Jomo Kenyatta University of Agriculture and

Technology (JKUAT)

School of Computing and Information Technology

(SCIT)

**Abstract**

Web based applications have become more and more interesting with users being required to register so that they can access their accounts. This is done with the use of usernames and passwords. The One time password (OTP) will be sent to the user via SMS to the user's mobile phone.

With these increasing web-based applications, people tend to choose passwords that are easy to remember. This poses a risk to controlling users account as these easy to guess passwords can be guessed easily or passwords stolen using phishing spyware or username and password can be replayed. In order to authenticate an active user, the distributed system needs some way of determining that a user is who he/she claims to be. We are implementing the use of the one-time password in an online banking system where users will have to login using the two factor authentication algorithm. The users will have to login with their normal username and password. This event will then prompt the system to send the second part of authentication which is the one time password that is sent to your mobile phone via a text-message. Therefore To reduce the damage of phishing and spyware attacks, web-based applications can deploy one-time password systems, where users use each password only once.

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device.

The most significant threat that is addressed by OTPs, in contrast to static passwords is that they are not vulnerable to replay and phishing attacks. Another advantage is that, a user who uses the same password for multiple systems is not made vulnerable on all of them if one of the systems is hacked.

**Acknowledgment**

We owe a great debt to a number of people who generously gave us so much of their precious time, their knowledge and their wisdom, and added a whole dimension to this project. In particular we would like to thank our supervisor, Dr. George Okeyo who gave us invaluable insights in the direction of this research project. We are also grateful to our classmates and the other members of the Computing department who co-operated with us throughout the entire duration of this project.

Thank you all.

Table of Contents

[Chapter 1: Introduction 6](#_Toc521985615)

[1.0) Background 6](#_Toc521985616)

[1.2) Problem Statement 7](#_Toc521985617)

[1.3) Justification 8](#_Toc521985618)

[1.4) Objectives 9](#_Toc521985619)

[1.5) Proposed Schedule. 9](#_Toc521985620)

[1.6) Budget for the project 9](#_Toc521985621)

[CHAPTER 2: LITERETURE REVIEW 9](#_Toc521985622)

[2.1 Methods of delivering the OTP 10](#_Toc521985623)

[2.2 Algorithms used in 2FA 11](#_Toc521985624)

[2.3 Why 2-factor authentication? 13](#_Toc521985625)

[2.4 Scope 13](#_Toc521985626)

[Chapter 3: Research Methodologies and Methods. 13](#_Toc521985627)

[Research Process 14](#_Toc521985628)

[Data Collection 15](#_Toc521985629)

[Ethical considerations 15](#_Toc521985630)

[Data Protection Bill 16](#_Toc521985631)

[Software used 16](#_Toc521985632)

[Chapter 4: System Analysis. 16](#_Toc521985633)

[4.1 Introduction 16](#_Toc521985634)

[4.2 Problem Specification 17](#_Toc521985635)

[4.3 System Analysis 18](#_Toc521985636)

[4.4 Requirement Specification 19](#_Toc521985637)

[4.5 Functional Requirements 19](#_Toc521985638)

[4.6 Non-functional Requirements 19](#_Toc521985639)

[4.7 Functional Modeling 20](#_Toc521985640)

[4.8 System requirements analysis 21](#_Toc521985641)

[4.9 Non-functional requirements 21](#_Toc521985642)

[Chapter 5: System Design 21](#_Toc521985643)

[5.1 Introduction 22](#_Toc521985644)

[5.2 Behavioral Modeling 23](#_Toc521985645)

[5.3 Data and Database Modelling 24](#_Toc521985646)

[5.4 Human Computer Interaction Layer Design 25](#_Toc521985647)

[5.5 Navigation Design 26](#_Toc521985648)

[Chapter 6: System Implementation 27](#_Toc521985649)

[6.1 Five areas of expectations from the developers 27](#_Toc521985650)

[6.2 Software implementation 27](#_Toc521985651)

[6.3 User Experience (UX) Design. 28](#_Toc521985652)

[6.4 Cost 28](#_Toc521985653)

[6.5 Account recovery 28](#_Toc521985654)

[6.6 Afrikas talking API 29](#_Toc521985655)

[6.7 Programing language 31](#_Toc521985656)

[6.8 Securing the application 32](#_Toc521985657)

[6.9 User Registration 32](#_Toc521985658)

[6.11 SMS authentication 34](#_Toc521985659)

[6.12 User login 35](#_Toc521985660)

[7.0 Testing 35](#_Toc521985661)

[7.1 Testing Objectives 36](#_Toc521985662)

[7.2 Achievements 36](#_Toc521985663)

[8.0 Conclusion 38](#_Toc521985664)

[Appendix 39](#_Toc521985665)

[Dependency management 40](#_Toc521985666)

[Bibliography 41](#_Toc521985667)

**List of figures**

[Figure 1: Gantt Chart 9](#_Toc521985156)

[Figure 2: budget. 10](file:///C:\Users\bened\Desktop\final%20project..docx#_Toc521985157)

[Figure 3: use case diagram 23](#_Toc521985158)

[Figure 4: sequence Diagram 24](#_Toc521985159)

[Figure 5: installation of afrikas’ talking via composer 30](#_Toc521985160)

[Figure 6 diagram showing Afrika's talking API key and username 30](#_Toc521985161)

[Figure 7: diagram showing Afrikas' talking laravel package on www.packagist.com 31](#_Toc521985162)

[Figure 8:diagram showing billing on afrika's talking dashboard 31](#_Toc521985163)

[Figure 9: diagram showing a user uers eloquent model to capture user details during reistration 32](#_Toc521985164)

[Figure 10: TrustBank registration form 33](#_Toc521985165)

[Figure 11:laravel password encryption 34](#_Toc521985166)

[Figure 12: user authentication. 35](#_Toc521985167)

[Figure 13: diagram showing TrustBank login screen 35](#_Toc521985168)

[Figure 14:test cases with katalon studio 36](#_Toc521985169)

# Chapter 1: Introduction

### 1.0) Background

With the current age and error, technology has been adopted in all sectors in our day to day lives. We all interact with these systems at least once on a daily basis. They may include digital library, banking systems, e commerce systems etc. Most of these systems still rely on the static password method as a way of authentication. Users tend to set passwords that are easy to remember making it easy for attackers to bypass their security.

Generally One-Time Password is certainly one of the simplest and most popular forms of two-factor authentication for securing access to personal online personal accounts. One-Time Passwords are often preferred to stronger forms of authentication such as Public-Key Infrastructure (PKI) or biometrics because an air-gap device does not require the installation of any client desktop software on the user machine, therefore allowing them to roam across multiple machines including home computers, kiosks, and personal digital assistants.

The OTP is generated in such a way that numbers between 10000 and 100000 are generated so as to form a four digit OTP which is then sent to the Users mobile phone.

### 1.2) Problem Statement

Although username and passwords are private tokens of users of a particular system, there is the danger of malicious entities being able to fraudulently obtain these valid credentials and use them to access the system posing as the owner of the account. Identification and authentication mechanisms are unable to give protection in cases where a malicious entity is able to acquire valid credentials of a trusted user hence some users that authenticate are not the genuine owners of the account. This means the access control system has been breached.

Another issue of Identification and Authentication services of an access control system is that there is no mechanism that will be able to alert a user when a malicious entity tries to use their credentials to log in. This means that a user does not have the ability to detect when their stolen credentials are used to access the system allowing the malicious entity to access content of the system without the knowledge of the access control system and the user

Many web users or web companies due to mistrust of web based applications, are not be willing to contribute their resources and usefulness to trusted people or other companies over the internet, or even cooperate in solving a grand challenge unless security mechanisms is put in place, guaranteeing security of their information. This calls for a tough security mechanism to be put in place. Many online businesses today also store personal information about customers and shoppers on websites, and this provides another way for your personal information to be accessed, without your permission or knowledge. Given sensitivity of accounting information or personal data and the increase of viruses or spyware, users tend to be scared and not willing to do some transactions online. To increase confidence of people on online web base applications, One-time password can be used because it is among the best ways of access control.

