NEAR EAST UNIVERSITY
INSTITUTE OF GRADUATE STUDIES
DEPARTMENT OF COMPUTER INFORMATION SYSTEMS

ARTIFICIAL INTELLIGENCE BASED AUTHENTICATION AND ANOMALIES DETECTION SYSTEM FOR IMPROVE M-BANKING SECURITY

PhD THESIS

Yakubu Bala MOHAMMED

Nicosia
July, 2022

NEAR EAST UNIVERSITY
INSTITUTE OF GRADUATE STUDIES
DEPARTMENT OF COMPUTER INFORMATION SYSTEMS

ARTIFICIAL INTELLIGENCE BASED AUTHENTICATION AND ANOMALIES DETECTION SYSTEM FOR IMPROVE M-BANKING SECURITY

PhD THESIS

Yakubu Bala MOHAMMED

SUPERVISOR
Prof. Dr. Nadire CAVUS

Nicosia
July, 2022

Approval

Thesis defense was held online. The Jury members declared their acceptance verbally, which is recorded.

Examining Committee Name-Surname Signature

Head of the Committee: Prof. Dr. Abdulsalam Y. Gital ………………………….

Committee Member*: Prof. Dr. Erbuğ Çelebi ………………………….

Committee Member*: Assist. Prof. Dr. Sahar Ebadinezhad ………………………….

Committee Member*: Assoc. Prof. Dr. Boran Sekeroğlu ………………………….

Supervisor: Prof. Dr. Nadire ÇAVUŞ ………………………….

Approved by the Head of the Department

10/08/2022

………………………….

Prof. Dr. Nadire CAVUS

Head of Department

Approved by the Institute of Graduate Studies

…../…../2022

………………………….

Prof. Dr. Kemal Hüsnü Can Başer

Head of the Institute

Declaration

I hereby declare that I was the one who carried out this research. Throughout the entire process, there was no evidence of unethical behavior. During the process of gathering the essential information, academic and ethical criteria were observed. During the study and writing of the thesis, I provided references to all the information gathered by this study, and there was no infringement of copyright.

.

Yakubu Bala MOHAMMED
08/08/2022

Acknowledgments

I would like to humbly acknowledge the effort, patience, guidance, and support of my supervisor Prof. Dr. Nadire Cavus. Without her encouragement and support this thesis would not have been achieved. She has ambled me through a rigorous scientific written process. Without her informative, educative and constant instruction, this thesis would not have reached its current stage.

I would also like to thank my thesis jury committee members for their support, encouragement, comments and suggestions towards the successful completion of this thesis. Also, I would like to thank the entire staff of Department of Computer Information Systems for the knowledge impacted during my coursework, support, patience, and encouragement towards the completion of this thesis. Likewise, I am very grateful to Prof. Dr. Abdulsalam Y. Gital of the Department of Mathematics and Computers Science, Abubakar Tafawa Balewa University, Bauchi for his mentorship throughout my PhD program.

My deep appreciation goes to my colleagues in the Department of Computer of Science, Abubakar Tatari Ali Polytechnic, Bauchi, for their supports, and encouragement throughout my PhD program. Also, I am very grateful to the Polytechnic management for given the opportunity to further my education abroad.

Above all, my boundless appreciation goes to my beloved parents for their training, prayers, support, and confidence in me. I would ever remain grateful to my late father Alh. Muhammad Adamu Waziri for the proper upbringing and edifying motivation. I would also like to thank and appreciate my beloved mother Hajiya Sa'adatu Aliyu for her endless love, support, prayers, and encouragement since from the start of my life. In the same vein, my gratitude goes to my lovely wife, children and other family members for their inspiration and helps.

Lastly, my appreciation goes to all my friends, and school mates who have always been source of strength and inspiration.

Abstract

Artificial Intelligence Based Authentication and Anomalies Detection System for Improve M-Banking Security

Mohammed, Yakubu Bala
PhD, Department of Computer Information Systems
Prof. Dr. Nadire Cavus

July, 2022, 135 pages

With the current trends in internet and mobile innovations, virtual financial markets are increasingly becoming an important part of people lives, and have begun to offer interesting and useful services such crypto-currency trading and m-banking services. For instance, m-banking platform allows individuals to pay for goods, services, and earn money through crypto-currency transaction's using mobile devices, anytime and anyplace. But people concern for safety have continue to hinder its advancement, especially in developing nations such as Nigeria, as information convey through m-payments channels are becoming more susceptible to different forms of attacks, and threats. Thus, the aim of this study is to investigate the influence of security on m-banking, and propose an AI based authentication and anomalies detection system using four AI based ensemble approach; GPR, BRT, ANN, SVM, and one novel model (FFNN) were developed for the estimation of security effects on m-banking progress using 978 datasets obtained from three study locations i.e., Nigeria, Iraq, and Cyrus. Subsequent to the models' development, a "sensitivity analysis" was conducted to choose the most relevant input parameters in the study locations. Performance of the proposed AI models was assessed using Nash-Sutcliffe efficiency (NSE), and Correlation coefficient (R). Findings of the study reveal that all the proposed AI models exhibited higher forecasting accuracy in predicting the influence of security on m-banking with NSE values > 0.95 in both calibration and testing phases with SVM outperforming the other models. Also, it was found that the ensemble method enhanced the performance of the sole models; SVM, GPR, ANN, BRT by 2%, 4%, 6%, and 8% respectively. Furthermore, the study sensitivity examination results found security to be the most dominant input parameters, signifying the predicted influence of safety on m-banking in the study locations. Similarly, the usability testing results justify the robustness of the proposed AI based system as majority of the participants expressed satisfaction with the system security features. The study results can assist customers in understanding the vulnerability of present verification methods, payment institutions in understanding the influence of security on m-banking, and as inspiration for researchers to embrace AI based techniques.

Keywords: Artificial intelligence, m-banking security, machine learning, ensemble techniques, privacy

Özet

M-Bankacılık Güvenliğini Artırmak İçin Yapay Zeka Tabanlı Kimlik Doğrulama ve Anormallik Tespit Sistemi

Mohammed, Yakubu Bala
Doktora, Bilgisayar Enformatik Anabilim Dalı
Prof. Dr. Nadire Cavus

Temmuz, 2022, 135 sayfa

İnternet ve mobil alanındaki teknolojik yeniliklerden dolayı sanal finans piyasaları giderek insan yaşamının önemli bir parçası haline geliyor ve kripto para ticareti ile m-bankacılık hizmetlerinde faydalı hizmetler sunmaya başlamıştır. Örneğin, m-bankacılık platformu, bireylerin her zaman ve her yerden mobil cihazları kullanarak kripto para işlemlerini gerçekleştirerek mal ve hizmetler için ödeme yapabilmelerine, bunun sonucunda da mal ve para kazanmalarına olanak tanımaktadır. Ancak, m-ödeme kanalları aracılığıyla aktarılan bilgiler, farklı saldırı ve tehdit biçimlerine karşı daha duyarlı hale geldiğinden, özellikle Nijerya gibi gelişmekte olan ülkelerde güvenlik konusundaki endişe duyulmasına neden olmaktadır. Bu nedenle, bu çalışmanın amacı, güvenliğin m-bankacılık üzerindeki etkisini araştırmak ve dört AI-tabanlı topluluk yaklaşımı kullanarak AI-tabanlı bir kimlik doğrulama ve anormallik tespit sistemi önermektir. GPR, BRT, ANN, SVM ve yeni bir model (FFNN), m-bankacılık ilerlemesi üzerindeki güvenlik etkilerinin tahmin edilmesi için, Nijerya, Irak ve Kıbrıs gibi üç çalışma konumundan elde edilen 978 veri seti kullanılarak geliştirilmiştir. Modellerin geliştirilmesinin ardından, çalışma lokasyonlarında en uygun girdi parametrelerini seçmek için bir "duyarlılık analizi" yapılmıştır. Önerilen AI modellerinin performansı, Nash-Sutcliffe verimliliği (NSE) ve Korelasyon katsayısı (R) kullanılarak değerlendirilmiştir. Çalışmanın bulguları, önerilen tüm AI modellerinin, hem kalibrasyon hem de test aşamalarında NSE değerleri > 0.95 ile güvenliğin m-bankacılık üzerindeki etkisini tahmin etmede daha yüksek tahmin doğruluğu sergilediğini ve SVM'nin diğer modellerden daha iyi performans gösterdiğini ortaya koymuştur. Ayrıca, topluluk yönteminin tek modellerin SVM, GPR, ANN, BRT performansını sırasıyla %2, %4, %6 ve %8 arttırdığı tesbit edilmiştir. Ayrıca, çalışmanın duyarlılık incelemesi sonuçları, güvenliğin en baskın girdi parametreleri olduğunu bulmuştur. Bu da, çalışma lokasyonlarında güvenliğin m-bankacılık üzerindeki tahmin etkisini göstermektedir. Benzer şekilde, kullanılabilirlik testi sonuçları katılımcıların çoğunun sistem güvenlik özelliklerinden memnun olduklarını ortaya çıkardığından önerilen AI-tabanlı sistemin sağlamlığını da doğrulamaktadı. Çalışma sonuçlarının, müşterilerin mevcut doğrulama yöntemlerinin güvenlik açığını anlamalarına, ödeme kurumlarının güvenliğinin m-bankacılık üzerindeki etkisini anlamalarına ve araştırmacıların AI-tabanlı teknikleri benimsemeleri için ilham kaynağı olmasına yardımcı olacağı umut edilmektedir.

Anahtar Kelimeler: Yapay zeka, m-bankacılık güvenliği, makine öğrenimi, topluluk teknikleri, gizlilik

Table of Contents

CHAPTER I

CHAPTER II

CHAPTER III

CHAPTER IV

CHAPTER V

CHAPTER VI

List of Figures

List of Tables

List of Abbreviations

AI: Artificiial Intelligence

ANFIS: Adaptive Neuro Fuzzy Inference System

ANN: Artificial Neural Network

AV: Aggregate Value

BRT: Boosted Regression Tree

CA: Cronbach Alpha

CR: Composite Reliability

D&M: DeLone and McLean

DC: Coefficient of Determination

DDoS: Distributed Denial of Service

EANN: Emotional Artificial Neural Network

e-Pay: Electronic Payment

GBC: Gradient Boosting Classifiers

GPR: Gaussian Process Regression

ICT: Information and Communication Technologies

IDT: Innovation Diffusion Theory

LM: Laban Movement

LMS: Learning Management Systems

LSBoost: Leas-Square Boosting

M-Banking: Mobile Banking

MC: Mean Centred

MFA: Multi-Factor Authentication

MITB: Man-in-the-Browser

MITM: Man-in-the-Middle

ML: Machine Learning

MLR: Manifold Linear Regression

MMN: Min–Max Normalization

M-Payment: Mobile Payment

NFC: Near Field Communication

OTP: One-Time Password

PS: Pareto Scaling QA: Quality Assessment

SA: Simple Averaging

SVM: Support Vector Machine

TAM: Technology Acceptance Model

TPB: Theory of Planned Behaviour

TRA: Theory of Reasoned Action

UTAUT: Unified Theory of Acceptance and Use of Technology

VSS: Variable Stability Scaling

WA: Weighted Averaging

CHAPTER I

INTRODUCTION

In this chapter, theoretical background regarding "m-banking" security challenges, patronage and advancement, aims of the research, benefits to be derive from this research, importance, and contribution to the department of computer information systems, and problems that necessitate the conduct of this research were discussed.

1.1 Background

With recent progress in internet and mobile technologies, and crypto-currency investment, digital payment systems are gradually becoming an essential part of persons lives, and have begun to provide flexible, interesting, and useful services not only to individuals but also organizations e.g., crypto-currency and m-banking services (Szumski, 2020). "M-banking is a subset of m-commerce" which allows individuals or groups of individuals to send and receive payments, sell goods or services, and generate contents through radiocommunication such as mobile devices regardless of time or space. As m-commerce is gradually becoming attractive in emerging digital payment markets, m-banking systems will continue to facilitate virtual dealings between organizations and individuals (Baabdullah et al., 2019; Dauda & Lee, 2015). Also, m-banking is defined as a payment platform in which moveable devices are use to initiate, authenticate, and approve financial transactions of all kinds in a seamless and smooth way (Nguyen, 2020). It, therefore, consists of four commonly used terms such as electronic banking, online banking, mobile banking, and/or internet banking.

In the past twenty years, the banking sector, specifically digital payment systems e.g., m-banking, online payments, and crypto-currency market had witnessed rapid progress, especially in developed countries e.g., UK, US, France, Germany, Russia, and China. In the last quarter of 2019, the global virtual payments market was estimated to have a net value of over 4.2 billion USD, and is expected to reach 8.7 billion USD by the end of 2025 (Alkhowaiter, 2020). During a senior conference series in 2019 (i.e., ePay summit) which is a conference series usually organized to showcase the most innovative banking and financial technologies. The Vice president of STC Pay (Mr.

