University of Nairobi

SCHOOL OF COMPUTING AND INFORMATICS

Automated Detection and Recovery of Stolen Electronic Gadgets using Radio Frequency Identification in Kenyan Universities

KELVIN KARIUKI

P53/79662/2015

<u>Supervisor</u>

Prof. W. Okelo-Odongo

November 2016.

THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN DISTRIBUTED AND COMPUTING TECHNOLOGY OF THE UNIVERSITY OF NAIROBI

Declaration

This project, as presented in this report, is my original work and has not been presented for any other University award.

Student Signature: __________________ Date: _______________________

Kelvin Kariuki Mwangi (P53/79662/2015)

This project has been submitted in partial fulfillment of the requirements of the Master of Science Degree in Distributed Computing Technology of the University of Nairobi with my approval as the University supervisor.

Supervisor Signature: ________________ Date: _______________________

Prof. W. Okello-Odongo

Acknowledgments

I take this opportunity to thank God for being with me during this period of completing my assignment. He has given me adequate strength and has also protected me.

I also thank the panelists Prof. W Okello-Odongo, Dr. Christopher Chepken and Dr. Stephen Mburu for their compassionate guidance and follow up during the project period under the able leadership of the chair Dr. Evans Miriti.

A big appreciation goes to my project supervisor, Prof. W Okello-Odongo for his endless help, support and guidance throughout this entire period, he has been more than just a Supervisor to me but a friend who has given me brilliant ideas on how to improve the project and sacrificed a lot of his personal time to make sure that the research paper is up to standards and has met all the required guidelines.

I also want to take this opportunity to thank all the lecturers that have ever taught me in this course, they were a source of inspiration and due to the good foundation they laid in me I have been able to come up with a well formulated research project. I also thank all my classmates for their support and ideas towards improving my system.

Lastly I thank my parents for their encouragements, the school of computing for their excellent coordination of our studies and the university as a whole for giving a conducive learning environment.

Abstract

The Radio Frequency Identification (RFID) Technology is an important type of wireless sensor network that can be used for automatic detection of stolen electronic gadgets. Advancements in technology in the production of electronics have made more people desire to own devices such as laptops, smart phones, fridges, washing machines among others hence raising their demand not only on the genuine markets but also on the black market. In this research, we develop a model leveraging RFID technology to help end the rapid growth of theft cases involving electronic devices in Kenyan Universities. A prototype is built from the design and deployed using Arduino Mega board and MFRC Arduino card reader. We present our implementation experiences and the experimental results. In order to evaluate the efficiency and accuracy of the proposed system, we also conduct a test-driven simulation based on real data collected from the experiments. This indeed demonstrates that the prototype RFID system can be more efficient and accurate compared to the traditional methods of device ownership verification in large communities such as universities and tertiary institutions, and hence will greatly help in reducing electronic device theft in these institution of higher learning.

Keywords Radio Frequency Identification, Wireless Sensor Networks, Electronics, Arduino.

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

RFID – Radio Frequency Identification

CUE – Commission for University Education

ICT - Information Communication Technology

PCs – Personal Computers

GPS - Global Positioning System

LF – Low Frequency

HF – High Frequency

UHF – Ultra High Frequency

Chapter 1: Introduction

1.1 Background of the Study

The use of information technology for security operations can improve efficiency and accuracy at the gates of fenced compounds like universities and therefore decrease property crime on electronic devices. One of these technologies is RFID (Radio Frequency Identification) technology. This technology uses radio waves for identification (Antii et al, 2014). Irani et al., (2010), refers to RFID as a technology that is used for automatic identification of physical objects and people using radio frequency.

It has been argued by (Irani et al., 2010) that the rapid decrease in the price of the RFID tags have led to its wide and swift adoption and utilization in various contexts. Recently many business scenarios are implemented using RFID technology such as patient safety, inventory management, supply chain management, transportation and cargo tracking and many more domains (Fosso Wamba et al., 2010). However, no research has been reported on how to apply this technology on the tracking of personal and companies' electronic assets in compounds that are fenced and have designated entry and exit points (Gates). This paper focuses on this gap.

World over, universities are responsible for research, knowledge generation and innovation that is necessary for driving local social, technological and economic development (Commission for Higher Education, 2016).This learning and research is mainly made possible by use of technology like the internet and electronic assets like laptops and Personal computers (PCs). The increase in demand of these devices have led to an increase in their theft and subsequent growth of the stolen goods market.

The growing number of universities and the increase in the variety of study programmes as indicated by Commission for University Education (CUE), has led to a massive growth in the number of students' enrolment in the universities over the past years and these numbers are expected to rise. The rapid ICT (Information Communication Technology) developments in the country has led to a paradigm shift in the curriculum and has greatly changed the routines of traditional academic research. This in turn has led to a massive ownership of laptops, PCs (Personal Computers) and other electronic devices by both students and staff, especially the academic staff, for research purposes.

This increase in the ownership of electronic devices in Kenyan Universities has also been emphasized by Kashorda and Waema (2014) in their E-Readiness survey of Kenyan Universities where they projected that, by 2015, 75% of students will own laptops and 10% of the students will own PCs. Additionally, Kashorda and Waema (2014) showed that student enrollment had doubled within the period 2008 to 2013, while the number of full-time teaching staff had increased by 30.9%.

Although security agencies screen people using the traditional methods like book records verification or using the bar code system, these methods are quite time consuming, cumbersome, inaccurate and repetitive.

Allowing security agencies to screen people and electronic devices as they pass through the exit point or any other checkpoint using RFID technology might improve the checkout verification time, improve the accuracy of the verification and hence reduce the electronic assets theft menace. This method will provide a timely, efficient and accurate information of the owner of a tagged device hence automatically detecting and preventing theft.

This thesis reports the findings of a thorough study to establish the benefits of RFID technology in electronic assets tracking and how such benefits can be applied in the institutions of higher learning in Kenya. Emphasis is placed on the establishment of an efficient and accurate practice of owner device verification using RFID technology. Also central to the research study is exploration of the possibility of sharing a common database among the universities and their contributions to and expectations of the outcomes.

1.2 Problem Statement

Majority of adults in this technological error own an electronic asset, university students in particular, own Laptops, personal computers and other electronic equipment which they frequently use and need for their studies and research activities. The Commission for Higher Education (CUE) indicates that there are twenty three public chartered universities, ten public university constituent colleges, seventeen private chartered universities, five private university constituent colleges, fourteen institutions with letter of interim authority and one registered private institution giving a total of seventy registered universities in Kenya.

It is interesting to note that some survey which was carried out in 2013 (Kashorda and Waema, 2014) identified that 53% of students in universities own laptops and 17% own desktops, while in some particular universities the ownership was as high as 86%.This translated to about 220, 000 students who owned laptops and 70, 000 who owned desktops. These numbers are expected to rapidly increase with the increase of the number of students who are admitted into institutions of higher learning in the coming years.

The more you use your personal computer, laptop, tablet or even smart phone, the more you tend to lose it at some point. Losing a laptop or an electronic device you depend on for your studies or work, either by misplacing it or by theft can be devastating. This causes a great financial loss as these devices are relatively expensive and even worse, the loss of personal files, photos, documents and other data can be even more painful.

As criminologists (Clarke and Webb, 1999) remarked, electronics assets fall under the ‘hot product’ category, meaning, they are among the consumer items that are most attractive to thieves. He goes further to say that most residential burglary have been repeatedly found to target electronic items like the television set, personal computer, laptops, the radio player among other personal items.

The trauma of losing an expensive electronic device is made worse by the fact that the thieves sell these devices at different geographical locations from the one in which they stole, hence reducing the chance of ever getting it device back. In this scenario, these electronic device are stolen from one university and sold to students or staff in other universities since the greatest demand come from them.

The stealing of these valuable electronic devices has been a common issue not only in our universities but in the society at large. What fuels this vice is the large, ready and free market of ‘cheap’ stolen electronics devices. The free market of stolen electronic goods ensures a constant demand and supply chain of these devices.

Most burglars and prolific thieves steal to raise money, to do so, they always need to sell the electronic devices they steal as soon as possible. For their mission to be successful, they always want to complete two main objectives without getting caught. The first objective being, stealing the electronic device, and secondly, to sell the stolen device as soon as possible.

More often than not, the thieves sell these devices not far away from the location from which they stole it. In this case, electronic devices like laptops are stolen from one university and sold to students in a nearby university. Most people even buy these stolen devices without their knowledge or consent and these devices never get back to the owner. This creates a demand for our own victimization and also fuel the victimization of others who genuinely own electronic devices.

The current methods of device ownership verification like the book register and the barcode system have been unable to solve this problem, as the former has no intelligence of detecting a stolen device, is inaccurate as a person can write a wrong serial number, is cumbersome and repetitive while, on other hand, the later lacks the ability to automatically detect a hidden device hence and is also time consuming as it relays on line of sight therefore the owner of the device has to remove it from the bag for scanning.

The main aim of this study is to find out how we can use RFID technology to thwart the two objectives of the thieves mentioned above and come up with a recommendation for an efficient practice of electronic device tracking using RFID technology in Kenyan Universities.

1.3 Main Objective

The main objective of this study is to establish a tracking solution leveraging RFID technology to enhance the accuracy and efficiency of mobile electronics ownership verification in Kenyan Universities.

1.3.1 Specific Objectives

I. Investigate the current methods and the use of Information Technology in electronic device ownership verification in Kenyan Universities.
II. Design an electronic assets tracking system using RFID.
III. Develop a prototype.
IV. Evaluate the prototype.

1.4 Significance of the study

According to Clarke (1999, p.35), products that are easily moved have higher chances of being stolen. Most electronic devices fall under this category and are generally referred to as criminogenic. These highly vulnerable products are supposed to be given more protection. One of the ways in which we can effectively prevent electronic assets theft is by use of technology at the exit points of Universities and big buildings in order to verify the ownership of a device.

Lahtela et al., (2008) points out that RFID technology presents a way to move from manual identification process to an automatic identification process. He goes on to add that, using this technology is far more reliable than handwritten information. Majority of the universities in Kenya use the handwritten process in verifying the ownership of electronic devices owned by either the students or the staff.

This method is quite cumbersome and time wasting, furthermore, each university have their own book hence making it a repetitive process of registration of the devices during entry to the university and the entire process is dump as it cannot verify the legitimate ownership or detect a stolen electronic device.

This study intends to come up with an innovative, low cost electronics tracking method which takes advantage of an emerging wireless communication technology; RFID. The main idea is to make it virtually impossible for people to own and, with or without their knowledge, purchase and use stolen electronic devices. It will also make it possible to be able to recover most of the stolen electronic devices through the real-time notifications of the RFID system, more so, it will provide a readily available record of individual's devices serial number which is a key component required by the police in order for them to help a victim recover a stolen electronic device.

This theft can also be potentially very dangerous, as any criminal who steals your laptop or personal computer could then have access to your email, facebook, or online banking accounts, which combined with other personal data on your laptop, could make identity theft easy.

It has been argued by (Sutton et al., 1998) that stolen goods markets can be tackled through interagency partnerships which include the police, local authorities, housing associations among others. In regard to electronics theft, especially laptops, tablets, and personal computers, universities will be viewed as an important partner.

If we kill the free market of stolen electronic devices, by adopting the RFID tracking technology, then we will kill the stealing habit. This will reduce by almost 80% crime targeted towards our electronic devices which include burglary, robbery or petty theft.

1.5 Scope and limitation of the Study

This study will be limited to two universities in Kenya, The University of Nairobi and Multimedia University of Kenya. This research project will systematically investigate the use of RFID technology in curbing electronic assets theft by conducting a case study analysis. These two universities will provide an opportunity to gain rich, comprehensive and in-depth information on the study.

The limitation of this approach is the generalization and the determination of the extent to which the findings will be applied to other universities in Kenya. This issue will be considered throughout the research period and will be addressed further in subsequent chapters.

Chapter 2: Literature Review

2.1 Introduction

In this second chapter, relevant literature information that is related and consistent with the objectives of the study is reviewed. Important issues and practical problems are brought out and critically examined so as to determine the current facts.

2.2 Theft of Electronics devices in Kenyan Universities

The increased use of ICT for teaching, learning and research in Kenyan Universities has led to a high demand of electronic devices like laptops, PCs and smartphones. This in turn has made these devices 'hot products', which Clarke (1999) describes as items that are most targeted and stolen by thieves. Sutton (2015) argues that statistical research done in the past has proven that most thieves have an ever-changing hierarchy of goods that they prefer to steal.

Cases of laptop, PCs, tablets and smart phones theft have been on the rise in Kenyan Universities in the recent past. These devices have a common attribute that is summarized in the acronym CRAVED that mean they are Concealable, Removable, Available, Valuable, Enjoyable and Disposable (Sutton, 2015).

Theft cases in universities are mostly carried out by; students themselves, members of staff or visitors who come to visit the students in their hostels or those that come to visit staff members in the staff quarters. Although most universities are well fenced and have designated and well secured exit points, not all but a few, use a traditional handwritten method of device ownership verification hence making it impossible to detect or prevent these theft in a timely and efficient fashion.

According to a survey carried out by IPSOS in 2015, 1st Quarter Social, Political, Economic and Cultural Survey, fewer Kenyans were reporting crime incidences that they were involved in than in previous surveys. This stood at 46% and was attributed to that fact that majority of the crime victims were not satisfied with the police response. 43% of those interviewed mentioned that the authorities response was weak and often without any follow-up investigation.

This may explain why few students and staff members report the theft cases of their valuable electronic gadgets to the University's Security Department and even a lesser number these victims proceed to report to the police station.

A few of those that report find themselves stumbling when asked of the serial number or IMEI (International Mobile Equipment Identity) by the authorities, which is supposed to help in the investigations. When this information completely lacks, it makes it very hard or almost impossible for the authorities to track the device hence reducing the chances of recovering it.

2.3 A Free Ready Market for Stolen Electronics

Stutton (2015) claims that the demand for and prices of goods in the legitimate markets influence the products that are hot in the stolen goods markets. He continues to point out that most prolific thieves don't steal items for their own use but for selling or swapping for drugs.

This case is profound in most of our universities as most thieves, especially among the students, are often alcoholics or drug addicts. So they steal in order to make quick cash for this vices.

Thieves generally prefer to sell the stolen electronic items locally, in this case, to other students within the university or to students or staff in other and neighboring universities since that is where the demand is highest. This vice is propelled by the large and free market of stolen electronic devices and the fact that it is almost impossible to identify a stolen electronic item.

The lack of universities in using a common system of device ownership verification has also fueled this vice, hence a device stolen from one university and sold to an innocent or willing buyer in another university is almost impossible to recover.

2.4 Existing Solutions

2.4.1 Handwritten records for check-in and check-out

Many universities, companies and big buildings use this traditional and crude method. It involves registering your personal and device details in a book as you enter their compound or premise.

This method is out rightly backward and inefficient especially during the check-out process, as you have to manually go through multiple records searching where you wrote your details for the device ownership to be validated.

The same routine is repeated when you visit another university or building yet these books have no intelligence of recognizing whether the device is stolen or whether it really belongs to the person holding it or not. The entire procedure is repetitive, time-intensive and cumbersome.

2.4.2 Bar-Coding Systems

This is a data scanning method that is made up of an information system and a bar code scanner that is used to retrieve the serial number information from a bar-code tag attached to an electronic device.

Devices are registered in an information system with their serial number and scanned for ownership verification during checkout by staff, students and visitors.

It is a more advanced technique compared to the handwritten verification method but it has a number of challenges including; it requires a line of sight, can only read one tag at a time, have difficulty in reading a worn-out bar-code tag and since the tag is visible, it is easy to tamper with the tag or even change it.

2.4.3 Locks

These locks are analogous to the bicycle chain lock and their main purpose is to anchor the portable electronic device to a heavy and less portable item like the table or to attach multiple electronic devices together hence making them less portable and difficult to carry. They are usually made up of a woven steel cable and have either a keyed lock or a combination lock and alarm system.

This method is a fairly inexpensive way of ensuring that our electronic devices are not easily stolen. However, depending on the cable strength, the cable can be easily cut and the device stolen.

2.4.4 GPS Tracking

The Global Positioning System (GPS) is a reliable and highly accurate, three-dimensional navigation system. It consists of a number of satellites that orbit the earth twice a day transmitting precise timing information. (Gehlot, 2002) describes the system as having a three major components which are: a communicator; a location sensor and a security controller.