### 1.3) Justification

Most online user access control systems provide only one authentication factor when validating users. Even if users adopt use of strong validation schemes such as strong passwords and visual captcha to authenticate users, there will always be that possibility of malicious entities obtaining valid credentials of users. Once this happens, the victims who have their credentials stolen are left unprotected since these malicious entities will be able to pose as the victims and deal damage to their user accounts. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay, phishing or XSS attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user, who uses the similar password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further accessing web based online applications needs to be controlled to secure user's data and information and control information sharing while guaranteeing ownership, provenance consequence of the scenarios of which Web-based applications are going to serve. Web-based applications that are accessed via a single account and there is a need for user access control into such an ecosystem, when people share data, users will not be willing to contribute unless mechanisms guaranteeing their work are in place secure user access control and data ownership can help raise user's confidence of such an environment.

### 1.4) Objectives

The main goal of this degree project is to provide TRUST BANK with a suitable 2FA method that allows customers to securely access their accounts.

The main goal has been divided into the following sub-goals:

* Analysis of existing 2FA methods
* To implementing access control to a web based application (TRUST BANK) using a 2 factor authentication algorithm.
* To enhance security of online users by introducing a multifactor authentication system by introducing the second factor of authentication which id the OTP after the use of login credentials which is the username and the password (static).

### 1.5) Proposed Schedule.

Figure 1: Gantt Chart

### 1.6) Budget for the project

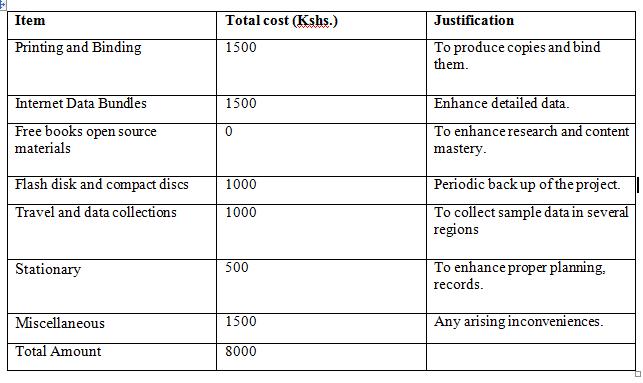


Figure : budget.

CHAPTER 2: LITERETURE REVIEW**.**

A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication. a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* ( a smartcard or specific mobile phone) as well as *something a person knows* (such as a PIN or password).

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user, who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the *previous* session, thus reducing the attack surface further.

OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore, they require additional technology to work.

### 2.1 Methods of delivering the OTP

#### 2.1.1 Phones

A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement. However, the cost of text messaging for each OTP may not be acceptable to some users. OTP over text messaging may be encrypted using an A5/x standard, which several hacking groups report can be successfully decrypted within minutes or seconds. Additionally, security flaws in the SS7 routing protocol can and have been used to redirect the associated text messages to attackers; in 2017, several O2 customers in Germany were breached in this manner in order to gain access to their mobile banking accounts. In July 2016, the U.S. NIST issued a draft of a special publication with guidance on authentication practices, which discourages the use of SMS as a method of implementing out-of-band two-factor authentication, due to the ability for SMS to be intercepted at scale.

### 2.2 Algorithms used in 2FA

An OTP value can be generated through two standards governed by the Initiative for Open Authentication (OATH): HOTP or TOTP. In this section details about these OTP schemes are given and the two algorithms are presented.

**2.2.1 OTP**

RFC 2289 describes a One-Time Password System. OTPs were mainly to counter a “replay attack”, in which information is eavesdropped and captured on a network connection in order to be used later to access a system. The system described in the RFC relies on a secret pass-phrase that is used to generate a series of OTPs. The strength of the system is that the user’s pass-phrase never has to traverse the network, therefore it is invulnerable to replay attacks; moreover, added security is given by the property that no secret information has to be stored on any system. However, OTP offers no protection against social engineering or active attacks. There are mainly two requirements for an OTP-system to work. First, the generator must generate the OTP from the user’s secret pass-phrase and from the information provided by the server. The server, on the other hand, must send a challenge to the generator, must verify the received OTP, must store the last valid OTP it received, and must store the OTP sequence number. The OTP generator passes the pass-phrase, along with a seed received from the server through a secure hash function to produce a one-time password.

**2.2.2 HOTP**

HOTP algorithm is used to generate one-time passwords based on the Hashed Message Authentication Code (HMAC). The algorithm relies on few factors such as a shared secret key and a moving factor.

The symbols introduced by the RFC are:

* an 8-byte counter value C that is the moving factor. This counter has to be synchronized between the client (generator) and the server (validator),
* a shared secret K between client and server. Each generator has a unique and different K,

HOTP is based on using the HMAC-SHA-1 algorithm. Since the output of the algorithm is 160 bits, the value is truncated in order to easily be read by the user.

**2.2.3 TOTP**

HOTP algorithm, where the moving factor is based on a time value. This time-based OTP algorithm provides short-lived OTPs which strengthen security. The basic different between the TOTP algorithm and the HOTP algorithm is that a value T derived from a time reference replaces the counter C.

With regard to security RFC 4226 states that even if an adversary is able to observe numerous message exchanges of successful authentication attempts and knows how build a function in order to generate HOTP values, then the adversary will not have a significant advantage over a random guess.

**2.2.4 HOTP or TOTP**

The main difference between HOTP and TOTP is that the OTPs generated through the TOTP algorithm are short-lived (generally with a lifetime of less than 30 seconds), while the OTP generated through the HOTP algorithm is potentially longer-lived. This means that the security provided by a TOTP implementation is better than an HOTP implementation for two reasons. First, if an HOTP password is compromised, it can be valid for a “long time”, while a TOTP password is only valid for a number of seconds choosing otp. TOTP implementation of the OTP is preferable due to its enhanced security. If the OTP scheme is based on a software solution, then the OTP is generated by an application on the phone.

**The main advantages of receiving the OTP via SMS is that the user does not have to own a smart phone, since all mobile phones are able to receive SMSs.**

Implementing a TOTP application solution means that not everyone is able to use it. Moreover, SMSs are convenient since there is no need to download an application or perform any setup. In terms of deployment, an SMS-based solution is simpler than an application-based solution since it does not require the company to write an application to generate TOTPs or to modify its servers in order to meet the requirements of the TOTP algorithm. Also, the client device generating the TOTP does not need to be connected to the Internet (as the protocol also works in offline mode).

On the other hand, there are some disadvantages in using SMS delivery of OTPs. The first disadvantage is due to limited network coverage as poor network coverage would imply the impossibility for the user to authenticate using 2FA.

Moreover, sending OTPs though SMS is no longer considered secure due to the vulnerabilities of the GSM network and due to malware & Trojans designated to intercept SMSs. Our assumption is that SIM exchange will not compromise the TOTP codes since the codes are independent of the SIM card.

Why 2-factor authentication

* .The banking procedure is convenient through internet banking in terms of time (24\*7) and operation, its acceptance would be greater.
* Instead of just relying on something you know (like your password), 2FA combines both something you know (like a PIN number) and something you have (like your mobile phone).

### 2.3 Why 2-factor authentication?

* The banking procedure is convenient through internet banking in terms of time (24\*7) and operation, its acceptance would be greater.
* Instead of just relying on something you know (like your password), 2FA combines both something you know (like a PIN number) and something you have (like your mobile phone).
* The banking procedure is convenient through internet banking in terms of time (24\*7) and operation, its acceptance would be greater.
* Instead of just relying on something you know (like your password), 2FA combines both something you know (like a PIN number) and something you have (like your mobile phone).

### 2.4 Scope

Two-factor authentication (2FA) schemes aim at strengthening the security of login-password–based authentication by deploying secondary authentication tokens. In this context, SMS-based 2FA schemes require no additional hardware (such as a smartcard) to store and handle the secondary authentication token, and hence are considered as a reasonable trade-off between security, usability, and cost.

To minimize implementation cost, complexity of the system and to effectively deriver an efficient mode of 2FA, we strictly limit this project to SMS based to implement one time password in verifying users credentials.

Advantages of sms-based authentication

* It makes life easier for your customers and colleagues
* With SMS-based 2FA, there’s no need for any new technology. The user already has the tools they need to complete the process and, crucially, they know how to use them.
* It’s simpler (and more cost-effective) for your business
* With no new hardware and software to rollout, there’s no need to develop a training or ‘adoption’ program.