Alenazi A.) stressed that “in addition to governments’ insistence for cashless policies, advances in internet technologies, mobile-phone penetrations, and people desire to trade and earn money via virtual market such as crypto-currency market are other reasons for the accelerated growth of digital payment systems” e.g., m-banking (Alkhowaiter, 2020: p.7).

With the recent advances in the virtual payments market, especially the virtual currency i.e., crypto-currency, it is expected that m-banking may likely have a brighter future. The system will enable e-commerce organizations, banks, and other financial institutions to gain competing benefit via the provision of services such as “concert payment, tram, parking fees, taxis and flights fares payments by allowing users to use moveable device to connect to a server in order make payments by verifying, authorizing, and confirming the completed transactions” (Kumar et al., 2020: p.13). Additionally, the system now allows individuals and organizations to earn money via crypto trading’s by buying and/or selling of crypto coins using any devices, anytime, and anyplace. M-banking system comprises of various gadgets (i.e., technologies) offered to users as well as the different tasks executed by the payment institutions in conveying such payment transactions (de Reuver & Ondrus, 2017).

Though, m-banking is increasingly becoming popular, and essential part of people lives in advance countries like Germany, Russia, UK, Australia, China, and France to mention but few, due to its affordance and suppleness. However, data stored or transmitted through m-banking systems were subjected to different attacks, security threats, and risks. Thus, organizations and different group of users may conceive m-banking benefits differently, and accept innovative banking and financial payments technologies accordingly. With continued increase in online fraud, issues connected to providing secured and suitable “m-banking services” are of crucial importance, expressly on individual’s resolved to accept, utilize, and continual patronage. The platform (i.e., m-banking) is of special interest not only to stakeholders but also scholars, this is because financial institutions, trusted third-parties, systems/software service providers, and payment organisations can greatly benefit from better comprehension of the safety, secrecy, authentication, and other crucial matters undermining “m-banking” continuous patronage, and advancement, especially in countries with evolving virtual payments systems e.g., Nigeria, Iraq, India, and Cyprus.

Although, few security architectures and solutions have been offered by prior studies in an attempt to enhance m-banking functionality, secrecy, cost, scalability, and security (e.g., Chaimaa et al., 2021; Emeka & Liu, 2017; Vishnuvardhan et al., 2020; Zefferer & Teufl, 2013). However, information and transactions transmitted via m-banking platform were subjected to different forms of attack, threat, and risk due to rise in internet crime i.e., online fraud (Cavus et al., 2021a). Also, m-banking growth and continual patronage continues to face a lot of challenges such as information quality, cultural background, services quality, protection, user verification, and secrecy issues, especially in multilingual countries with emerging digital payments market. The system encompasses of at least four divergent parties i.e., "internet services providers, imbursement institutions, telecommunication services providers, and user mobile devices each carrying out certain value-added tasks in the imbursement delivery conduit. Thus, making it more susceptible to attacks" (Chanajitt et al., 2018: p.14).

Factors affecting computer-based systems adoption, in this case innovative banking and payment technologies such as "m-banking" are normally forecasted using classical replicas such as; "Models of Information Systems Success" by DeLone and McLean (2003) which highlights the significance of autonomous parameter in computer-based systems studies, "Technology Acceptance Model (TAM)" by Davis (1989) which emphasized the importance of perceived usefulness and ease of use, Ajzen (1991) "Theory of Planned Behaviour (TPB)", Venkatesh et al. (2012) stretched "Unified Theory of Acceptance and Use of Technology (UTAUT2)", Fishbein et al. (2007) revised "Theory of Reasoned Action (TRA)", which explained individuals' action from mental standpoint, and updated "Innovation Diffusion Theory (IDT)" for technologies approval and use. These models were used by a large number of studies, and are still valid, reliable and effective in investigating factors influencing computer-based systems acceptance and usage in certain countries, but cannot perform well in multilingual countries, and countries with emerging digital payment systems.

Though, the above-stated classical replicas and innovative diffusions have enhanced our understanding of issues affecting digital payments systems i.e., m-banking, and technology espousal in general not only in developed nations, but also in developing nations (e.g., Baabdullah et al., 2019; Lu et al., 2017; Malaquias & Hwang, 2016; Merhi et al., 2019; Sharma, 2019; Wessels & Drennan, 2010; Zhou et al., 2021). However, these models have proved to offer lower prediction accuracy compared to AI-based models in terms of accurate and reliable prediction of "nonlinear processes" (Nourani et al., 2020). These limitations and other problems associated with the empirical models give rise to the application of different machine learning models such as “support vector machine (SVM), artificial neural networks (ANN) gaussian process regression (GPR), boosted regression tree (BRT), generic algorithm (GA), and adaptive neuro fuzzy inference system (ANFIS) models” for prediction of human emotions, behaviour, and attitude toward computer-based systems such as m-banking systems, due to their flexibility, reliability, robustness and accuracy in handling uncertain data (Andaryani et al., 2021). For instance, Sharma (2019) in their study compared the performance of conventional models with neural network (ANN) model to explain customers’ behavioural intent to use m-banking, and the findings confirmed the prediction ability of the ANN model over the conventional model used. Another study conducted by Wang et al. (2021) in Pakistan in an attempt to find “AI-powered financial investment” in the Pakistani banking sector, the results indicated that machine learning models have superior estimation ability than the classical models. furthermore, Cavus et al. (2021a) compared the performance of classical model with an AI-based model (i.e., ANN), and the outcomes clearly shows that the ANN model has more prediction skills than the classical models as it was able to detect and manipulate the study hidden data. also, Yin and Vatrapu (2017) used machine learning models i.e., gradient boosting classifiers (GBC), and gaussian process regression (GPR) to compare the performance of ML models with classical models with regards to classifying cybercrime entities, and the outcomes showed that the ML models have superior prediction ability than the empirical models.

Though, quite a number of m-banking studies were conducted using empirical methods which are time consuming, not reliable, and sometimes produced inaccurate results (Nourani et al., 2020). Also, few AI-based single modelling approach have been employed for the prediction of m-banking determinants. However, user verification and other security issues still remain an obstacle to m-banking continued patronage and development, especially in developing nations. To overcome the limitations of the classical and AI-based single modelling process, four different AI techniques i.e., ANN, BRT, SVM, and GRP were used in this research in order to forecast the influence of security on “m-banking” continuous patronage, and advancement in the study locations. It was found that, ensemble approach i.e., combining two or more different AI-based models for estimation is more effective, and can improve models’ estimation precision in computer-based studies such as innovative financial systems (Zhao et al., 2021).

1.2 Statement of the Problem

With the recent inclinations in digital currency investment e.g., crypto-currency trading, virtual payments market, specifically m-banking services station, and financial segments are increasingly becoming attractive and parts of people lives in both advanced and evolving virtual markets, particularly among African nations due to its affordance, suppleness, and opportunity to earn money. Although, "m-banking" is expected to have a sunnier future. But, different organizations, individual, or groups of individuals may perceive its benefits differently and accept it accordingly. For instance, Africa is considered to be the most global multi-ethnic region (Kamdjoug et al., 2021). In addition to users' behaviour and culture, Chanajitt et al. (2018) argued that people's concern for security and confidentiality of data transmitted via m-banking platforms may likely be another issue affecting m-banking continued patronage and progress globally. While there are needs to understand the culture, behaviour, and security preferences of different users' groups, little effort was made using empirical models such as UTAUT, TRA, D&M, IDT, TAM, and TPB etc., in an attempt to address the problem.

Though, the above-mentioned systems diffusion, and theoretical models are still valid and useful, and have enhanced our understanding of the issues affecting innovative banking and financial technologies, in this case m-banking technologies. However, predictions based on these models are usually bias-based, expensive, time consuming, unreliable, and at times produced inaccurate results (Cavus et al., 2021a; Nourani et al., 2020). The authors used both the two approaches (i.e., AI based and classical) in their studies and found the AI approach to be more consistent, faster, precise, and produced better results compared to the classical techniques.

To overcome the limitations of the classical models, and address the security dynamism, and impediments of m-banking diffusion, different approaches are required e.g., AI-based techniques to investigate the impacts of protection and other factors on "m-banking" continuous patronage and advancement. For instance, Zhao et al. (2021) stressed that AI-based techniques are more robust and accurate in modelling or simulating complex non-linear problems such as m-banking with high level of precision compared to empirical models. Though, AI approach may offer reliable and precise results, it is also known that ensemble methods, i.e., combining two or more different AI approaches may produce different outcomes for a particular problem than the single modelling approach. Thus, the need for different AI approaches to predict the impact of protection on "m-banking" continuous patronage due to its complexity.

1.3 Aim and Objectives

Main goal of the study, and objectives required to achieve this goal were offered in the following subsection.

1.3.1 Aim

The main aim of this study is to investigate the impacts of security on "m-banking" advancement in Nigeria, Iraq, and Cyprus, and propose an AI-based authentication and anomalies detection system for improved m-banking security in emerging digital payment markets. The aim can be achieved through the following objectives.

1.3.2 Objectives

- To perform a sensitivity examination for the selection of key input parameters for the developed AI-based models.

- To determine the correlation between the selected input parameters and m-banking continuous patronage and advancement in study locations.

- To develop and validate 4 different AI-based single models (i.e., ANN, SVM, GPR, and BRT), and one novel model (ensemble) for the prediction of security influence on m-banking advancement.

- To compare the performance of the study developed single models in terms of predictions of security effects on m-banking.

- To develop one-nonlinear (i.e., FFNN) and 2-linear (i.e., weighted and simple averaging) ensemble models for enhancing the efficacy of the separate models in predicting security influence on m-banking.

- To design an AI-based authentication and anomalies detection system for improved m-payment systems security.

1.4 Contribution to the Department of Computer Information Systems

Staff of computer information systems department (CIS) who are information systems analyst, designer, and researchers can derive the following benefits from this study; i) Understand the key factors affecting computer-based systems usage e.g., m-banking, ii) use the study proposed AI-based system to secure institutional databases, and web-based learning technologies e.g., learning management systems (LMS) from unauthorize access, iii) use the study approach (AI-based techniques) to obtain precise and reliable results which are generally difficult to obtain using empirical models such as TAM, TPB, D&M, TRA, UTAUT, and IDT without prior knowledge or deep understanding of the concept. In addition to the above-mentioned benefits, the study methods (e.g., Ensemble approach) can serve as motivation for scholars in computer and IT related fields to embrace machine learning approach. Lastly, the study sensitivity examination process may enable information systems scholars understand the importance of selecting relevant input parameters in research as the study highlights how inclusion of irrelevant parameters can reduce results accuracy and vice versa.

1.5 Significance of the Study

The study proposed models highlight the robustness and superiority of AI-based models over the classical models usually used by majority of scholars in engineering and sciences, as the models predicts with higher accuracy the effects of protection and other selected parameters on “m-banking” continuous patronage and advancement. Also, the study provides an inclusive and excellent results by: i) identifying the main security, authentication, and secrecy issues affecting not only m-banking platforms, but also all virtual payment systems, ii) highlights the main determinants of “m-banking” continuous patronage in evolving digital payment markets, and iii) showcase the benefits of using ensemble approach over single modelling process. Furthermore, the study proposed AI-based authentication and anomalies detection system can assist in detecting velocity anomalies, and improve user verification processes. This is because attackers usually carry out attack from location other than the location of legitimate user, moment after the legitimate user log onto the system or out, and the proposed system has the ability to handle such attacks by detecting velocity anomalies during and after login.

1.6 Overview of the Study

The study is aimed at examining the influence of safety, confidentiality, and user authentication challenges on “m-banking” continuous patronage and advancement in three different study locations (i.e., Cyprus, Iraq, and Nigeria) which are considered as countries with emerging virtual payment systems.

In the first chapter of the research, “m-banking” benefits, security and other challenges, significance of the study, problems background, main purposes of the research, and objectives required to accomplish these purposes were offered. Also, contributions of the study to the department of “computer information systems” were highlighted.

In the second chapter, PRISMA approach for conducting meta-analysis and literature reporting (i.e., systematic literature) was employed to identify the missing gaps in the literature with regards to “m-banking” security challenges. Also, the chapter highlights the followings; literature selection process such as addition and elimination criterions, quality assessment procedure, and trends in m-banking studies.

Having identified the missing gaps from prior m-banking research in the second chapter, an AI-based authentication and anomalies detection systems was developed and tested using usability testing questionnaire adopted from Lewis, (2006) in the third chapter. Furthermore, methods employed by this research such as “research design, study areas selection, data collection tools, participants, and methods of data analysis were all discussed in the chapter.

In chapter four, the study data were analyzed using 4 AI-based techniques, and the research proposed AI models were validated using five indices of; i) “Root mean square error” (RMSE), ii) “Nash-Sutcliffe efficiency” (NSE), iii) “Mean absolute error” (MAE), iv) “Percentage bias” (PBIAS), and “Correlation Coefficient” (R). Likewise, the usability testing results for the proposed AI based system were also presented in the chapter.

Results of the study were debated in the fifth chapter of the research. Findings of the research shows that the AI models predict the influence of security and other choosing input parameters on m-banking patronage and continued progress in the study areas with higher accuracy with NSE values > 0.9 compared to other classical models usually used by prior m-banking scholars.

