Strathmore University
SU+ @ Strathmore University Library

Electronic Theses and Dissertations

2017

A Public key infrastructure based model for verification of title deeds in Kenya

Fanon Kimani Kariuki
Fuculty of Information Technology (FIT)
Strathmore University

Follow this and additional works at https://su-plus.strathmore.edu/handle/11071/5633

Recommended Citation

Kariuki, F. K. (2017). *A Public key infrastructure based model for verification of title deeds in Kenya* (Thesis). Strathmore University. Retrieved from http://su-plus.strathmore.edu/handle/11071/5633

This Thesis - Open Access is brought to you for free and open access by DSpace @Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @Strathmore University. For more information, please contact librarian@strathmore.edu

A Public Key Infrastructure Based model For Verification of Title Deeds in Kenya

Fanon Kimani Kariuki
056207

Submitted in partial fulfillment of the requirements for the Degree of Master of Science in Information Technology (MSc. IT) at Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

June 2017

This thesis is available for Library use on the understanding that it is copyright material and that no quotation from the research thesis may be published without proper acknowledgement

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University.

FANON KIMANI KARIUKI

9th June 2017

Approval

The thesis of Fanon Kimani Kariuki was reviewed and approved by the following:

Dr. Humphrey Njogu,
Senior Lecturer, Faculty of Information Technology,
Strathmore University

Dr. Joseph Orero,
Dean, Faculty of Information Technology,
Strathmore University

Professor Ruth Kiraka,
Dean, School of Graduate Studies,
Strathmore University

Abstract

The Kenya lands administration process faces many challenges arising from the use of a paper based system. Over the years, this system has come under scrutiny because of inconsistencies, irregularities and the bulk of physical records that when tampered with undermine the integrity of records kept. This problem makes it difficult to quickly and accurately verify the validity of any given title deed and has also caused an influx of counterfeit title deeds which throws ownership of land into dispute. In order to verify the authenticity of a title deed, one has to fill out forms and pay a fee at the lands offices, and then go through a slow and inefficient process due to the voluminous records associated with the current paper based system.

Despite digitization efforts in 2014 aimed at streamlining service provision, title deed verification still remains a critical challenge. Financial institutions are therefore reluctant to issue loans with land as collateral because it is a slow and often inaccurate process to ascertain true ownership of land, and this may lead to loss of potential customers.

Based on the challenges of identifying true land ownership by authenticating title deeds, this study will adopt the Public Key Infrastructure (PKI) model which incorporates the use of a trusted third party (Certification Authority) to create digital certificates. The Nairobi Lands registry will act as the Certification Authority in this study, within which there will also be a registration function (Registration Authority or RA) and a key generator to generate a public-private key pair.

The RA will confirm title land owners' details, and the CA will issue digitally signed certificates, which will be used by financial institutions to compare to physical title deeds for discrepancies, and thus authenticate them. The PKI model's ability to provide digital certificate validation, time stamping, data confidentiality and authenticity makes it a suitable choice to eliminate the authentication related challenges experienced currently.

This study aims to develop a prototype using a waterfall software development model to validate the proposed title deed verification solution. The prototype will be tested to validate its accuracy and efficiency in authenticating sample title deeds.

Keywords

Public key infrastructure (PKI), Certification authority (CA), Registration authority (RA), public key, private key

Table of Contents

List of Figures

List of Tables

Definition of Terms

CA- This is an entity that issues digital certificates (Thales e-security, 2016)

Digital Certificate- an electronic document used to prove the ownership of a public key (Christof et.al, 2010).

Key -This a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm (Audun, 2013)

PKI- A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption (Thales e-security (2016).

RA -An authority in a network that verifies user requests for a digital certificate and tells the Certificate Authority (CA) to issue it. RAs are part of a public key infrastructure (PKI), a networked system that enables companies and users to exchange information and money safely and securely. (RSA, 2016)

RSA - This one of the most widely used public key cryptographic algorithms that can be used for public key encryption and digital signatures. Its secrecy is based on the difficulty of factoring large integers. (RSA, 2016).

X.500- This is a series of computer networking standards covering electronic directory services (RSA , 2016)

Abbreviations/Acronyms

ASAL - Arid and semi-arid Lands

CA - Certification Authority

CASE - Computer-Aided Software Engineering tools

CORBA -Common Object Request Broker Architecture

CRL -Certificate Revocation List

DMZ - Demilitarized Zone

FTP -File Transfer Protocol

GB -Gigabyte

HIPO -Hierarchical Input Process Output Model

HTTP -Hypertext Transfer Protocol

HTTPS -Hypertext Transfer Protocol Secure

LAN -Local Area Network

LDAP -Lightweight Directory Access Protocol

PKI -Public Key Infrastructure

RA - Registration Authority

RAM -Random Access Memory

RSA- (Ron Rivest, Adi Shamir and Leonard Adleman) an asymmetric cryptographic algorithm

RUD - Requirements Understanding Document

SPSS - Statistical Package for Social Sciences

SSL -Secure Sockets Layer

USSD -Unstructured Supplementary Service Data

VFM -Verification module

Acknowledgements

I thank God, for giving me the health, the strength and grit to accomplish all that I have so far. My heartfelt thanksgiving also goes to my supervisor, Dr. Humphrey Njogu, for his assistance, guidance and patience throughout my research. I finally wish thank my classmates for their camaraderie and help as we trudged together through this journey.

Dedication

I dedicate this work to my Father, Prof. James Kariuki Mutiti, who inspired me in words, action, and spirit to brave it all, and conquer it all. This is also for my mother, Jane Nyakibia, for all the lessons and for all the love, all the time. This is especially dedicated to my sisters; Zindzi, Rainha and Ivy-Virginia, my cavalry when the center cannot hold, and my vanguard when it is go-time!

Chapter One: Introduction

1.1 Background of the study

Land is the most valuable natural resource which when well-planned and developed offers major prospects for increases in output and incomes for the people, especially for those who are near or below the poverty line. For efficient land planning and optimum use, it is essential that there be clarity and certainty about land ownership. Kenya's land mass is approximately 587,900 square kilometers. An estimated 17.2 % of this mass area comprises land of high and medium potential while the remaining over 80% is arid and semi-arid land. An overwhelming 80% of the population lives in the 17.2% land category where the indigenous forests are also located. The bulk of land in the country (80%) thus supports only 20% of the population (The Kenya Land Alliance report, 2010).Agriculture remains the backbone of the national economy. The sector contributes to over 25% of the GDP while employing and supporting over 80% of the population (The Kenya Land Alliance report, 2006).

With land being such a critical resource in Kenya, land administration must therefore be done in a manner that is transparent, fair to all and brings about integrity. Nyakundi (2012) observes that a good land rights administration serves a purpose, among other things, to improve and guarantee security of land tenure, reduce land disputes and guarantee the result of judicial procedures relating to land rights. Land administration in Kenya has however faced many challenges. This is because the system used currently is largely paper based, and the corresponding voluminous records are challenging to keep track of and retrieve easily for verification purposes. In addition, according to the Kenya land alliance report (2006), any stealing, duplicating or altering of records goes undetected because of the disorganized and inconsistent nature of the paper based system, which impedes any title deed authentication process.

In 2014, Kenya embarked on a program of re-engineering its land registry business processes with a view of providing efficient and timely public by digitizing records service (Kahuho, 2016). One of the key registries in Nairobi has been fully digitized to date but its services do not include verification of title deeds as there is no link to the master registry title deed database.

Many countries have digitized their land management processes and thus make verification of title deeds quick and reliable. Imran et.al (2013) observes that in the United states for instance, the ArcGIS Parcel data model has been used. This model incorporates GIS technology, hardware and software components and strict business rules to capture data and records and store them in a digital format. Further, these records can only be accessed or manipulated by only authorized individuals to ensure that the integrity of data is maintained. The ArcGIS model uses several techniques, such as satellite imagery, to capture geographical data of the land. This is then compared and aggregated with existing ownership records. This geospatial data is always up to date, and verification of ownership of a piece of land can be done online or through the use of a mobile app, as long as a user is authorized to do so. This is in stark contrast to the digitization in Kenya, where only physical records are converted into digital format. The cadastral maps however remain in paper format.

Due to the challenges experienced at the lands offices, and the short falls of the paper based system, it takes a long time to authenticate a title deed. Further, the results may also be inconsistent, which adversely affect the bank's position in disbursing a loan. For this reason, there has been a decline in the use of title deeds as collateral or the demand for alternate or additional collateral by financial institutions. This also means that financial institutions lose many customers who may wish to use the banks' loan facilities.

A solution to this problem may be realized by implementing a system that incorporates the security principles embedded in a Public Key Infrastructure (PKI) and asymmetric encryption to ensure the integrity of title deeds is maintained. Asymmetric keys work using a key pair; one public key for encryption and another mathematically related but different private key for decryption. These keys are associated with an entity that needs to authenticate its identity or encrypt data. Each public key is published in a communal data store (in a digital certificate), usually a directory of some description. Data encrypted with the public key can only be decrypted with the corresponding (and unique) private key. The private key is kept secret and stays with the user, either on the hard disc of their computer or on a token such as a smart card.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, where a root trust authority (CA) enables users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party by using digital certificates. Thales e-security (2016) states that a digital certificate is a digital form

of identification, much like a passport or driver's license and is a guarantee issued by a third party (certification authority or CA) and contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate issuing authority (CA) so that a recipient can verify that the certificate is real.

The Nairobi Lands registry will be entrusted as the Certification Authority (CA), and will also have a registration function or the Registration Authority (RA). The RA will verify the land owner's details and the title deed details, after which the CA will issue a time stamped, digitally signed digital title deed. The CA's private key will be used to sign this digital title deed, and the publicly available CA's public key will be used to verify this signature.

A private and public key pair will be generated by the key generator and issued for the title deed holder; the public key will be on the digital title deed and the private key will be given to the land owner in a physical key card, and will be used for matching to it during verification. The digital title deeds will be stored in a directory only accessible to authorized institutions that will take part in the verification process. These institutions will also be issued with a private key in a key card, and access to the directory will be granted when the access control module matches the private key in the key card to the corresponding public key.

Once the system reads the private key on the land owner's key card, the digital title deed with the corresponding public key is displayed. In addition to this, the digital signature on this digital title deed is verified, and thus the details contained in this digital title deed will be deemed to be authentic.

1.2 Statement of the problem

The land administration system in Kenya is largely paper based and the associated records in the system are voluminous. This type of record keeping is often an inconvenience because access to these records is very slow, and it is vulnerable to adulteration and inconsistencies. Further, verification of title deeds is very slow, inefficient and often inaccurate. For this reason, there has been an influx of counterfeit title deeds in Kenya in efforts to propagate fraudulent activities involving title deeds. It is imperative for financial institutions to verify the validity of title deeds before disbursing a loan where land is used as collateral. However, because of the slow, inaccurate and inefficient process of verification, financial institutions often turn

down loan applications or ask for alternate collateral. These financial institutions end up losing many customers and consequently much revenue, which is bad for their business, and a disadvantage to deserving land owners.

1.3 Research Objectives

The following are the objectives that this study aims to achieve in its entirety:

i. To identify factors that influence land title deed verification,
ii. To review the current land title deed verification models and solutions,
iii. To design and develop a system that uses the PKI model to enable efficient verification of land title deeds in Kenya,
iv. To validate the accuracy and efficiency of the proposed system.

1.4 Research Questions

The following are the research questions that this project will seek the answers for:

i. What are the factors that influence land title deed verification in Kenya?
ii. What are the merits, demerits and research gaps of the current land title deed verification models and systems?
iii. How will the proposed system be designed and developed using the PKI model, and how will it work to make land title deed verification in Kenya more efficient?
iv. How will the proposed system be validated in terms of accuracy, efficiency and performance?

1.5 Justification

The title deed verification process is very slow because of the time taken to go through relevant records in the current paper based system to complete verification. This is a major challenge for the lands registry because handling many verification requests takes a long time. It is also a challenge to genuine land owners because title deed counterfeiting puts their ownership into doubt, and also prospective land owners have no assurance that they are purchasing land from a legal owner. Financial institutions experience major challenges during title deed verification and therefore do not trust title deeds because of the influx of counterfeiting. For this reason, they opt to either decline land as collateral, or ask for additional collateral during disbursement of loans.

The proposed system aims at eliminating these challenges by using a PKI based verification model to make verification of title deeds more efficient. Such a system will be of benefit to land owners to be able to prove ownership, and to prospective land owners to give reassurance in their purchase.

A quick, efficient and accurate title deed verification system will be beneficial to financial institutions because it will reduce verification time and thus hasten loan processing time. Financial institutions will be able to access digital signed certificates and compare them to physical certificates and complete verification easily. Streamlining loan disbursement processes yields great financial benefits to banks, as well as ensures that land owners who wish to procure loans access the services faster.

1.6 Scope of the study

The study will be conducted in Kenya, specifically at Nairobi's lands registry. This is because the lands registries in the various counties in Kenya have a similar structure, and therefore any system developed in Nairobi would be central and can be replicated countrywide. The study will also include financial institutions in Nairobi that seek to verify title deeds at the lands registry.

1.7 Conclusion

The current paper-based land management system is Kenya has many challenges, one of which is voluminous records that make it very difficult to verify title deeds. The large numbers of records are also susceptible to tampering which undermines any verification processes. As a result, counterfeit title deeds carry weight because there is no way to verify validity, and financial institutions as an example make it harder to access loans to customers who present title deeds as collateral. This study however adopts a PKI based verification model to provide a means to verify title deeds quickly, securely and efficiently, and thus reinstate make counterfeiting of title deeds obsolete.

Chapter 2 : Literature Review

2.1 Introduction

In the investigation of the research problem and to further understand the concept, a review of the challenges encountered in title deed verification in Kenya today will be conducted in an empirical framework. Next, the theoretical framework that encompasses relevant publications and works by other scholars in the field of cryptography, as well as in the integration of PKI model in the development of other systems will be done. Lastly, the conceptual framework which seeks to amalgamate these ideas with the proposed area of investigation will be done to conclude the chapter.

2.2 Land in Kenya

As stated in the Kenya Land alliance report (2002), land is the most important resource in Kenya. However, of the total area of 582,646 km^2, only 17% is suitable for rain-fed agriculture. Arid and semi-arid lands (ASALs) comprising grassland and savannah rangelands cover the remaining 82%. The rangelands are home to 85% of total wildlife population, and 14 million people practicing dry-land farming and pastoralism. An overwhelming 80% of the population lives in the 17% land category where the indigenous forests are also located. The bulk of land in the country (80%) thus supports only 20% of the population (The Kenya Land Alliance report, 2010).

There are different types of land tenure-ship in the country as defined in the Kenya Constitution (2010). They include Freehold, Leasehold, Customary and Public/State Land. Foreigners can only access ownership on a leasehold basis. Freehold tenure-ship has no restrictions as to the use or occupation. Leasehold tenure-ship is the interest in land for a specific period of time for a fee. Public land is owned by the government, and leased out for a fee out to the public for public projects and amenities. Customary/community land is given out to a particular community for special reasons, and it is for community based uses.

2.3 The use of land as collateral

Lending institutions play a major role in economic growth and development through provision of credit to execute economic activities. However, the major concern of any lender while advancing credit is how they will get their money back (Fleisig, 1995), and this implies that the engagement between lenders and borrower is accompanied by certain level of risk,

which can be mitigated by the use of collateral. Collateral can generally be described as a defined asset issued by the borrower to the lender, in a show of commitment towards repaying the loan advanced (Fleisig, 1995).

In Kenya, land is the prime asset used as collateral in order to secure loans from financial institutions. In order to secure a loan in Kenya, a financial institution has to conduct a world search at the central registry to verify identification details. The financial institution has to also check the validity of the presented title deed at the lands registry. This usually is a costly and slow process because of the unique challenges experienced at the lands registry, which in turn has turned many financial institutions away from accepting land as collateral to other more attractive forms of collateral (FSD-Kenya, 2009).

2.4 Challenges experienced by financial institutions in land verification

In order for financial institutions to be able to accept land as collateral for a loan, a verification process must first take place. The financial institution first checks the applicant's identification details in the national identification database. The financial institution also has to check the details of the presented title deed in the central title deeds database at the lands registry. This process is carried out by the financial institution's valuing department. The verification process has to be done by filling out requisite forms and physically presenting them to the lands registry.

The system used at the lands registry is largely paper based, and the records to be searched are voluminous. The process of searching for the records to ascertain that they exist and that they are as accurate as purported takes a long time. Further, because of many paper based records and in case of irregularities, the results of a search may yield inconsistent and unreliable results. The slow speed of the search also slows down the loan processing time. FSD-Kenya, (2009) estimates that it costs a total of 5.78% of the loan amount and sixty working days just to process a loan where land has been used as collateral. The inefficiency, slow speed and inconsistency of the title deed verification process thus force financial institutions to decline the use of land as collateral, and instead ask for alternate forms of collateral for loan disbursement purposes.

2.5 Cryptography concepts

This section reviews some concepts, techniques, features and infrastructures that are used in cryptographic processes.

2.5.1 Cryptography

Audun (2013) defines cryptography as the science of providing security for information by writing or solving codes for the sole purpose of concealing the confidential information from unauthorized eyes and ensure immediate detection of any alteration made to the concealed information.

2.5.2 Symmetric Encryption

Christof (2010) describes symmetric encryption as a way to encrypt or hide the contents of the plaintext where the sender and receiver both use the same secret key. Symmetric encryption is not sufficient for most applications because it only provides secrecy but not authenticity in that if the key is stolen, the attacker can change the content easily and the receiver would not be able to know (Audun, 2013). As with all cryptographic methods, another problem with symmetric cryptography is with the secure distribution of the keys. It is very important that the keys be distributed in such a manner that they do not fall into unintended hands so as to secure the cryptographic process (Thales e-security, 2016).

2.5.3 Public Key Encryption

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key and each key performs a unique function: the public key is used to encrypt and the private key is used to decrypt (Christof et.al, 2010). It is computationally infeasible to compute the private key based on the public key. Because of this, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, and ensuring only the owners of the private keys can decrypt content and create digital signatures (Audun, 2013). Since public keys need to be shared but are too big to be easily remembered, they are stored on digital certificates for secure transport and sharing. Since private keys are not shared, they are simply stored in the software, on the operating system or on hardware such as smartcards (Audun, 2013).

PKIs provide a framework that enables cryptographic data security technologies such as digital certificates and signatures to be effectively deployed on a mass scale. As a foundational element of many trusted systems, PKIs are already present in more places than one would generally think, supporting identity management services within and across networks, and underpinning online authentication capabilities (Thales e-security, 2016).

2.5.4 PKI Components

There are three core functional components to a PKI as outlined in the work done by Thales e-security (2016): The Certificate Authority (CA), an entity which issues certificates. CAs manage the lifecycle of all digital credentials within a PKI, including their issuance, renewal, and revocation of digital certificates. The digital credential, validates the ownership of a public key by the named subject of the certificate. When receiving digitally signed information, the certificate enables users (signers and verifiers) to validate that the private key used to create the signature indeed belongs to them as rightful owners (Thales e-security, 2016). The repository for keys, certificates and Certificate Revocation Lists (CRLs) is usually based on a Lightweight Directory Access Protocol (LDAP)-enabled directory service.

2.5.5 PKI functions

The PKI has several functions that are paramount to its efficiency and suitability for use. RSA (2016) outlines the functions as follows:

Issuing certificates: The CA signs the certificate, thereby authenticating the identity of the requestor, in the same way that a notary public vouches for the signature and identity of an individual. In addition, the CA "stamps" the certificate with an expiration date. The CA may return the certificate to the requesting system and/or post it in a repository

Revoking certificates: A certificate may become invalid before the normal expiration of its validity period. For instance, an employee may quit or change names, or a private key may be compromised. Under such circumstances, the CA revokes the certificate by including the certificate's serial number on the next scheduled CRL.

Storing and retrieving certificates: The most common means of storing and retrieving certificates is via a directory service, with access via LDAP. Other options include X.500 compatible directories, HTTP, FTP, and e-mail.

Providing trust: Each public key user must have at least one public key from a CA that the user trusts implicitly. Organizations can establish and maintain trust within a single security management domain through a thorough audit of the CA's policies and procedures, repeated at regular intervals. However, organizations need to evaluate (and accept or reject) certificates from CAs not under their direct control, such as CAs of other business units or partners. This can be accomplished through hierarchical certification path processing or direct cross-certification.

2.5.6 Digital Signatures and Digital Certificates

Christof (2010) describes a digital signature as an attachment to an electronic message that includes a mathematical digest of the message created using public key cryptography hence it is specific to both the signer of the message and the message itself. A digital signature can therefore be used as an affirmative identity of both the message sender and the message itself.

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (Audun 2013). A digital certificate provides identifying information and it is forgery resistant and can be verified because it was issued by an official, trusted agency. RSA (2016) further states that certificates contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real. To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority.

2.6 Application of Technology in land ownership verification

Partial digitization of records in Kenya took place in 2014, and with this it was possible to pay land rates online. Further, a mobile based land rate payment service was introduced. However, applicants still have to register their property before they can be able to fully use the service. This means that there is a lot of data that has not been inputted into the system, and subscribers have to do it themselves via a USSD (Unstructured Supplementary Service Data) service as shown in Appendix D. This could pose a challenge in the consistency of data in the future because fraudulently, users may register parcels of land that they do not own.

In contrast, the Rwanda Natural Resources Authority (RNRA) has made it easier for any person to check the status of a particular plot of land through the use of a USSD based service as

shown in Appendix D. Users do not register parcels of land, they only query the system for information. The system fetches information about the requested plot number and the subscriber gets the status of the plot comprising of area, registered owners, whether it is disputed or presented as collateral at any bank.

