AN ENHANCED MODEL FOR SECURING PASSWORD AUTHENTICATION USING TYPING PATTERN

By

ADJEI-TWUM YEBOAH

(BSc. Information Technology Education)

A Thesis submitted to the Department of Computer Science, Kwame Nkrumah University of Science and Technology in partial fulfilment of the requirements For the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

College of Science

JUNE, 2018

DECLARATION

I hereby declare that this study is the result of my own original work and that no part of it has been published by another person or presented for another degree in this University or elsewhere to the best of my knowledge. Except where necessary, acknowledgement was duly made in the text.

ADJEI-TWUM YEBOAH 20429861 ……... ……
Signature Date

Certified by:

DR. JAMES BEN HAYFRON-ACQUAH …… ……
(Supervisor) Signature Date

Certified by:

DR. M. ASANTE …… ……
(Head of Department) Signature Date

ABSTRACT

Data security is a critical concern for most organisations. Textual password is the commonest authentication system for verifying users though there are a number of well known vulnerabilities associated with it. The other alternatives like biometrics and graphical passwords also have their drawbacks. The aim of this study was to propose a scheme that provides another layer of security to textual password by using a typing pattern which does not require extra device. Therefore, making it cost effect. The cost of data breach is a universal concern and an area of importance for every modern organisation. Developing a scheme for enhancing password authentication, will improve the security of data therefore reducing data breach. Implementation of this scheme will provide security for users who lose their usernames and passwords since just the username and the password will not be able to log in a user. This scheme will reduce most of the attacks on textual password such as phishing, keylogging, brute force attacks, etc. The research questions that guided the study were, how can a model be developed to enhance the security of password authentication? And to what extent will user authentication model using typing pattern make password authentication more convenient and secure? Experiment method was used by the researchers to find answers to the research questions. 20 participants made up of equal number of novice and expert users representing the general populace of computer users were used in the study. The results of the study revealed a very low false rejection rate and false acceptance rate. The proposed scheme prototype demonstrated that the scheme is viable in practice and cost effective. The study also revealed that by using this model, users do not really need to pick a complex password that they might forget, but rather a good rhythm different from their natural typing rhythm that will be difficult to guess.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENT

Now to the King eternal, immortal, invisible, to God who alone is wise, be honor and glory forever and ever. Amen. (1Ti 1:17)

My utmost appreciation is to God almighty for endowing me with the abilities, strength and discernment to complete this thesis successfully. My heartfelt appreciation is to my proficient and approachable supervisor Dr. James Ben Hayfron-Acquah for taking a lot of time off his busy schedule to supervise this work and whose priceless inputs have really made this thesis see the light of day.

To the participants that made this work possible, I say may God bless you for your time and patience. Finally, a big thank you to my family and friends especially Abigail N. Amankwaah who through diverse ways supported me to finish this work.

ABBREVIATIONS AND ACRONYMS

ATM	Automated Teller Machine
DH Protocol	Diffie – Hellman Protocol
DNA	Deoxyribonucleic Acid

EER	Equal Error Rate
ENISA	European Union Agency for Network and Information Security
FAR	False Acceptance Rate
FRR	False Rejection Rage
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IE	Internet Explorer
MIT	Massachusetts Institute of Technology
MULTICS	Multiplexed Information and Computing Service
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
PIN	Personal Identification Number
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SMS	Short Message Service
SSL	Secure Socket Layer
TOTP	Time-based One Time Password
XSS	Cross-Site Scripting

CHAPTER ONE

INTRODUCTION

1.0 Background of Study

For an organisation to thrive in this modern business world, management of information within the organisation is very vital. To provide quality customer service and keep customers for a very long time, one has to manage customer information very well and have the information that customers need. The workforce, from the senior managers to operational managers need to share and use authorised information in order to make healthier business decisions irrespective of their geographical locations, whether they are at the same premise or distance apart. Just as blood is so essential to human existence, so is information to the success of an organisation.

Organisations are made up of different levels of management and departments. There are certain data that are meant for the consumption of a particular level of management, department or an individual alone. The other stakeholders are not supposed to have access to these data. Individuals that deal with these organisations also sometimes provide sensitive information to these organisations and therefore demand that only authorised users of the data can get access to it. This need gave birth to data security. Data security refers to defensive digital privacy methods that are applied to avoid unauthorised access to computers, databases and websites ("What is Data Security?," n.d.). Security threats to computerised information systems, confidential data include unauthorised access, modification, malicious damage of hardware, software, data or communication network resources. The aim of data security is to provide security, ensure integrity, confidentiality and safety of an information, hardware, software and data.

Authentication is a key concept in data security. Authentication refers to the verification of the identity of the user. Authentication is done in three different forms; something the person knows

(knowledge based) e.g. User ID and Password, something the persons has (object or token based) e.g. ID Card and smartcard and something a person is (biometric) e.g. signature detection and finger print. Password authentication which is a knowledge based authentication is the commonest mechanism for verifying the identity of users. Most digital systems use password as their primary means of authentication. Most people are conversant with logging in to their operating systems, accessing their email or signing-in to a social media network. Passwords are also used in other systems such as banking terminals, web and desktop applications like websites. Some network components like routers and switches also employ the use of passwords.

Password security is a challenge of ever growing importance. The amount of user identity information is rising intensely with increase in internet services. This increase in computing power and sophisticated networks have also increased the vulnerabilities of these systems. More than a million accounts were hacked and compromised from the servers of an online gaming company (DiGiacomo, 2017). The data that were leaked included usernames, passwords, email addresses, IP addresses, and other optional record fields. Organisations are revealing more incidents where data was breached or stolen.

The past few years have been momentous, contending with cyber-attacks almost every week. In the summer of 2012 ENISA published that just in a couple of months 18.4 Million passwords had been stolen (ENISA, 2012). Many big companies were hacked and some events surrounding the breach made it public. In some cases, the perpetrators were the ones that made the breach public, in others the organisation found it necessary to inform their users about the incident and recommend the appropriate actions to be taken to safeguard their information. One of such breaches was the very public release of 6.5 Million passwords from Linkedln on June 6 2012. Though most of the passwords released were still hashed, some of the easy passwords had been

already exposed (Silveira, 2012a). Immediately after the events, Linkedln prevented access to the compromised accounts of their affected users and advised that everyone changes their password regularly to allow them take advantage of the newly implemented salting of their password database. The salt would help Linkedln attain an "extra layer of security that is a widely acknowledged best practice within the industry" (Silveira, 2012b).

The mismanagement of passwords ranks very high as one of the main courses that hackers use to gain access to a system. Prior research identified the presence of human error risks to the security of information systems. The past research outcomes of password issues as a human error risk factor has been further recognized as a danger to security by the University of Findlay Center for Terrorism Preparedness (2003), who came out with a vulnerability assessment technique to help organizations identify their weaknesses in terms of information security (Carstens et al., 2004).

With the ever-increasing use of information technology in our daily lives, there are also an everincreasing number of user accounts and passwords we have to remember and manage. The choice of passwords used for different information systems presents a dilemma. Users are tempted to use a single password across many sites thereby making these systems more vulnerable. Compromising one password can help an attacker take over several accounts (Gaw & Felten, 2006).

A lot of studies have gone on in the field of password security to find effective and more secure ways of managing passwords. One of the areas is hashing algorithms. For years, NIST has tirelessly worked to come out with standards on hashing algorithms. It explained the SHA family and has been bringing it up-to-date whenever there is a reasonable indication that the current ones are no longer enough. The development of SHA-3 became necessary as a result of the attacks that were discovered against SHA-1. Attacks against several cryptographic hash algorithms were

successful and serious attacks were published against the NIST approved SHA-1 within the years 2004 and 2005 (NIST, 2016).

Carstens et al. (2004) identified vulnerabilities produced through user actions. Their objective was to predict the vulnerability that a particular action of a user can cause. Their survey results indicated that individuals with eight to eleven passwords are at greatest risk of not remembering their passwords at least once a month. Therefore, the individuals resort to writing their passwords on a piece of paper to help them recall these passwords latter. The use of several passwords across different information systems resulted in a lot of studies in managing these several passwords of a user.

Silver et al. (2014), studied the security of popolar password managers and their policies on automatically filling in Web passwords. They examined browser built-in managers, and 3rd party managers and observed significant differences in autofill policies among password managers. They identified a number of vulnerabilities with these password managers and how these vulnerabilities could best be addresed.

The world is becoming closer and closer day by day because of the use of computer systems. The society depends mostly on the internet to transact business. There are a lot of confidential informaiton for users circulating over the internet. This confidential information is mostly accessed by users through password authentication (usersname and password). However, this mechanism is fragile through some user actions and some malicious software. Therefore an enhanced security is required to ensure that only authorised users will be able to access the account. This study therefore aims at improving the login-password authentication using a typing rhythm.

1.1 Problem Statement

Integrity, confidentiality and availability of information is an area of concern to every organisation. Every organisation hopes that data integrity is not violated, thus data is not modified without the owner's authority. They also hope that sensitive information belonging to an individual, an organisation or a body couldn't be accessed by unauthorised people. Finally, they hope that information would be available to authorised people on demand. Individuals with electronic accounts such as emails, also hope that no other person apart from themselves can access those accounts. If anyone can access the account, she must have given the person her credentials.

However, this is not the case with the status quo. There are countless events where people's accounts have been compromised and series of reports detailing data breaches. On April 29, 2015, ZenPayroll discovered that it had been the target of phishing, an illegal attempt to obtain sensitive information that permitted an unauthorized person to access one ZenPayroll email account ("Itrc Data Breach Reports," 2015). 8Track, one of the most well-known internet radio service providers, was hit with a data breach which compromised 18 million user accounts. The data hacked included usernames, email addresses, and partially encrypted passwords ("Data breach statistics 2017," 2017).

During 2016, there were several prominent account hijacks in which the targeted service was not breached, but rather a large number of the targeted service's clienteles were denied the control of their accounts because they had reused the same email and password from another online account. For example, Tabao, a Chinese auction site suffered a brute force attack where more than 20 million accounts where hijacked. The attack leveraged more than 100 million combinations of collected credentials from other breaches ("IBM X-Force Threat Intelligence Index," 2017).

These data breaches cut across most sectors. According to the Ponemon 2016 cost of data breach report, the greatest number of organizations that reported they have been breached were in the business sector, representing 45 percent of all breached organizations; followed by healthcare and the medical industry at 35 percent; education at 9 percent and the financial services sector at 5 percent ("IBM Cost of Data Breach Study - United States," 2017).

According to Verizon's 2017 Data Breach Investigations report, one of the primary causes of data breaches is weak passwords and/or stolen passwords. The easiest, fastest and least noticeable way that hackers use to obtain unauthorized access is to leverage a weak and/or stolen passwords ("Verizon Data Breach Investigations Report," 2017). Figure 1.1 reveals the tactics involved in breaching data and their percentages as reported by Verizon Data Breach Investigation report.

Figure 1.1: *How data breaches occur "Verizon Data Breach Investigations Report," (2017)*

From figure 1.1, 81% of hacking-related breaches are as a result of weak passwords and/or stolen

passwords. In at least one event relating to Dropbox, hackers acquired a password from a worker and used it to gain access to that worker's account. From there they got access to Dropbox user's account information ("Check Point 2013 Security Report," 2013). Password security concerns is an issue of ever-growing importance which cannot be taken too lightly.

There are various ways that a legitimate user loses his or her password. A legitimate user may lose his or her password through over the shoulder attack, an observer can observe over the shoulder of a legitimate user who is typing his or her password and steal the password. Through brute force attack, a user's account can also be compromised. In a brute force attack, automated application is employed to produce a huge number of consecutive guesses as to the value of the desired data. An experimental or a heuristic method used to gain user credentials such as a user password or Personal Identification Number (PIN) ("What is a Brute Force Attack?," n.d.). One example of a type of brute force attack is known as a dictionary attack, which might try all the words in a dictionary to find a match. To guard against brute force attacks, users are forced to use very complex passwords to either extend the time frame for breaking it or make it more cumbersome for the brute force software to break it. Because of the complexity of the password, users end up writing them in a book or keeping them in an electronic file which also compromises the password. Those who do not want to write also turn to use simple passwords because they don't want to forget their passwords. These easy to remember passwords are also susceptible to brute force attacks (Carstens et al., 2004).

Keyloggers pose another threat, they are a type of malicious malware that record the users' keystrokes and capture the characters that are pressed in and writes the data to a file. According to Webopedia, a keylogger is a kind of surveillance software that has the ability to track every keystroke you make to a log file ("What is Keylogger? Webopedia Definition," n.d.)

There are several ways where users' textual password can be compromised thus posing a threat to system security. These threats which include stealing the password using client-side malware (keyloggers), phishing the password using a spoofed website, and stealing the password from an authentication server are not really helped with a strong password (Bonneau et al., 2015). This study therefore seeks to strengthen the password security so as to make it more difficult or prevent a malicious person who uses phishing techniques or other methods to steal passwords from legitimate users from gaining access to unauthorised accounts.

1.2 Research Objectives

The main aim of this study was to enhance the security of password authentication by adding another layer of security using a rhythmic typing.

The specific objectives are:

i. Develop a more convenient and secure model for authenticating users of a computer system.

ii. Determine the convenience and efficiency of the system.

These objectives formed the basis for formulating the research questions that provided support for the main purpose of the study: An enhanced model for securing password authentication using typing pattern.

1.3 Research Questions

An examination of the purpose of the study and review of the literature revealed that the following research questions were suitable to form the focus of this study:

i. How can a model be developed to enhance the security of password authentication?

ii. To what extent will user authentication model using typing pattern make password authentication more convenient and secure?

1.4 Research Scope

Ensuring the integrity, confidentiality and availability of data transcend beyond password authentication. Even with password authentication, the architecture of password security system goes beyond user validation. It encompasses data transmission (i.e. the user credentials that are being transmitted to the password storage for validation), the password file (i.e. the password storage system). Hashing and salting of the password file and user actions are all different but important security areas of study that come together to ensure comprehensive security of data. However, this study focused on enhancing password authentication security.

1.5 Significance of the Study

As it has been established, the cost of data breach is a global concern and an area of concern for every modern organisation. It is therefore paramount that mechanisms are put in place to strengthen the security of data. Almost every individual has at least one account that is protected with a password. This accounts include email account, ATM, a student or staff portal, social media account, among other online and offline accounts. Hence a study to enhance password security is essential not only for organisations but individuals that operate with these organisations as well.

A study on the security of password authentication system is important for several reasons. First, developing a model for enhancing password authentication, will improve the security of data therefore reducing data breach. Second, though it is not advisable that users write their passwords, some users still write because they don't want to forget. This study when implemented will provide another layer of security for these users, knowing that even if the password falls in the wrong hands there is still a tendency that their accounts cannot be accessed. Third, a lot of people are afraid to

deal with online companies because they are afraid their accounts can be compromised, this study will therefore give them the confidence to deal with the online companies because of the assurance of security. Finally, this study will reduce over the shoulder attacks, brute force attacks, other phishing attacks and keyloggers that steal users' password.

1.6 Limitations of the Study

This model was evaluated using False Acceptance Rate (FAR) and False Rejection Rate (FRR). Due to limitations of financial, material and time resources, the number of participants for the experiment was not sufficient enough to really ascertain the effectiveness of the model. Though one of the subtle objectives of this model is to reduce brute force attacks, due to limited resources, the system couldn't be tested against brute force attacks.

1.7 Organisation of the Study

This study is in five chapters. Chapter One is basically the introduction. This deals with the background of the study, the statement of the problem, the objectives of the study and the research questions of the study. It also includes the significance of the study, the limitations and the delimitations of the study, and the organization of the study. Chapter Two focuses on the review of related literature which is relevant to the study. Methodology of the study is the subject of Chapter Three. It provides details on research design, population, sample and sampling techniques. It also indicates the instruments used in the data collection procedures, pilot study and intervention design and implementation. In Chapter Four, results of the study are presented. Finally, discussion of the results, summary of findings, conclusions, recommendations and suggestions for further research form the concluding chapter of the report.