This method of tracking has not been widely adapted in electronics tracking as compared to vehicle tracking. This is due to the inherent technical challenges that GPS faces which include availability, accuracy, power consumption, size and the cost involved in implementing it,(Chadha, 1998).

Chadha (1998) further describes each of those challenges experienced by GPS as follows:

1. Availability – he claims that GPS systems in urban areas may be completely blocked by buildings or the signal maybe attenuated by the dense foliage of trees hence reducing the visibility of GPS satellites.
2. Accuracy – he argues that the use of time varying bias reduces the potential accuracy of GPS Systems to around 100 meters.
3. Power consumption – he suggests that power consumptions reduction can be achieved by using hardware and software power-management techniques.
4. Size – he argues that a GPS receiver may now be small enough to fit in a wallet but is still too large to be integrated in smaller equipment like cell phone or smart watches.
5. Cost – according to Chadha, the cost of acquiring a GPS receiver and that of integrating it into another platform can go up to about $100. This is relatively expensive to a common Kenyan.

According to (Werb et al., 2004), GPS systems are unable to track when the tag moves indoors as the GPS satellite signals become inaccessible. This makes its availability and usability in tracking electronic assets low.

2.5 Radio Frequency Identification

RFID tags are typically made up of an integrated circuit that is operatively coupled to an antenna (Cybulski et al., 2003). The entire circuitry is usually fabricated on a thin plastic sheet. Each tag has a few bytes of memory which contains its unique identification number and sometimes other information related to the item which it is tagged to.

(Want, 2006) claims that RFID devices are divided into two main categories which include active and passive RFIDs. He continues to say that active tags need a power source which can either be connected to a power infrastructure or use in internal battery. On the other hand, passive RFID do not require a power source.

Of interest to this research is the passive tags since they do not need a battery and they have an ‘indefinite operational life’ as stated by (Want, 2006). The tags are also small enough to be embedded into electronic devices or even to an adhesive label.

A passive tag may use one of the following frequencies shown below (Zayou et al., 2014), which consequently affects its read range.

Type	LF	HF	UHF
Range : (passive)	Few centimeters	50 cm	6 m
Advantages	- Non affected by water - Non affected by metals - Frequency use without restriction	- Non affected by water - Non affected by metals - Multiple tag read	- Long range - Standard - High rate - Easy to produce with low cost (5 cents)

		- Non affected by electrical noise	
Drawbacks	- Expansive - Noise - Low rate (70 ms to read one tag)	- Range < 1m - Less efficient than LF (water and metals)	- Absorbed by water - Reflected by metals - limited memory - interference with many applications
Applications	- Animal tracking - Identification	- Credit card, Access control card - Passports	- Industry - Retail Chain

Table 1Types of Frequencies used by a Passive RFID Tags

2.5.1 Application areas of RFID

RFID is used for a wide range of applications in almost every field including health, education, industry, transport, security, warehousing, internet of things agriculture, just to mention but a few.

In their paper "Supply Chain Management for Generic and Military Applications using RFID", (Oh et al., 2012) extensively discuss how this technology is used in warehousing and military operations. (Zayou et al., 2014) further discusses the use of this technology in agriculture and environment monitoring.

RFID is greatly used in supply-chain management, this, according to (Oh et al., 2012), is attributed to the fact that they have an ability to create a seamless flow of information through all the layers of supply chain in near real time. They have other benefits that far surpass their predecessor technology, bar codes, as they do not require line of sight and can be read simultaneously. However, as further explained by (Oh et al., 2012) they have the problem of lost or damaged tags or readers that have to be addressed. RFID adoption in supply chain also faces other non-technical challenges such as the cost, lack of standards, resistance to cooperation to maintain information transparency and privacy concerns (Osyk et al., 2012)

In hospitals, RFID is used to enhance patient's safety by uniquely identifying a patient hence reducing mediational errors such as incorrect dose of medication, wrong time of administration of medication, wrong medications delivered due to misidentifying a patient among others (Lahtela et al., 2008) , the challenge here is the integration of the automated identification using RFID with the automatic medication dispenser to ensure the system works properly without confronting medication errors and lack of patient safety.

In precision agriculture, which is a farming management concept that utilizes modern technologies to improve farming efficiency, RFID has been used in a sub-soil sensing system to sense and collect data about the soil in order to aid in intelligent irrigation (Wang et al., 2014). It is also used in animal identification and tracking, and circulation of agricultural products (CHEN et al., 2013)

Many researchers have done many studies on the adoption and application of RFID technology, however, very little has been done on how this technology can be used to track electronic devices at the exit points of institutions or buildings. Indeed, a need exits for a theft detection system in order to end electronics theft from our universities.

2.6 Proposed Solution

RFID tags have a microchip that is used to store information such as a unique serial number. The antenna enables the microchip to transmit the information to a reader which then transforms the information into a format that is understandable by the computer.

All electronic devices have a globally unique serial number. The RFID system will involve tagging these machines with a transponder tag which will store their serial number, the transponder unique id together with the device serial number will in turn be stored in a database using a web application.

At the exit point of the university, students, staff and visitors will be scanned by a guard on duty using an RFID reader which will transmit the serial number of their machine via Bluetooth to an office computer system or an NFC enabled tablet in order to validate the ownership of the device.

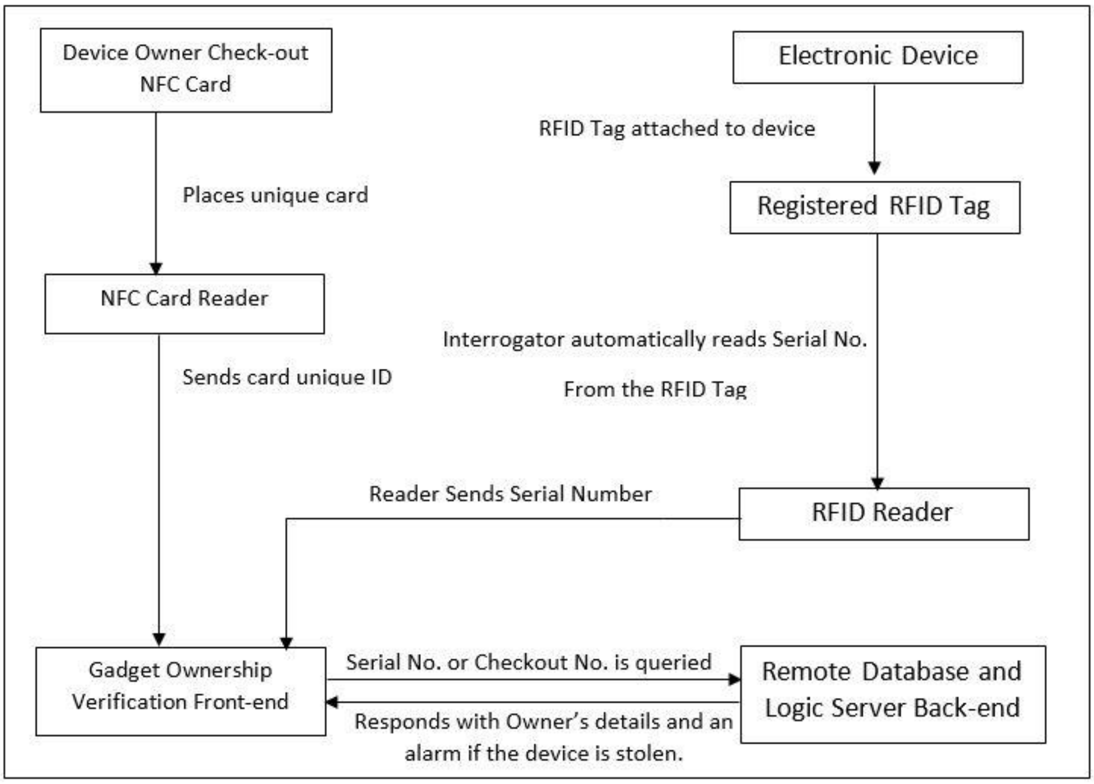

Device Owner Check-out NFC Card
Places unique card
NFC Card Reader
Sends card unique ID
Electronic Device
RFID Tag attached to device
Registered RFID Tag
Interrogator automatically reads Serial No.
From the RFID Tag
RFID Reader
Reader Sends Serial Number
Gadget Ownership Verification Front-end
Serial No. or Checkout No. is queried
Responds with Owner's details and an alarm if the device is stolen.
Remote Database and Logic Server Back-end

Figure 1 Conceptual Framework of the System

Chapter 3: Research Methodology

3.1 Introduction

This project is based on experimental research. A prototype will be designed and developed, thereafter, the prototype will be evaluated in order to come up with appropriate conclusions and recommendations.

This chapter presents the research methods that I will use for the course of the study in order to achieve my research objectives. It covers the methodology, research design, data collection procedures, data analysis techniques and data presentation procedures.

3.2 Methodology

In this project, the Agile methodology; Dynamic Systems Development Method (DSDM) Atern was used. The choice of this methodology was guided by the need to have a working system with high speed, high quality and within tight timescales.

The DSDM Atern methodology is a practical methodology that provides everything that is needed to specify and design all types of projects including IT Systems. The distinguishing features and advantages of using DSDM Atern methodology as discussed by (Dybå and Dingsøyr, 2015) Include:

- Agile methods are flexible in that they embrace change. With the current speed on technology revolution, change is inevitable before, during and after the development of a system. Unlike the traditional water fall model, DSDM Atern accommodates any change that occurs during the software development life cycle.
- DSDM Atern is focused on simplicity without compromising quality. More code will mean more bugs hence every functionality should well designed and kept simple but the quality of the system is given the highest priority.
- DSDM Atern encourages sustainable development, this is because it is always expected for a business need which a system solves to grow and therefore the system should always be able to accommodate those changes. This ensures that the systems created are sustainable.
- Iterative and Incremental Development. The traditional waterfall model had no option of going back to some steps once they were done, in DSDM Atern, you can always go back. Here iterative means the capability of going back to some

of the steps while incremental implies that there are small releases and in each release, it will always build on the previous function.

- In a DSDM Atern project, requirements are prioritized using the MoSCoW prioritization technique, the letters in the acronym stands for
    - Must have ~ these are features that must be included in the system, if this requirement is left out then the project has failed.
    - Should have ~ these are the features that are not very critical but are still very important to the system. These requirements are of high value to the users.
    - Could have ~ these are the features that can be included in the system if it does not cost much time and effort. These requirements might be removed from the project scope if the project timescale is at risk.
    - Won't have this time ~ these are the requirements that are requested but are excluded from the project scope due to certain constraints.

  This ensures that the most important requirements come first in the priority list hence delivering the most important functionalities on time and on budget.

The project used the five phases of DSDM Atern lifecycle as discussed by (Tri et al., 2016)

- Feasibility Phase ~ here a through feasibility assessment of the needs of the system were looked into. This included an overview of the project from a business and technical perspective. The outcome of this phase was an outline solution and a feasibility prototype.
- Foundations phase ~ this phase focused on the definition and prioritization of the system requirements. High level models were used to analyze the scope of the system project. The end to end diagrams were used to communicate the requirements, and identify the inconsistencies, dependencies and omissions.
- Exploration phase ~ in this phase, the business model, design model and prototype for the system were developed. This was done incrementally in order to deliver detailed models as each increment is undertaken.
- Engineering phase ~ this phase involved the building of the system which was informed by the models from the previous phase. The system was built

incrementally, a module at a time to ensure that the system is precise and detailed.

- Deployment phase ~ this phase involved running the prototype as if it were on a productive environment and testing it. Both black box and white box testing were performed to the prototype during this phase.

3.3 Research Design

This project started by reviewing the relevant literature including the current technological and non-technological solutions for securing electronics assets and went further to study the RFID technology which this solution uses. The literature reviews was used to understand how RFIDs have been used in other fields like supply chain management to track and monitor goods.

The requirements of this RFID security solution for electronic assets was derived from the observation of users interacting with a live barcode system. The choice of this observation was informed by the need to gain in-depth understanding of live users' interacting with the barcode system.

The RFID system was then developed using the DSDM Atern methodology of developing information systems. This methodology was chosen since it enables incremental delivery of the solution at every phase hence ensuring that the project ends on time and on budget. This methodology was used for the analysis and design of the RFID system.

The data generated by the system was analyzed to get the average response time. This average was compared to the date collection. The evaluation of the system and the comparison of the data formed the basis of concluding on the system.

3.4 Data Collection Procedure

This study used the observation data collection method. The researcher observed users interacting with the RFID application and measured the transaction duration as carried out by the users. The transaction durations were compared to the durations generated by the system to ascertain the functionalities of the system. Measurements of the transactions were done in different scenarios/settings.

3.4.1 Observation Settings

During this data collection, the study focused on specific activities as carried out by the user during the transaction execution.

1. Scenario One: A student being checked-in using the manual handwritten record method.
2. Scenario Two: A student being check-out using the manual handwritten method.
3. Scenario Three: A student being checked-out using the bar code system.
4. Scenario Four: An experiment of the time taken to check-out a student using the RFID system.

Twenty five runs were performed on each of the scenarios in order to ascertain their efficiencies. The experiment will be performed repeatedly and the results are within a narrow margin and are non-parametric (Cumming, n.d. 2011) hence, a minimum sample size of fifteen can be able to demonstrate a valid statistical significance (Mugenda and Mugenda, 2012)

3.5 Transactions of the RFID System

The transactions for this system were as outlined below:

- Application launch ~ this defines opening the RFID application for use. A web browser was used to open the application.
- Application Login ~ this transaction was defined as the activities from the time a user submits their login credentials to the time the user is completely authenticated to use the RFID application.
- Reading a tag ~ this transaction involved placing the RFID tag in the proximity of the reader in order for it to be interrogated. It included the time between when the readers beeps indicating a read and when that data appears on the web form.
- Querying the database ~ this transaction was defined as the activity from the time the query is done to when a response is given. The feedback was outputted on the web page.

- Application Logout ~ this transaction encompassed the activity from when the user clicks on the logout command to when they are completely logged out of the application.

Transaction durations were measured as follows:

- Application launch duration ~ duration form the time a user enters the application web address to the time the application is opened on the users' web browser.
- Application login duration ~ duration from the time the user submits their login credentials to the time they are authenticated and the application is fully available for use.
- Reading a tag ~ duration from the time the reader beeps indicating a read to the time when the data appears on the web form.
- Querying a database ~ this is the duration from the time the query is made to the time that feedback is displayed on the web page.
- Application logout ~ this is the time from when the user clicks on the logout button to the time the application completely logs them out and redirects to the login page.

3.6 Data Analysis

The collected data will be analyzed using quantitative data analysis method. This involved descriptive analysis where the frequencies and percentages will be used to present the quantitative data in form of tables and graphs.

According to (Mugenda and Mugenda, 2012), a sample size of 10% from the target population can make a reasonable size for experimental studies, or 30% or more is required for descriptive studies. This study will use 10% of the total target sample size to conclusively evaluate the study.

3.7 Tools Design

The RFID system was developed using the Arduino Integrated development environment. The system runs on the web platform which provides the user interface. The database runs on MySQL RDBMS.

3.7.1 Tools and Skills

In realization of the goals of this project, the following tools were used:

a) Arduino IDE
b) MySQL database
c) Web platform
d) Internet services
e) Web programming skills

3.8 System Design

The system was designed using the DSDM Atern methodology guidelines. In designing the system, we focused on show how the different components will interact and work together in order to achieve the projects objectives.

3.9 System Evaluation and Recommendations

The system was evaluated by analyzing the data generated by the system. Based on the interpretation of the results further study is recommended on the system.

Chapter 4: System Analysis and Design

4.0 Introduction

This phase involved analysis and design of the proposed system. The system has been developed to demonstrate the use of RFID technology in tracking of electronic assets. The system has been developed using the Agile development methodology: DSDM Atern which is used for developing software systems in a flexible manner.

4.1 System Analysis

Analysis started by reviewing literature on some of the existing system that are used for tracking electronic devices. In order to gather the requirements of the system to be developed, we studied how the manual bar code system works.