2.7 Existing Solutions for land title deeds verification

2.7.1 Land Management Information System in Korea

Choe (2004) describes a Land management information system (LMIS) in Korea that has a topographical map, a cadastral map, and a zoning map built into the land database with a general aim to provide the general population the correct information about land in a timely and efficient manner. The problem that existed was that due to the separation of different functions, there were many duplications in land transactions and land ownership data. It was easy for government employees recording and transacting similar framing operations, which corrupted the land ownership documents. As a result, Koreans often had to travel to the requisite offices to ascertain the correctness and authenticity of their documents, a process that took several months to complete.

In the LMIS, an open architecture, which emphasizes development of IT systems, economical efficiency and extensibility, was designed to support heterogeneous dispersion-environment among municipalities. Korea has adopted a three-tiered client server architecture (Clients Application Server-Database Server) that applies the standard specifications of CORBA (Common Object Request Broker Architecture) and the server can be divided into data provider, edit agent, and map agent (Figure 2.1). The map provider searches spatial data from GIS engine and transmits the data to map agent and clients; an edit agent carries out editing of the spatial data (input, revision, and deletion). The map agent creates map images by using the spatial data received by the data provider and transmits the images to the clients. The map agent is embodied and operated by Java regardless of the platforms. Lastly, a web server provides requisite to the relevant organizations through the intranet and also inquiries into the land documents for civilians through the Internet.

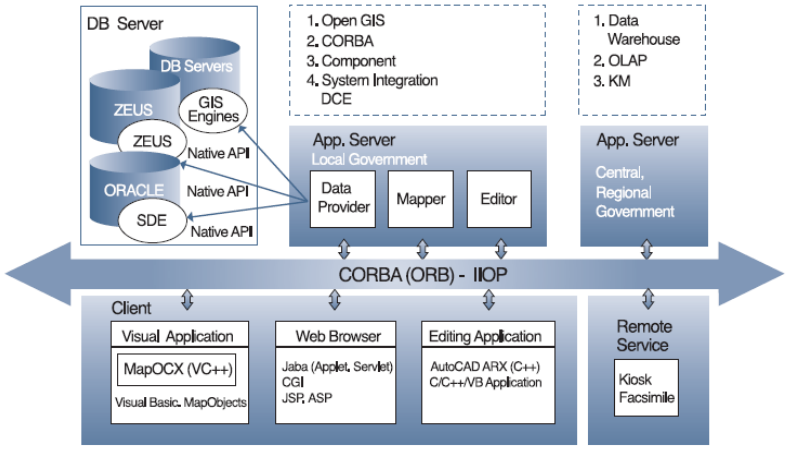


Figure 2.1: Basic architecture of the LMIS

2.7.2 Electronic Land Register in Estonia

Vali (2014) describes a digital land registration system in Estonia developed for the sole purpose of getting rid of a paper-based system to improve efficiency, and to enhance the authentication of land ownership. The Land Register in Estonia is maintained by Land Registry departments of local law courts. Ownership relations and limited real rights established on the registered immovable for the benefit of third persons need to be entered in the Land Register. Estonian Land Register is a title based electronic register. All the land of Estonia has entered into land register (except state-owned land) and the whole land register is accessible online and all register parts are valid electronically. The owner does not need a paper certificate to prove the right to the immovable. Land Register archive contains applications and documents submitted on the immovable and these documents are mostly on paper. About 75 % of all documents are produced by notaries. Since 2007 June all notarized applications (deeds) are registered automatically in digital form in Land Register information system.

As shown in figure 2.2, if an owner wants to sell their land or real property they have to go to the notary. The notary performs necessary inquiries and prepares the contract (deed). Information from other state registers, also from land register, is possible to import directly into contracts. The notary then sends digitally signed (qualified digital signature) contract and application electronically to land register where it is automatically registered. The registrar receives electronic application which includes structured data and a digitally signed contract.

After the registrar checks the application and ascertains that all the necessary information is presented an assistant judge makes an entry to land register. The registrar then sends the decision to notary and participants.

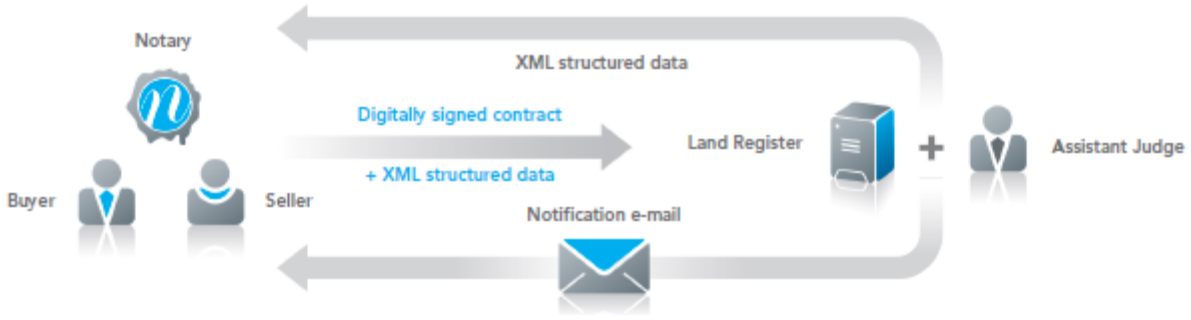


Figure 2.2: digitized land buying process in Estonia

2.7.3 A prototype for the Authentication of University Certificates: A case of Strathmore University

In addition to applications in authenticating land ownership, the PKI technology and digital signature authentication features have also been applied in other areas for authentication. Kamanda (2015) outlines a system for authenticating university certificates as shown in figure 2.3. The prototype made use of digital signatures in order to ensure the authenticity of certificates provided to former students by a university. The digital signature used is unique to each student's certificate, and a copy of the same is created and stored in the system. The signature ensures that the certificate has not been tampered with in any way. The system also has a data store where signed and secured certificates are kept. A secure document delivery approach- which means documents will be rendered, and not stored on the machine-will be used to access these certificates. Access to this data will only be through secure layers such as OpenSSL, and users will have to log in using valid usernames and passwords.

The access is provided through a web portal accessible anywhere in the world, provided there is an internet connection. The limitations of this study are that the scope is only limited to Universities, and that the study did not go into detail on regulations, policies, and policy making in the topic of enrolment fraud.

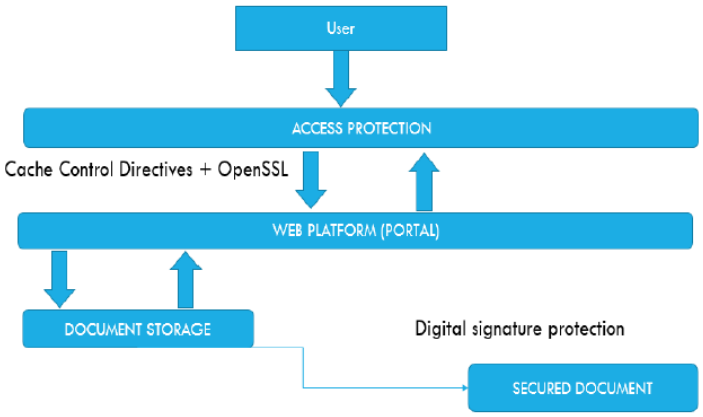


Figure 2.3: Basic architecture of the University certificates authentication system

2.8 Conceptual Framework

This study is based on a conceptual framework that uses a PKI model. The Land registry will be entrusted to be the Certification Authority (CA) within which there will be a Registration function (Registration Authority.) As illustrated in figure 2.4, the proposed system has the following components: the Certification Authority (CA), the Registration Authority (RA), a Certificate Directory, a Key generator and several verification modules (VFM).

The RA's primary function will be to verify the identification details of a land owner, as well as ensure that the details on the physical title deed presented are consistent with what is in the title deed master database. The CA's function upon verification of a physical title deed will be to issue a corresponding digital title deed. The digital title deed will contain the name of the land owner, details of the piece of land, date of issue, the land owner's public key as well as the digital signature of the CA.

The directory will contain all valid digital title deeds, and will only be accessed by institutions that have been vetted and approved by the Lands registry. The digital title deeds will be have the land owner's public key on them, and retrieval will only be possible when the corresponding private key is used.

The Key Generator will generate a private-public key pair for land owners and for financial institutions. The private key will be embedded onto a smart card, and the key pair is then forwarded to the RA.

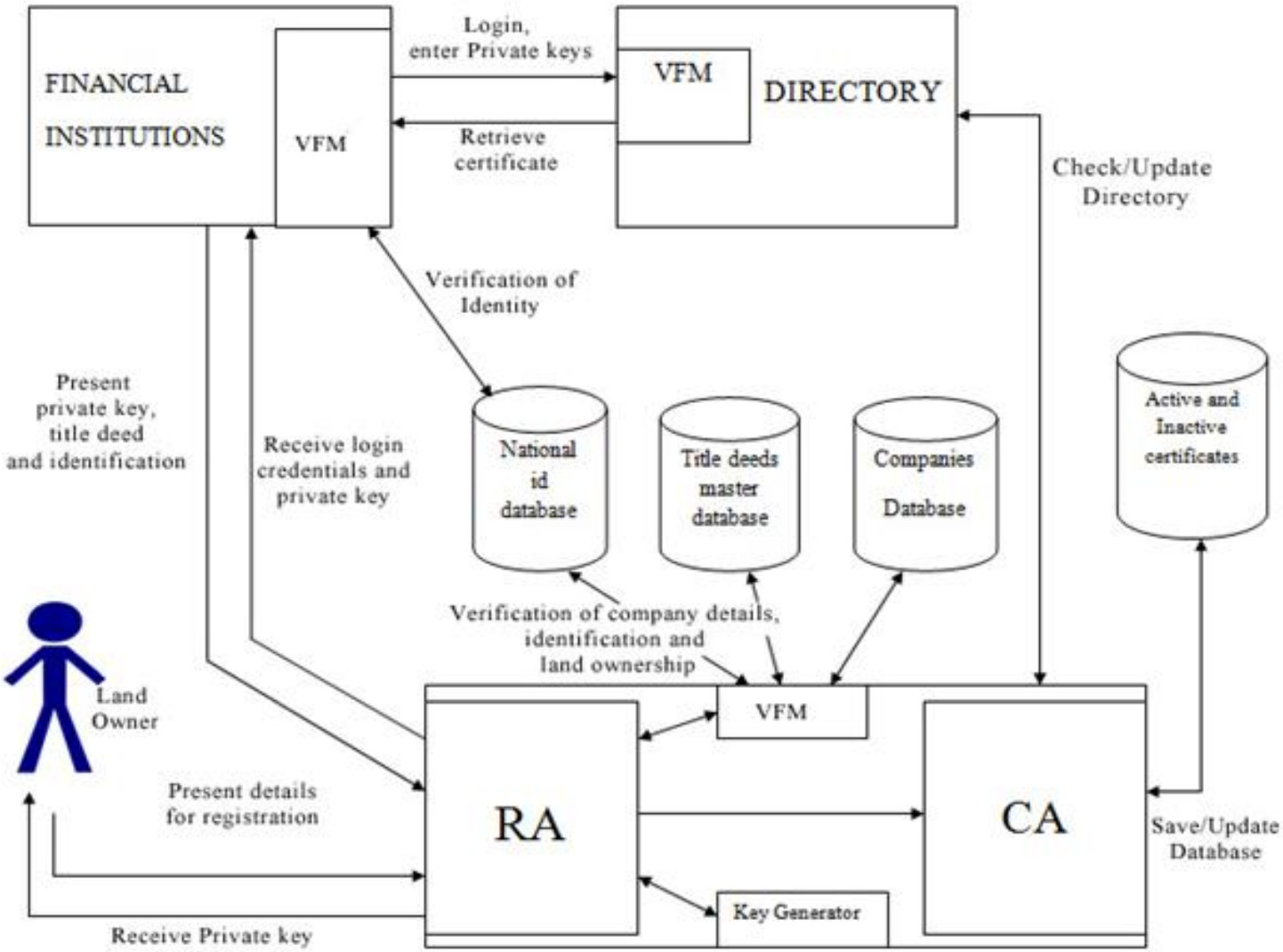


Figure 2.4: The Conceptual Framework

When a land owner presents their identification details and physical title deed, the RA via the VFM checks the respective databases for verification, after which the details are forwarded to the Key Generator, which generates a public-private key pair. The private key will be put on a smart card, and both the smart card and the public key are sent back to the RA. The RA gives the land owner his private key smart card for safe keeping, and sends the verified land owner's details and his public key to the CA. The CA then issues a digital title deed, complete with the requisite details and the embedded public key. This digital title deed is sent to the directory, and also a copy of the digital title deed is saved in the active certificates database. Any previous deed associated with the piece of land is revoked, and removed from the active directory, and put into the inactive certificates database.

A financial institution wishing to access this service also presents their details to the RA for verification. Once these details are verified via the VFM in the companies' database, the information is sent to the key generator and a private-public key pair is generated. The financial institution is issued with the private key smart card, which will be used for verification as the financial institution accesses the directory. The directory VFM security feature will match the financial institution's private key with the associated public key; if they match then authentication and access is granted.

When a land owner presents their physical title deed to a financial institution, the institution's VFM accesses the directory using their private key smart card. After this, the land owner inputs their private key smart card, and the certificate that has the corresponding public key is retrieved. The financial institution can then compare the details of the digital title deed with those on the physical title deed and verification occurs. If the two do not match, the physical certificate is counterfeit and the applicant is holding the title deed or the private key illegally, and the land registry is notified to put a hold on the piece of land as well as the authorities for further action.

2.9 Conclusion

The public key infrastructure is very instrumental in providing a secure environment for secure exchange of information. Central to the PKI, the certificate authority issues digital certificates which further ensure the authenticity of the identity of not only the participants in the

system but also of all information exchanged. The architecture therefore is robust enough to tackle the problem of land administration in Kenya, and fulfill the objectives set out in this study.

Chapter 3 : Research Methodology

3.1 Introduction

This chapter focuses on the research methodology to be used in this study, and will help to provide an outline that will be used to guide this research. The data that will be gathered through the use of various methods and techniques will be used in the development of the proposed title deed verification model discussed in the previous chapter.

The chapter begins with an outline of the research design, then describes the scope of the study. Next, the chapter provides information on the population, and the chosen method of sampling. The chapter then describes the software development process, the data accuracy and the confidentiality. A conclusion then ends this chapter.

3.2 Research Design

This research will be conducted as an exploratory research study because of the nature of the problem. The advantages of using the exploratory research design as stated by Creswell (2014) are that it increases a researcher's understanding of the subject. This is important because the researcher will be able to study the process of title deed verification, identify the challenges present and therefore develop a solid, well founded solution. Further, exploratory research helps to save on resources because it can flag dead ends early and prevent a researcher from conducting research in areas that are likely to be of no benefit to the research. This will help the researcher to conduct the research in a reasonable time frame and also assist in designing and developing the PKI based verification model for title deed verification.

3.3 Location

This study will be conducted in the central registry, in Nairobi, because of proximity, as well as the similarity in structure of land registries across the country. The ministry of Lands and Physical planning is the overall authority in Land administration matters in Kenya. Within this ministry, the Lands department is tasked with the mandate of registering land transactions, land valuation, land surveying and mapping, adjudication and administration of public and community land. Under this department, there are land registries that are located throughout the country, with the central registry being in Ardhi house, in Nairobi.

3.4 Population

Creswell (2014) refers to the population as an aggregate or totality of all the objects, subjects or members that conform to a set of specifications. In this study, the population includes the following:

Financial institutions: There are 47 registered banks in Kenya, and employ a total number of about 1000 workers in Nairobi. For this study, two of the largest banks will be chosen, a branch for each bank.

The Kenya lands registry**:** The land registries in Kenya operate under the mandate of the Lands department, in the Ministry of Lands and Physical planning in Kenya. There is at least one land registry in each county. The Nairobi land registry has 30 employees that work in the title deeds registration department, and will be the focus of this study.

3.5 Sampling

According to Mugenda and Mugenda (1999), a simple random sample is one in which each member of the population has an equal and independent chance of being selected, while a proportional sample is where the sample size is a fraction of the whole sample size. Proportional random samples of interview subjects will be chosen from the three categories in the population. Mugenda and Mugenda recommend the formula (1999):

nf= n/ (1 + (n/N)) to be used to calculate sample size.

According to the above formula:

nf= desired sample size when the population is less than 10,000,

n= desired sample when the population is more than 10,000,

N= estimate of the population size.

Mugenda and Mugenda(1999) outline that when the population is more than 10,000 individuals, 384 of them are recommended as the desired sample size. According to the above formula, the following were the computed sample sizes:

Land registry workers: The estimated number of workers who work in the title deeds registration department that is relevant to this study is 30, so using the formula, a total number of 28 workers.

Financial institutions: Two branches of financial institutions namely Equity Bank and National Bank were chosen because of the number of their location in Nairobi's central business district and the number of clients they serve per day. The National bank's Harambee avenue branch and Equity bank's Moi avenue branch were chosen. The total number of workers in both branches who work in loan disbursement and Title deed verification is 20. Using the formula therefore, a sample of 19 workers will be chosen, 10 from one branch and 9 from the other.

3.6 Software Methodology

This research will adopt the waterfall software development model. The sequential phases in Waterfall model are outlined in figure 3.1. The advantages of using the waterfall model are that it is simple and easy to understand, which eases the work of the researcher (Predrag et.al (2010)). Further, it is easy to manage due to the rigidity of the model. Based on the scale and complexity of the proposed PKI based title deed verification system, it is also important that model phases are processed and completed one at a time so as to adhere to the timeframe allocated for completion.

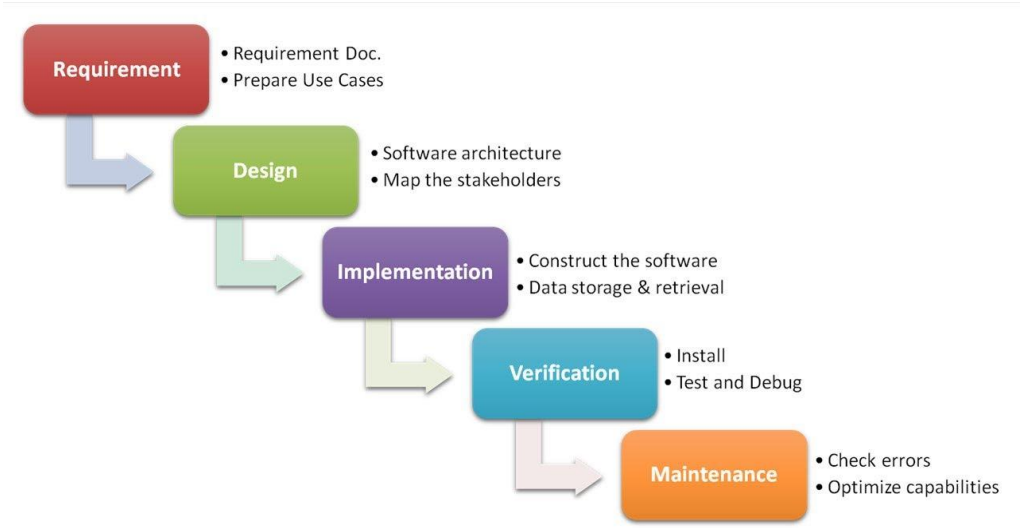


Figure 3.1: Software development life cycle

The following subsections describe the activities that will take place in each phase, and the tools and technologies that will be used.

3.6.1 Gathering Requirements and Analysis

This is the first phase of development where all the requirements are to be gathered, documented and analysis carried out (Predrag et.al (2010)). A requirements feasibility test will be done to determine whether the requirements are testable or not. The deliverables of this phase are the RUD (Requirements Understanding Document). For this study questionnaires are going to be used to collect information from the relevant subjects of study. The reason questionnaires are chosen is because they are relatively easy to analyze, and that a large sample of the given population will be contacted at a relatively low cost (Creswell, 2014). Sample questionnaires are attached on Appendix A, and will be used to obtain information from financial institutions as well as employees at the Nairobi Lands registry.

The Statistical Package for Social Sciences (SPSS version 11.5) will be used to run descriptive statistics such as frequency and percentages so as to present the quantitative data in form of tables and graphs based on the major research questions. The qualitative data generated from open ended questions will be categorized in themes in accordance with research objectives and reported in narrative form along with quantitative presentation. The qualitative data will be used to reinforce the quantitative data.

The deliverable at this phase therefore will be a comprehensive feasibility study of the title deed authentication problem. Additionally, a software requirements document and the preliminary design specification for the solution proposed to solve the title deed authentication problem will also be developed. After analyzing and methodically working through each requirement, dependencies will be handled and plans instituted to mitigate risks.

3.6.2 Software Design

This study intends to use system design tools such as the Data dictionary, data flow diagrams, class diagrams, database schema, process specifications, data models, system models, system flowcharts and input and output design forms. Also Computer-Aided Software Engineering tools (CASE) will be used for implementing these tools. These tools will be useful to design user interfaces, to design data and processes that will constitute the architecture of the

proposed PKI based title deeds verification system. The deliverables at the end of this phase will be design specifications for the proposed title deed authentication solution and a test plan.

3.6.3 Implementation of the system

During systems implementation, this study aims to construct and put the proposed title deed authentication system in place. Application programs shall be written, tested and documented. Also, operational documentation and procedures are completed and approval will be obtained from users and management. The objective of this phase will be to deliver a completely functioning and documented title deed authentication information system that has been reviewed and approved (Predrag, 2010). Final preparations will include the users and performing the actual transition (conversion) from the old system to the new one and training the users. The tools used in this phase will be the Java programming language and also the mongo database whose use will be to store data.

This study will take advantage of structured walkthroughs, testing procedures and automated regression testing. Further, this study will make use of use of CASE tools during this phase, where the system will be tested against user requirements until it obtains an acceptable level of functionality. The deliverable at the end of this phase will therefore be the title deed authentication software program.

3.6.4 Verification, Testing and Deployment

Once the code is developed, it will be tested against the requirements to make sure that the product is actually solving the needs addressed and gathered during the requirements phase. During this phase functional testing like unit testing, integration testing, system testing, and acceptance testing and non-functional testing is to be done. After successful testing the PKI based title deed verification will be put through beta testing. If any changes are required or if any bugs are caught, they will report it to the researcher. Once those changes are made or the bugs are fixed then the final deployment will begin. The deliverables at the end of this phase will be an updated test plan and an updated design specification for the title deed authentication software.