CHAPTER TWO

LITERITURE REVIEW

2.0 Introduction

The purpose of this study is to enhance password authentication using typing pattern. This chapter takes a look at the existing literature in relation to the study. Materials written by other persons or authors in context with the topic were considered. First, we briefly examine the history of password authentication. We then look at the recent studies in relation to the topic.

2.1 History of Password Authentication

Passwords were originally used in the 1960s for accessing time-shared mainframe computers. During the development of the first time-sharing operating systems in the 1960s, passwords were

added to safeguard against practical jokes and researchers using unauthorised resources. The 1961 Compatible Time-Sharing System at MIT was likely the first to deploy passwords in this way. Multiple cases were recounted of users predicting one another's passwords and also at least one leak of the master password file that was stored in unencrypted format.

These concerns were effortlessly surmounted because all users were part of the same academic organization. The development of access control in MULTICS and Unix in the 1970s, passwords were adapted to defend sensitive information and computational resources. Passwords were protected by MULTICS by storing them in hashed form, a practice first developed by Roger Needham and Mike Guy at the University of Cambridge in the 1960s. With the mid-1990s the advent of the World Wide Web and e-commerce, efforts were made to substitute passwords with public-key cryptography via Secure Sockets Layer (SSL) client certificates or the competing Secure Electronic Transaction (SET) protocol. As Web-based services increased, usability issues arose that had not occurred for system passwords. Resetting forgotten passwords, previously a manual task for IT support staff, was automated through email, creating a common central-pointof-failure for most users. The prevalent availability of smartphones may be changing the paradigm, however, as in the early 2010s a number of online services, including Facebook, Google, and Twitter deployed free smartphone applications to serve as a second factor based on the emerging Time-based One-Time Password (TOTP) standard. Other applications send codes via Short Message Service (SMS) as a backup authentication mechanism. A few services have provided dedicated tokens as a second factor, usually in companies at greater risk of fraud (such as eBay and World of Warcraft) (Bonneau et al., 2015).

2.2 Related Work

In this study, our concentration was to add an extra knowledge based layer of security to the usual password authentication to improve its security. Researchers have come out with many alternative solutions for authenticating users, one-time passwords, biometrics, and graphical passwords. While these alternatives are quite auspicious, textual password is still prominent in user authentication.

User authentication is in three main forms. Knowledge based, object based and biometric based. This classification is shown in figure 2.1.

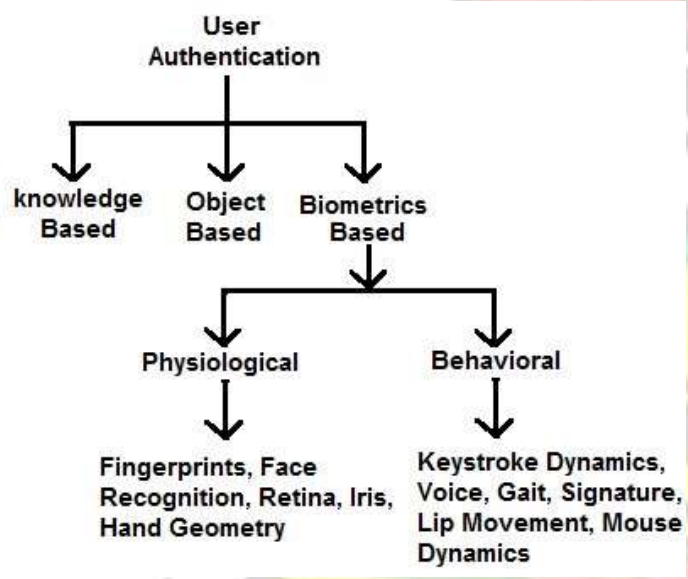


Figure 2.1: *Classification of authentication techniques (Guljari et al., n.d.)*

Carstens et al., (2004) evaluated the human impact of password authentication practices on information security. The purpose of their study was to come out with a model for assessing the human effect on password authentication. The study was focused on measuring the impact of password demands as a means of authentication and mitigating the risks that come about when these demands go beyond human capabilities.

Specifically, they were looking at:

- Evaluating user practices in determining passwords.
- Determining vulnerabilities produced through user actions.
- Testing the practicality of individuals customizing their passwords applying meaningful data and mnemonic devices in password formation.
- Determining the human impact that password authentication issues have on information security.

A survey was conducted to find out how the number of passwords a person has to remember impacts the security of an information system. The results of the survey were evaluated to aid the researchers in coming out with password guidelines that were used in a case study experiment.

A case study was performed at a larger US government agency with 30 participants. The participants created 3 password protected Microsoft word documents five days a week for three weeks. This was done to determine how individuals are able to remember a password created using generic instructions versus password created using mnemonic instruments.

The first stage of their experiment, required participants to form their own passwords that conform to strict password rules. These rules were:

i. Passwords should not be less than 7 characters in length

ii. Passwords should include symbols iii. Password cannot use the same term beyond two times iv. Password should not be a dictionary word or proper noun

v. Password must not be data about the individual such as social security number, date of birth, etc.

The second stage of the research mandated participants to create their passwords by chunking meaningful data together. The security of the password rules used in each stage were evaluated

using the multiplicative rule to determine how many guesses an individual will make to get the simplest proposed password.

Their survey results showed that those individuals with eight to eleven passwords were more likely not to remember their passwords at least once a month. Therefore, these individuals resorted to writing down these passwords in a book to refer to when signing in into their accounts. The results of the case study of the federal agency indicated that participants who formed their own passwords following the stringent password guidelines are more likely to forget their passwords than those who utilize mnemonic devices. 50.7% of the participants who formed their passwords using password rules were able to remember all the three passwords created. 72.7% of the participants who formed their passwords utilizing mnemonics were able to remember all the three passwords created.

The study therefore suggests that the use of mnemonic devices in password formation may impact information security positively. Their study also revealed the vulnerabilities caused by human factor on information systems. Some of these vulnerabilities identified are weak passwords, common passwords, visible passwords, and security policies not followed. They also stated that these vulnerabilities are caused by too many systems requiring passwords, and complexity of passwords making it difficult for the individual to commit to memory.

One strength of their study was that, the study was able to identify that individuals with 8 or more passwords are more likely not to remember their passwords at least once a month. This is significant in the sense that a lot of people have so many accounts online and this finding will aid the stakeholders to find a better way of managing their passwords or the passwords of their clients. Example of such is password managers. It was also able to bring out the fact that because of the complexity of the passwords, individuals are likely to write them down. So far as the password is

written down, it can be seen and used by others. Utilizing mnemonics have also been revealed through their study to be more secure than a usual password that will just conform to the password guidelines.

Though this study presents a lot of strengths, it doesn't solve all the problems with password authentication. From the results of their study, 27.3% of the participants that created their passwords through utilizing mnemonic devices still couldn't remember all the three passwords created and 23.5% still referred to a paper to recall their passwords which means the passwords were still written (Carstens et al., 2004). Although users are often advised to create passwords using mnemonic devices, little empirical evidence is there to prove it effectiveness (Kuo et al., 2006).

Kuo et al. did a study on the effectiveness of mnemonic passwords. A survey was conducted to gather sample of mnemonic and control passwords. This survey ran for fifteen days in February, 2006. Participants were individuals who were eighteen years and over, and had about 5 passwordprotected accounts online. The clear text passwords were imported for their analysis; therefore, participants were advised not to use passwords that they are currently using or have previously used. The passwords generated by the participants were analysed using several methods. Attempt was made to crack the passwords. The control passwords were matched against John the Ripper's English dictionary, and the mnemonic passwords were matched against a computer-generated mnemonic dictionary. The results from the cracking exercise were used to score the strength of the passwords. The control passwords were tested against a dictionary of about 1.2 million words and the mnemonic passwords were tested using 400,000 word mnemonic dictionary. Both the control and mnemonic passwords were subjected to brute force attack for 62 hours.

The results of their research revealed that more control passwords were compromised than the mnemonic passwords. Eleven percent (11%) of control passwords versus four percent (4%) of mnemonic passwords were cracked (Kuo et al., 2006). The emphasis here is that inasmuch as mnemonic password is preferred to control password, it is still vulnerable and can be cracked.

Dhamija and Perrig proposed an authentication scheme using graphics. The purpose of their study was to develop a system which sought to address the fundamental limitation of knowledge-based authentication which is human limitation to recall strong passwords. Instead of recalling passwords and pins, they rather propose an image-recognition system where the user identifies a number of images from a set of images that she selected when she was creating the account.

Their proposed system has three phases, portfolio creation phase, training phase and authentication phase. During the first phase which is the portfolio creation phase, the user picks a specific number of images from a pool of images presented by the server. Figure 2. 2 exhibits sample images that are used at the first stage of their prototype.

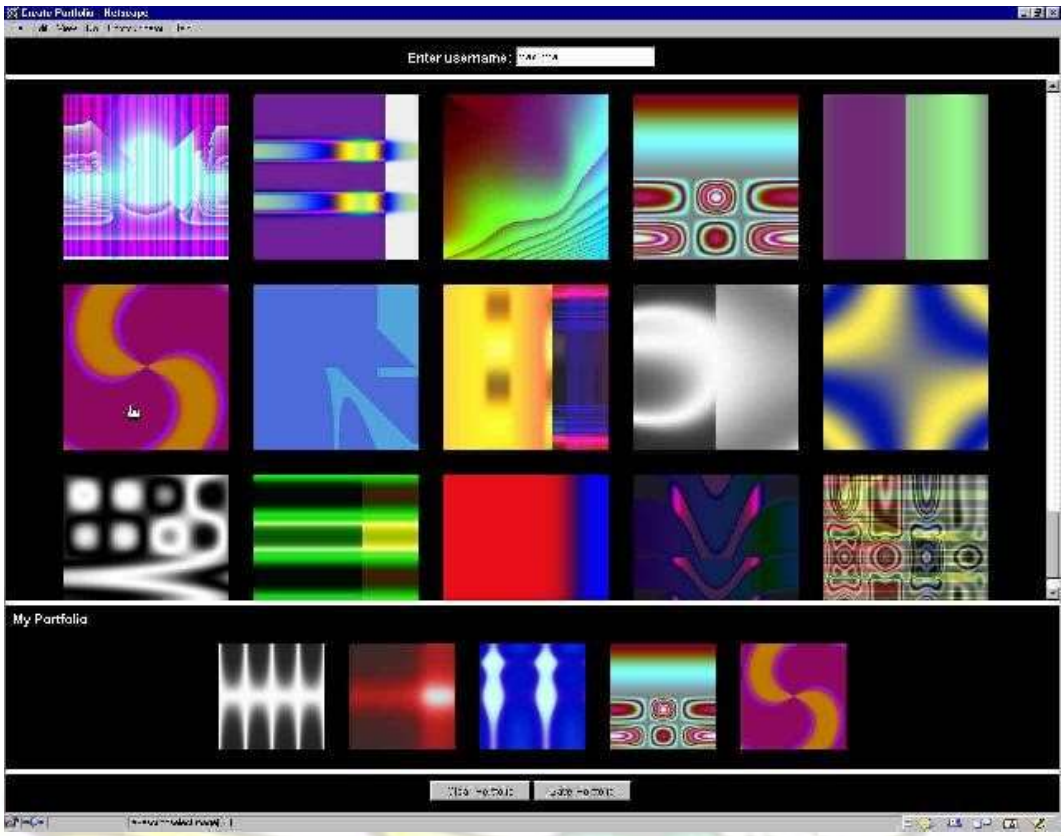


Figure 2.2: *Portfolio selection window (Dhamija & Perrig, 2000)*

From the window presented in Figure 2.2, the user selects the specific number of images that will be her authentication images. Example is shown in Figure 2.3.

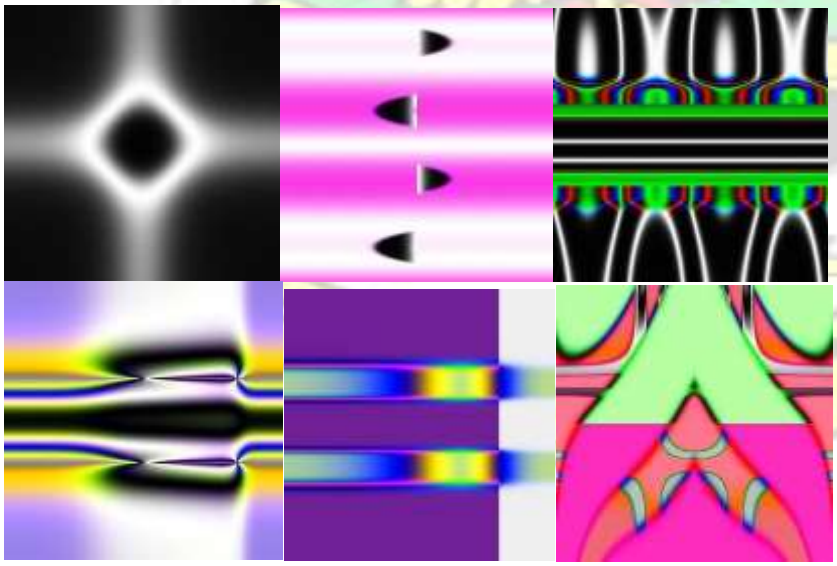


Figure 2.3: *Examples of randomly selected images (Dhamija & Perrig, 2000).*

After the images are selected by the user, the system moves to the second phase, which is the training phase. The purpose of this stage is to improve the probability of the user remembering the images that she chose. This is done by letting the user select the images in her portfolio from a collection of images which contains decoy images.

The final stage, authentication stage is where the user tries to get access to the system by selecting the images she chose at the portfolio creation phase. A server stores all the selected images of the users and presents a challenge to users who try to get authenticated. If the images selected by the user match the images she chose during the portfolio creation phase, the user is authenticated.

Twenty participants were selected to test the developed Deja Vu prototype. This phase consisted of two sessions. During the first session, participants were asked to create a four-digit PIN and a minimum of six characters' password. Participants also created two types of image portfolio, one consisting of five Random Art images and another consisting of five photographs.

Participants next had to access their created accounts using all the four authentication techniques, in the same order they were created. To authenticate using image portfolios, the users had to select their five chosen images from randomly intermixed images. The total images to select from is twenty-five. After one week, the participants again try to authenticate themselves using all the four techniques PIN, password and the image and photograph portfolios created in the first session.

From their study, they observed that a number of errors were made with the PINs, passwords and portfolios. These errors were more prevalent with the PINs and the passwords than the portfolios. Even after one week, the number of unrecoverable errors made with the PINs and passwords were far higher than the images. Majority of participants reported that it was easier to recall photo

portfolios than PINs and passwords and that, they will prefer that if the system is secure enough that is, image selection times were improved. Table 2.1 presents the results of their survey. The number of the twenty participants that failed to login after creating the accounts.

Table 2.1: *Percentage failed logins*

	PIN (%)	Password (%)	Art (%)	Photo (%)
Failed Logins	5	5	0	0
Failed Logins (after one week)	35	30	10	5

Source: (Dhamija & Perrig, 2000)

From their study, the participants found it easier to recall the images they selected for their authentication better than the passwords or the PINs. Participants didn't need to memorize any strings of characters that do not make meaning to them. This system would have been a better alternative to passwords and PINs, users would prefer this system to passwords because they wouldn't have to do a lot of mental exercise by memorizing (Dhamija & Perrig, 2000).

However, there are a number of drawbacks with their system. One, over-the-shoulder attacks. A user selecting these images can easily be seen by another person around. This is a common drawback of textual passwords. An attacker can easily see and identify the images more than the keys the user is typing. Another drawback is that, the sever storing the images stores the seed of the images in clear text. An attacker can therefore access this data though measures are implemented by their system to make it more difficult for an attacker to get access to it. Again, educated guess, is another drawback. An attacker who knows a user's taste in images and colours can predict which images are the user's portfolio.