# Chapter 3: Research Methodologies and Methods.

The purpose of this chapter is to provide information about the research methodologies and methods used in this project. We are going to focus on research strategies, data collection, and quality assurance.

This chapter is has Sections that describes the research process underlying the project, presents details about the methodologies, methods adopted in order to select the most suitable 2FA method and explaining how data was searched and collected and presents some ethical aspects linked to it. We also detail the techniques used to evaluate the reliability and validity of the data collected.

### 3.1 Research Process

Research involves a process which focus is on objectively gathering information that will be analyzed in order to come to a conclusion. This project’s research process includes multiple steps that are interlinked with each other. These steps are:

* selection of the topic area,
* formulation of the problem,
* formulation of the goals of the thesis,
* review of the literature,
* selection of methods of data collection
* analysis of data
* Reaching conclusions.

Selection of a topic area was the first step. This project focuses on the weak security offered by passwords and on how to make authentication more secure. The topic of this project was found to be interesting because it addresses an underrated but serious problem.

Identifying a problem related to the topic area is the goal of the second step. The problem is the weak security of Single Factor Authentication (i.e., passwords) in the field of digital assessment platforms. After the problem has been identified, the aims and objectives of the project had to be stated in order to determine the scope, the depth, and the direction of the work. In order to avoid setting unrealistic goals and aims, the research objectives were formulated according to specific, measurable, achievable, realistic and timely objectives. Therefore, the goal of the project was set to identify and implement a suitable 2FA method for TrustBank for securing users’ accounts. It is a goal that was regarded as achievable and realistic at the beginning of the project, and it is also considered to be timely.

Once the problem and the scope are identified, existing literature on the topic has to be searched and reviewed. This step allows the researcher to find previous work regarding the problem and data related to it. The first stage in the literature search was to identify search terms. The main search terms in this project were 2FA, authentication, data breaches, two-factor authentication with one time passwords, different 2FA methods, authentication factors, types of authentication, sending OTP, UX with 2FA, cost of 2FA, algorithms used in OTP and other. In the second stage, online literature was found using these search terms.

The different types of research methods can be divided into several categories depending on the nature, the scope, and the purpose of the research. The general classification of the different methods is quantitative and qualitative. The quantitative research method is based on numbers and calculations while the qualitative one is based on perceptions and feelings and aims to provide depth of understanding. This project follows the quantitative method as it relies on existing data and information and on surveys carried out by the researcher.

### 3.2 Data Collection

Data collection is the process by which the researcher collects information from all the relevant sources chosen in the previous steps of the research process. The collected data can be divided into two categories: secondary data collection and primary data collection. Primary data are collected by the researcher conducting the research through methods like surveys, interviews or questionnaires. Often, when the research problem is unique, there is no available related work, then the researcher has to collect the data him or herself.

### 3.3 Ethical considerations

There a main objective regarding ethics is to keep security and confidentiality of the data used.

The main issues with secondary data are related to potential harm to individuals as well as the issue of consent. Data could contain identifying information about participants, which means that the researcher re-using this data should describe how the privacy and confidentiality of the participant will be protected. If the data does not contain any identifying information, then the researcher should confirm that the data is anonymous and acknowledge the source of the data.

The data collected was also relevant as it was not outdated and it perfectly fits the problem of this thesis. Moreover, the data was assessed as being accurate. The data was detailed, exact, and comprehensive. The articles chosen presented a throughout discussion of the subject and all sides of the main issue were addressed.

### 3.4 Data Protection Bill

The Kenya Data Protection Bill, 2018 presented by chairperson of the Committee on Information, Communication and Technology contains provisions that will significantly change how public and private entities handle information entrusted to them.

According to the Bill, companies will now have to inform users of any personal data they are collecting, the purpose for collecting that data and how long the same will be stored. The law also gives users the right to decline to have their data collected or processed as well as demand to have false data corrected or deleted upon demand. A person found guilty of interfering with the personal data of others or infringes on their right to privacy will be liable, on conviction, to a fine not exceeding Sh500,000 or to imprisonment for a term not exceeding two years, or to both. The Bill is, however, mum on penalties or fines subject to corporates found guilty of the same and leaves it to the complaints commission to decide the course of action.

### 3.5 Software used

With regard to the design and implementation of the prototype, the software used has to be decided. The way in which the software will be decided reflects the abilities and skills the authors have acquired during their studies. The main line that will be followed is to use well-known programs/software. Implementation Chapter will provide information about the software used when implementing the solution.

# Chapter 4: System Analysis.

### 4.1 Introduction

Lonnie D.(2007) explains system analysis as the process of dissecting a system with the sole objective to learn how the component pieces interact to achieve their functions. The aim of performing this activity is to find out how the current system operates (i.e. where one exists) and thus identify where the problems are incurred hence solutions to these problems can then be identified. This activity further enables the analyst to further identify some additional requirements which the user needs and thus incorporate the same in the construction of the new system. This is further realized in the data collection process where the additional information is gathered from the respective stakeholders. System analysis answers the questions of who will use the system, what the system will do and where and when it will be used. It is a process of collecting and interpreting facts, identifying the problems, and decomposition of a system into its components. System analysis is conducted for the purpose of studying a system or its parts in order to identify its objectives. It is a problem solving technique that improves the system and ensures that all the components of the system work efficiently to accomplish their purpose.

### 4.2 Problem Specification

With the increasing number of web based Applications and users registering or opening many accounts online these applications, there is a high tendency of users choosing simple or easy passwords. Also users make a mistake of writing these passwords on paper or anywhere they would reach for them easily. In addition to social engineering, password phishing using spyware for passwords stored in electronic form causes a lot of risk to users’ information. Designing One- time-password, which is sent to the mobile phone of the user and used once can help secure many user's web based accounts. The task is therefore to come up with an application that allows for this kind of online access control using OTP to personalize such online access, which is more secure than static passwords. Access control systems are responsible for authenticating and authorizing users to access content in the system.

#### 4.2.1 Feasibility Study

The feasibility analysis examines the technical, economic, and pros and cons of developing the system, and it gives a slightly more detailed picture of the advantages of investing in the system as well as any obstacles that could arise. It also identifies the important risks associated with the project that must be addressed if the project is approved. The fact finding process that revealed the ability to successfully complete the proposed system thus providing the justification for the efficiency and effectiveness of the system. It was aimed at establishing whether it is necessary to develop the proposed system feasibility study includes three techniques namely:

#### 4.2.2 Technological Feasibility

Most organizations are connected to network and it is technologically feasible The SMS based means of sending the OTP is compatible to most mobile phones and so the system is technological feasibility is viable.

#### 4.2.3 Technical Feasibility

Familiarity with the application: The analyst of the application is familiar with the web based Applications area and OTP. Therefore, there is a lesser chance of misunderstanding the user needs or missing opportunities for improvement. Familiarity with the technology: The developer is familiar with web application development and thus there are lesser chances that problems will occur and delays be incurred because of the need to learn how to use the technology. This section looks to answers 3 questions:

1. Are the required resources available?
2. Is the required technology available or not?
3. Is the required know how available or not?

It also establishes the proposed system's interaction with other systems. Only designers, analysts and developers constitute the team foundation in terms of skilled labour. Users only ought to be computer literate. The system seeks to be resource friendly.

#### 4.2.4 Operational Feasibility

This basically deals with how well the system will be accepted by its users’ and incorporated into the ongoing activities of the users. It was of great importance to include users in the analysis of the system in order to get feedback on acceptable ways of implementing the lock mechanisms on user access controls. From the users' feedback, the system was deemed to be operationally feasible as it improved on the security of user.

#### 4.2.5 Economical Feasibility

This section is aimed at determining the positive economic benefits to an organization that the proposed system is to provide. It includes identification and quantification of all benefits projected. It answered the following question:

1. Will users derive an economic benefit from the proposed system?
2. Will the cost of implementation be justifiable?

The added security layer that will be included will not be costly to incorporate and manage. From the findings, the added security layer will also increase cost of attacking the system hence ensuring income from using the system will be more secure hence increasing computational trust of the system.

### 4.3 System Analysis

#### 4.3.1 Requirement Analysis

This is the process of studying and analysing the customer or the user needs to arrive at a definition of software requirements. The software requirements were identified by analysing existing systems and online.