3.6.4 Maintenance

During systems operation, maintenance and enhancements sometimes are requested to resolve problems identified by users during the previous stage. Maintenance changes are then to be made to correct errors or to conform to government or users requirements outlined. Enhancements will include modifications that increase capability and functionality of the system to make it better and more conforming to feedback obtained during the subsequent phases (Predrag, 2010).

The tools used in this study include incremental models consisting of data dictionary, data flow diagrams, process specifications, data models, system models, system flowcharts, structure charts, HIPO (hierarchical input process output model) charts, and input and output design forms. Also, CASE products, application generators, and fourth generation languages will be used by this study because they are readily available in the market and because they ensure that a thorough job is done at a relatively low cost. The deliverable at the end of this phase will be an operating manual for the title deed authentication software.

3.7 Data Accuracy and Reliability

In order to ensure that the collected data is accurate and can be relied upon, this study will use SPSS tools to clean data. In the cases of missing data for example, the use of SPSS Data Validation add-on module will enable the researcher to easily identify suspicious or invalid cases, variables, and data values; view patterns of missing data; and summarize variable distributions. With this knowledge the researcher can determine data validity and remove or correct suspicious cases at his discretion prior to analysis.

3.8 Confidentiality

The data collected as this study is conducted will not be shared elsewhere. The study will be conducted in accordance and adhering to the ethical standards of Strathmore University. Further, an introduction letter signed and stamped by the Dean of the faculty is to be presented to each institution where data will be collected. The letter introduces the researcher as well as gives an assurance to the institution(s) that no confidentiality breaches occur. A sample introduction letter is attached in the appendix. The researcher will explain to the respondents about the research and that the study will be for academic purposes only. It will be made clear that the participation is voluntary and that the respondents will be free to decline or withdraw any time

during the research period. Respondents will not coerce into participating in the study. The participants will have informed consent to make the choice to participate or not. They will be guaranteed that their privacy will be protected by strict standard of anonymity**.**

3.9 Conclusion

This will be an exploratory study that will be conducted in the central registry in Nairobi. The data collection will be on a population that consists of employees in financial institutions and the central land registry. The study will employ the waterfall model in the software methodology, which outlines that a phase has to be completed before another commences. Each phase will use a diverse number of tools which will optimize the success and the timely production of the requisite deliverables. SPSS tools will be used to check for data accuracy, as well as to clean data, and ensure that the collected data can be relied upon. The researcher will conduct the research while adhering to the strict ethical standards of the University, and will safeguard all data collected from any distribution or sharing that is unauthorized.

Chapter 4 : Data Analysis

4.1 Introduction

The aim of this chapter is to critically analyze data that was collected in the questionnaires, and to infer and learn new aspects of the research question as well as to either confirm or negate the aspects of the questions that were already known. For this study, the primary reason for data collection was to confirm whether or not fraudulent title deeds was a genuine problem. Further, the data collection was aimed at finding out whether a software system would help solve this problem, and what features of such a system would be most useful. Lastly, the data collection would help to find out new information.

4.2 Response Rate

A total of 50 questionnaires were handed out to the respondents. Out of these, 47 were returned and only 3 questionnaire remained unaccounted for. Out of the 47 returned questionnaires, 20 were filled out by employees in managerial positions, which accounts for 42.6% of the respondents. Table 4.1 summarizes this information.

Table 4.1: The questionnaire response rate

	Issued Questionnaires	Returned Questionnaires	Response Rate
Managerial positions	20	20	100 %
Subordinate staff	30	27	90 %
Total	50	47	94 %

4.3 What is your position of employment?

A total of 20 respondents (42 %) indicated that they worked in managerial positions, while 27 respondents (58 %) indicated that they worked in non-managerial positions. Both respondents in managerial and non-managerial positions would be of paramount importance to the research because they would give an insight in the policies and processes of their respective organizations on how they conduct title deed verification, challenges faced and how they deal

with these challenges, and whether there is a gap that this research can address. Figure 4.1 summarizes these findings.

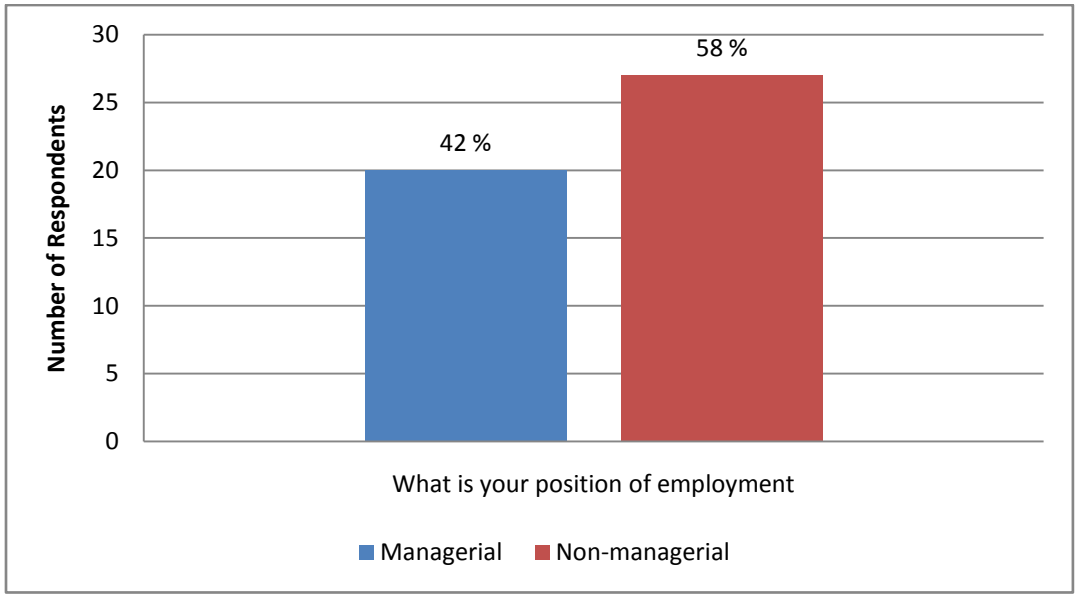


Figure 4.1: The respondents' position of employment

4.4 Does your institution have an information technology system?

All respondents said that their institutions use information technology systems for their business processes. This shows that the respondents' area of work exposes or requires them to have some knowledge of information technology systems. This would be advantageous in that it would be easy to train the employees on the use of the title deed verification system when completed.

4.5 How would you rate your information skills generally?

A majority of respondents indicated that their IT skills were average and above average level. This is an indicator that the use of IT systems at work helped sharpen their IT proficiency. This means that their exposure to information technology systems as earlier observed in section 4.4 has helped to develop their capability in honing and enhancing their information technology skills, which would also be an added advantage when introducing the title deeds verification system when complete. The findings are summarized in figure 4.2.

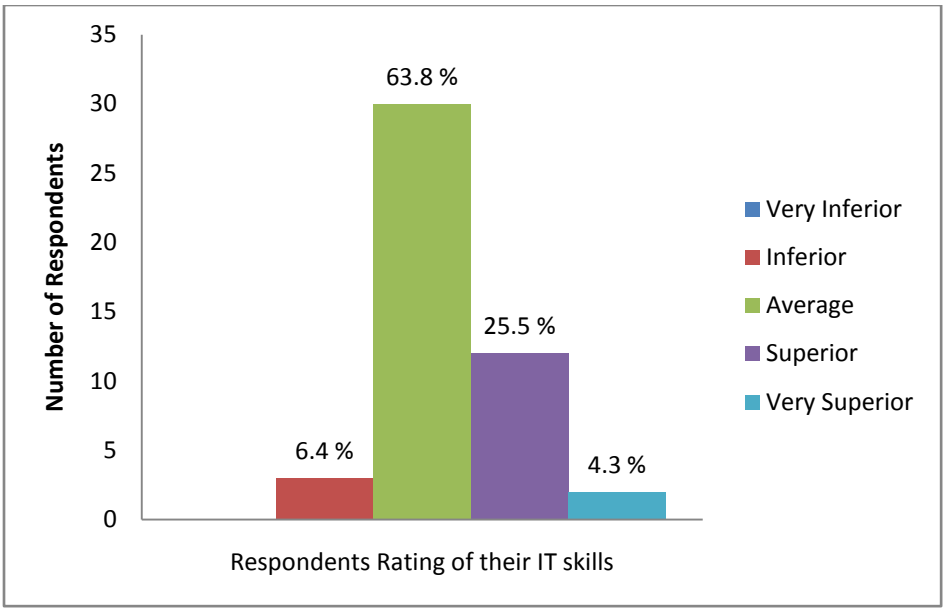


Figure 4.2: Respondents rating of their IT skills

4.6 Where is data in you information system stored?

A total of 59% of respondents indicated that data was stored in a database within the organization's buildings while 41% of the respondents indicated that data was stored in a database at an external location. This signifies that one organization (financial institutions) store their data at external locations, perhaps at a head office or central location, while the other institution (the lands registry) stores its data at that location. Further, it is evident that financial institutions that already access data at external locations already have the infrastructure and capability to securely access the proposed title deed verification system over a network without significant changes or increasing security vulnerabilities. Figure 4.3 summarizes the results.

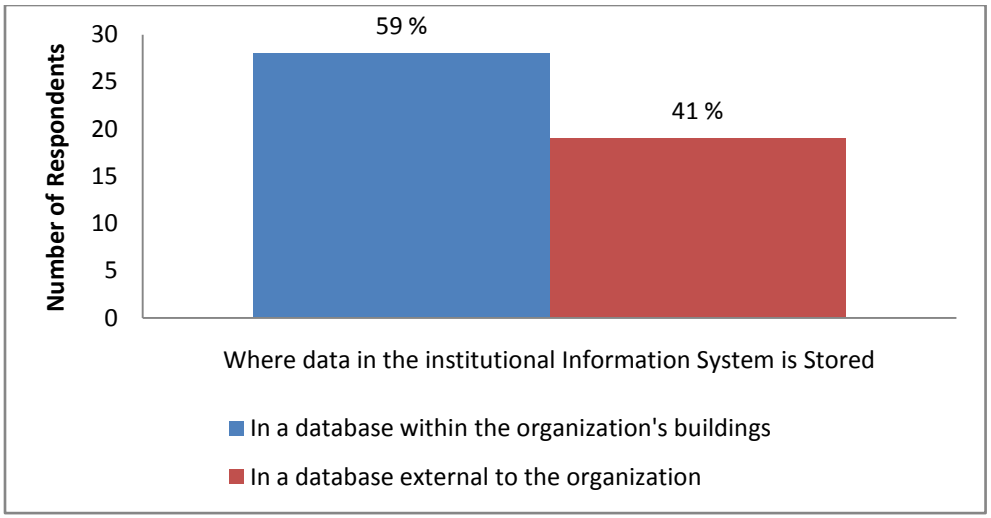


Figure 4.3: Where institutions store their data

4.7 How do you access data in the information system?

All respondents indicated that they access the data using a web browser over a network, as opposed to a stand-alone location. This shows that data is constantly accessed and updated by many people throughout each working day, and that there already exists infrastructure that the proposed title deed verification system can be used on, which makes implementation easy. This also puts forth the need to secure data, and to include multiple layers of security as well as to closely scrutinize data access in a system that has multiple access points.

4.8 Has a case of counterfeit title deeds ever been brought to your attention?

All respondents indicated that at least a single case of counterfeit title deeds had been brought to their attention before. This indicates that there is indeed a problem of title deed counterfeiting presented at these institutions, which further emboldened and gave merit to the proposal to develop a title deed verification system to be used in these institutions.

4.9 What alerted you to the fact that it was a counterfeit title deed?

A majority of the respondents indicated that they only realized that the title deed was counterfeit after a search had been conducted at the lands registry. This shows that the counterfeiting techniques are so advanced and were done in a manner undetectable by the majority, and the only way to reveal it was by conducting a search at the lands registry. This inability to detect counterfeiting also shows that currently title deeds have no significant

distinguishing features that are easy to identify when duplication occurs. The results are summarized in figure 4.4.

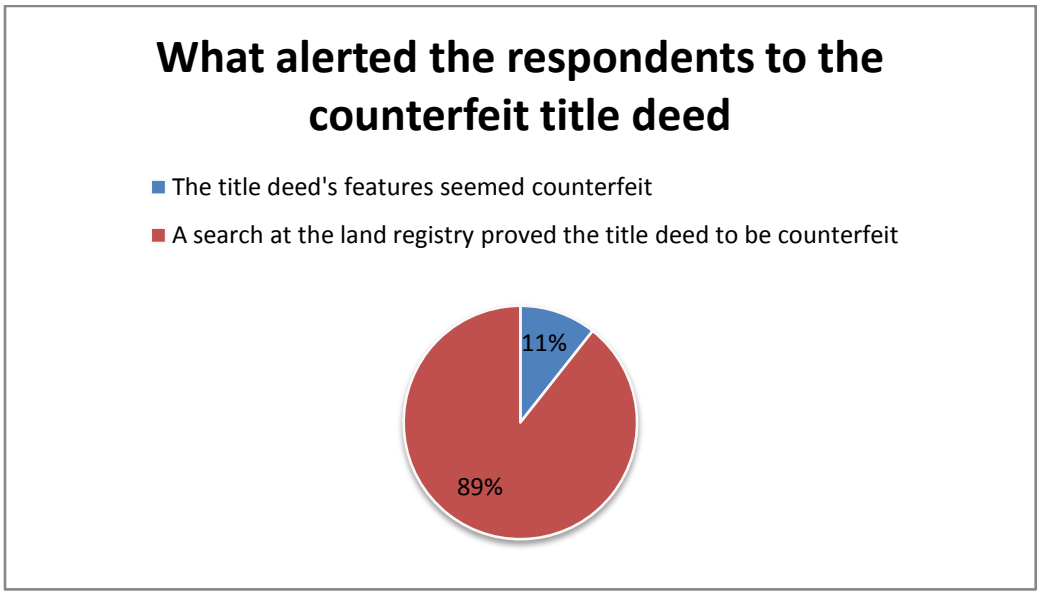


Figure 4.4: What alerted the respondents to the counterfeit title deed(s)

4.10How long does it take to verify the authenticity of a title deed?

A large number of respondents indicated that it takes a minimum of 5 days to verify the authenticity of a title deed, which brings to light the fact that the verification process is slow and experiences challenges. The current system is paper based and has voluminous records, which explains the slow verification times. This laxity also means that the processes in these institutions that rely on the verification of these title deeds have to be delayed by at least five days, a lag which can prove costly especially to financial institutions. Figure 4.5 summarizes these results.

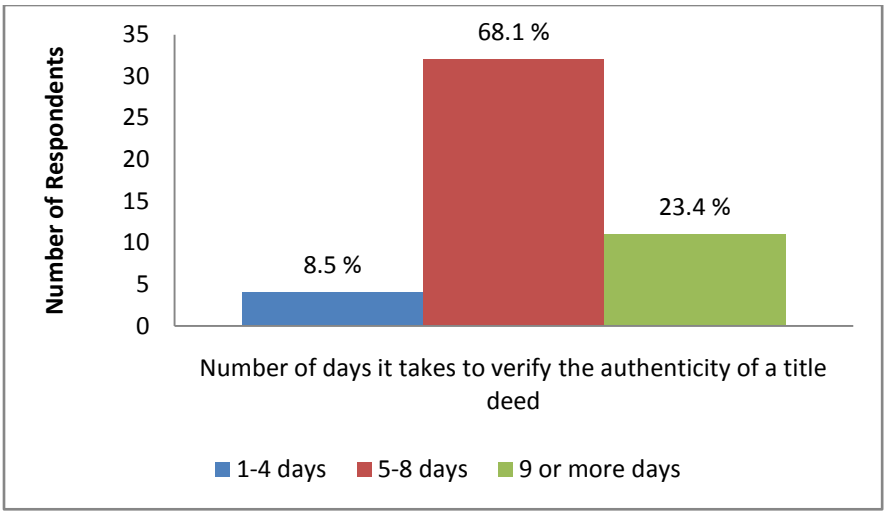


Figure 4.5: Number of days it takes to verify the authenticity of a title deed

4.11 The title deed records are organized and easily accessible in the current system

The majority of respondents disagreed with this statement, which shows that the general assertion is that the records in the current system are not organized and easily accessible. This is as a result of the respondents' interaction with the current verification system, and from the challenges they experienced while trying to verify the authenticity of title deeds. Figure 4.6 gives a summary of these responses.

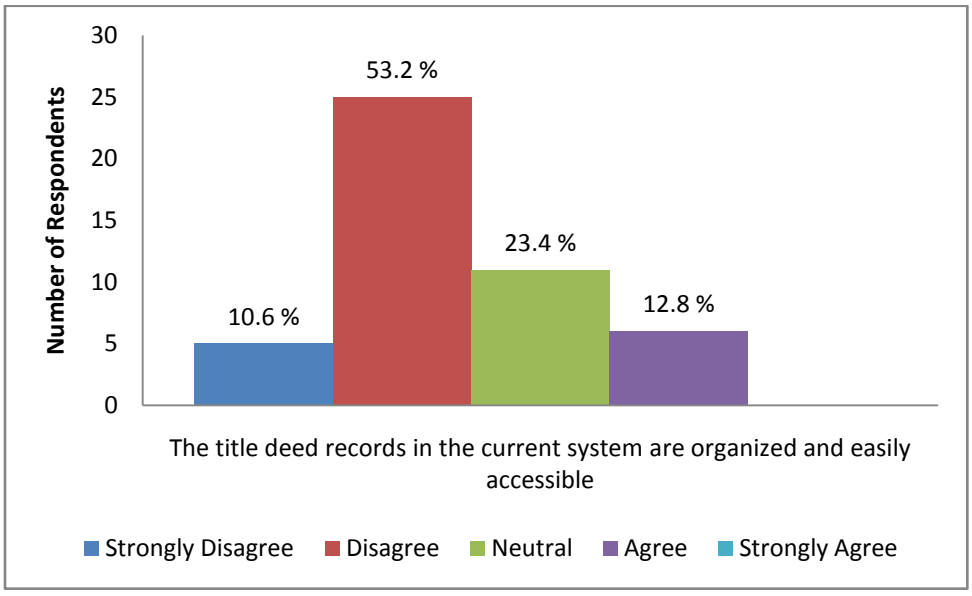


Figure 4.6: Responses to whether title deed records in the current system are organized and easily accessible

4.12 The integrity of title deeds can be interfered with in the current system

A large number of respondents were in agreement with this statement showing that the current system is indeed very prone to alterations that can undermine the integrity of records, which presents a gap. This agreement is indicative of the fact that in their capacities or their jobs, the respondents' interaction with the system led them to believe that vulnerabilities that can undermine integrity of title deed data do exist. These answers are represented in figure 4.7 below.

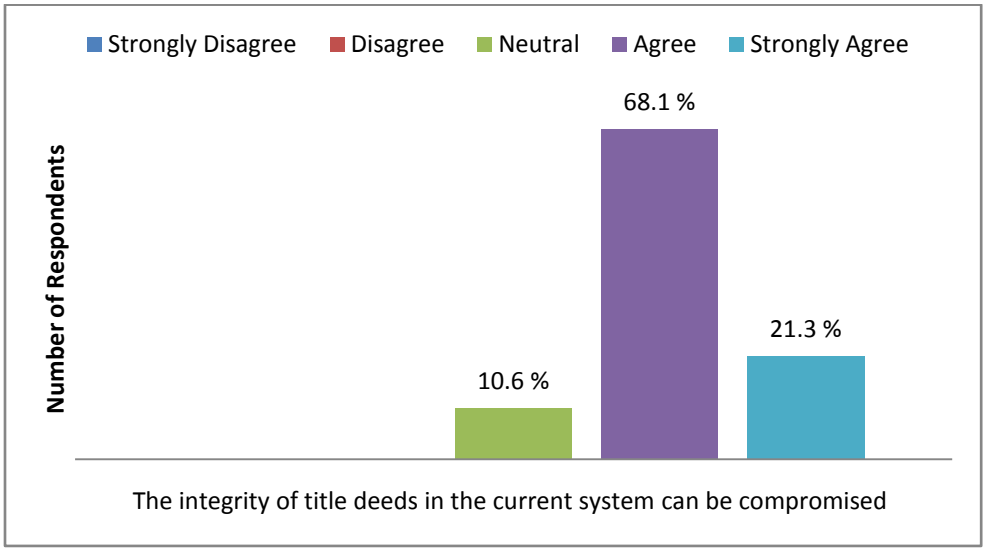


Figure 4.7: Responses to whether the integrity of title deeds can be compromised in the current system

4.13 It is very easy to track changes in title deed details in the system

A majority of the respondents disagreed with this statement, which means that they believe that it is not easy to track any changes made to title deed data in the current system due to the many challenges and shortcomings that are present. Their experience in carrying out a title deed verification had them encounter challenges that slowed the process down, and as seen earlier made the process take an average of five days. The results are summarized in figure 4.8 below.