Therefore, this system has its challenges like any other system. In this study, the emphasis is placed on the rhythm rather than the complexity of the textual password. Rhythms are easier recalled than text so the users' burden of picking and memorizing a very complex password is alleviated. An

attacker who chances on the users' password is now faced with the task of identify the rhythm that will be used to type the password. A good simple password that can be easily recalled by the user without having to write it is okay if the rhythm is good enough.

A similar work was done by Sreelatha, Shashi, Anirudh, Ahamer, & Manoj Kuar. They agreed to the fact that most graphical authentication systems are vulnerable to shoulder surfing. Therefore, they proposed a system that combines text with images or colours to create session passwords for authentication.

They proposed two authentication schemes, pair-based authentication scheme and hybrid textual authentication scheme. During the registration stage of the pair-based authentication scheme, the user provides her password which will be stored on the server. During login, the user is presented with a 6 x 6 grid consisting of numbers and alphabets which changes during every session. This is depicted in Figure 2.4.

***Figure 2.4**: Login interface of the pair-based authentication scheme (Sreelatha et al., 2011).*

The session password is generated from the original password submitted by the user during the registration phase. User considers her original password in pairs, for example; if the password is 'cd3k', the first pair is the 'cd'. The first character of the pair represents the row while the second character represents the column of the grid. Intersection of the pair produces the first character of the session password. In this example the intersection of 'cd' is '8', hence '8' is the first character of the password. This continues until you are done with all the pairs in the original password.

During the registration phase of their hybrid textual authentication scheme, the user is presented with different colours of which the user rates from 1 – 8. The same rating can be assigned to different colours. Example of the registration interface presented to the user is shown in figure 2.5.

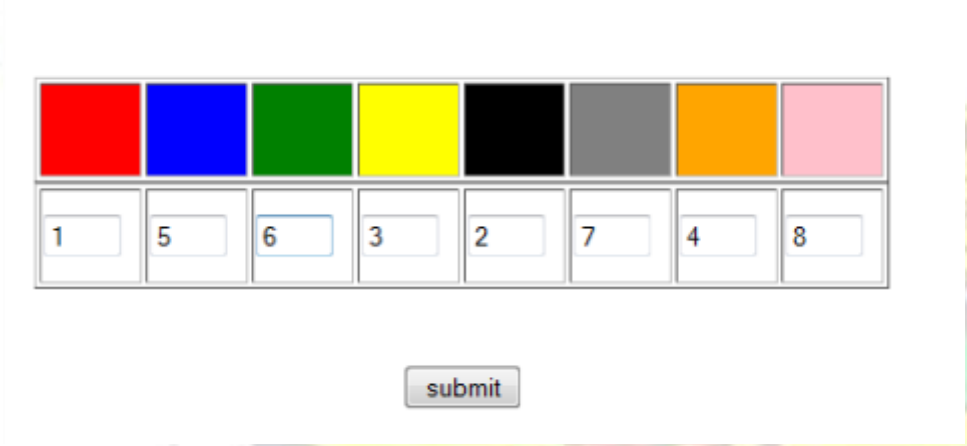
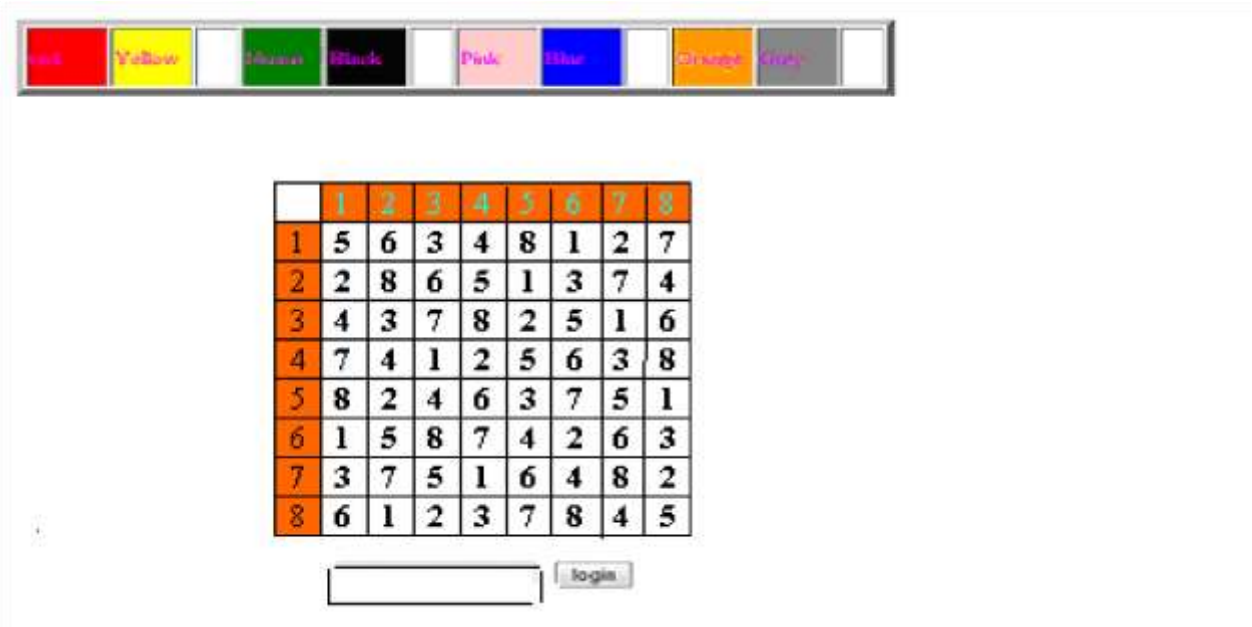


Figure 2.5: *Registration interface of the hybrid textual authentication scheme (Sreelatha et al., 2011)*

During the login stage, the user once again is presented with another interface with a set of colours based on the colours she selected during registration. The interface comprises of strips of colours based on the colours chosen and 8 x 8 grid of digits 1 – 8 placed randomly. Example is shown in figure 2.6.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Figure 2 6: *Login interface of the hybrid textual authentication scheme (Sreelatha et al., 2011).*

The colour strip contains four pair of colours, the first colour of a pair represents a row and the second colour of that pair represent a column. Based on the ratings given to the colours during registration, the session password is generated. For example, the first pair comprise of colours red and yellow. From the registration interface, the rating for colour red is 1 and that of yellow is 3. Therefore, the first pair produces the number 4, which is the intersection of 1 and 3 from the 8 x 8 grid. Hence, 4 is the first session password. This continues for the other pairs and eventually produces a password of '4311'.

One significant advantage of the pair-based authentication scheme is that the password changes during every login so the system administrator doesn't have to worry about users changing their passwords frequently. However, both schemes are still susceptible to many authentication attacks. With both schemes, the session password is generated from the grid of characters presented to the user and the intersection of the pairs can still be guessed using brute force (Sreelatha et al., 2011).

Also, these schemes are mostly suitable for PDAs because it's still vulnerable to shoulder surfing as the intersections of the pairs will still have to be typed using the keyboard. Another challenge is that the user is still bound to forget her original password or ratings for the colours and may end up writing them somewhere. Again, this authentication system is relatively slow.

Due to advancements in Information Technology, information security has become an inseparable component of Information Technology. There are quite a lot of techniques and schemes available for verifying the identity of a user. A study was conducted on the most commonly used authentication methods. The study discusses the simplest authentication methods as well as the available biometric authentication methods such as voice, iris, fingerprint, and face authentication.

The paper also looks at the current trends on the real life authentication methods which comprise symmetric, public-key, token, and biometric authentication techniques. The research demonstrated that inasmuch as password authentication is the most common used technique in authentication protocols, and it is also cheaper to implement, in terms of security password authentication is considered very weak. This weakness according to their research is because of software attacks. On the other hand, the study also showed that the password authentication system is very safe if the password is computed between the communication parties by employing publickey cryptographic system such as DH protocol.

The study also revealed that the standard token system is mostly useful for authentication systems whose risk level is not high, i.e. low to medium risk type authentication situations. Whereby, high risk authentications should rather implement multi-factor authentication. In biometric systems, they advised that though voice authentication is the commonest biometric authentication system, iris biometric should be implemented for high risk situations. The various performance rates among these biometric authentication methods are illustrated in table 2.2 below.

Table 2.2: *Performance comparison between biometric authentication methods*

	Finger	Voice	Iris	Face
Type	Physical	Behavioral	Physical	Behavioral
Method	Active	Active	Active	Passive
Equal Error Rate	2 – 3.3%	<1%	4.1 – 4.6%	4.1%
Failure to Enroll	4%	2%	7%	1%
Nominal False Acceptance Rate	0.1%	<1%	6%	4%
Nominal False Reject Rate	0.1%	<1%	0.001%	10%
System Cost	High	Low	Very High	High

Source: (Ao & International Association of Engineers, 2014)

The research concluded that most of the biometric techniques for authentication are secure, professional and provide very accurate authentication process. However, they require extra tools which make them very expensive to implement. The alternative provided by them is the DH public key method. Which they believe is also secure (Ao & International Association of Engineers, 2014).

Physiological biometric authentication though very secure require extra tools to implement, making it more expensive. Again, if the user has a disability or is deformed, for example, if the user has no hand she cannot be enrolled onto the system if the system is using finger print authentication. Password authentication is preferred in most situations because it is relatively cheaper and everybody can enroll. This study employs a multi-factor authentication system which does not require any extra tool to authenticate users. Hence the system this study proposes is cheaper and also robust against attacks.

Biometric authentication has become quite popular today due to their advantages. The user does not need to carry a card around, or recall a password. It cannot be shared or misplaced. This has

warranted a lot of studies in the area of biometric authentication. Bhattacharyya et al., (2009) did a review on biometric techniques and technologies. Among the ones they reviewed are:

i. Finger print technology: optical finger print sensors capture the pattern of the furrows and ridges of an individual finger which is unique to every individual. Finger print is one of the most popular biometric techniques used to ascertain the identity of a user. However, too wet or dry fingers will not produce an accurate image for processing. An example of a finger print captured is shown in figure 2.7.

Figure 2. 7: *Finger print (Bhattacharyya et al., 2009)*

ii. Face recognition technology: A computer system that automatically identifies or verifies a person from a digital image or video source. The face recognition system usually looks for the position of the eyes, nose and mouth and the distances between them. A drawback of this technology is that the system finds it difficult to differentiate between people that look very alike like identical twins. Figure 2.8 shows an example of a face recognition system.

Figure 2. 8: *Face recognition (Bhattacharyya et al., 2009)*

iii. Iris technology: The pupil of the human eye is encircled by a coloured area known as the iris. This is the section of the eye that is used by the iris technology. Research has shown that iris pattern is unique. It is said that an artificial duplication of the iris is virtually impossible due to distinct features of the iris. Sample iris image is shown in figure 2.9.

Figure 2. 9: *Iris image (Bhattacharyya et al., 2009)*

iv. Hand Geometry: This is the measurement of the user's hand in terms of height, width, thickness and surface area of the hand. This technology is based on the fact that the shape of a person's hand varies and doesn't change over time (Bhattacharyya et al., 2009).

v. Voice recognition technique: Studies have shown that voice pitching is unique to individuals. However, voice recognition techniques rather look at the way a person speaks which is behavioural than the pitch itself which is physiological biometric. One disadvantage is that surrounding noise greatly affects the accuracy of the sound sample.

vi. Signature verification technique: One of the behavioural biometrics is the signature of an individual. The nature and style that an individual signs her signature are measured and stored for verifying the user later. The characteristics that are measured include; pressure used in signing, direction, strokes length, number of strokes, duration, etc. During the verification process, the comparison is not between the appearance of the signature. That is, whether the two signatures (the original signature signed during the registration process

and the signature being used to be verified) look alike or they are the same. Rather, the dynamics of signing the signature is what is compared. Therefore, an attacker cannot deduce how the signature was written by merely looking at it. The most popular device for capturing signature dynamics is the traditional tablet, special purpose devices can be employed too. A disadvantage is that; a person's signature is not always consistent. The way and style the signature is written could be slightly different though it is the same person. This could affect the verification process. A sample signature captured using a tablet is shown in figure 2.10.

Figure 2. 10: *A signature captured using tablet (Bhattacharyya et al., 2009)*

A notable drawback of this technique is that a user does not see what she is writing on the tablet but rather on the monitor of her computer which can confuse her. Again, the user's signature on paper looks a bit different from the resulting signature produced by the tablet.

There are other biometric authentication methods which are not quite popular due to the fact that they are quite expensive or complex to implement and some are still in the stage of research and development. Some of these biometric techniques are;

- Palmprint: verifies a user using the valleys and the ridges of the palm instead of just the fingers.
- Hand vein: Uses the vein pattern in the hand.

- DNA: This requires a form of tissue, blood or other bodily sample for verification. For a user to be duly verified, the sample has to go through processes and this delays the verification process. DNA is employed mostly in crime detection.
- Thermal imaging: Works like the hand vein geometry, uses infrared to produce an image of the vein pattern in the face.
- Ear shape: This technology uses the ear markings to verify the identity of a person. Employed in law enforcement.
- Body odor: Research has shown that most of human characteristics are unique including how the person smells. Technological devices capture this smell from parts of the body like the back of the hand and convert it into a template.

The above techniques are evaluated in table 2.3.

Table 2.3: *Evaluation of Biometric techniques*

Biometric	**FAR**	**FRR**
Face	1%	10%
Finger print	2%	2%
Hand geometry	2%	2%
Iris	0.94%	0.99%
Voice	2%	10%

Source: (Bhattacharyya et al., 2009)

As presented in table 2.3, iris technique appears to be the most secure since the false acceptance and false rejection is very low. However, voice and face recognition are not quite convenient since the number of eligible users that may be denied access is quite high.

The growth of web applications has increased the number of online accounts a single user may have. Since password is predominantly the most used authentication system, users tend to have so many passwords that they have to manage. This is because of the security threat posed by using a single password across several platforms. This challenge drew attention to the study of password management. A password manager is a software that stores all the individual passwords of a user in a single file. This file is protected with a very strong password which is the only password the user has to memorise. A number of studies have already gone on and is still going on in this area.

Various sprouting corporate challenges complicate password management by increasing exposure to hacking and phishing attacks, or complicating protective measures. To help businesses address these difficulty, various password management solutions are entering the marketplace, each with different strengths and weaknesses. Some browser vendors provide password management systems, some are provided by third parties, and many are network based where passwords are backed up to the cloud and synced across the user's devices such as Apple's iCloud Keychain (Silver et al., 2014).

Most users are not familiar with security issues associated with some of these password managers. Silver et al did a comprehensive study on the vulnerabilities of theses password managers. They studied the autofill policies of ten popular password managers across four browsers. Some of the vulnerabilities identified are:

i. Sweep attacks: An attacker takes advantage of the authomatic password autofill to steal the user's login details across multiple sites at once without the user visiting those sites. ii. Attack amplification via password sync: Most password managers are able to sync passwords across several devices. These password harmonization services can possibly result in password mining from devices without them ever having visited the victim site.

iii. Injection Techniques: An attacker injects a login window into any webpage in the origin of the actual login page and launches a password mining attack against that page.

iv. Active Mixed Content: HTTPS webpages that contain active content (e.g., scripts) that are sent and received over HTTP is also a potential vector. If rendering active mixed content is enabled in the user's browser, any HTTPS page containing active mixed content is a threat to injection. Silver, et al., further opined that Chrome, Firefox, and IE block active mixed content by default but provide a user option to enable it. Safari, Mobile Safari, and the Android stock browser allow active mixed content to be fetched and executed without any warnings. Several types of active mixed content, especially those processed by browser plugins, are harder to block.

v. XSS Injection: A cross-site scripting vulnerability in a page allows the attacker to inject JavaScript to change the page as needed. If an XSS vulnerability is present on any page of the victim site, the sweep attacks will work even if the site's login page is served over HTTPS.

Obviously, password managers though to some extent will take the burden of memorising so many passwords off the shoulders of users, come with their own limitations. When the password protecting the password file is compromised, all the accounts belonging to the user are compromised and the other vulnerabilities outlined above. A more robust technique which will still not burden the user of memorising and recalling very complex passwords is needed.

