GRAPHICAL BASED AUTHENTICATION MODEL FOR AN ELECTRONIC PAYMENT (E-PAYMENT) SYSTEMS

BY

SANI, Suleman Isah Atsu

MTech/SICT/2018/8454

DEPARTMENT OF COMPUTER SCIENCE

FEDERAL UNIVERSITY OF TECHNOLOGY

MINNA

AUGUST, 2021

GRAPHICAL BASED AUTHENTICATION MODEL FOR AN ELECTRONIC PAYMENT (E-PAYMENT) SYSTEMS

BY

SANI, Suleman Isah Atsu

MTech/SICT/2018/8454

A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGERIA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF TECHNOLOGY (M.Tech) IN COMPUTER SCIENCE

AUGUST, 2021

ABSTRACT

Client authentication is an essential component in nearly all electronic payment systems. This provides foundation for client the legal access control and user liability. The most foremost used authentication technique is the textual or traditional alphanumeric password. However, this method suffers several setbacks that include password guessing, slow login, duration time of execution and hard to remember the password. To provide an easy, friendly user interface and more secure authentication technique, knowledge-based graphical password authentication is employed in this research work of graphical based authentication for an electronic payment system (model) which uses a click point image or set of images for authentication. In this research, the similarity measure is found as an important task for document retrieval, text matching and retrieval of images from the database that is similar to query image. In order to achieve an optimal performance of the system and make it robust in the face of many challenges, an experiment was conducted during the login session using different algorithms that include Euclidean distance, Cosine similarity, City block distance (Manhattan) and Jaccard distance. The registration and login time were utilized to test the reliability, efficiency and robustness of the graphical scheme. The performances of these algorithms were evaluated and compared using various metrics such as the duration of login (execution time), the login success rate and the matching error (image matching point). The city block distance showed the best results and with an outstanding performance of execution time of 0.0318 milliseconds with matching error of 1.55231 and an acceptable login success rate of 64% compared to Euclidean distance with execution time of 0.0482 milliseconds, matching error of 1.55233 and login success rate of 92%. Many authentication-based applications including electronic payment systems find the use of graphical password to be robust especially with regard to security and ease of use. Hence, in this research work, a comprehensive research studies are carried out on existing graphical authentication password techniques with keen emphases on their suitability for electronic payment systems. This study has shown that graphical based password technique would be the most reliable authentication technique for e-payment systems.

TABLE OF CONTENTS

		PAGE
Cover Page		
Title Page		ii
Declaration		iii
Certification		iv
Acknowledgement		v
Abstract		vi
Table of Contents		vii
List of Tables		xii
List of Figures		xiii
Abbreviations		xvi
CHAPTER ONE		
1.0	**INTRODUCTION**	1
1.1	Background to the Study	1
1.1.1	Introduction of graphical password Authentication	3
1.2	Statement of the Research Problem	5
1.3	Aim and Objectives	7
1.4	Scope of the Study	7
1.5	Significance of the Study	7

1.6 Organization and Structure of the Thesis 9

CHAPTER TWO

2.0 LITERATURE REVIEW 11

2.1 Electronic Payment System 11

2.1.1 Types of Electronic Payment Systems 15

2.2 Types of authentications 18

2.2.1 Password Authentication 18

2.2.1.1 Password Authentication Vulnerabilities 18

2.2.2 Smart Card Authentication 19

2.2.2.1 Vulnerabilities with Smart-Card Authentication 19

2.2.3 Knowledge-based Authentication 19

2.2.4 Biometric Authentication 20

2.2.4.1 Vulnerabilities with Biometric Authentication 21

2.2.5 Digital Certificate Authentication 22

2.2.5.1 Vulnerabilities with Digital Certificate Authentication 22

2.2.6 Types of Attacks on passwords 22

2.2.7 Merits and Demerits of Electronic Payment Systems 24

2.2.7.1 Merits of Electronic Payment Systems 24

2.2.7.2 Demerits of Electronic Payment Systems 25

2.3 Graphical Password Authentication Schemes (GPAS) 26

2.3.1 Categories of Graphical Password Authentication Techniques 27

2.3.2 Recognition Graphical User Authentication Schemes 28

2.3.3 Recall based Graphical User Authentication Algorithms 32

2.3.4 Cued Recall Based Algorithms 37

2.3.4.1 Cued Click Points (CCP) 37

2.3.4.2 Persuasive Cued Click-Points (PCCP) scheme 37

2.4 The Main Factors in Graphical Password Authentication Techniques 38

2.4.1 Usability 38

2.4.2 Password Space 38

2.4.3 Password Entropy 39

2.4.4 Hotspot 39

2.4.5 Security 40

2.5 Related Studies 40

2.6 Summary of Review 44

2.7 Performance Metrics 45

2.7.1 Distance Metrics Overview 46

2.7.2 Cosine Distance and Cosine Similarity 46

CHAPTER THREE

3.0 PRESEARCH METHODOLOGY 47

3.1 Research Design Framework 47

3.1.1 Registration Interface 48

3.1.2 Login Interface 48

3.1.3 Verification and Validation 49

3.1.4 Authentication Interface 49

3.1.5 The Equation for the E-Payment Model 50

3.2 Proposed Graphical Authentication Model 52

3.3 The Requirements for the Authentication Model 53

3.3.1 Data Collection method 55

3.4 Performance Evaluation 55

3.4.1 Login Success Rate 55

3.4.2 Execution Time for the Algorithms 56

3.4.3 Matching Errors for the Algorithms 56

3.5 Similarity Measure 58

3.5.1 Euclidean Distance algorithm 68

3.5.2 Cosine Similarity 59

3.5.3 City Block Distance (Manhattan) 60

3.5.4 Jaccard Distance Algorithm 61

CHAPTER FOUR

4.0 IMPLEMENTATION, RESULT AND DISCUSSION 63

4.1 The System Implementation 63

4.1.1 Home Page 63

4.1.2 Registration Phase 64

4.1.3 Image Graphical Password Creation 65

4.1.4 Login Phase. 67

4.1.5 Electronic Payment Interface (Page) 70

4.1.6 Implementation of the Database (Server) 71

4.2 Experimental Results 72

4.3 Login Success Rate 72

4.4 Execution Time 75

4.5 Matching Errors for the Algorithms 78

4.6 Discussion of Results 80

CHAPTER FIVE

5.0 SUMMARY, CONCLUSION AND RECOMMENDATION 83

5.1 Summary 83

5.2 Conclusion 85

5.3 Contribution to knowledge 86

5.4 Recommendation 87

REFERENCES **88**

APPENDIX **95**

LIST OF TABLES

Tables		Pages
4.1	Login Success rate	73
4.2	Average Login Success rate in percentage	74
4.3	Execution Time for the algorithms	76
4.4	Average Matching Error of the images clicking point per user login	79
4.5	Comparison of Results for the Evaluation Performance of the algorithms	82

LIST OF FIGURES

Figures		Pages
2.1	Credit Card Payment Flow and Settlement/Funding	17
2.2	Categorization of graphical password authentication techniques	27
2.3	A Sample of Awase-E algorithm	29
2.4	A Sample of Passfaces algorithm	29
2.5	A Sample of Déjà vu algorithm	30
2.6	A Sample of Picture Password	31
2.7	Sample of Colour Login algorithm	31
2.8	Sample of Jensen et al Technique	32
2.9	A Sample of Blonder algorithm	33
2.10	A Sample of PassPoints	33
2.11	A Sample of Draw a Secret	34
2.12	A Sample of Passdoodle	35
2.13	A Sample of Syukri algorithm	35
2.14	A Sample of Qualitative DAS	36
2.15	Samples of PassMap	36
2.16	Sample of Cued Click Points	37
2.17	Sample of Persuasive Cued Click-Point	38
3.1	Block diagram for the Proposed Graphical Based Authentication Model	47

3.2	Drop down menu of the various algorithms used during the login sessions	58
4.1	Home page of the Graphical Scheme	63
4.2	Registration Phase	64
4.3	A 3x3 grid images display	65
4.4	First image used to create graphical password	66
4.5	Second Image used to create graphical password	66
4.6	Third Image used to create graphical password	66
4.7	Login Phase (Interface)	67
4.8	A 3x3 Graphical Grid Image Display during the login phase	68
4.9	First Image used to Login into account in with Euclidean algorithm	69
4.10	Image used to Login into account with Cosine similarity algorithms	69
4.11	Second image used to Login into account	69
4.12	Third image used to Login into account	70
4.13	Electronic payment interface	70
4.14	E-payment phase and various card types/payment procedures	71
4.15	Database implementation for login data, algorithms and matching errors	71
4.16	Database implementation showing user’s registered and login coordinates	72
4.17	Bar Chart of the login success rate	73
4.18	The average login success rate in percentage for all the algorithms	74
4.19	The pie chart for Login Success Rate in percentage	75

4.20 Bar Chart of the Execution time for the different users on each algorithm 76

4.21 Bar chart of the average execution time obtained for the algorithms 77

4.22 Pie Chart of the execution time for the algorithms 77

4.23 Matching error of each algorithm during users' interaction with the system 79

4.24 Average Matching error for each algorithm during users' interaction 80

ABBREVIATIONS

ATM: Automated Teller Machine

EP: Electronic Payment

EPS: Electronic Payment System

EC: Electronic Commerce

SRS: Software Requirements Specification

PHP: Personal Home Page /Hypertext Preprocessor

MySQL: My Structured Query Language

CSS: Cascading Style Sheets

HTML: Hypertext Markup Language

XAMPP: Cross-platform, Apache HTTP Server, MySQL, PHP and Perl

Apache: HTTP Server

PhpMyAdmin: MySQL, Database Administration tool

ECD: Euclidean Distance

CS: Cosine Similarity

CBD: City Block Distance

JD: Jaccard Distance

T: Transaction

TA: Type of Authentication

GBAM: Graphical Based Authentication Model

GPAS: Graphical Password Authentication Scheme

LSR: Login Success Rate

ET: Execution Time

ME: Matching Error

arccos: Inverse Cosine

CVV: Card Verification Value

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Study

With technological advancements, the electronic payment system has grown significantly. A shopping centre, an oil company, and the Western Union issued a customer card in 1914 to make it easier for consumers to pay for products and services. In addition, the banking industry issued credit cards (Fatonah, *et al.*, 2018). Initially, all credit card payments were made on paper, until the 1990s, when the card was completely converted into an electronic device (Joseph & Richard, 2015). In 1918, the evolution of electronic payments started when the Federal Reserve Bank exchanged currency via telegraph for the first time (Paytech & Series, 2017). Electronic payments, despite being designated in 1960, are now widely used due to the progression of e-commerce and scientific improvements. The research community worked tirelessly to develop various online payment models such as the Model Asokan N. and JW models (Pant, 2011).

The term "electronic payment" can refer to e-commerce, which is a method of buying and selling goods and services over the internet, or any type of electronic funds transfer. It is also known as electronic cash transfer for business to business (B2B), business to customer (B2C), person to person (P2P), and, more recently, administration to customer (A2C) transactions. A2C payments are used to pay taxes to the government (Joseph & Richard, 2015) and (Atema, 2014).

However, the concept of e-commerce does not stop with the purchase and sale of goods. It also encompasses the entire purchasing process, which includes developing, marketing, selling, delivering, servicing, and making purchases (Joseph & Richard, 2015) and (Pant, 2011).

Payment systems and protocols have evolved alongside the growth of e-commerce. Customers, merchants, and payment gateways currently comprise the payment system, with a merchant receiving a customer's payment information and forwarding it to a payment gateway to process the payment. However, this puts a customer's payment information at risk since a retailer may save the customer's payment information in either plain or encrypted form and then abuse it. It is also likely that a merchant's server, which transfers payment details from a customer to a payment gateway, has been hacked and the merchant is unaware of it (Pant, 2011).

Taking all of this into account, this study proposed a secure online payment system in which customers' payment information is secured without being compromised, even in encrypted/hashed form (Pant, 2011; Khan, 2017; Oney, *et al.*, 2017).

End-to-end processing and manual e-payment or manifesto commitment are the two types of e-payment systems used around the world. End-to-End processing involves all processes being completed electronically, from approvals to the beneficiary receiving value, whereas manual e-payment is a hybrid of manual and electronic processes used when the available infrastructure does not support End-to-End processing. Cards, internet mobile payments, financial services, biometric payments, and electronic payment networks are just a few examples of e-payments.

Some of the problems faced in an E-payment system includes Integrity (ensuring that transmitted financial information remains unchanged in transit), Confidentiality (ensuring that transactions are secure from potential eavesdroppers), Reliability (ensuring that there is a reduced chance of failure), and Non-reputation (ensuring that all parties have non-deniable proof of receipt), Authorization/Authentication (ensuring that users are recognized and given the rights and privileges that they desire).

Several works have been proposed in addressing the challenges with authentication in an electronic payment system. One of the methods is traditional. Only recently, other methods such as fingerprint-based biometrics were introduced. There are various methods of Authentication namely; Traditional based (Text) based, Biometrics based and Graphical authentication methods.

1.1.1 Introduction of Graphical Password Authentication

A username and textual-based passwords, also known as alphanumeric passwords, are the most commonly used techniques in knowledge-based authentication. Fernando Corbato was a computer scientist who pioneered password security in computer science and around the world in 1960. He is widely regarded as the "godfather of modern computer passwords". He came up with the concept while working at the Massachusetts Institute of Technology (Khan, 2015; Sun *et al.,* 2018; Akram *et al.,* 2017). Traditional authentication methods have found use in a variety of domains, including electronic payment systems. For example, one of the major drawbacks of the conventional approach is the difficulty in remembering passwords. According to research works, users prefer short passwords or passwords that are easy to recollect, like a nickname, first name, or a variety of names, consistent with research. As a result, these passwords have vulnerabilities and can be guessed or manipulated easily.

Khan *et al.,* (2019); Sun *et al.*, (2018); Akram *et al*., (2017); Mayuri *et al.,* (2013); and Hafiz, *et al.,* (2008) according to their reports, “In the tech world, a team of cybersecurity experts at a major corporation inspected a network password cracker and randomly cracked eighty percent (80%) of the passwords in less than half a minute.” Furthermore, passwords that are difficult for attackers to guess or break down are often difficult to recall.

Graphical passwords, as introduced by Ritu *et al.* (2015) and Osunade, *et al.* (2019) are an additional form of user authentication that uses an object/photo as the password rather than alphabets and figures (alphanumeric). On a computer screen, a picture is shown, and the user is instructed to click on a few particular areas of the image. The user will be authenticated if the appropriate area or regions are clicked. The idea is to increase password accessibility and protection by using the ability to remember picture images better than textual characters. The fact that graphical passwords are easier to recall than conventional alphanumeric passwords is one of their most significant advantages. Humans have memories and can recall places they have been, things they have seen in their surroundings, and they have known for a long time (Kadu & Therese, 2017). Knowledge-based graphical password schemes include recognition-based, cued recall-based, and pure recall-based graphical password schemes. Recall-based drawing involves recreating a previous image and sketching it out on a map using a mouse or stylus. While password recognition necessitates the memorization of an image during the password creation process, it also necessitates the recognition of picture images. Cued recall password schemes, on the other hand, usually have a collection of picture images that must be recollected and precisely aimed at a location on the image.

According to Ahsan & Li (2017), Blonder's graphical authentication password appears to be the only knowledge-based scheme option other than the alphanumeric password approach. There are currently a large number of graphical schemes available. A graphical password scheme, according to Akram *et al.* (2017) is an authentication method that allows the user to choose from a set of image files and display them in an interface. As a result, the graphical images used in the authentication technique are used as passwords. This is known as graphical authentication. Since humans can memorize picture images better than text, Razvi (2017) suggested an authentication algorithm as an alternative to

conventional authentication, which was adopted. As a result, graphical user authentication was seen as more user-friendly and reliable than conventional authentication. When opposed to conventional techniques, graphical authentication passwords are difficult to crack or penetrate using traditional attacks, which offer a higher degree of protection for graphical user authentication. Recall and recognition-based algorithms, according to Razvi (2017) are two classes of graphical algorithm techniques that are possible alternatives to conventional passwords. Users click the right image in a specific order from a group of images shown to them in recognition-based functions.

According to Masihuddin *et al.* (2017), data protection and knowledge are extremely valuable and significant in the field of information systems. Data protection is based on technology that protects data information from alteration or accidental changes to the actual text, non-authorization to monitor access, and on-demand accessibility to grant clients. All the security features mentioned above should be present in an electronic payment system. Clients should not trust any e-payment system that does not include a security feature. Furthermore, trust is critical in ensuring that the electronic payment system is accepted by the clients. A graphical-based authentication method is used to provide clients with a secure, perfect, and effective electronic payment system.

1.2 Statement of the Research Problem

In recent years, researchers have emerged with different algorithms as touching or clicking point graphical passwords authentication and different approaches have been implored on various platforms. Some of the researchers are aimed at developing graphical password schemes that would be suitable to the users/clients while making an electronic payment, and keeping security in check (Razvi, 2017).

Electronic payments despite their numerous benefits come with them are challenges world over, due to advancements in technology in use (khan *et al.*, 2017). The challenges faced in Traditional authentication (alphanumeric or textual) and fingerprint authentication in Electronic Payment Systems are prone to hacking or rather vulnerable to attack because they are easy to guess, hard to remember passwords and slow login. Hence this study, to overcome or address the challenges associated with traditional authentication (alphanumeric and text-based) and fingerprint authentication, a graphical-based authentication method is proposed. The graphical-based authentication method provides the user/clients of electronic payment systems with the choice to select a stronger password and memorable images, compared to less and vulnerable alphanumeric and fingerprint authentication. In the graphical authentication method, a user is provided with a user-friendly interface that has fast login access and fast execution time when compared with alphanumeric and fingerprint authentication while keeping security preserved (Razvi, 2017) and (Veerasekaran *et al.*, 2015).

This research work is inspired by the works of Razvi (2017) and Veerasekaran *et al.*, (2015). In the work of Veerasekaran *et al.* (2015), where few metrics such as login success rate and time of execution were used to evaluate the performance of a few algorithms that include Euclidean distance, Vertical Eclipse, and Horizontal Eclipse. This, however, does not provide enough metrics to be able to evaluate the robustness of the efficiency of the algorithms. Hence, this research work includes other metrics such as the login success rate, execution time and matching error, to give a more robust and efficient evaluation of the algorithms. Akram *et al.* (2017) presented that the difficulties in remembering passwords are major disadvantages of the traditional method. These Passwords suffer drawbacks, and it is easily predicted or hacked. Akram *et al.* (2017) also

stated that the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques.

1.3 Aim and Objectives of the Study

This study is on the development of a Graphical Based Authentication (GBA) Model for Electronic Payment Systems (E-payment). This will be achieved by the following objectives:

(i) To develop a framework model for graphical-based authentication system (scheme).

(ii) To develop a mathematical model for the graphical-based authentication for the electronic payment (e-payment) system.

(iii) To evaluate the efficiency and performance of the graphical-based mathematical model designed in (ii) with other existing models.

1.4 Scope of the Study

This study focused on developing a Graphical Based Authentication Model for Electronic Payment System for clients/users of online transactions. The approach is focused on the Performance evaluation of the proposed graphical scheme using different distance measure algorithms to obtain exact image matching/clicking points and metrics such as execution time, login success rate and matching error to provide authentication mechanisms for better login, fast execution time with minimum error, usability and security for the system.

1.5 Significance of the Study

This study is focused on providing security, protection and the benefits of graphical-based authentication mechanisms for users:

(i) **Benefits of the Study:** This study focuses on providing reliable, proficient, and rapid transaction handling, as well as the secure transmission of information of electronic payment or online transactions between e-businesses such as purchasers, dealers, and banking institutions, as well as customer/client access control during the registration and authentication phases. E-commerce platforms can use graphical authentication. It also provides strict security measures for users and customer trust. Furthermore, a graphical authentication scheme provides a user-friendly password interface while also increasing security. The best performance on electronic payment systems is provided by graphical authentication passwords.

(ii) **Beneficiaries of the Study:** Clients/customers/users can benefit from graphical password authentication for electronic payment (scheme) systems in a variety of ways, including; It enables clients/customers to keep up with international payment mechanisms, such as conducting global level transactions in a fraction of a second. It gives clients rapid settlement and authorization with minimal fraud and security lapses. This study can be applied to E-commence platforms such as Konga and Jumia e-commerce platforms in Nigeria. Graphical password provides a user-friendly interface where the customer/clients are allowed to select their different images or components to create and enter textual and graphical passwords.

(iii) **Modes of Benefit by customers:** Customers gain access to their accounts through a simple login interface, enhanced password memorability, highly secure electronic transactions, and an easily accessible system that enables customers to make payment transactions directly from their homes. They are also able to complete transactions in a shorter amount of time. The customers are secured from

dictionary attacks, guessing attacks and brute force search as they are infeasible. Graphical Authentication passwords also provide data protection, ensuring that the privacy of customers/clients' and e-electronic platform's data information is protected against alteration or unintentional changes to the actual text, non-authorization to monitor access, and the ability to grant clients access on demand.

1.6 Organization and Structure of the Thesis

This thesis comprises the Preliminary pages and five Chapters covering from Chapters One to Chapter five:

Chapter One gives the introductory background to the research study including a concise introduction of graphical password authentication. It also consists of the Statement of the Research Problem, Aim and Objectives, Scope of the Study, and the Significance of the Study.

Chapter two gives the Literature Review of the previous related research works that were carried out by other researchers. It also discussed types of electronic payment and types of authentications, graphical schemes, The main factors in graphical password authentication techniques.

Chapter three discusses the Methodology utilized to address the problem. This justifies/validates the methodology utilized to getting the solution to the problem. It involves the method of data collection, capturing of different picture images as data used for graphical password creation, performance metrics and use of similarity distance measures.

Chapter four of this study presents the details of the experimental study conducted and the various results obtained, results from the discussion, compared and cross-validation with existing graphical methods.

Chapter five covers the summary of the research work, the conclusion on the result/findings were drawn, contributions to knowledge and the recommendations for further studies.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Electronic Payment System

An electronic payment system is a method of exchanging value (usually money) for goods, services, or information. There are numerous methods for paying for goods electronically, including credit cards, e-cash, e-cheques, and stored-value cards. The most common method of payment over the Internet is by credit card. Banks all over the world have invested in magnetic strip card technology to ensure that processing credit cards and cheques are done efficiently, securely, and quickly (Oney *et al.*, 2017; Lin & Nguyen, 2011; Ahmed *et al.*, 2019; Ryan *et al.*, 2016).

In 1990, the consumer and business worlds were exposed to a new way of doing business with the introduction of electronic commerce (e-commerce). Since then, e-commerce has evolved greatly, resulting in tremendous benefits for consumers and companies all over the world. With so many companies doing business this way, it is clear that e-commerce has a bright future ahead of it, and businesses will reap the most benefits. The online business model is responsible for the majority of e-popularity commerce's success. It enables the online purchase and sale of goods, as well as the provision of various services and information and the immediate exchange of money between transacting parties. Electronic payments are a type of business payment that involves exchanging money electronically through e-commerce (Oney *et al.*, 2017).