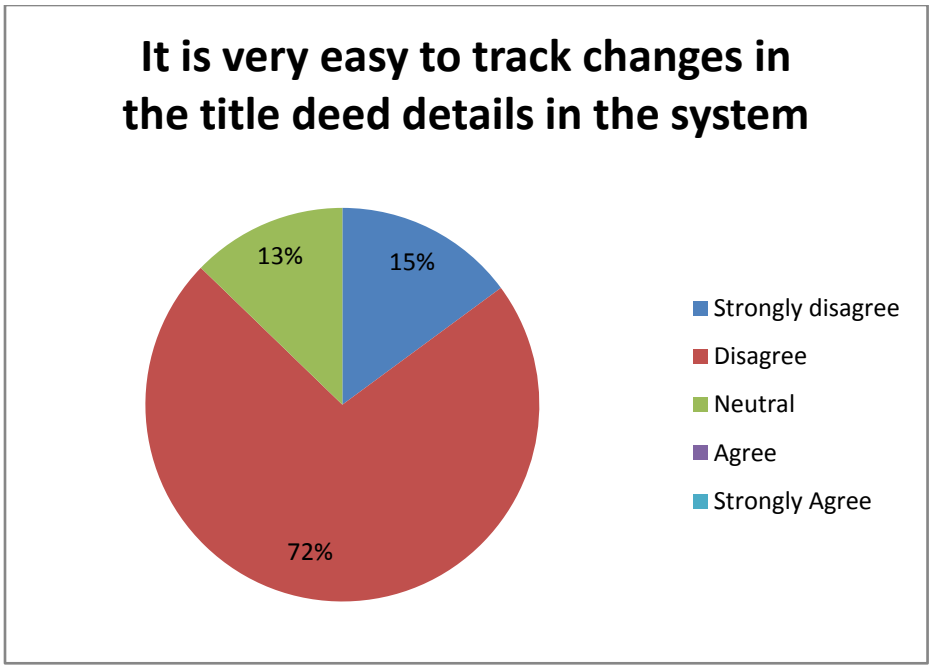


Figure 4.8: Responses to whether it is easy to track changes in the title deed details in the current system

4.14 The current system helps and makes it easy to verify the authenticity of title deeds

A majority of the respondents indicated that they do not believe that the current system makes it easy to verify the authenticity of title deeds; they believed that the many challenges present in the system impede the efficiency and accuracy of the current system to help in the verification of title deeds. The results are summarized in figure 4.9 below.

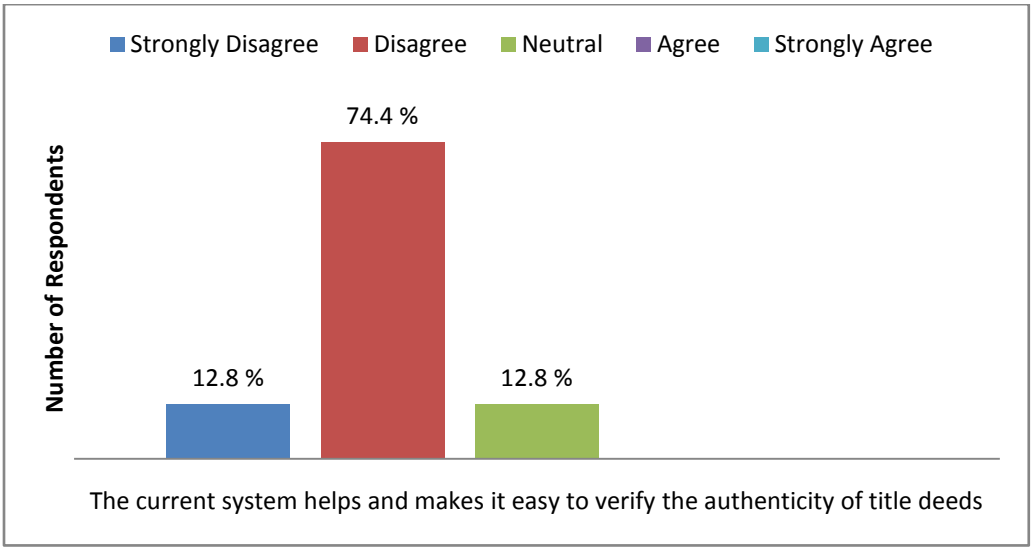


Figure 4.9: Responses to whether the current system helps and makes it easy to verify the authenticity of title deeds

4.15 Currently, title deeds have easily distinguishable features that help spot counterfeit title deeds

Most of the respondents disagreed with this statement, and believed that title deeds do not have easily distinguishable features that can help identify whether a title deed is counterfeit or not. The title deeds do not have clear and hard to duplicate features or seals and therefore it is not very easy to differentiate between a counterfeit title deed and a genuine one. Figure 4.10 below summarizes these observations.

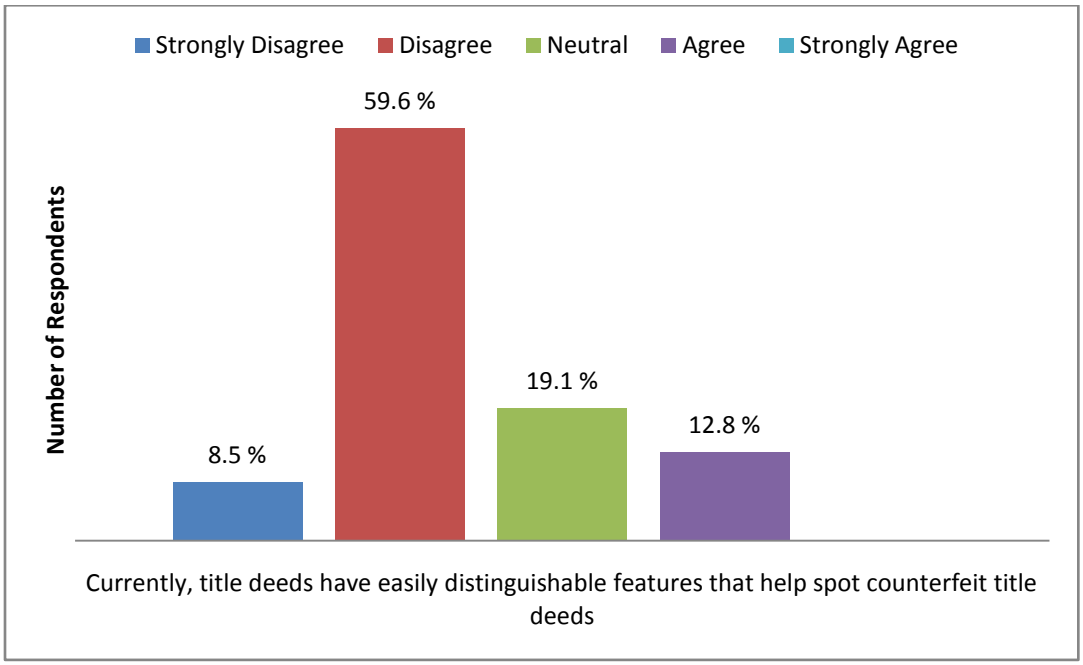


Figure 4.10: Responses to whether title deeds currently have easily distinguishable features that help spot counterfeiting

4.16 An IT system can be used to deal with the challenges in the verification of title deeds

The majority of respondents thought that the advantages that an information technology system brings about could make the title deed verification process quicker, more effective and also ensure that the integrity of data is maintained. Having been in institutions that use information technology systems, and being of average IT proficiency, the respondents believed that there could be real benefits reaped should an IT system be used to streamline the title deeds verification process. The results are summarized in figure 4.11 below.

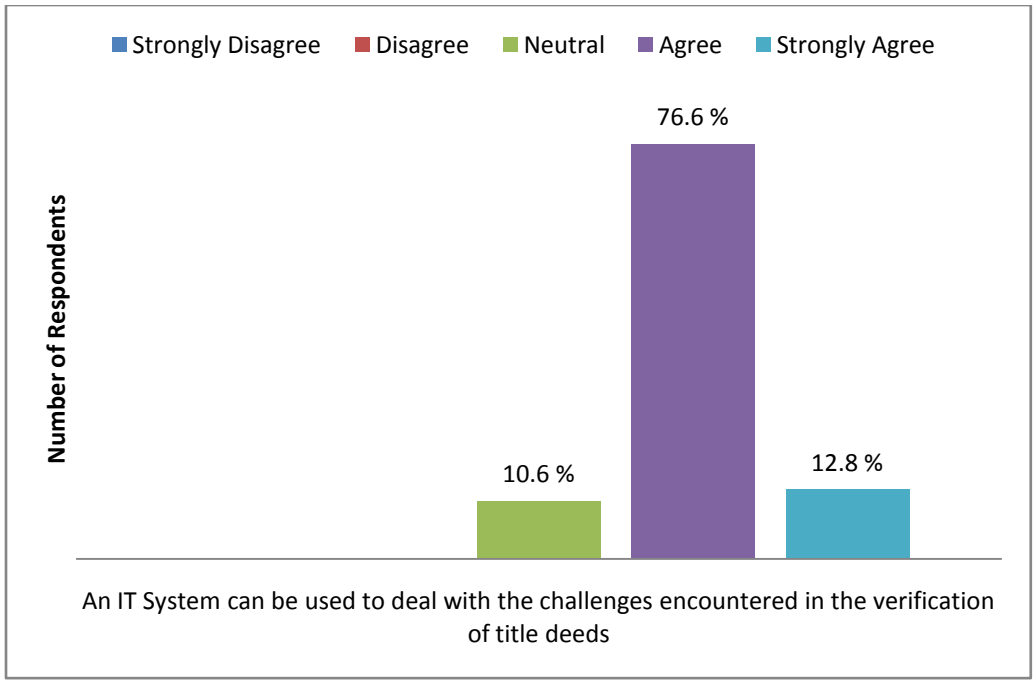


Figure 4.11: Responses to whether the respondents think an IT System can be used to deal with the challenges encountered in the verification of title deeds

4.17 Features in an IT system that would be of benefit to the title deed verification process

The respondents were asked to rank features on an IT system that they believe would be of benefit to the title deed verification process. A majority indicated that a system which is quick, accurate and consistent was what they thought would be of paramount benefit. This is mostly because of the challenges they currently face in terms of the slow speed and inaccuracy of the current system. The respondents also believed a system where non-repudiation was enforced would be of benefit, which is because currently the data integrity is not always ensured. The results are summarized in table 4.2 below.

Table 4.2: Ranking of features of an IT system that would be of benefit to title deed verification

System Feature	Number of Respondents
The system should be make it easy to check for title deeds quickly, accurately and consistently (functionality)	18 (38.2 %)
When title deed data is changed in the system, it easy to know who did it and when they changed the data (non-repudiation)	12 (25.6 %)

Title deeds data in the system has to be secure and cannot be changed without authorization (data security and integrity)	9 (19.2 %)
Only authorized individuals can be able to access private title deed data stored in the system (authentication)	8 (17 %)

4.18 Questions for employees in managerial positions

This question was only to be filled by the respondents in managerial positions. A total of 20 respondents worked in managerial positions as had earlier been indicated. It required the respondents to indicate among the answers given what accurately represented their answer. The answers provided were strongly disagree, Disagree, Neutral, Agree and Strongly Agree.

4.18.1 Organizations have elaborate systems to verify the authenticity of title deeds

The majority of respondents indicated that they either disagreed or were of a neutral opinion towards this statement. This shows that the respondents are unsure of the existence or just how elaborate title deed verification systems in their organizations are. This lack of well-established systems shows that there is indeed a gap in the process of title deed verification. Figure 4.12 summarizes these results.

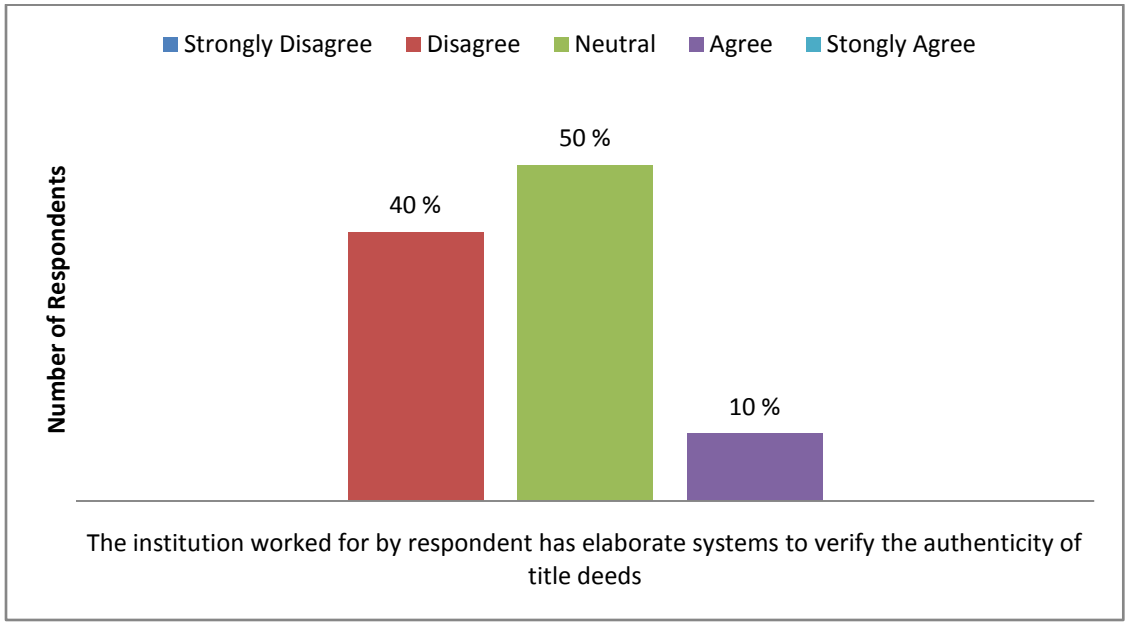


Figure 4.12: Responses to whether the respondents think their respective organizations have elaborate systems to verify the authenticity of title deeds

4.18.2 The Land Registry provides adequate title deed verification services

A majority of the respondents were of the opinion that the land registry does not provide adequate title deed verification services, and that the verification process always had many challenges. The services provided for title deed verification were slow and ineffective, and sometimes produced inconclusive results. Further, the influx of counterfeit title deeds necessitated for a quick and reliable system, which was not present at the land registry. The results are summarized in figure 4.13 below.

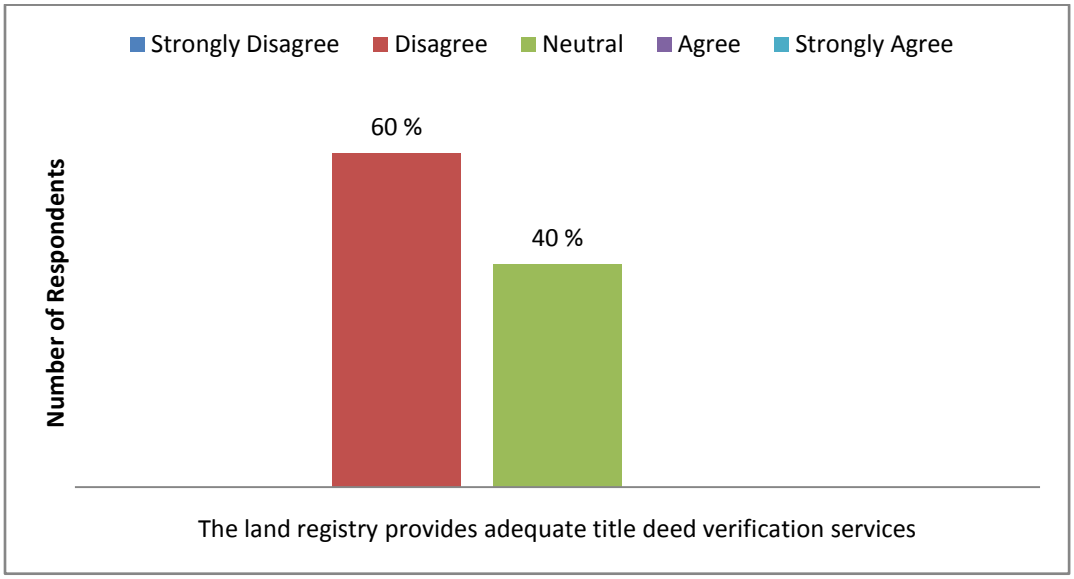


Figure 4.13: Responses to whether the respondents believe that the land registry provides adequate title deed verification services

4.18.3 Do organizations have policies in place to help deal with the issue of counterfeit title deeds?

Many respondents indicated that their sentiments were neutral, which means that they were not completely sure that their respective institutions have elaborate policies that help to deal with the issue of counterfeit title deeds. This shows that indeed the policies in place are not elaborate enough or strong enough to curb title deed counterfeiting. There is indeed a gap present, and an elaborate title deed verification system couple with well instituted policies will help in dealing with the problem of title deed counterfeiting. Figure 4.14 summarizes the responses below.

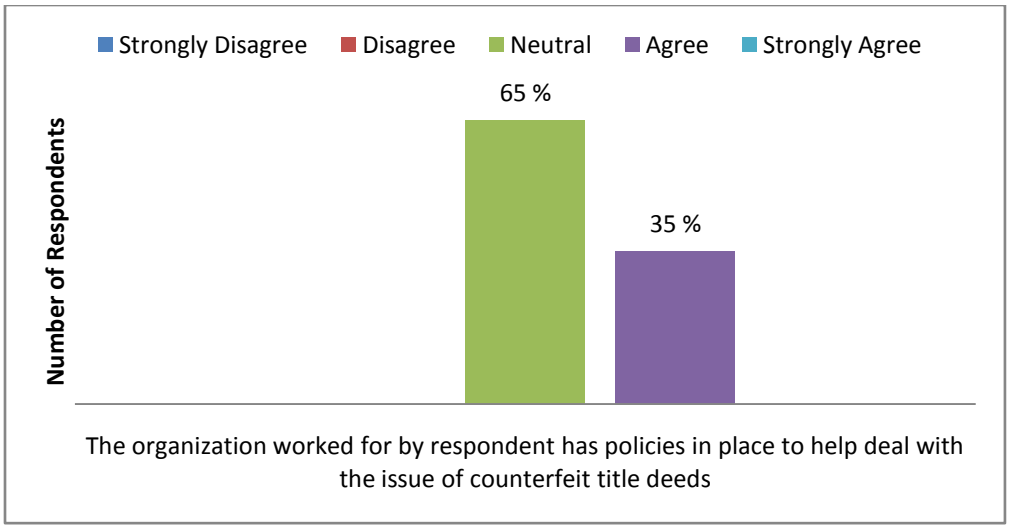


Figure 4.14: Responses to whether the respondents believe that their respective organizations have policies in place to deal with the issue of counterfeit title deeds

4.19 Conclusion

A total of 50 questionnaires were issued, and a total of 47 were returned, which accounts for a 94% response rate. Of these, 20 were in managerial positions, which is a 42% of the respondents. The questions were a closed ended questions; with answer choices given in order to quantify the responses in relation to the total sample. The questionnaire had three sections; a general review section that sought to find out information regarding the challenges faced during title deed verification. The second section sought to find out if an IT system would be of help in title deed verification and also what features of that IT system would be of the most benefit to title deed verification. The last section was only to be filled by respondents in managerial positions, and it sought to find out the challenges of title deed verification and policies and measures in place to curb the same from a managerial (and organizational) stand point.

Chapter 5 : System Design and Architecture

5.1 Introduction

The design stage of any software focuses on the concept flow of the untended functioning of the final product. This process utilizes tools to bring out a graphical representation of the system engine. Waldo (2006) notes that any design task is undertaken to reduce the abstraction of an otherwise complex solution to an engineering problem. The aim of this chapter therefore is to design a prototype for the authentication of title deeds while adhering to the requirements collected and analyzed in the previous chapter.

5.2 System Architecture

Figure 5.1 shows the proposed system's architecture. The system has three zones. Zone one includes the registration authority and the verification module. This zone also has an identity management layer which restricts access to only the authorized land registry clerks and the system administrator and grant the allowed privileges.

Zone two includes the key generator, the certification authority and the systems' databases. This zone also has a more elevated security level because of the data stored and the core processes executed here.

Lastly, Zone three includes the digital title deeds directory to be accessed by financial institutions. This zone also has an identity management layer that grants access to authorized financial institutions to the directory. An overview of the system is shown in figure 5.1 below, and an in-depth look at the components and the modules follows after that.

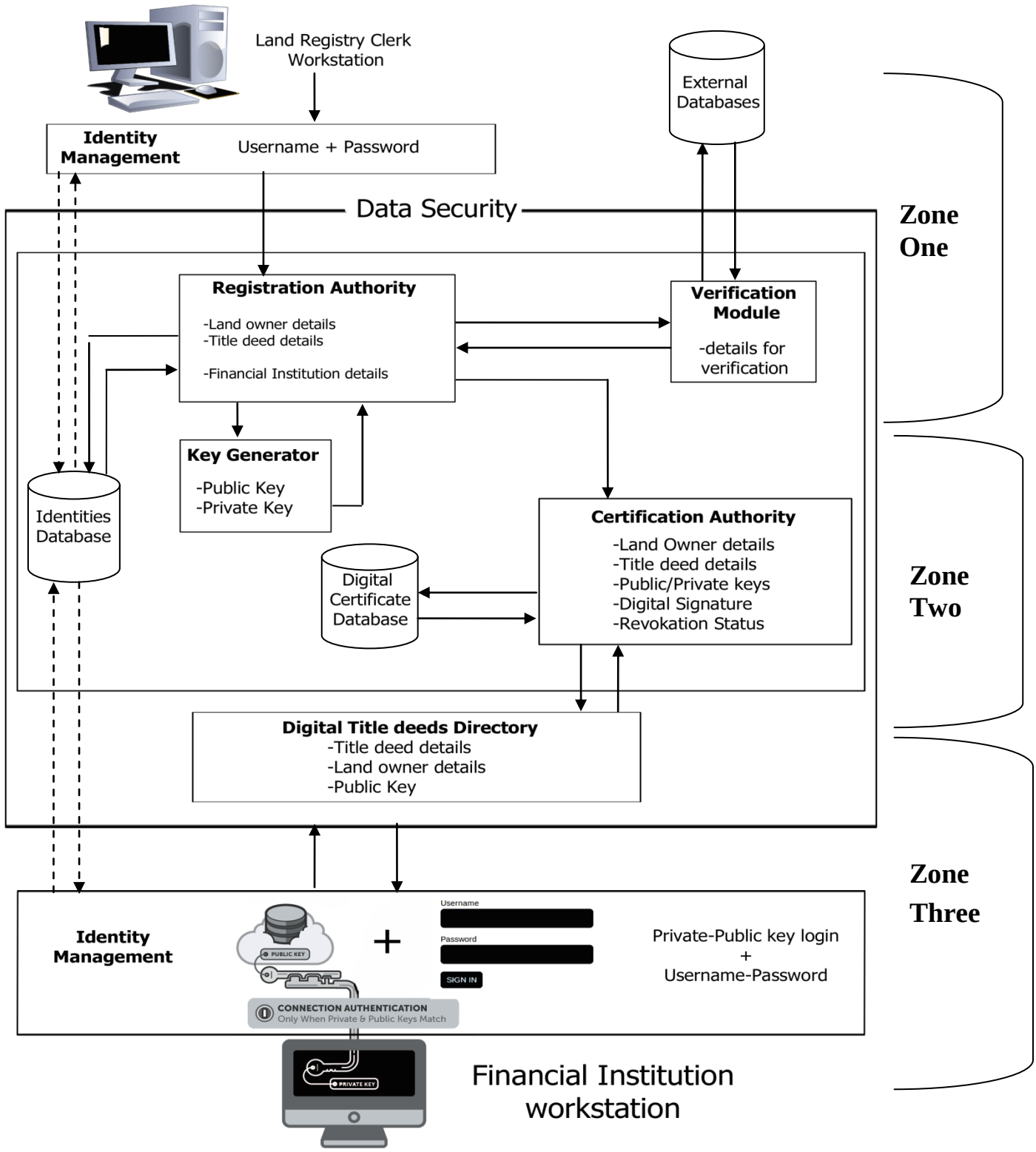


Figure 5.1: The System Architecture

5.2.1 Zone One

1. **The Registration Authority**

The registration authority is responsible for all registration of entities into the system. The entities to be registered include title deed owners, financial institutions and the land registry clerks. Title deed holder's details such as their name, identification number and pin number are captured alongside the details of their corresponding title deed details such as title deed number. Financial institution details to be captured include the name of institution and the institution's pin number. Clerks are also registered into the system and also default login details issued. The registration component then forwards registration details to the verification module for verification purposes. Verified details are then saved and forwarded for use in other components.

