [
        'model' => $model,
    ]);
    }
}

/**
 * Creates a new People model.
 * If creation is successful, the browser will be redirected to the 'view' page.
 * @return mixed
 */
public function actionCreate2()
{
    $model = new People();

    if ($model->load(Yii::$app->request->post()) && $model->validate()) {
        Yii::$app->response->format = Response::FORMAT_JSON;
        if($model->save()){
            return "saved";
        }
    }
}

```

```

        } else {
            return "unsaved";
        }
    } else {
        return $this->renderAjax('create2', [
            'model' => $model,
        ]);
    }
}

/**
 * Updates an existing People model.
 * If update is successful, the browser will be redirected to the 'view' page.
 * @param integer $id
 * @return mixed
 */
public function actionUpdate($id)
{
    $model = $this->findModel($id);

    if ($model->load(Yii::$app->request->post()) && $model->save()) {
        return $this->redirect(['index']);
    } else {
        return $this->render('update', [
            'model' => $model,
        ]);
    }
}

```

```
    }  
}  
  
public function actionUpload(){  
    $post = Yii::$app->request->post();  
    Yii::$app->response->format = Response::FORMAT_JSON;  
    return $_FILES;  
}  
  
/**  
 * Finds the People model based on its primary key value.  
 * If the model is not found, a 404 HTTP exception will be thrown.  
 * @param integer $id  
 * @return People the loaded model  
 * @throws NotFoundHttpException if the model cannot be found  
 */  
protected function findModel($id)  
{  
    if (($model = People::findOne($id)) !== null) {  
        return $model;  
    } else {  
        throw new NotFoundHttpException('The requested page does not exist.');    }  
}
```



```
}

```

- **CHECK OUT**

```
<?php

```

```
use common\models\Status;

```

```
use common\models\Identity;

```

```
use common\models\Companies;

```

```
use yii\widgets\ActiveForm;

```

```
?>

```

```
<div class="row">

```

```
    <div class="col-lg-6">

```

```
        <div class="scroll-area profile-information">

```

```
            <div class="profile-pic text-

```

```
center">

```

```
                <p class="myImage">

```

```
                    <imgsrc="<?= 'data:image/png;base64,'.$model->checkedin->image ?>"

```

```
                />

```

```
            </p>

```

```
</div>
```

```
</div>
```

```
</div>
```

```
<div class="col-lg-6">
```

```
<table class="table table-hover table-bordered">
```

```
<tbody>
```

```
<tr>
```

```
<td width="180"><b>First Name</b></td>
```

```
<td><?= $model->checkedin->firstname?></td>
```

```
</tr>
```

```
<tr>
```

```
<td><b>Last Name</b></td>
```

```
<td><?= $model->checkedin->lastname?></td>
```

```
</tr>
```

```
<tr>
```

```
<td><b>Type of Identifier</b></td>
```

```

        <td><?= isset($model->checkedin->idn_id)?Identity::findOne($model-
>checkedin->idn_id)->description:"" ?></td>

        </tr>

        <tr>

        <td><b>ID Number</b></td>

        <td><?= $model->checkedin->idnumber?></td>

        </tr>

        <tr>

        <td><b>Status</b></td>

        <td><?= isset($model->checkedin)?Status::findOne($model->checkedin-
>stt_id)->description:"" ?></td>

        </tr>

        </tbody>

</table>

</div>

</div>

<div class="row">

```

```

<div class="col-lg-12">

<table class="table table-hover table-bordered">

<tbody>

<tr>

<td width="180"><b>Destination</b></td>

<td><?= isset($model->cmp_id)?Companies::findOne($model->cmp_id)-
>description:""?'></td>

<td><b>Organization From</b></td>

<td><?= $model->organisation_from?'></td>

</tr>

<tr>

<td><b>Person To Be See</b></td>

<td><?= $model->person_to_see ?></td>

<td><b>Reason</b></td>

<td><?= $model->visit_reason?'></td>

</tr>

```

```
        </tbody>

</table>

    </div>

</div>

<div class="row">

    <div class="col-lg-12">

        <?php $form = ActiveForm::begin(["id"=>"my-form"]); ?>

        <?= $form->field($model,'checked_out')->hiddenInput(["value"=>1])-
>label(false)?>

    <div class="row">

        <div class="col-lg-12">

            <?= $form->field($model,'check_out_comment')-
>textarea(["rows"=>2])?>

        </div>

    </div>

</div>

<button class="btn btn-danger">Check Out</button>

<?php ActiveForm::end(); ?>
```

```
</div>
```

```
</div>
```

```
<?php
```

```
// Ajax Submit code for adding/Editing countries
```

```
$script = <<< JS
```

```
    $('form#my-form').on('beforeSubmit', function(e) {
```

```
        var \form = $(this);
```

```
        $.post(
```

```
            \form.attr("action"),
```

```
            \form.serialize()
```

```
        ).done(function(result) {
```

```
            if (result == 'saved') {
```

```
                $(\form).trigger("reset");
```

```
                window.location.href="";
```

```
            } else {
```

```
                $("#message").html(result.message);
```

```
    }  
  
  })  
  
  .fail(function(){  
  
    console.log("server error");  
  
  });  
  
  return false;  
  
  });  
  
JS;  
  
$this->registerJs( $script );  
  
?>
```

Appendix 9: System Evaluation Form

Instructions: Answer by ticking Yes or No

Questions	Response	
A. Usability		
1. Is the System user-friendly?	Yes	No
2. Would you require technical support to use the System	Yes	No
3. Are various functions well integrated?	Yes	No
4. Would you require to learn other things before using the system	Yes	No
5. Is the system fast to learn?	Yes	No
6. Various functions are well integrated	Yes	No
B. Effectiveness	Yes	No
1. Does the System help you achieve your objective?	Yes	No
2. Would you recommend the system to other owners of commercial buildings?	Yes	No
3. Did the System meet your expectations?	Yes	No

4. Does the System take into consideration the users' needs?	Yes	No
C. Efficiency	Yes	No
1. The software is fast enough	Yes	No
2. The system sometimes hangs unexpectedly	Yes	No
3. Are the instructions prompted by the System helpful?	Yes	No