4.1.1 Observed the Bar Code System

The analysis phase was done to understand the requirements of the system to be developed. It involved observing a user interacting with the bar code system. The user interactions that were observed included all transactions involved in checking-out a machine using the bar code application. These transactions included:

- Launching the application from a web browser
- Logging into the application using an email address and password
- Scanning a device serial number
- Reading the users details
- Logging off the application

In order to measure transaction duration in this setting, an online clock system was used. This used the start stop mechanism. Measurement of the transaction durations was done while the user was carrying out the transaction.

4.1.2 Proposed System

The proposed system was developed to demonstrate the use of RFID in tracking electronic devices. The proposed system eliminates the need to have and use a bar code scanner which requires line of sight and hence enable automatic identification of tagged devices.

The system will also demonstrate how the elimination of a human user during the transaction will improve the accuracy and efficiency of the system.

4.1.3 User Requirements

This section identifies what the user understands as the expected functionalities of the system. Requirements were generated from the manual system observed. This included:

- A user should be able to login to the system
- A user should be able to scan the barcode of a device using a barcode scanner
- The system should poll the database for relevant information
- The system should notify the user of a stolen device
- Provide historic as well as real time data of the applications performances
- The performance measures should be measured by the system during user interaction

4.1.4 System Functional Requirements

These requirements describe the requirements expected from the system. The system required from the user requirements in this system include:

- All users should be authenticated by use of an email address and a password which will have been stored in the database.
- The system should be able to pick the starting time and completion time of a transaction during a device search.
- The system should use the start and completion time of a transaction to calculate the transaction duration.
- The calculated durations should be stored in a database.
- Users should be able to query the database for real time and historical data.
- Users should interact with the system on a graphical user interface.

4.1.5 System Non-Functional Requirements

- Performance Requirements: The system should operate with minimum supervisions upon its deployment. It should be self-healing and therefore be able to recover automatically when a module fails, or be up with minimum intervention.
- Privacy Requirements: all the sensitive data like passwords should be hashed before they are stored in the database.
- Maintainable: the system should be easy to update and maintain, the different modules should require minimum effort to maintain.

4.2 Analysis using DSDM Atern

The Agile methodology: Dynamic Software Development (DSDM) Atern was used in the analysis phase of this system. This methodology is mainly used for designing and developing software projects.

4.2.1 System Specification

This phase involved specifying the system functionalities using goals and scenarios. It also involved identifying the system inputs, outputs and external data that describes the system's interface to its environment. The phase started with a brief description of the system then proceeded to define the requirements of the system in terms of:

- The use case scenarios
- Functionalities, and
- The interface of the system

4.2.1.1 System Description

The propose system provides an RFID solution to tracking of electronic assets. The system demonstrate the use of radio frequency identification technology in securing electronic assets by tagging the assets with RFID tags and having readers at the exit point to automatically and intelligently detect an electronic device as a user exits with it from the institution or building.

4.2.1.2 Overall System Goal

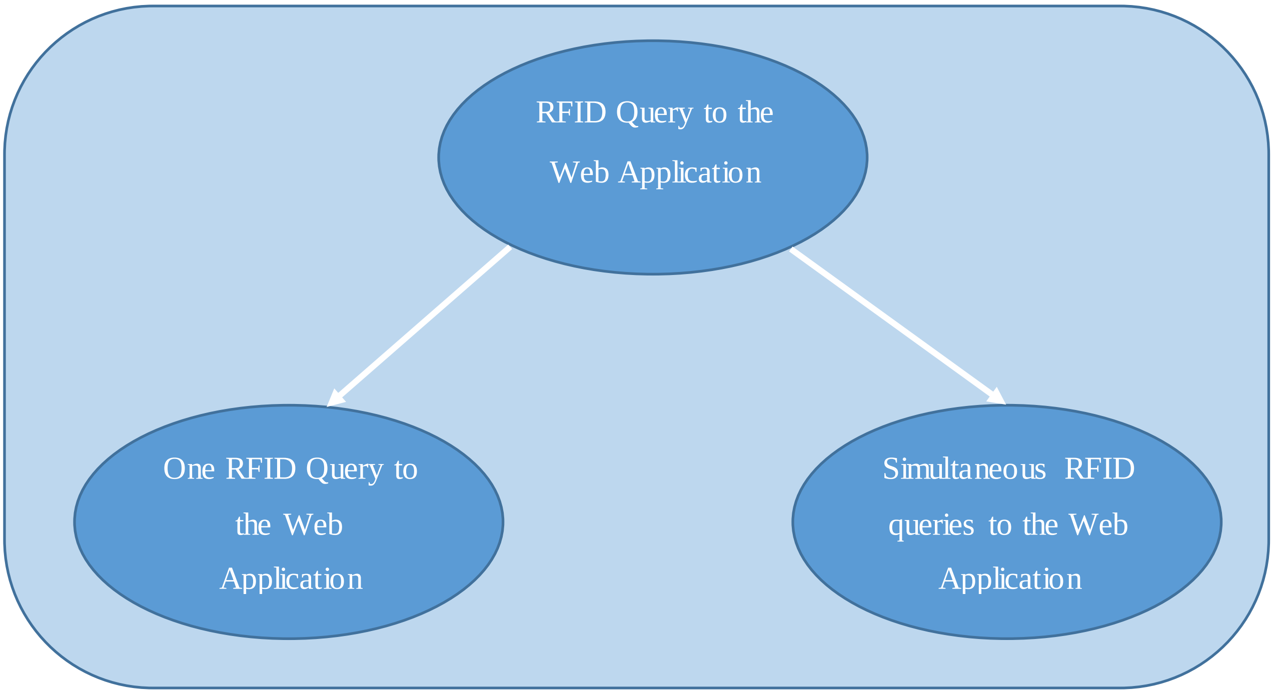
The system goals describe the main purpose of the system, what the system is expected to achieve. The overall goal of the system is to use RFID technology to automatically detect and verify device ownership. Above all, it will measure the effectiveness of the system through measurement of performance metrics such as detection rate and response time.

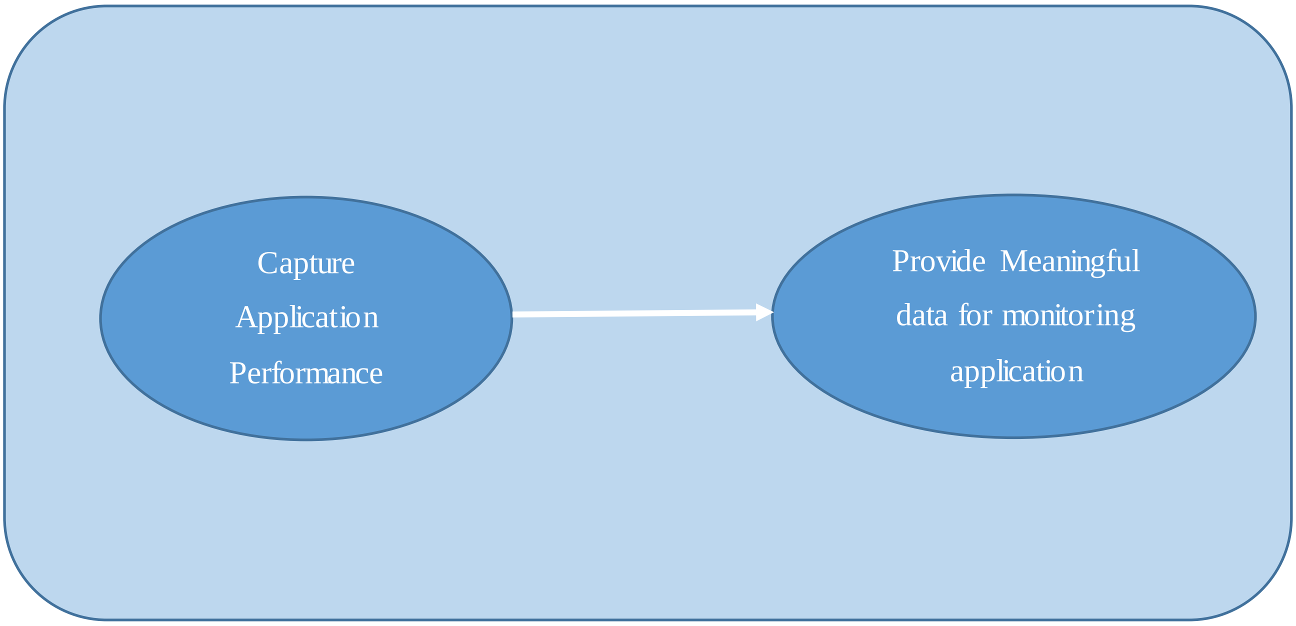
4.2.1.3 System Sub-Goals

The sub-goals for the system as derived from the main goal of the system were defined as below:

- Allow one RFID query to the web application
- Allow more than one RFID query to the web application simultaneously

- Provide meaningful data for monitoring and tracking the application performance.


RFID Query to the Web Application
One RFID Query to the Web Application
Simultaneous RFID queries to the Web Application


Capture Application Performance
Provide Meaningful data for monitoring application

4.2.1.4 Use Case Scenario

The use case scenario was used to represent specific system functionalities. They were used to describe sequence of events associated with a particular goal of the system or responding to a particular event.

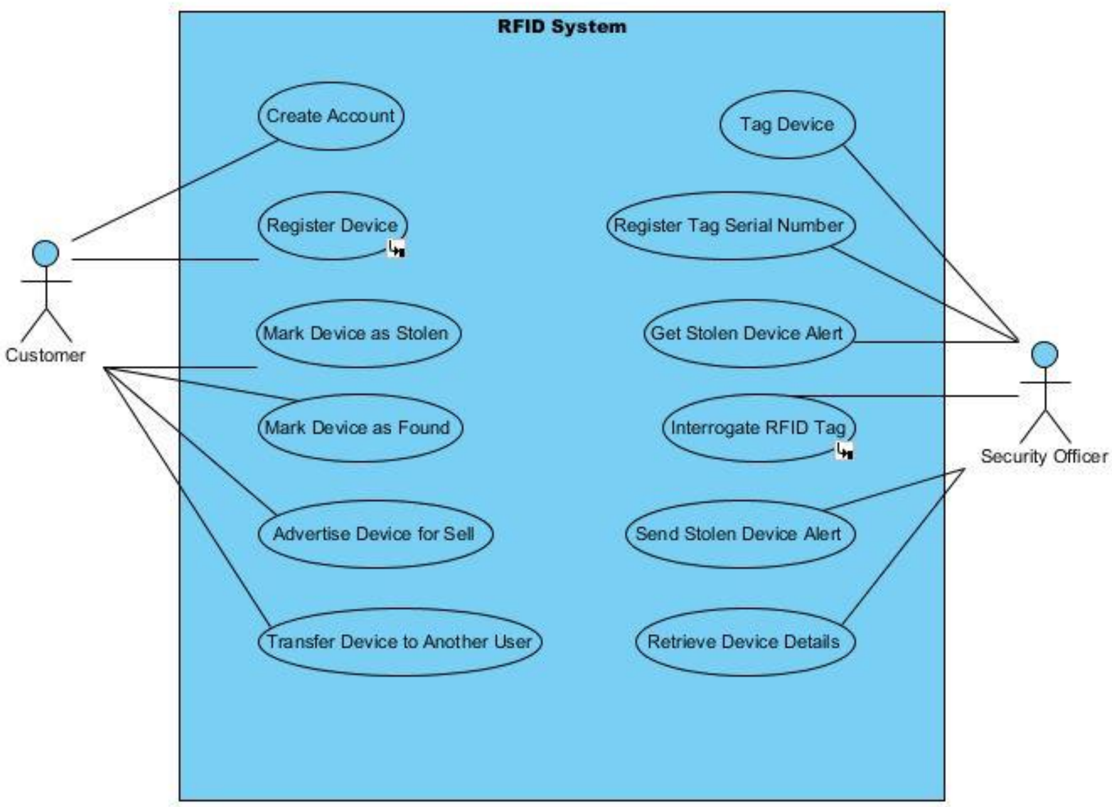


Figure 2 Use-Case of the System

4.2.1.5 System Functionalities

The system functionalities are derived from the system goals. The functionalities define what the system is capable of doing. In this project the system functionalities identified were:

- User details management on the database i.e. registration and modification.
- Device details management on the database i.e. registration and modification.
- One or more RFID interaction with the web application.
- Measurement of performance during user interaction with the web application.
- Provide historic as well as real time data of the application performances.

4.3 System Design

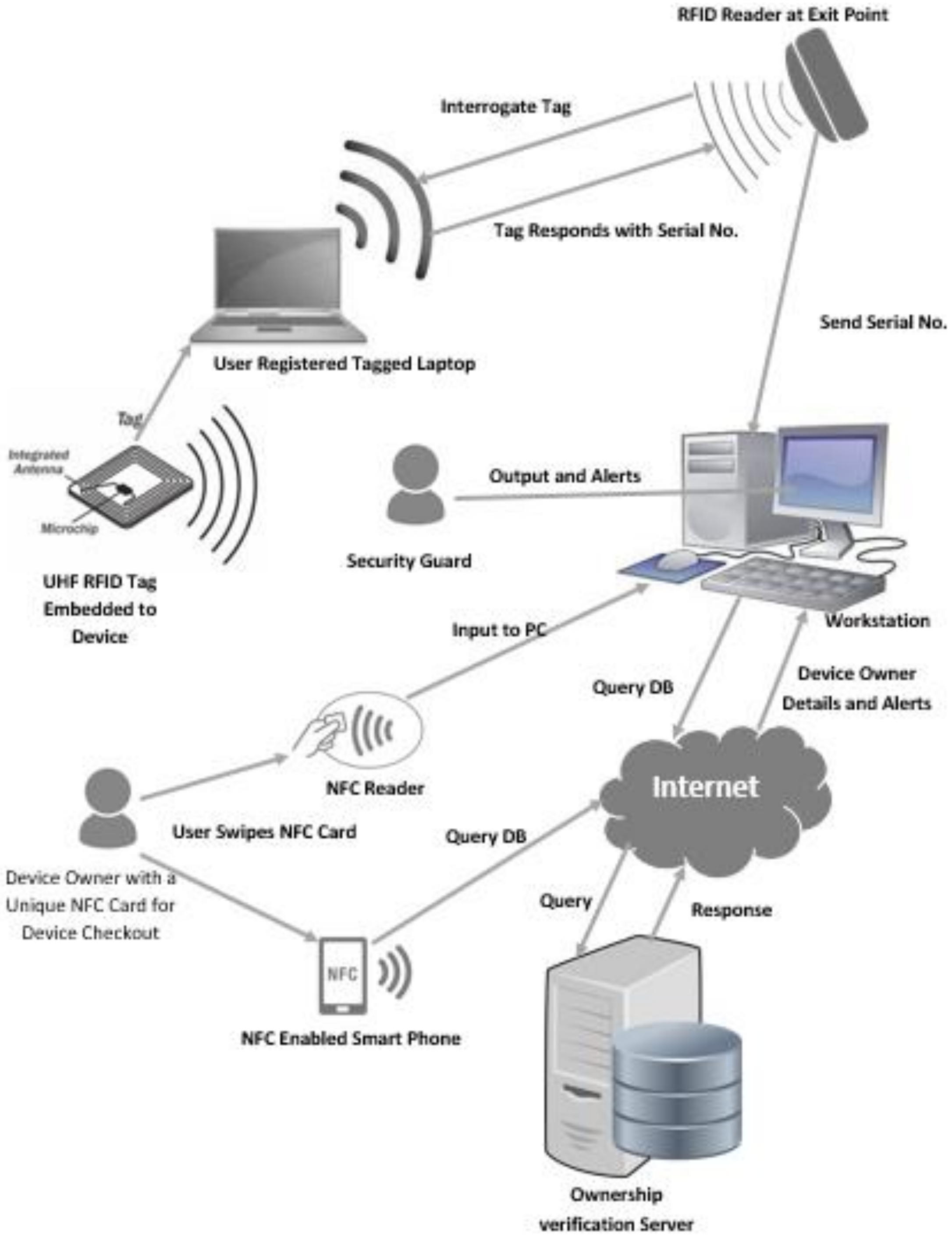
4.3.1 Architectural Goals and Constraints

This section describes the software requirements and the objectives that have some significant impact on the architecture of the entire system.