A thriving electronic commerce ecosystem has resulted from the widespread use and commercialization of the Internet. According to Durgun & Caner (2015) and Oney *et al.* (2017), Transparency, pace, privacy, and global accessibility are just a few of the benefits of electronic commerce (EC) over conventional commerce, all of which help to simplify

and improve users lives. These benefits contribute to EC's success and the productivity of companies that use it. EC has been described in a variety of ways due to its widespread use, but the best concept for this study is "the exchange of business knowledge, the maintenance of business relationships, and the completion of business transactions through telecommunication networks" (Oney *et al.*, 2017).

EC is focused on electronic payment systems (EPS), which are becoming increasingly important for both businesses and customers as the scale of electronic commerce increases. Oney *et al.* (2017) EPS are payment systems that enable organizations and individuals to conduct safe electronic commerce transactions. According to Oney *et al*. (2017) and Rouibah *et al*. (2016) EPS is one of the most significant determinants of performance for companies that operate electronically. As a result, since the advent of EC, EPS has received a great deal of attention from researchers and practitioners. Although EPS has increased significantly over the last decade.

One of the most significant factors stifling e-commerce growth has been identified as a lack of perceived protection and confidence (Ryan *et al.*, 2016). The majority of trust theories are based on interpersonal interactions and long-standing relationships (Adepoju & Alhassan, 2010). However, since e-commerce lacks these two essential components, it is difficult to build and maintain confidence in this scheme. This is why, before discussing the problem of consumer confidence and privacy, it is important to have a thorough understanding of EPS and to inspect technological protections designed to minimize the risk of e-commerce.

To begin with, electronic trading and EPS offer emerging countries the ability to boost their economic growth (Durgun & Caner, 2015) and (Okon, 2018). Second, customers in small economies are unable to profit from the economies of scale and favorable business

opportunities found in conventional marketplaces. As a result, e-commerce offers a way for EPS adoption to spread.

With the establishment of the European Central Bank, EPS grew into one of the most relevant and functional financial instruments for clients and businesses. Fintech companies, such as Stripe, have been able to meet the needs of EC users, such as e-payment, which is a required step in the completion of an electronic transaction. Electronic payment is the digital transmission of a value from an employer to an employee, according to Mushkudiani (2019) and Georgescu (*n.d.*) individuals may use e-payment systems to help them handle their finances more effectively. Electronic Payment System achieves two basic targets:

(i) Imitation of real-world payment frameworks.

(ii) the systematization of new payment processing methods.

According to Masihuddin *et al.* (2017), as the monetary exchange became more complicated and difficult, users abstractedly represented values, evolving from barter to certified notes of money, cheques, payment orders, debit and credit cards, and now electronic payment systems. Currency can be falsified, cheques can bounce, and signatures can be forged, to name a few well-known problems or vulnerabilities in conventional payment methods. In comparison, a well-designed electronic payment system can provide superior protection to traditional payment methods while still allowing for greater versatility in use. Among other things, the convenience of allowing money transactions, as well as more reliable and faster access to capital resources, has propelled the e-payment system ahead of the cash currency-based system. The former cash-based payment system is gradually being replaced by electronic payment systems as more transactions take place on the e-commerce site. As a result of this advancement

in the global business platform, most businesses have naturally moved away from traditional paper-based cash exchanges and toward an electronic payment system, also known as the e-payment system. These electronic systems can be viewed as a method of paying for goods or services that have been established online through the internet. According to Masihuddin *et al.* (2017), an Electronic Payment System is a type of inter-organizational information system (IOS) that connects a number of organizations and individuals for money-related transactions. It may be necessary to have complex interactions between partners, the environment, and technology.

The term "electronic payment system" refers to a wide variety of electronic multichannel services. It is used for a number of purposes, all of which feature the increased imprecision that e-payment is known for in the literature. Mobile banking, electronic cash, online banking, electronic broking, and electronic finance are examples of e-payment.

According to Alsaiari *et al.* (2014), online banking, also known as Internet banking, is a method of providing banking services to customers electronically. Accessing account information, transferring funds between accounts, and making electronic payments and settlements are all examples of online banking services. To reduce the risks associated with online banking while also increasing customer protection, trust, and acceptance of this electronic service channel, customers' online accounts must be safely secured by improving user authentication without compromising the users' experience.

Various types of common attacks against the finance industry included tampering, brute force, and spyware. Payment cards, passwords, and bank account details were the most common targets of such breaches. Using other user’s authorization access allows a user to gain unauthorized access in a simple and undetectable way (Alsaiari *et al.*, 2014).

According to Alsaiari *et al.* (2014), authentication-based attacks were responsible for roughly four out of every five breaches involving hacking (guessing, cracking, or reusing valid credentials). As a result of espionage-related breaches, authentication credentials theft presented a high value of the loss. When the idea of a suitable authentication replacement is widely accepted, approximately 80% of these attacks are forced to adapt.

Alsaiari *et al.* (2014) both service providers and customers are concerned about the critical importance of securing the wide range of banking services that are being deployed over the Internet. As a result, extreme caution is always exercised in protecting the e-banking system as well as customer information.

The first line of defense is to protect the authentication system from fraud and identity theft (Alsaiari *et al.*, 2014). According to Alsaiari *et al.* (2014) that currently, the traditional text-based password is the primary form of knowledge-based authentication and user authentication, and while there are many techniques for securing passwords, most are insufficient in the face of attackers' tools. The shortcomings of the textual password are well known, and they affect both usability and security. As a result, the need for alternative methods has arisen, and various alternative knowledge-based techniques, such as graphics-based passwords (recognizing graphical elements such as images, iconography, grid images) or associative/cognitive questions, have been proposed (Alsaiari *et al.*, 2014). Each approach has its own set of merits and demerits (Alsaiari *et al.*, 2014).

2.1.1 Types of Electronic Payment Systems

Electronic Payment Systems can be categorized into five main types. These are as follows:

Electronic cash is a form of payment that associates a unique identification number with a particular amount of money. For e-commerce, this method was created as a replacement for credit and debit cards. Physical banknotes and coins have digital counterparts known as an electronic currency. Individuals must purchase digital currency from the authorizing firm to use this system. Electronic telecommunication networks can be used to move the digital cash that has been bought. Digital currency can provide advantages such as buyer secrecy, worldwide credibility, and convenience in the case of so-called micropayments.

Pre-paid cards: A merchant provides client/users with a pre-paid card for a specific amount that client/users can use in-store or online. Pre-paid cards are often provided as "gift cards," allowing the recipient to choose from a range of goods or services up to the card's pre-loaded limit, but they are often used by individuals who pre-load the card for personal use. Most pre-paid cards are only valid for one transaction and expire after a certain amount of time if they are not used; however, some retailers have started to enable Customers are encouraged to use pre-paid cards that do not have an expiration date and for several transactions within a certain time frame. Prepaid cards are common among consumers because of their convenience and ease of use (Ahmed *et al.*, 2019).

Credit cards are plastic-like payment cards that allow users to make online purchases. Credit cards are the most widely used electronic payment method (Asaolu *et al.,* 2011). Credit cards are a user-friendly medium with a complex transaction process.

Debit cards (also known as credit cards or check cards) are plastic cards that allow users to withdraw money from their bank accounts without having to deal with a banker and pay for products and services online. Debit cards are issued by banks (both governmental and non-governmental) and financial service providers. Banks (both governmental and non - governmental) and other financial service providers issue debit cards. Unlike credit

cards, when an individual uses a debit card, the money is automatically withdrawn from his or her bank account. One of the most commonly used e-payment methods is the debit card (Lin & Nguyen, 2011).

Electronic cheques an electronic cheque is a form of digital payment that functions similarly to a paper cheque. The fact that an electronic audit debits or credits real funds electronically distinguishes it from a paper check. In comparison to the other e-payment options, the electronic check is the least common (Joseph & Richard, 2015).

Based on the information presented above, it is apparent that pre-paid, credit, and debit cards are the most commonly used electronic payment methods, with electronic cash serving as a backup. Electronic cash has been mostly used for small-value transactions while pre-paid, credit and debit cards have been employed for most types of transactions except small-value transactions. Prepaid, credit, and debit cards should not be used for small-value transactions because they can be prohibitively expensive when used for small amounts. Since no single e-payment system dominates the market, all of them can be considered alternatives.

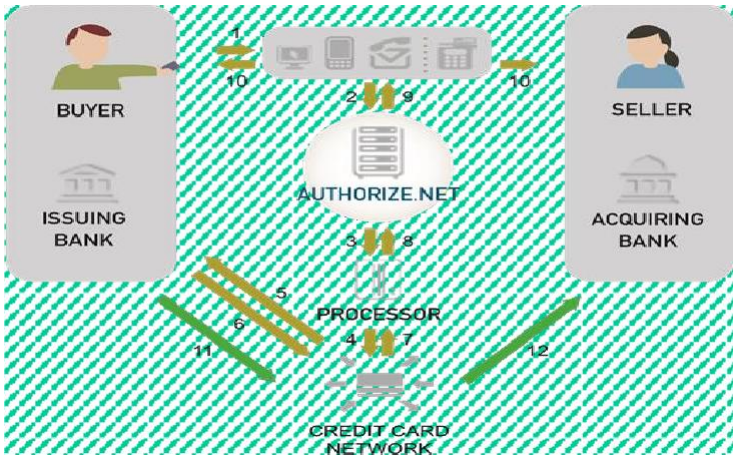


Figure 2.1: Credit Card Payment Flow and Settlement/Funding (Google, 2020b) and (Joseph & Richard, 2015)

Credit Card Payment Flow

Authorization (determining if payment information is legitimate and funds are available on the customer's credit card) and settlement (transferring funds into the merchant's account) are the two steps of the credit card payment process.

Authorization

Steps 1, 2, 3, …up to 10 in figure 2.1 represent the authorization phase. Authorize.Net routes the payment details to the credit card networks on behalf of the merchant then returns the results-approved or declined (Bezhovski, 2016) and (Google, 2020b).

Settlement/Funding

Steps 11 to 12 in figure 2.1 are the settlement phase, also known as funding. The funds for the transaction are sent to the merchant's bank by the customer's credit card issuing bank. The funds are then deposited into the merchant's bank account by the bank, usually within two to four business days (Google, 2020b).

2.2 Types of Authentications

2.2.1 Password Authentication: This form of verification requires the user to recall what they already know. This strategy is divided into two sections. The username comes first, followed by the password. Only the user knows the password, which is a coded combination of letters and numbers (Lal *et al.,* 2016).

A longer password is much more difficult to crack, which is one of the benefits. It is important to use good passwords when it comes to passwords. A powerful secret key is made up of a mix of capitalized, lower case, numbers, and one-of-a-kind characters.

2.2.1.1 Password Authentication Vulnerabilities: When a user enters a password, the most serious issue is password sniffing. At various stages of communication, an attacker

can sniff the password. Even if the password is complex, the attacker may be able to guess it.

The human factor is the key issue with usernames and passwords:

(i) If easy to remember, the password is easy to guess or search.

(ii) If written down, the password is easy to steal.

(iii) Users/clients may share passwords.

(iv) If difficult to remember, passwords can be forgotten.

2.2.2 Smart Card Authentication

A smart card is a credit card-sized card with an embedded certificate that allows the owner to be identified. The user can use a smart card reader to verify the identity of the individual. To provide multi-factor authentication, smart cards are often used in conjunction with a PIN. To put it another way, the user must have (the smart card) and the PIN, as stated by (Ahsan & Li, 2017) and (Lal *et al.*, 2016).

2.2.2.1 Vulnerabilities with Smart-Card Authentication: Some smart card withdrawals are made because the user cannot remember the PIN and must type it on the back of the smart card. If the user's card is stolen, it can be used against him quickly (Lal *et al.,* 2016). After a certain number of failed attempts, the smart card can be locked. Since it is portable, it can be stolen. Phishing can affect some users who make frequent online purchases. Shoulder surfing can be dangerous at times (Lal *et al.,* 2016).

2.2.3 Knowledge-based Authentication

There are two types of knowledge-based authentication techniques: textual user authentication and graphical user authentication (Khan, 2015). Textual user authentication relies on digits or alphanumeric characters, whereas graphical

authentication relies on images, graphical 2D objects such as pictures (Khan, 2015). Furthermore, there are various authentication methods by which a user can be authenticated, such as location and time. Another option is time-based authentication, which only allows a user to access during specific periods. Because knowledge-based authentication is the most useful, most internet applications, E-mail servers, social networks, and distributed systems use knowledge-based authentications to verify the credential ID (Khan, 2015). When compared to token-based passwords, knowledge-based passwords are more secure. The user can enter his or her ID and secret key, which may be alphanumeric or digits, as well as a special character, and the secret key will be checked to see whether the user is genuine or not. As a consequence, when a user attempts to use the system, the system decides if the user is real or an imposter. As a result, when the user uses the device, it will determine if the user is legitimate or an imposter. If the user is legitimate, he or she will be allowed to log in and use his or her privileges. Many empirical studies show that text-based passwords are difficult to remember and can be broken. A good secure password should be at least 8 characters long and contain both digits and capital letters (Khan, 2015).

Blonder (1996) proposed the graphical password concept. The concept of a graphical password is based on the findings of some psychological studies. Furthermore, a graphical visual object or image is easier to recall than a text-based password (Khan, 2015).

2.2.4 Biometric Authentication

Biometric authentication is a means of defining and/or confirming a user's identity by measuring their specific physiological or behavioural characteristics (Lal *et al.*, 2016). Physiological biometrics include fingerprints, facial recognition, iris scans, hand geometry, and retina scans (Lal *et al.*, 2016). Behavioural biometrics include voice

recognition, gaits, keystroke scanning, and signature scanning. Fingerprints and handprints are the most popular biometric methods in use today. Fingerprint readers are used on many computers, and they can also be used on USB flash drives (Ahsan & Li, 2017) and (Lal *et al.*, 2016).

Biometric authentication is commonly used and has a high level of security.:

(i) It saves the user the time and effort of remembering passwords.
(ii) Biometrics are one-of-a-kind and straightforward.
(iii) Replicating biometric features is extremely difficult.
(iv) The biometric features are irreversible.
(v) Biometric technology is used in airports, customs, and jails.
(vi) The fingerprint scan is small and not expensive.
(vii) Biometrics can be used in smartphone devices.
(viii) Eye scan is perfect and accurate in identifying users.

2.2.4.1 Vulnerabilities with Biometric Authentication

Biometrics provides the best protection but is prone to errors, whereas a fingerprint scan is very reliable because the fingerprint pattern is difficult to guess (Lal *et al.*, 2016). A false rejection error occurs when a device incorrectly rejects a known user and reports that the user is not a known error message (also known as a type 1 error). A false acceptance error (also known as a type 2 error) occurs when a system incorrectly identifies an unknown user as a known user (Lal *et al.*, 2016). Sensitivity can usually be adjusted in biometric systems, but this has an impact on accuracy. Owing to vendor-specific formats, there is also a lack of a true standard. There are also problems with user acceptance and when a user's fingerprint is scanned, they can feel guilty. Finger injuries can also obstruct the scanning method (Lal *et al.*, 2016).

2.2.5 Digital Certificate Authentication

Digital certificate authentication is in form of encryption that works similarly to a passport on the internet. Digital certificates, which use public key and private key information, essentially ensure to the recipient of a message that the message is coming from a specific person. The most significant benefits of digital certificate-based authentication are privacy-related. Digital certificates protect private data by encrypting communications such as emails, logins, and online banking transactions. Digital certificate systems are also user-friendly since they normally operate automatically and require little intervention or involvement on the sender's or recipient's part (Ahsan & Li, 2017) and (Lal *et al*., 2016).

2.2.5.1 Vulnerabilities with Digital Certificate Authentication: Some smart card withdrawals are made because the user cannot remember the PIN and must type it on the back of the card. If the user's card is stolen, it can be used against him quite quickly. After a certain number of failed attempts, the smart card can be locked. Since it is portable, it can be stolen (Ahsan & Li, 2017) and (Lal *et al.*, 2016).

2.2.6 Types of Attacks on Passwords

(i) Brute force attacks

In this attack, the attacker program impersonates a real user and attempts to log into the system by selecting the correct password from the graphics. A brute force attack differs from a dictionary attack in that it does not use dictionaries of alternative passwords. Instead, to gain access to the system, the attacker tries every possible password. Graphic passwords, on the other hand, are more resistant to Brute Force attacks than text passwords because they have a larger password space (Sepideh, 2019), (Shah *et al.*, 2018) and (Rathanavel, 2017).

(ii) Dictionary attacks

This attack uses an exhaustive list of words, such as a dictionary, to break the password. This dictionary includes terms that are likely to be used as passwords by the user. Unlike a brute force attack, a dictionary attack cracks passwords using a structured key search, taking into account only those possibilities that are most likely to succeed, but it cannot crack the password every time, as a brute force attack would. This type of attack is uncommon with graphical passwords. (Thirunavukkarasu, 2017) and (Yesseyeva *et al.*, 2016).

(iii) Guessing Attacks

It is the most common type of attack on alphanumeric passwords where the attacker tries to defeat the authentication system by merely inputting words that he feels an average user can use as a password. It is very likely to be successful if the attacker has little knowledge of the user.

(iv) Shoulder surfing Attacks

An attacker may often discover a user's password by peering over their shoulder as the name suggests (Sepideh, 2019). This kind of intrusion is popular in crowded places where people are unaware of their surroundings (Thirunavukkarasu, 2017) and (Yesseyeva *et al.*, 2016).

(v) Social engineering attacks

A description assault is another name for this. It refers to psychologically persuading people to conduct acts or reveal sensitive information. To gain people's trust and expose sensitive information, it uses a number of deceptions, which leads to a variety of scams and frauds (Sharifi & Shamsi, 2014).

2.2.7 Merits and Demerits of Electronic Payment Systems

2.2.7.1 Merits of Electronic Payment Systems

Customers can pay for goods and services without using cash by using credit cards, cell phones, or the internet. E-payment has a number of benefits, including cost reductions and time optimization, increased sales, and lower transaction costs. It is, however, vulnerable to internet fraud and attack and may potentially increase business costs (Fatonah *et al*., 2018; Kwadzo *et al.*, 2018; Masihuddin *et al.*, 2017).

(i) Increased Speed and Convenience

When compared to traditional payment methods such as cash or check, e-payment is far more convenient. Customers/users do not have to wait in line for their turn to transact because payment for goods or services can be made online at any time of day or night, from any location in the world. They also do not have to wait for a cheque to clear at the bank before getting the money they need to shop. E-payment also reduces the security risks that come with dealing with cash.

(ii) Increased Sales

As internet banking and shopping become more popular and widespread around the world, the number of customers/clients who make cash payments is decreasing. According to the Bank rate, more than two-thirds of customers carry less cash regularly, indicating that electronic payments are becoming the preferred method of payment. As a result, businesses can sell to customers who prefer to pay electronically while maintaining a competitive edge over those who only accept traditional payment methods.

(iii) Reduced Transaction Costs

Although there are no extra costs associated with using cash, trips to the store are normally expensive, and checks require postage. On the other side, there are normally no or very small fees when a user swipes his card or pays online. In the long term, electronic payments can save both individuals and companies hundreds to thousands of dollars in transaction fees (Fatonah *et al.*, 2018).

2.2.7.2 Demerits of Electronic Payment Systems

(i) Security Concerns

E-payments are secured by symmetric encryption and other security measures, but they are still vulnerable to hacking. Phishing attacks, for example, are used to trick unsuspecting users into providing their e-wallet log-in information, which fraudsters then capture and use to gain access to the victims' personal and financial data. Inadequate authentication is also a problem with e-payment systems. If superior identity verification systems like biometrics and facial recognition are not used, someone can use another person's cards and e-wallets and get away without being detected. Some customers may be hesitant to use e-payment systems due to security concerns (Masihuddin *et al.*, 2017).

(ii) Disputed Transactions

If a client uses the company's electronic money without permission, the client/customer will note the unusual charge and file a claim with the customer’s bank, online payment processor, or credit card company. However, without adequate details about the individual who made the transaction, winning the claim and getting a refund can be difficult.

(iii) Increased Business Costs

With the introduction of e-payment systems, there is a greater need to protect sensitive financial information stored in a company's computer systems from unauthorized access. Enterprises that have in-house e-payment systems must incur additional costs in order to acquire, install, and maintain sophisticated payment-security technologies.

2.3 Graphical Password Authentication Schemes (GPAS):

A password is a secret code that is used for authentication. Passwords are the most widely used means of distinguishing users of computer and communication systems. It should only be understood by the user. A graphical password is an authentication scheme that works by making the user choose from images displayed in a particular order in a graphical user interface (GUI), (Computing, 2014). For this reason, the graphical-password approach is sometimes referred to as graphical user authentication (GUA), (Akram, *et al*., 2017), and (Computing, 2014).

User authentication is a critical and fundamental component of the majority of computer security systems. Biometrics is one of the security mechanisms used to address the issues with conventional username-password authentication. However, in this case, the researcher used an alternative method of the images as passwords. (Akram *et al.*, 2017).

Graphic passwords are passwords that are built on picture images rather than alphanumeric strings, and they are one of the authentication schemes. Graphical passwords are being used to increase memorability and reduce the likelihood of insecure passwords being chosen. The use of images as passwords is supposed to increase overall password protection. Graphical Based Authentication (GBA) was introduced in 1996. According to Blonder (1996), the picture images are shown on the screen, and the user is required to click on a few regions. The user is authenticated if they click on the right

regions. The user must pick memorable locations in a picture as a password in the graphical password scheme. The nature of the image and the specific sequence of click points influence the selection of memory locations in the image. In the graphical password scheme, the user must identify previously seen images depending on whether the image is known or unknown. In this password scheme, cued recall is used as a transitional mode of memory between pure recall and recognition. Cued recall is the process of scanning an image to identify previously selected positions in the image. Viewing the image informs or cues users about their previous selections. Graphical Passwords can be divided into several techniques (Veerasekaran *et al.*, 2015).

2.3.1 Categories of Graphical Password Authentication Techniques

Various techniques have been identified over time. The knowledge-based scheme is the most common among them, as it is regarded as the most important technique in terms of protection and usability. This method has been suggested to address a number of flaws in standard password techniques. The reason for this is that, as seen in Figure 2.2, the text is much more difficult to identify, memorize, and recall than pictures (Kadu & Therese, 2017). Currently, certain existing graphical password authentication methods can be classified into four categories as follows (Kadu & Therese, 2017):

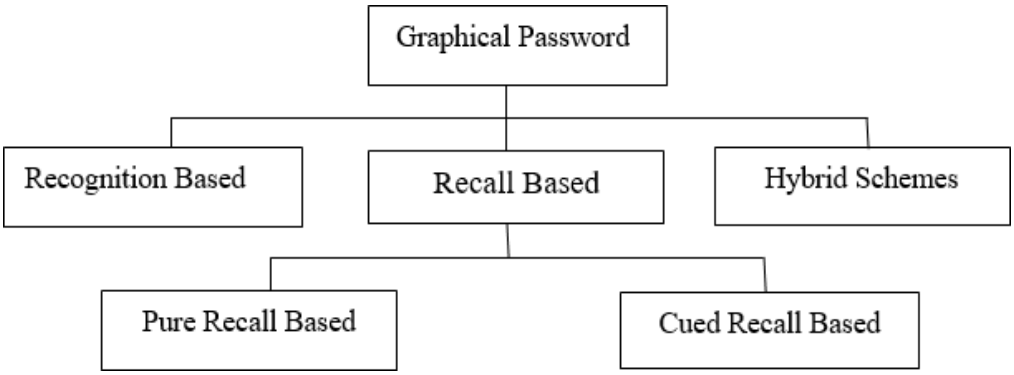


Figure 2.2: Categorisation of graphical password authentication techniques (Kadu & Therese, 2017) and (Istyaq & Saifullah, 2016).