### 4.4 Requirement Specification

A requirement is simply a statement of what the system must do or what characteristic it must have. Requirements can be mainly divided into two: either functional or non-functional.

A functional requirement relates directly to a process the system has to performer information it needs to contain. A non-functional requirement refer to behavioural properties that the system must have, such as performance and usability.

### 4.5 Functional Requirements

**1. Create an account:**

Anyone wishing to use this online service must register as a user by creating an account. The system should allow for creation of unique accounts for each user.

2. **Sign up a registered** user of the web based Application. Those wishing tossing up as users will submit their application through filling in an online form. The form will be relatively short but just enough to capture all the relevant details.

3. The system should be able to deny access to **unauthenticated users**. Without correct username and password and the OTP, the system should not allow access to the secure user information in the web based application.

4. Generate and **send the One Time Password**.

5. **Search for user details**: The users of the system will be able to access the system to look for user record. The search can be done based on specific attributes such as specific username. Alternatively, the search may be done via the user name which case a detailed record the user will be provided.

### 4.6 Non-functional Requirements

1. **Accuracy and timeliness** in the process of producing and sending OTP. This is very important because the six digit OTP in only valid for a short period of Time.

2. **Performance** -this refers to the speed, capacity and reliability of the system. The requirements include:

1. The system should be available for use 24 hours a day, 365 days per year.
2. An interaction between the user and the system should not exceed 2 seconds.

3. **Usability:** Should allow ease of use. Documentation: Should be well documented to facilitate use of the system.

4. **Security** -this basically refers to how secure the system is in terms of allowing only specific people to access the system at specific times. The requirements include:

1. The users of the system can only access specific information in the web based application.
2. The users cannot be able to modify data related to other users, though they can modify data about them save for unique identifiers.

5. **Performance** -this refers to the speed, capacity and reliability of the system.

The requirements include:

1. The system should be available for use 24 hours a day, 365 days per year.
2. An interaction between the user and the system should not exceed 2 seconds.

6. **Operational** -this basically involves the physical and technical environments in which the system will operate. Thus, they include:

1. The system should be able to work on any web browser.
2. The system will be able to operate in Windows, Macintosh and Linux environments as it will be running in a web browser.

7. **Adaptability:** It should be easy for users to adapt to the application.

8. **Accessibility**: The user interface will be responsive to cater for the devices that users might have to access the system.

### 4.7 Functional Modeling

Functional models describe business processes and the interaction of an information system with its environment. In object-oriented systems development, two types of models are used to describe the functionality of an information system:

1. Activity diagrams support the logical modeling of business processes and work flows.
2. Use cases are used to describe the basic functions of the information system.

#### 4.7.1 Use case Descriptions

The use case communicates at a high level what the system needs to do. Use cases capture the typical interaction of the system with the systems users (end users and other systems). The following use cases were developed after reviewing the requirements.

There is only one actor in the system. The user can perform the following actions. First he/she has to log in to the system. The log in with user name and password utilizes the user private username and password and database function to create account to check whether the user has an account. The log in with OTP uses users’ information in the database to check or match. After logging in, the user can create do their bank transaction He can also maintain the system with regular updates.

### 4.8 System requirements analysis

Hardware constraints Minimum or actual hardware speciation required:

None- Software Constraints System interface will be implemented using HTML5, Vue.js (a JavaScript framework), and Tailwind CSS (A utility first CSS framework). Backend of the system will be implemented using Laravel 5.6; a PHP framework. Justinmind will be required too to create mock-ups and Katalon studio for Automation testing.

Database constraints. Database of the system will strictly be implemented using MySQL database.

### 4.9 Non-functional requirements

This section species the quality factors required by the system which are not related to the specific functional requirements:

# Chapter 5: System Design

### 5.1 Introduction

The design of the system will aim to identify the subsystems in the project, the interactions between the subsystems, system states and the logical flow of events within the system. During the system design we identify the data relationships and the database schema elements. The design also seeks to define how the user will interact with the system and the desired system user interfaces.

This chapter describes the process followed in defining the architecture, components, modules, interfaces, and data for the system to ensure that it satisfies the specified requirements. The system design was approached through the main sections as outlined below.

**5.1 Use Cases**

A use case diagram in the Uniﬁed Modelling Language (UML) is a type of behavioural diagram deﬁned by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. Interaction among actors is not shown on the use case diagram. If this interaction is essential to a coherent description of the desired behaviour, perhaps the system or use case boundaries should be re-examined. Alternatively, interaction among actors can be part of the assumptions used in the use case.

Use case: A use case describes a sequence of actions that provide something of measurable value to an actor and is drawn as a horizontal ellipse.

**Actor:** An actor is a person, organization or external system that plays a role in one or more interaction with the system.

**System boundary boxes (optional**): A rectangle is drawn around the use cases, called the system boundary box, to indicate the scope of system. Anything within the box represents functionality that is in scope and anything outside the box is not.

**Include:** In one form of interaction, a given use case may include another. ”Include is a Directed Relationship between two use cases, implying that the behaviour of the included use case is inserted into the behaviour of the including use case.

**Extended use case**: In another form of interaction, a given use case (the extension) may extend another. This relationship indicates that the behaviour of the extension use case may be inserted in the extended use case under some conditions. The notation is a dashed arrow from the extension to the extended use case, with the label”extend”. Modellers use the ”extend” relationship to indicate use cases that are ”optional” to the base use case.

**Associations:** Association between actors and use cases are indicated in use case diagrams by solid lines. An association exists whenever an actor is involved with an interaction described by a use case. Associations are modelled as lines connecting use cases and actors to one another, with an optional arrowhead on one end of the line. The arrowhead is often used to indicating the direction of the initial invocation of the relationship or to indicate the primary actor within the use case.

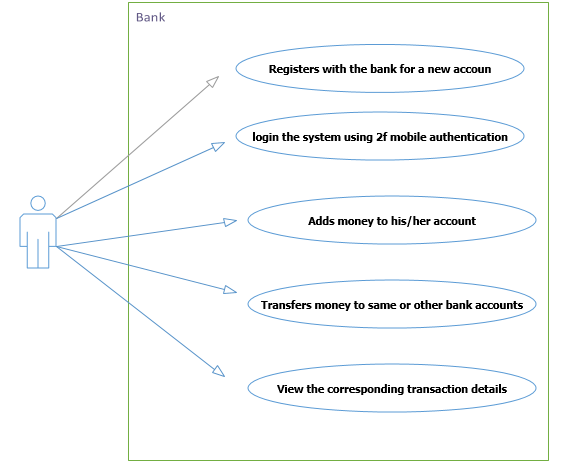


Figure 3: use case diagram

### 5.2 Behavioral Modeling

Behavioural models describe the internal dynamic aspects of the system that supports the business processes in an organization. It describes what the internal logic of the processes is. In this chapter, we describe three Unified Modelling Language (UML) diagrams that are used in behavioural modelling (sequence diagrams and activity diagrams).

**5.2.1 Logical Sequence of Activities in the System**

Sequence Diagram: Login

USER

MOBILE

SYSTEM

DATABASE

OPENS APP

GETS OPTIONS

TO LOG IN

LOGS IN WITH

USERNAME AND PIN

GETS FEEDBACK FROM USER

AND SENDS IT TO THE SYSTEM

FOR VALIDATION

GETS THE VALIDATION REQUEST

RECIEVES VALD

QUERY AND CHECKS

GENERATES OTP

AND SENDS IT TO

THE USER

RECIEVES THE OPT AND

DISPLAYS IT VIA SMS FROM

AFRICAS TALKING

ENTERS THE RECEIVED OTP

GETS THE USERS INPUT AND

SENDS IT TO THE SYSTEM FOR

VERIFICATION

COUNTER CHECKS WITH THE

GENERATED OTP

GRANTED ACCESS TO THE

SYSTEM

.

DISPLAYS HOMEPAGE

.

VIEWS AND PROCEEDS WITH

THE INTENDED TRANSACTION

.