- Technical Platform: The web interface will be hosted on a Linux server.
- Persistence: Data will be saved in a MySQL relational database.
- Security: the system will be secured in order to ensure that only authenticated users can make changes to their electronics details. Users will have to login using a username and a password. The passwords will be hashed using SHA2 before they are saved in the database.
- Availability: High availability is required since the system is supposed to be a real-time system. Lack of availability may make the system non-reliable since a stolen device may not be detected. The target availability is 24 hours a day, 7 days a week. Maintenance will be done in a parallel change over manner, hence not affecting the availability of the system.
- Performance: Search queries should answered 98% of the time below 5 secs.

4.3.2 System Architecture

The RFID System Architecture will be as shown below.



RFID Reader at Exit Point
Interrogate Tag
Tag Responds with Serial No.
Send Serial No.
User Registered Tagged Laptop
Tag
Integrated Antenna
Microchip
UHF RFID Tag Embedded to Device
Output and Alerts
Security Guard
Workstation
Input to PC
Query DB
Device Owner Details and Alerts
NFC Reader
User Swipes NFC Card
Query DB
Internet
Device Owner with a Unique NFC Card for Device Checkout
Query
Response
NFC
NFC Enabled Smart Phone
Ownership verification Server

Figure 3 Overall System Architecture

4.4 Data Flow Diagrams (DFD)

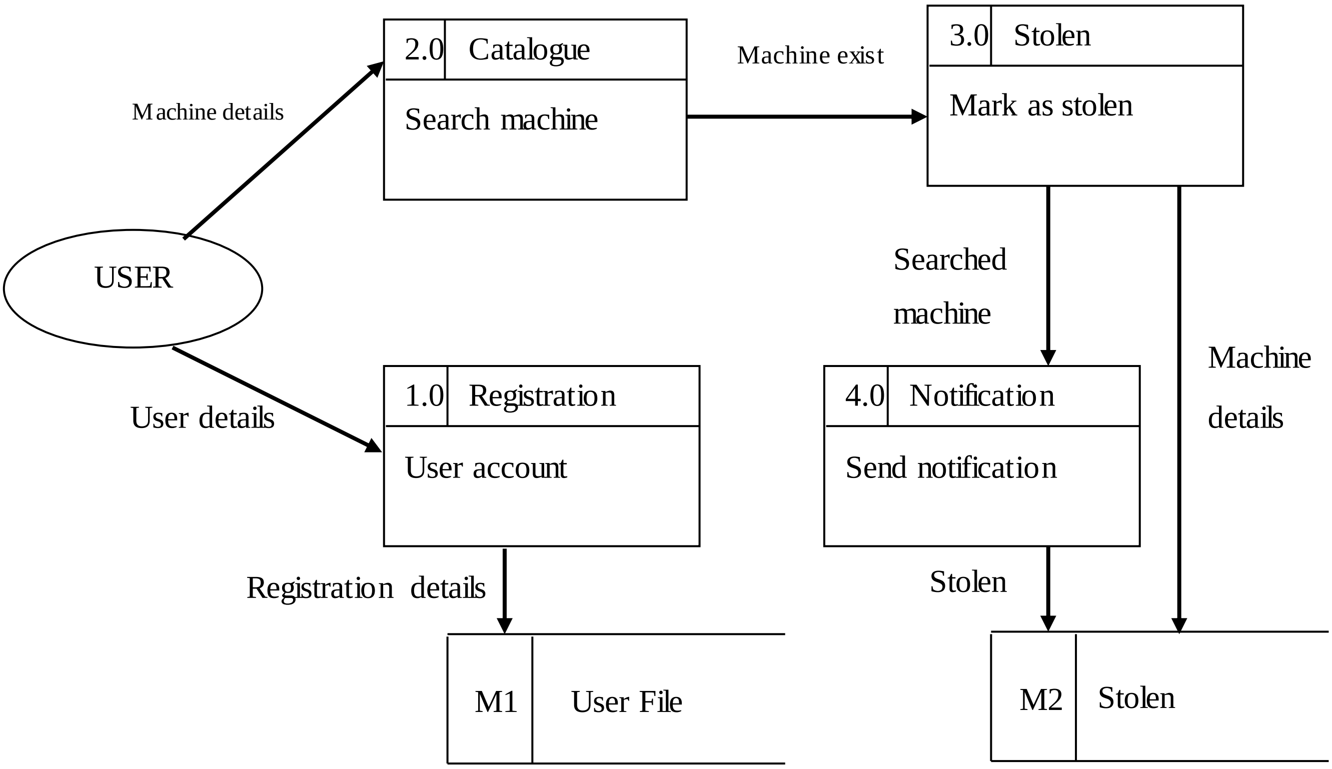
Data flow Diagram is a process model, which shows the systems input, processing and output of data. It functionally decomposes the requirements specifications down to the lowest level of details and describes the data flows through the system and not how data is processed. Process models may be used to model business systems usually at a fairly high level. DFD model shows the movement and processing action data is subjected to as it moves through the system.

4.4.1 Importance of a Data Flow Diagram

i. The diagram provides a basic understanding of how the system works.
ii. DFD simplifies the problem so as to make design stage easier.
iii. DFD may be drawn to represent different levels of details.

4.4.2 Level 1 DFD for the Proposed System

Figure 4: Level 1 DFD



4.5 Flowcharts

4.5.1 Device registration flowchart

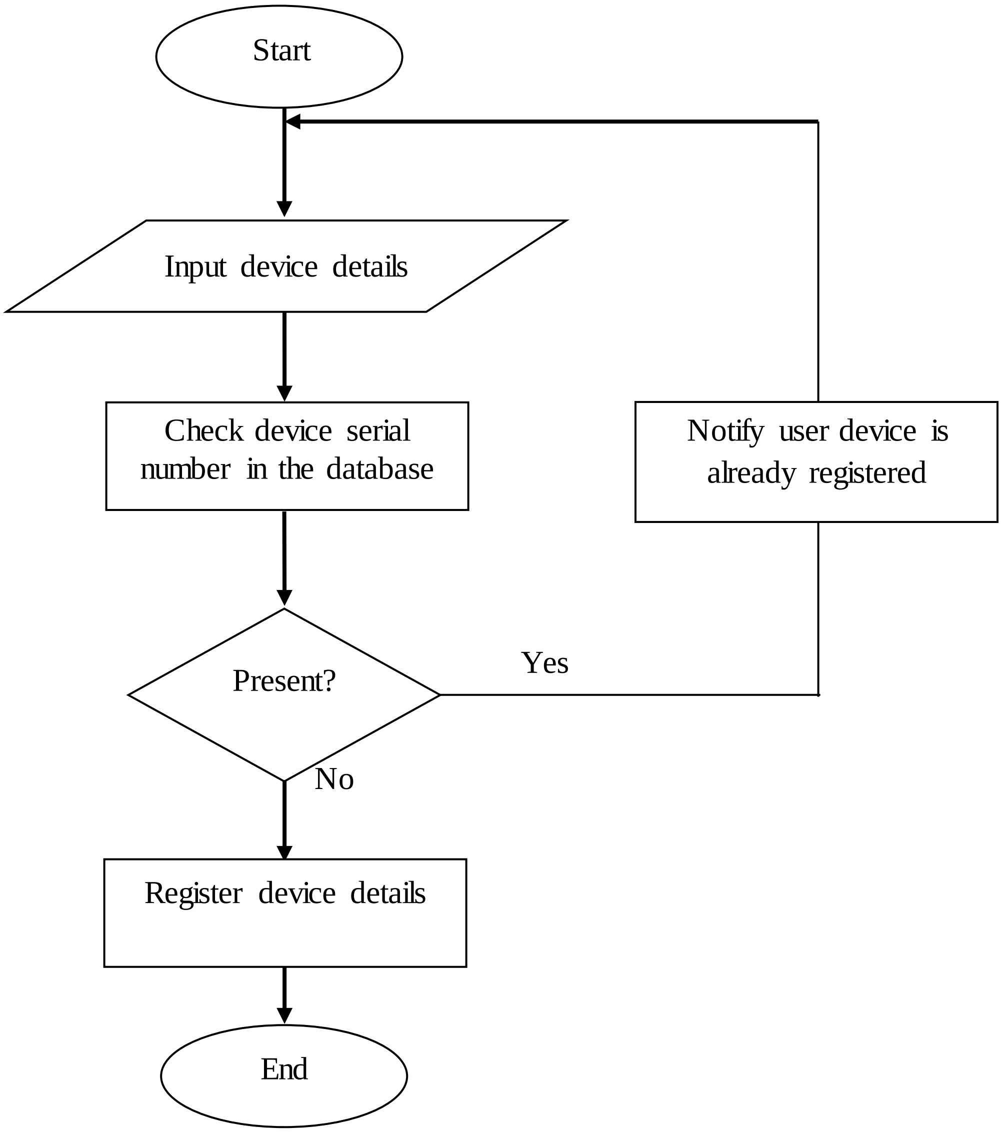

Start
Input device details
Check device serial number in the database
Notify user device is already registered
Present?
Yes
No
Register device details
End

Figure 5: Device registration flowchart

4.5.2 Search Device flow chart

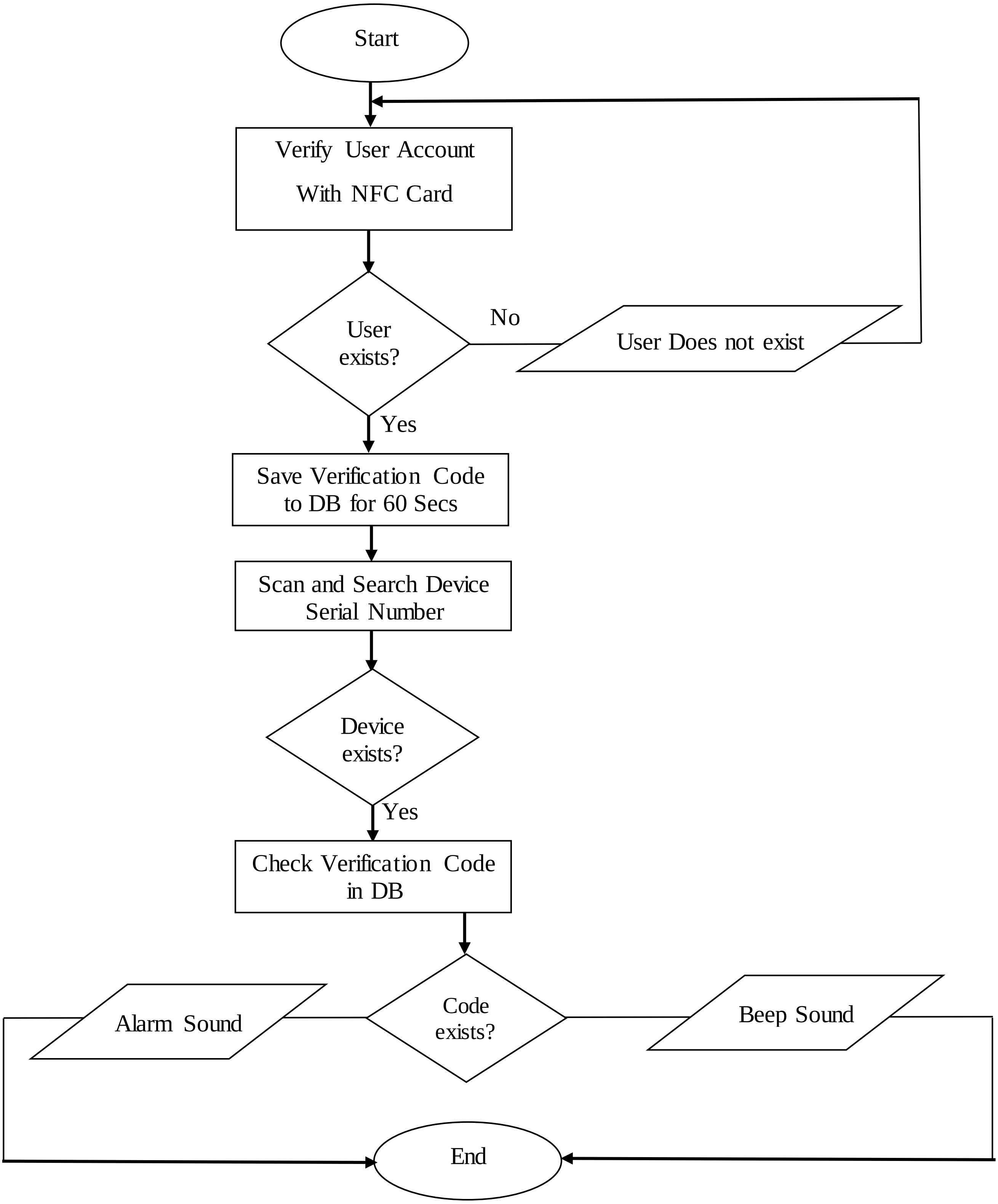


Figure 6: Search Device flow chart

4.6 Database Design

4.6.1 Normalized Database

Table 2: Normalized database

UNNORMALIZED	1st NORMAL FORM	2nd NORMAL FORM
1. National id number	**User**	**User**
2. First name	1. ID	1. ID
3. Last name	2. First Name	2. First Name
4. User email	3. Last Name	3. Last Name
5. Gender	4. Email	4. Email
6. Location	5. DOB	5. DOB
7. Contacts	6. National ID	6. National ID
8. Username	7. Gender	7. Gender
9. NFC Card No.	8. Contacts	8. Contacts
10. D.O.B	9. Location	9. NFC Card No.
11. Date in	10. NFC Card No.	10. Location
12. Date out	11. Password	11. Password
13. Group id	12. Date in	**Stolen_devices**
14. Ob number	13. Date out	1. Id_no
15. Police station Name	14. Visitor id	2. Serial
16. Police Number	15. Group id	3. Comment
17. Comment		4. Police name
18. Profile picture	**Devices**	5. Police ob
19. Suspect	1. Id_no	6. Police contact
20. Time	2. Name	**Share**
21. Status	3. Model	1. Owner_id
22. Group name	4. Serial	2. Id_no
23. Description	5. Police name	3. Serial
24. Category	6. Police ob	**Profile_pic**
25. Title	7. Police contact	1. Id_no
	8. Owner_id	2. Picture
	9. Location	**Notification**
	10. Comment	1. Id_no
	11. Price	2. Sus_id

	12. Description 13. Category 14. Date 15. Time **Gate** 1. Gate id 2. Gate name 3. Username 4. Location 5. Email 6. Contacts 7. Password 8. Check in 9. Check out 10. Visitor 11. Image	3. Serial 4. Time 5. Status **Gates** 1. Gate id 2. Gate name 3. Username 4. Location 5. Email 6. Contacts 7. Password **Device** 1. Id_no 2. Name 3. Model 4. Serial **Advertise** 1. Image id 2. Image 3. Description 4. Title 5. Price 6. Date 7. Location

4.6.2 Data Dictionary

This is a term for information that describes the data that will be held in a database - the meta-data content. The data dictionary is a component of a well-documented database. It allows database users, including administrators and others who interface to the system to identify the expected data in each table and column of the database, even without accessing the database.

Table 3: User Details

Table Name	**Field Name**	**Data Type**	**Data Size in Bytes**	**Column Status**
User	ID	Number	25	NOT NULL
	First Name	Text	25	NOT NULL
	Last Name	Text	25	NOT NULL
	Email	Text	25	NOT NULL
	DOB	Date	25	NOT NULL
	National ID	Number	6	NOT NULL
	Gender	Text	10	NOT NULL
	NFC Card No	Text	25	NOT NULL
	Contacts	Text	15	NOT NULL
	Location	Text	25	NOT NULL
	Password	Text	25	NOT NULL

Table 4: Device

Table Name	**Field Name**	**Data Type**	**Data Size in Bytes**	**Column Status**
Device	Id_no	Number	6	NOT NULL
	Name	Text	20	NOT NULL
	Model	Text	20	NOT NULL
	Serial	Text	25	NOT NULL

Table 5: Advertise

Table Name	Field Name	Data Type	Data Size in Bytes	Column Status
Advertise	Image id	Number	5	NOT NULL
	Image	Text	20	NOT NULL
	Description	Text	50	NOT NULL
	Title	Text	25	NOT NULL
	Price	Text	25	NOT NULL
	Date	Date/Time	25	NOT NULL
	Location	Text	25	NOT NULL

Table 6: Stolen device

Table Name	Field Name	Data Type	Data Size in Bytes	Column Status
Stolen_device	Id_no	Number	6	NOT NULL
	Serial	Text	25	NOT NULL
	Comment	Text	50	NOT NULL
	Police name	Text	25	NULL
	Police ob	Text	25	NULL
	Police contact	Text	15	NULL

Table 7: Gates

Table Name	Field Name	Data Type	Data Size in Bytes	Column Status
Gates	Gate id	Number	5	NOT NULL
	Gate name	Text	25	NOT NULL
	Username	Text	20	NOT NULL
	Location	Text	25	NOT NULL
	Email	Text	25	NOT NULL
	Contacts	Text	15	NOT NULL
	Password	Text	25	NOT NULL

4.6.3 Entity Relationship Diagrams

An ER is part of a system development methodology that provides an understanding of the logical data requirements of a system independently of the systems' organization and processes. It reflects a static view of the relationship between different entities.