(i) Recognition Technique: - Users pick pictures and symbols from a list of picture images in a recognition technique. During the authentication point, it is important to remember the pictures or signs from the collection of picture images that were selected earlier during the registration process (Istyaq & Saifullah, 2016)

(ii) Recall Based Technique: - Clients have a hard time remembering passwords, so recall-based is very easy and fun to use. It is, however, more reliable than the recognition method (Istyaq & Saifullah, 2016).

(iii) Cued Recall Technique: - Clients are given a hint or clue by the Cued Recall scheme. This hint or clue usually aids clients in quickly, accurately, and conveniently reproducing their password. Its operation is similar to that of recall schemes, but it combines recall and cueing (Kadu & Therese, 2017).

(iv) Hybrid Schemes: - This scheme is known as the hybrid strategy because it incorporates two techniques to form a new scheme in order to correct bugs or setbacks in one scheme, such as shoulder surfing and spyware attacks. The most common drawbacks are usually addressed by hybrid authentication techniques (Kadu & Therese, 2017).

2.3.2 Recognition Graphical User Authentication Schemes: -

The following are some examples of graphical user authentication algorithms that use recognition:

(i) Awase E Algorithm: - Users must pick and register images classified as "transfer images" with the system using this algorithm. Following authentication, a sequence of photographs in the order in which they were sent will be shown. The user must select "transfer image" if the image object is visible in the grid but if the image does not appear in the grid, the user must select "no pass picture." This can be used as a compilation of decoy images. The authentication method is randomly replicated a certain number of

times. Since this method does not allow for the display of a zero number of pass-images during an authentication stage, at least one pass-image will be shown. The pass-image and decoy image's positions on the image grid are chosen at random.

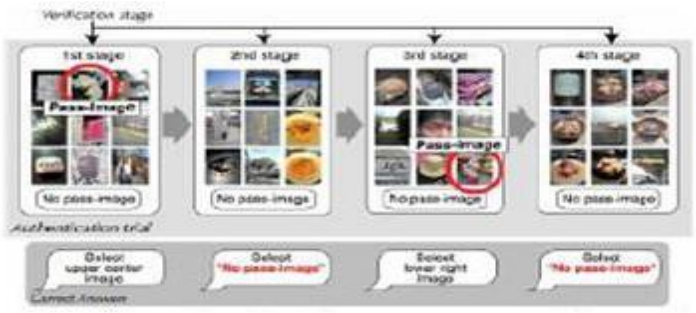


Figure 2.3: A Sample of Awase-E (Ekeke *et al.,* 2013).

(ii) Passfaces: - Passface is a Real Clients Corporation company product in which the consumer must choose a face from a grid of picture faces. One of the most appealing features of pass face is how difficult it is to hack, differentiate, or recall. The user must choose four human faces from a grid of nine photos before completing the authentication process. The user typically selects faces based on their characteristic similarity, the login method can be uncomfortable, and face blind people cannot use the PassFaces algorithm (Thirunavukkarasu, 2017; Khodadadi *et al.,* 2016; Rathanavel, 2017).

Figure 2.4: A Sample of Passfaces (Kumar *et al.,* 2013; Ekeke *et al.,* 2013; Deorankar, 2017; Mahore, 2017)

(iii) Déjà vu: - Dhamija and Perrig (2000) as cited by Awodele Oludele *et al.,* (2017) proposed the Déjà vu algorithm in the year 2000. This necessitates a user picking a certain number of images from a vast array solely based on visualization technique. The user is

needed to recognize the selected image during an authentication session, during which the user is authenticated. This algorithm, according to Dhamija and Perrig (2000), is more stable because the authentication key cannot be written because conceptual images are difficult to describe in words (Rathanavel, 2017; Khan *et al.*, 2019; Awodele Oludele *et al.*, 2017; Zabidi *et al.*, 2019). The drawbacks of this algorithm are that it necessitates the loading of a large number of images into the database and that the authentication process can be lengthy.

Figure 2.5: A Sample of Déjà vu (Yesseyeva *et al.*, 2016; Khodadadi *et al.*, 2016; Ahmad, *et al.*, 2016; Veesekaran *et al*., 2015).

(iv) Picture Password: - In their study, Jensen *et al.* (2003) as cited by Ekeke *et al.* (2013) and Veesekaran *et al.* (2015) suggested that the algorithm be created and implemented specifically for mobile devices (mobile). The user chooses a theme, such as cats or dogs, during the registration process. This theme is made up of thumbnail photos that have been password-protected in order of appearance. To generate a password for authentication, the user must use a stylus to record the order of the images inside the theme during the registration stage. Since the size of thumbnail images is limited to thirty (30), each thumbnail picture is assigned a number, and the order of image selection produces a numerical password space, the number of password spaces is assumed to be small. Jensen *et al.* (2003) note in their paper that a user can generate a new numerical value by combining two or more thumbnail images from the same period. The disadvantage is that the newly created password is difficult to recall.

Figure 2.6: A Sample of Picture Password (Ekeke *et al.*, 2013) and (Veesekaran *et al.*, 2015).

(v) Colour Login Algorithm: - Gokhale, *et al.* (2016) the background color of this algorithm is used to minimize login time. Furthermore, the use of multi-color is meant to confuse fraudsters, but user authorization is easy. Shoulder surfing attacks are not a problem for the algorithm. It has the drawback of having less password space than alphanumeric or text passwords (Saranya & Sharavanan, 2017).

(a). The displayed screen (b). A completed round

Figure 2.7: Colorlogin (Saranya & Sharavanan, 2017; Awodele Oludele *et al,* 2017; Farmand & Zakaria, 2010)

(vi) Jensen et al Technique: - Gokhale *et al.* (2016) and Akram *et al.* (2017) suggested this graphical technique mechanism for handheld devices (mobile) and personal digital assistants (PDAs). To begin, the user must choose a theme, such as dogs, cats, or rats. Users can see the theme photos in a 5 x 6 grid. In addition to this, each image is

represented by a thumbnail number. The user must then recall the previously selected images and choose the image using the stylus in the correct order for authentication. This technique reduces the number of images to 30, resulting in a limited password space. Each image is given a numerical value, and a numerical password is created by selecting a sequence. Numerical passwords are typically less reliable than text passwords at some stage. To get around this, the user can pick two images at once with a single click to increase the password space number. However, this has the downside of adding ambiguity and difficulty to the user's experience.

Figure 2.8: Cats and dog theme (Ekeke *et al.*, 2013)

2.3.3 Recall based Graphical User Authentication Algorithms

Recall-based graphical user authentication algorithms can be divided into two categories. Pure recall and cued recall are the two forms. A variety of algorithm examples are also available, such as follows:

(i) Grey E. Blonder Algorithm: - Blonder in the Year (1996), as presented by Farmand & Zakaria (2010); Ekeke *et al.* (2013); Khan *et al.* (2019) proposed an algorithm in which a user is given an image during the registration process that they want. He then chooses a hit region or a position within the image at this stage. During the authentication session, a picture image is shown for the user to choose from predefined authentication regions. The key benefit is that it is easier to remember than text-based passwords. The

lack of memorable password space is a drawback of this scheme. (Saranya & Sharavanan, 2017).

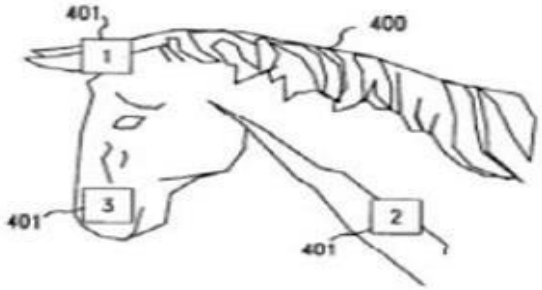


Figure 2.9: A Sample of Blonder (Ekeke *et al*., 2013) and (Yesseyeva *et al.*, 2016)

(ii) Pass Points: - This algorithm was created by Zimmermann & Gerber, (2020) and Ashwini & Sreedhar, (2015) but Grey Blonder's methodology effectively expanded it by eliminating the predefined margins and any artificially generated images that could be used. The algorithm helps the user to pick various areas of the image sequentially. To create a password, users must select any region on the image during registration. A user is expected to click the close place on the selected click point during the login process, and the tolerance of each selected click point is determined. To verify their identity, they must click through the tolerances of the selected click regions in the correct order. The downside is that although the password is easy to construct, users would have difficulty remembering it as compared to textual passwords. The login time is considerably longer as compared to a text-based password.

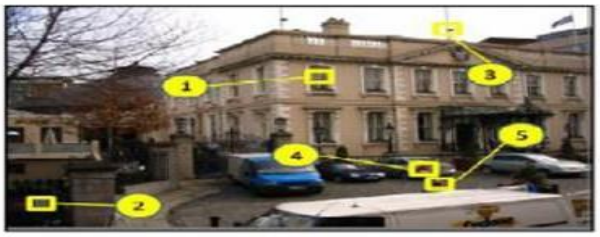


Figure 2.10: A Sample of PassPoints (Ekeke *et al.*, 2013) and (Yesseyeva *et al.*, 2016)

(iii) Draw A-Secret (DAS):- In this algorithm, Computing (2014) the researcher proposed a technique in which the user produces a sketch of an image in a 2D grid of G x G. This technique uses rectangular grids of x and y coordinates. The grid values are saved in the order in which they are drawn on this page. To touch the same coordinate grid during authentication, he or she must redraw the same frame. It has the advantage of having a larger and more secure password space than a text-based password. It also has the drawback of using a shaky drawing that is vulnerable to dictionary attacks.

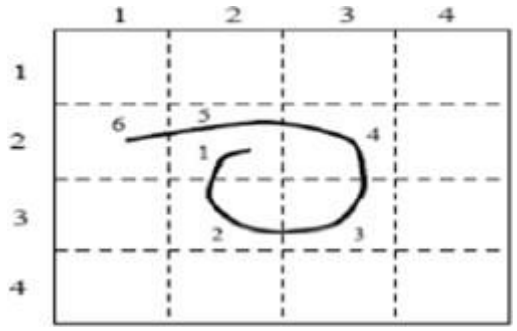


Figure 2.11: A Sample of Draw a Secret (DAS) on 4x4 Grid (Kadu & Therese, 2017) and (Ekeke *et al.,* 2013)

(iv) Passdoodle: It refers to a DAS-related algorithm. It allows a user to make a drawing that can be used as a password without the use of a grid. Users could remember the final drawing but made mistakes remembering the figure, sequence, or direction of the pen stroke, according to Goldberg *et al*. (2002) as cited by Ekeke *et al.* (2013) who looked at a small paper-based Passdoodle sample. In addition, the user must generate a doodle password if he wants to be authenticated. Khan *et al.* (2019) demonstrated that the algorithm was much more difficult to hack due to a large number of possible doodle passwords. Users could correctly recognize a complete doodle password as a textual password (Suru & Murano, 2019) and (Mathur & Lokhande, 2017). Other users draw

users to the system, which makes it vulnerable to attacks like shoulder surfing, guessing, and spyware.

Figure 2.12: A Sample of Passdoodle (Ekeke *et al.*, 2013)

(v) Syukri Algorithm: Kadu & Therese, (2017) in this algorithm, the user must use a mouse to draw their signature. The user is not required to recall the drawn signature by the algorithm. There are two steps to it: authentication and registration. One of its benefits is that it is difficult to counterfeit, and it is ideally suited for smartphones and other devices with a stylus. The disadvantage of this scheme is that using a cursor to write a signature is inconvenient for users.

Figure 2.13: A Sample of Syukri algorithm (Ekeke *et al.*, 2013) and (Yesseyeva *et al.*, 2016).

(vi) Quantitative DAS Algorithm (QDAS): This algorithm is a DAS-improved graphical scheme in which each stroke is coded and formed. When compared to the DAS technique, the QDAS provides a larger password space. The scheme's drawback is that users would have a harder time remembering the sequential order than with the original DAS strategy. Its benefit is that it mitigates the drawbacks of shoulder surfing.

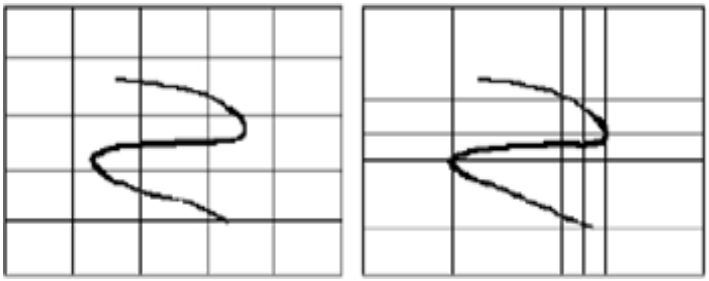


Figure 2.14: A Sample of Qualitative DAS (Ekeke *et al.*, 2013)

(vii) PassMap: For password authentication, this algorithm employs a Map. PassMap consists of two steps: registration and authentication. The user can select a Map (for example, a World Map, an African Map, or any region) and then States, Cities, or a country that he wants to visit or has recently visited during the registration process. If a user correctly identifies the selected point on the Map, this algorithm will authenticate the user. Its drawbacks include being vulnerable to Brute Force and Dictionary attacks. It is easy to use, comfortable, and resistant to shoulder surfing (Dogo, 2018).

(a). African Map (b). World Map

Figure 2.15: Samples of PassMap (Dogo, 2018)

2.3.4 Cued Recall Based Algorithms

2.3.4.1 Cued Click Points (CCP)

This algorithm was created to minimize patterns and hotspots. The user in this scheme clicks on one point per image in a sequence of images. The following image is based on the previous click-location points. Because user testing and analysis revealed no evidence of patterns in Cued Click-Points, pattern-based attacks appear to be ineffective. Even though the results showed that hotspots continue to be a problem (Ritu *et al.*, 2015)

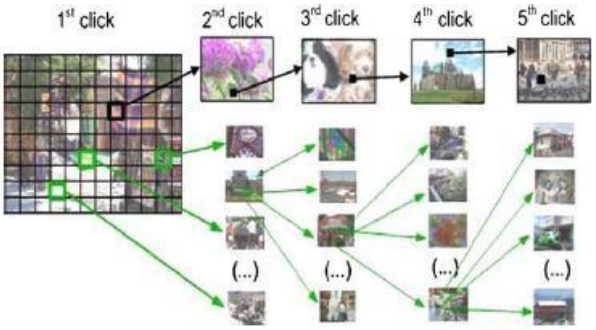


Figure. 2.16: A Sample CCP (Veerasekaran *et al.*, 2015; Computing, 2014; Ritu *et al.*, 2015)

2.3.4.2 Persuasive Cued Click-Point (PCCP)

The PCCP system (Ritu *et al.*, 2015) was created to encourage users to choose fewer likely images as passwords. The primary function of PCCP is to allow the user to select a click point within the image highlighted viewport. The user can reposition the viewport until it finds a suitable location. The images are displayed normally without a viewport during authentication. Although it reduces the effects of hotspots, shoulder surfing remains an issue.

Figure 2.17: A Sample PCCP (Computing, 2014; Sun *et al.*, 2018; Ritu *et al.*, 2015)

2.4 The Main Factors in Graphical Password Authentication Techniques.

The main factors involved in graphical authentication passwords as presented by Saranya & Sharavanan, (2017) and Awodele Oludele *et al.*, (2017) are follows:

2.4.1 Usability

One of the essential and significant points for graphical authentication passwords is that picture images or objects are simpler to memorize compared to textual passwords. One of the main criticisms amongst the users of graphical authentication techniques is that the registration and login procedures consume a lot of time, for example in the recognition-based approaches, a user is required to choose few images from a pool of image groups. Also, in the authentication stage, a user needs to recognize or validate pass-images by going over all the images shown. These processes are time-consuming, boring, and hectic for users. As a result of this, users sometimes see the graphical password as less suitable compared to the textual password and so the majority of users are not acquainted with the graphical password.

2.4.2 Password Space

Graphical password security system highly relies on enough huge password space. It is one of the main resilient to brute force attacks. Password space can be calculated using:

$$SPACE = M^N \quad (2.1)$$

where M denotes the number of characters and

N denotes the length of the password.

For example, for the textual-based password of a given length = 8 and 64 printable character alphabet, the number of possible passwords will be 648 = 2.8 X 1014 (Awodele Oludele *et al.*, 2017) and (Lashkari *et al.*, 2011).

Graphical Password Space differs from one graphical authentication scheme to the other. For instance, N can be the number of rounds and M can be the number of pictures utilised in each of the rounds. Also, N can be the number of pixels on the picture image while M is the number of locations that are clicked on the picture image (Awodele Oludele *et al.*, 2017) and (Saranya & Sharavanan, 2017).

2.4.3 Password Entropy

Password Entropy is normally used in measuring the security of a generated password, in terms of difficulty in guessing the password. Password Entropy can be computed using:

$$\text{Entropy} = N\log_2 (|L| |O| |C|) \quad (2.2)$$

Where N denotes the length or number of runs, L denotes locus alphabet as the set of all loci and O denotes the object alphabet C denotes the colour of the alphabet. (Osunde *et al.*, 2019)

2.4.4 HotSpot

Hotspots in graphical password authentication refer to the point on the image that tends for it to be chosen by the users because of the attractive look or because of how catchy those points look to the users of the scheme. Attackers mostly pay more attention to those points for them to launch an attack (Ashwini & Sreedhar, 2015).

2.4.5 Security:

The most crucial aim of the authentication technique is to exploit the effectiveness of password space. An effective password space is determined by the user's behaviour. Security and usability of a system are acceptable, since increasing the security of a system would lead to a decrease in usability (Shah *et al.,* 2018) and (Computing, 2014).

2.5 Related Studies

Several researchers over the years have emerged with different algorithms as touching or clicking point graphical passwords authentication and different approaches have been implored on various platforms. Some of the researchers are aimed at developing graphical password schemes that would be suitable to the users while keeping security in check.

Veerasekaran *et al.* (2015) proposed a graphical password technique based on Persuasive Cued Click Points. The user is authenticated in their scheme based on a group of some picture images as well as the approximate pixel of the user's click. Their mechanism increases the application's security. Traditional authentication methods, according to the researcher, are vulnerable to hacking. Text-based passwords can be difficult to use if users choose different passwords for increased security. As a result, remembering several passwords would be challenging.

The researchers utilized Persuasive Cued Click Point (PCCP) that boosts the users to choose a hard password for a more secured manner. Veerasekaran *et al.* (2015) further carry out an experimental study to examine how they can increase the proportion of recognition efficiency and carried out laboratory studies to compared various techniques and the time taken for execution. The researchers employ three types of algorithms: Euclidean distance, Horizontal Ellipse, and Vertical Ellipse, with execution times varying from algorithm to algorithm. They presented it as a password-based authentication that

can offer better security that will efficiently raise the password space, login success rate, and security.

Razvi (2017) proposed graphical password authentication which states that despite all the encryption and security provided by Banks, they still face all the hacking attacks while using alphanumeric and digital signature and any other login methods and so suggested using “graphical passwords” as they are more secure from any hacking attacks.

The results of this proposed scheme conclude that to overcome frauds, hacking data, or steal data from the banking sector, this technique should be implemented to protect customer/client identity.

The work of Shah *et al.* (2018) presented a graphical password scheme based on colours and numbers, which is purely recognition-based. In their algorithm, the user has to first enter a username and after which the user is told to rate colours from 1 to 8 randomly. Then, during the login procedure, the user after entering the correct username, the login interface based on the colours selected by the users is displayed including the number grid of size 8x8. The scheme is also based on rows and columns. After the user is successfully authenticated, he is then granted access to the system. But during the next login, the password format changes.

The work of Deorankar (2017) and Mahore (2017) carried out research work to merge two factors for their graphical scheme (that helps in generating strong passwords). They made their scheme similar to the pass faces system where one image is used with several faces on the screen and the user clicks 2 or 3 faces as the password but here, they implored the second layer of security to ensure strong authentication (which will make the login process slow). They implored the use of login indicators that are generated once, and they allowed for all the images selected by the users to be displayed on a single web page. In

their algorithm, at the authentication phase, a login indicator would be generated and given to the user through various ways such as audio, visual, or text.

Ahsan & Li, (2017) carried out research work on pure recognition-based graphical passwords and came up with an algorithm called the “image sequence technique”. In their technique, users during registration will upload images from their directory into the scheme in a particular sequence during login and the user will have to remember the sequence in which the image was uploaded in the first instance during registration. In their work, after the user uploads the images (4 or 6), then those images are added into a group of random images in which the user will select the images personally uploaded.

Awodele Oludele *et al.* (2017) proposed a shoulder-surfing resistant graphical authentication scheme to address the major issues with the graphical authentication schemes that have been developed. In summary, the proposed scheme provides a high level of resistance to shoulder surfing attacks, reduces the need to upload pictures, and aids in the scheme's selection of objects. Their proposed scheme utilizes a set of coloured rows and columns which will assist users in identifying their chosen cell. The interface design elaborates on the cued recall graphical technique being utilized. This scheme involves the following: i. Rows and Columns, ii. Cells and iii. Inserting Values into the cells. Their findings were that the schemes still have some flaws, implying that there is no such thing as a perfect graphical authentication scheme; each scheme has advantages and disadvantages, making it a suitable candidate for different environments and/or events based on its architecture.

Sun *et al.* (2016) proposed PassMatrix, a novel authentication system based on graphical passwords, to combat shoulder surfing attacks. PassMatrix, with a one-time valid login indicator and circularize horizontal and vertical bars covering the entire scope of pass-

images, provides no hint for attackers to figure out or narrow down the password, even when they conduct multiple camera-based attacks. Their results showed that the proposed system is more resistant to shoulder surfing threats while still being usable.

The work of Mohammad & Maria, (2018) presented a new password scheme that employs a graphical user interface for password entry. The password consists of multiple graphical objects that are integrated to form one picture. The main advantage of this approach is making user authentication more user-friendly where it is often easier to remember a scene than an alphanumeric password. The user creates the password scene by selecting from the available shapes where the selection process is combined with the selected objects to create the actual password. The scene created by the user is transformed into an alphanumeric password where the number of combinations used in creating this alphanumeric password from the given objects of the scene prevents brute-force attacks. These combinations include the choice of objects to use, the number of times each object is selected, the order of object selection and object sizes. The results and analysis of the proposed scheme showed it to be secure and easy to use.

In the research work of Yesseyeva *et al.* (2016) they proposed a new graphical user authentication scheme called the Tri-Pass. In this scheme to create a password user has to choose one image from the pool of images and then select any three points by clicking on the image called the password point. To login, the user has to repeat the same sequence of activities carried out in the first stage. The proposed new algorithm is based on two techniques, namely the PassPoint and Triangle algorithms. In the proposed algorithm, they focused on the features and benefits of these two algorithms and combined them to achieve the highest level of security and usability possible.