GETS THE OTP FROM THE

SYSTEM AND DISPLAYS IT

INPUTS THE OTP

NOT VALID

VALID

STORES THE

GENERATED OTP

NOT VALID

VALID

Figure 4: sequence Diagram

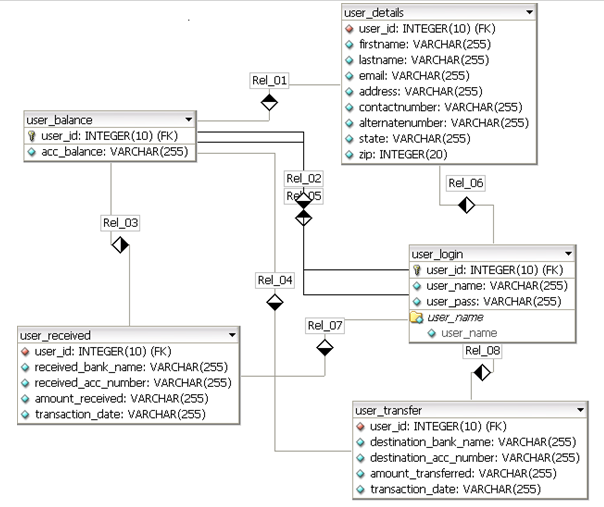
### 5.3 Data and Database Modelling

#### 5.3.1 Database design

This section describes the process of creating data models of the system database.

These models help to give clear relations of objects and their interactions in the database. Below are the models that were chosen to represent the system. The following classers are mapped in the database.

#### Class diagram

****

### 5.4 Human Computer Interaction Layer Design

The human computer interface layer defines the way in which the users will interact with the system and the nature of the inputs and outputs that the system accepts and produces. The user interface includes three fundamental parts which were reviewed in the construction of the system:

1. Navigation mechanism, the way in which the user gives instructions to the system and tells it what to do (e.g., buttons, menus). The system thus consisted of menus and button which acted as `guides' and when clicked resulted in the execution of various commands
2. Input mechanism, the way in which the system captures information (e.g., forms for creating new users). this application mainly deals with controlling access by generating OTPs to be used by users.
3. Output mechanism the way in which the system provides information to the user or to other systems (e.g., reports, Web pages). This application provides SMS based One Time password.

### 5.5 Navigation Design

The navigation component of the interface enables the user to enter commands to navigate through the system and perform actions to enter and review information it contains. A good navigation component is one the user never really notices. It simply functions the way the user expects, and thus the user

gives it little thought.

The following navigation controls will be used:

1. **Menus:** In the design of the navigation, menus and links will be heavily utilized in order to prevent the user from making mistakes e.g. during typing. Thus direct manipulation was exemplified.
2. **Messages:** they are the way in which the system responds to a user and informs him or her of the status of the interaction. There are many different types of messages, such as error messages, confirmation messages, acknowledgment messages, delay messages, and help messages. These will be included in this system as shown in the sample below.

User modules/pages Log in page: This form requires users to input the necessary details that are required to validate a user and create a session. Upon successful validation users are redirected to the intended page otherwise they are redirected back with error that the log in details are incorrect.

This page will be used to collect the main details of a user that will be sufficient

to provide quality service once the user successfully registers.

# Chapter 6: System Implementation

The purpose of system implementation is to build a properly working system and install it in an organization.

In **computer** science, an **implementation** is a realization of a technical specification or algorithm as a program, software component, or other **computer** system through **computer** programming and deployment. Many implementations may exist for a given specification or standard.

**Systems implementation** is the process of:

1. defining how the information system should be built (i.e., physical system design),
2. ensuring that the information system is operational and used,
3. ensuring that the information system meets quality standard (i.e., quality assurance).

### 6.1 Five areas of expectations from the developers

1. Goals: the reasons for developing the system
2. Importance: the importance of the problem being addressed
3. Patterns of use: the way the system will be used
4. Impacts: system impacts on the organization
5. Evaluation criteria

### 6.2 Software implementation

This section describes how the design was implemented and which tools were used during the development of this implementation. Some important parts of the code are shown as well as the database scheme.

1. **Software and tools used**
2. **Laravel**
3. **Tailwind Css**
4. **Africas talking API**
5. **fixer.io API**
6. **Katalon studio**
7. **composer**
8. **Vue.js**

A detailed use of the software can be found on the appendix page.

### 6.3 User Experience (UX) Design.

To start, it has to be said that increased security comes with a loss of convenience and ease of use. Therefore, designing a user-friendly 2FA is a hard task due to the fact that authentication poses many contradictions to the principles of Human-Computer Interaction (HCI), as secure authentication often compromises the user’s experience. However, our study, concluded that the usability of different 2FA methods varied depending on the users’ demographic background.

### 6.4 Cost

In terms of cost, the TOTP solution is more convenient since it is nearly free (once it has been implemented). The TOTP protocols are open source, which means that the only cost will be based upon the amount of time necessary for TrustBank to implement the protocol in its servers and to develop an app that generates TOTPs.

Implementing an SMS 2FA will have an on-going cost to TrustBank, changed at normal SMS rates by the service provider since the company will have to utilize a communication platform, and also perform HTTP request from third party SMS gateway provider.

### 6.5 Account recovery

The more secure the authentication process is the harder it is to regain control over the account, as more information has to be proven. This means that while 2FA strengthens the security of the account at login, it also makes it more difficult and troublesome for the account possessor to regain control over an account. This difficulty in account recovery should be kept in mind, as if not implemented thoughtfully it could enable an intruder to steal an account. An unavailable mobile device implies the inability of the user to use the second authentication factor. Depending on which 2FA method is used and whether the device is broken or lost there are different ways of dealing with account recovery.

|  |  |
| --- | --- |
| Case | Recovery |
| Forgotten password | E-mail with reset link  (SMS if number stored |
| Broken device | SMS with code |
| Lost device | Backup code or peer  recovery. (SMS if number recovery stored) |
|  |  |

A forgotten password is one of the most common reasons for being unable to access an account. The most common method used in order to recover the account in this scenario is to send a recovery link or temporary password to the user’s email address, which was registered during account creation. Sometimes the password or the link is sent to an alternative mail address, still provided by the user during account creation. This method is the easiest and probably the most logical one to deal with forgotten passwords. Regardless of the 2FA method used, the account recovery mechanism should work in the same way as described in the previous section; hence 2FA would not be bypassed. Even if a potential intruder manages to reset the password, the second authentication factor would still be required in order to gain access and therefore the account is still secured with 2FA. Inability to provide the second factor of authentication The inability to provide the second factor of authentication could be due to either loss of the user’s mobile device or it being broken. By the term broken we mean a mobile device that is in possession of the user but is unusable. A lost mobile device means that the user has no physical access to the device. Storing the user’s phone number during the registration process makes it easier to deal with account recovery in case of a broken mobile device, regardless of the 2FA method chosen for login. This is true since the SIM card is still in possession of the user, hence the user could move this SIM card to another devices and an SMS could be sent with either a code to login or a restore code to reset the password. On the other hand, the process of recovering the account becomes complicated if 2FA relies on OTP and no phone number is linked to the account. This case is handled in the same way for both a lost and broken mobile device. The problem that arises, in this case, is that authentication is dependent upon the application.

### 6.6 Afrikas talking API

The most common API among developers is to use Africas’ talking Mobile services, ranging from USSD, SMS, Short code to mobile money check out. SMS service is used to send verification codes to users mobile phones, in combination with a username and password to strengthen the security of users’ logins. The main advantages offered by the OTP solution provided by Afrikas’ Talking are that there is no need for client software further easing its implementation and that they have the cheapest SMS service platform.

In order to verify the OTPs, two options can be followed by the company / developer:

* Use Afrikas own web server called Afrikas talking, which is available after getting an free API key or host a verification server. Implementations of such a server written in Go, Python, and PHP are available on the website.
* Laravel developers can access Afrikas’ talking package from packagist.com. The developer can install via composer dependency manager.