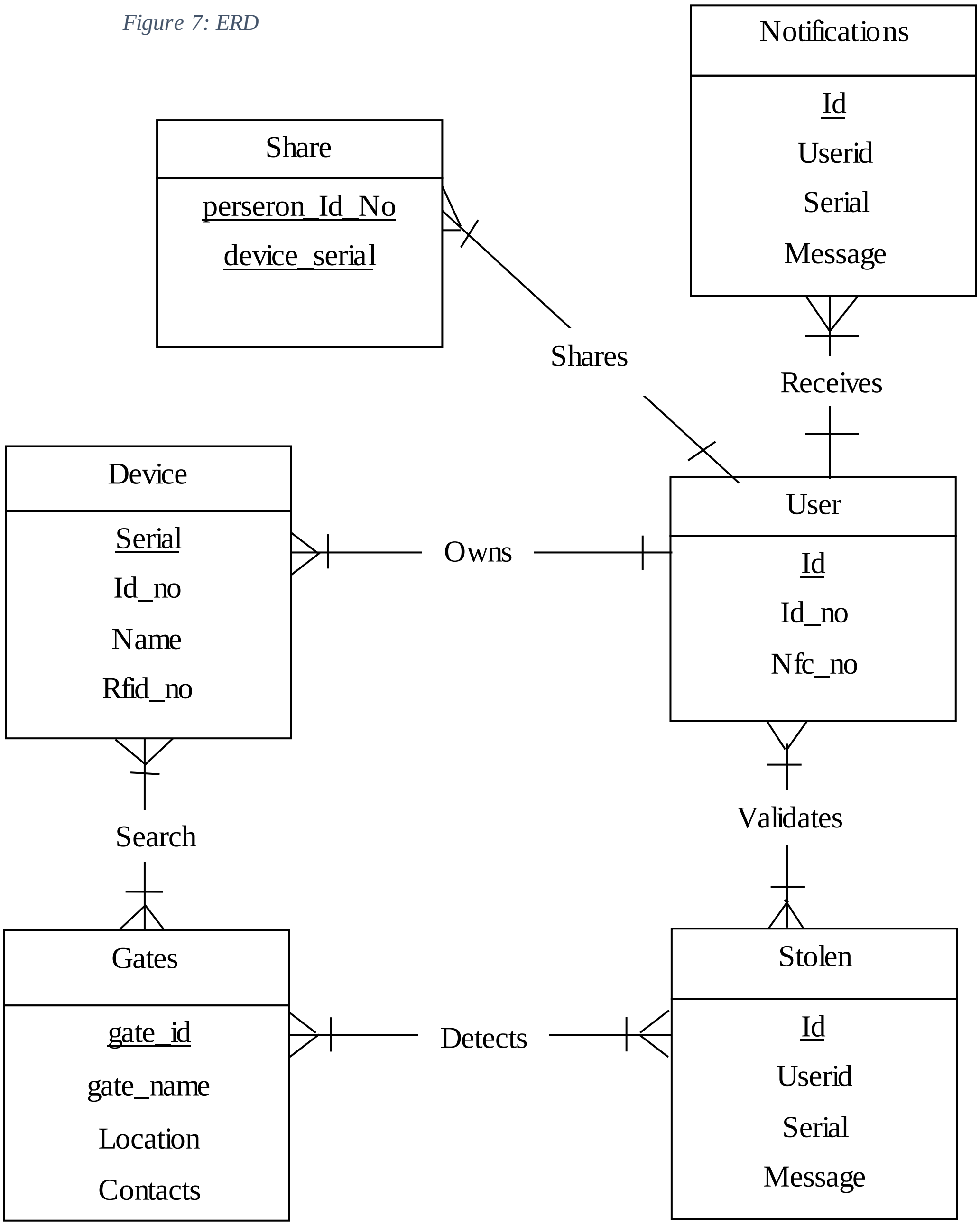
i. **One- to –one (1:1) -** for any entity type 1 there may only be one member of entity type 2 and for any entity of type 2, there is only one member of entity type 1 associated with it.

ii. **One-to-many (1: *) -** for any entity type 1 there may be many members of entity type 2, and for any entity type 2; there is only one member of entity type 1 associated with it.

iii. **Many-to-many (* :*) -** for any entity 1 and 2 there may be many members from each entity. For entities, which reflect a many to many, decomposition must be done so as to achieve data integrity.

ENTITY RELATIONSHIP DIAGRAM

Figure 7: ERD



4.7 System Interface

The System consists of various modules and entities which will be communicating concurrently in order to achieve its objectives. All these modules and entities need to interface with each other in order to facilitate the intercommunication between them. The diagram below shows the various interfaces required.

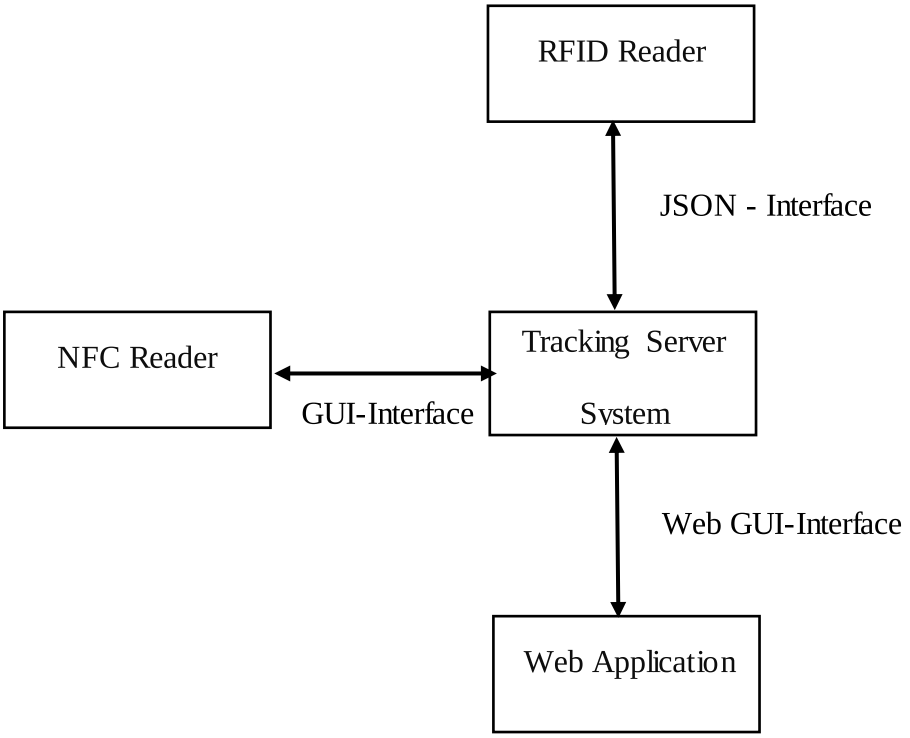


Figure 8 System Interface

4.7.1 The JSON Interface

The RFID Reader will communicate with the system using JSON which stands for JavaScript Object Notation, JSON is a standard format used to transmit data in form of attribute-values pairs. The JSON message format looks like this:

RFID Reader data format:

```
{
        “serial_no”:”CNDOSK238S”
}
```

The serial_no is the globally unique identification number of the rfid tag that has been tagged into the electronic device. It is sent to the system which checks to confirm that the exit of the device has been authorized by the NFC Card, If the checkout has been authorized, a value 1 is sent to the RFID reader which makes a beep sound, if it has not been authorized, then a value 0 is sent to the RFID reader which produces an alarm sound.

4.7.2 The GUI Interface

The Web Login Interface

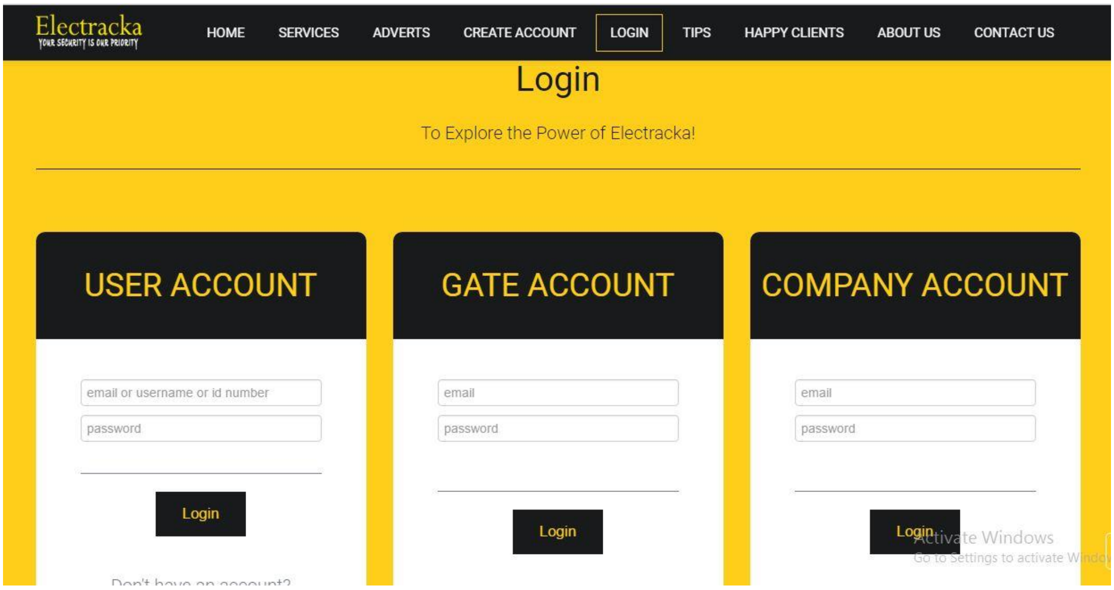


Figure 9 Web Login Interface

The Register Device Web Interface

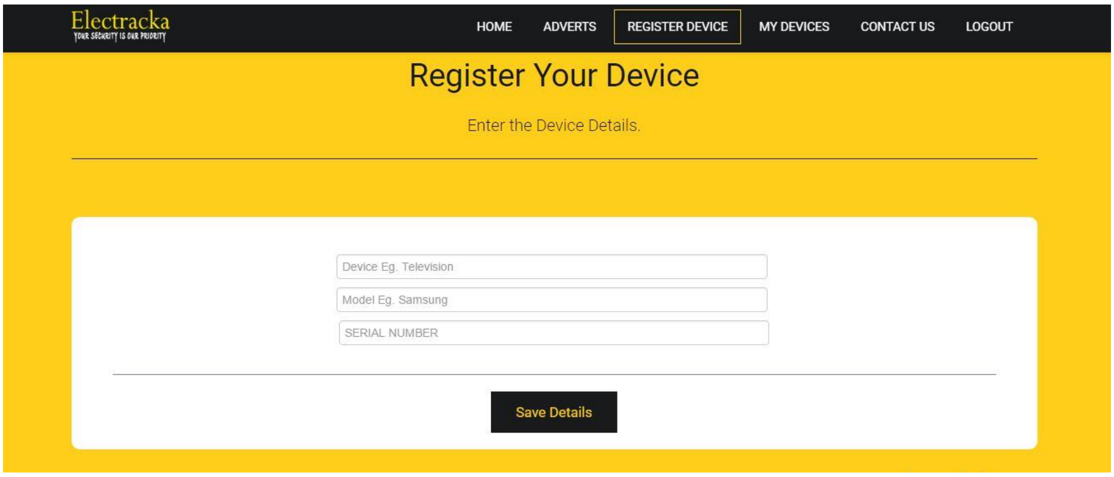


Figure 10 Register Device

The Device Checkout Interface

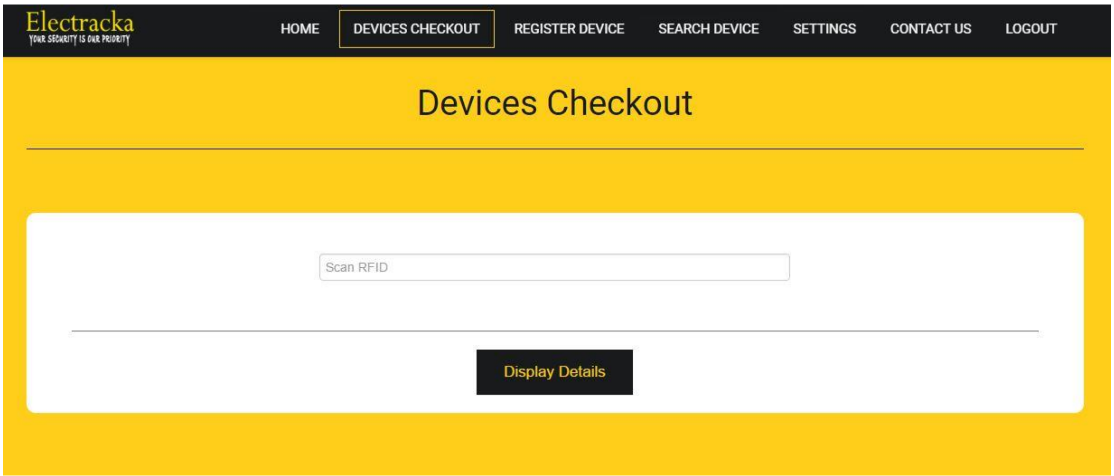


Figure 11 Device Checkout

Search Device Interface

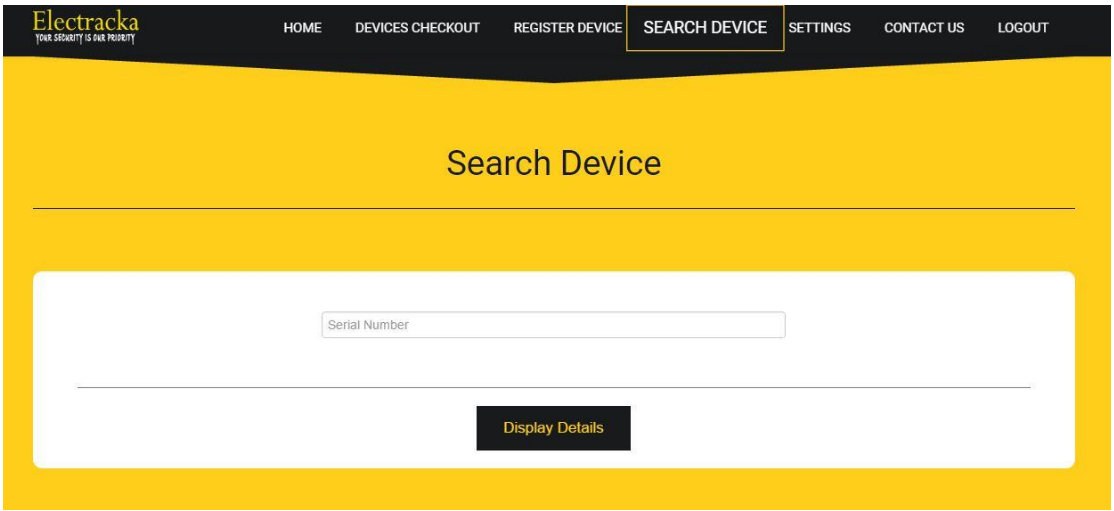


Figure 12 Search Device

Chapter 5: System Implementation and Testing

5.1 Arduino RFID Reader

The prototype RFID reader was built using the Arduino programming language. An Arduino Mega board was used as the microcontroller, while an MFRC522 RFID board was used as the reader.