The analyses of their questionnaire results revealed that the majority of the users are given good feedback about the whole prototype evaluation and usability features built in the prototype. Also, from the result, most of the users were satisfied with registration time, but the login time of this graphical password scheme in comparison with the text-based scheme is much longer. Overall, more than 80% of respondents were pleased with the performance of the prototype system, which is an excellent result.

Osunade *et al.* (2019) suggested a scheme that uses a combination of the DAS and Story algorithms. To increase memorability, users are advised to mentally create a story connecting the images they have selected. Instead of clicking on their password pictures (pass-images), users must draw an ordered curve over them. Pass-images and decoy images are used to trick peepers when the user's curve moves through them. The drawing starts and finishes with random images to avoid showing the first and last pass images. When the user sketches the curve, the drawing trace is cleared, reducing the possibility of passwords being revealed. Furthermore, when the user draws a curve across the pass files, random curves are shown. During the login process, the device shows degraded images that are difficult to discern from a distance or a side view.

Osunade *et al.* (2019) The results of the user study's shoulder-surfing test show that the proposed system is immune to shoulder-surfing attacks, despite the fact that the attackers understand how the proposed system and the underlying algorithm operate.

2.6 Summary of Review

It has been observed from the reviewed works of literature that the adoption of e-payment systems despite the numerous challenges is taking over from the traditional method of transaction. It is also observed that few security challenges have been fairly addressed although more of these challenges keep emerging in the technologies in use. Measures

have been put in place to authenticate the use of electronic payment systems such as password authentication, biometric authentication and the current one is the graphical password authentication mechanism.

Further, over the years, the rate at which user's online account and bank account are being hacked has increased greatly, because users are found of choosing passwords that are easy for them to remember and also very easy for attackers to acquire using the conventional alphanumeric password scheme. Thus, Graphical passwords, on the other hand, provide users with the advantage of memorability and a friendly user interface other than alphanumeric passwords while keeping security in check.

2.7 Performance Metrics

System evaluation metrics are regarded as an important phase in research work, in which standard goals are measured to compare experimental results with the existing graphical scheme (Wazir *et al*., 2020). This also clarifies evaluation as a systematic procedure for evaluating a designed scheme for its architecture, framework, and benefit. Evaluation is a vital process in which a thorough examination, consideration, or attentiveness and judgment of the system yield accurate results. These include; evaluation method, security evaluation, usability evaluation, usefulness, and utility evaluation (Mihajlovic & Xiong, 2019).

In this study, the Similarity Metrics, Distance measure metric, login success rate metrics, the Execution time of algorithms or time speed in milliseconds metric and percentage matching errors of the algorithms are used to determine the robustness, efficiency, and performance of the system (Khan *et al*., 2019).

2.7.1 Distance Metrics Overview

Distance metrics are essential for determining the similarity or regularity of data images. It is important to know how image data are associated with each other, how different data are from each other, and what measures are considered to compare them. The first goal of metric calculation in a particular problem is to get an appropriate distance and similarity function. Metric learning has emerged as a well-liked issue in many learning tasks, and it can also be utilized in a wide variety of settings.

A metric also referred to as a distance function, is a function that defines the distance or space between two or more elements or objects in a group. A group with a metric is known as metric space. This distance metric is extremely important in clustering techniques. The main contribution of this work is the investigation of performances of the similarity metric (Bora & Gupta, 2014) and (Similarity *et al.*, 2020).

2.7.2 Cosine Distance and Cosine Similarity

The cosine distance and cosine similarity metrics are primarily used to discover similarities between two data points. The cosine similarity, or the number of similarities, decreases as the cosine distance between the data points increases, and vice versa. As a result, points that are close to each other are more similar than points that are far apart. Cosine similarity is given by Cos θ, and cosine distance is 1- Cos θ (Similarity *et al.*, 2020).

Cosine Similarity is introduced as a method of reducing the illegal user's login time, which is thought to be crucial to a password scheme's usability. It aims to motivate the user by providing a fun, friendly interface that improves the user experience and provides an acceptable login time. The use of the Cosine Similarity algorithm to Login is a promising technique (Saranya & Sharavanan, 2017).

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Research Design Framework

The schematic block diagram shown in figure 3.1 depicts the research designed framework of this study. This framework involves steps from the Registration Interface to the Login Interface and finally, E-Payment Login interfaces where a user can make his or her electronic payments either by Credit Card, Smart Card and Debit Card respectively. Clients can also make a transfer of funds. The algorithms follow the steps in figure 3.1 to produce and evaluate the results:

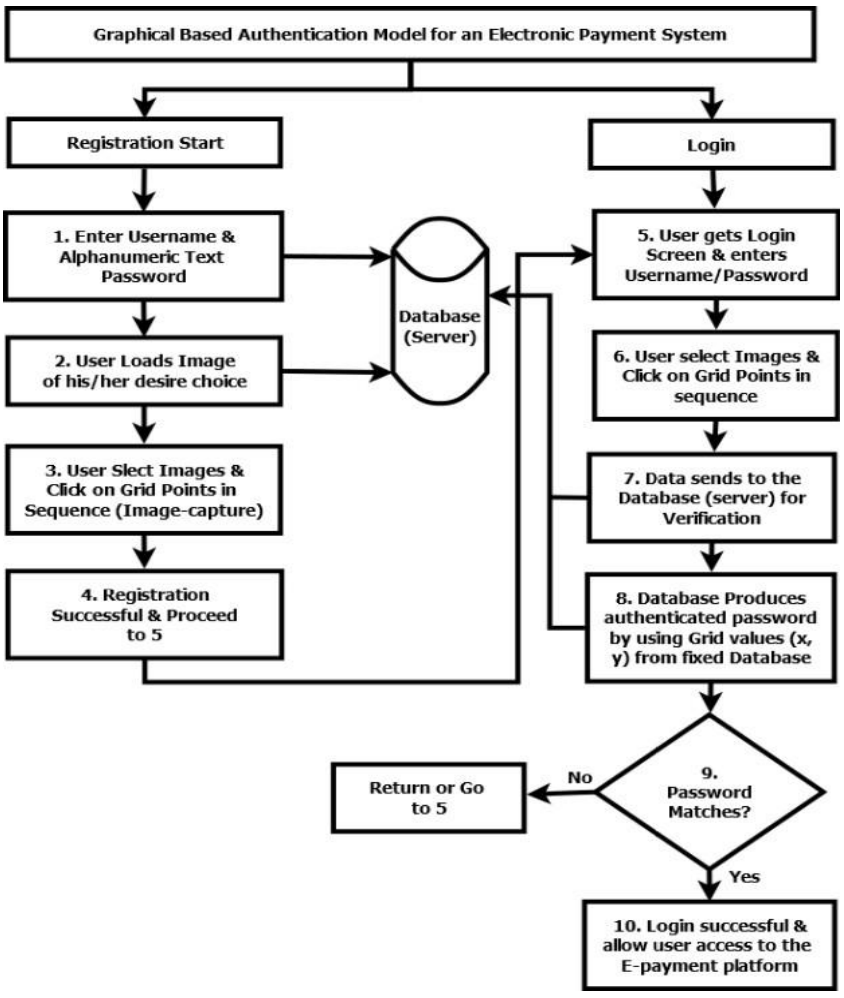


Figure 3.1: Schematic diagram for the Proposed Graphical Based Authentication Model

The interface components for the Proposed Graphical Based Authentication (GBA) Model (Figure 3.1) are explained as follows:

3.1.1 Registration Interface

Step 1: User enters personal information: In every model (system) the user must register as a new user with the model. The proposed graphical model's block diagram (figure 3.1) begins with the registration process, in which the user enters personal information such as a username, email identification, phone number, textual password, and saves it to the Model's server (database). Here the registered user identification, password, email address and mobile number are used to create a textual password and save it in the model's database.

Step 2: User loads images of their own choice: After saving the personal identification/details, the user loads their own desired images and presses the next button to now move onto a 3x3 graphical image grid display.

Step 3: User Selects images and clicks on the grid points in sequence: The image grid contains a set of images, and the user must select images in sequential order and click once on a selected point on each of the three images to generate a graphical password. The image is captured by the model using the generated registered coordinates x1, y1 and stored in the database using the user ID generated at the end of the registration process.

Step 4: Registration successful: After the password entry, the user clicks on the register button. The model sends a registration successful message. If not, successful it sends an error message.

3.1.2 Login Interface

Step 5: User gets login scheme (model): After successful completion of registration procedures with the model (system), the user then proceeds to step 5 to login into the

model as a new user by providing correctly username, textual password and graphical password which the user entered during the registration phase. Here the user selects the algorithms from the pulldown menu to login into the model.

3.1.3 Verification and Validation

Step 6: Select images and click grid points in sequence: Once a user login correctly with the username and textual password used during the registration, a 3x3 images grid display is shown. When the user clicks an image in the grid display, it zooms in to give the user a better look at it. Here again, a user picks a set of images in sequential order and clicks on the same 3 different images on the clicked point chosen as a password during the registration.

Step 7: Data is sent to the server: The data or login coordinates values x2, y2 generated by the model (scheme) are sent to the server for password matching or against the registered coordinates for verification and validation.

Step 8: Server produces encrypted password by accessing grid values from the fixed database: Here the server produces the encrypted images on a request by the user for validation.

3.1.4 Authentication Interface

Step 9: If the password matches, access is granted as follows: If the graphical images entered by the user in the sequential order are correct, the user is legitimately granted access to the **electronic payment interface** to conduct electronic transactions (E-Payment's transactions).

Step 10: If the password does not match, it moves to step 5: If a user is denied access to the model the user simply switch to step 5, alternatively, the user can simply select the

Forgot Password option, and a 7-digit random alphanumeric code will be sent to the email address used during the registration process, allowing the user to reset their password.

3.1.5 The Equation for the E-Payment Model

Let $\mathbf{EP} = (\sum_{k=1}^{n} \mathbf{T} + \mathbf{T_A})$ (3.1)

represents the general equation for the model.

Where:

EP is Electronic Payment (E-Payment)

T is Transaction.

$\mathbf{T_A}$ represents the type of distance measure authentication of users.

n denotes the number of transactions.

K = 1 is constant for authentication for one transaction

Therefore, substituting $\mathbf{T_A}$ with the various distance measures in equation **3.1** gives the following equation:

$\mathbf{EP} = (\sum_{k=1}^{n} \mathbf{T} + (ED, JD, CBD, CS))$ (3.2)

Where:

ED = Euclidean Distance

JD = Jaccard Distance

CBD = City Block Distance (Manhattan Distance)

CS = Cosine Similarity

For simplicity and clarity, substituting $\mathbf{T_A}$ with a formula that denotes each distance measure, starting with ED, JD, and followed by CDB and CS in that order.

That is, for Euclidean distance (ED), the following is obtained,

$$\mathbf{EP} = \left(\sum_{k=1}^{n} \mathbf{T} + \sqrt{\sum_{i=0}^{n} (X_i + Y_i) 2 .} \right) \quad (3.3)$$

Where:

EP = Electronic Payment (E-Payment)

(Y_i, X_i) = Registered coordinates

(Y_j, X_j) = Login coordinates

In the case of Jaccard Distance (JD), the following is given:

$$\mathbf{EP} = \left(\sum_{k=1}^{n} \mathbf{T} + X_i * X_j / (|X_i|^2 + |X_j|^2 - X_i * X_j) \right) \quad (3.4)$$

Where:

(Y_i, X_i) = Registered coordinates

(Y_j, X_j) = Login coordinates

For City Block Distance CBD, the equation is as follows

$$\mathbf{EP} = \left(\sum_{k=1}^{n} \mathbf{T} + \sum_{j=1}^{n} |X_{sj} - X_{tj}| \right) \quad (3.5)$$

Where:

(Y_i, X_i) = Registered coordinates

(Y_j, X_j) = Login coordinates

And finally, for the Cosine Similarity, the equation is given as follows.

$$\mathbf{EP} = \sum_{k=1}^{n} \mathbf{T} + \frac{(\sum^{n} A_{i*B})_{i}}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}} \quad (3.6)$$

Where:

(Y_i, X_i) = Registered coordinates

(Y_j, X_j) = Login coordinates and A^2i and B^2i are components of vector points A and B respectively (Similarity *et al.*, 2020).

Therefore, in this study the Mathematical Equation for the E-Payment Model is given as:

$$\mathbf{EP} = (\sum_{k=1}^{n} \mathbf{T} + \mathbf{T_A}) \quad (3.7)$$

Where: **T** = Transaction (it includes registration, login, verification, e-payment) and

$\mathbf{T_A}$ = Type of Authentication

3.2 Proposed Graphical Based Authentication Model (GBAM)

The aim of this research work is to develop a model on graphical based authentication passwords for an Electronic Payment (e-payment) System. And to implement this model, four phases were involved: Home page, Registration phase, Login Phase (Image password creation), Image password authentication and electronic payment interface as shown in figure 3.1. The following system research tools were also used in implementing this graphical scheme:

HTML (Hypertext Mark-up Language) is used to build and design the layout of a graphical-based scheme in order to achieve a grid framework.

CSS (Cascading Style Sheet) is used for the presentation and selection of each row and column.

JavaScript was used in interacting with the user- username checking and password listing. It is also used in graphical interfaces for password creation, setup and generation. It performs well in both the frontend and backend frameworks in this thesis.

MySQL, PHP - database is used where selected data Picture images, Username and password are loaded and to handle the password verification.

PHP (Hypertext Pre-processor) is used as a link to the database and as a server scripting language, XAMPP (Cross-platform, Apache, MySQL, PHP and Perl) – It is a software designed for window operating system, database, web server and scripting software.

XAMPP server software provides an environment for testing MySQL, PHP and Apache projects locally on a computer.

PhpMyAdmin: This is a user-friendly GUI for managing database operations. The Model (scheme) was hosted on 4 GB RAM, 800 MHZ, Intel, Core i5, 15.6 Inches screen display with a resolution of 1366x768 pixels running on windows 7, keyboard and mouse.

3.3 The Requirements for the Authentication Model

The two essential requirements used for this graphical scheme are Software and Hardware system.

Software:

The implementation of these graphical models was developed using system research tools such as HTML, CSS, XAMPP and JavaScript all at frontend and backend, and Web Browser was used (Google Chrome) and a Server (Database).

Hardware:

To be able to configure these graphical models, the following hardware component was required and was used: Database Server and an electronic device such as Laptop or Desktop with a 4GB Memory Capacity.

Functionality:

The functional requirements for this graphical system include the following:

(i) The Graphical system must permit the users to choose their preferred picture images for the graphical password.

(ii) The graphical scheme has to automatically generate registered coordinates (x1, y1) and login coordinate (x2, y2) from the chosen images.

(iii) The graphical system should effectively recognize and authenticate or validate the existing registered user as well as their graphical password with the system.

(iv) This system should be able to sense the registration phase if coordinates were chosen consecutively.

(v) The scheme should be able to signify if a username is taken or not during the registration phase.

Non-Functionality:

Non-functional requirement postulates some criteria which can be used to assess the graphical scheme's processes. Some of these processes include the following:

(i) The graphical scheme developed must be highly user-friendly.

(ii) It must be easy and simple to use (usability).

(iii) The scheme must be memorable and easy to interact with.

(iv) The graphical scheme must be reliable and retain information data.

3.3.1 Data Collection

The secondary data collection method was used for this study. This was done by data capturing of different picture images. The picture images collected as data are obtained from Shutterstock (2020), Pexels (2020) and Google (2020a). The images collected were used to determine their x and y coordinates during the registration and login processes.

3.4 Performance Evaluation

The performance of these algorithms was compared using various metrics such as login time (execution time), login success rate and matching error.

This research study conducted an experiment involving five (5) participants (users) to compare different distance measure algorithms and their various times taken for execution, login success rate and matching error. The registration and login time was utilised to test the reliability, efficiency and robustness of the graphical model (scheme).

3.4.1 Login Success Rate

Five 5 participants (users) were selected from the Computer Science Department, Federal University of Technology, Minna. The five (5) participants were requested to take part in the registration procedure by entering their username, text password, email and phone number. Also, they have to choose an image password in sequential order and click on the three different images one at a time. Each attempt was reported as either successful or failure. This means that the success rate can be calculated based on the successful login of a user as.

$$\text{Login Success Rate (LSR)} = \frac{\mathbf{N_S}}{\mathbf{N_A}} * \mathbf{100}\% \quad (3.8)$$

Where $\mathbf{N_S}$ is the Number of Successful Login by a user, $\mathbf{N_A}$ is the Number of Attempts to Login by a user

3.4.2 Execution Time for the Algorithms

In this experiment, the same 5 participants used the four different algorithms: Euclidean distance, Cosine similarity, City Block distance and Jaccard distance. Here the time taken for execution differs from one algorithm to the other. Every participant was permitted to register and create an image password in sequential order. After this, participants login into their accounts respectively by utilising one algorithm at a given time. The execution time was taken from the point where each participant (user) clicks on the algorithm from the dropdown menu to submit a password for authentication until the participant views E-payment interface files on successful login. The execution time is computed as:

$$\text{Execution Time (ET)} = \mathbf{T_2} - \mathbf{T_1} \quad (3.9)$$

$$\text{Average Execution Time (AET)} = \frac{\mathbf{T_2} - \mathbf{T_1}}{\mathbf{P_s}}$$

Where $\mathbf{T_2}$ is the End Time of Successful Login by a user, $\mathbf{T_1}$ is the Start Time of Login by a user and $\mathbf{P_s}$ is the total number of participants.

3.4.3 Matching Errors for the Algorithms

The idea of the Matching error stems from the computation of an average angular error as described in Simon *et al.* (2011). It is an important metric that allows for an effective evaluation of the performances of the different algorithms (Euclidean distance, Cosine similarity, City block distance and Jaccard distance) for similarity measure between different vectors points. It describes the angle between the vector points at the login phase and the vector points at the user registration, all in 2D space. The matching error between

two vector points is computed as the inverse cosine of the ratio of the dot product of the vectors and the product of their lengths: The general equation is given by:

$$\boldsymbol{ME = arccos}\ \frac{U*U_e + V*V_e + 1}{\sqrt{(U)^2+(V)^2+1}\sqrt{(U_e)^2+(V_e)^2+1}} \qquad (3.10)$$

Where:

U, V - denote the vector point (x, y) obtained during the login phase (x2, y2)

Ue, Ve - (e) represents the vector points that are obtained during user registrations and save in the database (x1, y1)**.**

arccos represents the inverse cosine and **ME** is the matching error computed between the vector points obtained during the user login and the vector points during the registration phase. To avoid division by zero, one is added to both the nominator and denominator as shown in equation (3.10).

Now equation (3.10) can also be expressed (formulated) using variables x, y as expressed in equation (3.11):

$$\mathbf{ME = arccos}\ \frac{(X2*X1) + (Y2*Y1) + 1}{\sqrt{(X2)^2 + (Y2)^2 + 1}\sqrt{(X1)^2 + (Y1)^2 + 1}} \qquad (3.11)$$

Equation (3.11) was used in this work to calculate the matching errors involving matching of two points during the register and login sessions of coordinates (x1, y1) and (x2, y2).

In this research work, the matching error gave the error rate of the graphical scheme (model) in the process of matching two points that are, the points at registration and login phase. A minimum matching error means that the graphical scheme is robust and reliable, ensuring the security and usability of the entire system.

3.5 Similarity Measure

The similarity measure is an important task for document retrieval, text matching and retrieval of images from the database that is similar to the query image. To achieve an optimal performance of the system and make it robust in the face of many challenges, an experiment was conducted during the login session using different algorithms that include Euclidean distance, Cosine similarity, City block distance and Jaccard distance (figure 3.2).

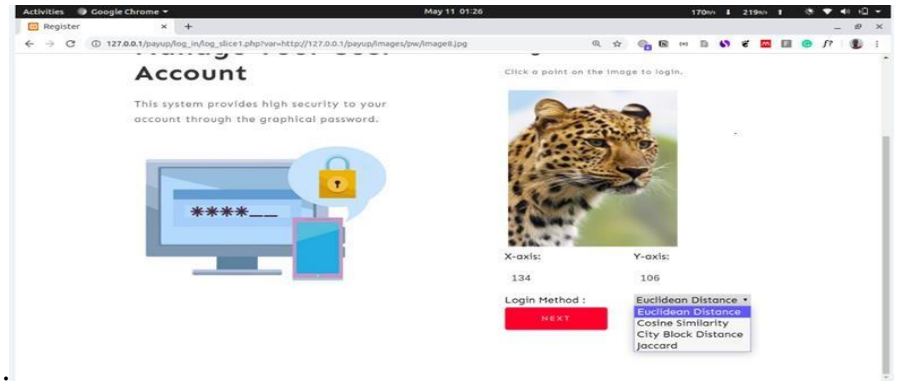


Figure 3.2: Dropdown menu of the various algorithms used during the login sessions.

3.5.1 Euclidean Distance algorithm

The Euclidean distance is the most widely used similarity measure. It has vast applications in image and document retrieval, text matching. The Euclidian distance measures are used to compute the distance between a given vector point and some other vector points save in the database. It determines the root of square differences between the coordinates of a pair of objects (Bora & Gupta, 2014). Euclidean is the distance between two points in a plane or 3D space that measures the length of a segment connecting the two points. For vectors x and y, distance d (x, y) is given by the general equation for Euclidean distance (Ponnmoli, 2014):

$$d = \sqrt{\sum_{i=1}^{\eta} (x_i + y_i)^2} \quad (3.12)$$

Where:

x and y are n-dimensional vectors.

In this work, mathematical equation (3.13) was used to calculate Euclidean distance involving two pair matching points at register and login of *(x1, y1) and (x2, y2)*:

$$d = \sqrt{(x1 - x2)^2 + (y1 - y2)^2} \quad (3.13)$$

Where:

x1, y1 - registered coordinates saved in the database during registration

x2, y2 - login coordinates.

Here the threshold value for Euclidean distance is ≤ 5.

3.5.2 Cosine Similarity

The Cosine Similarity begins by finding the cosine of the two non-zero vectors. The introduction of cosine similarity in this work is to eliminate ambiguous matching results between different vector points such as those obtained during user registration and those from the user login phase. The idea of cosine similarity is to measure the orientation of two vectors. The cosine similarity has been used in many applications including data mining, text matching and document retrieval.

Given two vectors of points, A and B, the cosine similarity, cos(θ), is represented by using a dot product and magnitude as defined in equation (3.14) as the general equation (Bora & Gupta, 2014).

A.B = ||A||.||B|| Cos θ

$$\text{Cos } \theta = \frac{A \,.\, B}{||A||||B||} = \frac{\sum_{i=1}^{n} A_{i*B_i}}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}} \quad (3.14)$$

Where A^2i and B^2i are components of vector points A and B respectively (Similarity *et al.,* 2020).

The value for cosine similarity is less than or equal to one.