A behavioural biometric technique which is closely related to this study is the keystroke dynamics. Research has revealed that every user has a unique typing speed and style (Guljari et al., n.d.). This technique is equally cheaper since no extra device is required to implement, just software is needed.

In the study conducted by Guljari et al, they examined the dynamics involved in measuring keystrokes. According to their study, the features that are extracted are:

- Latency of keystroke
- Duration of keystroke
- Hold time
- Overall typing speed
- Frequency of errors
- Force of hitting keys when typing.

Out of these features the most commonly used keystroke dynamics feature is latency of keystroke and dwell time. Latency of keystroke describes the elapsed time between successive keys. Dwell time describes the duration between when a key is pressed and when it is released. The research also pointed out the most commonly used metrics for evaluating authentication systems. These metrics are the false acceptance rate (FAR) and false rejection rate (FRR). False acceptance rate defines the rate at which unauthorised users are granted access and false rejection rate is the rate at which legitimate users are denied access. Another security metric is the equal error rate (EER) which is the ratio of FAR divided by FRR. The lower the ERR, the better the authentication system (Patil & Renke, 2016).

Patil & Renke proposed an authentication system using keystrokes dynamics. When a user starts the application to be registered, a window is displayed to the user where she provides her username and password. When the password and the confirmation password match, the user is taken to the next stage where she types a given sentence ten times. The keystroke analysis is triggered when the user begins to enter the sentence, features like the dwell time and the flight time are measured

and analysed. The averages are calculated and stored in the database together with the password and username. A database table used by Patil & and Renke is shown in figure 2.11.

User Name	*Password*	*Mean (Mean Dwell)*	*Mean (Mean Interval)*	*Mean (SD Dwell)*	*Mean (SD Interval)*	*SD (Mean Dwell)*	*SD (Mean Interval)*	*SD (SD Dwell)*	*SD (SD Interval)*
Rohit	123	96.4600	175.7000	12.6975	110.2368	7.3461	13.8475	5.2093	9.4830
Rohit	123	98.1200	157.6800	13.7716	99.6234	5.1667	6.2810	4.9376	7.2932
patil	123	106.9400	160.9800	14.1134	100.4300	6.8326	8.3668	5.0013	6.4157
Saee	456	124.1900	170.8500	19.5792	123.9245	8.9117	28.9373	10.3670	41.8961
chandu	123	98.9833	217.2333	53.0199	190.5662	26.0138	6.0146	15.6338	123.0760
Saee	456	95.6200	159.1400	12.0134	14.8588	7.4198	13.6899	3.5414	11.7910
abhi	abhi	77.6750	239.8000	31.8558	213.2051	14.5622	71.8452	3.8252	75.1338
kamal	ashok	109.3000	170.5200	31.1811	124.4723	16.5345	15.9889	21.5353	14.5791
Patil	rohit	94.9895	442.9137	18.8481	353.7030	7.4868	38.6774	3.0138	102.3967
sandeep	deep	125.1286	223.9857	60.3746	155.0951	23.2529	38.1803	8.6884	68.6612

Figure 2. 11: *Keystroke dynamics database used by Patil & Renke*

The login window of their system is shown in figure 2.12. During login, the user enters her username and password, if they match what is in the database, she is taken to the next stage to reenter the sentence she entered during the registration stage. Again, the keystroke analysis is calculated and compared to what is in the database, if there is a match, the user is granted access otherwise denied.

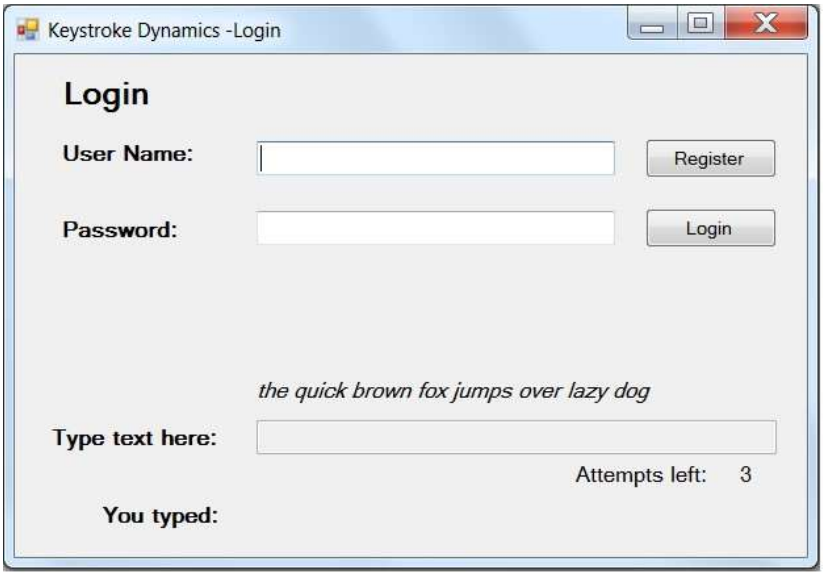


Figure 2. 12: *Keystroke dynamic login window used by Patil & Renke*

A major drawback of this design is the total time the user has to use to register. Entering the sentence provided a number of times before she can be registered, this affects the performance of the system. Again, since this technique is a behavioural biometric, with time as the user's typing style and speed change, it increases the false rejection rate.

In another study relating to keystroke dynamics, the researchers used the password field to extract the keystroke features. This is faster in terms of performance than the study conducted by Patil & Renke. With their scheme, the user enters her username and password, and as the password is being entered, the features will be calculated (Monrose, Reiter, & Wetzel, 2002). One advantage of this scheme is that the user may not even be aware that her typing style is being analysed to harden her password. An attacker who chances on the textual password may not be able to login because the typing styles are not the same. As said before, the challenge of this technique is that a user whose typing style changes substantially will find it difficult to login into her own account. Also, different keyboard styles affect the feature analysis, meaning a user who tries to login by using a different style of keyboard from the one she used to register may not be able to get access.

In conclusion, several authentication techniques are available for verifying the identity of a user. The most common method is the textual password. However, the vulnerabilities produced by this technique like phishing attack, dictionary attack, shoulder surfing, etc., have resulted in a lot of research to salvage the situation. A strong and complex password that contains numbers, symbols, letters (both upper and lower cases) and lengthy password can make the system more secure. But the primary problem here is the challenge in recalling those passwords. Though complex and strong password is more secure is still vulnerable to brute force attacks.

The other techniques being used instead of textual password are biometrics and graphical passwords. These two techniques are not problem free either, they have their own disadvantages.

Graphical passwords like the ones that have been reviewed in this study, have their strengths. Some of these strengths are that the user doesn't have to remember a complex password, some are shoulder surfing resistant. But some have shoulder surfing issues and some have usability problems. Biometric techniques such as DNA, palmprint, hand vein, ear shape, body odor are quite intrusive and not very popular in access control. Biometric methods like finger print, iris scan, facial recognition, voice recognition are quite popular but expensive to implement. Identification process of some of the biometric techniques too can be quite slow. They are also not convenient for deformed people. A more secure and convenient system is therefore required to mitigate most of the challenges suffered by the reviewed techniques.

In this study, we propose a multi-factor authentication system. This scheme doesn't require extra device to implement. Therefore, relatively cheaper than most of the biometric techniques. Unlike the other keystroke dynamics where the typing style and typing speed of the user is used, a calculated rhythm is used in the proposed scheme. One advantage of this calculated rhythm is that, it does not change over time. A rhythm is a rhythm today and will remain the same rhythm in ten

years' time. In terms of performance too it is fast since the password field is used to extract the features.

Another importance of the proposed scheme is that, it makes it more difficult for an attacker who chances on the password file even though the user may have chosen a simple or poor password, to still break into the user's account. This scheme conceals the details about which features of the user's password is extracted and analysed. An attacker who gets the password file, and all the details about how the features were extracted and computed can deduce the time intervals between the keystrokes, the proposed scheme prevents this.

CHAPTER THREE

METHODLOGY

3.0 Introduction

The literature reviewed, revealed most of the vulnerabilities posed by the current authentication schemes being used. This study was conducted to find a better scheme which doesn't call for any extra device or expenditure, but yet more robust to authenticate users. This chapter discusses vividly all the steps and methods used to achieve the objectives of the study.

Based on the reviewed literature, and to appropriately answer the research questions, experiment method was adopted for this study. First part of this section looks at the design of the proposed system and the second part is the experimentation phase where carefully selected participants were used to try the system. This will enable the researchers evaluate the system accordingly.

3.1 Tools

The following hardware and software tools were used to enable the researchers address the research questions.

Hardware

- Dell laptop computer ○ Model: Inspiron 5551 ○ CPU: Intel(R) Pentium(R) CPU N3540 @ 2.16GHz
    - ○ Memory: 4GM

Software

In order to develop a login program based on the proposed model, the following software were required:

- Visual Studio 2012
- SQL Server Management Studio

3.2 Design Phase

The design phase of this study is characterised by two sections, user registration phase and user login phase.

3.2.1 User Registration Phase

During this stage, the user is presented with a registration form just like any other user authentication scheme, she then provides her user name and password. Before she enters her password, she must have a rhythm in mind that she is going to use to type her password. Most of the works done in the area of keystroke dynamics use the user's typing style but this study proposes a novel approach where a calculated rhythm is used to type the password. For example, if the user's password is 'k2fu44', she doesn't type it using her normal typing style or speed. But rather she creates a rhythm for it. Figure 3.1 shows an example of how she can type this rhythmically.

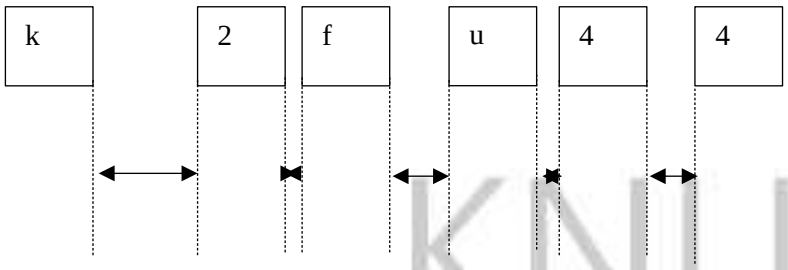


Figure 3. 1*: Timing differences between successive keystrokes*

The timing differences between the successive keys form the typing pattern or rhythm. Example, the latency between key 'k' and key '2' is 2.4 seconds, between '2' and 'f' is 0.3 seconds, between 'f' and 'u' is 1.9 seconds etc. These timing differences create the rhythm for the password.

The user re – enters her password for confirmation using the same rhythm. If the user name already exists, a message is displayed to the user to change the user name. Example of the message displayed to the user is shown in figure 3.2.

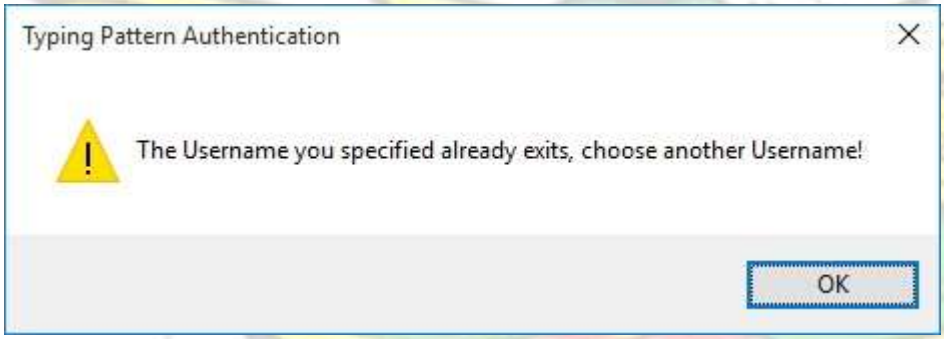


Figure 3.2: *Error message when the user name already exists*

After the user name verification, the two passwords are compared, if they do not match, another validation message is displayed to the user. Example of the message displayed to the user is shown in figure 3.3.

Figure 3. 3: *Error message when passwords do not match*

As the user types the password, the keystroke features are extracted and temporarily stored. As it has been explained in the literature review, latency of keystrokes also known as the flight time and dwell time, are the most common used feature of keystrokes dynamics (Guljari et al., n.d.). This study made use of flight time feature of the keystroke dynamics. If the two passwords provided by the user do match, the patterns for typing the passwords are also compared to see if there is a match. If the matching accuracy is 75% and above, the details provided by the user including the typing pattern is saved in the database. If there is no match, an error message is shown to the user. Sample of the database used is shown in figure 3.4 and the registration interface used is shown in figure 3.5.

Tools Window Help

UTESCO\SQLEXPRE...ern - dbo.UsersTB

ID	Username	Pswd	Ave1	Ave2	Ave3
1	Fred	445462	63651070214.3713	1.6251	5.3257
2	Dany	jk241a	63653246522.7653	0.2666	7.7402
3	Bridget	SR43CD	64651540977.3622	1.7326	8.1010
4	Mike	45432	63655541177.2154	0.1432	6.0407
5	Vero	daddy56	62353241034.5654	0.3223	4.0252
6	kofi	tab222	63652641121.7653	1.4544	4.5872
7	Paa	1234	64554248744.7653	2.0255	6.5445
8	Yaa	33dd33	63651240977.5555	1.1201	5.5444
9	Mommy	45cat	63351240733.7653	1.1281	6.3341
10	Marvin	0233454aa	63651249886.7653	1.9237	5.3265
11	NULL	NULL	NULL	NULL	NULL

Figure 3. 4: *Database for storing user credentials*

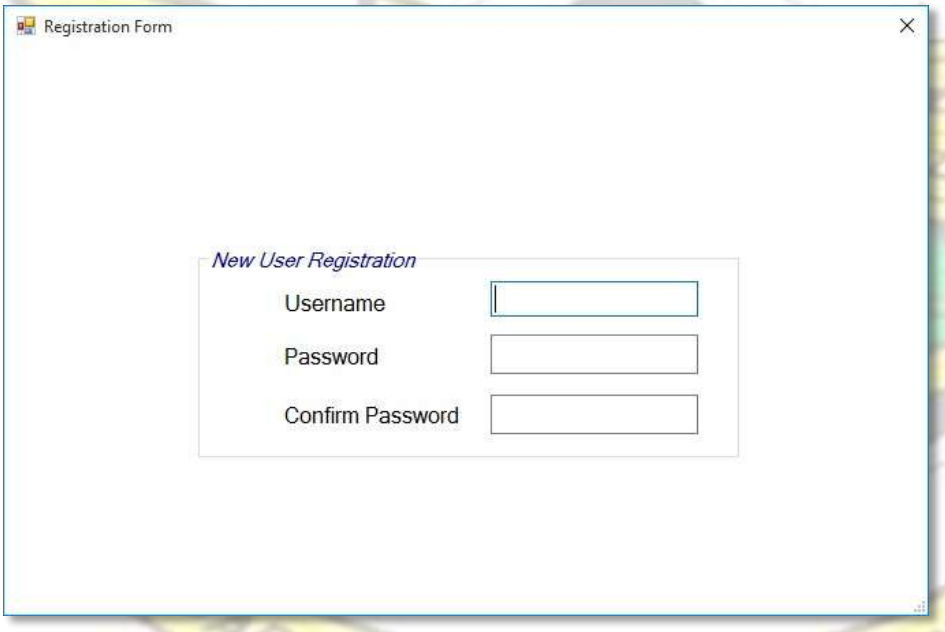


Figure 3. 5: *Registration interface*

To get a more accurate pattern computation, the Enter key is used instead of an OK button. The design model of the registration phase is shown in figure 3.6.