Figure 5: installation of afrikas’ talking via composer

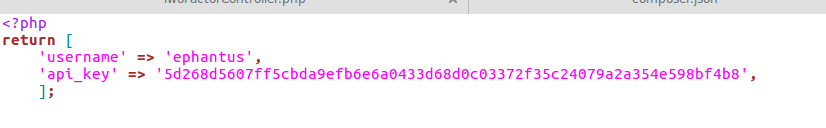


Figure 6 diagram showing Afrika's talking API key and username

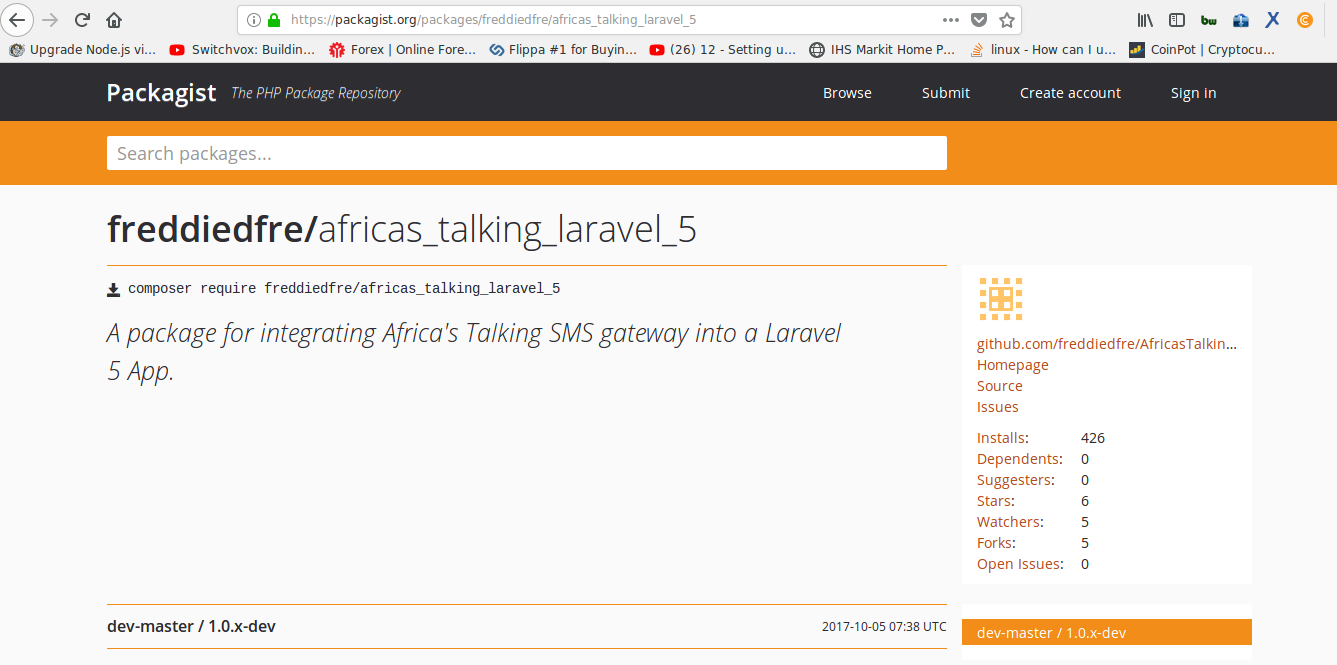


Figure 7: diagram showing Afrikas' talking laravel package on [www.packagist.com](http://www.packagist.com)

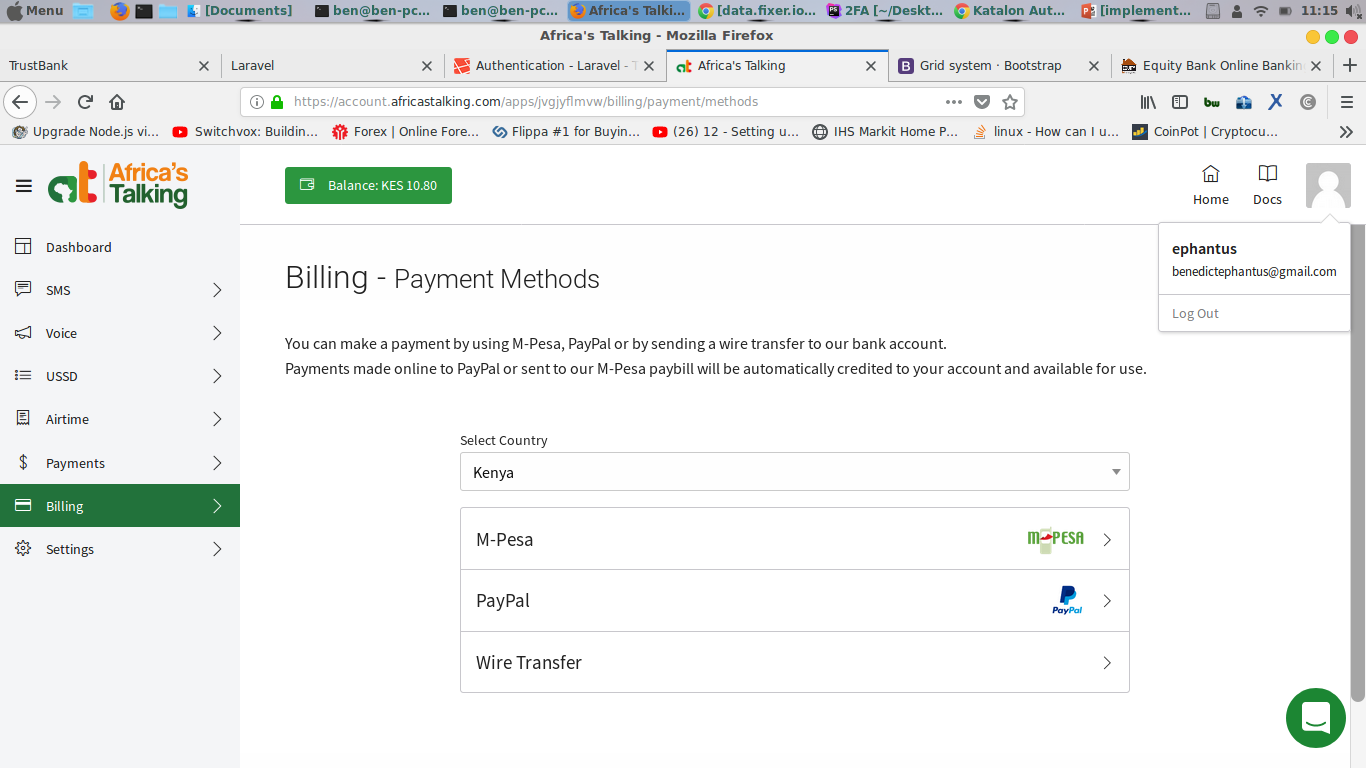


Figure 8:diagram showing billing on afrika's talking dashboard

### 6.7 Programing language

The first choice to made was to choose which programming language to use for implementing the server side of f the solution, the client side, and the database. The web page was written in HTML and Tailwind CSS — as these are the standard languages for creating web pages rapidly. JavaScript and Vue.js framework were used to develop models that engaged calculations like loan interests, and to stream line some process more comfortable. The server side was implemented using Laravel for the same reasons. The database used was MySQL.

### 6.8 Securing the application

Users security was given the highest priority, from users’ password hashing to security of users’ input from

Cross-site scripting (XSS attack), Laravel proves easy way to implement.

Laravel makes it easy to protect your application from cross-site request forgery(CSRF) attacks. Cross-site request forgeries are a type of malicious exploit whereby unauthorized commands are performed on behalf of an authenticated user. The user is protected from copying of user details entered in input boxes.

Laravel automatically generates a CSRF "token" for each active user session managed by the application. This token is used to verify that the authenticated user is the one actually making the requests to the application.

### 6.9 User Registration

We first dealt with registration of the user. TrustBank stores the full name of the user, the mail address and the gender of the user. For the purpose of the implementation, we chose to not take into account the user’s full name or gender. In order to implement the SMS 2FA option, our implementation requires the user to provide a valid phone number during registration. Laravel assist in creating models with easy. The eloquent model attributes are mapped in the database through migrations.