2. **The Verification Module**

The verification module's sole purpose is to securely interact with databases external to the system so as to verify details presented by entities during registration. The verification module queries the national identification database to check whether a land owner is a citizen as well as for the correctness of all identification information. Further, the national title deeds database is also queried to check for the validity of a title deed, as well as to see that the piece of land belongs to the title deed holder presenting the title deed. The verification module also checks the business registration database to verify that a financial institutions details presented are correct. Once a verification query is executed, the module returns the results to the registration component for appropriate action.

3. **The identity management module**

This module primarily manages all login processes into the system in zone one and in zone three. There are only two entities that have direct access into the system (or parts of it); the land registry clerks and the financial institutions. The clerks are required to login using their username and password. However, financial institutions' access have two layers of security; a username-password combination as well as a private-public key login. This ensures that external access into the system is highly secure, and that only authorized parties can be able to access the directory. The digital title deeds also contain a public key, and in order for any access to be possible a corresponding private key has to be inputted. The title deed owner is furnished with this private key smart card during the registration process.

5.2.2 Zone Two

1. The Key Generator

The Key generator is responsible for generating a private-public key pair for each verified entity. Once verification of details for title deed holders and for financial institutions has been done, the key generator generates a key pair for each. These keys are to be used by financial institutions to login into the directory, and by the title deed owners to retrieve their respective digital title deed from the directory. Once a key pair is generated, the private key is then put into a smart card, and the two are forwarded to the registration component for further action.

2. The Certification Authority

The certification Authority is responsible for generating a digital title deed using the information received from the registration component. This component also maintains a list of all digital title deeds in a database, as well as broadcasting all active title deeds in a directory. The certification authority is also responsible for revoking digital title deeds as necessary, and deactivating them from the directory.

3. The system databases

The system's databases are where the information in the system will be securely stored. There is an identities database where all information of the entities in the system is stored. This database is important in identities management and also in login processes (for those authorized to login into the system). There is also a digital title deeds database that contains all the digital title deeds issued by the certification authority. These also have a revocation status filled in, and from here they are encrypted and broadcasted onto the directory for retrieval by financial institutions.

5.2.3 Zone Three

1. The digital title deeds directory

This contains all valid digital title deeds that have been issued by the certification authority. The directory is accessed by financial institutions after successful login, and all title deeds are only retrieved if the inputted private key using the smart card matches the public key contained in the correct title deed.

2. **The identity management module**

This works in a similar manner as that in zone one, and manages all login by the financial institutions.

5.3 System Design

5.3.1 The System Partial Domain Model

A domain model is a real world representation of the meaningful conceptual classes of a system, without focusing too much on the software blocks that make up the system. Figure 5.2 below shows the associations that connect these conceptual classes along with the respective attributes for each class. Some of the entities represented include the land owner, the financial institution, the digital title deed and the land registry clerk. These are some of the important entities in the system, each of which has a primary key. Each primary key acts as a foreign key where one entity interacts with another. For example, a land owner's primary key is a foreign key on a digital certificate (digital title deed). The reason foreign keys have been created is to maintain the integrity of data in the system, as well as reduce the likelihood of input errors in the system.

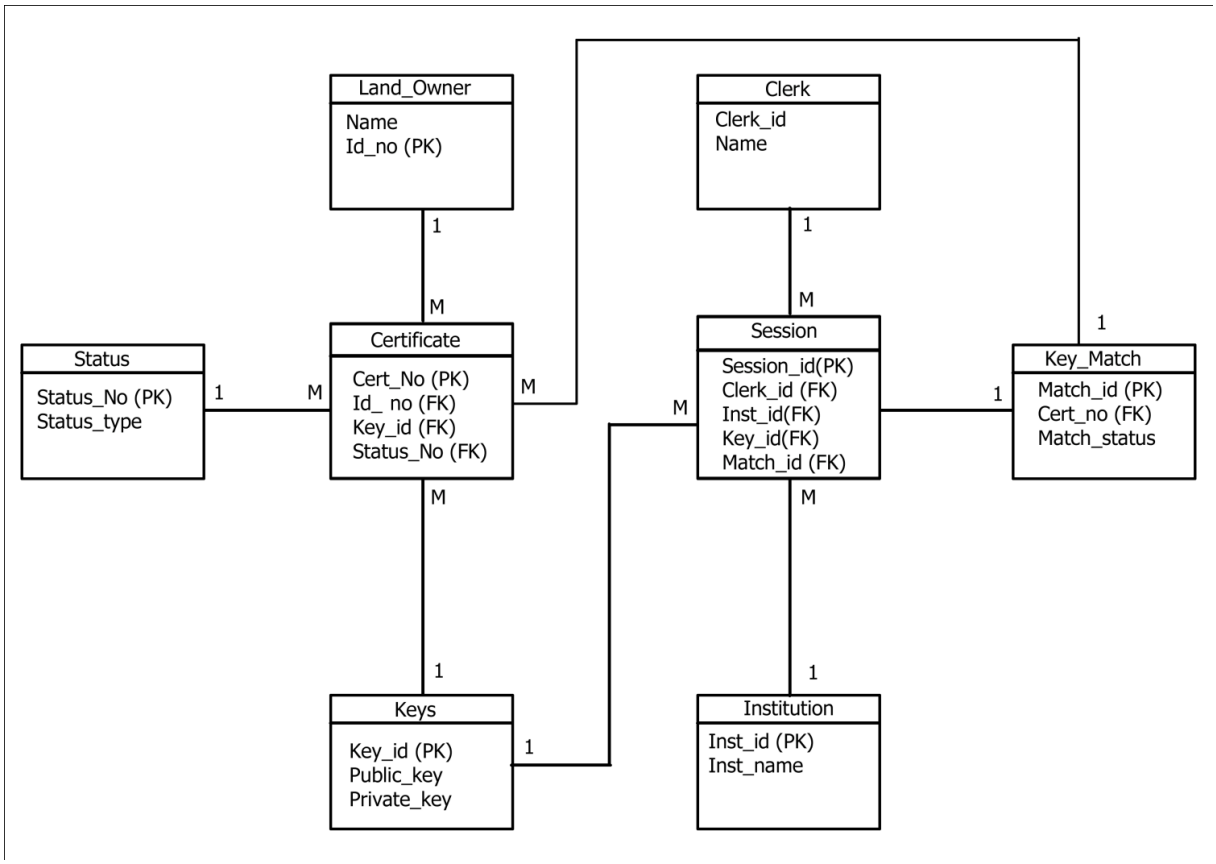


Figure 5.2: The Partial Domain Model

5.3.2 The System Data Flow Diagrams

1. The Context level Data Flow Diagram

The context diagram depicts the big picture of the central system with respect to the entities that interact with it. The key entities that interact with the system are the title deed holders as well as the financial institutions seeking to verify the authenticity of title deeds. Title deed holders present their details and these are the inputs to the system. They consequently receive a private key, an output of the system. Financial institutions also present their details to the system, and get a private key in return. In order to verify a title deed, the institution uses their private key to login, and then receive authorization from the system. Once they input the title deed holder's private key using the smart card they finally get the corresponding digital title deed for verification purposes. Figure 5.3 below shows the context level data flow diagram.

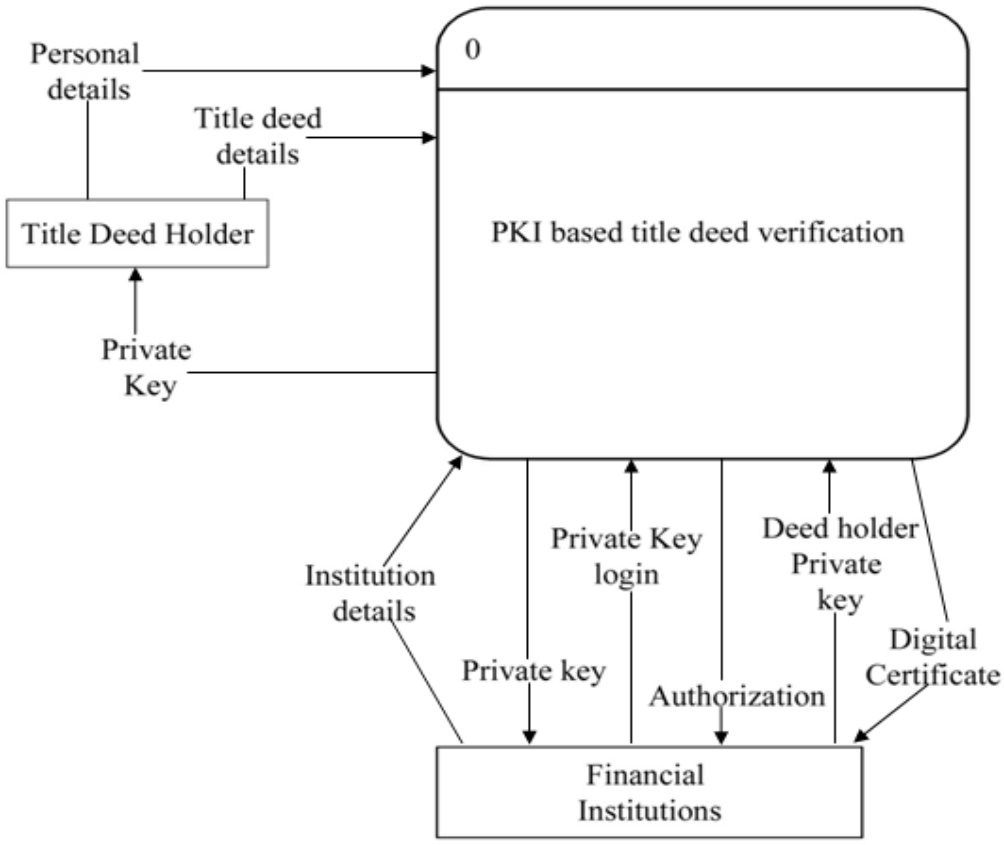


Figure 5.3: The Context Level Data Flow Diagram

2. The level 0 Data Flow Diagram

The level 0 diagram shows the appropriate components and relevant processes for this level. This includes the integral processes, data flows, data stores and the entities involved. The registration process is central to the system, and receives verified details from the external entities, after which it triggers the key generation process so that a private and public key pair is generated. Once these details are saved, the certificate generation process and the directory listing processes occur respectively to ensure that a digital title deed is generated and listed in the digital certificate directory for access by financial institutions seeking verification. Figure 5.4 below shows the level 0 data flow diagram.

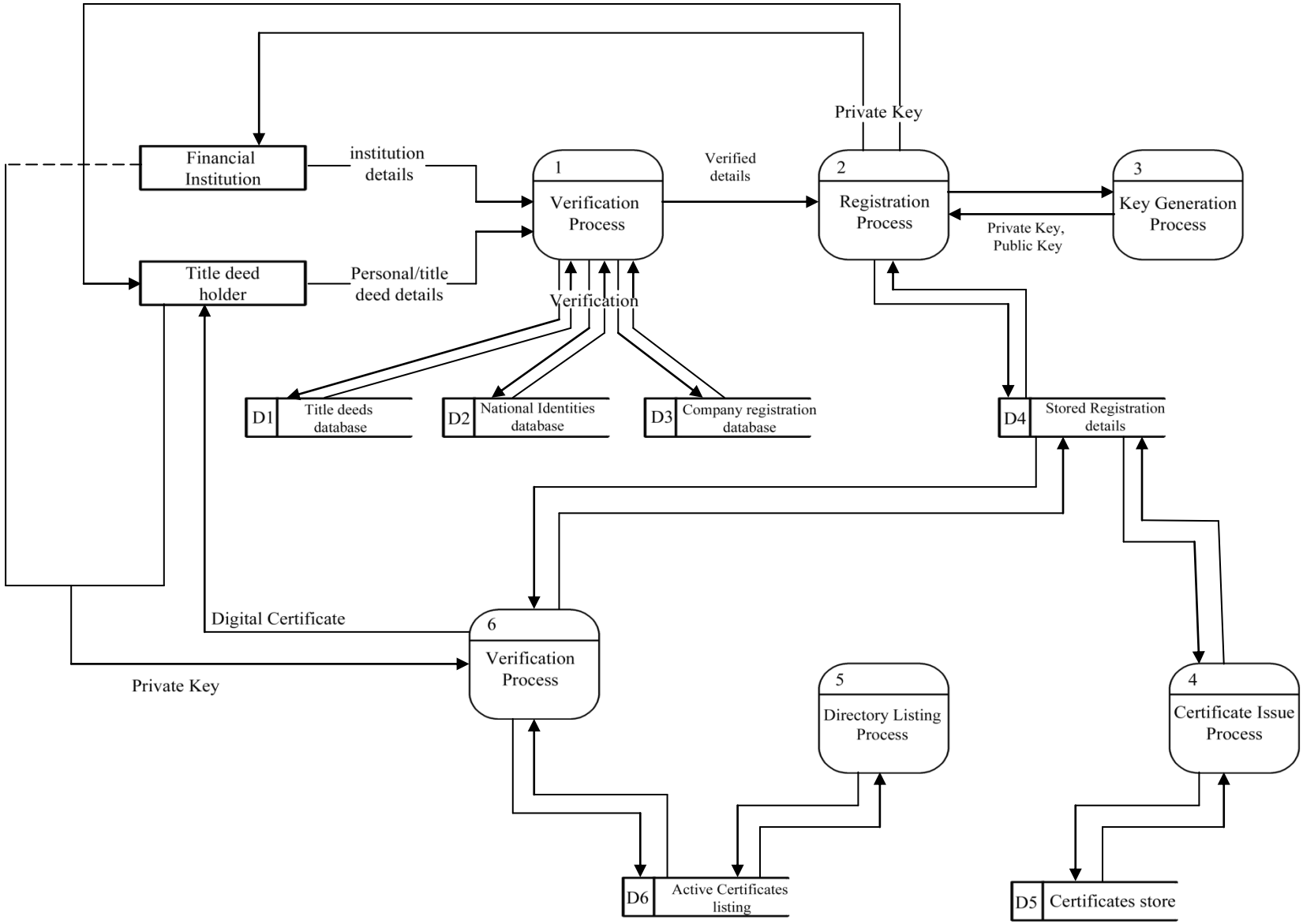


Figure 5.4: The level 0 Data Flow Diagram

5.3.3 The System Use Case Scenarios

These are the descriptions of different scenarios in the system, and outline who the primary actors are and what their inputs and outputs from the system are. These scenarios also give a description of how the system responds to requests from the primary actor, and also describe what a successful transaction is supposed to be.

1. The System Administrator Use Case

The main actor in this use case is the land registry administrator. The administrator is able to login into the system and also update his login credentials. The administrator is able to add a clerk onto the system and verify or disapprove any clerk registration details, as well as issue temporary logon credentials. The administrator is also able to add a land owner into the system, approve or disapprove registration, and also generate a private-public key pair for the same. Further, the administrator is also be able to generate a digital certificate (digital title deed) for an approved land owner, as well as update details onto the directory. Finally, the administrator is be able to add a financial institution onto the system, approve or disapprove registration of the same and issue logon credentials, which include generating and issuing a private-public key pair. The system administrator use case is represented in figure 5.5 below.

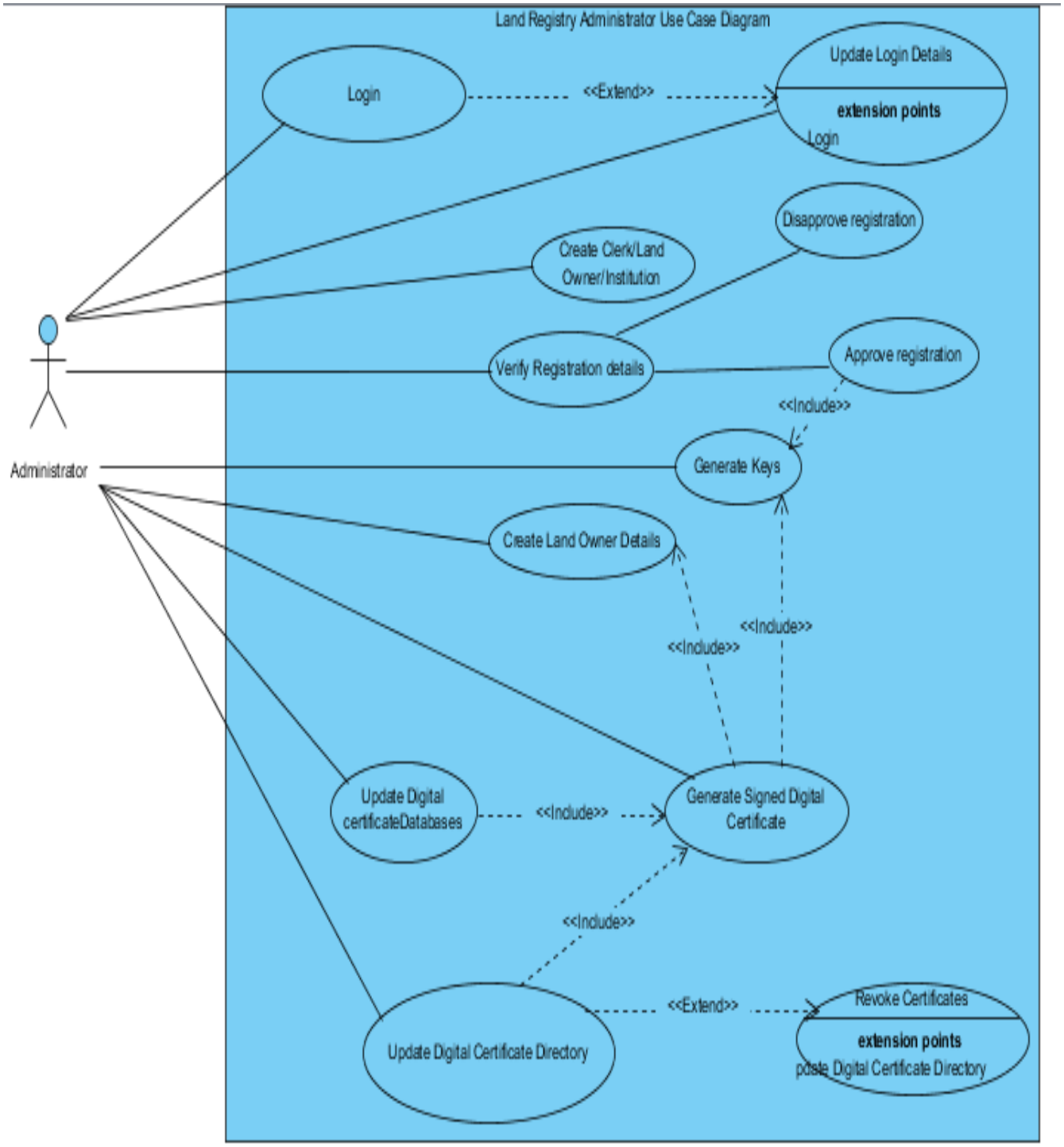


Figure 5.5: The Land Registry Administrator Use Case

2. The Land Registry Clerk Use Case

The land registry clerk is able to login into the system, as well as view and update the personal details. The clerk is also be able to add a land owner, approve or disapprove registration, and then generate and issue a public-private key pair. The clerk is also be able to generate a digital certificate (digital title deed) for an approved land owner, and then update these details onto the directory. Finally, the clerk is able to add a financial institution to the system, approve or disapprove registration, then generate and issue a public-private key pair to an approved institution. The land registry clerk use case is shown in figure 5.6 below.

Figure 5.6: The Land Registry Clerk Use Case

3. The Financial Institution clerk Use Case

A financial institution able to access the directory is already issued with login credentials which include a private-public key pair upon successful registration. The institution then uses these credentials to login into the system, where they are able to view and edit their information. The institution is also be able to access the title deeds directory, and when they enter the private key using the smart card of the land owner they are able to view the corresponding title deed to the land owner's private key entered. The financial institution clerk use case is shown in figure 5.7 below.