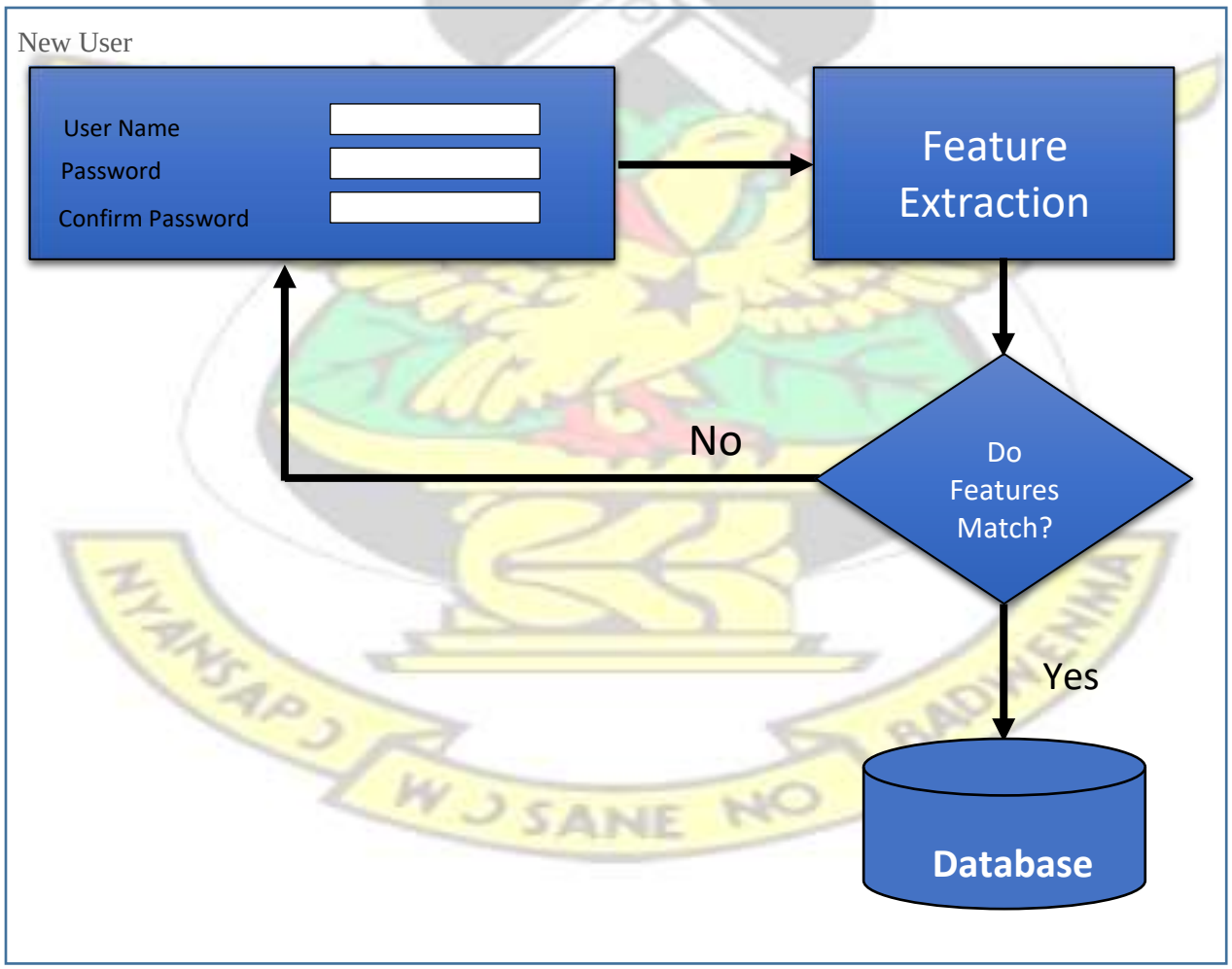

New User
User Name
Password
Confirm Password
Feature Extraction
No
Do Features Match?
Yes
Database

Figure 3. 6: *Flowchart of the registration process*

After the user enters her credentials using a calculated rhythm, these features are extracted, analysed and then compared. If there is a match, the details are stored in the database otherwise the user is prompted to re-enter them again.

3.2.2 User Login Phase

Figure 3.7 depicts the design model of the login process of this study.

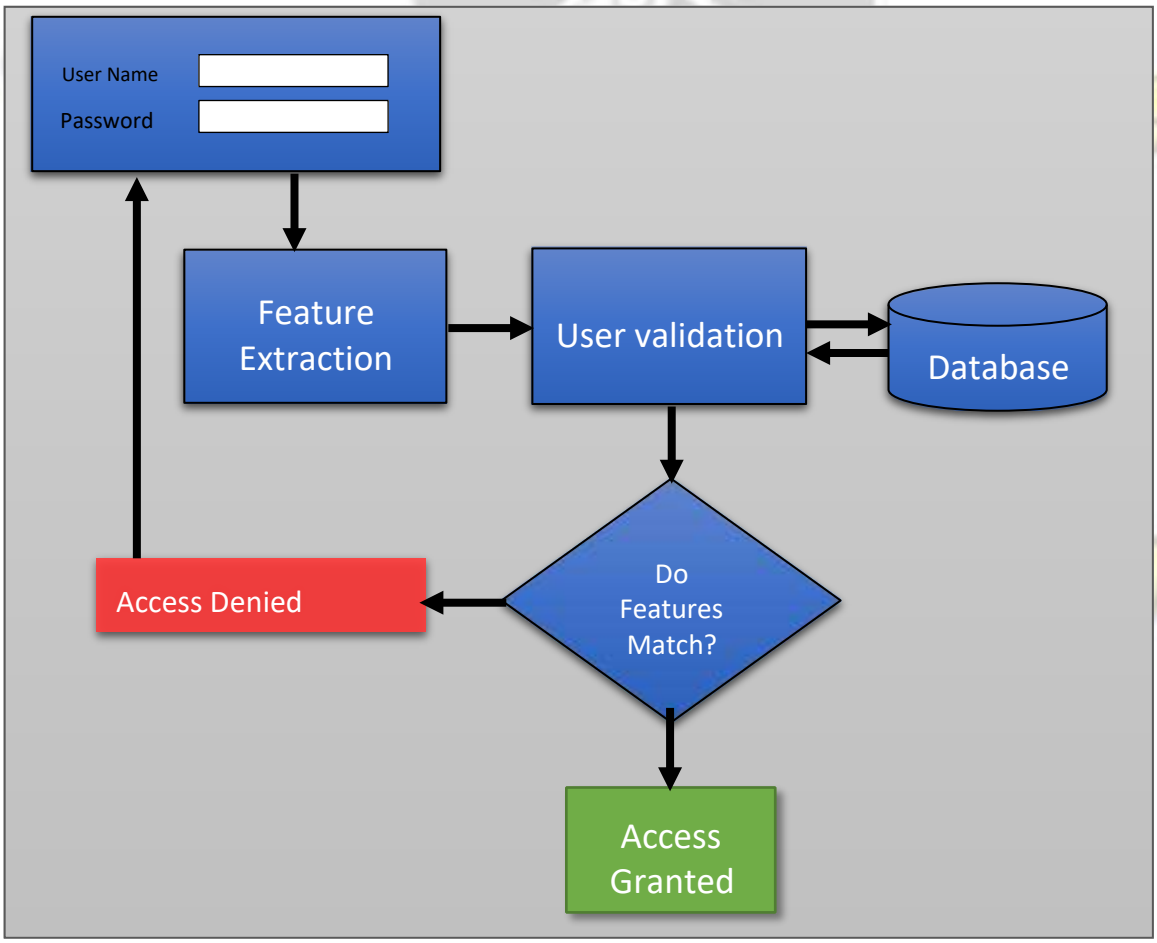


Figure 3.7: *Flowchart of the Login process*

An unknown user enters her credentials to be verified. First of all, the system checks whether a user name and a password have been entered otherwise a validation message like the one shown in figure 3.8, is displayed to the user.

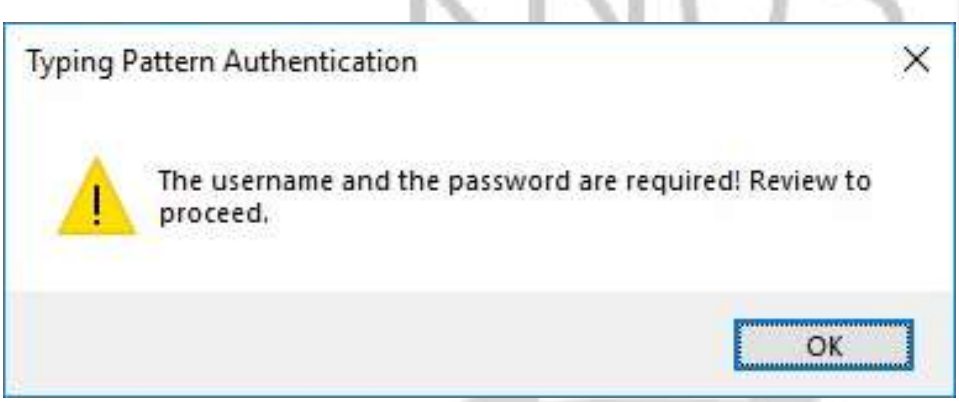


Figure 3.8: *Validation error displayed to the user when she forgets to type either the username or the password.*

If the user provided her username and password, these features are extracted and compared to the original data in the database. First, the username and the textual passwords are compared to see if they match. If they do not match, another validation message like the one shown if figure 3.9 is displayed to the user.

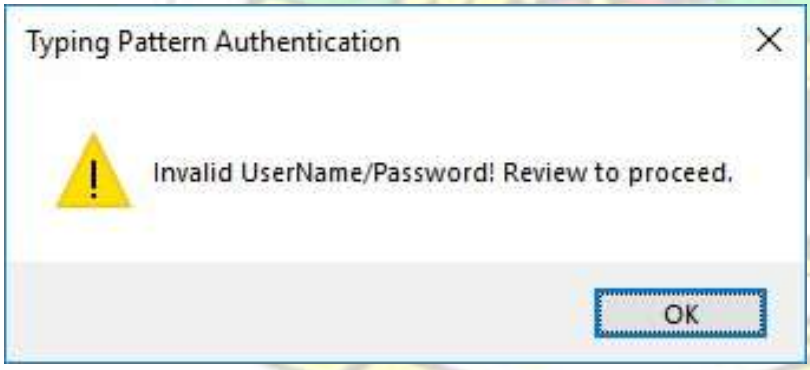


Figure 3.9: *Validation error shown to the user if either the username or the password do not match.*

However, if there is a match, the system then goes further to compare the patterns (latencies between successive keys). If the matching accuracy is 75% and above, the user is verified otherwise rejected. For the purpose of this study, the validation error message that is shown to the user when the username and the password match but the patterns do not match is different from the one shown in figure 3.9. The error message displayed to the user when the patterns do not match is shown in figure 3.10.

Figure 3.10: *Error message when the patterns do not match.*

In a real world implementation, the error message will be the same when either the textual password or the patterns do not match. This will make it more difficult for an attacker who tries to break into the system. She is faced with the task of recognizing the extra layer of security that has been added.

The login interface of the authentication scheme is shown in figure 3.11.

-

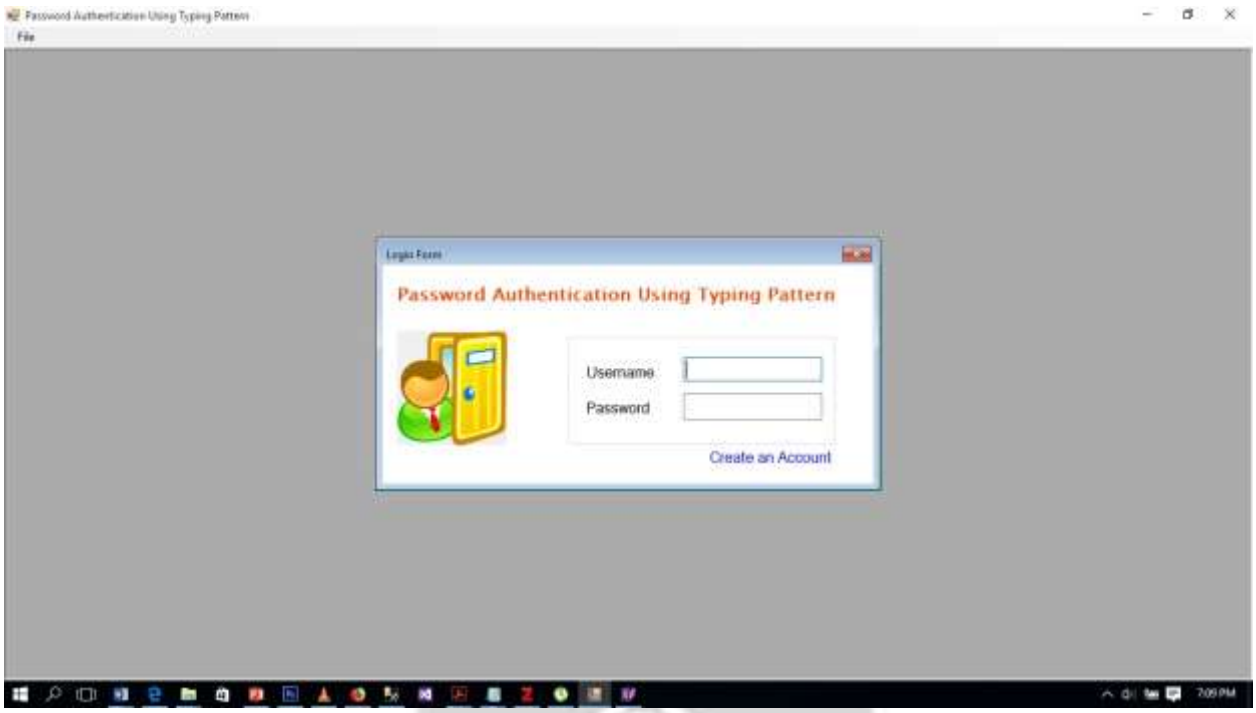


Figure 3.11: *Login interface*

3.3 Experimental Phase

The purpose of designing this authentication scheme is to find solutions to most of the problems posed by the current authentication schemes. To find out whether this scheme is more secure and convenient for users and it is even viable, an experiment was conducted using twenty participants. The participants were carefully chosen to be a representative of the general populace of computer users. An equal number of novice and proficient users and males and females were chosen. All the selected participants were quite familiar with textual password authentication. These participants were selected from the staff and students of Suhum Senior High Technical School. The experimental phase is characterised with six different stages.

The first stage of the experimental phase is the briefing stage. As this scheme is new, participants were comprehensively briefed about the technique. The registration process and the login process were appropriately demonstrated to the participants to enable them understand the scheme better.

During the second stage, the participants were asked to pick their passwords and rhythms. They were advised to do it independently and surreptitiously. They were also advised to select a username and a password they were not already using since this exercise is for an academic purpose and the passwords will be taken from them. The patterns chosen by the participants were practiced several times until they got used to it. The next step is to get enrolled onto the system using the chosen rhythmic pattern.

The third stage of the experimental phase is the login stage. Participants were asked to log in into the program using the username, password they provided during the registration stage. These passwords are to be accompanied with their respective patterns otherwise they will be denied access. The purpose of this stage is to enable the authors measure the false rejection rate (the number of legitimate users that will be denied access). Every participant had at most three attempts to successfully log in. if she is unsuccessful after the three attempts, she is temporarily logged out because she could be an imposter. This mechanism is to prevent an imposter who chances on the username and password of a legitimate user from trying to guess the rhythm. The message that is displayed to the user after the three attempts is shown in figure 3.12.

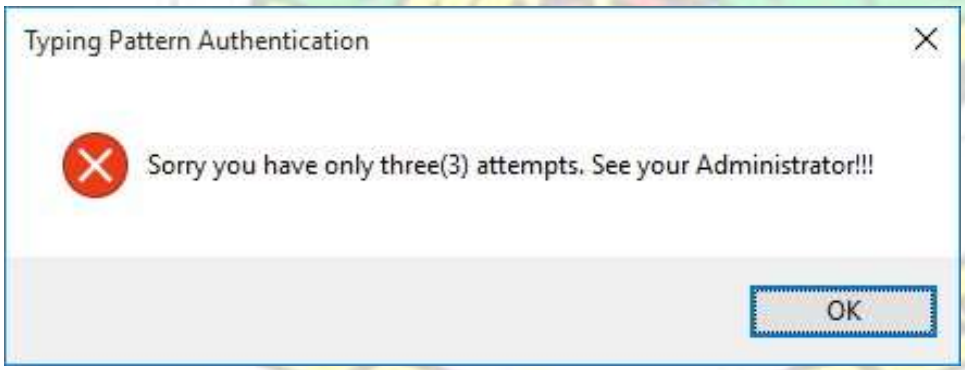


Figure 3.12: *Error message shown to a user who tries to login more than three attempts.*

If the user successfully logs in, another message is shown to the user to welcome her. This is shown in figure 3.13.