In this research work, Cosine similarity was calculated using equation (3.15) as it involves two points as register and login of coordinates *(x1, y1) and (x2, y2).*

$$\text{Cosine Similarity} = \frac{(x1 * y1) + (x2 * y2)}{\sqrt{x1^2} * \sqrt{x2^2} + \sqrt{y1^2} * \sqrt{y2^2}} \quad (3.15)$$

Where parameters:

x1, y1 - registered coordinates saved in the database during registration

x2, y2 - login coordinates.

3.5.3 City Block Distance (Manhattan)

The City Block distance (CBD) is also called the Manhattan distance in an **n-dimensional** vector space with fixed Cartesian coordinates between two vectors X_{sj} and X_{tj} is the sum of the lengths of the line segment projections between the points onto the coordinate axes. The mathematical formula of the city block or the Manhattan distance is given by (4.5):

$$CBD_{st} = \sum_{j=1}^{n} |x_{sj} - x_{tj}| \quad (3.16)$$

Where n is the number of variables, and X_{sj} and Y_{tj} are the values of the j^{th} variables at points x and y respectively (Ponnmoli, 2014).

The city block or Manhattan distance is the simple sum of the horizontal and vertical components, while the diagonal distance is calculated by using the Pythagorean Theorem. For example, if two points u = (x1, y1) and v = (x2, y2) are two points (Malkauthekar, 2013), then the city block distance between u and v is given as:

$$CBD = ||x1 - x2|| + ||y1 - y2|| \quad (3.17)$$

In most cases, the City Block distance is greater than or equal to zero. For identical points, the measurement would be zero, while for points with little similarity, the measurement would be high. The city block distance is used in image processing, visual image tracking, and many machine learning algorithms to measure both horizontal and vertical distances.

Where CB ranges between 0 and 1 but not greater than one.

In this work, City block distance was calculated by using equation (3.18) - Pythagorean Theorem:

$$\mathbf{CBD} = \sqrt{(x1 - x2)^2 + (y1 - y2)^2} \quad (3.18)$$

Where:

x1, y1 - registered coordinates saved in the database during registration.

x2, y2 - login coordinates.

3.5.4 Jaccard Distance Algorithm (JD)

The Jaccard distance calculates similarity by dividing the intersection by the union of the vector points. The Jaccard distance algorithm can be used to compute the similarity between two data sets (Tairi & Abbad, 2016). The general formulae could be stated as:

$$JD = \frac{(x_i.x_j)}{(|x_i|^2 + |x_j|^2 - x_i.x_j} \quad (3.19)$$

Where:

JD refers to the Jaccard distance.

x_i, x_j are n-dimensional vectors.

The range value for the Jaccard distance (JD) is between 0 -1.

Like other algorithms, the Mathematical equation (3.20) was used in this work to calculate Jaccard Distance involving two points at register and login sessions of coordinates (x1, y1) and (x2, y2):

$$\mathbf{JD} = (x1 * y1)\ \frac{(\boldsymbol{x1} * \boldsymbol{y1}) + (\boldsymbol{x2} * \boldsymbol{y2})}{(\boldsymbol{x1} + \boldsymbol{x2}) + (\boldsymbol{y1} + \boldsymbol{y2}) - (\boldsymbol{x1} * \boldsymbol{y1}) + (\boldsymbol{x2} * \boldsymbol{y2})} \qquad (3.20)$$

JD ranges between 0 and 1 but not greater than one

Where:

x1, y1 - registered coordinates saved in the database during registration.

x2, y2 - login coordinates.

JD - threshold value ≤ 1.

Each user has a login coordinate which is cross-referenced with the initial coordinate on registration.

CHAPTER FOUR

4.0 IMPLEMENTATION, EXPERIMENTAL RESULTS AND DISCUSSION

4.1 The System Implementation

System implementation completely involves the assembling and articulating of various components to form the new graphical method and the experimental performance test is carried out on it to see its result. The threshold in this context is a range of value (s) to accommodate bits of error in coordinate selection. In this proposed graphical scheme, each user logs on to the home page and then clicks on register to create an account then fills in their demographic data.

4.1.1 Home Page

Figure 4.1 shows the interface that was used by users to interact with the system while making use of the graphical scheme. Where new users are expected to make registration and existing users are expected to input in their accurate personal information details for authentication.

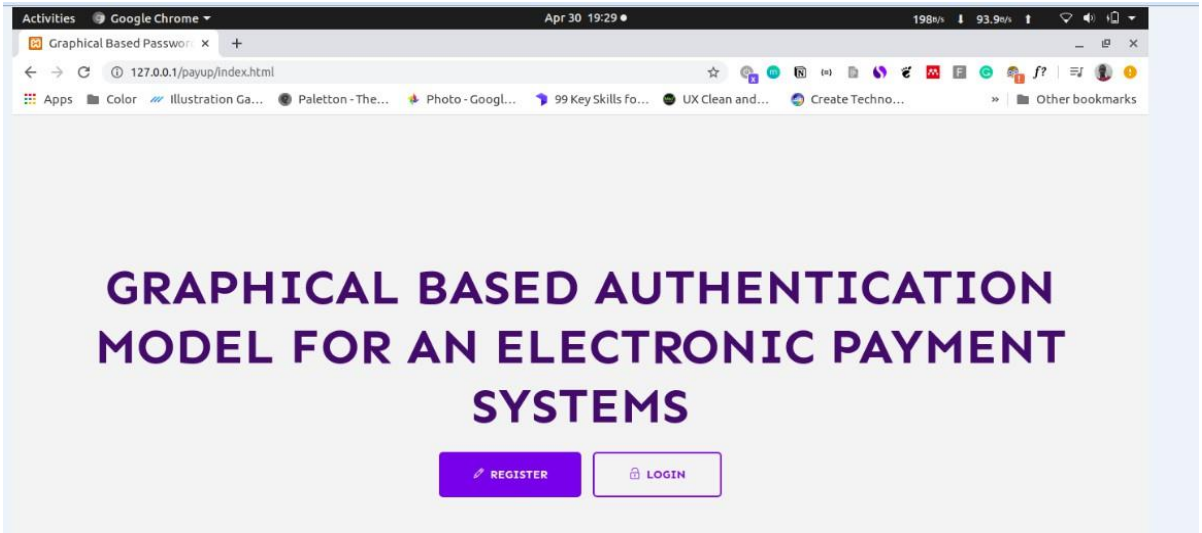


Figure 4.1: Home page Interface of the Graphical Scheme.

4.1.2 Registration Phase

This phase requires the user to enter the personal details into the system and this is the first crucial step to utilise the graphical scheme. For authentication to be possible in a web application, each user needs to create and save the account details in the database.

During the registration phase, the user must click on the registration button as shown in figure 4.1 which leads the user to a page where to fill in personal unique identification details as shown in figure 4.2. On clicking the user Registration button, the system generates a unique user ID known as coordinates. Immediately the user submits personal details and the text password, it will be redirected to the next phase, where the user is required to create a graphical image password and save it in the database.

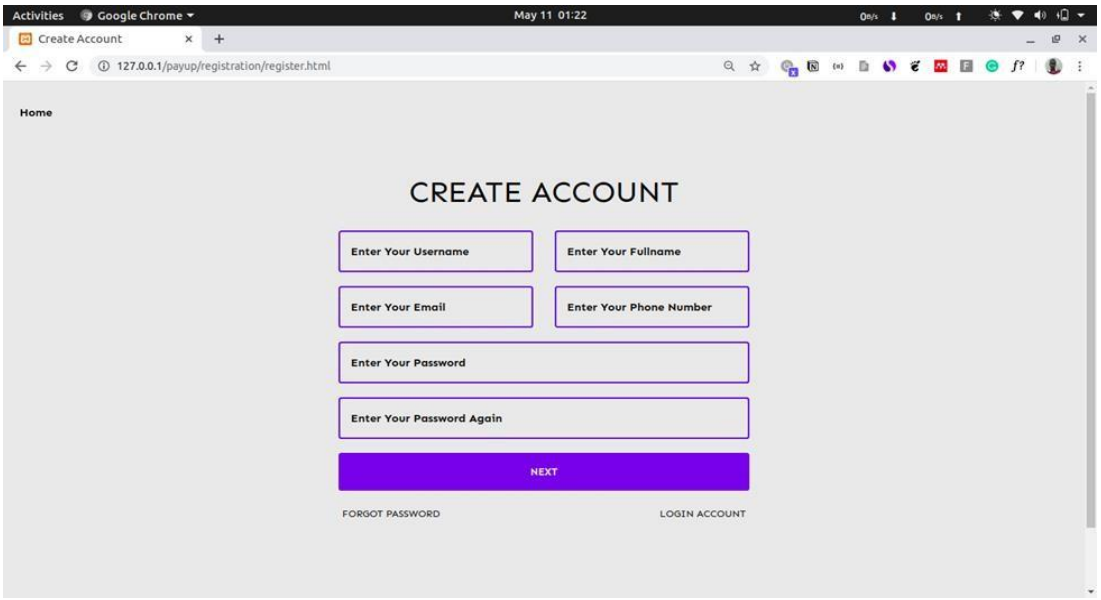


Figure 4.2: Registration Phase

User Identification

In this system, a username which is a vital component of the scheme uniquely identifies the user and serves as the primary key. Two users with the same username cannot be granted access into the system else it sends an error message.

4.1.3 Image Graphical Password Creation

During this phase, the user will be shown a series of images from which to select a password. The images from which the user should select the click points for the accurate login shall be generated at random and presented to the user in an image grid format, as shown in figure 4.3. During the password creation process, the user must select one-click point per image.

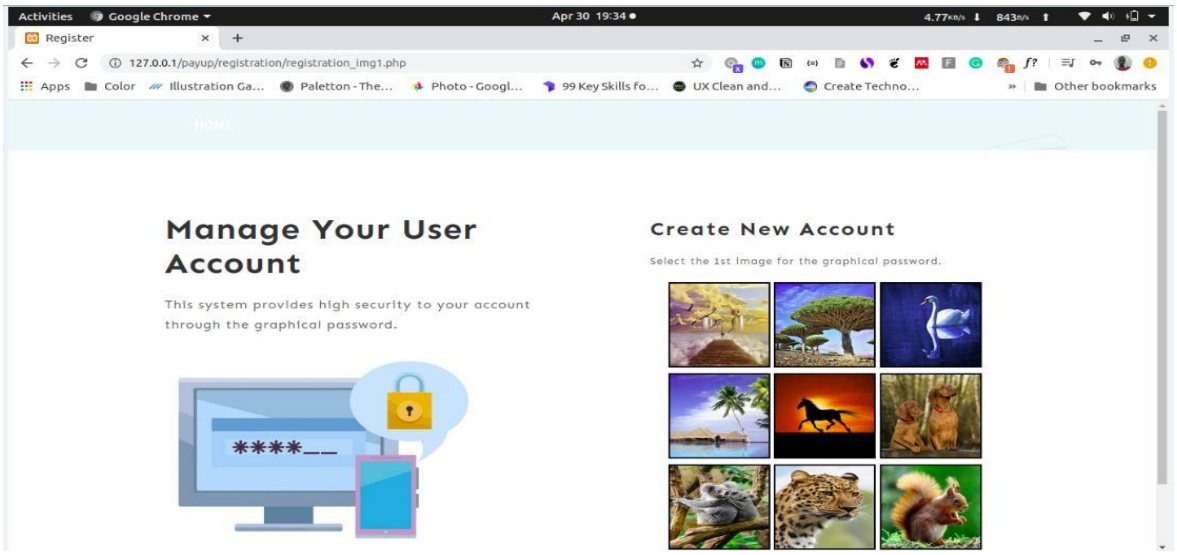


Figure 4.3: A 3x3 grid images display

After the user has entered a username and password, the user will then choose images for the graphical password. This phase involves the following:

(i) The user selects his or her preferred images as a password from the image of figure 4.3 In this scheme three (3) images are considered as shown in figure 4.3 and figures 4.4, 4.5 and 4.6.

(ii) The user clicks on the images in the same sequence as selected.

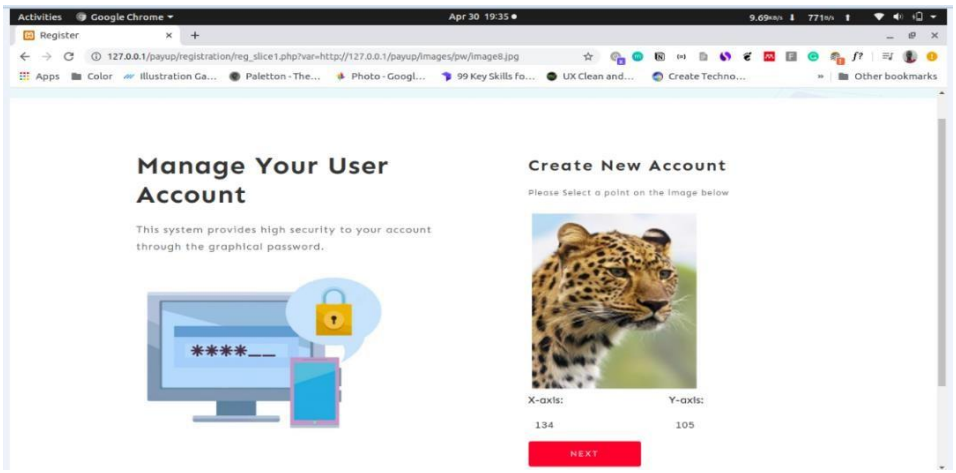


Figure 4.4: The first image used to create a graphical password.

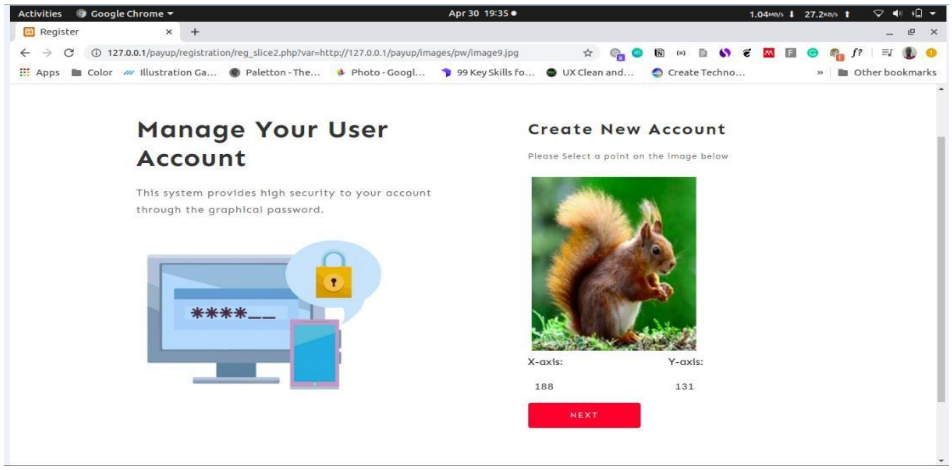


Figure 4.5: Second Image used to create a graphical password

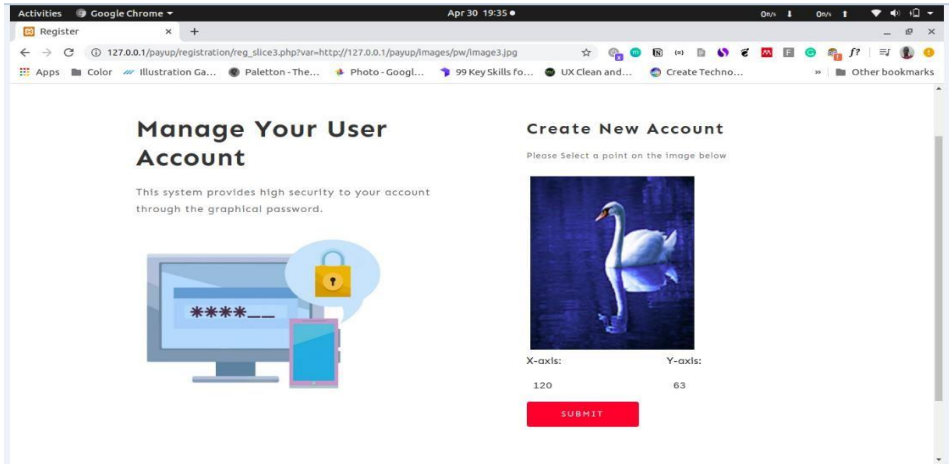


Figure 4.6: The third Image used to create a graphical password.

4.1.4 Login Phase.

In the Login phase as shown in figure 4.7, the user enters the username and textual password to check if the ID is valid or not. If it is valid then the matching images will be displayed. On this image, the user will have to choose click points by using the single click technique.

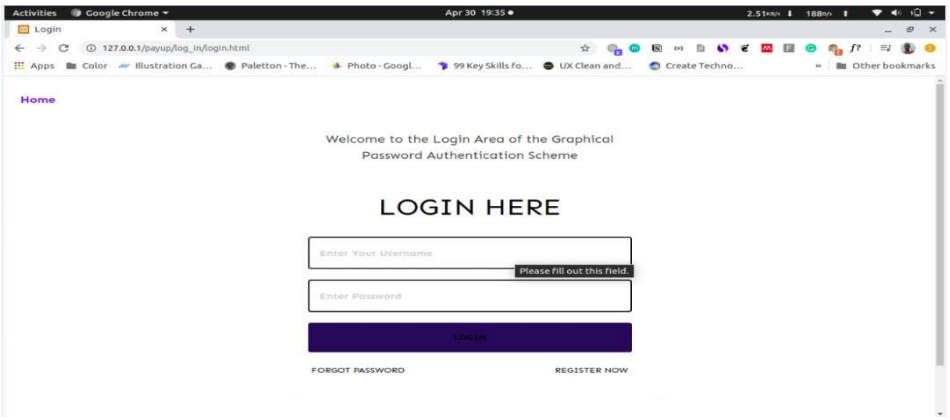


Figure 4.7: Login Phase (Interface)

After a user has successfully registered with the system and the personal details provided by the user are validated or text matched with that in the database to ensure a valid user has been given access. This entirely involves the username and the graphical password. The user will either use Jaccard, City Block, Cosine similarity and Euclidean algorithm to login into the system.

Now following the registration form (figure 4.2) is a set of 3x3 grid images which will serve as the graphical password, each user will select three images in sequence to which would be entered each time in the same sequence to access the E-payment interface. Each image provides a coordinate (x1, y1) on account creation stored in the database.

The user logs in using their respective username and text password followed by their graphical password based on recognition, the users are provided with four algorithms namely, Euclidean Distance, Cosine Similarity, City Block Distance and Jaccard

Distance to which they will select on to login. These algorithms calculate the recognition rate of the scheme used with the containment of minimal error in its threshold.

In this phase, the user must log in with Username and Text Password to view the image grid (Figure 4.8), to be able to go through the exact sequence of click points.

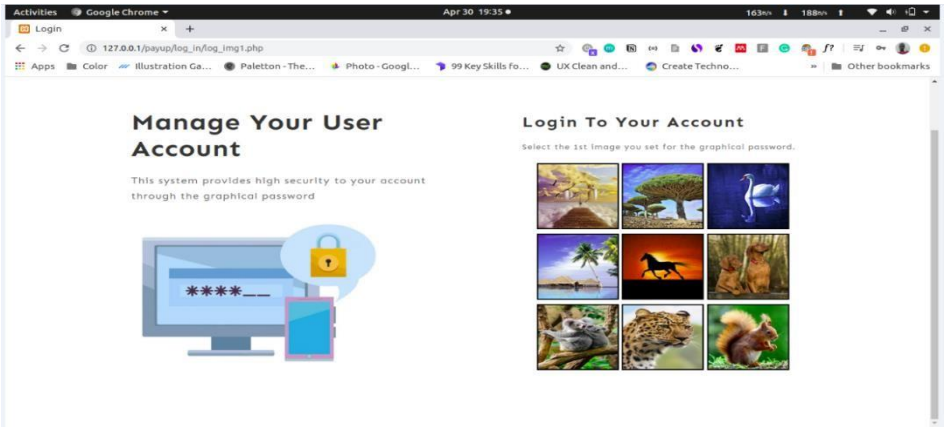


Figure 4.8: A 3x3 Graphical Grid Image Display during the login phase

The user must click on the images that were chosen as the password. The images must be in the same order as they were when the password was created. When the user clicks an image in the 3x3 image grid display of figure 4.8, the image enlarges to provide the user with a larger view of the image. The user can now click on the point chosen as a password when creating the password. The user must repeat the process until all three images have been selected with their respective click-points.

Every image's click-point refers to x-y coordinates. These coordinates are saved in the database with a link to the images selected for each user ID. The user is given the option to select any of the algorithms after clicking on the final image and its click-point. Users are provided with four algorithms in the implemented system.

The following figures were used to login into the graphical scheme in a sequential manner as they were seleted during the graphical password creation: Figure 4.9 is the first

graphical image utilized to login into the account using Euclidean distance algorithm and the login coordinate x2, y2 are generated as the user clicks the valid point on the image.

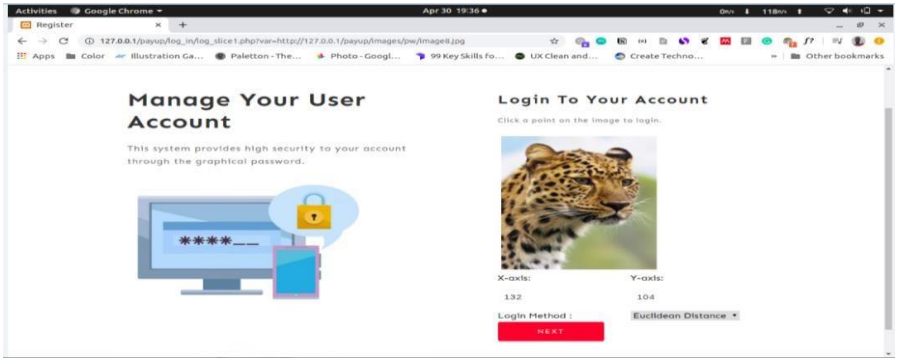


Figure 4.9: The first Image used to login into account with the Euclidean algorithm.

Figure 4.10 is the image used to login into the account. Similarly, Cosine similarity algorithm is used to login into the graphical scheme where login coordinates x2, y2 is also genberated.

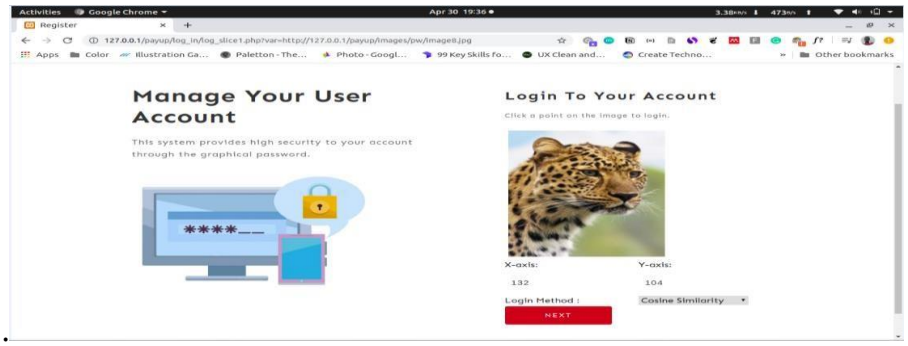


Figure 4.10: Image used to login into account with Cosine similarity algorithms.