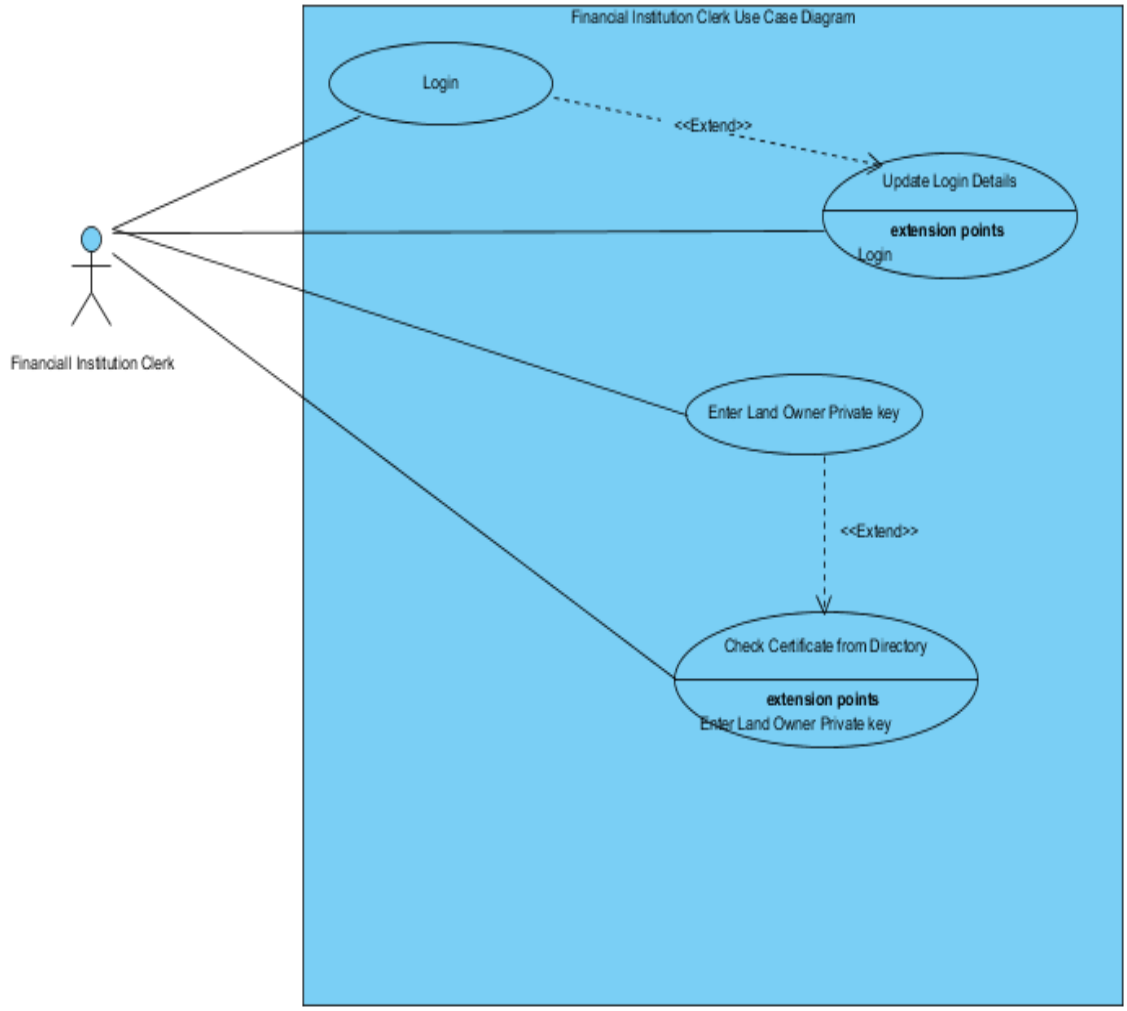


Figure 5.7: The Financial Institution Clerk Use Case

5.3.4 The system Use Case Narratives

1. **Use Case Scenario 1**

Primary Actor: The Land Registry Clerk

Pre-Conditions: The Land Registry Clerk is logged in, properly identified and authenticated into the system

Post-Conditions (Main Success Scenario): A title deed holder is successfully registered into the system, presented with their private key and their digital certificate saved onto the directory.

Flow of Events

1. A national identification card and a title deed of the land owner are available at hand.	
2. The clerk enters these identification details (full name, id number), as well as the title deed information (title deed number), and prompts the system to verify these details.	
	3. The system provides a verification confirmation.
4. The Land registry clerk prompts the system to generate keys	
	5. The system generates a public/private key pair and presents the user with a prompt to save the private key.
6. The Land registry clerk chooses to save the private key	
	7. The system saves the private key into the smart card and presents a confirmation message.
8. The Land registry clerk prompts the system to generate a digital title deed	

	9. The system generates a digital title deed and presents the deed for viewing, and also a confirmation prompt for saving.
10. The clerk confirms the details and clicks to save the details.	
	11. The system saves the digital title deed to the digital title deeds directory, and presents a confirmation message
12. The clerk then issues the saved private key smart card to the title deed holder	

2. **Use Case Scenario 2**

Primary Actor: Land Registry Clerk

Pre-Conditions: The Land Registry Clerk is logged in, properly identified and authenticated into the system

Post-Conditions (Main Success Scenario): A financial institution is successfully registered into the system and presented with their private key smart card.

Flow of Events

1. A business registration certificate is available at hand	
2. The clerk enters the business identification details (full name, pin number) and prompts the system to verify these details.	
	3. The system provides a verification confirmation.
4. The Land registry clerk prompts the system to generate keys	
	5. The system generates a public/private key

	pair and presents the user with a prompt to save the private key.
6. The Land registry clerk chooses to save the private key	
	7. The system saves the private key into a smart card and presents a confirmation message.
8. The Land registry clerk prompts the system to save the details and generate temporary login credentials	
	9. The system saves the details, and generates a temporary logon credentials. The system prompts the user to save the credentials.
10. The clerk confirms the details and clicks to save the details.	
	11. The system saves the details and presents a save confirmation message
12. The clerk then issues the saved private key smart card and saved logon credentials to the financial institution	

3. Use Case Scenario 3

Primary Actor: Financial Institution Clerk

Pre-Conditions: The Financial Institution is registered into the system and issued with logon credentials as well as a private key.

Post-Conditions (Main Success Scenario): After successful authentication, the financial institution clerk is able to access the directory and successfully retrieve a title deed.

Flow of Events

1. A successfully registered title deed holder's national identification card, the physical title deed and the issued private key smart card are at hand.	
2. The clerk enters the logon credentials (username and password).	
	3. The system confirms that the credentials are valid and prompts the user to enter their private key smart card onto the system slot.
4. The clerk enters the private key smart card onto the system slot	
	5. The system confirms that the private key is valid and allows the financial institution to access the digital title deeds directory.
6. The clerk prompts the title deed holder to input their private key smart card onto the system slot.	
	7. The system checks the directory and displays the corresponding digital title deed, and prompts the user to confirm whether to save or discard.
8. The clerk saves the digital title deed	
	9. The system saves the digital title deed.
10. The clerk exits the system	
	11. The system exits, and displays a successful exit confirmation message.

5.3.5 The System Sequence Diagram

The system sequence diagram shows the sequence of processes between all the system users or actors, and the system itself. The main entities interact with the system are the system administrator, the land registry clerk and the financial institution clerk. The system administrator registers the land registry clerk, upon which the system gives a prompt to view, edit and approve these details.

The land registry clerk is then be able to add a financial institution and generate keys, each time getting a corresponding message from the system. The land registry clerk also is able to add a land owner using personal and title deed details, generate the corresponding keys then generate a digital title deed, each time getting the corresponding feedback from the system.

The financial institution is be able to login into the system using credentials login as well as using their private key smart card. Once they enter the land owner's private key smart card, retrieval of the corresponding digital title deed occurs for comparison. Figure 5.8 shows the proposed system's sequence diagram.

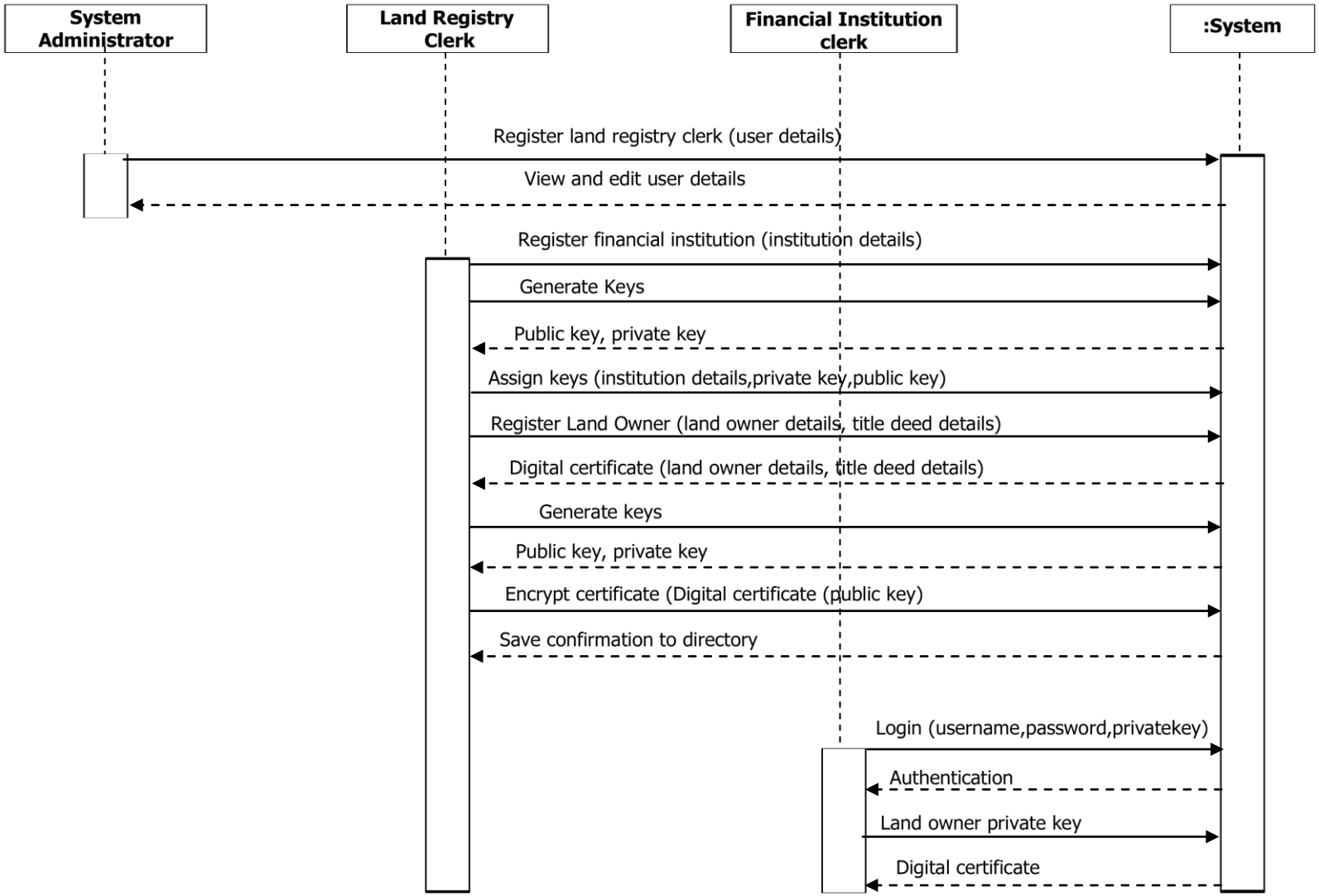


Figure 5.8: The System Sequence Diagram

5.4 Network design

The following network infrastructure plan is be used to implement the title deed verification system in a secure and accessible environment. The system is hosted on an internal server on a local area network (LAN). However, the LAN is subdivided into two; an internal protected network and an internal Demilitarized zone (DMZ). The DMZ is where the title deeds directory server is placed, and financial institutions can access it. Before they get to it however access is limited using a router and an external firewall. The internal protected network holds the application servers and the database containing crucial information, and is separated from the rest of the network by an internal firewall. The workstations in the land registry are hosted in this part of the network. Finally, there is a network intrusion detection system that monitors the whole network for any anomalies. Figure 5.9 illustrates the network architecture.

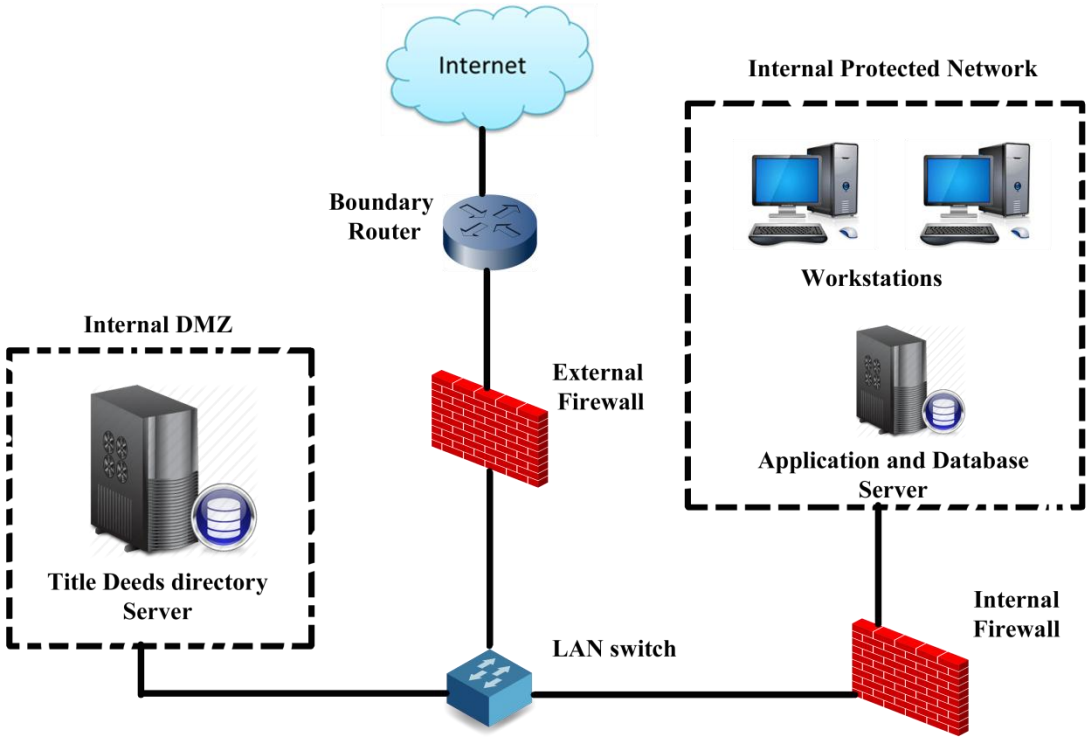


Figure 5.9: The Network design

5.5 Security Design

5.5.1 User Access

There are three access levels into the proposed system. There is the administrator access, which accesses all parts of the system. The administrator is able to perform all tasks that all other entities in the system can perform, primarily to check functionality and to conduct maintenance onto the system. However, all login and access is monitored and logged. The administrator has to use a username and a password to access the system. The password is enforced to include lowercase and uppercase letters, at least a number and should also be a minimum of eight characters long.

There is also the land registry clerk access; this access is only be allowed specific access onto the system. The land registry clerk also uses a username and a password enforced to include lowercase and uppercase letters, at least a number and also should be a minimum of eight characters long.

Lastly, there is the financial institution access, and this access is only allowed to access the digital title deeds directory. The login access is two layered; there is the use of a username-password combination, as well as a private key login. The private key and username-password are issued upon successful registration. This multilayered login is necessary for added security of the system's data.

5.5.2 Network Security

As shown in figure 5.9 in the network design, there are two firewalls in the network to create layers of security. Further, the network is segmented to include a demilitarized zone (DMZ) where the title deeds directory is hosted and the internal protected network, where the system and its database are hosted. This separation makes it harder for intruders to penetrate via the network and compromise data.

5.5.3 Security Protocols

A protocol is a set of rules and conventions that define the communication framework between two or more agents. These agents, known as principals, can be end-users, processes or computing systems. The system is accessed over a web browser, and therefore the HTTPS protocol is used. HTTPS is the protocol for accessing a secure Web server when authentication and encrypted communication is possible, and does so by encrypting the session data using the

SSL (Secure Socket Layer) protocol ensuring reasonable protection from eavesdroppers and man-in-the-middle attacks.

5.6 System Wireframe

Upon login, the administrator, the land registry clerk and the financial institution clerk are able to view and edit their personal details. The administrator is able to add a clerk into the system, add a title deed holder and even a financial institution. Further, the administrator can verify details of added persons, generate keys and digital certificates and also access the title deed directory.

The land registry clerk is able to view and edit their details, add a financial institution and a title deed holder, verify details, generate keys and digital certificates and also access the title deeds directory.

A financial institution upon login is able to view and edit their details, and once authenticated they can further access the title deeds directory. Figure 5.10 shows this information in a wireframe.

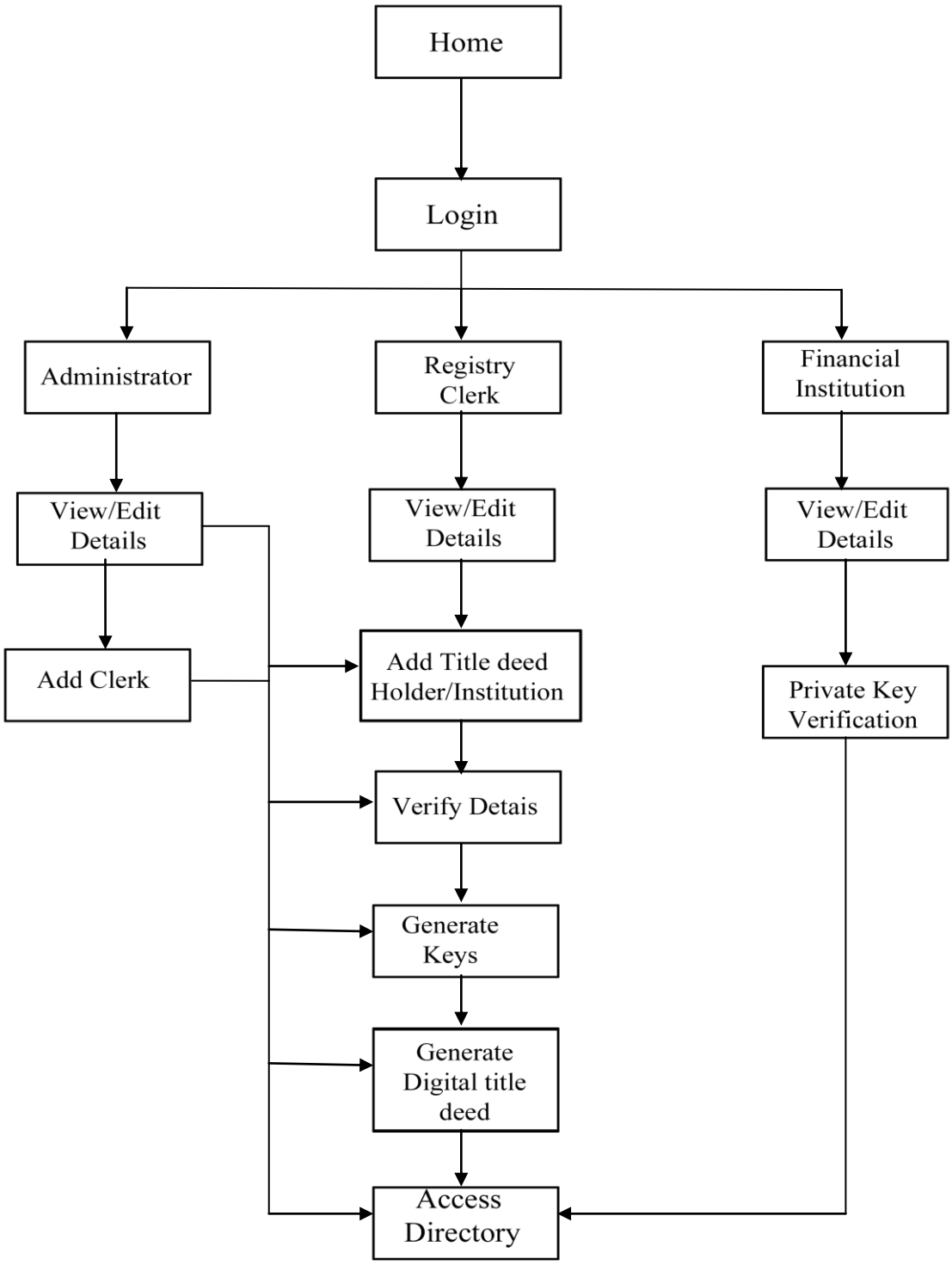


Figure 5.10: The System Wireframe

Chapter 6 : Implementation and Testing

6.1 Introduction

The title deed verification prototype will be used by many individuals, and therefore needed to have features that enhance the user experience. Myers and Rosson (2000) outline the need to spend time focusing on the user interfaces and system usability, and stress that it is important to do so since the efficiency with which the end user achieves their desired result from the system is increased as a result. This chapter therefore focuses on the tools, requirements and functionalities achieved while developing the proposed title deed verification prototype.

6.2 Prototyping tools used

The proposed title deed verification prototype was developed using the Java programming language. In order to improve concurrency while using a minimum number of kernel threads, the vert.x toolkit was used. This tool kit enables the system to scale up, and to handle multiple requests and multiple transactions without having to increase the hardware capacity. The title deed verification prototype was expected to have many title deed verification requests in order to ease the current burden on the Land registry which necessitated its robustness and scalability with minimum interferences. In addition to this, the itext library was also be used which enables the title deed verification prototype to generate digital title deeds, and to further encrypt and decrypt them. The databases used were a combination of Mysql databases and Mongodb (no transactions database), in order to ease and quicken storage and retrieval of data.

6.3 System Requirements

The minimum system requirements for the development of the title deed verification prototype were as follows:

1. A laptop computer with Windows 7 Operating system (64bit) installed.
2. The computer's processor speed was 3.4 GHz, a minimum RAM of 2GB, and minimum hard disk space of 20 GB.