According to the MFRC522 data sheet at (http://www.nxp.com/documents/data_sheet/MFRC522.pdf) it describes it as a highly integrated reader/writer integrated circuit that is used for contactless communication at 13.56 MHz

The prototype after the interconnection looked as shown in the diagram below:

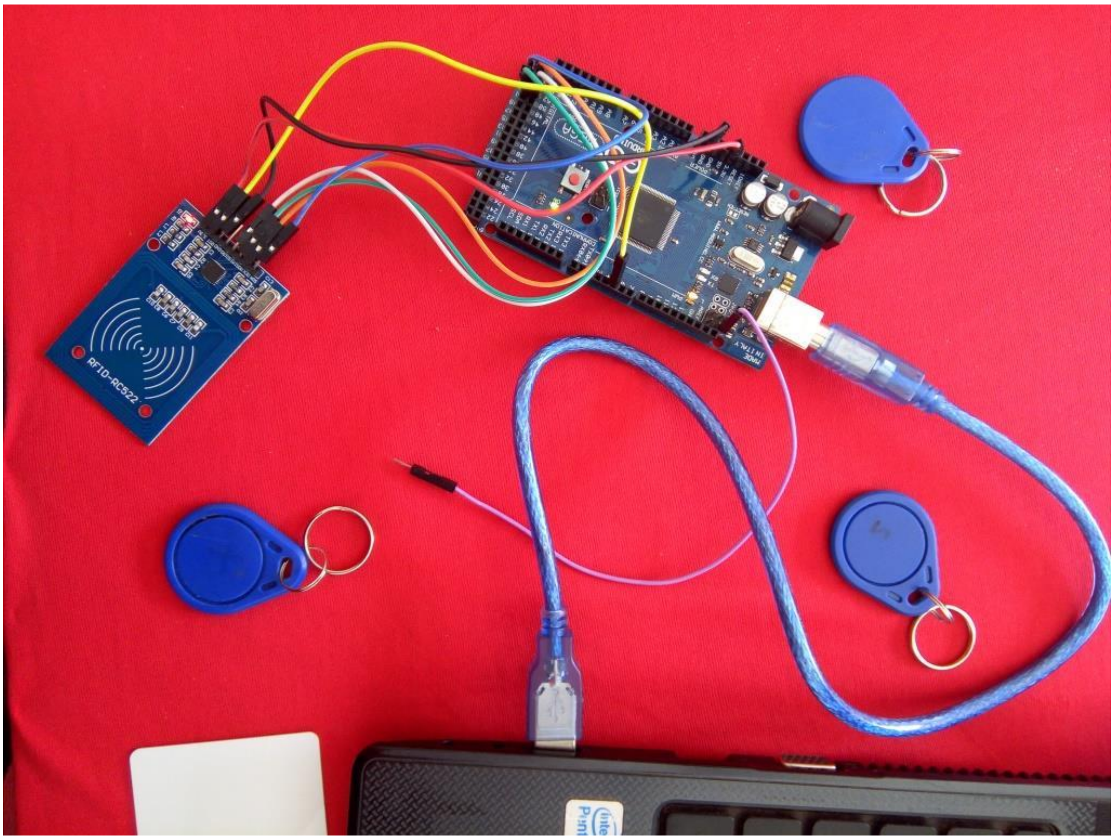


Figure 13 RFID Reader Prototype

After setting the Arduino RFID reader, I tested to confirm it could read the 13.56MHz RFID cards that I had and it succeeded. The images below were captured to illustrate that activity.

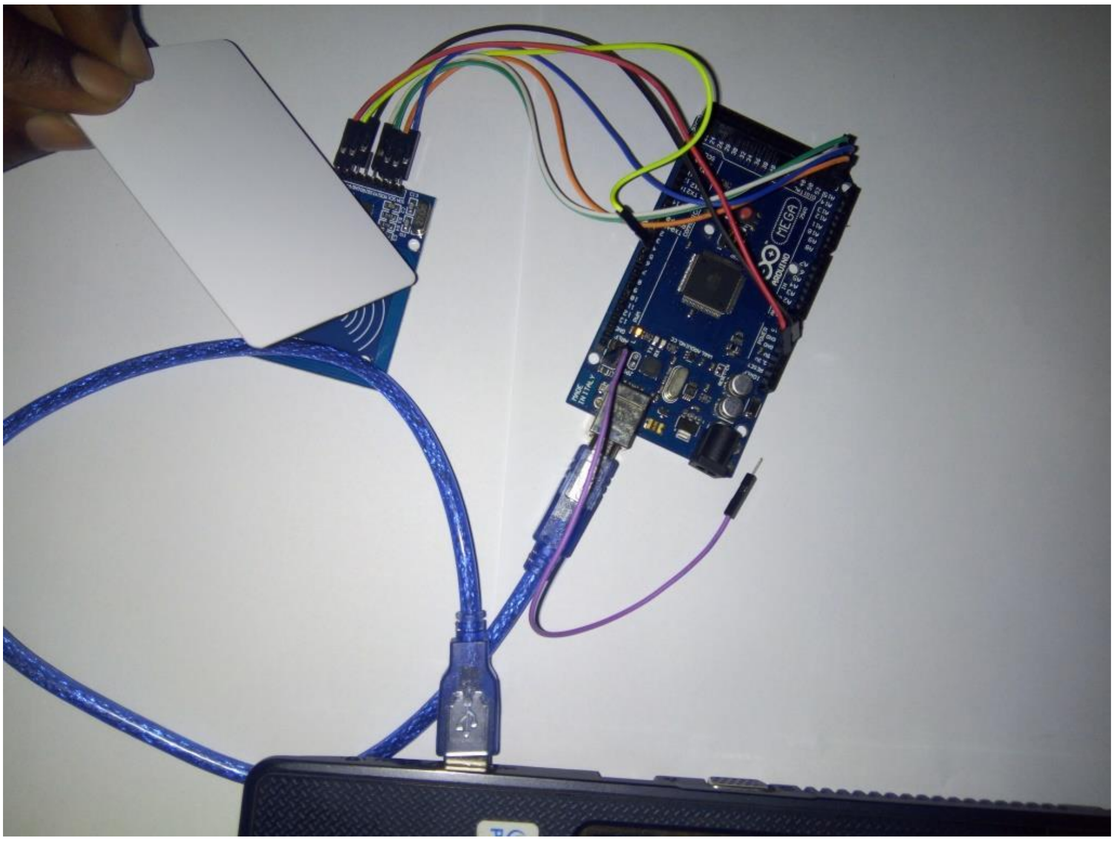


Figure 14 Reading a Tag

5.2 System testing

This is carried out to ascertain if the system actually delivers what the user needs are. Loading the system with reasonable amount of data to find out how first it can process it and how much data it can store without breaking down does this.

5.2.1 Approach of boxes

Software testing methods are traditionally divided into black box testing and white box testing. These two approaches are used to describe the point of view that a test engineer takes when designing test cases.

5.2.1.1 Black box testing

Black box testing treats the software as a "black box"—without any knowledge of internal implementation. Black box testing methods include: equivalence partitioning, boundary value analysis, all-pairs testing, fuzz testing, model-based testing, traceability matrix, exploratory testing and specification-based testing.

5.2.1.2 White box testing

White box testing is when the tester has access to the internal data structures and algorithms including the code that implement these.

The following types of white box testing exist:

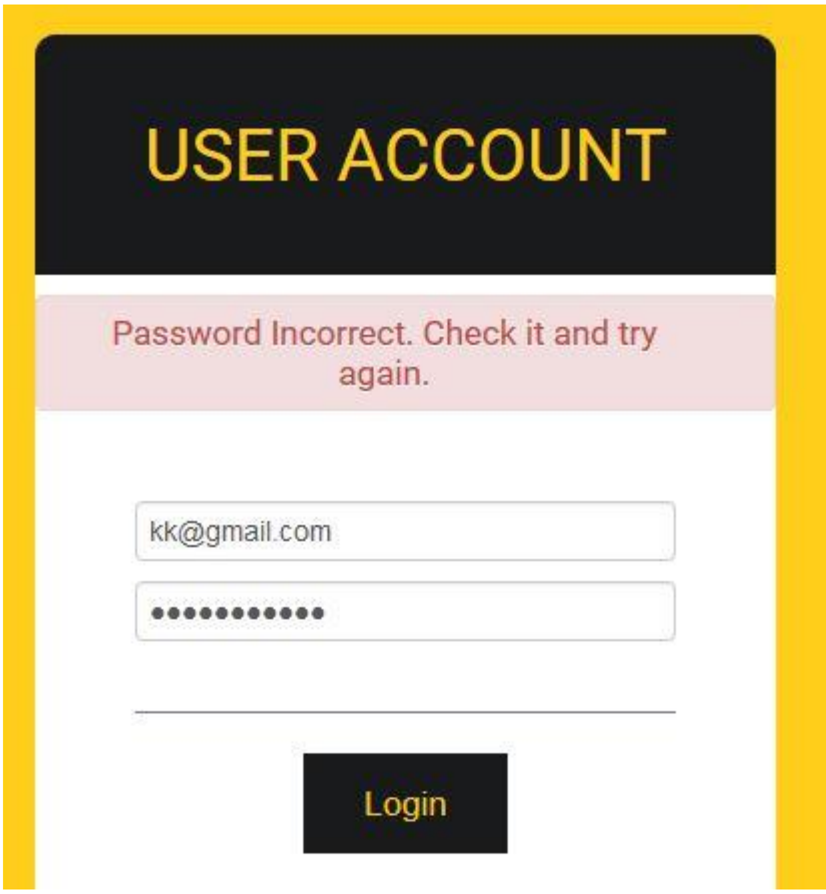
i. API testing (application programming interface) - Testing of the application using Public and Private APIs
ii. Code coverage - creating tests to satisfy some criteria of code coverage (e.g., the test designer can create tests to cause all statements in the program to be executed at least once)
iii. Fault injection methods
iv. Mutation testing methods
v. Static testing - White box testing includes all static testing

Testing

The areas of the system to be tested include:

a) Login form

If the user enters the correct username and password he/she will be able to view user home page. If user enters the wrong password an error message will be displayed, as show on the screen capture below.



Password Incorrect. Check it and try again.

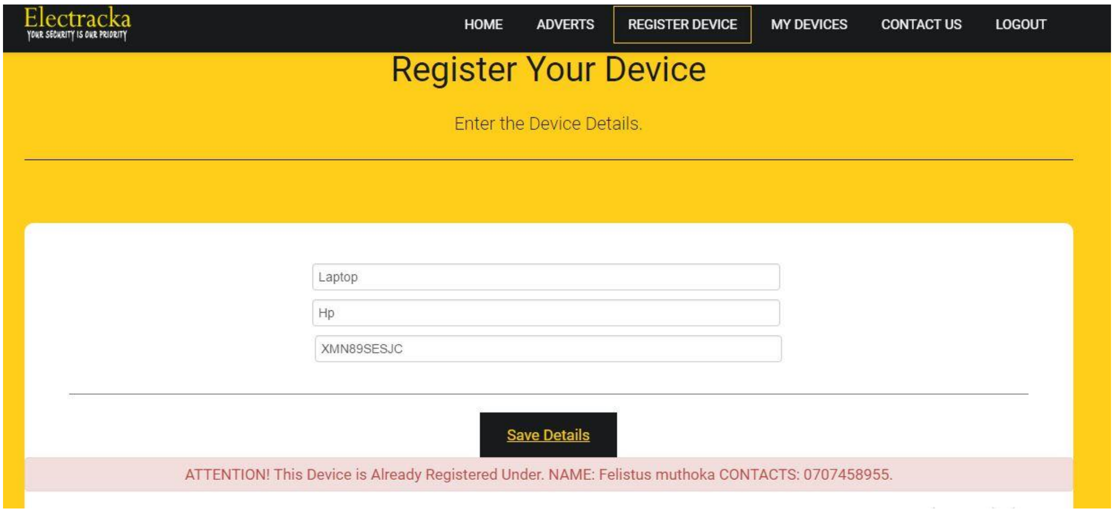
kk@gmail.com

••••••••••••

Figure 15 Username and Password Mismatch Feedback

b) Device registration form

If the user tries to register an already registered device, the following message shown on the screen capture below will be displayed by the system.



Register Your Device

Enter the Device Details.

Laptop

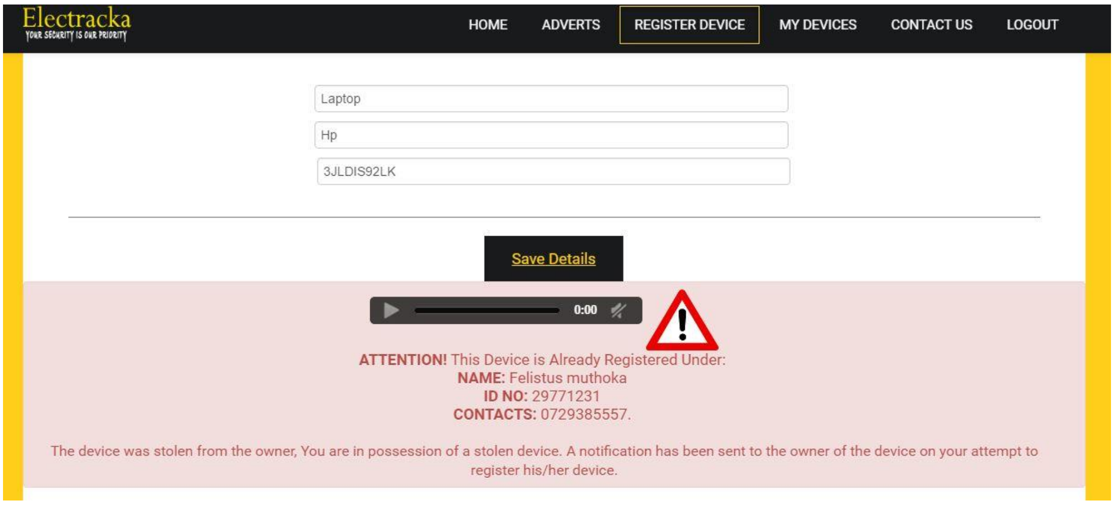
Hp

XMN89SESJC

ATTENTION! This Device is Already Registered Under. NAME: Felistus muthoka CONTACTS: 0707458955.

Figure 16 Registering Someone Else's Device

If the device trying to be registered is marked as stolen by the owner of the device, the following warning message will be displayed to the user as shown on the screen capture below.



Laptop

Hp

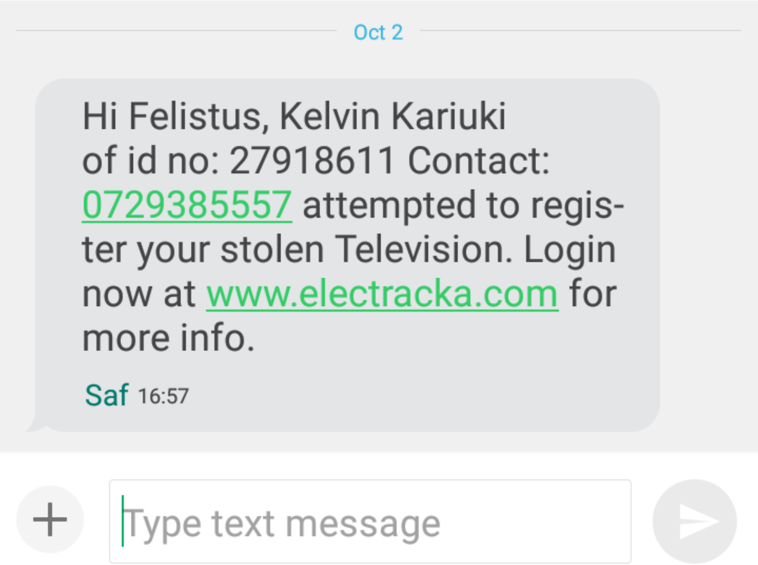
3JLDIS92LK

ATTENTION! This Device is Already Registered Under:
NAME: Felistus muthoka
ID NO: 29771231
CONTACTS: 0729385557.

The device was stolen from the owner, You are in possession of a stolen device. A notification has been sent to the owner of the device on your attempt to register his/her device.