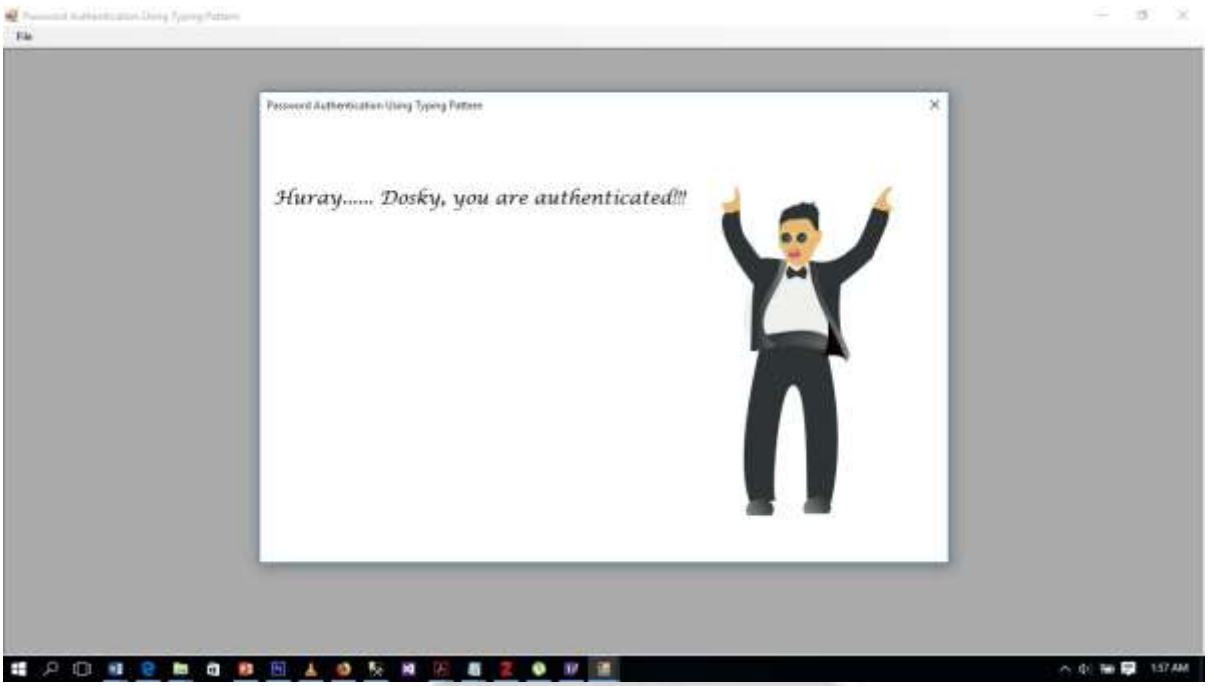


Figure 3.13: *Message shown to a user who successfully logs in.*

During the fourth stage, the participants were put into two groups. Participants in each group gave their usernames and passwords to the other participants in the other group without their typing patterns. The purpose of this was to measure the false acceptance rate. The participants now posing as imposters then try to log in using another person's username and password. The rate of user access was then measured.

The fifth stage was done to examine how secure the system is against shoulder surfing. The participants were regrouped; the first group were made to observe the second group whiles they type in their credentials to get authenticated. The second group also had their turn to observe their counterparts. They were then asked to sign in based on what they observed. Again, the total number of participants that were able to access the system were measured.

Finally, to ascertain the number of users who will be able to log in after a period of time without writing the password nor the rhythm, participants were called again after two weeks to access their accounts again. The false rejection rate was measured again.

As it has been highlighted in the literature review, the most common metrics for evaluating authentication schemes are the false acceptance rate and the false rejection rate (Guljari et al., n.d.). These metrics were applied to the various stages of the experiment and the results are discussed and analysed in the next section of the study.

CHAPTER FOUR

ANALYSIS OF RESULTS

4.0 Introduction

The purpose of this study was to propose a model that seeks to enhance the security of password authentication by adding another layer of security using typing pattern. The previous chapter

discussed the systematic approach and the methodology that were adopted by the researchers to achieve the objectives set. This section of the study focuses on the results analysis of the study.

4.1 Legitimate User Authentication

As it has been explained, False Rejection Rate defines the number of legitimate users that are denied access (Patil & Renke, 2016). The third stage of the experiment phase was conducted to measure the false rejection rate. Users after creating their accounts using a typing pattern for the password, had maximum of three attempts to log in into their accounts. The results indicated that all twenty (20) participants representing 100% were able to log in within the given three attempts. No participant was rejected or was unable to log in. The number of participants that were able to log in against those who were unable is illustrated in figure 4.1.

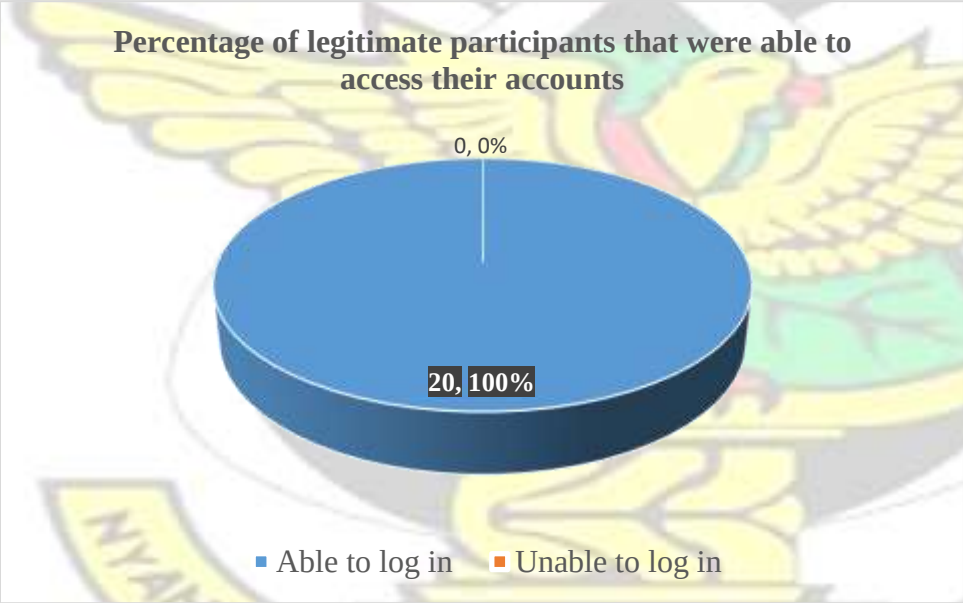


Figure 4.1: *Chart depicting percentages of participants that were able to access their accounts.*

Out of the 20 participants, 16 of them representing 80% were able to log in at the first attempt, 4 of the participants representing 20% logged in at the second attempt. This is illustrated in figure 4.2.

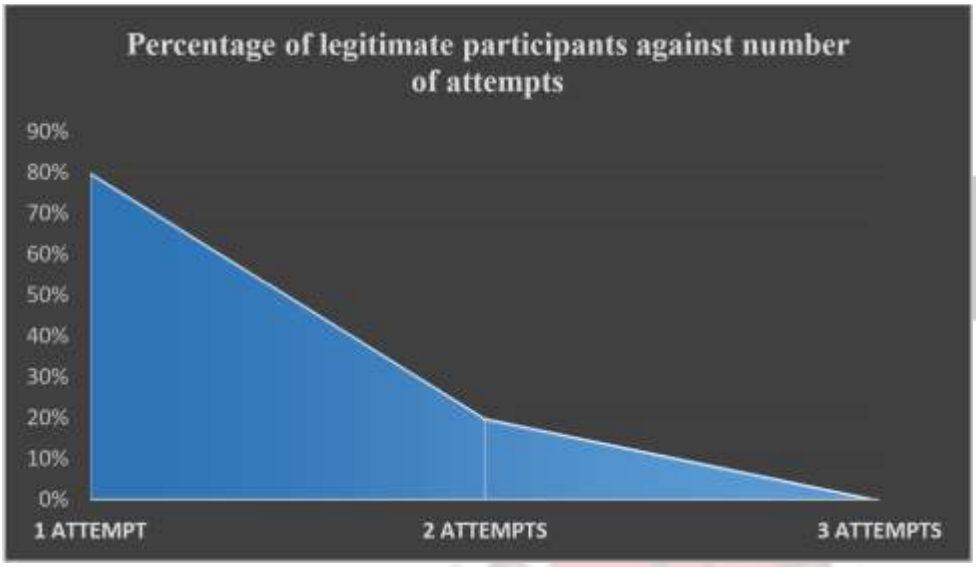


Figure 4.2: *A chart showing percentage of legitimate participants and the number of attempts made.*

4.2 Imposter User Authentication

The objective of the fourth stage of the experimental phase was to determine the number of imposters that will be verified as legitimate users after being given the usernames and passwords of legitimate users. This is known as false acceptance rate. The participants after being grouped into two, were given usernames and passwords of legitimate users to attempt to log in. The results of the fourth stage of the experiment indicated that two (2) of the accounts created by the participants representing 10% were logged in by imposters and eighteen (18) of the accounts representing 90% could not be accessed by imposters. This is shown in figure 4.3.

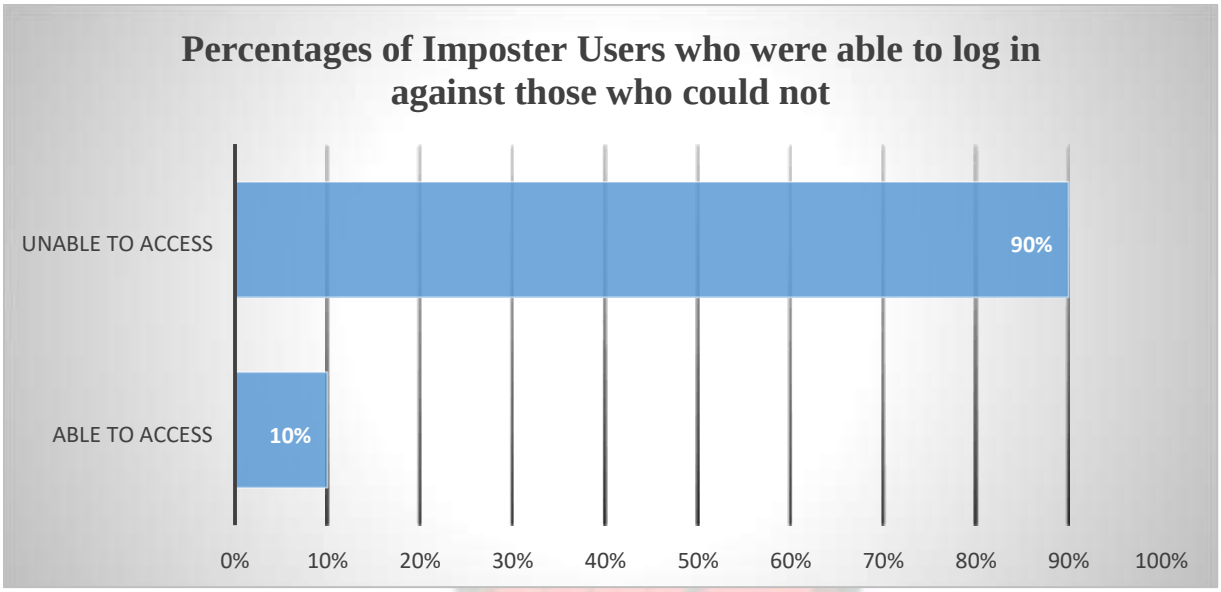


Figure 4.3: *A chart illustrating the percentage of imposters that were authenticated against those that were not.*

The 10% of the accounts that were illegitimately accessed, the imposters were able to succeed at the third attempt. This is illustrated in figure 4.4.

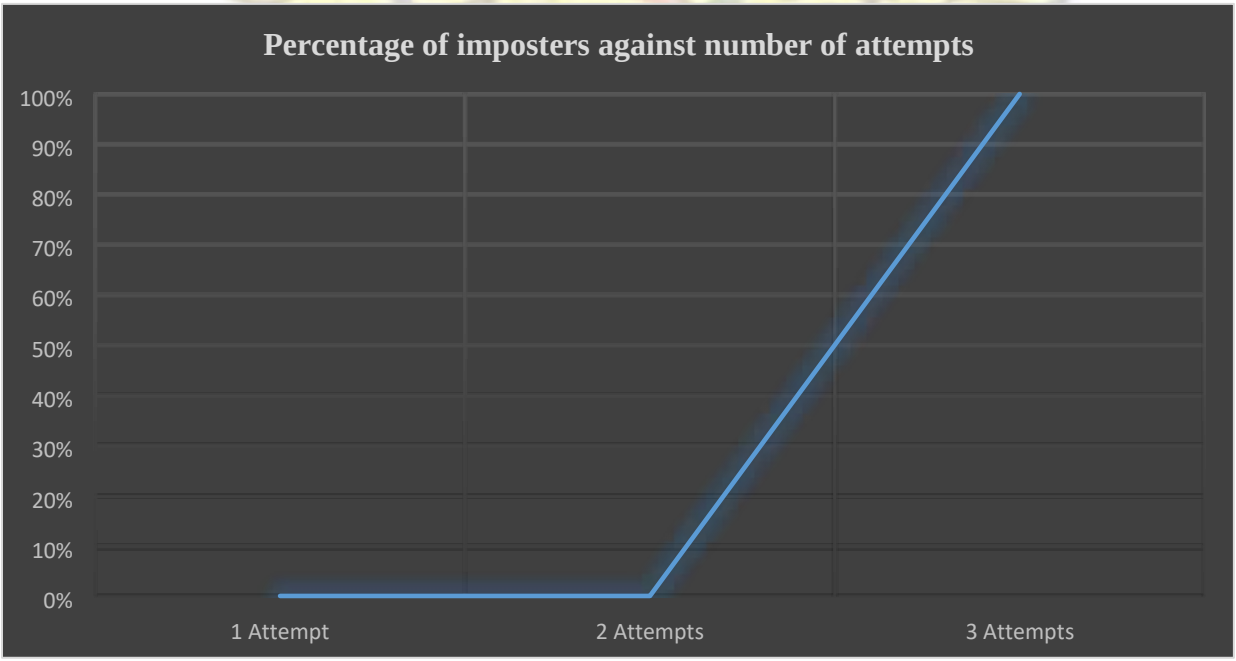


Figure 4 4: *A chart illustrating the percentages of imposters and the number of attempts made.*

4.3 Shoulder Surfing Imposter Authentication

After some participants posing as imposters to access accounts created by other participants, another set was made to observe another group as they type their username and password. The objective of this was to determine the resistance of this scheme to shoulder surfing attacks. Literature revealed that most schemes are vulnerable to shoulder surfing attacks. To therefore determine how secure the proposed scheme is, it needed to be evaluated to see how secure it is against shoulder surfing attacks.

Participants were put into two groups again. Whiles one group entered their usernames and passwords the other group observed them type. After the observation they were made to access those accounts they observed. The results indicated that 15% of the total participants posing as shoulder surfing imposters were able log in into other users' accounts after observing them and 85% even after observing the legitimate users, couldn't access their accounts. This is illustrated in figure 4.5.