6.4. System Functionality

The prototype development was primarily focused on functionality, as well as easy to use interfaces. This section looks at some of the functionalities of the key interfaces of the title deed verification prototype achieved.

6.4.1 Login

The system was designed to have a simple login interface. Upon entering user details, the system would be able to internally verify the credentials as well as determine what access level the user has, and then direct the user to the section of the system they were authorized access. The login interface can be seen in Appendix D.

6.4.2 Dashboard

Once an administrator or a land registry clerk successfully logs in to the system, a landing page showing the different main processes appears. This dashboard gives the user options whether to register a new title deed holder, or a new financial institution, to view digital certificates or to generate keys. This interface also allows a user to view keys already generated. The interface also shows a list of the latest logins to the system. A snapshot of the interface is shown in Appendix D.

6.4.3 Details Verification

Once a title deed holder has been registered, the personal details have to be verified by querying the external databases. By filling out the requisite details, a clerk is able to verify the validity of a title deed and the title deed holder's personal details. This is shown in Appendix D.

6.4.3 Key Generation

Once a title deed holder's details are verified, the clerk has to generate keys so that the public key can be embedded onto the digital title deed and the private key can be put into a smart card and issued to a title deed holder. Key generation is done using the RSA algorithm. Once a clerk generates the keys, a success message appears in un-editable fields on the form as shown in Appendix D, but the keys remain hidden. Upon saving, the private key is saved onto a smart card, and the public key forwarded for digital title deed generation.

6.5 System Security

6.5.1 User Access Levels

Table 6.1 shows the access levels that were created from the various categories of individuals allowed to interact with the system, and the login credentials that they were required to use.

Table 6.1: User Access Levels

User Access Level	Login Credentials	Credentials Constraints
System Administrator	Username and Password	Password has to be at least eight characters long. It should also include a lowercase and uppercase letter and a number.
Land Registry Clerk	Username and Password	Password has to be at least eight characters long. It should also include a lowercase and uppercase letter and a number.
Financial Institution Clerk	Username and Password, Private Key	Password has to be at least eight characters long. It should also include a lowercase and uppercase letter and a number. The private key is issued upon successful registration. At login, it must match the corresponding public key stored in the system. If one level of security fails, login is denied.

6.5.2 Key Generation, Encryption and Decryption

In order to be able to create a digital signature, or to encrypt a digital title deed, a private and a public key is needed. The prototype is developed using java, and special java classes are imported in order to perform key pair generation using the RSA algorithm. The classes imported are java.io.FileOutputStream, java.io.IOException,java.security.KeyPair, java.security.KeyPairGenerator, java.security.NoSuchAlgorithmException, java.security.NoSuchProviderException, java.security.PrivateKey and java.security.PublicKey. These key pairs form the foundation on which the proposed system is founded for encryption and decryption, as well as for login purposes for the financial institutions access. The keys generated are 1024 bits in length. Three important methods used are Generatekeys(), SignLicense () and

VerSig(), which are used to generate keys, sign/encrypt a digital title deed and verify the signature/decrypt a digital title deed respectively. These methods use internal Java libraries to perform these tasks. Once title deed holders' details are verified and saved and digital title deeds generated, they are converted and saved in the PDF format to make them easier to encrypt and decrypt, as well as to broadcast in the title deeds directory. A sample of the code used to perform these tasks is shown on Appendix 3.

6.6. System Testing

6.6.1 Unit testing:

Unit testing is testing performed on standalone modules or components to ensure that they have been developed correctly. Thorough test cases and scenarios were created to test the various modules in the title deed verification prototype to find out whether they performed as expected and whether they met the user requirements. Table 6.2 shows a sample unit testing scenario for the login module and the title deed verification module.

Table 6.2: Sample Test Cases

Test Scenario	Test Case	Test Steps	Test Data	Expected Results	Actual Results	Fail/Pass
Check Land Registry Login Functionality	Check response on entering valid username and password	1.Launch Application 2. Enter Username 3. Enter Password 4. Click Login button	Username: admin Password: Admin@@1	Login must be successful	Login was successful	Pass
Check Land Registry invalid Login Functionality	Check response on entering invalid username and password	1. Launch Application 2. Enter Username 3. Enter Password 4. Click Login button	Username: xxxx Password: hsjddb	Login must be unsuccessful	Login was not successful	Pass
Check Land Registry Invalid Login Functionality	Check response on entering no username and password	1. Launch Application 2.. Click Login button	No username and password	Login must be unsuccessful	Login was not successful	Pass

Check verification module functionality	Check response on entering valid title deed holder credentials	1. Enter title deed holder personal identification number 2. Enter title deed number	1.ID number: 24673677 2. Title deed number:234/W87/199	Credentials must be found to be correct	The credentials were found to be correct	Pass

6.6.2 Integration testing

Once each module had successfully gone through unit testing, all were combined together as a whole and to test how they work together, which constituted the integration testing of the prototype. Their interconnectedness and efficiency as well as ability to securely exchange data was tested to ensure that the prototype performed as designed, and that given the inputs, the outputs were as expected. Once integration testing was successfully completed, the prototype was introduced to respondents for usability testing.

6.6.3 Usability testing

In order to test the usability of the prototype, 5 respondents from the land registry were allowed to use the prototype and then had to answer several questions. The sample of the questionnaire used is attached in the appendix, and the results for the usability test are represented in table 6.3 below.

Table 6.3: Usability Test Respondents' results

PART 1	Respondent 1	Respondent 2	Respondent 3	Respondent 4	Respondent 5
1. Name (Optional)	N/A	N/A	N/A	N/A	N/A
2. What is you IT proficiency level?	Above Average	Average	Average	Above Average	Above Average
PART 2					
3. What is your opinion of the user interfaces of the title deed verification prototype?	Appealing	Appealing	Appealing	Appealing	Appealing
4. What was the level of difficulty of use of the title deed verification prototype?	Easy	Fairly Easy	Fairly Easy	Easy	Easy
5. Do you think much training will be needed in order to learn how to use the final system?	No	Minimal Amount	Minimal Amount	No	No
6. Do you think the prototype has adequate security features?	Yes	Yes	Yes	Yes	Yes

7. Do you think the prototype adequately performs title deed verification?	Yes	Yes	Yes	Yes	Yes
8. Do you think the title deed verification prototype was exhaustive in addressing the difficulties associated with title deed verification?	Fairly exhaustive	Fairly exhaustive	Fairly exhaustive	Exhaustive	Exhaustive
PART 3					
9. Do you think the title deed verification system would improve the title deed verification process?	Yes	Not Sure	Yes	Yes	Yes
10. Would you recommend the adoption of the title deed verification system by the relevant stakeholders once development is complete?	Yes, But with improvements	Yes, But with improvements	Yes, But with improvements	Yes, But with improvements	Yes, But with improvements
12. What improvements would you like to see implemented in the title deed verification prototype?	RESULTS SHOWN BELOW				

The following were the recommendations made by the respondents to the usability test questionnaire. The results exclude recommendations repeated by respondents.

1. Improve the color scheme of the prototype and the interface styling to match the color schemes of the organization, and of other systems currently in use.

2. Include a feature to increase and decrease the fonts on the system to accommodate individuals who may have difficulties in seeing the fairly small fonts of the system.

3. Improve the way private keys are inputted into the system to be an automatic method, because it may be a challenge for people to remember the keys.

Chapter 7 : Discussions, Conclusions and Recommendations

7.1 Introduction

This chapter discusses the problem, the objectives, the prototype developed and the findings of this research, and helps to show how the findings help to meet the objectives of this research. This chapter also outlines the contribution to research and also gives the challenges encountered. Finally, the chapter outlines the conclusions drawn, the recommendations and suggested areas for further research.

7.2 Discussion of the Research

The title deed verification process in Kenya is slow and inefficient because of the current paper based system being used. As a result, there has been an influx of counterfeit title deeds, which has forced financial institutions to decline the use of land as collateral for loans, which impedes their business and deprives worthy customers of these financial services.

This research's objectives therefore are to identify the factors that influence land title deed verification and to review the current land title deed verification models and solutions. Further, the research aims to develop a prototype that uses the PKI model to enable efficient verification of land title deeds in Kenya, and then validate the accuracy and efficiency of that prototype.

With the aim of understanding whether title deed counterfeiting is a problem in Kenya, and after interviewing a sample number of respondents, I observed that all of the respondents have had a case of counterfeit title deeds brought before them, as seen in chapter 4. Further, 89% of these respondents, as shown on figure 4.4, were only able to establish that these title deeds were counterfeit after presenting them to the lands registry for verification, which means that the title deeds had no obvious signs that they were counterfeit. This shows the there is indeed a problem in title deed counterfeiting and that there is an acute advancement of counterfeiting techniques, which necessitates the development of a system that will quickly and efficiently differentiate between a counterfeit and a genuine title deed.

Given the responses from the majority of respondents and as shown on figure 4.5, the findings indicate that it takes about 5-8 days to verify the authenticity of a title deed using the current verification model. It is also conclusive as shown in figure 4.6 that the title deed records

in the current system are not organized or easily accessible, and this explains the slow and inefficient title deed verification process. A majority of the respondents were of the opinion that the integrity of the records in the current verification system could be compromised, and that tracking changes in the system's data was difficult, and thus making title deed verification a difficult process. The conclusion therefore is that the current title deed verification models are inefficient, slow and unreliable.

Given the respondents' answers, I observed that an information technology system could be used to help increase the efficiency and accuracy of title deed verification process. Some of the features that the respondents regarded highly were speed of verification, accuracy, non-repudiation, security and strict authentication of users of such a system.

The respondents also indicated that their respective organizations have policies to deal with title deed verification problems, but they do not have elaborate systems that help them enforce these policies, as shown in figure 4.14. This problem, compounded with the assertion that the lands registry does not have a robust, quick, efficient and reliable title deed verification system led me to conclude that there is indeed a problem in title deed verification, and an information technology system with the proposed features can help streamline this process.

The proposed title deed verification model incorporates the security features found in a public key infrastructure model for security purposes and also to enforce a condition where there would be non-repudiation and integrity of data. Further, the confirmation of the CA's digital signature on the digital title deed further ensures that it is authentic and the details on it can be trusted. The PKI model, as discussed in Chapter 2, comprises of a registration authority (RA) and a certification authority (CA) as its main components. Further, the PKI model also uses public key-private key matching pairs as well as signed digital certificates, all which ensure that trust and security of information between communicating parties is maintained.

By mimicking the PKI architecture, the developed prototype has a registration authority; this module is responsible for the verification of details of title deed owners and financial institutions that wish to be registered into the system, and then a private-public key pair is generated. The prototype also has certification authority, where the verified and registered details of a title deed holder are forwarded and a digital title deed is generated. The title deed also has the CA's digital signature as proof that the details have not been altered in any manner. The

digital title deeds also contain the title deed holder's public key, and can only be retrieved using the corresponding private key. The private key is issued to the title deed holder in a smart card upon successful registration. The digital title deed is broadcasted in a directory that can only be accessed by registered and authorized financial institutions.

Financial institutions are registered in the same manner as title deed holders. Their registration details also have to be verified in the companies' registration database, after which a public-private key pair is generated. Their public key is stored and they are issued with their corresponding private key in a smart card. By matching their public and private keys, the directory authenticates financial institutions and grants them access. After this, the title deed holder's private key is inputted and it retrieves the corresponding digital title deed. The details on this digital title deed can then be compared with those on the physical certificate, and thus verification can occur.

The land management information system developed by Choe (2004) is described in chapter 2. It outlines the use of maps incorporated into the land database, and these records are accessed over a web browser. Further, the electronic land register in Estonia developed by Vali (2014) is also discussed and it comprises of an electronic land register, but all land transactions have to be notarized before being digitally signed and updated into the system. The developed prototype is different from these two systems in that it does not focus on the issuing process of title deeds or cadastral zoning of parcels of land. The prototype primarily focuses on establishing the authenticity of title deeds by using the existing land records. Kamanda (2015) describes a system for the authentication of university certificates. These certificates are uploaded by authorized users then digitally signed, and a person wishing to verify the authenticity of a physical certificate can log into the system and verify that a digital copy exists and also verify the digital signature. The developed prototype therefore incorporates this concept of matching physical and digital copies of certificates, the use of digital signatures and further incorporates the security features of a PKI model to ensure that all data in the system is trustworthy and reliable.

The prototype is developed using the Java language, and also incorporating the vert.x framework to ensure concurrency of processes and also the itext library to create digital title deeds. The RSA algorithm is used to generate keys, which were then used to access the digital title deeds.

After the prototype was developed, 5 respondents from the land registry were allowed to use it to test its functionality. They were then asked to fill out a brief questionnaire to give the researcher feedback on what their sentiments were after using the prototype. The results, as shown in table 6.3 show that the respondents found the prototype's interface design to be appealing. They also found it easy to use, and did not think that upon completion there would be the need for a vigorous training exercise of the system because of its simplicity. The respondents also thought that the prototype had adequate security features in its design. It was also unanimous that the prototype was exhaustive in its purpose to verify title deeds, and that they would recommend its use in title deed verification, but on condition that several improvements be made.

7.3 Contribution to Research

The PKI model has been incorporated in many models since its inception, but mostly it has been used to ensure that communication between machines is secure and reliable. Many document verification models, such as the one proposed by Kamanda (2015), only employ the use of digital signatures. The prototype developed in this research however mimics the PKI model in its entirety, and therefore makes it a unique application of the model. The PKI model is robust and secure, and these features are advantageous in that they can pave way for further expansion of the idea to encompass other applications in land administration that are not limited to verification. Upon successful implementation, the prototype developed in this research can be scaled up without losing functionality or security, and can have modules added on that integrate or connect other relevant systems.

7.4 Challenges Encountered

i. Identifying individuals who had a grasp of cryptographic concepts was a challenge. Most respondents had a background in the use of information technology systems, but most did not have any knowledge in the machinations and working concepts behind them. However, such knowledge was not mandatory, but it could have been helpful in explaining the working theory behind the proposed prototype.

ii. Scheduling of interviews and subsequently the demonstration of the prototype was a challenge since it was to be conducted on working days. The institutions were usually

busy environments, and it was imperative to fit my interviews in between the respondents' free time.

iii. A total of 50 questionnaires were issued, but only 47 were returned. Data analysis was therefore conducted without data from the 3 respondents' missing questionnaires.

iv. The prototype had to be hosted online so that it could be accessed by the respondents for testing. However, internet access at the lands registry was significantly slow at times, and therefore slowed down the testing. This was overcome by supplementing using a copy of the prototype hosted locally on my personal laptop.

7.5 Conclusions

Title deeds counterfeiting is a grave problem in Kenya, and this problem is accentuated by lack of a quick and efficient title deed verification system. Further, the paper based system in use is prone to devices that may undermine the consistency and integrity of data. For this reason, financial institutions have made it harder for loan applicants to use land as collateral, which bars potential loan applicants as well as reduces business for these financial institutions.

This research therefore focused on studying this problem with the aim of developing a title deed verification solution to be used by financial institutions and the land registry alike. The title deed verification model uses the security features and concepts in a public key infrastructure model (PKI) to ensure that all data contained in the system is not only secure but also trustworthy. The PKI model has proved invaluable in its applications in other works, and its strengths make it suitable to solve the problem of title deeds counterfeiting that revolve around integrity and verification of records.

After completion of the research and the analysis of data, the prototype developed was found to have met most of the research objectives and answered most of the research questions. Further, the interviewed respondents, who work at the land registry, were satisfied with the functionality of the prototype to an acceptable degree, having also put forth their recommendations on how to make it better. This satisfies the system requirements set forth in chapter 4 of this research.

7.6 Recommendations

Based on the study, the following recommendations are made in order to improve the process of title deed verification in Kenya:

i. There is a need to fully digitize the processes at the lands registry. This includes digitizing the process of mapping land parcels across the country, and then digitizing the process of land allocation onto those mapped parcels of land. This streamlines the process of the issuing of title deeds, which will make verification very easy. A fully digitized land management system will also seamlessly integrate with a modified version of the prototype developed in this research.

ii. It is imperative to develop easily identifiable security features onto title deeds that make it very hard to forge. This will be the first security measure to curb counterfeiting, which will also work in tandem with a title deed verification system.

7.7 Suggestions for further research

Although having captured the gaps in title deed verification as outlined in literature review, the proposed system still has areas in which further research can be conducted. The prototype was impeded by scope and time constraints, but given more research then more information can be revealed.

Such a model can be employed to replace the current school certificates verification model that only employ digital signatures. There could be a central registry, and all parties wishing to verify the school certificates need to also be registered and given credentials with which to log in and access the directory.

Further, it can be used in the health sector to verify documents issued by doctors to patients. The health sector is an area that has also suffered from counterfeiting. There could be a central registry that registers all licensed medical practitioners. Once a practitioner issues a document to a patient, it is automatically uploaded to the directory. Parties wishing to verify the authenticity of documents, such as employers or insurance agents, can then use their credentials to access the directory to verify authenticity.

References

Audun, J. 2013. *"PKI trust models".* Theory and Practice of Cryptography Solutions for Secure

Information Systems (CRYPSIS). IGI Global, May 2013. ISBN13: 9781466640306

Choe, B. et.al. 2004. *"Land Management Information System in Korea".* KRIHS Special Reports. Korea Research Institute for Human Settlements, Korea.

Christof Paar & Jan Pelzl. 2010. *"Understanding Cryptography A Textbook for Students and Practitioners"*. Springer-Verlag, Germany.

Creswell, J.W. 2014. *"Research Design. Qualitative, Quantitative and mixed methods approaches."* 4th ed., University of Nebraska, Lincoln, USA.

Dewan, M. *"An idiots guide to Public Key Infrastructure".* Global Information Assurance Certification Paper. Version 1b. 27th September 2002. SANS Institute.

Financial Sector Deepening-Kenya (2009) *Cost of collateral in Kenya; Opportunities for Reform*. Nairobi. FSD Kenya.

Fleisig, H. (1995) *The Power of Collateral-How problems in securing transactions limit private credit for Moveable property.* Public Policy for the Private Sector-Note No 43. The World Bank.

Jin-Bao Liu et.al. 2007. *Design and Implementation of a PKI-Based Electronic Documents Protection Management System.* Third international Conference on International Information Hiding Multimedia Signal Processing. (IIH-MSP).

Kamanda, Ian Charles. 2015. *Prototype for the Authentication of University Certificates: A case of Strathmore University.* [Master's thesis]Nairobi, Kenya: Strathmore University.

Kenya Land Alliance. 2010. *"The Kenya Land alliance Case study."* Human rights, power and civic action in developing societies: comparative analyses (Ripoca). Norwegian Research Council.

Kenya Land Alliance. 2006. *"Unjust Enrichment: The Making of Land Grabbing Millionaires."* The Plunder of Kenya's State Corporations and Protected Lands. Vol. 2

Mugenda, O. M. and Mugenda, A. G. (1999). *Research Methods: Quantitative and Qualitative Approaches.* Nairobi: Acts Press.

Myers, B. & Rosson, M.B (2000). "Survey on User-Interface Programming. Proc. Of the 10th Annual CHI Conference in Human Factors in Computing Systems".

Naing, L. Winn &Rusli, B.N. (2006) *Practical issues in calculating the sample size for prevalence studies*. Archives of Orofacial Sciences.

Nyakundi, K.A.M. 2012. "*The problem of land rights administration in Kenya*." Nairobi University, Kenya.

Patton, M. (1990). Qualitative evaluation and research methods. Beverly Hills, CA: Sage.

Predrag M and Pere Tumbras (2010). *A Comparative Overview of the Evolution of Software Development Models.* International Journal of Industrial Engineering and Management (IJIEM), Vol.1 No 4, 2010, pp. 163 - 172 Available online at www.ftn.uns.ac.rs/ijiem. Accessed on 24th October 2016 at 3.05 pm.

Ramanathan, S. 2009. Introduction *of Land Title Certification System. State Level Reform.* JNNRUM Primers, India.

RSA Data Security. *"Understanding Public Key Infrastructure (PKI)" [*White paper]. Retrieved on September 10, 2016 at 3.05 pm from: ftp://ftp.rsa.com/pub/pdfs/understanding_pki.pdf

S. Imran, T. Ferdous, M. Adeel and M. Faheem, 2013. *"Existing land record management system of Pakistan and proposed Arc GIS parcel data model,".* International Conference on Aerospace Science & Engineering (ICASE), Islamabad, pp. 1-6.

Thales e-security. *"Securing your PKI-Building trust you can depend on"* [White paper] Retrieved on September 10, 2016 at 2.10 pm from Thales e-security website: http://resources.idgenterprise.com/original/AST-0073572_Securing_Your_PKI_Building_Trust_You_Can_Depend_On_wp.pdf

The Constitution of Kenya. Revised Edition 2010. Published by the National Council for Law Reporting.

The World Bank Databank (2016). *Food and Agriculture Organization*. Retrieved from http://data.worldbank.org/indicator/AG.LND.TOTL.K2 on 28th October 2016 at 3.00 pm.

Vali,I. et.al. 2014.*" Electronic land register which forcefully eliminates real estate fraud and corruption: Estonia".* XIX World Registry Law Congress. Santiago, Chile.

Viet, P. 2011, March. *"Focus on Land in Africa: History of land conflicts in Kenya".* World Resources Institute Annual Brief.

Wainaina, E. "*Here's why you should check your land records often*". Daily Nation. 8th October 2015. Accessed on September 10, 2016 at 3.10 pm from the Nation Newspaper website at: http://www.nation.co.ke/lifestyle/DN2/Here-why-you-should-check-your-land-records

Waldo, J. (2006). *On System Design, Perspectives* 2006-6 in an Essay Series Published by Sun Labs Sun Microsystems, Inc 1 Network Drive Burlington, MA 01803 1 781 442 0497

Wanga,J. *"Borrowers suffer as banks reject titles to give loans".* Daily Nation 4th October 2014. Accessed on: September 10, 2016 at 3.15 pm from the Nation Newspaper website at: http://www.nation.co.ke/news/Banks-Loans-Title-Deeds/1056-2475574-e5um6yz/index.html

APPENDIX A: DATA COLLECTION QUESTIONNAIRE

I am a Master's degree student Strathmore University, Faculty of Information Technology. I am in the process of writing my Masters' thesis and I am collecting data for that purpose. For my work, I am very interested in exploring the challenges encountered in the title deeds verification process in Kenya. Additionally I am interested in exploring the outcome and benefits to your institution of implementing an information technology title deeds verification system that incorporates cryptographic security features. I hereby request you to be a participant in this study.