In the sixth chapter of the study, conclusion regarding the impacts of security on “m-banking” continuous patronage, and advancement in the research areas were made. Also, in the chapter, recommendations for various m-banking stakeholders such as customers, banks and other imbursement organizations, and direction for upcoming studies were stated.

CHAPTER II

LITERATURE REVIEW

In this chapter, a systematic literature review (SLR) was conducted using PRISMA approach for conducting meta-analysis and literature reporting. Additionally, the section highlights the criterions used for database searches, and literature search terms, elimination, quality assessment queries, and addition. Also, trends in m-banking studies, and key findings of the SLR process were also offered in this chapter.

2.1 Theoretical Background

At present, the global financial market has continued to witness tremendous progress in the areas of evolving technologies. Banking sector is one of the segments that experienced the most innovative financial technologies in the form of m-banking (Gupta et al., 2017). In addition to the usual practice of receiving and making calls, mobile devices i.e., smartphones have surely changed the traditional communication channels between banks, individuals, and businesses (Shaikh & Karjaluoto, 2015). Researchers have expansively taken note of this distinctiveness and begin to recognize the importance of smartphones in the areas of e-commerce as individuals and organizations can receive and/or make payments anytime, anywhere through mobile phones. M-banking is an alternate platform of e-commerce which allows clients to enter their bank accounts in order to initiate and approve payments even while on the go (Baabdullah et al., 2019; Ha et al., 2012).

With the recent advances in the virtual payments market, especially the virtual currency i.e., crypto-currency market which allows people to earn money via crypto trading, it is expected that m-banking may have a brighter future. Also, a quite number of studies were conducted using empirical approaches in an attempt to discover the main factors affecting m-banking continual usage. However, its expansion is beyond the industry expectation due to people’s concern for security, privacy, and user verification challenges, especially in developing nations with emerging digital payment markets (Alkhowaiter, 2020). Thus, the need for an inclusive systematic review of related studies in order to have better understanding of the security, privacy, and authentication issues affecting m-banking continued patronage, and progress.

2.2 Systematic Literature Review Process

Though m-banking is forecasted to have a sunnier future, its attractiveness and progress continued to face a setback not only in emerging virtual payment markets e.g., Nigeria, and Iraq, but also in advanced digital markets due to people increased concern for safety, confidentiality, and verification challenges. In an attempt to address these problems, this study performed a systematic literature review (SLR) in order to identify the missing gaps from the literature with regards to user authentication challenges, influence of safety, and confidentiality issues on "m-banking" continual usage and development, especially in countries with evolving virtual payment systems. PRISMA statement i.e., Four-stage items reportage techniques for "Meta-Analysis and Systematic Literature Review" was adopted as per (Moher et al., 2010). Selection of databases, extraction of relevant literature based on the study theme was done in the first phase; While in the second phase, non-related articles were removed based on title and abstract; Exclusion and inclusion activities based on suitability (i.e., Eligibility) was performed in the third phase. Lastly, studies to be included in the SLR were picked in the fourth phase.

2.2.1 Strategy for Searching Related Studies

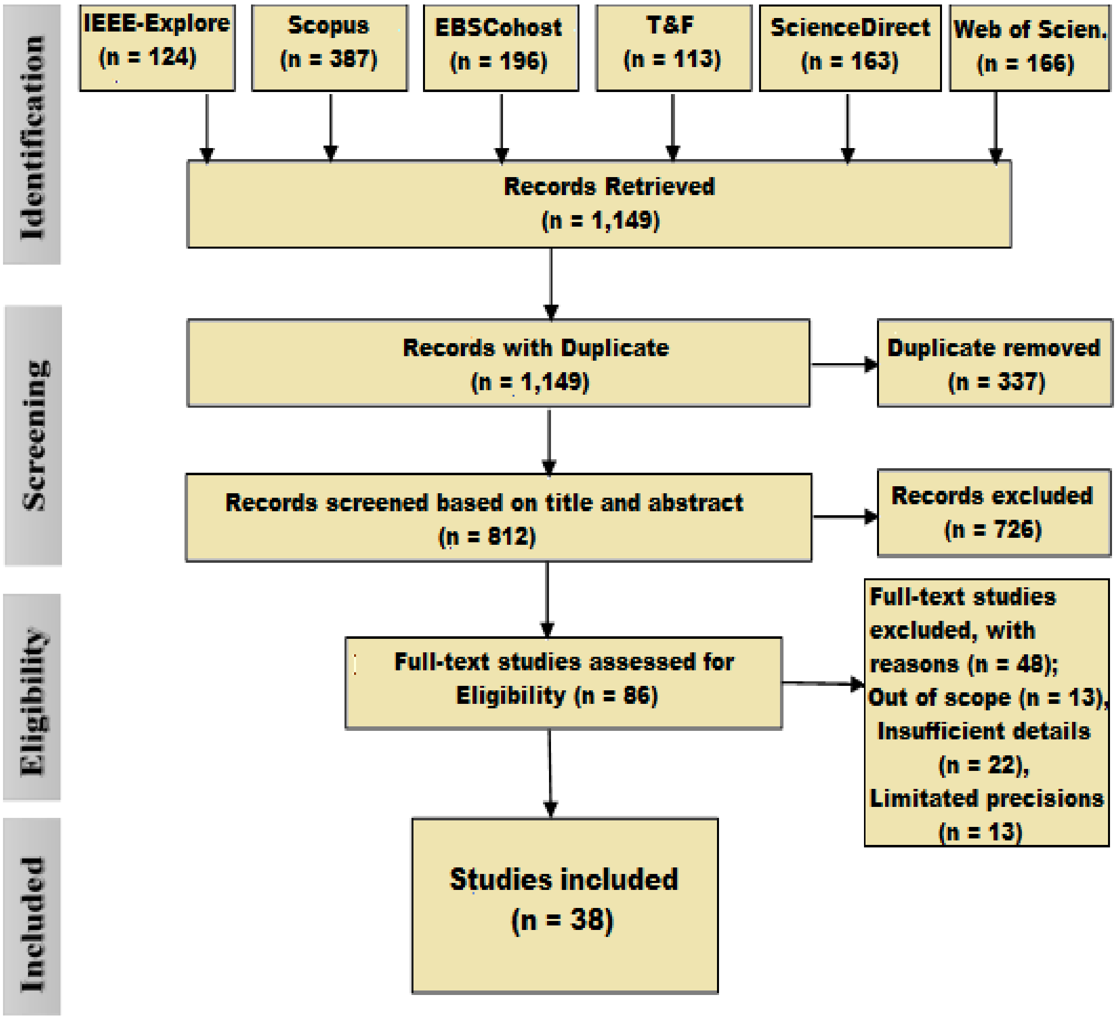
Six reputable online databases; EBSCOhost, IEEE-Xplore, Taylor & Francis, ScienceDirect, Web of Science, and Scopus were utilized and queried for related studies. Terms used in querying the databases are ("m-banking" OR "mobile banking" OR "internet banking" OR "m-payment") AND ("Security" OR "Privacy" OR "Risk" OR "Trust") AND ("Authentication methods" OR "Verification schemes" OR "Framework") studies published between 2013-to-2021, and written in English language are included.

2.2.2 Criteria for Selection of Related Studies

Nowadays, scholars in engineering, science, and social sciences used (PRISMA-E 2012) selection technique due to its precision and flexibility in literature reportage (Welch et al., 2016). This study too is not an exception. Thus, employed the same approach. The study key selection standards are; studies that discussed m-banking protection and privacy issues, and verification challenges. Irrelevant studies based on title and brief descriptions (abstracts) were removed at the early evaluation stage by the researchers. Therefore, the study inclusion and exclusion standards were used in selecting studies to be included in the review, and those to be excluded. Studies that met the review inclusion standards were extracted from the source and imported into a worksheet designed for the study. Full-text of the selected studies were obtained by the authors for further assessment in the subsequent screening phase. While, in the second screening phase, the authors independently read the full-text of each of the extracted studies using the review quality assessment queries, search terms, and purpose in order to determine their significance. Due to travel restriction caused by "COVID-19 Pandemic", google meet and zoom platforms were used by the authors to resolves any disagreement concerning study relevancy. One thousand, one hundred and forty-nine (n=1,149) studies were extracted from the selected databases. After removing duplicate copies (n=337), eight hundred and twelve studies (n = 812) were further screened based on titles and brief descriptions out which seven hundred and twenty-six (n=726) were removed. Full-text of the remaining eighty-six studies (n-86) were obtained for further evaluation in the third (eligibility) phase, out of which forty-eight studies (n = 48) were removed due to the following reasons; i) Out of scope (n = 13), ii) Inadequate details (n = 22), and iii) Insufficient precisions (n = 13). Details of the study inclusion and exclusion standards are presented in Table 1. Thus, thirty-eight studies (n=38) fulfilled the study inclusion standards. The above-mentioned review procedure was achieved with the aid of "PRISMA" approach as shown below.

Figure 1.

PRISMA Diagram of the Study


Identification
Screening
Eligibility
Included
IEEE-Explore (n = 124)
Scopus (n = 387)
EBSCohost (n = 196)
T&F (n = 113)
ScienceDirect (n = 163)
Web of Scien. (n = 166)
Records Retrieved (n = 1,149)
Records with Duplicate (n = 1,149)
Duplicate removed (n = 337)
Records screened based on title and abstract (n = 812)
Records excluded (n = 726)
Full-text studies assessed for Eligibility (n = 86)
Full-text studies excluded, with reasons (n = 48); Out of scope (n = 13), Insufficient details (n = 22), Limitated precisions (n = 13)
Studies included (n = 38)

2.2.3 Studies Exclusion and Inclusion Criteria

Preliminary relevance for all extracted studies was ascertained based on the study heading and description. Where heading and description seemed to deliberate on the review procedure, then its reference and full-text were extracted and grouped for further evaluation as shown in Figure 1. The study elimination and inclusion standards were offered in Table 1.

Table 1.

Study Exclusion and Inclusion Criteria

Criteria for Inclusion
Published studies between 2013-to-2021
Articles written in English
Articles that examined m-banking authentication, protection, and secrecy challenges
Articles that are accessible online
Criteria for Exclusion
Studies written in another language not English
Non availability of full-text
Purpose of research not evidently stated
Duplicate studies
Studies with inadequate facts
Studies with inadequate precision
Studies that are outside the scope of this study
Studies that focused on "m-banking adoption" only

2.2.4 Quality Assessment

To ensure adherence to the review designed procedures, the process was carefully monitored by the researcher in order to improve the review quality. Also, the author supervised the progress of all activities at each stage in order to confirm that each activity conformed with the study standards and intended deadlines for completion. Furthermore, the author created an "EndNote library" and worksheet for accurate citations, and referencing of the choosing studies. Five evaluation questions i.e., "Quality Assessment Queries" (QAs) were formulated to assess the quality of all the extracted articles in order to pick the most pertinent studies that respond to the review queries. Exported data, observations, and other important information were kept in the worksheet specially designed for the review. Furthermore, to ensure balanced and positive evaluation of the selected studies. The 86 articles (n = 86) whose full-text were obtained for eligibility was marked with “Yes” if the paper answers half or more than half of the study quality assessment queries, and marked with “No” if it did not answer any of the quality assessment queries. It was discovered that some studies partially answered the review QA queries. For this reason, scores or values were assigned to each study based on responses to the review QA queries. There are only three possible answers for each question i.e., “Yes”, “No”, and “Partial”, where “Yes” = 1, “partial” = 0.5, and “No” = 0, as suggested by (Liao et al., 2020). Table 2, depicts the study Quality assessment queries.

Table 2.