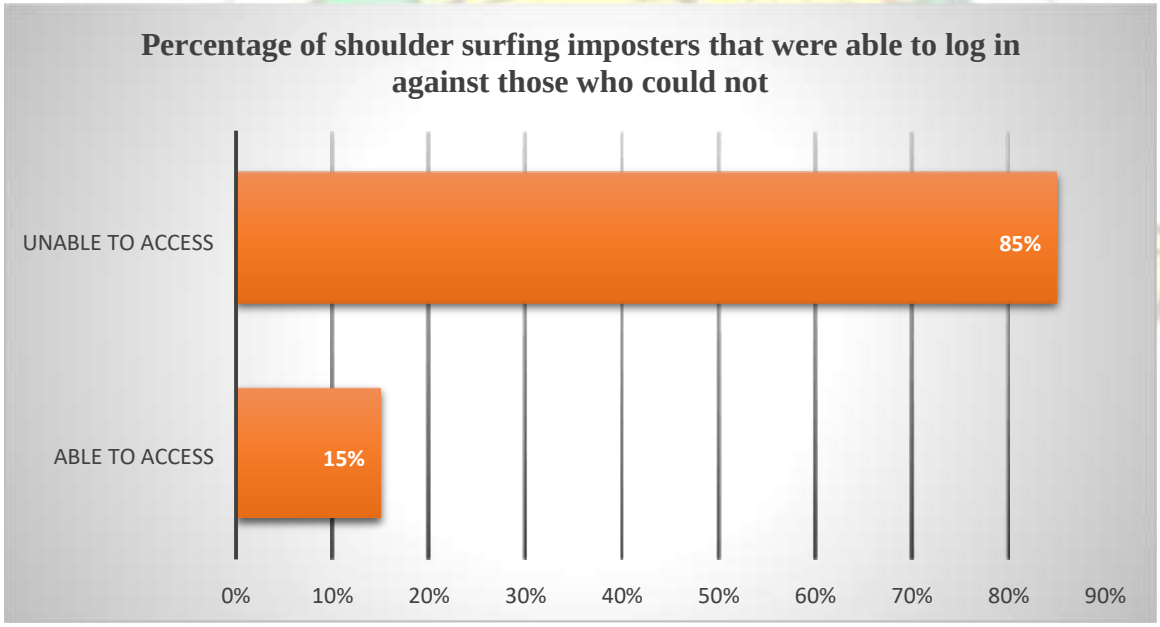


Figure 4.5: *A chart showing the percentage of shoulder surfing imposters that were successful against those that were not.*

Five percent 5% of the shoulder surfing imposters were successful at the first attempt, 5% was also successful at the second attempt and another 5% at the third attempt. This is demonstrated in figure 4.6.

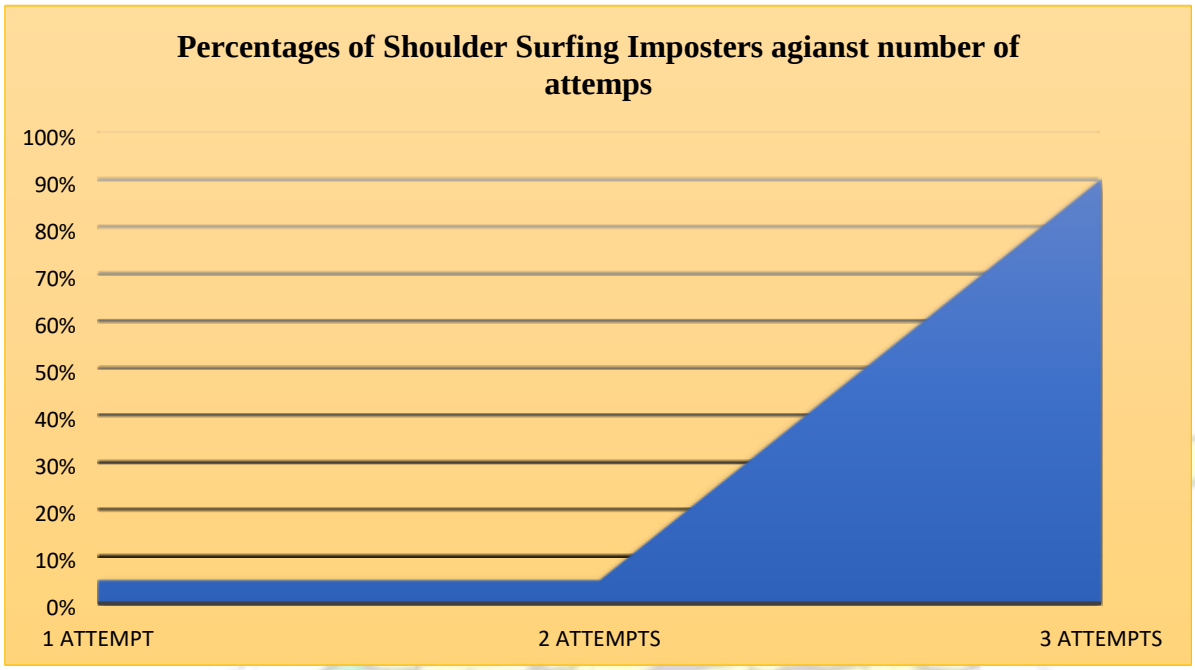


Figure 4.6: *A chart indicating percentages of shoulder surfing imposters against the number of attempts made.*

4.4 FRR of Legitimate Users after Two Weeks

To determine how convenient the proposed scheme is, participants were called again after two weeks. Legitimate users were made to log in into their accounts again. The results indicated 75% of the legitimate users were able to log in after two weeks and 25% could not log in. This is compared with the first results and illustrated in figure 4.7.

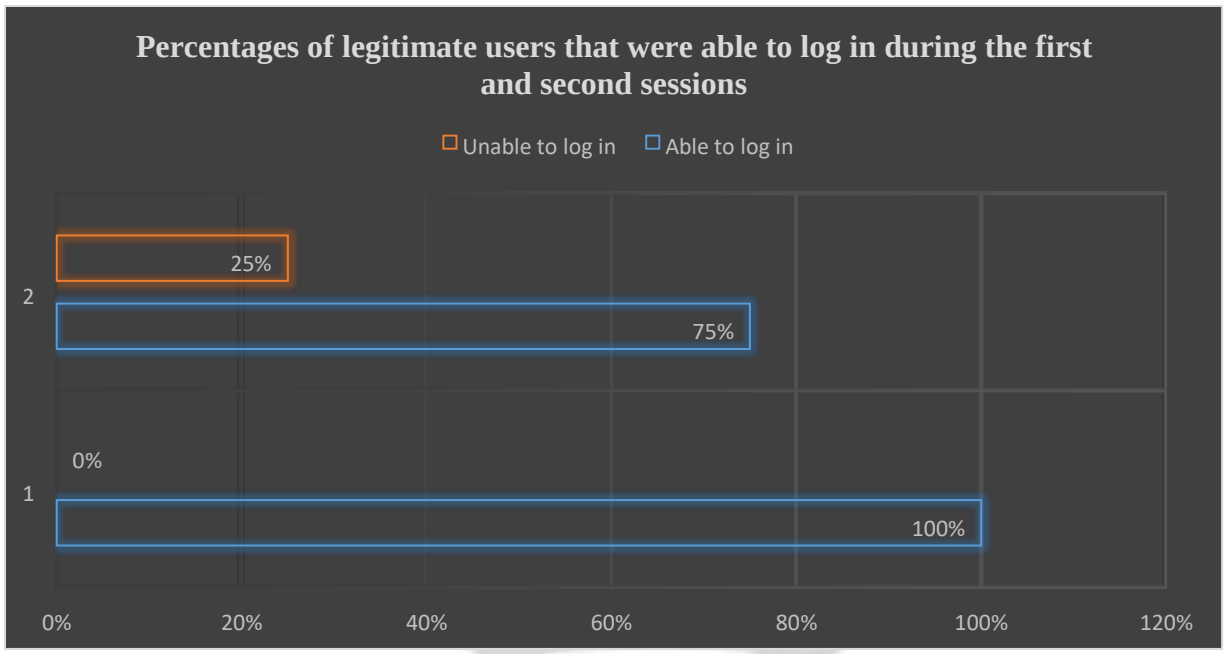


Figure 4.7: *A chart showing percentages of legitimate users that were able to log in during the first and second sessions.*

The number of attempts made in the second session has again been compared with the first session in figure 4.8.

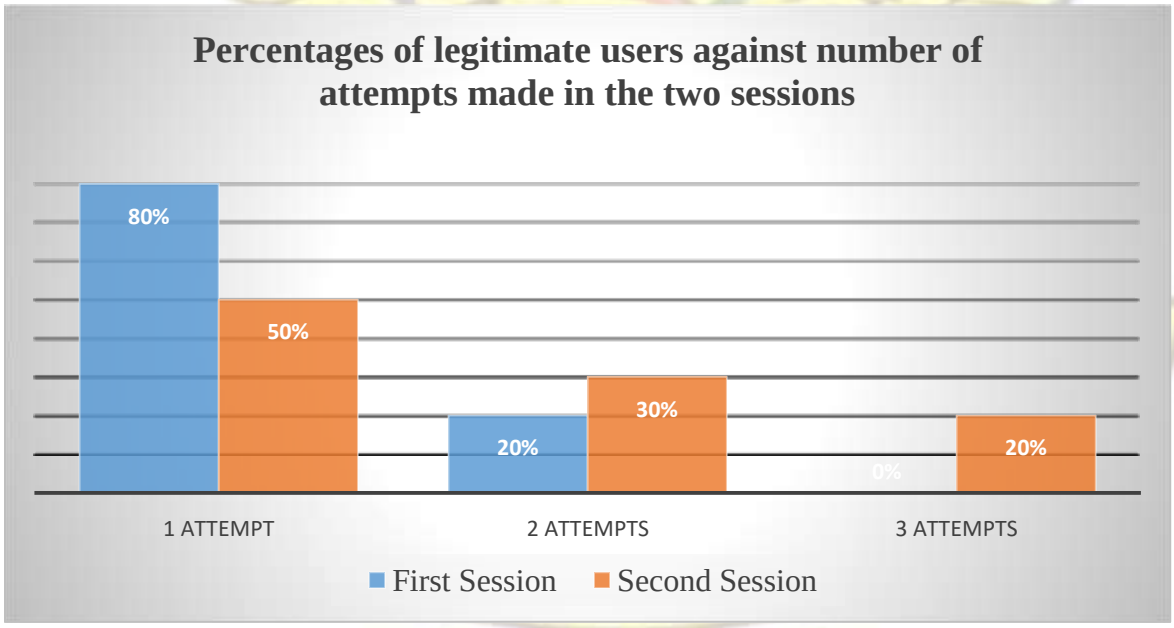


Figure 4.8: *A chart showing percentages of legitimate users against number of attempts made in both sessions.*

4.5 Imposter User Authentication after Two Weeks

The results revealed that no imposter was able to log into any of the legitimate accounts. This is illustrated in figure 4.9 and the number of attempts made is illustrated in figure 4.10.

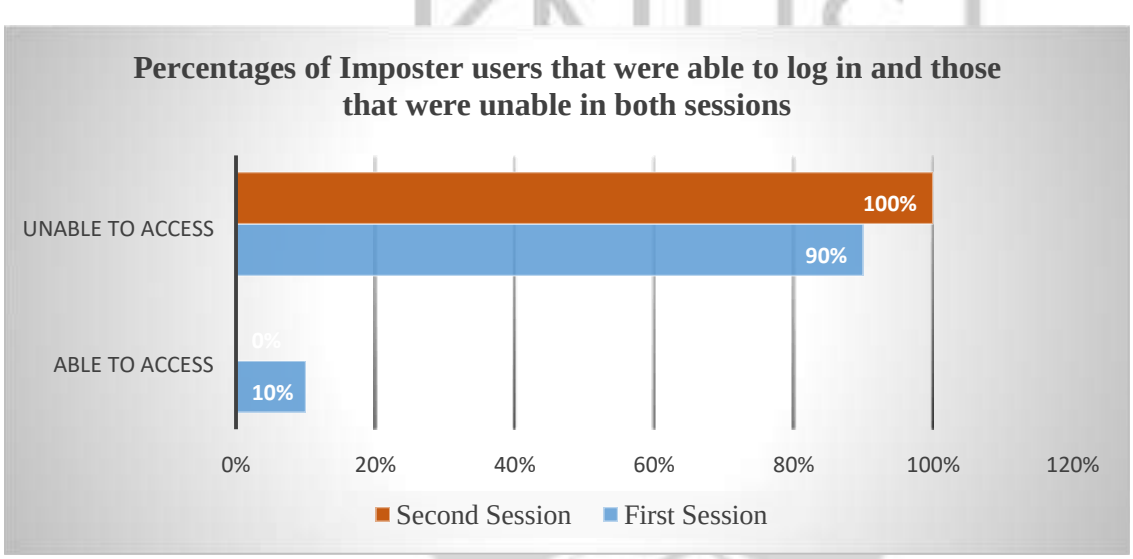


Figure 4.9: *A chart illustrating percentages of imposter users that were able to log in and those who could not log in during both sessions.*

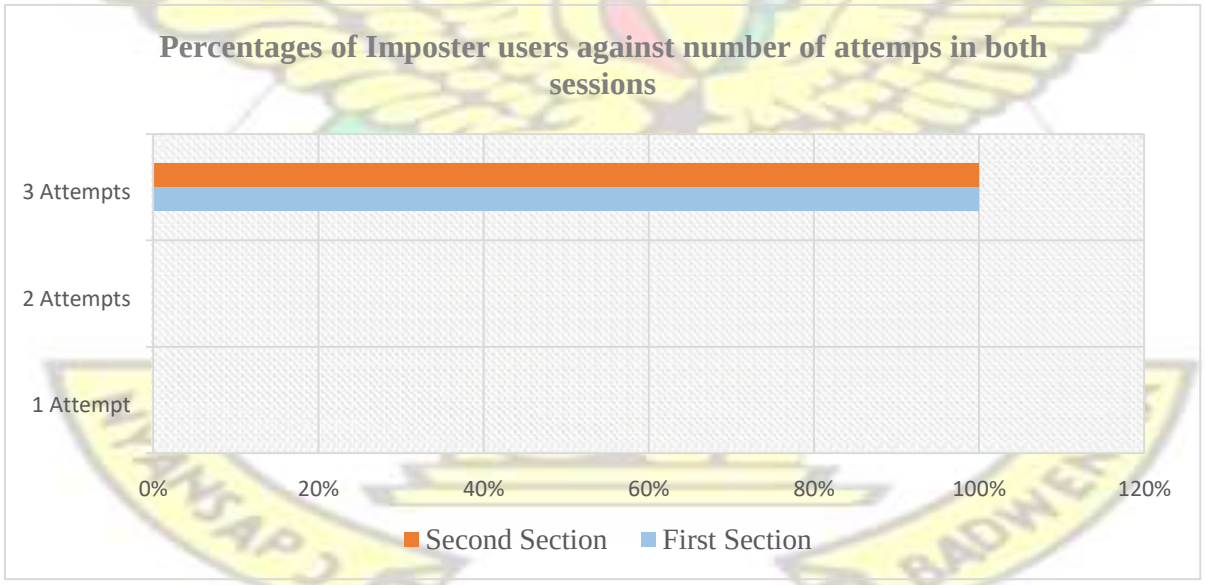


Figure 4.10: *A chart showing percentages of imposter users against number of attempts made in both sessions.*

4.6 Shoulder Surfing Imposter User Authentication after Two Weeks

Those who posed as shoulder surfing imposters were ones again given the usernames and passwords to try again. The results indicated that 100% of the participants could not log in again after the two weeks. This is illustrated in figure 4.11.