Figure 17 Trying to Register a Device Marked as Stolen

The owner will also get an sms notification with your national identification details as shown below:



Oct 2

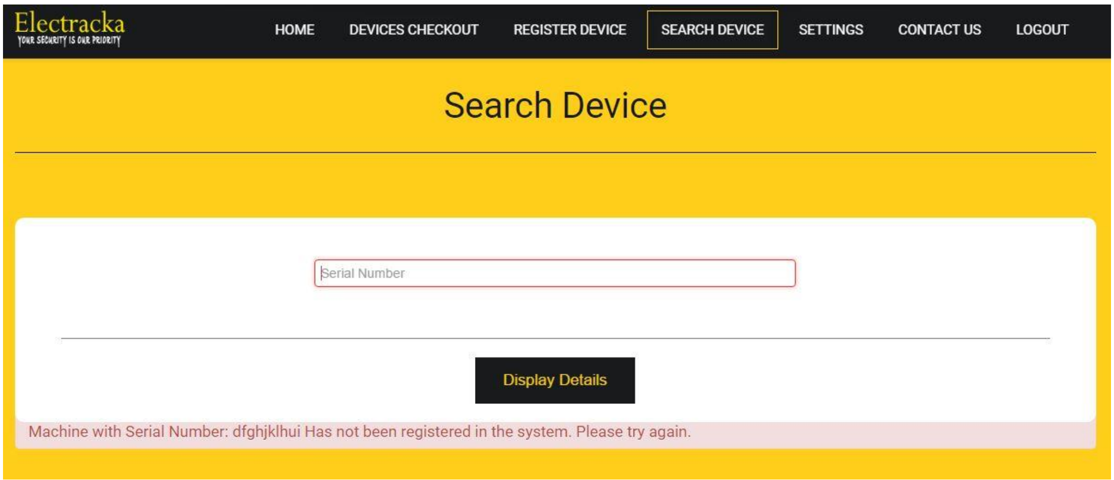
Hi Felistus, Kelvin Kariuki of id no: 27918611 Contact: 0729385557 attempted to register your stolen Television. Login now at www.electracka.com for more info.

Saf 16:57

Figure 18 SMS Notification on Trying to Register a Device Marked as Stolen

c) Search device form

If a device searched does not exist, the message on the screen capture below will be displayed to the user.



Search Device

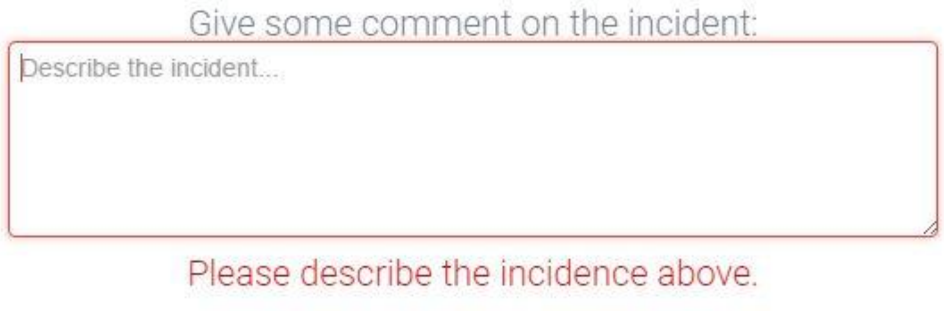
Serial Number

Machine with Serial Number: dfghjklhui Has not been registered in the system. Please try again.

Figure 19 Searching a Device that has not been Registered

d) Mark device as stolen form

The user must give a brief statement on the incident in order to be allowed to mark a device as stolen, the following error message shown on the screen shot below is displayed to the user if this field is ignored.



Give some comment on the incident:

Describe the incident...

Please describe the incidence above.

Figure 20 Error Message on Stolen Device Comment

5.3 Maintenance

This is the last step in the development of my system, however long the development period; the maintenance cycle will be several times long. This is because the system must first of all pay for itself and then it must provide a return on the investment.

5.4 Resource Requirement

5.4.1 Software requirements

i) Windows 7 operating system.

ii) Web browser.

5.4.2 Hardware Requirements

A laptop or desktop with the following hardware specifications:

i. Processor: Pentium 4 or above
ii. RAM :1 GB or above
iii. Hard disk: 40 GB or above.

5.5 System Technical Evaluation

The system was subjected to a technical evaluation that focused on a number of variables like the response time, read range and detection rate. This was done so as to evaluate the functionalities and usability of the system.

5.5.1 Response Time

This was sub-divided into three different scenarios:

1. Scenario One – measured the response time when a device that has not been registered is searched in the system.
2. Scenario Two – measured the response time when a stolen device is searched.
3. Scenario Three – measured the response time when a registered device that exits is search in the system.

5.5.1.1 Scenario One

This scenario focused on measuring the response time when a device that has not been registered in the system is scanned. The results were as follows as shown the table below.

Scenario One ~ Device Not Registered

Test	Start Time	End Time	Response Time (Milliseconds)
1	1474445104	1474445104	30125
2	1474445112	1474445112	2399
3	1474445115	1474445115	2235
4	1474445119	1474445119	2260
5	1474445122	1474445122	2296
6	1474445125	1474445125	2201
7	1474445128	1474445128	2340
8	1474445131	1474445131	2313
9	1474445133	1474445133	1403
10	1474445136	1474445136	2378
11	1474445259	1474445259	2186
12	1474445262	1474445262	1939
13	1474445263	1474445263	2161
14	1474445265	1474445265	2309
15	1474445266	1474445266	2264
16	1474445269	1474445269	1631
17	1474445271	1474445271	1908
18	1474445272	1474445272	2216
19	1474445274	1474445274	1779
20	1474445275	1474445275	2409
21	1474445300	1474445300	1657
22	1474445301	1474445301	2198
23	1474445303	1474445303	2123
24	1474445304	1474445304	2409
25	1474445306	1474445306	2329
		Average	**3258.72**

Table 8 Scenario One ~ Device Not Registered

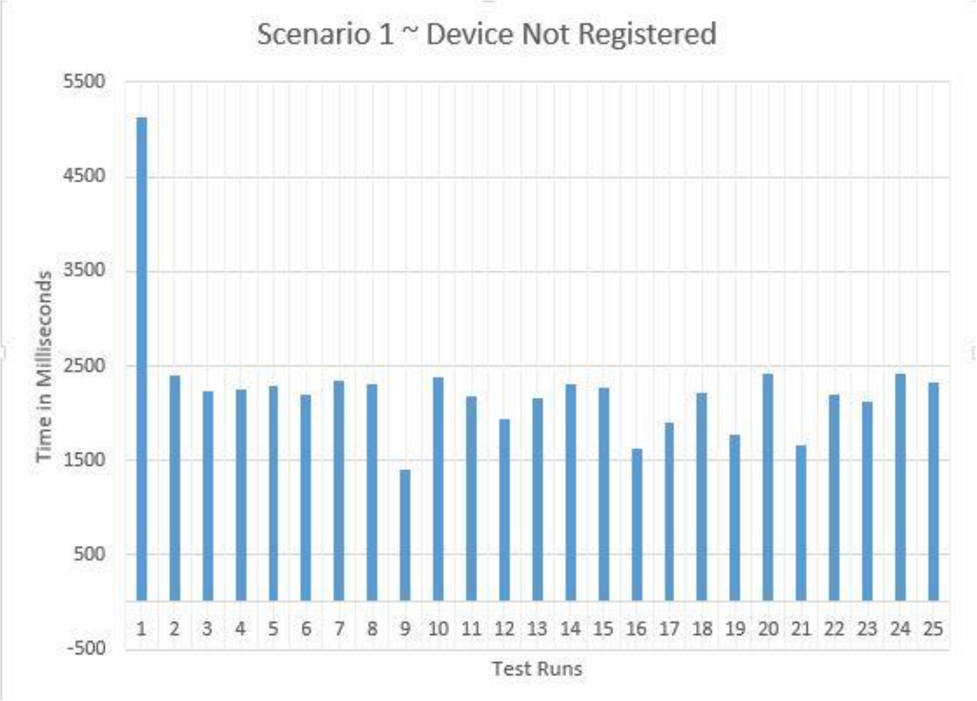


Figure 21 Bar Chart ~ Device Not Registered Response Time

5.5.1.2 Scenario Two

This scenario measured the response time when a device that has been marked as stolen by the owner is searched in the system. The results were as shown in the table below.

Scenario Two ~ Stolen Device

Test	Start Time	End Time	Response Time (Milliseconds)
1	1474446403	1474446404	1044815
2	1474446495	1474446496	106559
3	1474446500	1474446501	57667
4	1474446503	1474446503	63903
5	1474446506	1474446506	61881
6	1474446508	1474446508	63938
7	1474446509	1474446509	81071
8	1474446511	1474446511	66703
9	1474446513	1474446513	65974
10	1474446514	1474446515	65202
11	1474446516	1474446516	66681
12	1474446518	1474446518	61385
13	1474446519	1474446519	69757
14	1474446521	1474446521	66949
15	1474446522	1474446522	75779
16	1474446523	1474446524	76285
17	1474446525	1474446525	75152
18	1474446526	1474446526	74460
19	1474446527	1474446527	98116
20	1474446529	1474446529	63115
21	1474446530	1474446530	60637
22	1474446531	1474446531	62518
23	1474446533	1474446533	101667
24	1474446534	1474446534	57956
25	1474446535	1474446535	61592
		Average	109990.48

Table 9 Scenario Two ~ Stolen Device

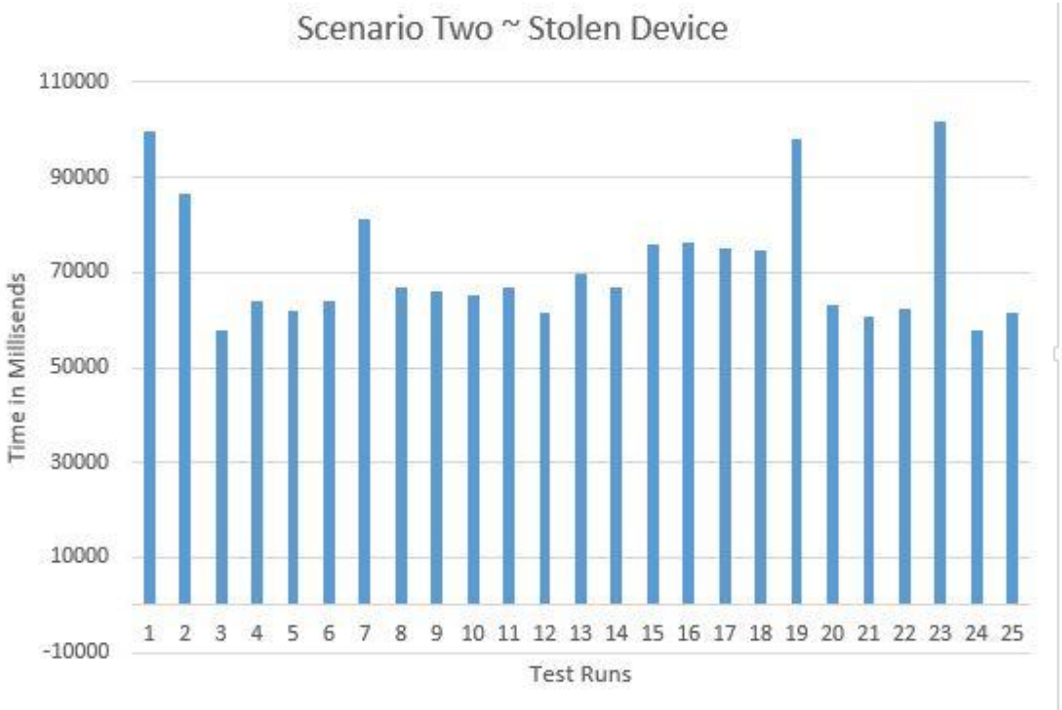


Figure 22 Bar chart ~ Stolen Device Response Time

5.5.1.3 Scenario Three

This scenario measured the response time when a device that has been registered and has not been marked as stolen is searched in the system. The findings were as shown in the table below:

Scenario Three ~ Registered Device

Test	Start Time	End Time	Response Time (Response Time)
1	1474445742	1474445742	2821
2	1474445744	1474445744	1024
3	1474445746	1474445746	2585
4	1474445747	1474445747	2657
5	1474445748	1474445748	2445
6	1474445749	1474445749	2513
7	1474445750	1474445750	2579
8	1474445752	1474445752	2477
9	1474445753	1474445753	2805
10	1474445754	1474445754	2667
11	1474445755	1474445755	2317
12	1474445757	1474445757	2526
13	1474445759	1474445759	2488
14	1474445760	1474445760	2421
15	1474445761	1474445761	1224
16	1474445762	1474445762	15840
17	1474445764	1474445764	2373
18	1474445765	1474445765	2789
19	1474445766	1474445766	1475
20	1474445767	1474445767	2115
21	1474445769	1474445769	3029
22	1474445770	1474445770	2358
23	1474445771	1474445771	2407
24	1474445772	1474445772	2677
25	1474445773	1474445773	3356
		Average	2958.72

Table 10 Scenario Three ~ Registered Device

Figure 23 Scenario Three ~ Registered Device

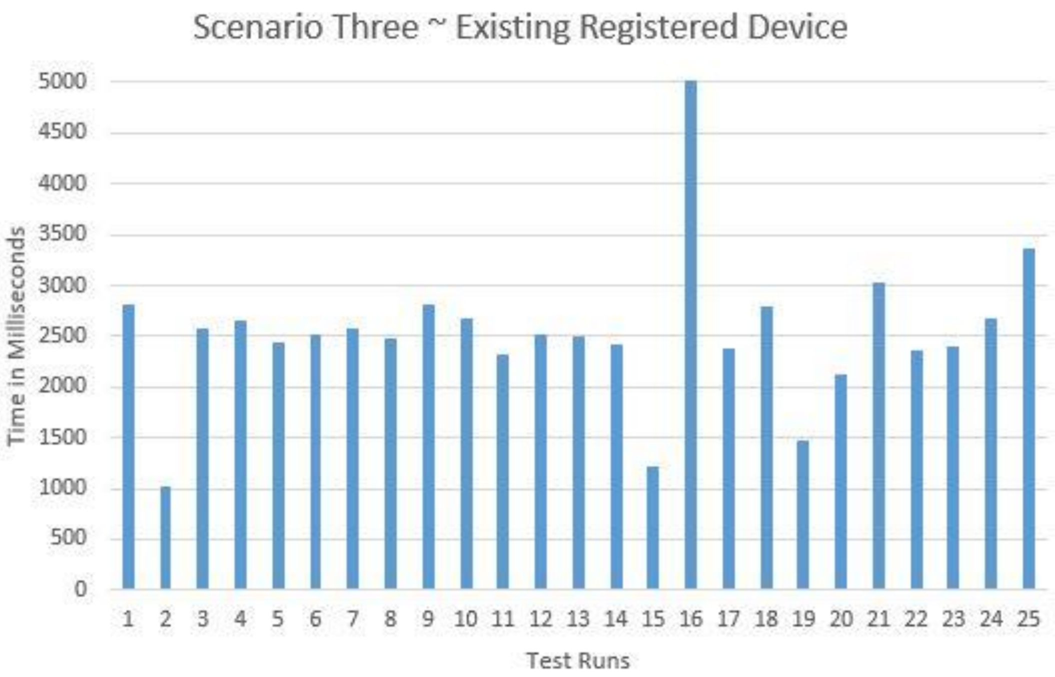


Figure 24 Bar chart ~ Existing Registered Device

5.5.2 Read Range

This was used to determine the average read range of the 13.56MHz RFID tag using the Arduino MRFC RFID card reader. Twenty Five runs were done and the read distance measured in centimeters, from these runs, the average read range was determined as shown on the table below:

Test Run No.	Read Distance (Centimeters)
1	2.4
2	2.5
3	2.6
4	2.3
5	2.3
6	2.4
7	2.5
8	2.3
9	2.6
10	2.3
11	2.4
12	2.5
13	2.4
14	2.6
15	2.4
16	2.3
17	2.3
18	2.4
19	2.4
20	2.5
21	2.4
22	2.3
23	2.5
24	2.6
25	2.4
Average Read Range	**2.424**