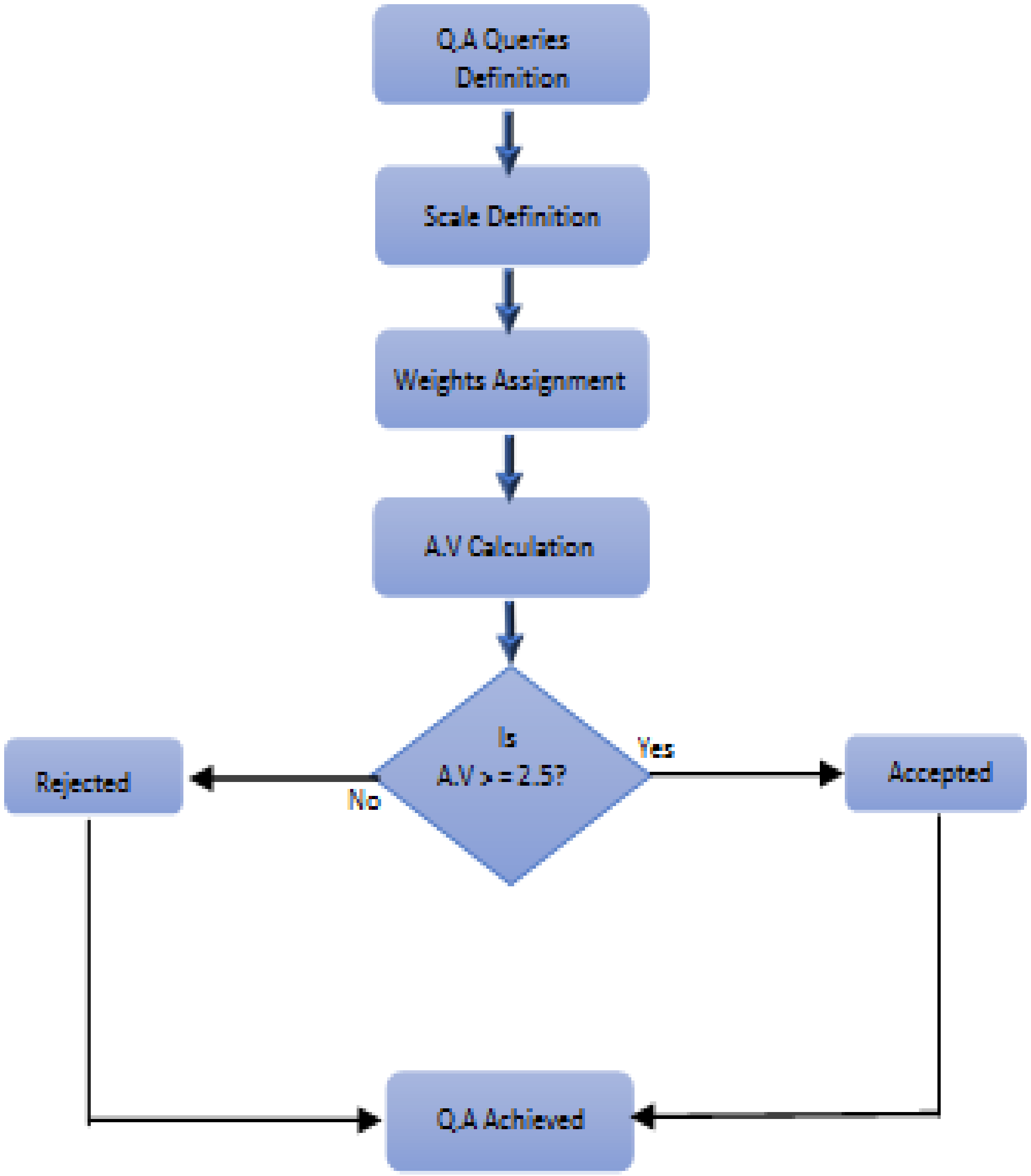
Study Quality Assessment Queries

Q. ID	Quality Assessment Queries
QAQ1	Are the study purposes clearly defined?
QAQ2	Are the study precisions sufficient?
QAQ3	Is any authentication, security, and privacy issues related to m-banking, m-payment, or internet banking reported?
QAQ4	Does the study provide answers to authentication, security, and privacy challenges of m-banking, m-payment, or internet banking?
QAQ5	Are the authentication, and other security issues of m-banking, m-payment, or internet banking contributes towards this study?

As seen in Table 2, QA queries were first defined, followed by scale definition and assignments based on the review QA queries list. The “aggregate value” (A.V) for each study was obtained after summating all the weightages given based on the review QA queries. Where the study A.V was higher than 2.5, then the study was accepted for inclusion, and if it was less than 2.5 then the study was rejected. Out of the eighty-six (n = 86) studies assessed for eligibility, forty-eight (n = 48) studies were rejected for having less than 2.5 A.V, while studies with A.V higher than 2.5 were included for final synthesis. Thus, thirty-eight (n = 38) studies were finally included in our study. Details of the review QA process is offered in Figure 2.

Figure 2.

Study Quality Assessment Flow Diagram



2.2.5 Extraction Procedure

In the extraction stage, 38 out of the 86 studies selected for eligibility assessment were found to be suitable for the review, thus considered for final synthesis. The following contents were extracted from the 38 studies.

Table 3.

Extraction Procedure

Contents
Published studies between 2013-to-2021
Articles (Conference proceedings and Journals)
Authors Name/Year of publication
Magazine Published
Number of Citations
Research Techniques/Architecture, and Framework for m-banking security
Aim of the study
Authentication, Safety, and confidentiality challenges in m-banking
Study Key Findings

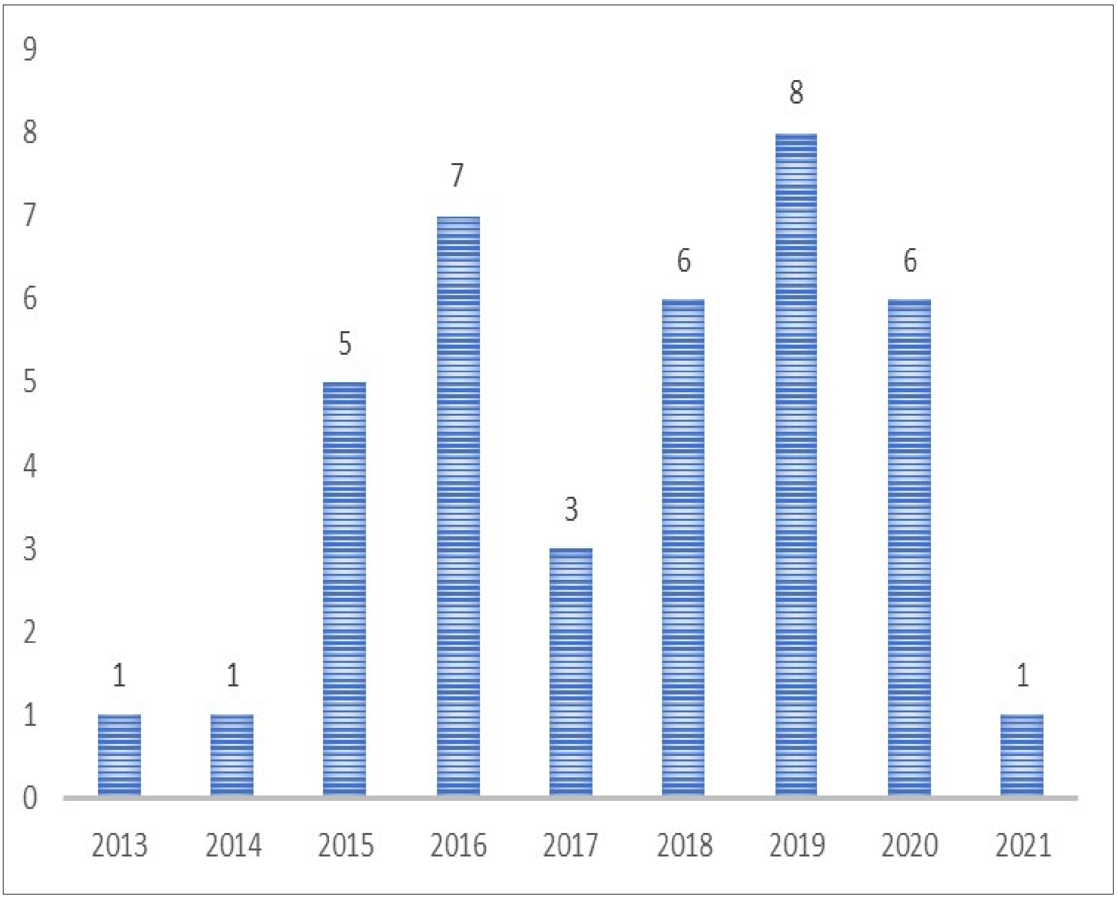
2.6 SLR Results

2.6.1 Distributions of M-banking Studies Over the Years

The inclinations of the studies based on the extracted data shows the most published magazine, the most quoted journal and references, and publications distribution over the years. As shown in Figure 3, few m-banking studies were conducted in the early period of last decade. However, with the increasing rate of mobile and internet penetrations, and customers affordance of m-banking apps, there was rapid increase in the number of publications in m-banking studies; from 2016-to-2020, particularly during the COVID-19 lockdown. It was observed that the increase may not be unconnected with the recent advances in crypto-currency market, and increasing rate of online fraud as "banks and customers" are calling for stronger user authentication techniques. Obviously, the number of studies on mobile payment systems, specifically m-banking will continue to increase until solutions regarding the security challenges are provided.

Figure 3.

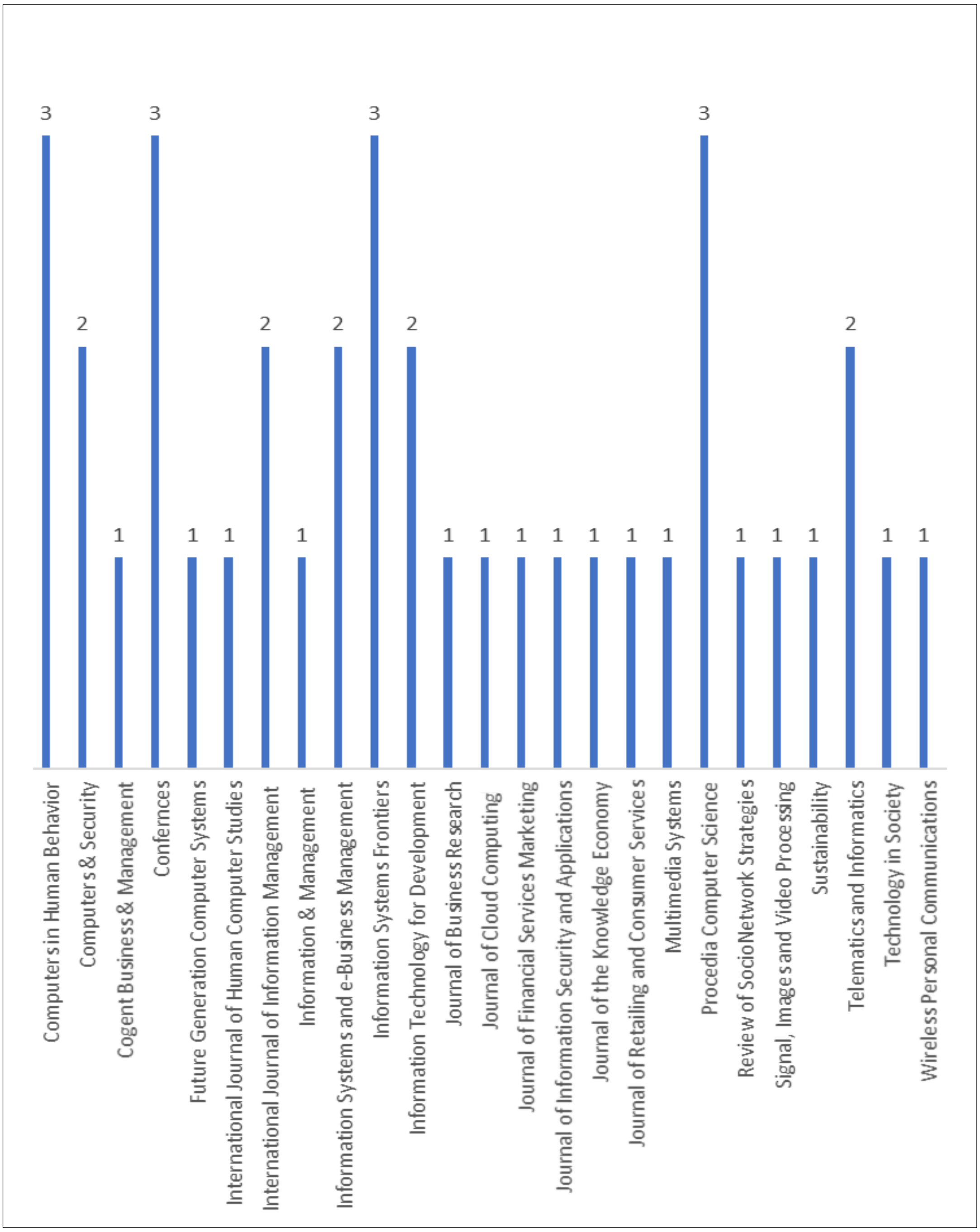
Distribution of M-banking Studies over the Year



Based on the extracted data per magazine, it can be said that the study provides a compressive systematic review of related studies as the 38 articles included in the study spread across 24 magazines which are either indexed as "Science Citation Index Expanded" (SCIE), "Science Citation Index" (SCI), "Social Science Citation Index" (SSCI), except Cogent Business & Management, and Review of SocioNetwork Strategies which are indexed as "Emerging Source Citation Index" (ESCI) in Web of science. To the best of the researcher's knowledge, this review is the first of its kind to have extracted data from 24 magazines comprising of high impact and low impact journals. As shown in Figure 4, high impact magazines have the highest number of included articles; “Computer in Human Behavior” (n = 3), “Information Systems Frontiers” (n = 3), “Telematics and Informatics” (n = 2), “Information Technology for Development” (n = 2), “Computers and Security” (n = 2), “International Journal of Information Management” (n = 2), “Sustainability” (n = 1), “Journal of Business Research” (n = 1), “Information and Management” (n = 1), “Technology in Society” (n = 1), “Multimedia Systems” (n = 1), “International Journal of Human Computer Studies” (n = 1), Future Generation Computer Systems” (n = 1), “Journal of Retailing and Consumer Services” (n = 1), followed by second quartile (Q2) magazines; “Information Systems and e-Business Management” (n = 2), “Journal of Knowledge Economy” (n = 1), “Journal of Cloud Computing” (n = 1), “Journal of Information Security and Applications” (n = 1).