Figure 9: diagram showing a user uers eloquent model to capture user details during reistration

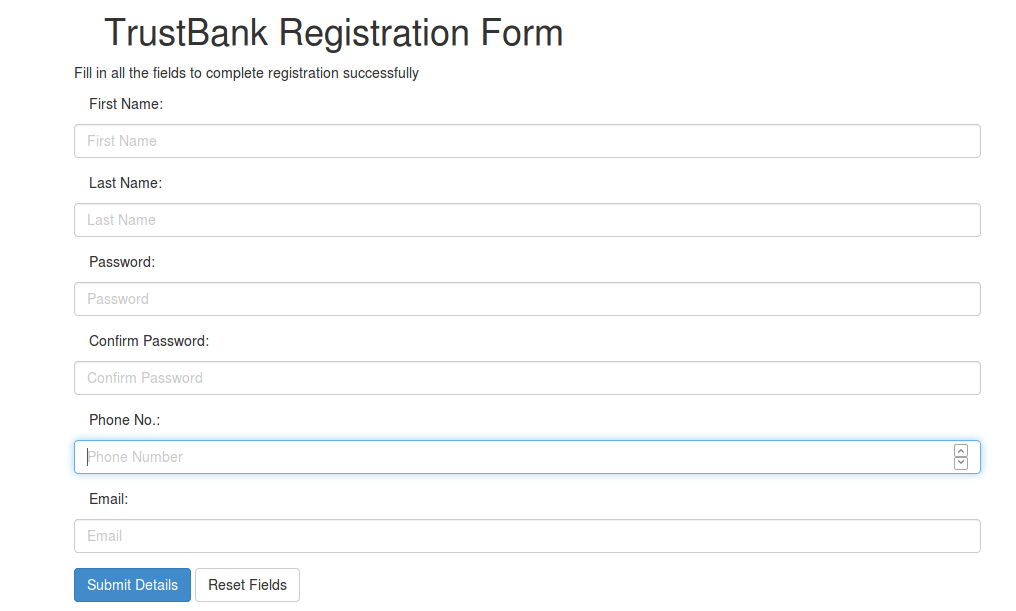


Figure 10: TrustBank registration form

#### 6.10 Password encryption

The email address, password, and phone number are then stored in a database. The password is encrypted through **argon** algorithm before being stored in the database.

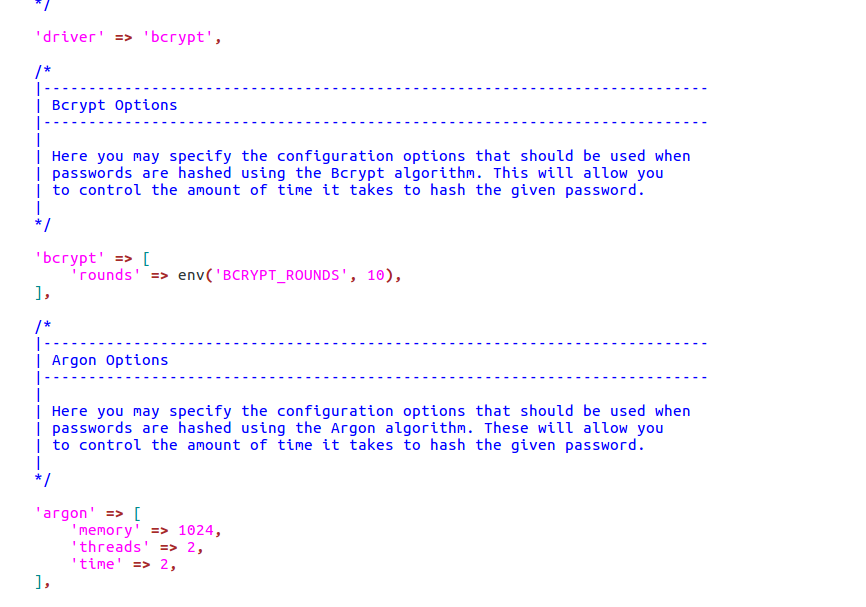


Figure 11:laravel password encryption

### 6.11 SMS authentication

If the user proceeding with login has SMS 2FA enabled, three additional PHP files are used to handle the login. First, the user clicks on login button, if correct login details are entered, they are redirected to verification where the user enters the sent Verification code from Afrikas’ talking Rest API as show in the figure below. The user is then redirected to a page that displays a form into which the SMS code has to be entered When the user enters s a code and clicks the validate e button, a 2FA controller file will check whether the code is correct and if so, then the user is granted access and redirect to online banking. If the code entered does not match, an error indicating incorrect code will be shown as in the figure below.

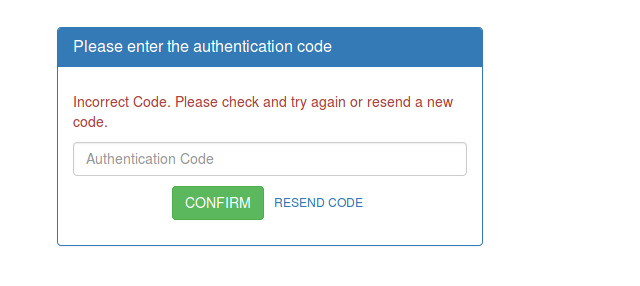
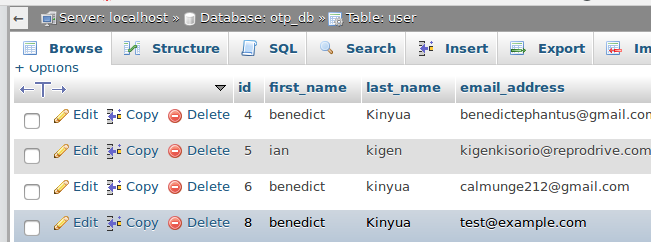


Figure 12: user authentication.



### 6.12 User login

This page checks whether the user-name submitted in already exists in the database,

if exists then, it will again redirect to register throwing an error –username already

exist, please try another one. and if does not exist, It will perform the following

steps:

1. Inserts a new user login details in user-login table namely, username and password. The user-id is an auto incremented field and increments its value by 1.
2. Based on the last inserted user-id in user-login table, it will insert a new record in user-details table updating all the contact details of the user.
3. Inserts a new record in user-balance table by a default value of zero in account balance.
4. Displays the login form and on submitting this form will redirect to home online banking page.

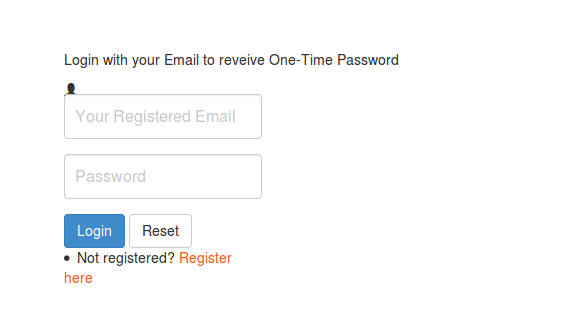


Figure 13: diagram showing TrustBank login screen

# 

# 7.0 Testing

Testing is the process of detection errors. Testing performs a very quality role for assurance and for ensuring the ability of software. The results of testing are used latter on during maintenance also.

### 7.1 Testing Objectives

The main objective of testing is to uncover a host error, systematically and the minimum effort and time starting formally, we can say:

1. Test is the process executing a program with the intent of finding an error.

2. A successful test is one that uncovers as ad yet undiscovered error.

Functional Tests are used to exercise the code with nominal inputs (input values) for which the expected values are available. We also know the boundary conditions for these inputs. For instance, functional testing of matrix multiplication can involve some data (matrices) for which the results are known in advance.

Performance Tests are utilized in order to determine the widely defined performance of the software system such as an execution time associated with various parts of the code, response time (in case of embedded systems), and device utilization. The intent of this type of testing is to identify weak points of a software system and quantifying its shortcomings, leading to further improvements.