Table 11 13.56MHz Read Range Test

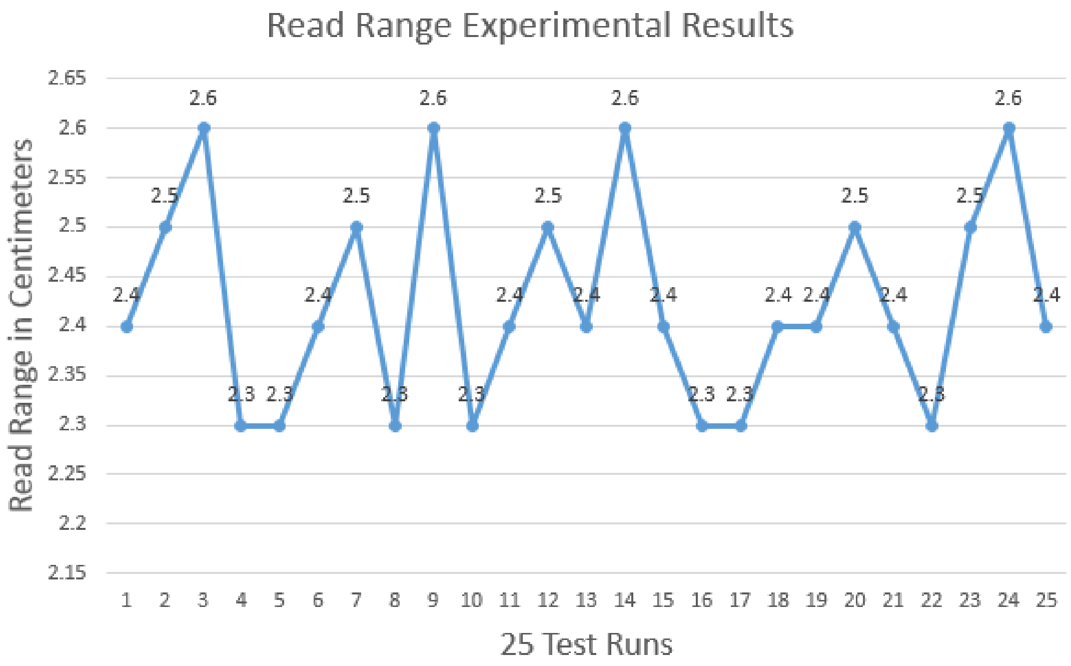


Figure 25 Bar Chart ~ Read Range of the 13.56Mhz RFID Tag using MFRC522 Arduino RFID Card Reader

5.5.3 Detection Rate

The detection rate, which is the ability of the reader to read the tag, was tested using the average read distance obtained in the previous experiments. The findings were as shown in the figure below:

Test Run No.	Detection Value within 2.4cm
1	1
2	1
3	1
4	1
5	1
6	2
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1
17	1
18	1
19	1
20	1
21	2
22	1
23	1
24	1
25	1

Table 12 Detection Rate ~ 13.56 MHz RFID Tag

Read Status	Frequency	Read/Miss Rate
Success	23	92%
Fail	2	8%

Table 13 Read Range Frequency

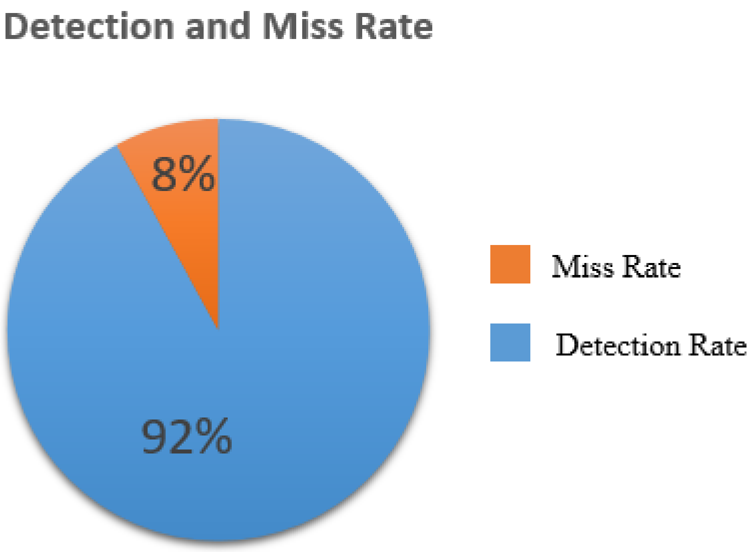


Figure 26 Detection and Miss Rate Pie Chart

5.5.4 Pre-test ~ Book verification procedure

A pretest study was done to the book verification procedure in order to determine the time takes for a device owner to register their device when coming into the institution and the time it takes for the ownership verification to be completed when they are leaving the university.

The data below was acquired through observation data generation strategy and the timing were capture in seconds by use of a stop watch.

		Using the Book for Device Verification		
Date	14/9/2016		Time	8.00am and 5.00pm
		Observer: Kelvin Kariuki		
			Time in Seconds	
	Check-In	Check-Out	Total Time	
1	68	52	120	
2	65	48	113	
3	65	55	120	
4	62	53	115	
5	70	52	122	
6	56	51	107	
7	62	48	110	
8	60	51	111	
9	68	52	120	
10	63	57	120	
11	68	52	120	
12	69	53	122	
13	65	52	117	
14	62	52	114	
15	62	54	116	
16	65	56	121	
17	64	57	121	
18	60	52	112	
19	67	53	120	
20	69	50	119	
21	61	49	110	
22	64	58	122	
23	64	56	120	
24	62	64	126	
25	64	52	116	
Averages	64.2	53.16	117.36	

Table 14 Book Device Verification Technique Timing

5.5.5 Pre-test ~ Barcode System

A pretest study was done to the existing barcode system in order to determine the efficiency of the system in a university setting when in use to verify device ownership. The data below was acquired through observation data generation strategy and the timing were capture in seconds by use of a stop watch.

Device Check out Using Bar Code System				
Date	14/9/2016		Time	5.00pm
Observer: Kelvin Kariuki				
No.	Time in Secs			
1	32			
2	29			
3	34			
4	28			
5	31			
6	30			
7	33			
8	29			
9	29			
10	30			
11	31			
12	35			
13	32			
14	32			
15	29			
16	30			
17	32			
18	36			
19	34			
20	31			
21	30			
22	29			
23	32			
24	32			
25	31			
Average	31.24			

Table 15 Bar Code Device Verification Technique Timing

5.5.6 Post-test study ~ RFID System

A post-test study was done to the proposed system in order to determine whether it achieves the project objective of efficiency. The data below was acquired through experimentation data generation strategy and the timing were capture in seconds by use of a stop watch.

Device Checkout Using RFID System				
Date	26/9/2016	Time	2.00pm	
Experimenter: Kelvin Kariuki				
No.	Time in Secs			
1	8			
2	6			
3	5			
4	7			
5	5			
6	6			
7	8			
8	7			
9	5			
10	8			
11	7			
12	8			
13	9			
14	7			
15	8			
16	5			
17	6			
18	7			
19	7			
20	8			
21	8			
22	6			
23	5			
24	8			
25	7			
Average	6.84			

Table 16 RFID Device Verification Technique Timing

5.5.7 Comparison of the Three Techniques

The results indicated that the book checkout method is the most time consuming, followed by the barcode system, while the RFID checkout method is the most efficient taking about seven seconds to checkout as shown on the chart below.

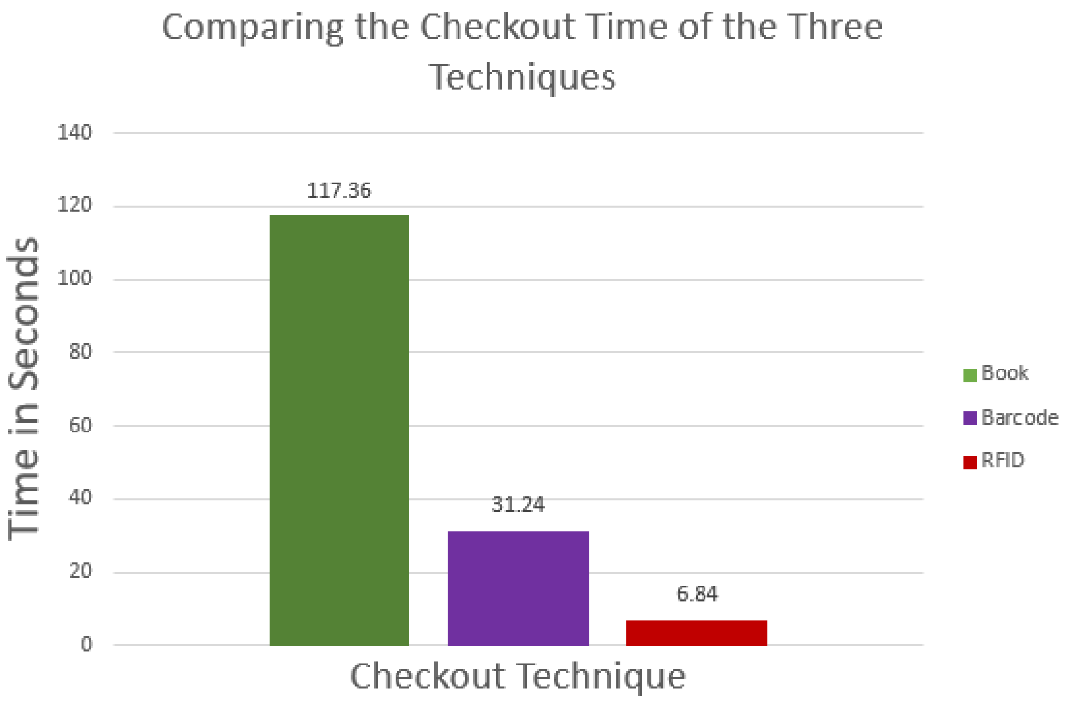


Figure 27 Comparisons of the Techniques

6.0 Conclusion

This paper presents a new, reliable, and seamless electronic asset tracking solution using RFID that helps to track and verify the ownership of an electronic asset in a real-time fashion.

The use of RFID technology in tracking electronic assets in Kenyan Universities has the potential to reduce property crime on electronic devices by giving real-time and accurate information about the ownership of a device on the exit point hence preventing the theft.

Compared to the traditional methods of electronic device ownership verification, which is the manual handwritten sign in and sign out using the serial number, this study has identified the benefits of RFID System listed hereunder:

I. It is highly efficient as it does not relay on line of sight like the barcode scanner.
II. It is accurate and effective in reading the serial number.
III. It will offer a real time tracking of these devices and raise alerts if a device has been stolen.

On the other hand, there is a limitation of the proposed system in that the Radio frequency may be unable to penetrate liquid and metal objects hence deterring the search process.

Overall, the proposed system is very simple to use and has more benefits as discussed earlier. Furthermore, the use of this technology will highly reduce or even eliminate the free market of stolen electronic devices, hence killing the demand which means less thieves will be motivated to steal.

6.1 Challenges

This study did a critical appraisal of the system, and also reviewed some of the challenges encountered during the software development life cycle as listed hereunder:

I. Importing the RFID tags and the reader was a big challenge as I had to wait for four weeks before I could get them into the country after ordering for them online.

II. Programming the Arduino Mega to act as a keyboard while using the RFID reader was an uphill task, fortunately I was able to follow tutorials on the internet and achieved it at last.

III. Due to timespan limitations, I did not cover some areas to the extent of my expectation like, testing the load conditions under which the prototype would reach saturation, implementing the prototype in the real world environment and evaluating it on that production environment.

6.2 Recommendations for Future Work

When the proposed system is built and implemented in the real world environment, we expect it the performance RFID solution to be fairly similar to the findings in this research. This is because, RFID relays on well developed and tested radio frequencies and the actual setup will have minimal differences with the developed prototype.

In future extensions of this study, I do recommend my fellow researchers to do an empirical evaluation of the system in a real-life context in order to determine and ascertain the predicted benefits as outlined by this study.

Another area of interest might be to look at the technical issues of the RFID system like the read range of the RFID tags under different conditions and the penetration challenges that they encounter in a real world functioning context.

APPENDICES

Appendix A: References and Bibliography

Chadha, K., 1998. The global positioning system: Challenges in bringing GPS to mainstream consumers, in: Solid-State Circuits Conference, 1998. Digest of Technical Papers. 1998 IEEE International. IEEE, pp. 26–28.

CHEN, J., LIN, Y., QIU, R., 2013. RFID-based Logistics Distribution System of Agricultural Products Research [J]. Logist. Sci-Tech 2, 5.

Clarke, R.V.G., Webb, B., 1999. Hot products: Understanding, anticipating and reducing demand for stolen goods. Citeseer.

Cumming, G., n.d. CONFIDENCE INTERVALS AND THE NEW STATISTICS.

Cybulski, E.R., Dehn, F.D., Francis, R.C., Hogerton, P.B., Kallestad, M.C., Kropp, K.M., McGee, J.P., Tong, S.-K., 2003. Radio frequency identification systems for asset tracking. US6669089 B2.

Dybå, T., Dingsøyr, T., 2015. Agile project management: from self-managing teams to large-scale development, in: 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering. IEEE, pp. 945–946.

Fosso Wamba, S., Barjis, J., Takeoka Chatfield, A., Barjis, J., Fosso Wamba, S., 2010. Organizational and business impacts of RFID technology. Bus. Process Manag. J. 16, 897–903.

Gehlot, N.L., 2002. Method and apparatus for automatic recovery of a stolen object. US6362736 B1.

Irani, Z., Gunasekaran, A., Dwivedi, Y.K., 2010. Radio frequency identification (RFID): research trends and framework. Int. J. Prod. Res. 48, 2485–2511.

Kashorda, M., Waema, T., 2014. E-Readiness survey of Kenyan Universities (2013) report. Nairobi Kenya Educ. Netw.

Lahtela, A., Hassinen, M., Jylha, V., 2008. RFID and NFC in healthcare: Safety of hospitals medication care, in: Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on. IEEE, pp. 241–244.

Mugenda, O.M., Mugenda, A.G., 2012. Research methods dictionary.

Oh, T.H., Choi, Y.B., Chouta, R., 2012. Supply chain management for generic and military applications using RFID. Int. J. Future Gener. Commun. Netw. 5, 61.

Osyk, B.A., Vijayaraman, B.S., Srinivasan, M., Dey, A., 2012. RFID adoption and implementation in warehousing. Manag. Res. Rev. 35, 904–926. doi:10.1108/01409171211272651

Sutton, M., Johnston, K., Lockwood, H., 1998. Handling stolen goods and theft: a market reduction approach. Home Office London.

Tri, H.M., Alsadoon, A., Prasad, P.W.C., Elchouemi, A., 2016. Progress of agile movements in Australia: Propose a Universal Dynamic System Development Method (UDSDM) and universal framework, in: 2016 7th International Conference on Information and Communication Systems (ICICS). IEEE, pp. 282–285.

Wang, C., George, D., Green, P.R., 2014. Development of plough-able RFID sensor network systems for precision agriculture, in: Wireless Sensors and Sensor Networks (WiSNet), 2014 IEEE Topical Conference on. IEEE, pp. 64–66.

Want, R., 2006. An introduction to RFID technology. IEEE Pervasive Comput. 5, 25–33. doi:10.1109/MPRV.2006.2

Werb, J., Underriner, K., Long, M., 2004. Asset and personnel tagging system utilizing GPS. US6700533 B1.

Zayou, R., Besbe, M.A., Hamam, H., 2014. Agricultural and Environmental Applications of RFID Technology. Int. J. Agric. Environ. Inf. Syst. IJAEIS 5, 50–65.

Appendix B: Sample Arduino RFID Reader Code

```
#include <SPI.h>

#include <MFRC522.h>


#define RST_PIN      5       // Configurable, see typical pin layout above

#define SS_PIN       53      // Configurable, see typical pin layout above


MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance


void setup() {

        Serial.begin(9600);         // Initialize serial communications with the PC

        while (!Serial);            // Do nothing if no serial port is opened (added for Arduinos based on ATMEGA32U4)

        SPI.begin();                // Init SPI bus

        mfrc522.PCD_Init();         // Init MFRC522

        mfrc522.PCD_DumpVersionToSerial();      // Show details of PCD - MFRC522 Card Reader details

        Serial.println(F("Scan PICC to see UID, type, and data blocks..."));

}


void loop() {

        // Look for new cards

        if ( ! mfrc522.PICC_IsNewCardPresent()) {

                return;

        }


        // Select one of the cards
```

```
    if ( ! mfrc522.PICC_ReadCardSerial())  {
        return;
    }

    // Dump  debug info  about the  card; PICC_HaltA()  is  automatically  called
    mfrc522.PICC_DumpToSerial(&(mfrc522.uid));
}
```