Figure 4.

Number of Articles per Journals



2.6.2 M-banking Security and Privacy Challenges

Though quite a number of m-banking studies were conducted. However, protection, secrecy, and user verification still remain an issue that require serious attention not only for payment institutions, but also for researchers. Thus, this study performed an inclusive systematic literature review in an attempt to find the main protection, secrecy, and verification challenges affecting "m-banking" continuous patronage and advancement in both evolving and advanced virtual payment markets.

For instance, Kemal (2019) conducted a study in Pakistan to assess m-banking usage by women recipients, and effects of new innovations on organizational properties using empirical approach. The author argued that government concern for security is the main barrier for government financial support to individuals as the Pakistani government finds it difficult to provide financial incentives to its citizenry via m-banking platform due to the high rate of internet fraud in the country, thus, affecting government incentives programmes. Another study conducted by Cavus et al. (2021a) in an attempt to investigate the key parameters affecting m-banking sustainable growth in developing nations. The authors found security, privacy, cyberspace laws, and infrastructural deficits to have negative effects on m-banking growth, especially in developing nations.

Rabaa'i and AlMaati (2021) examined the effects of antecedent variables in customers' intent to use m-banking service channels using an integrated approach of PLS-SEM. The authors' argued that people's concern for privacy, lack of trust, and customers' attitude toward innovative banking technologies negatively affects m-banking continual usage and progress. Similarly, Albashrawi and Motiwalla (2019) assessed the influence of personalization and secrecy issues on recurrent and continual usage of m-banking services using "Technology Acceptance Model" (TAM). The authors stated that privacy is one of the critical aspects of m-banking apps, and lack of options for customers to personalize their m-banking involvement negatively affects m-banking attractiveness in the study area. Thus, suggest further investigation of privacy factors in m-banking settings.

Another study conducted by Merhi et al. (2019) in an attempt to investigate the main factors that facilitate or hinder m-banking progress from multi-cultural context between British and Lebanese customers. The authors' stressed that safety and trust are the two main factors that negatively influenced m-banking adoption and continual usage among British and Lebanese customers, thus, suggest further investigation of these factors. Also, Sharma and Sharma (2019) examined the effects of privacy and channel excellence on m-banking continual usage using structural equation modeling (SEM) and artificial neural network (ANN). The authors found privacy and service quality to have a negative effect on users' intent and gratifications, which in turn affect m-banking development in the study location. Furthermore, the authors' discovered secrecy and self-directed inspiration to be the most influential forecasters of m-banking acceptance and continual usage.

Alalwan et al. (2018) assessed the different theoretical models that best describe the main influencing factors of m-payment systems. Specifically, the authors investigated the factors affecting m-banking attractiveness among Jordanian customers, and found security, confidentiality, and effort expectancy to be the main reasons for Jordanians' non usage or continued patronage of m-banking. Also, Malaquias and Hwang (2019) used quantitative assessment (i.e., multi-group analysis - SEM) to assess the key determinants of m-banking attractiveness among US and Brazilian customers. The authors stressed the importance of secrecy to customers, and stated that secrecy is the key factor responsible for slothful development of "m-banking platforms" in evolving and advanced virtual payment markets, in their case US and Brazil.

Barkhordari et al. (2017) investigate the influence of safety and secrecy in m-banking and other electronic payments systems using TAM. The authors found security rules intrusion, logical procedures, and internet vulnerability to be the foremost protection and secrecy issues affecting m-banking and other digital payment systems development and continued patronage. Thus, require serious attention from academics and virtual payments stakeholders. Additionally, Tandon et al. (2018) examined the effects of website functionality and perceived security on m-banking and online shopping using extended "unified theory of technology acceptance and use" (UTAUT) with external factor of risk. The authors argued that confidentiality risk, financial risk, and protection risk, are other aspects of virtual payments risk that negatively affects m-payment systems, specifically m-banking.

Another study conducted by Ammar and Ahmed (2016) to assess the influence of safety, secrecy, and other factors affecting Sudanese micro-finance to adopt m-banking channels in their dealings. The authors found that unsecure internet environments and disbelief amongst customers to be the leading factors delaying m-banking progress in Sudan, and other African countries. Also, Boateng et al. (2016) used TAM and human other behavioural theories to examined the influence of security, values, and secrecy on Ghanian consumers' decisions to accept or resist internet related banking such as m-banking. The authors found safety, secrecy, device types, and individuals' lifestyle to have negative influence on m-banking development in Ghana. Furthermore, Laukkanen (2016) in their study inspects the influence of security, values, privacy, and "image barriers" on consumers decisions to adopt m-banking using two-stage confirmatory approach and binary logic techniques, and the results showed that security concern, customers' values, and confidentiality issues significantly influence customers perception of m-banking risk.

Yang et al. (2015) examined the effects of "risk" and "trust" on customers behaviours towards m-banking. The authors found protection and secrecy issues such as; "privacy risk, economic risk, functional risk, and time risk" to be the main factors responsible for customers rejection of online payments. In this case m-banking. Similarly, Gupta et al. (2017) investigated the impacts of safety levels, risk, and control mechanism on "m-banking" espousal and continual usage in India. The authors found customers fear of security breaches, value, and demographic to have significant influence on customers' perceptions of "m-banking risk and control" which in turn influenced behaviour and intent to usage and continued patronage. Also, Asongu (2018) investigated m-banking determinants and smartphones penetration in relation to safety and secrecy issues in Sub-Saharan Africa. The authors' discovered absence of digital laws that safeguard customers in virtual payment environments negatively affect m-banking progress in sub-Saharan African nations.

Malaquias and Hwang (2016) used confirmatory-SEM techniques to examined the possible determinants of m-banking acceptance. The authors argued that protection and privacy are the two main determinants of m-banking, and are responsible for its slothful expansion in both developed and emerging nations. While Qasim and Abu-Shanab (2016) examined the effects of security and confidentiality factors on "m-banking" progress from network point of view. The authors stressed that Networks externalization, safety, and privacy were the most influential drivers of m-banking. Also, the authors argued that externalization of bank networks via m-banking platforms makes the network susceptible to different attacks by unauthorize persons which in turns affect its continual usage and development in many parts of the world. Similarly, Shaikh et al. (2015) and Shaikh and Karjaluoto (2015) in their studies inspect the significance of protection and confidentiality on "m-banking continual usage". Findings of the study revealed that "security and privacy were the two major factors responsible for changes in customers' commitment to m-banking" (Shaikh et al.,2015: p.8). Also, the authors argued that network externalization, clients' participation, awareness, and authentication are other aspects of m-banking protection and privacy issues that merit systematic examination, but maybe they were overlooked or superficially inspected by prior m-banking studies. Thus, increasing clients' concern about the "security" and "privacy" of m-banking.

Wang et al. (2016) conducted a study to investigate m-payments security, threats and challenges. The authors argued that protection of customer funds, credentials, and other sensitive information in virtual payment channels e.g., of m-banking is not an easy job considering the number of attacks that are successfully carried out on m-payment systems. Consequently, customers' concern for safety is the main challenging factor in all "m-payment systems" such as mobile banking and mobile health. Also, Montazemi and Qahri-Saremi (2015) conducted a study using "meta-analytic structural equation modelling techniques" to investigate factors affecting innovative banking technologies (e.g., m-banking) "Pre-adoption and Post-adoption". Findings of the study showed that secrecy is the main factor affecting "pre-adoption" and "post-adoption" of m-banking in most nations. Furthermore, the authors argued that secrecy has a significant effect on both traditional and modern banking transactions (i.e., physical and mobile banking). Thus, the need for more examination of the factor in order to have more ideas about its consequential effects in m-banking.

2.6.3 M-banking Authentication Challenges

For m-banking user authentication schemes, quite a number of studies were carried out, and few authentication frameworks and techniques were offered by scholars in an attempt to address the problems associated with the different authentication methods used by banks and other payment organizations. Different authentication methods exist such as single-factor authentication, two-factor authentication, multi-factor authentication, and biometric authentication to mention but a few. However, user verification processes in online environments still remain an issue not only for payments institutions, but also customers due to the vulnerability challenges associated with the present authentication techniques used by payments organizations as argued by prior m-payment studies. For instance, Karim et al. (2020) in their study assessed the challenges involved in different user authentication procedures in an online environment. The authors stressed that traditional Password is still the most common means of verification despites its usability and safety challenges. Also, the study's findings showed that users' find it difficult to memorized strong passwords.

Another study conducted by Bani-Hani et al. (2019) to examine the most common online verification schemes deployed by banks, and the possible third parties' attacks against these schemes. The authors discovered that password is the most widely used verification method. Furthermore, the authors argued that present authentication methods employed by banks are becoming more vulnerable to different forms of attacks and threats e.g., "man-in-the-middle (MITM), and man-in-the-browser (MITB) attacks". Also, Kiljan et al. (2018) examined the different verification techniques presently used by banks, and issues associated with the proposed ones. The authors found insufficient analysis of user reliability, intellectual capacity, actions, lack of user active participation, and other "m-banking essentials" to be the major problems affecting the robustness of both the employed and proposed verification techniques. Similarly, Zimmermann and Gerber (2020) examined individual perceptions with regards to the choice and usage of a particular m-payment verification scheme. The authors found single-factor and fingerprint verifications to be the most preferred authentication methods for the study participants due to ease of use, but not in terms of security viability. Thus, stressed the needs for more robust and flexible authentication methods.

Nagaraju and Parthiban (2015) investigated m-banking data security and privacy concerns in relation to public cloud, and the results revealed that multi-factors verification technique is complicated. The authors argued that the technique involved a lot of risk, and makes banking "governance, maintaining protection standards, regional confidentiality, and information laws" difficult (p.17). Additionally, Soviany et al. (2016) in their study which assessed the security challenges of mobile applications e.g., "m-banking and m-Health". The authors argued that present m-banking authentication methods employed by payment institutions e.g., one factor, two factor, and multi-factors techniques are not as vigorous as people may think in terms of precision regarding human verification in mobile applications such as m-health and m-banking. Thus, the need for a more robust confirmation techniques for mobile applications. Similarly, Apostolopoulos et al. (2013) in their study argued that large number of credentials, if not all credentials deposited in "Android applications" were vulnerable to different forms of attacks, and intrusion by unauthorized persons even in packages where security is paramount such as "m-banking, mobile-Health, and password manager applications".

Wang et al. (2020) examined the security failures of multi-factor authentication (MFA) in multi-server surroundings. The authors exposed the security defects of the five most foremost "multi-factor authentication" methods in multi-server surroundings. The authors identified session-specific and malicious insider attacks as new security challenges that affect the robustness of these foremost MFA schemes. Thus, nullify future use of these five techniques without further enhancement. Similarly, Sinigaglia et al. (2020) investigated the robustness and complexity of different MFA methods deployed by m-payment institutions. The authors argued that the MFA methods currently used by banks are not highly secured as anticipated in terms of "complexity, laws compliance, and robustness against well-established attacks" (Wang et al., 2020: p.7). Also, Chen et al. (2017) examined m-payment verification issues from customers, brokers, and banks perspectives using "Near Field Communication" (NFC). The authors argued that, though NFC is more secured compared to MFA techniques, especially in human verification. However, authentication of m-payments transactions using NFC method is difficult and challenging as attackers can take advantage of the card susceptibilities to intercept payment dealings during the authentication process between user device, NFC-enabled, and brokers.

Though, biometric authentication method is more robust and accurate compared to single-factor, two-factor, multi-factors, and other authentication techniques used by banks (Ogbanufe & Kim, 2018). However, some scholars argued that biometric authentication is the most inexpensive method, and is vulnerable to different forms of attacks. For instance, Basar et al. (2019) examined the problems associated with sensors and biometric verification schemes in m-banking stations. The authors argued that sensors and biometric authentication methods were susceptible to attacks via surface utilized by legitimate user. Thus, stressed the need for a more robust machine learning method. Furthermore, Alhothaily et al. (2018) examined the challenges of fingerprint and other sensors-based verification methods used in m-payment systems such as m-banking. The authors found sensors and biometric authentication to be vulnerable. Thus, stressed that absence of robust user authentication is the main reason why m-banking stations are becoming more vulnerable, and subjected to different forms of attacks that result in financial losses, and credentials theft by fraudsters.