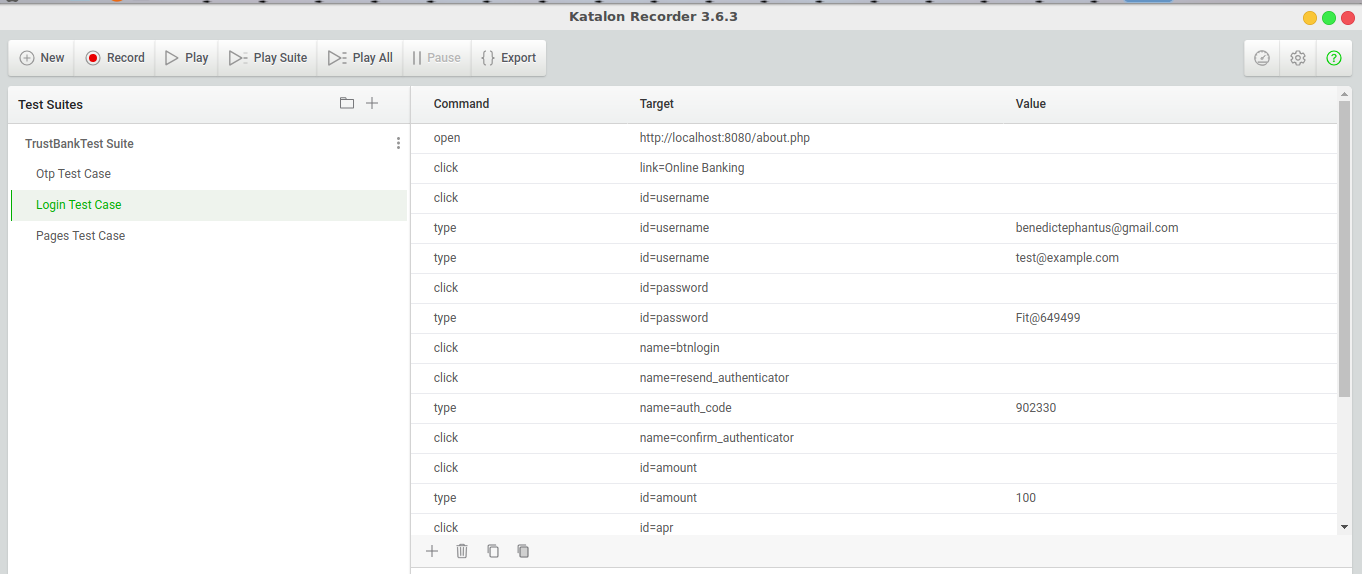


Figure :test cases with katalon studio

### 7.2 Achievements

The two main goals of the thesis project were met. A prototype 2FA solution was provided to TrustBank. Moreover, we analysed different 2FA methods in terms of cost, UX, deployment, and security. To analyse out-of-the-box solutions and how account recovery could be handled when implementing 2FA were goals as well.

We were also able to implement trade solutions to TrustBank web platform. The user can view up-to-date forex exchange displayed on the web application. We successfully made HTTP request from fixer.io using axios, a vue.js library for ajax call on API’s. Platform rich of information on Forex trade for our customers was put to consideration during development.

# 8.0 Conclusion

The traditional single-factor authentication is considered as “inadequate” to protect the transactions from criminal attacks such as account fraud and identity theft (FFIEC, 2005; Hong Kong Post 2007). A consensus regarding a more controlled protection over the security of online financial transactions has emerged and Kenyan Banks has been following a global trend to adopt multi-factor authentication. For example, the largest banks in Kenya are now offering the Short MessageService (SMS) payment security service using mobile phones as a different channel for authentication while others provide password-generating tokens to their Internet banking customers –as with Equity Bank online Banking.

However, despite its increased security assurance, the two-factor authentication techniques are not free from criticisms (Giessen 2006; Hoffman 2005). Schneider (2005) argues that two-factor

authentication will not prevent all the attacks happening in remote authentication environments over the Internet. Moreover, although some two-factor authentication supporters argue that the customers would feel confident and secured if they have an extra layer of security, there is a conception that two-factor authentication will be a barrier for users to adopt Internet banking services because it will increase the amount of users’ efforts to access their bank account and perform financial transactions (Matthews, 2006; Giessen 2006).

During the testing of the implementation, it was found that the system was working as expected and that our implementation of the two-factor authentication system was working and had better security compared to the conventional one-factor authentication system.

# Appendix

**PHP**:

PHP: Hypertext PRE Processor, is a widely used, general-purpose and server side scripting language that was originally designed for web development, to produce dynamic web pages. We can embed PHP into HTML and that usually runs on a web server, before that we have to configure and process PHP code used to create web page content from it. That configuration can be deployed on most web servers and also into almost every operating system and platform for free of charge.

Statistics shows PHP was installed on over 20 million websites and 1 million web servers.

**MYSQL**:

MYSQL is a RDBMS, which can be abbreviated as relational database management system. The database management system that we used in this application was MySQL .[MySQL database will allows users to create a relational database management system structure on the web-server that may be present in somewhere to store data like fields or records or user details. This program runs like a server providing multi-user access to a number of databases.

**CSRF**:

Cross-site Request forgery is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user’s web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful CSRF attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function via the target's browser without knowledge of the target user, at least until the unauthorized transaction has been committed.

**Laravel**:

A php framework intended for development of web applications with an organized file structure. We used it to develop the back end -eloquent models, controllers, and authentication logic.

**Vue.js**:

JavaScript framework for building web interfaces – we used Axios library for HTTP requests from fixer.io API

**Tailwind CSS**:

A utility first CSS framework for building custom user interfaces: We used it to develop the front end.

**Africa’s talking** :

AN API to service SMS, USSD, voice, payments and airtime applications.

**Fixer.io** :

An API used to capture the latest forex exchange prices.

**composer**

Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you.

## Dependency management

Composer is not a package manager in the same sense as Yum or Apt are. Yes, it deals with "packages" or libraries, but it manages them on a per-project basis, installing them in a directory (e.g. vendor) inside your project. By default it does not install anything globally. Thus, it is a dependency manager. It does however support a "global" project for convenience via the global command.

**Argon:**

argon is a password hashing scheme, which implements a memory-hard function with memory and time requirements as a parameter. It is designed so that any reduction of available memory imposes a significant penalty on the running time of the algorithm. Argon Collision and forgery resistance. Argon is a parametrized scheme with two main parameters:

• Memory size m (m cost). Argon can occupy any number of kilobytes of memory, and its performance is a linear function of the memory size.

# Bibliography

1. Michael Pearce, Ray Hunt, SheraliZeadally. Assessing and Improving Authentication Confidence Management, University of Canterbury, New Zealand and University of the District of Columbia.
2. Subashini, K., and Sumithra, G., “Secure multi modal mobile authentication using one time password.” 2 nd International Conference on Current Trends in Engineering and Technology (ICCTET), 2014, pp. 151-155. IEEE, 2014.
3. Suzumura T, Trent S, Tatsubori M, Tozawa A, Onodera T. Performance

comparison of Web Service Engines in PHP, Java and C,IEEE International

Conference on Web Services 2008.

1. Naphtali Rishe, Khaled Naboulsi, Ouri Wolfson, Bryon Ehlmann. An Effi-

cient Web-based Semantic SQL Query Generator .High Performance Database

Research Center, Florida International University.

1. Muhammad Saleem, Kyung-Goo Doh. Generic Information System Using

SMS Gateway. Fourth International Conference on Computer Sciences and

Convergence Information Technology 2009.

1. ‘What is 2FA?’, securenvoy.com. [Online]. Available:

https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm.

1. ‘National Information Assurance (IA) Glossary’. CNSS, 26-Apr-2010 [Online].

Available: https://www.ncsc.gov/nittf/docs/CNSSI-4009\_National\_Information\_Assurance.pdf.

1. ‘Recommendations for the security of internet payments’, European Central Bank,

Frankfurt, Germany, Jan. 2013 [Online]. Available:

https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpayme

ntsoutcomeofpcfinalversionafterpc201301en.pdf.

1. ‘Text for ITU - T Recommendation X. 1254 | ISO/IEC DIS 2911 5 – Information technology – Security techniques – Entity authentication assurance framework’, ISOIEC JTC 1SC 27, Nov. 2011 [Online]. Available: https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf.
2. C. Mulliner, B. Ravishankar, P. Stewin, and J.-P. Seifet, ‘SMS-Based One-Time Passwords: Attacks and Defense’, in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Berlin, Heidelberg, 2013, vol. 7967, pp. 150–159 [Online]. DOI: 10.1007/978-3-642-39235-1\_9
3. E. Feigenbaum, ‘A more secure cloud for millions of Google Apps users’, Google Cloud Official Blog. 20-Sep-2010 [Online]. Available:https://cloud.googleblog.com/2010/09/a-more-secure-cloud-for-millions-of.html.
4. S. Beaudin, ‘An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud’. Nova Southeastern University, 2016 [Online]. Available:

http://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1957&context=gscis\_etd.

1. K. M. Apampa, G. Wills, and A. David, ‘User Security Issues in Summative E- Assessment Security’, Int. J. Digit. Soc