Figure 4.11 is the second image used to login to the account. After cliking on the second image the next image is displayed for final cliking.

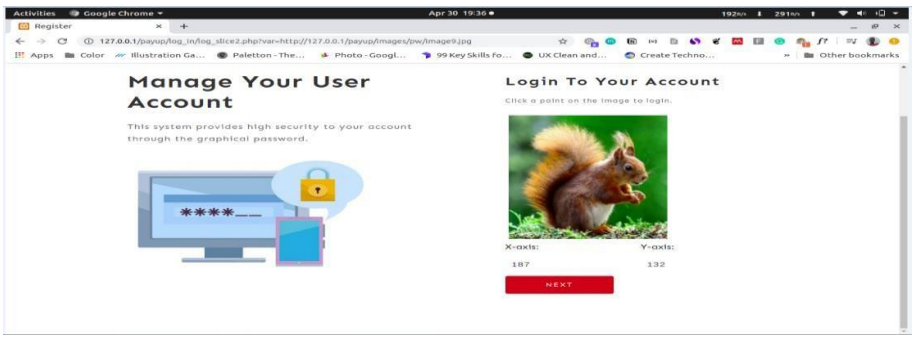


Figure 4.11: The second image used to login to the account.

Figure 4.12 is the third image used to login into the account. After clicking on the final image (the third image) as shown in figure 4.12 and its click-point, the user is given the

freedom to choose any of the distance algorithms. In this scheme, the user is provided with four algorithms namely; Euclidean distance algorithm and Cosine similarity algorithm, City Block distance algorithm and Jaccard distance algorithms.

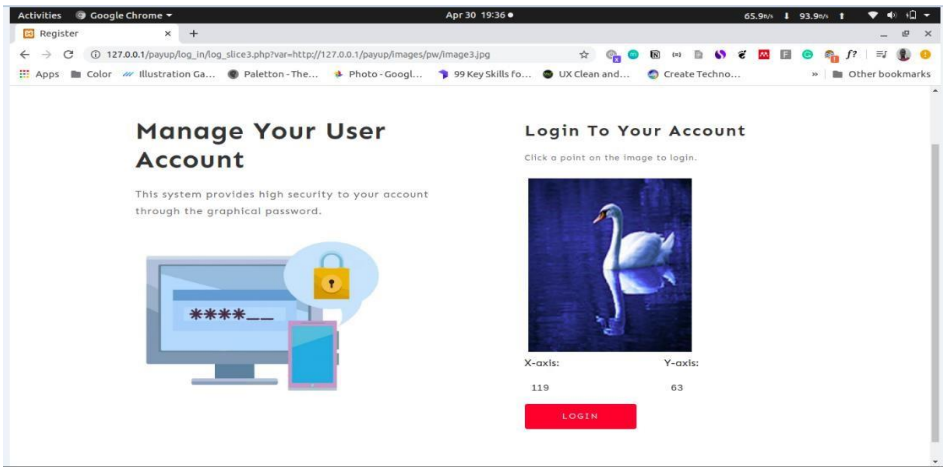


Figure 4.12: The third image used to log in to the account**.**

4.1.5 Electronic Payment Interface (Page)

This phase will display to the user an E-payment login screen where user/client can use their Automated Teller Machine (ATM) cards, Credit card, Smart card and Debit card for transactions. For example, a visa card, verve card can be used to make electronic payments or fund transfers. In this platform, some Card details such as Card number, Card Verification Value (CVV), the valid date will be required to allow effective E-payments or fund transfer (see figures 4.13 and 4.14).

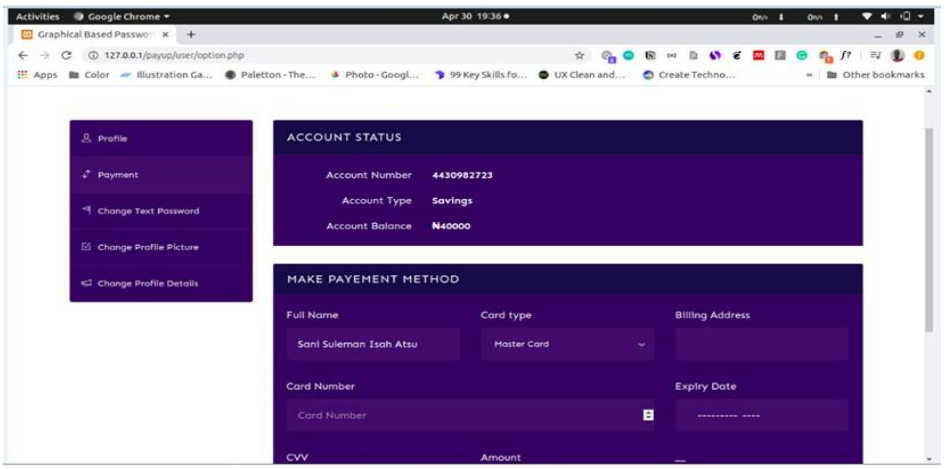


Figure 4.13: Electronic payment interface

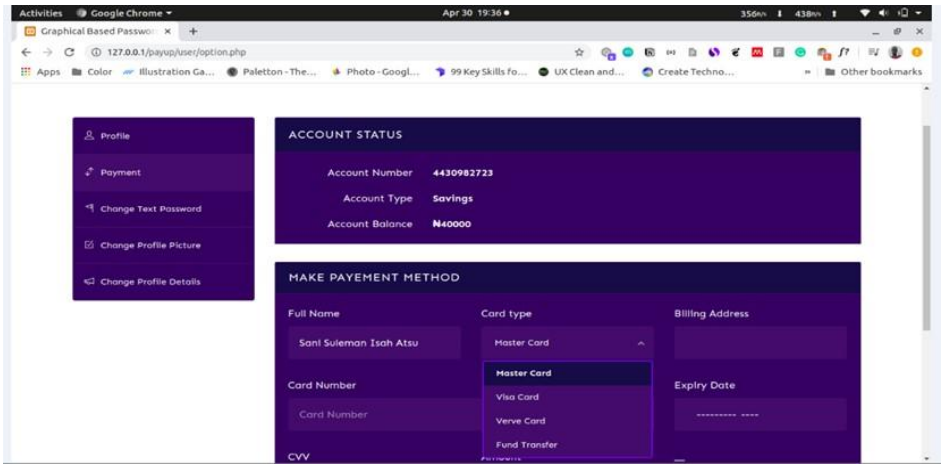
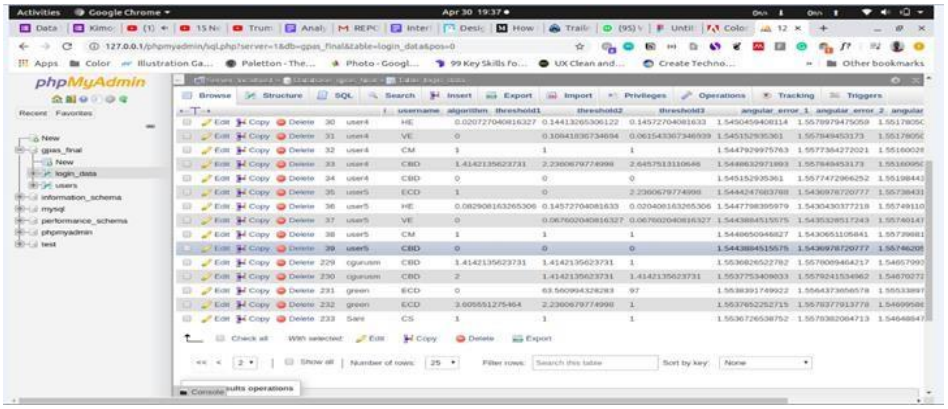


Figure 4.14: E-payment phase and various card types/payment procedures

4.1.6 Implementation of the Database (Server)

Database refers to a relationship that provides tables and other images or objects in an index format. In a database, tables comprise Rows and Columns (see figure 4.15).

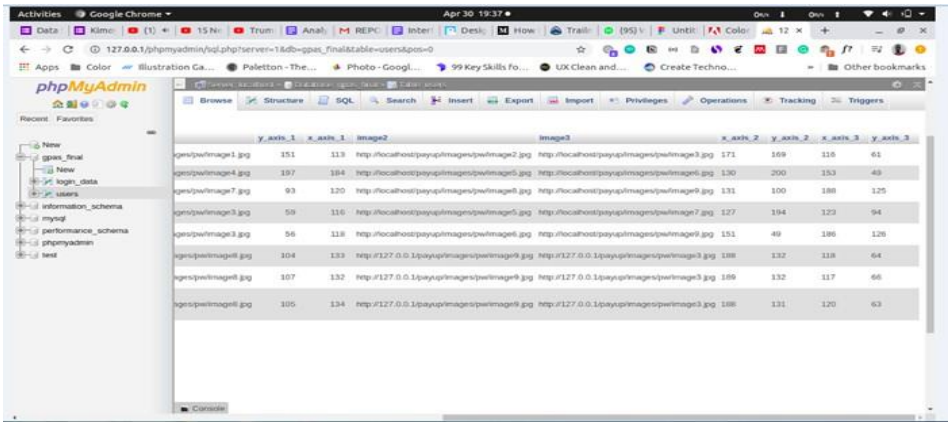


Figures 4.15: database implementation showing login data, algorithms and matching errors.

All the user detail data information such as username, text password, picture images, graphical password, registered and login coordinates are all saved and stored in the database. Database (Server) is being utilized for storing data information purposes. In this graphical scheme, the XAMPP server is used.

This database phase shown in figure 4.15 displays all login data and user's activities, such as login algorithms and matching errors, user unique ID and threshold values while figure

4.16 displays the registered/login coordinates of graphical images and demographic details all in rows and columns.



Figures 4.16: database implementation showing user's registered and login coordinates.

4.2 Experimental Results

This chapter analyzes the performances of all the different algorithms used for the proposed graphical-based authentication model to identify and recommend the most efficient and robust amongst them. To provide a fair and accurate evaluation for all the algorithms, metrics such as the login success rate, execution time and the average matching error are used. In particular, the average matching error in this aspect is very crucial for achieving a high login success rate. While the experiment has no limit as to the number of participants, here an experiment was conducted using five (5) participants (users). Each of these participants was allowed to interact with the system and for every interaction, the performance of each algorithm based on how successful a user can log in into the system, the duration of time it takes to log in and the average matching error between the click points at registration and login stages are evaluated and recorded.

4.3 Login Success Rate

Five (5) participants (users) were selected from the Computer Science Department, Federal University of Technology, Minna. The participants took part in the registration procedure by entering their username, email, phone number and text password. They have

to choose an image password in sequential order and click on the three different images one at a time. Each attempt is reported as either successful or failure. This means that the success rate can be calculated based on the successful login of a user. The result obtained by the participants on successful login is shown in tables 4.1 and 4.2.

Table 4.1: Login Success

	USERS					
ALGORITHM	USER_1	USER_2	USER_3	USER_4	USER_5	**Average**
Euclidean Distance	5	5	4	4	5	4.6
Cosine Similarity	5	5	5	5	5	5
City Block Distance	2	3	2	4	5	3.2
Jaccard Distance	5	5	5	5	5	5

Figure 4.17 shows a 2D graphical bar chart representation of results in table 4.1 as the login success. The bar chart shows that different users are login with algorithms one at a time and both individual login success with their corresponding average success login are recorded. It also shows how each different user is login successfully with different algorithms and the average login success is determined.

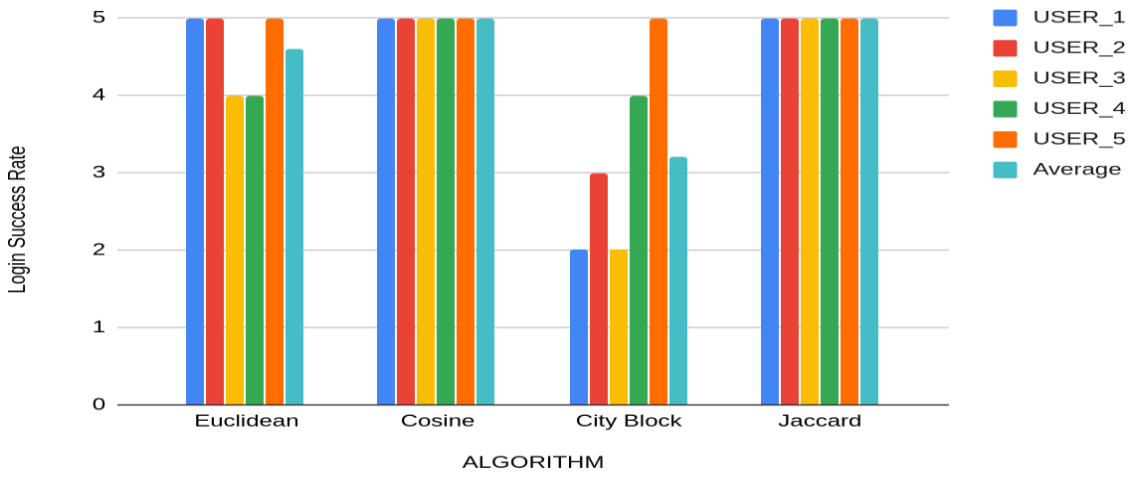


Figure 4.17: Bar Chart for the login success

In table 4.2, the participants' login success rate in percentage is shown. Here the Cosine Similarity and Jaccard distance algorithms gave a 100% login success rate which indicates that they have a higher recognition rate.

Table 4.2: Average Login Success rate in percentage

	USERS					
ALGORITHM	USER_1	USER_2	USER_3	USER_4	USER_5	**Average**
Euclidean Distance	100%	100%	80%	80%	100%	92%
Cosine Similarity	100%	100%	100%	100%	100%	100%
City Block Distance	40%	60%	40%%	80%	100%	64%
Jaccard Distance	100%	100%	100%	100%	100%	100%

Figure 4.18 shows a 3D graphical bar chart representation of results in table 4.2 as the average login success rate in percentage (%) in the Y-axis. The bar chart shows the success login rate of 5 different users that used 4 different algorithms one at a time to log in successfully and their login success rate and average login success rate are determined in percentage (%) in the X-axis.

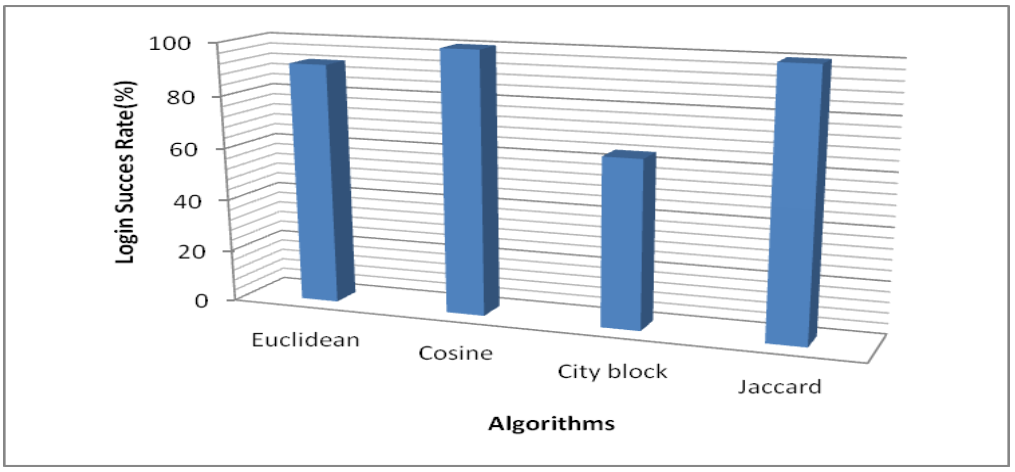


Figure 4.18: The average login success rate in percentage (%) for each user on all the algorithms

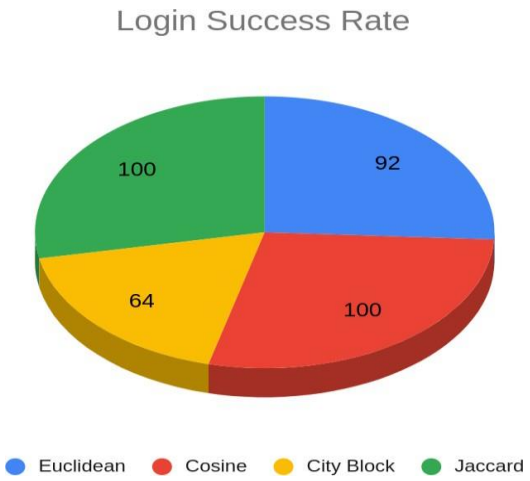


Figure 4.19**: T**he pie chart for Login Success Rate in percentage (%)

From the results shown (see table 4.1, table 4.2, figure 4.17, figure 4.18 and figure 4.19), it is observed that both Cosine Similarity and Jaccard Distance recorded a 100% average login success rate, indicating that they both have a higher recognition rate than Euclidean Distance and City Block Distance.

4.4 Execution Time

In this experiment, the same 5 participants used the four different algorithms: Euclidean, Cosine similarity, City Block distance and Jaccard distance. Here the time taken for execution differs from one algorithm to the other. Every participant is permitted to register and create an image password in sequential order. After this, they can log in to their accounts respectively by utilizing one algorithm at a given time. The execution time is taken from the point each participant (user) clicks on the algorithm from the dropdown menu to submit a password for authentication until the participant views E-payment interface files on successful login. The time taken by the four algorithms allows the data to be retrieved from the database (server) gave the following results.

Table 4.3: Execution Time for algorithms

	USERS					
ALGORITHM	USER_1	USER_2	USER_3	USER_4	USER_5	**Average time**
Euclidean Distance	0.06	0.039	0.07	0.043	0.029	0.0482
Cosine Similarity	0.043	0.025	0.03	0.03	0.067	0.039
City Block Distance	0.036	0.04	0.025	0.026	0.032	0.0318
Jaccard Distance	0.11	0.03	0.21	0.041	0.037	0.0856

Figure 4.20 shows a 2D graphical bar chart representation of the duration of execution time results in table 4.3 as the execution time for algorithms in milliseconds (Y-axis). The graphical bar chart shows how each of the 5 different login users using 4 different algorithms one at a time during the login procedure, to obtained both individual and average execution time of each algorithm in (X-axis).

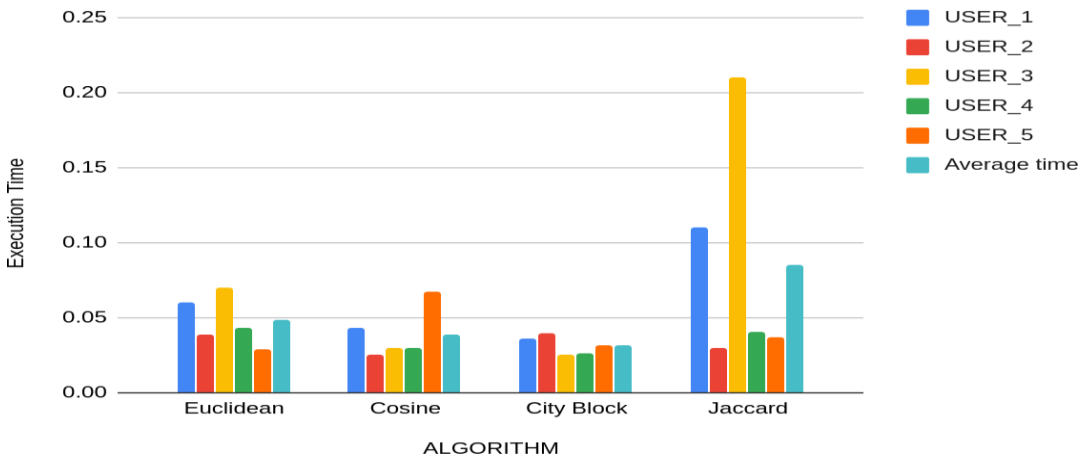


Figure 4.20: Bar Chart of the Execution time for the different users on each algorithm

Figure 4.21 shows a 3D graphical bar chart representation of the duration of execution in table 4.3 as the average execution time in milliseconds (Y-axis) by each algorithm. The bar chart shows how 4 different algorithms are used to the obtained average execution time of each algorithm (X-axis). The graphical bar chart shows outstanding performance by the City Block distance algorithm with the best execution time of 0.0318 milliseconds.

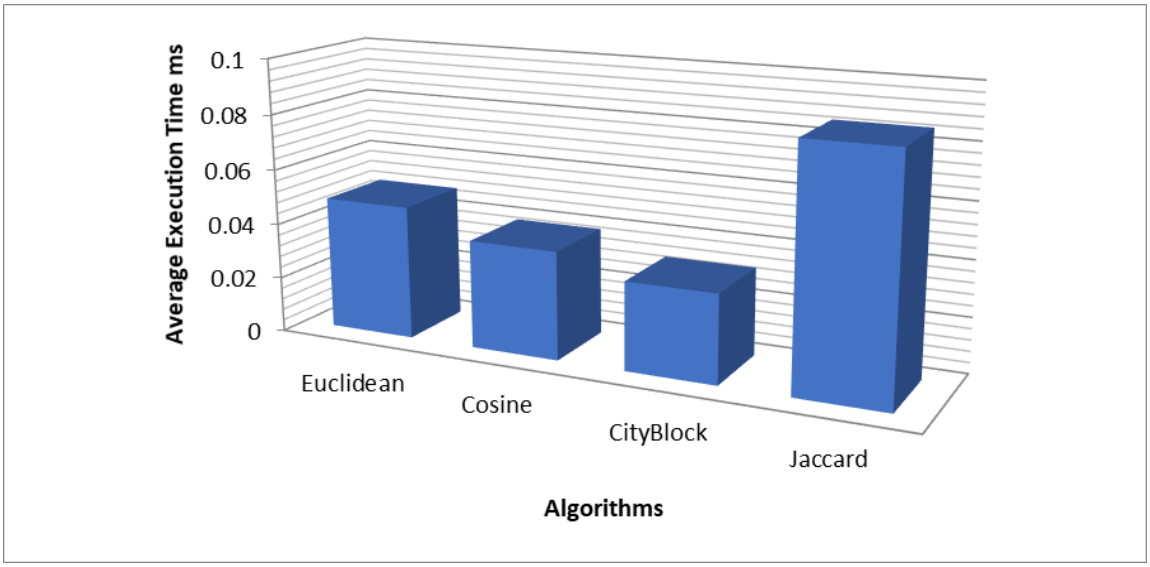


Figure 4.21: Bar chart of the average execution time in milliseconds obtained for the algorithms.

Figure 4.22 shows a pie chart representation of the duration of execution in table 4.3 as the average execution time in milliseconds by each algorithm. The bar chart also shows how 4 different algorithms users used one at a time during the login session to obtain the average execution time of each algorithm.