Barkadehi et al. (2018) assessed the usability and weaknesses of biometric authentication in relation to virtual payments, in this case m-banking. The authors discovered that even the newly introduced biometric authentication scheme were vulnerable for attacks, and stressed that authentication process is complex in terms of usability, safety, and availability. Furthermore, Abo-Zahhad et al. (2014) examined the present and future status of different biometric verification schemes in relation to real-time confirmation of user. The authors discovered safety and secrecy to be the major challenges of biometric verification schemes. This is because banks and other payment institutions may not be able to track and secure the surface utilized by legitimate users. Thus, the method is increasingly becoming more vulnerable. In addition to vulnerability challenges confronting the present authentication methods e.g., biometric and MFA, Khattak et al. (2021) stressed that failure of different authentication schemes to detect velocity anomalies i.e., determine the distance between where the first login was made and the second login attempt possibly attack is another reason for increased in the number of successful attacks on m-payments platforms. For instance, it is not possible for a user login from Istanbul, Turkey by 12 noon, and try to login again from Abuja, Nigeria by 12:30 or 13:00 PM as 1hour may not be enough for one to travel from Istanbul, Turkey, to Abuja, Nigeria.

2.6.4 Trends in M-banking and M-payments Studies

Based on the discussion above, and comments from literature, it can be said that majority of the m-banking studies included in the review focused on user authentication e.g., see (Apostolopoulos et al., 2013; Barkadehi et al., 2018; Khattak et al., 2021; Parker et al., 2015; Sinigaglia et al., 2020; Y. Wang et al., 2016; Zimmermann & Gerber, 2020). The increase in the number of m-banking studies, especially in the area of user authentication may not be unconnected with the increase in the number of online scams in order to highlight the challenges connected with the present authentication methods. Some of the studies proposed a framework for m-banking verification e.g., see (Abo-Zahhad et al., 2014; Aithal, 2015; Alhothaily et al., 2018; Basar et al., 2019; Chen et al., 2017; Karim et al., 2020; Nagaraju & Parthiban, 2015; Soviany et al., 2016; Thomas & Goudar, 2018). While others examined m-banking safety and secrecy in general e.g., see (Cavus et al., 2021a; Laukkanen, 2016; Liao et al., 2020; Malaquias & Hwang, 2019; Sharma & Sharma, 2019; Wang et al., 2021; Yang et al., 2015). Thus, it can be said that majority of the studies published in recent past focused on user authentication methods, safety, and secrecy issues.

Although, majority of present m-banking studies focused on protection, secrecy, and authentication issues affecting m-banking continued patronage and progress, Cavus et al. (2021a) in their study argued that people concern for safety and secrecy still remain the main reasons for customers lack of interest, and slow progress of m-payment systems e.g., m-banking, especially in countries with emerging digital payment systems (i.e., developing nations). Furthermore, Chanajitt et al. (2018) and Vishnuvardhan et al. (2020) in their studies argued that security still remain an issue not only for imbursement institutions, but also customers due to the vulnerability issues associated with the present authentication techniques employed by imbursement institutions. Similarly, Chaimaa et al. (2021) examined the problems associated with biometric and other verification schemes used by payment institutions. The authors argued that different biometric methods employed by banks were also susceptible for attacks via surface utilized by legitimate user. Thus, stressed the need for a strong artificial intelligence method that can detect and handle velocity anomalies. Table 4, depicts authors name/year of publication, number of citations, published magazines, and purpose of the studies included in the study SLR process.

Table 4.

Information Extracted from the Studies Included in the SLR Process

Authors Name/Year	**Number of Citations**	**Published Magazine**	**Purpose of the study**
Cavus et al. (2021a)	C = 16	Sustainability	To inspect the effects of “security and privacy on m-banking growth”.
Khattak et al. (2021)	C = 02	Multimedia System	To evaluate the security of “Internet Banking Services” (IBS) via deep assessment of big data.
Asnakew (2020)	C = 15	Review of Socio-Network Strategies	To examine the effects of antecedent variables in customers’ intent to use m-banking service channels.

Table 4 (Continued).

Karim et al. (2020)	C = 15	Journal of Information Security and Applications	To assess the challenges of different user authentication procedures in an online environment.
Sinigaglia et al. (2020)	C = 17	Computers & Security	To investigate the robustness and complexity of different multi-factor authentication (MFA) deployed by banks.
Wang et al. (2020)	C = 27	Computers & Security	To examine the security deficiencies of multi-factor authentication (MFA) systems in multi-server environment.
Zimmermann and Gerber (2020)	C = 37	International Journal of Human-Computer Studies	To investigate individual perceptions that influenced "adoption and usage" of a particular verification scheme used by banks and other "m-payment" systems organizations.
Albashrawi and Motiwalla (2019)	C = 56	Information Systems Frontiers	To assess the influence of personalization and secrecy issues on recurrent and continual usage of m-banking services.
Bani-Hani et al. (2019)	C = 24	Procedia Computer Science	To examine the most usual online verification schemes deployed by banks and possible third parties' attacks against these schemes.

Table 4 (Continued).

Basar et al. (2019)	C = 13	Procedia Computer Science	To examine the problems associated with “biometric and sensor” verification schemes in m-banking stations.
Kemal (2019)	C = 13	Information Technology for Development	To assess m-banking usage by women recipients, and effects of new innovations on organizational Properties.
Merhi et al. (2019)	C = 136	Technology in Society	To investigate the main factors that facilitate or hinder m-banking progress from multi-cultural context.
Sharma and Sharma (2019)	C = 237	International Journal of Information Management	To inspect the effect of privacy and channel excellence on “m-banking” continual usage.
Sharma (2019)	C = 101	Information Systems Frontiers	To investigate the effects of privacy and autonomous motivation in m-banking.
Malaquias and Hwang (2019)	C = 96	International Journal of Information Management	To assess the key determinants of m-banking usage.
Alalwan et al. (2018)	C = 270	Journal of Retailing and Consumer Services	To investigate different theoretical replicas that best describes the main influencing factors of m-banking usage.

Table 4 (Continued).

Alhothaily et al. (2018)	C = 03	Procedia Computer Science	To inspect the challenges of fingerprint and other sensors-based verification methods.
Asongu (2018)	C = 90	Journal of the Knowledge Economy	To inspects m-banking determinants and smartphones penetration in relation to safety and secrecy issues.
Barkadehi et al. (2018)	C = 65	Telematics and Informatics	To assess the usability and weaknesses of different m-banking user verification schemes.
Kiljan et al. (2018)	C = 42	Future Generation Computer Systems	To examine the different verification techniques used by banks, and issues related to the proposed ones.
Tandon et al. (2018)	C = 79	“Information Systems and e-Business Management”	To examines the effects of website functionality and perceived security on m-banking and online shopping.
Barkhordari et al. (2017)	C = 91	“Information Systems and e-Business Management”	To investigate the influence of safety and secrecy in m-banking and other electronic payments systems.
Chen et al. (2017)	C = 33	Wireless Personal Communications	To examines m-payment verification issues for customers, brokers, and banks

Table 4 (Continued).

Gupta et al. (2017)	C = 47	Information Technology for Development	To investigate the effects of security levels, risk, and control mechanism on m-banking espousal and continual usage
Ammar and Ahmed (2016)	C = 46	Cogent Business & Management	To assess the influence of safety, secrecy, and other factors on m-banking channels.
Boateng et al. (2016)	C = 160	Computer in Human Behavior	To examine the main determinants of "internet banking"
Laukkanen (2016)	C = 425	Journal of Business Research	To inspects the influence of security, values, privacy, and "image barriers" on consumers decisions to adopt or reject m-banking
Malaquias and Hwang (2016)	C = 333	Computer in Human Behavior	To examine the possible determinants of secrecy and protection issues in m-banking.
Qasim and Abu-Shanab (2016)	C = 168	Information Systems Frontiers	To offer better understanding of security and privacy factors influencing m-banking progress.
Soviany et al. (2016)	C = 05	Conference proceedings	To assess the security challenges of mobile apps e.g., "m-banking and m-Health".

Table 4 (Continued).

Y. Wang et al. (2016)	C = 86	Conference proceedings	To investigate m-payments security, threats and challenges
Montazemi and Qahri-Saremi (2015)	C = 273	Information & Management	To investigate factors affecting customers' "Pre-adoption and Post-adoption" of m-banking
Shaikh and Karjaluoto (2015)	C = 928	Telematics and Informatics	To "analyze and synthesize" present m-banking studies
Shaikh et al. (2015)	C = 61	Journal of Financial Services Marketing	To inspects the significance of security and privacy on m-banking conduits continual usage
Yang et al. (2015)	C = 339	Computers in Human Behavior	To examines the effects of "risk" and "trust" on customers behaviours towards m-banking
(Nagaraju & Parthiban, 2015)	C = 38	Journal of Cloud Computing	To investigate m-banking data security and privacy concerns, and to determine their influence on "m-banking continual patronage".
Abo-Zahhad et al. (2014)	C = 81	Signal, Image and Video Processing	To examines the different biometric verifications schemes

Table 4 (Continued).

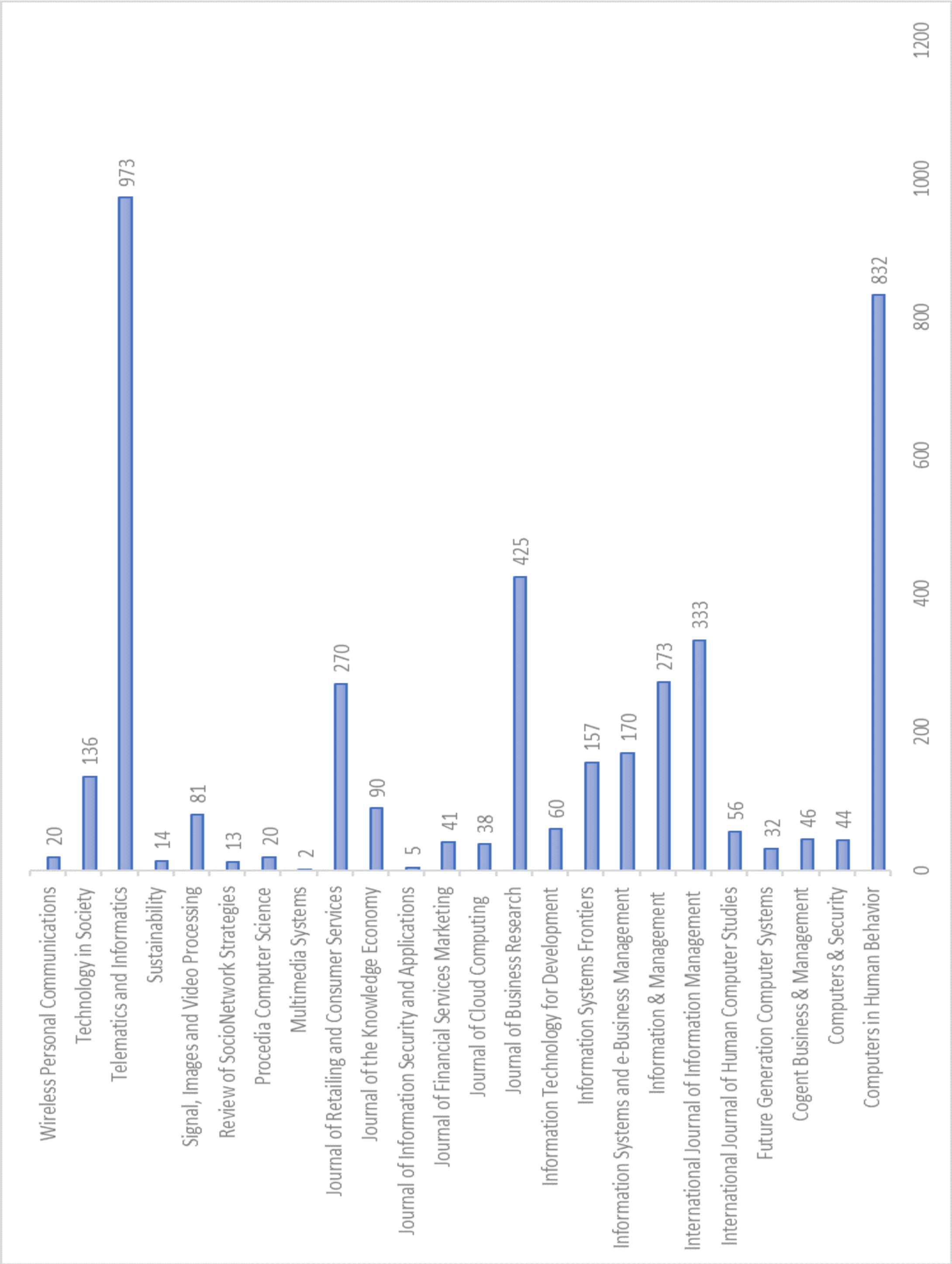
Apostolopoulos et al. (2013)	C = 35	Conference proceedings	To examine the vulnerability of user credentials deposited in “Android mobile devices”

2.6.5 Most Cited M-banking Studies

Based on the review extracted citations data, as seen in Table 4, the most cited articles are; Shaikh and Karjaluoto (2015) n = 928, Laukkanen (2016) n = 425, Yang et al. (2015) n=339, and Malaquias and Hwang (2016) n = 333 signifying the increased in number of m-banking research conducted from 2015-to-2021. Similarly, studies that received the highest number of citations were published in Telematics and Informatics (n = 973), Computers in Human Behavior (n = 832), and Journal of Business Research (n = 425) in the years 2015, 2016, and 2018, signifying the quality of studies published in high impact magazines. Furthermore, the number of citations received by the above-mentioned studies clearly highlights the importance of safety and secrecy, and justify the growing trends in m-banking studies, especially in the areas of security.