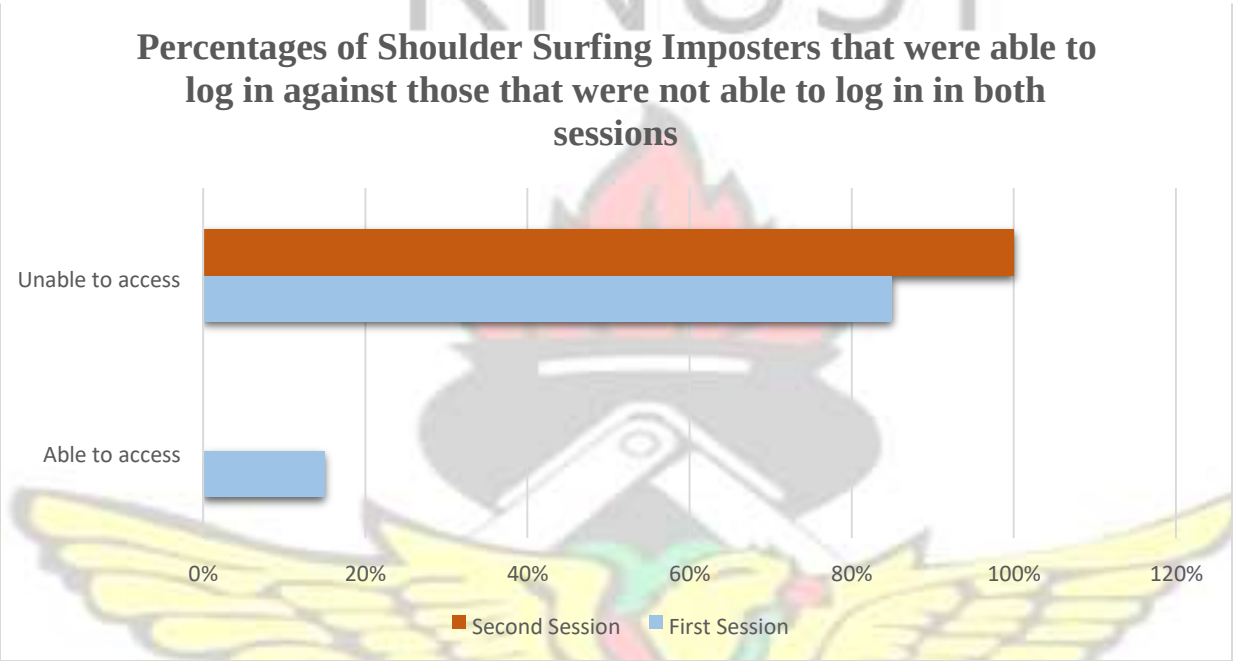


Figure 4.11: *A chart showing percentages of shoulder surfing imposters who were able to log in and those that could not in both sessions.*

Since no shoulder surfing imposter was able to log in after the two weeks, it means all the three attempts were exhausted by the participants. Again this is compared in figure 4.12.

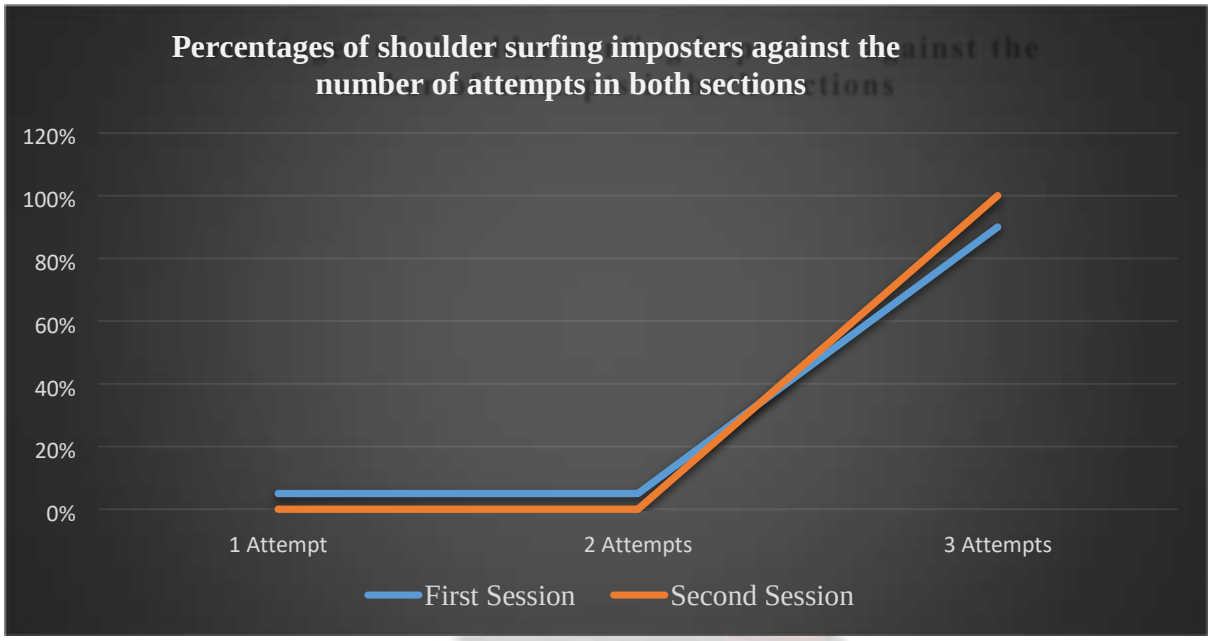


Figure 4.12: *A chart indicating percentages of shoulder surfing imposters against the number of attempts made in both sessions.*

The false rejection rates and the false acceptance rates of both sessions are shown in table 4.1.

Table 4.1: *FRR and FAR of both sessions*

Session	FRR	FAR
First Session	0%	10%
Second Session	25%	0%

CHAPTER FIVE

DISCUSSION, CONCLUSTION AND RECOMMENDATION

5.0 Discussion of Results

The purpose of this study was to propose an enhanced model for securing password authentication using typing pattern. To determine whether an authentication scheme is very secure and convenient, the false rejection rate and the false acceptance rate must be at the barest minimum (Patil & Renke, 2016). Therefore, the experiments conducted were to enable the researchers measure the false rejection rate and the false acceptance rate of the proposed scheme.

100% of the participants were able to log in into their accounts during the first session. This means that during the first session, the false rejection rate (FRR) was 0%. No legitimate user was rejected by the system or was unable to log in using the typing pattern. 80% of the legitimate users were successful at the first attempt and 20% at the second attempt. This means that no legitimate user tried even three times before getting access. During the second session (after two weeks), 75% of the legitimate users were able to log in successfully whiles 25% exhausted all their three attempts. The first session produced an FRR of 0% whiles the second session produced FRR of 25%, this is because first, the number of participants used are relatively small. Again, during the first session, the patterns adopted by the users were fresh in the memories of the participants so it was easier for them to recall. However, after the two weeks since they failed to practice the pattern, some failed to recall the actual patterns. This is one challenge of this study, if users fail to rehearse the rhythms constantly until it becomes part of them, they might forget the rhythm. Normal keystrokes dynamics will have a strength over the proposed scheme in this light since that scheme only uses the user's typing style and does not need to recall any rhythm.

95% percent of the imposter users could not log in and 5% was able to guess the pattern of a legitimate user. This makes the false acceptance rate (FAR) 5%. Since this scheme is a new approach, participants were not very acquainted with the picking of the pattern or rhythm. Hence, were virtually typing the password using their normal typing style. This makes it easy for an attacker to easily guess the pattern. This is a challenge of keystrokes dynamics that uses the normal typing styles of users, most users are likely to have similar typing style and speed and therefore can guess the typing style of another. A very good rhythm will make it very cumbersome for an attacker to guess. The single account that was compromised was successful at the third attempt. However, during the second session, the FAR was 0% since no imposter could log into the same accounts they tried in the first session. This proves how secure the scheme is against imposters who chance on people's usernames and passwords.

Most of the schemes reviewed are susceptible to shoulder surfing attacks. The proposed scheme was also tested against shoulder surfing attacks and the results indicated 85% of the shoulder surfing imposters after observing could not still access the accounts and 15% were able to access the accounts after observing the legitimate users type. Most of the participants though are familiar with user authentication since all of them have either Facebook or Email accounts, were not good with keyboarding. Most of them will use few fingers to type everything and that made it easy for the shoulder surfing imposters to observe them and caught the pattern. Patterns cannot easily be written down unlike passwords, if the pattern is not yours and you have not rehearsed it well you are bound to forget easily. None of the shoulder surfing imposters were able to log in again after the two weeks.

The few number of attempts made by legitimate users and the lower FRR indicate that the system is convenient to use. No other devices are required, the user does not need to carry anything along

which she could also forget. The FAR produced by this scheme even though the size of the participants is small, demonstrates how secure the proposed scheme is.

5.1 Conclusion

Textual password is the most common technique for authenticating users amidst all the drawbacks surrounding it which includes social engineering, dictionary attacks, eves dropping etc. Other alternative methods such as graphical passwords and biometrics have their own disadvantages, either they are too expensive to implement or vulnerable to attacks like shoulder surfing (Sreelatha et al., 2011).

This study proposed a scheme that adds another layer of security to the textual password which does not call for any extra device. The implementation of the proposed scheme is cost effective. As the proposed scheme prototype implementation demonstrates, this proposed method is viable in practice. The false acceptance rate produced in the study demonstrates that even if the username and password of a legitimate user is obtained by an attacker through social engineering, or other means, the attacker has a very little chance of breaking into the system. Therefore more secure than ordinary textual password. The proposed technique is easier to use irrespective of your level of expertise in computing. Legitimate users do not struggle to get authenticated.

A stronger password can to some extent make the system secure but the main problem has to do with the remembrance of those passwords (Sreelatha et al., 2011). Using the multiplicative rule, if a user decides to use all letters for her password, an attacker will have to do 308,915,776 combinations or attempts before she can guess it right (Carstens et al., 2004). The proposed scheme allows only three attempts that leaves an attacker 102,971,925.33 guesses. Of course it will be a herculean task for a human being to guess but not for computers especially in this age that the processing power of computers keeps doubling. However, even if the computer is able to guess

the password, it will be very difficult for the computer to guess the pattern that was used to type the password. With this scheme, users therefore do not have to pick a very complex password that they might forget or will need to write somewhere but rather get a good pattern that will be difficult to guess. It will be easier to remember the rhythms than the raw text. Though this system provides a lot of security, to some extent it is still vulnerable to shoulder surfing in a situation where the user does not know how to type and has to press the key with a single finger.

5.2 Recommendations

The researcher after the analysis of the results came out with the following recommendations for stakeholders in data security. Data security is an area of great concern for most organisations that work with information technology. Organisations that wish to enhance their data security especially in the area of user authentication without extra cost can implement the proposed scheme.

For system administrators that will want to implement the proposed scheme, the researchers recommend that:

i. Users of the system must be educated to pick a very good pattern that will be difficult to guess by an attacker. The accounts that were broken into in this study revealed that the legitimate users did not really pick a good pattern.

ii. Users rehearse their chosen patterns constantly; at least twice a day for a number of days. The legitimate users who could not access their accounts revealed that they did not practice the pattern again after the first attempt.

iii. Users must be made aware that as they type the credentials to be authenticated, other people could observe them and steal their credentials. Therefore, they should as much as possible

avoid using public systems to access their accounts. Also, as they type the credentials they should be mindful of their environment, bystanders, onlookers and cameras around. iv. Inasmuch as an attacker will struggle to break into their accounts if this proposed scheme is employed, they should avoid writing their passwords. The purpose of this study is to enhance the security therefore no room should be given to compromise the security.

v. As this study has revealed, the number of attempts for accessing an account must be limited. This is to prevent imposters from trying to guess the rhythm of a legitimate user.

This study focused on an aspect of data security which is authentication. Organisations that wish to implement this scheme should combine it with hashing and salting to make it more difficult for an attacker.

5.3 Future Research

Data security is an essential and critical concept and area of worry for most organisations. As such a lot of studies have gone into it and are still going on. Password systems cannot be ruled out; it is an important concept as far as data security is concerned. Though there have been studies on other authentication methods, password still remains the commonest. This study sought to enhance the security of textual password systems but it was not exhaustive, there are still more work that can be done in this area. Increasing the number of participants will make the results of the study more reliable.

Again, in future studies, this model will be tested against brute force attacks. This model is proposed to enhance the security of password authentication and also to make it more convenient for the users. The more password protected accounts a user has, the more likely she is to forget most of the passwords (Carstens et al., 2004). What impact will managing several accounts based on this model have on the model, how convenient will this model be in a situation where the user

has to manage several accounts based on this scheme? These are questions that will be addressed in future studies. This scheme made use of latencies between keystrokes features, the other features such as dwell time, pressure on the keys among other features will be exploited in future research.

REFERENCES

Ao, S. I., & International Association of Engineers (Eds.). (2014). *Cryptography Based Authentication Methods*. Hong Kong: IAENG, International Association of Engineers.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of U-and e-Service, Science and Technology*, *2*(3), 13–28.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM*, *58*(7), 78–87.

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security.

Check Point 2013 Security Report. (2013). Retrieved December 8, 2016, from http://www.checkpoint.com/campaigns/security-report/indexc. html

Data breach statistics. (2017, September 21). Retrieved October 23, 2017, from https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-firsthalf-of-2017/

Dhamija, R., & Perrig, A. (2000). Deja Vu-A User Study: Using Images for Authentication. In *USENIX Security Symposium* (Vol. 9, pp. 4–4).

DiGiacomo, J. (2017, October 18). Hacking Statistics for 2015 and 2016: How Bad Will 2017 Be? Retrieved October 23, 2017, from https://revisionlegal.com/data-breach/2017security-breaches/

ENISA. (2012, July 30). Password security: a joint effort between end-users and service providers. Retrieved October 23, 2017, from http://www.enisa.europa.eu/media/pressreleases/ Flash NotePasswords.pdf

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44–55). ACM.

Guljari, E., Lokhande, S., Mande, S., Reddy, L., & Maheswari, M. K. U. (n.d.). Authentication of users by Typing Pattern: A Review.

IBM Cost of Data Breach Study - United States. (2017, July 28). Retrieved October 25, 2017, from https://www.ibm.com/security/data-breach/index.html

IBM X-Force Threat Intelligence Index. (2017, March). Retrieved from https://public.dhe.ibm.com

Itrc Data Breach Reports. (2015, December 29). Retrieved October 23, 2017, from http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

Kuo, C., Romanosky, S., & Cranor, L. F. (2006). Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security* (pp. 67–78). ACM.

Monrose, F., Reiter, M. K., & Wetzel, S. (2002). Password hardening based on keystroke dynamics. *International Journal of Information Security*, *1*(2), 69–83.

NIST. (2016, May 9). Cryptographic Hash and SHA-3 Standard Development. Retrieved December 22, 2016, from http://csrc.nist.gov/groups/ST/hash/

Patil, R. A., & Renke, A. L. (2016). Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm. *International Journal of Computer Applications*, *144*(9).

Silveira, V. (2012a, May 7). An Update on Linkedln Member Passwords Compromised. Retrieved March 2, 2017, from http://blog.linkedin.com/2012/06/06/linkedinmember-passwords-compromised/

Silveira, V. (2012b, May 8). Taking Steps to Protect Our Members. Retrieved March 2, 2017, from http://blog.linkedin.com/2012/06/07/taking-steps-to-protect-ourmembers/

Silver, D., Jana, S., Boneh, D., Chen, E. Y., & Jackson, C. (2014). Password Managers: Attacks and Defenses. In *USENIX Security Symposium* (pp. 449–464).

Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M. S., & Manoj Kumar, V. (2011). Authentication Schemes for Session Passwords Using Color and Images. *International Journal of Network Security & Its Applications*, *3*(3), 111–119. https://doi.org/10.5121/ijnsa.2011.3308

Verizon Data Breach Investigations Report. (2017). Retrieved October 23, 2017, from https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf

What is a Brute Force Attack? - Definition from Techopedia. (n.d.). Retrieved October 24, 2017, from https://www.techopedia.com/definition/18091/brute-force-attack

What is Data Security? - Definition from Techopedia. (n.d.). Retrieved October 22, 2017, from https://www.techopedia.com/definition/26464/data-security

What is Keylogger? Webopedia Definition. (n.d.). Retrieved October 24, 2017, from https://www.webopedia.com/TERM/K/keylogger.html