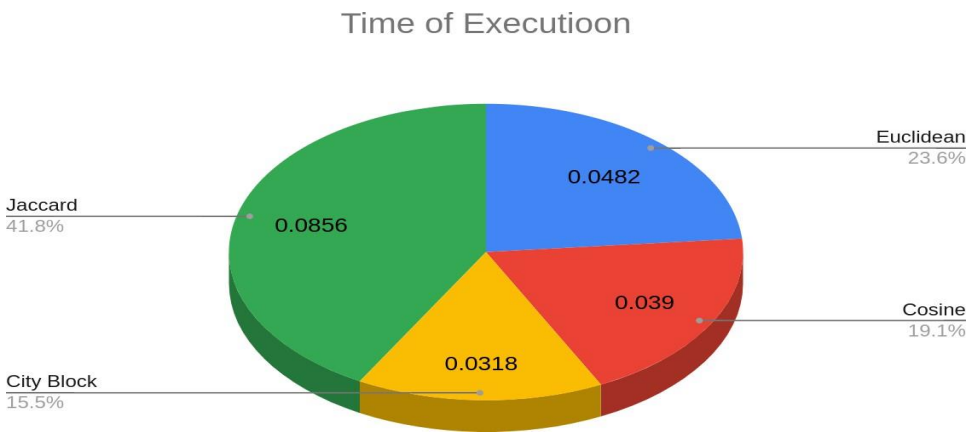


Figure 4.22: Pie Chart of the execution time for the algorithms

In this experiment, it is observed that City Block Distance has the best execution time followed by Cosine Similarity, Euclidian Distance and Jaccard Distance in that order respectively (see table 4.3, figure 4.21 and figure 4.22)**.**

4.5 Matching Errors for the Algorithms

Accuracy is always of the utmost importance in a high-standard performance measure. Compliance and input errors are factors that lead to mechanism matching and positional errors, and in this scheme, registration and login (input) errors are considered the error source. To keep the output error within the desired limits, the login algorithms use tolerance or threshold allocation, which has an effect on the system's dynamic performance.

In this research work, the matching error is taken as one of the standard performance evaluation metrics that gave good accounts of the errors that occurred during the registration process and the login procedures. The matching error gave the error rate of the graphical scheme due to the problem of matching points at the registration and login phase. During the point clicking on the picture images, there are minimal errors, and, in this case, the threshold of each algorithm is considered to minimize the system's matching error. If the matching error is at the minimum point at registration and login time during the matching of the coordinates, then the graphical scheme is robust and reliable. In this scheme, the average matching errors were determined by 5 participants that use four algorithms to register and log in. The algorithms used are; Euclidean distance, Cosine similarity, City Block distance (Manhattan) and Jaccard distance algorithms as shown in table 4.4.

Table 4.4: Average Matching Error of the images clicking point per user login

	USERS					
ALGORITHM	USER1	USER2	USER3	USER4	USER5	**AVERAGE MATCHING ERROR**
Euclidean Distance	1.55341	1.55404	1.55406	1.55162	1.54851	1.55233
Cosine Similarity	1.55342	1.55429	1.55406	1.55137	1.54844	1.55232
City Block Distance	1.55334	1.55408	1.55403	1.55162	1.54850	1.55231
Jaccard Distance	1.55330	1.55407	1.55418	1.55166	1.54887	1.55242

Figure 4.23 shows a 2D graphical bar chart representation of results of matching errors in table 4.4 and as in figure 4.23, the matching error is in (Y-axis). The bar chart shows how each of the 5 different users and 4 different algorithms are used to obtain both individual and average matching errors of each algorithm in (X-axis).

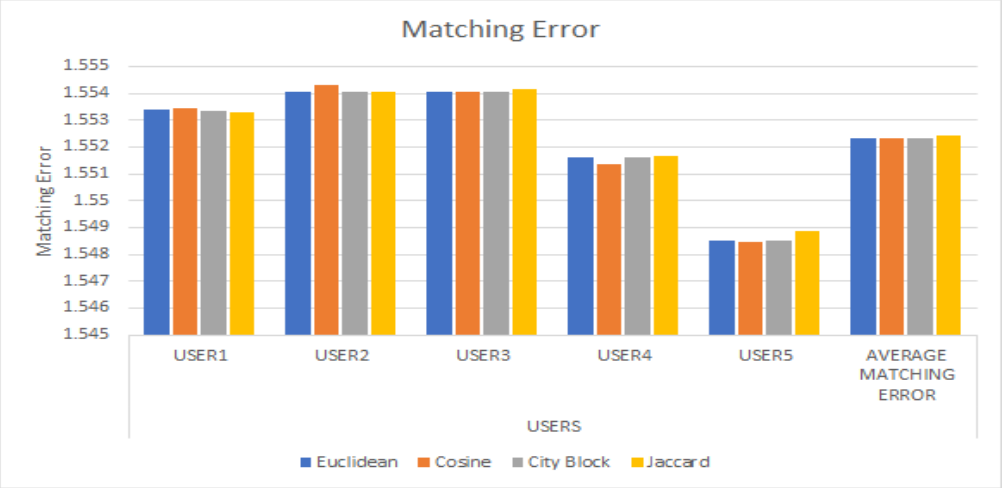


Figure 4.23: Matching error obtained for each algorithm during users' interaction with the system.

Figure 4.24 shows a 3D graphical bar chart representation of results in table 4.4 as the average matching error for each algorithm (Y-axis). The bar chart shows how 4 different algorithms are used to obtain the average matching error for each algorithm (X-axis). The bar chart shows the best performance by the City Block algorithm with an average matching error of 1.55231 during the image click point.

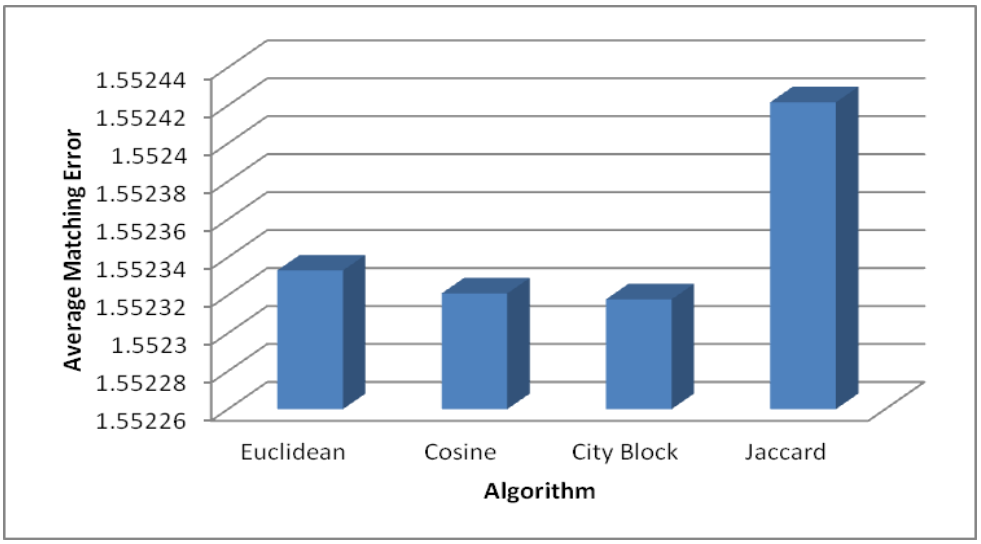


Figure 4.24: Average Matching error obtained for each algorithm during users' interaction with the system.

As can be seen from table 4.4 and figure 4.24, the City Block distance has the lowest matching error (minimum) in comparison to Cosine similarity distance, Euclidean distance and Jaccard distance.

4.6 Discussion of Results

One of the most crucial reasons for introducing similarity measures such as City block distance (CBD), Cosine Similarity (CS) and Jaccard Distance (JD) in this scheme is to analyse results and justify the effective performances of the individual algorithms used in the model (scheme) based on their execution time, login success rate and matching errors. In tables 4.3 and figure 4.21 it is observed that City Block distance has the best average execution time than other algorithms. City block distance has an average execution time value of **0.0318** milliseconds followed by Cosine similarity distance (0.039 milliseconds), Euclidean distance (0.0482 milliseconds) and Jaccard distance (0.0856 milliseconds) respectively. This analysis means that city block distance has the fastest execution time during the login session, and this indicates that the system usability and security could be robust with City block distance in place which conforms with the aims and objectives of this study.

It is also observed that based on login success rate in tables 4.1 and 4.2 and figures 4.17, 4.18 and 4.19, Cosine similarity distance and Jaccard distance have better average login success with values of 5 successive logins each and also average login success values of 5 rated as 100% each, followed by Euclidean distance (4.6) as 92% and City block distance (3.2) rated as 64%. This analysis also means that Cosine Similarity and Jaccard distance performs better than other algorithms during the login session.

As for the matching errors, from table 4.4 and figure 4.23 and 4.24, City Block Distance gave the lowest average matching error of **1.55231**, while Cosine similarity distance has 1.55232, Euclidean distance 1.55233 and Jaccard distance 1.55242 having higher matching error during their interactions with the model (scheme). The results of the matching error obtained for all the algorithms as shown in Figures 4.23 and 4.24 showed that the City Block distance outperformed all the remaining algorithms. This outstanding performance by City Block distance with minimum average error indicates that the system is robust and user-friendly.

Considering the general analysis of the performance results of the individual algorithms used in this graphical scheme (model), it is concluded that the utmost requirement in any computing arena is the consideration for the execution time and minimum error of the system which are paramount for a user-friendly and accurate system. Not only does the City Block performed better in terms of the execution time, but it has also outperformed other algorithms with low matching error in the model. Furthermore, the city block distance has also performed above average with a login success rate of 64%, which is quite within the range of an acceptable result for a system.

The fast execution time and minimum error performances achieved by City Block distance gave it an upper hand in terms of security, usability and robustness of the Model.

This means that if a system is slow in execution time, the users will have to stay much longer time on the system and this can attract attention or could create avenues for hackers to compromise the system or exposes users to Spyware, Internet phishing and Internet surfing attack.

Finally, the analysis of results for the similarity distance algorithms used in this model (scheme) conclude that City Block distance has an outstanding performance in terms of execution time, minimum matching error and its minimum performance in login success rate (above the average of 64%) and so it is recommended as the best algorithm in the model. Table 4.5 gives a detailed comparison of the evaluation performances of the algorithms.

Table 4.5: Comparison of Results for the Evaluation Performance of the algorithms

ALGORITHM	Login Success Rate (LSR)	Average Execution Time (AET)	Average Matching Error (AME)
Euclidean Distance	92%	0.0482 milliseconds	1.55233
Cosine Similarity	100%	0.039 milliseconds	1.55232
City Block Distance	**64%**	**0.0318 milliseconds**	**1.55231**
Jaccard Distance	100%	0.0856 milliseconds	1.55242

CHAPTER FIVE

5.0 SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

The first chapter focuses on the history of the research study on electronic payments, which began in 1918 when the Federal Reserve Bank first transferred currency via telegraph. Electronic payments, despite being designated in 1960, are now widely used due to the evolution of e-commerce and technological advancements. However, the evolution of electronic payment, graphical password authentication and review of other researchers' works were introduced in this research work to study the current security and usability challenges faced by customers/clients when making an electronic payment for goods and services. This chapter further deals with the aim and objectives, scope and significance of the study that includes the benefits derived by the customers/clients. The Statement of the Research Problem as regards the security and usability were spelt out for the proposed research work.

The second chapter presented a review of the literature and related studies that define electronic payment systems as a mechanism that describes how value (usually money) is exchanged for products, services, or information, and that transitioned from traditional methods to modern electronic payment systems. The chapter further enumerates five main types of electronic payment methods such as debit cards, credit cards, electronic cash, pre-paid card and electronic cheque. It reviewed various types of knowledge-based authentication techniques and their vulnerabilities. It also reviewed Graphical authentication password techniques that include Recognition based, Recall based and Hybrid based techniques, their attacks. Merits and the Demerits of electronic payment were discussed. Performance metrics and Distance metric overview is also highlighted.

Chapter three gives detail research methodology for the Proposed Graphical Based Authentication Model (GBAM). The research designed framework on image click point-based Graphical user authentication password for an Electronic Payment (e-payment) System was developed with its four components (interfaces) namely; Registration interface, Login interface and Image password authentication and E-payment interface. The following system research tools were utilized in the proposed graphical authentication scheme: HTML, CSS, PHP, Perl, and MySQL.

Chapter four involves the experimental results of the new proposed graphical-based authentication model. An experiment was conducted with 5 participants to register and login into the model (system). It also analyses the performances of all the different distance measures (algorithms) used for the proposed GBAM to identify and recommend the most efficient and robust amongst them. To achieve a fair and accurate evaluation for all the algorithms, metric such as the login success rate, execution time and the average matching error is utilized. The use of average matching error in this aspect is very crucial for achieving a high login success rate. Each of these participants was allowed to interact with the system and for every interaction, the performance of each algorithm based on how successful a user can log in into the system, the duration of time it takes to log in and the average matching error between the points at registration and login stages are evaluated and recorded.

Chapter five is the concluding part of the research study. It summarizes the entire research work into conclusion, contribution to knowledge, and recommendations for further studies.

5.2 Conclusion

This research study is on the Graphical Based Authentication Model for Electronic Payment Systems (E-payment). The aim and objectives of this study were first, to develop a framework model for a graphical-based authentication system (scheme). The design of the framework was achieved through an extensive and comprehensive study of all the various existing works and their approaches implored in Graphical-based password authentication models (scheme). After the full study of the various approaches in Graphical Authentication Models, a knowledge-based Graphical Authentication Password Schemes (GPAS), methodology approach was proposed.

The second objective is to develop a mathematical model for the graphical-based authentication for an Electronic Payment (e-payment) system. To achieve this, a mathematical model for electronic payment was developed using the framework in the block diagram of figure 3.1 with algorithmic procedures involving various components such as registration, login interface, image password creation authentication, and E-payment interface.

Thirdly, to test the efficiency and performance of the mathematical model developed for the electronic payment system with other existing models and to identify, and recommend the best performing algorithm, all algorithms were subjected to an evaluation process using standard metrics such as execution time, login success, and matching error. The four algorithms were used one at a time to login users into the proposed graphical model (scheme) to determine the most successful login, each login success rate was recorded against each algorithm. Also, the execution time of each of the algorithms was recorded and the fastest algorithm was determined during the experiment. In the final evaluation,

the matching errors that occurred during the registration and login stages were recorded and calculated, and the optimum error was also determined.

Based on these results of the experiments carried out with 5 participants, the City Block distance algorithm shows the best performance both in execution time and minimum matching error. This research work concludes that the City Block distance algorithm outperformed Euclidean distance, Cosine similarity, and Jaccard distance based on its average execution time of **0.0318** milliseconds, average matching error of **1.55231** and also, an acceptable optimal average login success rate of **3.2** rated **64%** was obtained. With this outstanding evaluation performance, City Block distance is therefore recommended as the best performing algorithm in the proposed GPAS Model for Electronic Payment System.

5.3 Contributions to Knowledge

The contributions to knowledge in this research work are as follows:

i. In this research work, a framework model for a graphical-based authentication System (GBAS) was developed.

ii. Mathematical model for graphical-based authentication for electronic payment was developed and similarity scores between the points of registration and login are defined using different distance measure algorithms such as Euclidean, city block, cosine similarity, and Jaccard.

iii. The adoption of city block distance as a similarity measure and the use of matching error as a metric in this graphical-based authentication model (scheme) justifies the robustness and effective performances of the scheme.

5.4 Recommendations

This study successfully designed a research framework scheme that improves memorability, user-friendly, login success, execution time, and matching error. In this study, the proposed graphical password authentication technique gave a fair level of security, usability, and robustness. However, future advanced research and broad studies in graphical authentication schemes are recommended here to achieve higher levels of superiority and much stronger security techniques for authentication, as well as its usefulness.

In addition to future work, it is recommended that future research work on graphical-based authentication should also include training on an operational basis as well as proper education on the usage and ways to select strong and accurate image click points as graphical passwords. It is also recommended that for future research work, at least twenty (20) participants (users) may be used to conduct the experiment and the number of images in 3x3 grid display can be more than the three images selected for graphical image password creation in this work may be small.

REFERENCES

Adepoju, A. S., & Alhassan, M. E. (2010). Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria - A Case Study of Selected Banks in Minna metropolis. *Journal of Internet Banking and Commerce,* 15(2), 1–10.

Ahmad, A., Asif, M., Hanif, M. K., & Talib, R. (2016). Secure Graphical Password Techniques Against Shoulder Surfing and Camera Based Attacks. *International Journal of Computer Science and Information Security (IJCSIS),* 14(10), 8.

Ahmed, A., Aziz, A., & Muneeb, M. (2019). Electronic Payment System: A Complete Guide. *Journal of Multidisciplinary Sciences*, 1(2), 1–17. https://doi.org/10.33888//jms.2019.121

Ahsan, M., & Li, Y. (2017). Graphical Password Authentication Using Images Sequence. *International Research Journal of Engineering and Technology (IRJET),* 4(11), 1824–1832. https://doi.org/10.13140/RG.2.2.29930.82887

Akram, T., Ahmad, V., Haq, I., & Nazir, M. (2017). Graphical Password Authentication. *International Journal of ComputerScience and Mobile Computing,* 6(6), 394–400.

Alsaiari, H., Papadaki, M., Dowland, P. S., & Furnell, S. M. (2014). Alternative Graphical Authentication for Online Banking Environments. *Proceedings of the 2014 Eighth International Symposium on Human Aspects of Information Security and Assurance (HAISA),* 122–136.

Asaolu, T. O., Ayoola, T. J., & Akinkoye, E. Y. (2011). Elecronic Payment System in Nigeria: Implementation, Constraints and Solutions. *Journal of Management and Society,* 1(2), 16–21.

Ashwini, M., & Sreedhar, K. C. (2015). Improved Persuasive Cued Click Points for Knowledge-Based Authentication. *2015 International Journal of Computer Science and Network Security.* 15(11), 95–100.

Atema, V. (2014). E-Commerce Adoption Among Small and Micro Enterprises in Nairobi a Research Project Presented in Partial Fulfillment of the Requirements for the Award of Master of Business Administration(MBA), School of Business of the University of Nairobi. (October).

Awodele Oludele, Olamide, K., & Remo, I. (2017). Shoulder Surfing Resistant Graphical Authentication Scheme for Web Based Applications. *2017 American Journal of Computer Sciences and Applications,* 1(7). DOI: 10.28933/ajcsa-2017-09-1801

Bezhovski, Z. (2016). The Future of the Mobile Payment as Electronic Payment System. *2016 European Journal of Business and Management*, 8(8), 127–132.

Blonder, G. E. (1996). Graphical passwords. I*n Lucent Technologies, Inc., Murray Hill, NJ, U. S.* Patent 5: 559-961, Ed. United States, 1996. https://patents.google.com/patent/US5559961A/en.

Bora, D. J., & Gupta, A. K. (2014). Effect of Different Distance Measures on the Performance of K-Means Algorithm: Experimental Study in Matlab. *2014 International Journal of Computer Science and Information Technologies,* 5(2), 2501–2506.

Computing, M. (2014). Comparative Study of Graphical. *International Journal of Computer Science and Mobile Computing*, 3(9), 361–375.

Deorankar, A. V. (2017). Secure Graphical Authentication System for Web Application. *2017 Paripexindian Journal of Research*, 6(5), 412–413.

Dhamija R. and Perrig, A. (2000). Deja vu: A User Study Using Images for Authentication. *In Proceedings of the 9th Conference on USENIX Security Symposium, USENIX Association,* 2000, vol 9, pp. 4–4. https://dl.acm.org/doi/10.5555/1251306.1251310

Dogo, S. H. (2018). An Improved Map Based Graphical Android Authentication System. *2018 Science World Journal*, 13(1), 23–27.

Durgun, Ö., & Caner, M. (2015). The Effects of Electronic Payments on Monetary Policies and Central Banks. *2015 Procedia - Social and Behavioral Sciences, World Conference on Technology, Innovation and Entrepreneurship*, 195, 680–685. https://doi.org/10.1016/j.sbspro.2015.06.271

Ekeke, E., Ugochukwu, K., & Jusoh, Y. Y. (2013). A Review on the Graphical User Authentication Algorithm : Categories Of Graphical User Authentication Algorithm. *International Journal of Information Processing and Management (IJIPM)*, 4(3), 238–252. https://doi.org/10.4156/ijipm.vol4.issue3.23

Farmand, S., & Zakaria, O. Bin. (2010). Improving Graphical Password Resistant to Shoulder-surfing: Using 4-way Recognition-Based Sequence Reproduction. *2010 2nd IEEE International Conference on Information Management and Engineering (ICIME)*, 1, 644–650. https://doi.org/10.1109/ICIME.2010.5478017

Fatonah, S., Yulandari, A., & Wibowo, F. W. (2018). A Review of E-Payment System in E-Commerce. *Journal of Physics: Conference Series*, 1140(1). https://doi.org/10.1088/1742-6596/1140/1/012033

Georgescu, M. (n.d.). The Emergence Of Electronic Payment Systems For The Growth Of E-Business. *2004 International Symposium Economics and Management of Transformation, SSRN: https://ssrn.com/abstract=903622*

Gokhale, A. S., Vijaya, P., & Waghmare, S. (2016). The Shoulder Surfing Resistant Graphical Password Authentication Technique. *2016 Procedia Computer Science, 7th International Conference on Communication, Computing and Virtualization*, 79, 490–498. https://doi.org/10.1016/j.procs.2016.03.063.

Goldberg, J., Hagman, J., and Saza.wal, V. (2002). Doodling Our Way to Better Authentication. *In Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota,* USA, 2002, pp, 868-869. https://doi.org/10.1145/506443.506639

Google. (2020a). Animal Images. Retrieved August 25, 2020, from Google website: https://www.google.com/search?q=Animal+Images&sxsrf=ALeKk029lC7GQ-cFc2oLyBql6bfKaU1zUg:1624128520313&source=lnms&tbm=isch&sa=X&ved=2ahUKEwik8JacrqTxAhUFCRoKHV7pCCAQ_AUoAXoECAEQAw&biw=1920&bih=937

Google. (2020b). E-commerce Getting Started Guide - Authorize.Net. Retrieved August 31, 2020, from Google website: http://www.authorize.net/solutions/merchantsolutions/onlinemerchantaccount

Hafiz, M. D., Abdullah, A. H., Ithnin, N., & Mammi, H. K. (2008). Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique. *2008 Proceedings - 2nd Asia International Conference on Modelling and Simulation (AICMS)*, 396–403. https://doi.org/10.1109/AMS.2008.136

Istyaq, S., & Saifullah, K. (2016). A New Hybrid Graphical User Authentication Technique based on Drag and Drop Method. *2016 International Journal of Innovative Research in Computer and Communication Engineering*, 4(8). https://doi.org/10.15680/IJIRCCE.2016. 0408138

Jensen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom, R. (2003). Picture Password: A Visual Login Technique for Mobile Devices. *National Institute of Standards and Technology Interagency Report (NISTIR)*, 7030, 2003, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.7030

Joseph, O., & Richard, I. (2015). Electronic Payment System in Nigeria: Its Economic Benefits and Challenges. *2015 Journal of Education and Practice*, 6(16), 56–63.

Kadu, D., & Therese, S. (2017). Different Graphical Password Authentication Techniques. *2017 International Conference On Emanations in Mordern Technology and Engineering (ICEMTE)*, 5(3), 56–58.

Khan, A. (2015). Secure Recognition-Based Graphical Authentication Scheme Using Captcha and Visual Objects. *2015 Computer Engineering Eastern Mediterranea University, Gazimağusa, North Cypru*.