Figure 5.

Number of Citation Per Journal



The purpose of conducting the SLR (Systematic Literature Review) is to examine the influence of safety, secrecy, and user authentication challenges on m-banking expansion and customers continued commitment from extant literature with the view to identify the missing gaps in the literature in order to propose an AI-based anomalies and user verification framework for the design of an AI-based system which may possibly reduce and/or solve the problems. Though, few authentication frameworks were offered in recent past, current m-banking studies highlight some of the key reasons why user authentication still remains an issue in m-banking. For instance, Kiljan et al. (2018) examined the different authentication techniques deployed by banks and frameworks offered by scholars. The authors argued that present authentication approaches neglect or casually considered the following issues; login anomalies, user intellectual capacity, active participation, honesty, action, and other “m-banking essentials” while designing the different schemes. These and other problems led to the failure of the existing verification schemes to adequately protect clients, and payment institutions from attacks.

2.7 Machine Learning Techniques

Deployment and use of Machine Learning (ML) techniques is increasingly becoming popular among scholars not only in engineering and science-based fields, but also in social and behavioural sciences due to its precision in prediction, classification, clustering, and pattern recognition (Salloum et al., 2020). In ML techniques tasks were assigned to a computer-based program to perform, and the machine gains more experience in performing these tasks, as it may continue to learn from its knowledge in case of quantifiable performance which in turn improves its performance on these tasks. Thus, the machine can make predictions and take decisions based on dataset concerning a particular problem e.g., cybersecurity, mortality, intrusion detection (Martínez Torres et al., 2019). For instance, computers can learn to predict “bank insolvencies” i.e., indebted individuals and organizations who may not be able to pay back their debts, or predict disease e.g., cancer from health investigations report of a patient (Petropoulos et al., 2020). Performance of the machine will improve as it gains more knowledge about the problem under investigation by analysing more reports. Also, performance of ML models is usually measured by counting the number of accurate detections and predictions of cases, in this case cyber-attack.

Nowadays, ML is widely used in different fields such as; robotics, health diagnosis, traffic noise forecast, pattern recognition, data mining, agricultural advisory, product recommendations, predictions of company market share, and cyber-crime.

Generally, ML addresses three different kinds of problems; i) regression, ii) clustering, and iii) classification. Each depends on the categories and types of training and testing dataset needed to choose from the available methods; “supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning” in order to apply the most suitable ML algorithm (Osisanwo et al., 2017: p.7).

2.8 Missing Gaps in Prior M-banking Studies

Despite the facts that quite a number of studies were conducted in an attempt to find explanations regarding factors influencing “m-banking” acceptance and continued usage. Safety and secrecy issues, and vulnerabilities of different verification systems employed by banks remain under-examined but merit detailed examination. Findings of the SLR exposed intrusion through other applications stuffed in mobile device, network vulnerability, malicious insiders’ attacks, “financial malware attacks”, and absence of classy security apparatus to be the key protection and privacy issues upsetting the expansion of “m-banking” in majority part the world. Also, outcomes of the study highlight other aspects of “m-banking” safety and secrecy issues that requires separate examination, and susceptibilities of present “authentication schemes” used in m-banking systems. Key findings of the SLR were discussed in chapter five (results and discussions) in a complete manner.

CHAPTER III

METHODOLOGY

In this chapter, algorithms, conceptual model, and pseudocodes of the proposed AI-based authentication and anomalies detection systems, and usability testing results were presented. Also, the study procedures (i.e., methodology) consisting of research design, choice of study areas, data gathering tools, samples, and approaches employed to scrutinize the study collated data were also offered in the chapter.

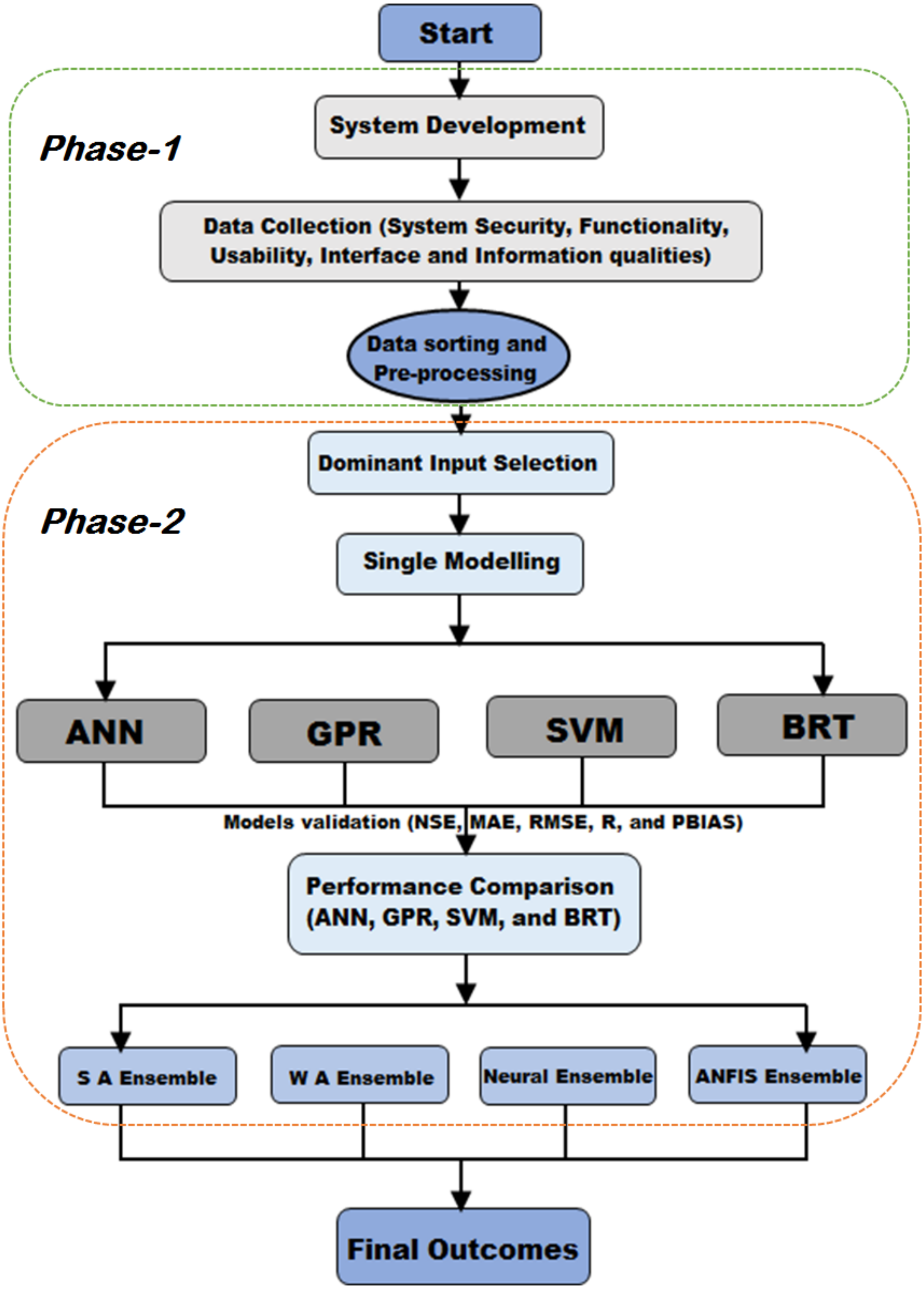
3.1 Study Design and Model

The study is a "Model-Driven Approach" which aimed at investigating the effects of security, privacy, and users' authentication challenges on mobile payment systems, specifically m-banking using four different AI-based models i.e., "Gaussian process regression" (GPR), "Boosted regression tree" (BRT), "Artificial neural network" (ANN), and "Support vector machine" (SVM) in order to overcome the limitations of the classical models. Mixed-method was employed (i.e., combination of qualitative and quantitative approach), due to the investigative nature of the study. The quantitative approach was used in weights assignment, and "aggregate values calculations" for all the extracted related studies during the reviewed process (i.e., Systematic Literature Review and Meta-Analysis process) in order to select the most appropriate studies that are relevant to the research. Also, the quantitative approach was used in analyzing the sensitivity of each of the study variables (i.e., system security, privacy, ease of use, interface and information qualities) in order to select the most dominant variable by calculating the "average coefficient of determination" (*DC*) of all the parameters. While, the qualitative approach was used to collect primary data from the study participants. Research of this kind requires data from primary source (Asastani et al., 2018). Data from participants is critical for this research due to the delicate nature of the issues under examination in the study areas. Thus, the need to obtained first-hand information from the participant in order to have better understanding of the issues hindering the progress of "m-banking" in the study locations.

The study methodology consists of two phases with six key stages as shown in Figure 6. This involves system development, selection of study areas and data collection in the first phase, while data sorting and pre-processed, key inputs selections, development of 4 single machine learning (ML) models validation of the study developed ML models, and the ensemble techniques were carried out in the second phase.

Figure 6.

Study Proposed Methodology


Start
Phase-1
System Development
Data Collection (System Security, Functionality, Usability, Interface and Information qualities)
Data sorting and Pre-processing
Phase-2
Dominant Input Selection
Single Modelling
ANN
GPR
SVM
BRT
Models validation (NSE, MAE, RMSE, R, and PBIAS)
Performance Comparison (ANN, GPR, SVM, and BRT)
S A Ensemble
W A Ensemble
Neural Ensemble
ANFIS Ensemble
Final Outcomes

3.2 Hypothesis

The main aim of this study is to investigate the impacts of security on “m-banking” advancement in Nigeria, Iraq, and Cyprus, and propose an AI-based authentication and anomalies detection system for improved m-banking security in emerging digital payment markets. To achieved these research objectives the following hypothesis were formulated:

- **H1:** There is a strong correlation between security parameters and people intend to use, and continuous patronage of m-banking in the study locations.
- **H2:** The AI based models estimate the influence of security on m-banking with higher precision.
- **H3:** The ensemble approach could enhance the estimation precision of the distinct AI models.
- **H4:** The proposed AI-based authentication and anomalies detection systems could be more robust and reliable compared to other verification schemes presently used by payment institutions.

3.3 Participants

The study is a cross-country approach. Therefore, participants for the study were drawn from three (3) different studies locations i.e., Nigeria, Cyprus, and Iraq (see Appendix – C). The three countries were choosing on the basis of continents (i.e., Africa, Asia, and Europe) in order to have better thoughts regarding the effects of security and confidentiality on “m-banking conduits”, and assess the robustness of the study proposed AI-based system in terms of protection, secrecy, ease of usage, interface qualities, anomalies detection from continental perspectives. Though, the research data was collected from three different (3) study locations, but the main study area of this research is Nigerian being the most underdeveloped nation among the three countries in terms of technological advancement. A total of nine hundred and ninety-six (996) responses were received from the three (3) different studies locations (i.e., Nigeria, Cyprus, and Iraq) out of which nine hundred and seventy-eight 978 (98.2%) were found to be valid and usable which is an “excellent response return rate for study with twenty-four (24) usability testing questionnaire items” as per (Fadlelmula et al., 2015: p.14). Additionally, to further confirm the study collected data excellent return rate, “Raosoft sample size software” a popular online software for calculating sample size was used to checked the accepted level of study sample size with "5% marging of error", "95% confidence level" and "50% response distribution" for the 996 study collected data. Recommended sample size result obtained from the software is (278) signifying the excellent return rate of the study collected data (978).

For the nine hundred and seventy-eight (978) valid and usable responses obtained from participants, seven hundred and six (706) responses were from Nigeria, accounting for (72.2%) of the total valid response obtained. This is because the main focus of this research is to address the problems associated with Nigerians mobile payment system, specifically m-banking system considering the few numbers of customers that utilized the service channel in the country, and vulnerability of the countries' financial system, especially "mobile payment systems" (Brody et al., 2020; Cavus et al., 2021a). While, one hundred and sixty-two (162) Cypriot partook in the study accounting for (16.6%) of the total participants, and one hundred and ten (110) participants are from Iraq which represent (11.2%) of the study usable response.

As shown in Table 5, the study sample comprised of 582 (59.5%) male respondents' and 396 (40.5%) female respondents. The proportion of the study gender dispersions were inconsequential, signifying the increased in female participation in scientific research that involved technological adoption and usage, especially in the areas of virtual payment systems (Glavee-Geo et al., 2017) For participants age, the age category that participated most in the study were young people whose age ranges between 26-35 which account for 567 (58.0%) of the study sample, and 18-25 whose account for 183 (18.7%) of the study sample, signifying younger generation passion for innovative banking and financial technologies (Tavera-Mesias et al., 2021). Furthermore, Giovanis et al. (2018) and Ofori and El-Gayar (2021) in their studies argued that "young people (Gen Y) are more likely to embrace new technologies e.g., m-banking as they are more used to social networking sites than the elderly people (Gen X)". Thus, always constitute majority of participants for research that involves investigation of newer technology acceptance and usage. while respondents between the ages of 36 and above account for 228 (23.3%) of the total participants.