All information you provide will be kept strictly confidential and under no circumstances will your individual responses be released or used for purposes other than this research. Please remember that your participation is entirely voluntary and you are free to discontinue at any time. However, your professional experiences and opinions are crucial to helping me understand the challenges currently experienced in the process of land administration in Kenya. I would greatly appreciate your taking time to complete this questionnaire.

BRIEF INSTRUCTIONS FOR THIS QUESTIONNAIRE

1. The questionnaire has three sections; the general information section, a section on the challenges in title deeds verification and lastly a section to only be filled in by employees in a management position. Please complete each section as necessary.
2. There are two types of questions; open ended and closed ended. To answer open ended questions, please fill in the space provided. To answer closed ended questions, please enter a tick [✓] in one of the boxes/spaces provided to indicate the answer that closely represents your answer for each question.

SECTION 1: GENERAL INFORMATION

i. What is your position of employment?

☐ Managerial ☐ Non-Managerial

ii. Does your institution have an information technology system?

☐ Yes ☐ No

iii. How would you rate your information skills generally?

☐ Very Inferior ☐ Average ☐ Very Superior

☐ Inferior ☐ Superior

iv. Where is data in your information system stored?

☐ In a database within the organization building

☐ In an external database at a location away from the organization building

v. How do you access the data in the system?

☐ By use of a web browser over a network

☐ By use of stand-alone stations at specific locations at the organization

vi. Has a case of counterfeit title deeds ever been brought to your attention?

☐ Yes ☐ No

vii. If yes, what alerted you to the fact that it was a counterfeit title deed?

☐ The title deed's features did not seem authentic

☐ After conducting a search at the lands registry it was confirmed that the title deed was counterfeit

SECTION 2: REVIEW OF CURRENT SYSTEM: CHALLENGES EXPERIENCED IN TITLE DEED VERIFICATION. Please tick the most appropriate box that corresponds to your answer

i. How long does it take you to verify the authenticity of a title deed?

☐ 1-4 days ☐ 5-8 days ☐ 9 days or more

ii. Please fill in the next section by ticking the most appropriate answer

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	I think that title deed records are organized and easily accessible in the current system					

2	I think the integrity of title deed data can be interfered with in the current system					
3	It is very easy to track changes in title deed details in the system					
4	The current system helps and makes it easy to verify the authenticity of title deeds					
5	Currently, title deeds have easily distinguishable features that help spot counterfeit title deeds					
6	I think an IT system can be used to deal with the challenges in the verification of title deeds					

iii. Which features of an IT system do you believe would help in enhancing the title deed verification process? [Please rate them on a scale of 1-5, with 1 being the lowest and 5 being the highest]

		1	2	3	4	5
1	Title deeds data in the system has to be secure and cannot be changed without authorization (data security and integrity)					
2	When title deed data is changed in the system, it easy to know who did it and when they changed the data (non-repudiation)					
3	The system should make it easy to check for title deeds quickly, accurately and consistently (functionality)					
4	Only authorized individuals can be able to access private title deed data stored in the system (authentication)					

SECTION 3: ONLY FOR EMPLOYEES IN MANAGEMENT POSITIONS. PLEASE TICK ALL THAT APPLY

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	My organization has elaborate systems to verify the authenticity of title deeds					
2	I believe that the land registry provides adequate title deed verification services					
3	My organization has policies in place to help deal with the issue of counterfeit title deeds					

INTERVIEW GUIDE.

1. Do you have an elaborate system to verify title deeds?
2. What are some of the challenges that you encounter during the process of title deed verification?
3. What are some of the policies does your organization have in place that outline how you handle cases of counterfeit title deeds?
4. Do you think that I.T can be used to help solve the challenges that are associated with title deed verification?
5. What features and functions would you expect from a title deed verification system?
6. What factors do you think influence title deed verification in Kenya?

APPENDIX B: PROTOTYPE USABILITY QUESTIONNAIRE

Prototype Usability Questionnaire

After you have tested the title deed verification prototype, please fill in this brief questionnaire. Thank you for your time and input.

PART 1: BACKGROUND

1. Name (Optional):

2. What is you IT proficiency level?

☐ Inferior ☐ Average ☐ Above Average

PART 2: PROTOTYPE USABILITY FEEDBACK

3. What is your opinion of the user interfaces of the title deed verification prototype?

☐ Not Appealing ☐ Appealing ☐ Very Appealing

4. What was the level of difficulty of use of the title deed verification prototype?

☐ Difficult ☐ Fairly Easy ☐ Easy

5. Do you think much training will be needed in order to learn how to use the final system?

☐ Yes ☐ Minimal Amount ☐ No

6. Do you think the prototype has adequate security features?

☐ Yes ☐ A fair amount ☐ No

7. Do you think the prototype adequately performs title deed verification?

☐ Yes ☐ To a small extent ☐ No

8. Do you think the title deed verification prototype was exhaustive in addressing the difficulties associated with title deed verification?

☐ Exhaustive ☐ Fairly Exhaustive ☐ Not Exhaustive

PART 3: RECOMMENDATIONS

9. Do you think the title deed verification system would improve the title deed verification process?

☐ Yes ☐ Not Sure ☐ No

10. Would you recommend the adoption of the title deed verification system by the relevant stakeholders once development is complete?

☐ Yes ☐ No

☐ Yes, But with improvements

11. What improvements would you like to see implemented in the title deed verification system?

1: .....

2: .....

3: .....

4: .....

5: .....

APPENDIX C: SAMPLE CODE SEGMENT

1. SAMPLE CODE TO GENERATE KEYS

```
package com.mkyong.keypair;


import java.io.File;

import java.io.FileOutputStream;

import java.io.IOException;

import java.security.KeyPair;

import java.security.KeyPairGenerator;

import java.security.NoSuchAlgorithmException;

import java.security.NoSuchProviderException;

import java.security.PrivateKey;

import java.security.PublicKey;


public class GenerateKeys {

	private KeyPairGenerator keyGen;

	private KeyPair pair;

	private PrivateKey privateKey;

	private PublicKey publicKey;


	public GenerateKeys(int keylength) throws NoSuchAlgorithmException,
NoSuchProviderException {

		this.keyGen = KeyPairGenerator.getInstance("RSA");

		this.keyGen.initialize(keylength);

	}
```

```
public void createKeys() {
        this.pair = this.keyGen.generateKeyPair();
        this.privateKey = pair.getPrivate();
        this.publicKey = pair.getPublic();
}

public PrivateKey getPrivateKey() {
        return this.privateKey;
}

public PublicKey getPublicKey() {
        return this.publicKey;
}

public void writeToFile(String path, byte[] key) throws IOException {
        File f = new File(path);
        f.getParentFile().mkdirs();

        FileOutputStream fos = new FileOutputStream(f);
        fos.write(key);
        fos.flush();
        fos.close();
}
```

```
    public static void main(String[] args) {
        GenerateKeys gk;
        try {
            gk = new GenerateKeys(1024);
            gk.createKeys();
            gk.writeToFile("KeyPair/publicKey", gk.getPublicKey().getEncoded());
            gk.writeToFile("KeyPair/privateKey", gk.getPrivateKey().getEncoded());
        } catch (NoSuchAlgorithmException | NoSuchProviderException e) {
            System.err.println(e.getMessage());
        } catch (IOException e) {
            System.err.println(e.getMessage());
        }

    }
```

}2. **SAMPLE CODE TO SIGN A DIGITAL TITLE DEED**

```
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.security.PrivateKey;
import java.security.Signature;
import java.util.Arrays;
import java.util.Properties;
import org.apache.commons.codec.binary.Base64;

public class SignLicense {
 public static void main(String[] args) throws Exception {
```

```
 if (args.length != 2) {
  System.out.println("Usage: SignLicense licenseFile privateKey");
  System.exit(1);
 }
 Properties license = new Properties();
 license.load(new FileInputStream(args[0]));
 PrivateKey privateKey = Utils.readPrivateKeyFromFile(args[1]);
 Signature signature = Signature.getInstance("SHA1withRSA", "SUN");
 signature.initSign(privateKey);
 String[] propKeys = license.keySet().toArray(new String[0]);
 Arrays.sort(propKeys);
 for (String propKey : propKeys) {
  if (!"Signature".equals(propKey)) {
   String propValue = license.getProperty(propKey);
   signature.update(propValue.getBytes("UTF-8"));
  }   }

 byte[] sig = signature.sign();
 license.setProperty("Signature", new String(Base64.encodeBase64(sig)));
 license.store(new FileOutputStream(args[0]), null);
} }
```

3. SAMPLE CODE TO VERIFY THE SIGNATURE ON A DIGITAL TITLE DEED

```
import java.io.BufferedInputStream;
import java.io.FileInputStream;
```

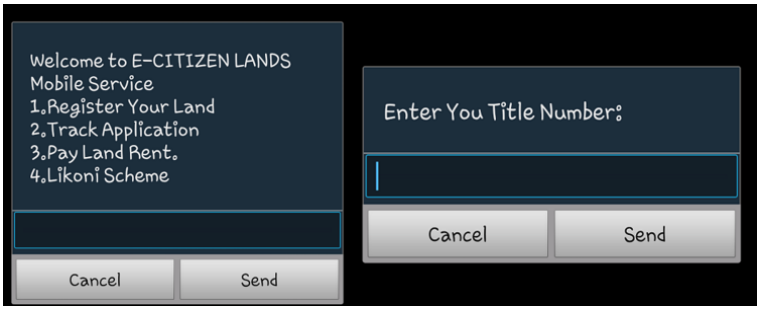
```
import java.security.PublicKey;
import java.security.Signature;
public class VerSig {
 private static byte[] PUBLIC_KEY = { 48, -126, 1, -73, 48, -126, 1, 44, 6,
   7, 42, -122, 72, -50, 56, 4, 1, 48, -126, 1, 31, 2, -127, -127, 0,
   -3, 127, 83, -127, 29, 117, 18, 41, 82, -33, 74, -100, 46, -20,
   -28, -25, -10, 17, -73, 82, 60, -17, 68, 0, -61, 30, 63, -128, -74,
   81, 38, 105, 69, 93, 64, 34, 81, -5, 89, 61, -115, 88, -6, -65,
   -59, -11, -70, 48, -10, -53, -101, 85, 108, -41, -127, 59, -128,
   29, 52, 111, -14, 102, 96, -73, 107, -103, 80, -91, -92, -97, -97,
   -24, 4, 123, 16, 34, -62, 79, -69, -87, -41, -2, -73, -58, 27, -8,
   59, 87, -25, -58, -88, -90, 21, 15, 4, -5, -125, -10, -45, -59, 30,
   -61, 2, 53, 84, 19, 90, 22, -111, 50, -10, 117, -13, -82, 43, 97,
   -41, 42, -17, -14, 34, 3, 25, -99, -47, 72, 1, -57, 2, 21, 0, -105,
   96, 80, -113, 21, 35, 11, -52, -78, -110, -71, -126, -94, -21,
   -124, 11, -16, 88, 28, -11, 2, -127, -127, 0, -9, -31, -96, -123,
   -42, -101, 61, -34, -53, -68, -85, 92, 54, -72, 87, -71, 121, -108,
   -81, -69, -6, 58, -22, -126, -7, 87, 76, 11, 61, 7, -126, 103, 81,
   89, 87, -114, -70, -44, 89, 79, -26, 113, 7, 16, -127, -128, -76,
   73, 22, 113, 35, -24, 76, 40, 22, 19, -73, -49, 9, 50, -116, -56,
   -90, -31, 60, 22, 122, -117, 84, 124, -115, 40, -32, -93, -82, 30,
   43, -77, -90, 117, -111, 110, -93, 127, 11, -6, 33, 53, 98, -15,
   -5, 98, 122, 1, 36, 59, -52, -92, -15, -66, -88, 81, -112, -119,
   -88, -125, -33, -31, 90, -27, -97, 6, -110, -117, 102, 94, -128,
   123, 85, 37, 100, 1, 76, 59, -2, -49, 73, 42, 3, -127, -124, 0, 2,
```

```
 -127, -128, 58, -114, -32, -48, 15, 95, 21, -103, -107, 51, 96, 9,
 -84, -27, 114, -81, 124, 79, -5, -18, -18, -62, -34, -33, -60, 69,
 -120, -108, -18, -1, 1, -127, -100, -52, 95, -28, -123, -106, -9,
 -49, 112, -55, 110, 66, 40, 68, 71, 59, -27, -57, 96, -41, -90, 45,
 -106, -106, -101, 116, 98, 12, -91, 127, 89, 14, 103, 113, -12, 80,
 -118, 118, -20, 71, -74, 74, -109, 1, -105, 126, 124, -90, 40, 110,
 64, -31, 60, 37, -6, -72, 124, -101, -25, -94, -122, -19, 21, 93,
 27, -54, -103, -74, 126, 17, -111, -59, -19, 63, 78, -71, -59, 78,
 114, -25, -86, 37, -125, -103, 76, -120, 115, -65, -119, -57, 34,
 98, -124, -93, -62, -70 };

public static void main(String[] args) throws Exception {

 if (args.length != 2) {
  System.out.println("Usage: VerSig "
    + "publickeyfile signaturefile " + "datafile");
  System.exit(1);
 }

 PublicKey pubKey = Utils.readPublicKeyFromBytes(PUBLIC_KEY);
 byte[] sigToVerify = Utils.readFile(args[0]);

 Signature sig = Signature.getInstance("SHA1withRSA", "SUN");
 sig.initVerify(pubKey);
 FileInputStream datafis = new FileInputStream(args[1]);
```

```
 BufferedInputStream bufin = new BufferedInputStream(datafis);

 byte[] buffer = new byte[1024];
 int len;
 while (bufin.available() != 0) {
  len = bufin.read(buffer);
  sig.update(buffer, 0, len);
 }

 bufin.close();
 boolean verifies = sig.verify(sigToVerify);
 System.out.println("signature verifies: " + verifies);

}

}
```

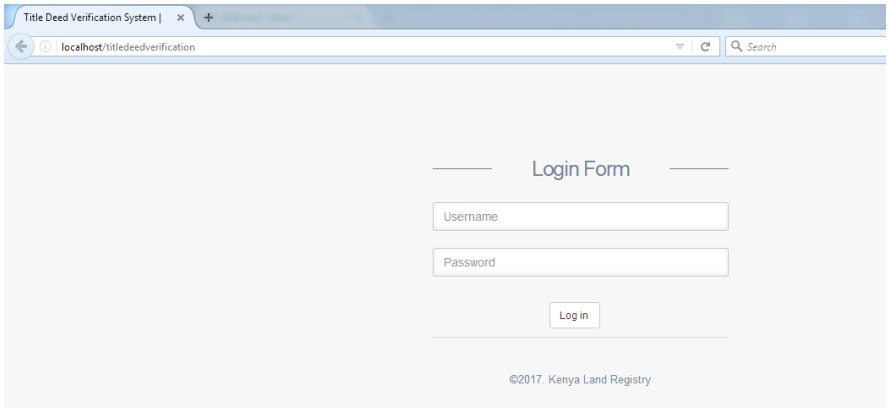
APPENDIX D: SCREENSHOTS

1. E-Citizen USSD service

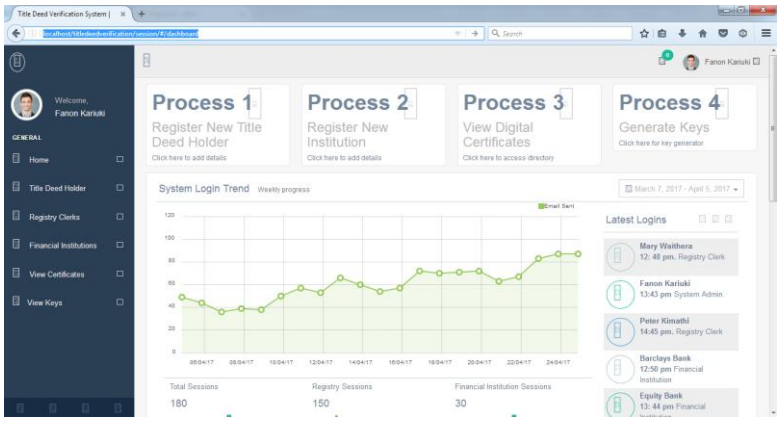


2. Use of technology in land administration in Rwanda

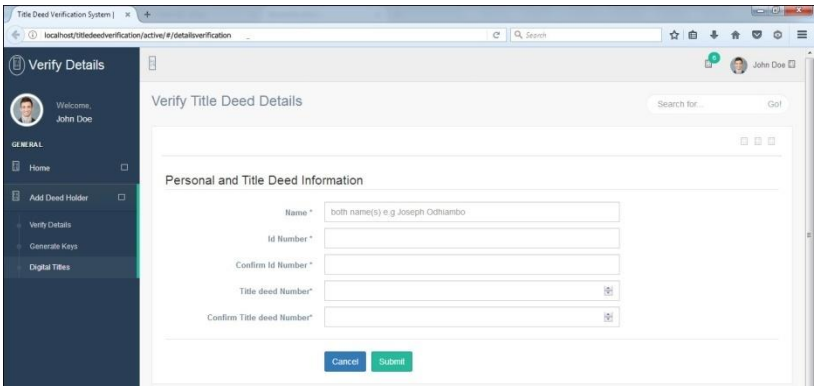
3. System Interfaces: The Login Form



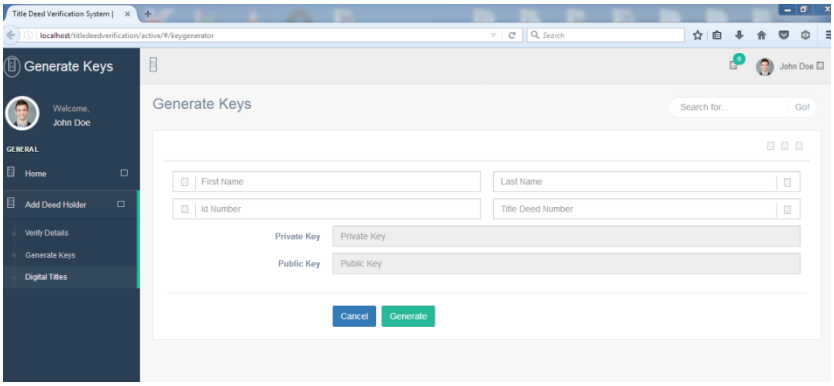
4. The Dashboard after Successful login



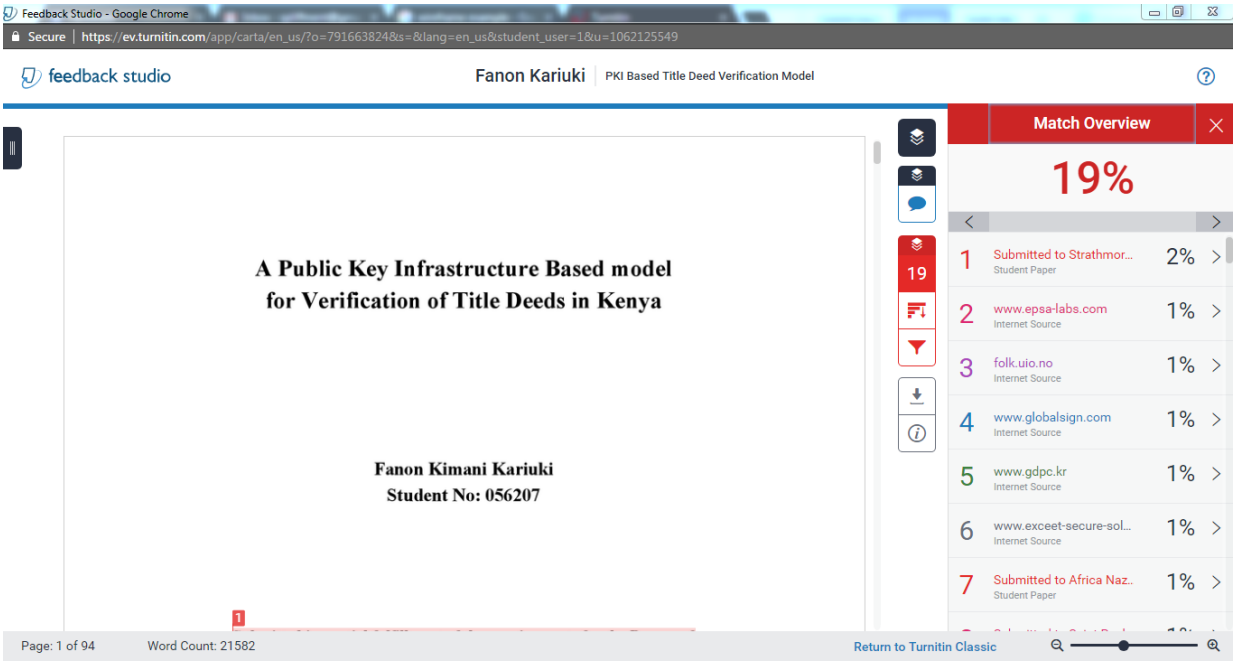
5. Details verification interface



6. The Key Generation Interface



APPENDIX E: ORIGINALITY REPORT



PKI Based Title Deed Verification Model

ORIGINALITY REPORT

19%	14%	2%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Strathmore University Student Paper	2%
2	www.epsa-labs.com Internet Source	1%
3	folk.uio.no Internet Source	1%
4	www.globalsign.com Internet Source	1%
5	www.gdpc.kr Internet Source	1%