Khan, H. U. (2017). An Assessment of the Impact of Mobile Banking on Traditional Banking in Nigeria. *2017 International Journal of Business Excellence*, 11(4), 446–463. https://doi.org/10.1504/IJBEX.2017.10003308

Khan, M. A., Din, I. U., Jadoon, S. U., Khan, M. K., Guizani, M., & Awan, K. A. (2019). g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices. *2019 IEEE Transactions on Consumer Electronics*, 65(2), 215–223. https://doi.org/10.1109/TCE.2019.2895715

Khan, M. A., Ud Din, I., Jadoon, S. U., Khan, M. K., Guizani, M., & Awan, K. A. (2019). G-RAT | A novel Graphical Randomized Authentication Technique for Consumer Smart Devices. *IEEE Transactions on Consumer Electronics*, 65(2), 215–223. https://doi.org/10.1109/TCE.2019.2895715

Khodadadi, T., Islam, A. K. M. M., Baharun, S., & Komaki, S. (2016). Evaluation of Recognition-Based Graphical Password Schemes in Terms of Usability and Security Attributes. *International Journal of Electrical and Computer Engineering*, 6(6), 2939–2948. https://doi.org/10.11591/ijece.v6i6.11227

Kumar, H., Arohi, S., & Khan, F. U. (2013). Graphical Password Authentication Schemes: Current Status and Key Issues. *International Journal on Engineering Innovative Technology (IJEIT)*, 10(2), 437–443.

Kwadzo, F. A., Adroe, R. K., & Asante, D. M. (2018). Analysis of Electronic Payment Systems in Ghana - A Case Study of Mobile Payment System. *International Journal of Scientific Research and Management*, 6(06), 17–25. https://doi.org/10.18535/ijsrm/v6i6.ec02

Lal, N. A., Prasad, S., & Farik, M. (2016). A Review of Authentication Methods. 2016 *International Journal of Scientific and Technology Research,* 5(11), 246–249.

Lashkari, A. H., Manaf, A. A., Masrom, M., & Daud, M. S. (2011). Security Evaluation for Graphical Password. *2011 International Conference on Digital Information and Communication Technology and Its Applications (DICTAP) 2011, Proceedings, Part I. 166, pp. 431-444. Dijion, France: Springer Heidelberg Dordrecht.*

Lin, C., & Nguyen, C. (2011). Exploring e-payment adoption in Vietnam and Taiwan. *Journal of Computer Information Systems,* 51(4), 41–52. https://doi.org/10.1080/08874417.2011.11645500

Mahore, T. R. (2017). Secure Graphical Password Scheme. *2017 International Journal of Research Publications in Engineering and Technology (IJRPET),* 3(3), 144–147.

Malkauthekar, M. D. (2013). Analysis of Euclidean Distance and Manhattan Distance Measure in Face Recognition. *IET Third International Conference on Computational Intelligence and Information Technology (CIIT),* 503-507. doi:10.1049/cp.2013.2636

Masihuddin, M., Ul, B., Khan, I., Ul, M. M., & Mattoo, I. (2017). A Survey on E-Payment Systems : Elements, Adoption, Architecture, Challenges and Security Concepts. *Indian Journal of Science and Technology,* 10(20). https://doi.org/10.17485/ijst/2017/v10i20/113930

Mathur, H., & Lokhande, V. (2017). Improved Pass-Matrix for Graphical Authentication. *2017 International Journal of Advanced Research in Computer and Communication Engineering,* 6(2), 140–143. https://doi.org/10.17148/IJARCCE.2017.6232

Mayuri, G. M., Krishna, S. V., & Tech, M. (2013). Graphical Based Secure Authentication System for Online Applications. *International Journal of Computer Trends and Technology (IJCTT),* 4(8), 2868–2872.

Mihajlovic, M. & Xiong, N. (2019). Finding the Most Similar Textual Documents Using Case-Based Reasoning. *Cornell University*. https://arxiv.org/abs/1911.00262

Mohammad, E., & Maria, A. (2018). An Improved Authentication Scheme Based on Graphical Passwords. *2018 International Conference on Innovative Computing, Information and Control,* 2(8), 775-783. https://doi.org/10.24507/icicel.12.08.775.

Mushkudiani, N. (2019). Development of Electronic Payments in Georgia. *Journal of Economics and Culture,* 15(2), 64–74. https://doi.org/10.2478/jec-2018-0021

Okon, A. N. (2018). Mobile Banking Transactions and Bank Profitability in Nigeria. *International Journal of Economics, Commerce and Management,* 6(6), 692–716.

Oney, E., Guven, G. O., & Rizvi, W. H. (2017). The Determinants of Electronic Payment systems Usage from Consumers' Perspective. *Journal on Economic Research-Ekonomska Istrazivanja,* 30(1), 394-415. http://doi.org/10.1080/1331677X.2017.1305791

Osunade, O., Oloyede, I. A., & Azeez, T. O. (2019). Graphical User Authentication System Resistant to Shoulder Surfing Attack. *Advances in Research*, 19(4), 1–8. https://doi.org/10.9734/AIR/2019/v19i430126

Pant, S. (2011). A Secure Online Payment System. *University of Kentucky UK, Journal on Computer Science. 1, Retrieved August 25, 2020, Google website.* https://uknowledge.uky.edu/cs_etds/1

Paytech, T., & Series, R. (2017). Digital payments in education Saving time for better outcomes. *2017Journal Article on The Paytech Revolution Series*.

Pexels. (2020). animals. Retrieved August 25, 2020, from Pexels website: https://www.pexels.com/search/animals

Ponnmoli, K. M. (2014). Analysis of Face Recognition using Manhattan Distance Algorithm with Image Segmentation. *2014 International Journal of Computer Science and Mobile Computing*, 3(7), 18–27.

Rathanavel, V. (2017). Graphical Password as an OTP. *International Journal of Engineering and Computer Science*, 6(1), 1–6. https://doi.org/10.18535/ijecs/v6i1.41

Razvi, S. A. (2017). Implementation of Graphical Passwords in Internet Banking for Enhanced Security. *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, 35-41. DOI: 10.1109/ICCONS.2017.8250743

Ritu, K., Singh, R. R., & Kumar, B. (2015). Comparative Analysis of Recall-based (Drawmetric) and Click-based (Locimetric) Graphical Password Authentication Schemes. *2015 International Journal of Computer Science and Information Technologies*, 6(2), 1573-1577.

Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. *Electronic Commerce Research and Applications*, 19, 33–43. https://doi.org/10.1016/j.elerap.2016.07.001

Ryan, D., Media, U. S., & Gabay, J. (2016). Praise for Digital Marketing Strategy. 1-339. https://lccn.loc.gov/2016007169

Saranya, P., & Sharavanan, S. (2017). Authentication Scheme for Session Passwords Using Color and Image. *2017 International Journal on Smart Sensing and Intelligent Systems*, 9, 590–603. DOI:10.21307/ijssis-2017-272

Sepideh, F. (2019). Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing, Smudge and Brute Force Attack. World Academy of Science, Engineering and Technology, *International Journal of Computer and Information Engineering*, 13(12), 616–620. https:// doi.org/10.5281/zenodo.3593252

Shah, M., Naik, R., Mullakodi, S., & Chaudhari, S. (2018). Comparative Analysis of Different Graphical Password Techniques for Security. *2018 International Research Journal of Engineering and Technology (IRJET)*, 5(4), 1873–1877

Sharifi, E., & Shamsi, M. (2014). Evaluate the Security and Usability of Graphical Passwords. *2014 International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, 3(8).

Shutterstock. (2020). Animal Images. Retrieved August 25, 2020, from shutterstock website: https://www.shutterstock.com/images

Similarity, J., Algorithm, C., Vector, D., Distance, M., Measure, P., Score, S., & Han, J. (2020). Cosine Similarity. 1, 1–22.

Simon B., Scharstein, D., Roth, S., Black, M. J., & Szeliski, R. (2011). A Database and Evaluation Methodology for Optical Flow. *2011 International Journal of Computer Vision,* 92(1), 1–31. https://doi.org/10.1007/s11263-010-0390-2

Sun, H., Chen, S., Yeh, J., & Cheng, C. (2016). Authentication System. *Transactions on Dependable and Secure Computing,* 5971(c). https://doi.org/10.1109/TDSC.2016.2539942

Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2018). A Shoulder Surfing Resistant Graphical Authentication System. *IEEE Transactions on Dependable and Secure Computing*, 15(2), 180–193. https://doi.org/10.1109/TDSC.2016.2539942

Suru, H. U., & Murano, P. (2019). Security and User Interface Usability of Graphical Authentication Systems - A Review. *2019 International Journal of Computer Trends and Technology (IJCTT)*, 67(2). https://doi.org/10.14445/22312803/IJCTT-V67I2P104

Tairi, H., & Abbad, A. (2016). Combining Jaccard and Mahalanobis Cosine Distance to Enhance the Face Recognition Rate. *Journal of Wseas Transactions on Signal Processing*, 12, 171–178. E-ISSN: 2224-3488

Thirunavukkarasu, M. (2017). An Improving Method of Grid Graphical Password Authentication System. *International Journal of Engineering Research and Applications*, 07(05), 40–43. https://doi.org/10.9790/9622-0705044043

Veerasekaran, Ms S., Khade., A. Gaikwad V.B. (2015). Using Persuasive Technology In Click Based Graphical Passwords. 2015 *International Journal of Technical Research and Applications,* 31(31), 29-36.

Wazir, W., Khattak, H. A. L. I., Member, S., Almogren, A., Member, S., Khan, M. A. L. I., Member, S. (2020). Doodle-Based Authentication Technique Using Augmented Reality. *IEEE Acces Journal*, 7. 1-13. DOI:10.1109/ACCESS.2019.2963543

Yesseyeva, E., Yesseyev, K., Abdulrazaq, M. M., Lashkari, A. H., & Sadeghi, M. (2016). Tri-Pass: A New Graphical User Authentication Scheme. *International Journal of Circuits, Systems and Signal Processing,* 8, 61-67.

Zabidi, N. S., Norowi, N. M., & Rahmat, R. W. O. K. (2019). On the Use of Image and Emojis in Graphical Password Application. *2019 International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8(8), 379–385.

Zimmermann, V., & Gerber, N. (2020). The Password is Dead, Long Live the Password – A Laboratory Study on User Perceptions of Authentication Schemes. *2019 International Journal of Human-Computer Studies,* 133(2020), 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006

APPENDIX: SOURCE CODE:

Source code Snippet for Euclidean Distance, Cosine Similarity, City Block Distance and Jaccard Distance Algorithms

```
$result = mysqli_query($con,"select image1,y_axis_1,x_axis_1,image2,y_axis_2,x_axis_2,image3,y_axis
_2,x_axis_3,y_axis_3 from users where username='$name'");
$row=mysqli_fetch_assoc($result);
 $h1 = $row['x_axis_1'];
 $k1 = $row['y_axis_1'];
 $h2 = $row['x_axis_2'];
 $k2 = $row['y_axis_2'];
 $h3 = $row['x_axis_3'];
 $k3 = $row['y_axis_3'];
if ($type == "ECD"){

                $start_time = microtime(TRUE);
                $r1 = sqrt(pow(($h1 - $x1 ),2) + pow(($k1 - $y1 ),2));
                $r2 = sqrt(pow(($h2 - $x2 ),2) + pow(($k2 - $y2 ),2));
                $r3 = sqrt(pow(($h3 - $x3 ),2) + pow(($k3 - $y3 ),2));
                $e1 = acos((($x1 + $h1) + ($y1 + $k1) + 1) / (sqrt(pow(($y1),2) + pow(($k1),2)+1) *  sqrt(po
w(($x1),2) + pow(($h1),2)+1)));
                $e2 = acos((($x2 + $h2) + ($y2 + $k2) + 1) / (sqrt(pow(($y2),2) + pow(($k2),2)+1) *  sqrt(po
w(($x2),2) + pow(($h2),2)+1)));
                $e3 = acos((($x3 + $h3) + ($y3 + $k3) + 1) / (sqrt(pow(($y3),2) + pow(($k3),2)+1) *  sqrt(po
w(($x3),2) + pow(($h3),2)+1)));
                if($row['image1']==$layer1 && $row['image2']==$layer2 &&          $row['image3']==$lay
er3 && $r1 <= 5 && $r2 <= 5 && $r3 <= 5){
                   $end_time = microtime(TRUE);
                   $time_taken = ($end_time - $start_time)*1000;
                   $t3 = round($time_taken,5);
                   $t = $t4 + $t3;
                   $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3, matching_error_1, matching_error_2, matching_error_3,time,failed_attempt)
                   VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t','$attempt')");
            if ($query){
                    header('Location:../user/user_profile.php');  }
            else {
                   $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thr
eshold2,threshold3, matching_error_1, matching_error_2, matching_error_3,time,failed_attempt)
                   VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                   header('Location:invalid_textpw.html');
                   $_SESSION['selectagain']=1;  }}
      else {
                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3 matching,_error_1, matching _error_2, matching_error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                header('Location:invalid_textpw.html');
                $_SESSION['selectagain']=1;}}
//ECD
//Cosine Similarly
else if ($type == "CS"){
                $start_time = microtime(TRUE);
                $r1  = (($h1 * $x1) + ($k1 * $y1))/ (sqrt(pow(($h1),2)) * sqrt(pow(($x1),2))  +  sqrt(pow(($k
1),2)) * sqrt(pow(($y1),2))) ;
                $r2  = (($h2 * $x2) + ($k2 * $y2))/ (sqrt(pow(($h2),2)) * sqrt(pow(($x2),2))  +  sqrt(pow(($k
2),2)) * sqrt(pow(($y2),2))) ;
                $r3    = (($h3 * $x3) + ($k3 * $y3))/ (sqrt(pow(($h3),2)) * sqrt(pow(($x3),2))  +  sqrt(pow(($
k3),2)) * sqrt(pow(($y3),2))) ;
```

```
            $e1 = acos((($x1 + $h1) + ($y1 + $k1) + 1) / (sqrt(pow(($y1),2) + pow(($k1),2)+1) *  sqrt(po
w(($x1),2) + pow(($h1),2)+1)));
            $e2 = acos((($x2 + $h2) + ($y2 + $k2) + 1) / (sqrt(pow(($y2),2) + pow(($k2),2)+1) *  sqrt(po
w(($x2),2) + pow(($h2),2)+1)));
            $e3 = acos((($x3 + $h3) + ($y3 + $k3) + 1) / (sqrt(pow(($y3),2) + pow(($k3),2)+1) *  sqrt(po
w(($x3),2) + pow(($h3),2)+1)));
            if($row['image1']==$layer1 && $row['image2']==$layer2 &&        $row['image3']==$lay
er3 && $r1 <= 1 && $r2 <= 1 && $r3 <= 1){
              $end_time = microtime(TRUE);
              $time_taken = ($end_time - $start_time)*1000;
              $t3 = round($time_taken,5);
              $t = $t4 + $t3;
              $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3, matching_error_1,matching_error_2, matching_error_3,time,failed_attempt)
              VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t','$attempt')");
          if ($query){
                header('Location:../user/user_profile.php');}
          else {
                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thr
eshold2,threshold3,angular_error_1, matching_error_2, matching_error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                header('Location:invalid_textpw.html');
                $_SESSION['selectagain']=1;  }}
    else {
            $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3,angular_error_1, matching_error_2, matching_error_3,time,failed_attempt)
            VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
            header('Location:invalid_textpw.html');
            $_SESSION['selectagain']=1;}}

//City Block Distance
else if ($type == "CBD"){
            $start_time = microtime(TRUE);
            $r1  = sqrt(abs(($h1 - $x1) + ($k1 - $y1)));
            $r2  = sqrt(abs(($h2 - $x2) + ($k2 - $y2)));
            $r3  = sqrt(abs(($h3 - $x3) + ($k3 - $y3)));
            $e1 = acos((($x1 + $h1) + ($y1 + $k1) + 1) / (sqrt(pow(($y1),2) + pow(($k1),2)+1) *  sqrt(po
w(($x1),2) + pow(($h1),2)+1)));

            $e2 = acos((($x2 + $h2) + ($y2 + $k2) + 1) / (sqrt(pow(($y2),2) + pow(($k2),2)+1) *  sqrt(po
w(($x2),2) + pow(($h2),2)+1)));
            $e3 = acos((($x3 + $h3) + ($y3 + $k3) + 1) / (sqrt(pow(($y3),2) + pow(($k3),2)+1) *  sqrt(po
w(($x3),2) + pow(($h3),2)+1)));
            if($row['image1']==$layer1 && $row['image2']==$layer2 &&        $row['image3']==$lay
er3 && $r1 <= 1 && $r2 <= 1 && $r3 <= 1){
              $end_time = microtime(TRUE);
              $time_taken = ($end_time - $start_time)*1000;
              $t3 = round($time_taken,5);
              $t = $t4 + $t3;

              $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3, matching_error_1, matching_error_2, matching_error_3,time,failed_attempt)
              VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t','$attempt')");
          if ($query){
                header('Location:../user/user_profile.php');  }
          else {
                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thr
eshold2,threshold3, matching error_1, matching_error_2, matching_error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                header('Location:invalid_textpw.html');
```

```
                    $_SESSION['selectagain']=1;}}
      else {
                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3, matching _error_1 matching,_error_2, matching_error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                header('Location:invalid_textpw.html');
                $_SESSION['selectagain']=1;}}
//Jaccard Distance
else if ($type == "JA"){
            $start_time = microtime(TRUE);

            $r1  = (abs((($h1 + $x1) + ($k1 + $y1)) - (($h1 * $k1) + ($x1 * $y1)))/ abs((($h1 * $k1) + ($
x1 * $y1))));
             $r2  = (abs((($h2 + $x2) + ($k2 + $y2)) - (($h2 * $k2) + ($x2 * $y2)))/ abs((($h2 * $k2) +
($x2 * $y2))));    $r3  = (abs((($h3 + $x3) + ($k3 + $y3)) - (($h3 * $k3) + ($x3 * $y3)))/ abs((($h3 * $k3)
+ ($x3 * $y3))));
            $e1 = acos((($x1 + $h1) + ($y1 + $k1) + 1) / (sqrt(pow(($y1),2) + pow(($k1),2)+1) *  sqrt(po
w(($x1),2) + pow(($h1),2)+1)));

            $e2 = acos((($x2 + $h2) + ($y2 + $k2) + 1) / (sqrt(pow(($y2),2) + pow(($k2),2)+1) *  sqrt(po
w(($x2),2) + pow(($h2),2)+1)));

            $e3 = acos((($x3 + $h3) + ($y3 + $k3) + 1) / (sqrt(pow(($y3),2) + pow(($k3),2)+1) *  sqrt(po
w(($x3),2) + pow(($h3),2)+1)));
            if($row['image1']==$layer1 && $row['image2']==$layer2 &&          $row['image3']==$lay
er3 && $r1 <= 1 && $r2 <= 1 && $r3 <= 1){
                $end_time = microtime(TRUE);
                $time_taken = ($end_time - $start_time)*1000;
                $t3 = round($time_taken,5);
                $t = $t4 + $t3;


                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3, matching _error_1, matching _error_2, matching _error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t','$attempt')");
            if ($query){header('Location:../user/user_profile.php');}
            else {
                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thr
eshold2,threshold3, matching _error_1, matching _error_2, matching _error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                header('Location:invalid_textpw.html');
                $_SESSION['selectagain']=1;}}
      else {
                $query = mysqli_query($con,"insert into login_data(username,algorithm,threshold1,thresh
old2,threshold3, matching _error_1, matching _error_2, matching _error_3,time,failed_attempt)
                VALUES('$name','$type','$r1','$r2','$r3','$e1','$e2','$e3','$t4','1')");
                header('Location:invalid_textpw.html');
                $_SESSION['selectagain']=1;}}
?>
```

Source Code Snippet for E-payment Interface

```
<?php
$message = "";
require_once ('db.php');
if (isset($_POST['pay'])){
   $fullname = mysqli_escape_string($con,$_POST['fullname']);
   $cc = mysqli_escape_string($con,$_POST['cc']);
   $exp = mysqli_escape_string($con,$_POST['exp']);
   $cvv = mysqli_escape_string($con,$_POST['cvv']);
   $pricel = $price;
   $item  = $title;
   $itemid = $id;
   $transactionid =  rand(00000,999999999999999);
   $date = date("l jS \of F Y h:i:s A");

   $sql = "INSERT INTO transactions(Transaction_Id,Card_No,CVV,Expiry_Date,fullname,Amount,Ite
m,itemId,date_)
                              VALUES('$transactionid',
                              '$cc',
                              '$cvv',
                              '$exp',
                              '$fullname',
                              '$pricel',
                              '$item',
                              '$itemid',
                              '$date')";
   $query = mysqli_query($con,$sql);
     if ($query){
  echo '<script type="text/javascript">
  window.location= "anim.php?t='.$transactionid.'";
</script>';
}
else{ echo 'failed';}}

ob_end_flush();
  ?>
```

Source Code Snippet for registration Interface

```
<?php

session_start();
ob_start();

include('db.php');
$name=$_SESSION['a'][0];
$passwords=$_SESSION['a'][1];
$realname=$_SESSION['a'][2];
$email=$_SESSION['a'][3];
$phone_no=$_SESSION['a'][4];
$image1=$_SESSION['a'][5];
$y_axis=$_SESSION['a'][6];
$x_axis =$_SESSION['a'][7];

$image2=$_SESSION['a'][8];
$y_axis_2=$_SESSION['a'][9];
$x_axis_2 =$_SESSION['a'][10];

$image3=$_SESSION['a'][11];
$y_axis_3=$_SESSION['a'][12];
$x_axis_3 =$_SESSION['a'][13];

$userimages = "../user/images/user/default.png";
//
$query="INSERT INTO users(username,password,name,email,phone,image1,y_axis_1,x_axis_1,image2,
y_axis_2,x_axis_2,image3,y_axis_3,x_axis_3,userimage)
VALUES(
'$name',
'$passwords',
'$realname',
'$email',
'$phone_no',
'$image1',
'$y_axis',
'$x_axis',
'$image2',
'$y_axis_2',
'$x_axis_2',
'$image3',
'$y_axis_3',
'$x_axis_3',
'$userimages')";
$result=mysqli_query($con,$query);

if ($result){
      echo ' <script type = "text/javascript">alert("Registration Complete! Proceed to Login")</script>';
     session_destroy();
     header('Location:../log_in/login.html');}
else {echo ' <script type = "text/javascript">alert("Error in Registration Please Retry!")</script>';
     header('Location:register.html');}
?>
```

Code snippet for Login Interface

```
<?php
include("db.php");
include("db.php");
    if (isset($_POST['submit'])){
      $name=$_POST['name'];
      $pw=$_POST['password'];
      $password=md5($pw);

      $query="select * from users where username='$name' and password='$password'" ;
      $result=mysqli_query($con,$query);
      $count = mysqli_num_rows($result);
      if($count > 0)
      {
        session_start();
            $_SESSION['uname'] = $_POST['name'];
        header('Location:log_img1.php');}
       else {header('Location:invalid_textpw.html');}}
 ?>
```