For educational qualifications, respondents with "Bachelor Degrees and/or Higher National Diplomas" constituted majority of the participants, as they account for 569 (58.2%) of the total participants, followed by participants with "Masters Degrees or higher" signifying the quality, accuracy, and reliability of the responses obtained. While respondents with "secondary school certificates" (SSCE) account for 135

(13.8%), and those with "National Diplomas" (ND) account for 124 (12.7%) of the total participants. For "employment status" of the respondents, students constituted the majority of the participants as they account for 368 (37.6%) of the study sample, followed by academics 220 (22.5%) affirming the quality and reliability of the responses obtained in the study. While 215 (22.0%) of the responses were obtained from other civil servants (i.e., public and private employees). Business individuals account for 162 (16.6%) of the study total usable response. To check the robustness of the study Proposed AI-based system, 13 (1.3%) online security experts participated in the study. The experts checked the security features, interface and information qualities of the proposed system, and confirmed that the system is capable of addressing some of the security challenges confronting not only m-payment systems (m-banking), but also other online verification challenges. Information regarding participants' demographic profile is presented in Table 5.

Table 5.

Sample Characteristics

Variables (Demographic)	Frequencies	Proportion
Nationality		
Nigeria	706	72.2
Cyprus	162	16.6
Iraq	110	11.2
Gender		
Male	582	59.5
Female	396	40.5
Age group		
18-25	183	18.7
26-35	567	58.0
36 and above	228	23.3
Educational qualification		
SSCE	135	13.8
ND	124	12.7
Bachelor/HND	569	58.2
Masters or higher	150	15.3
Employment status		
Academics	220	22.5
Students	368	37.6
Other civil servants	215	22.0
Business	162	16.6
Security experts	13	1.3

Note: (HND = Higher National Diploma; SSCE = Senior Secondary Certificate; and ND = National Diploma).

3.4 Study Areas Selection and Data Collection Tools

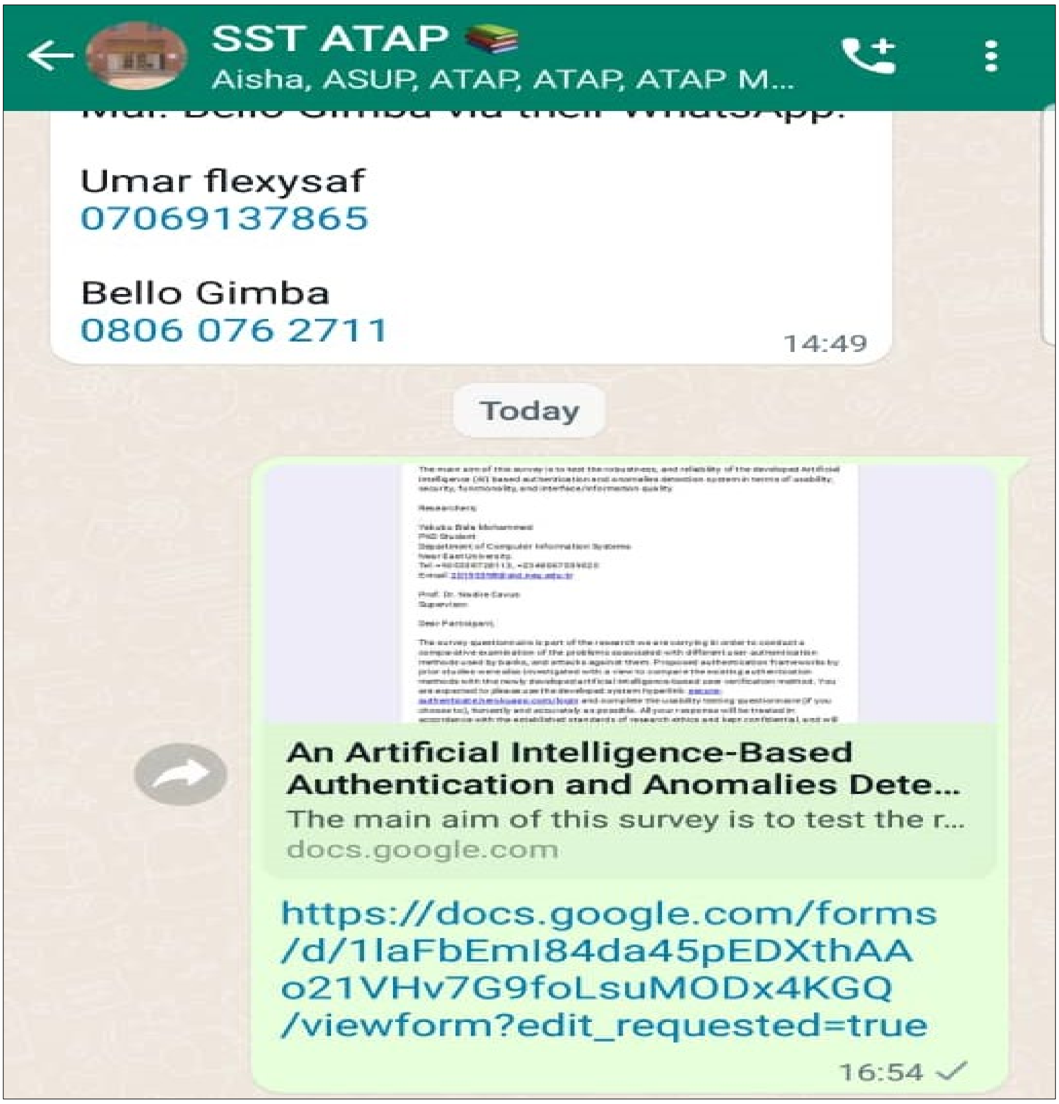
The study data was collected using “questionnaire method” as recommended by (Agarwal, 2011; Bahrammirzaee, 2010) that “questionnaire method” is the most appropriate technique for studies that involved investigation of human behaviour, feelings, and emotions toward a particular technology, especially in the testing of a newly developed systems in order to obtain users’ opinion regarding the functionality, interface and information quality of the developed system. The study “usability testing questionnaire” comprises of two parts; the first part (A), contained respondents’ characteristics details’ such as “age, gender, educational qualification, employment status, and nationality”, while the subsequent part (B) contained answers that best mirror participants’ opinion regarding the usability, secrecy, security, information and interface qualities of the study proposed system comprising of five (5) cluster queries system usability, system privacy, system security, interface and information qualities using “5-point Likert scale (see Appendix – C), ranging from (1) Strongly disagree to (5) Strongly agree in order to assess the study usability questionnaire items” as per (Wu & Leung, 2017).

The study data was collected using one of the most popular online data collection tools, (google form), in an anonymous manner i.e., the survey process was designed in such a manner that respondents’ details’ such as email, name, and IP address were not captured during response submission. The survey link was sent to the participants through social networking sites (e.g., Instagram, Facebook, Twitter, WhatsApp etc.,).

For the study AI-based techniques, Bhaskar et al. (2006) and Wei et al. (2013) in their studies argued that machine learning (ML) studies that involve regression problems e.g., human behaviour towards computer-based system such as m-payments systems (m-banking), traffic noise, energy loads, and clinical research” requires 80% - to - 90% valid response rate. Furthermore, the authors discovered that ML studies that have more than 90% valid responses hardly produce poor or inaccurate results. Thus, justifying the study excellent return rate of 98%, and accuracy of the study findings (Wei et al., 2013). Images of the study data collection tools were presented below.

Figure 7.

WhatsApp Data Collection (Academics Staff Platform)



SST ATAP

Aisha, ASUP, ATAP, ATAP, ATAP M...

Mal. Bello Gimba via their WhatsApp.

Umar flexysaf
07069137865

Bello Gimba
0806 076 2711

14:49

Today

The main aim of this survey is to test the robustness, and reliability of the developed Artificial Intelligence (AI) based authentication and anomalies detection system in terms of usability, security, functionality, and interface/information quality.

Researchers:

Yakubu Bala Mohammed
PhD Student
Department of Computer Information Systems
Near East University
Tel: [illegible]
Email: [illegible]

Prof. Dr. Nadire Cavus
Supervisor

Dear Participant,

The survey questionnaire is part of the research we are carrying in order to conduct a comparative examination of the problems associated with different user authentication methods used by banks, and attacks against them. Proposed authentication frameworks by prior studies were also investigated with a view to compare the existing authentication methods with the newly developed artificial intelligence-based user verification method. You are expected to please use the developed system hyperlink: secure-authenticate.herokuapp.com/login and complete the usability testing questionnaire (if you choose to), honestly and accurately as possible. All your responses will be treated in accordance with the established standards of research ethics and kept confidential, and will

An Artificial Intelligence-Based Authentication and Anomalies Dete...

The main aim of this survey is to test the r...

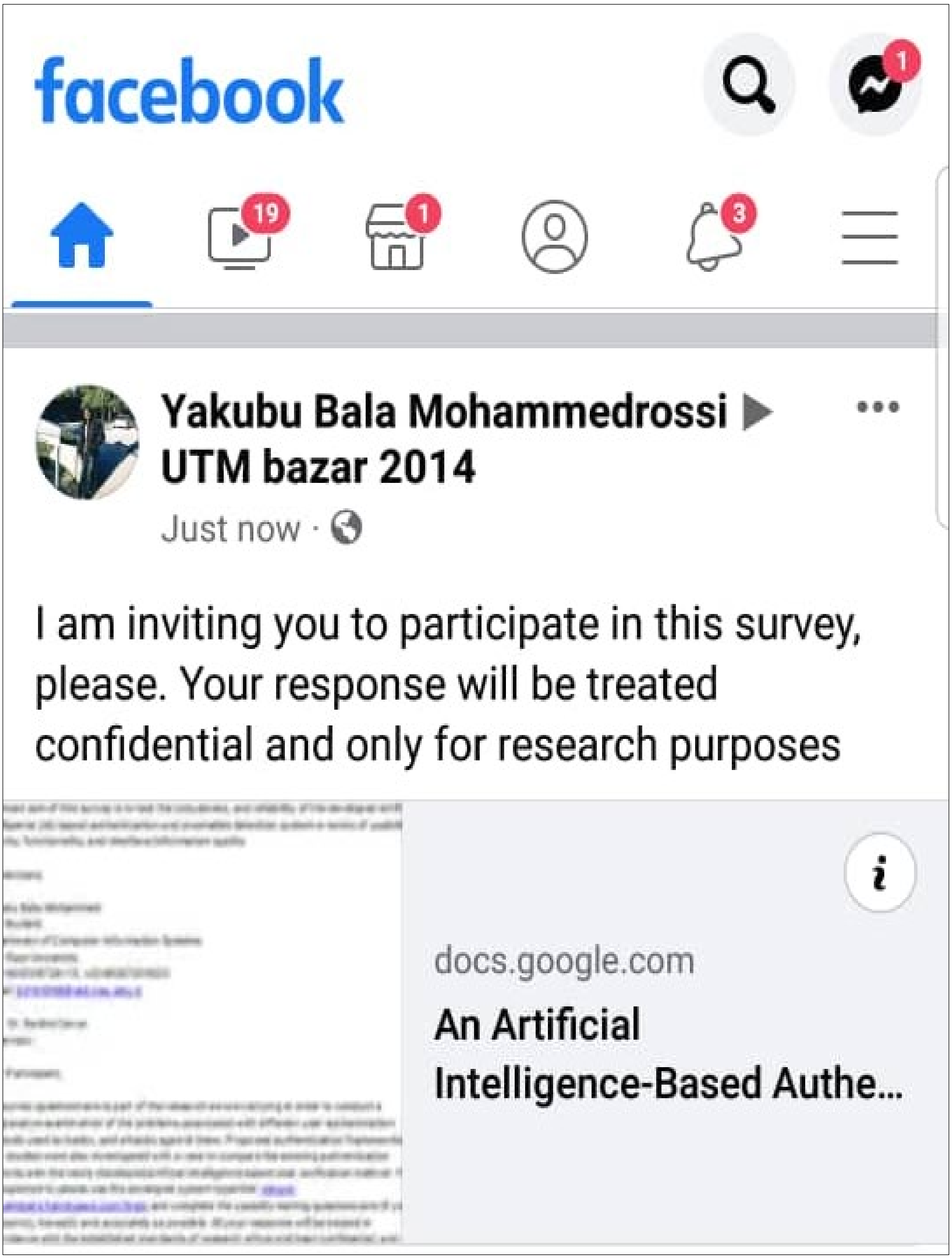
docs.google.com

https://docs.google.com/forms/d/1laFbEml84da45pEDXthAAo21VHv7G9foLsuMODx4KGQ/viewform?edit_requested=true

16:54 ✓

Figure 8.

Facebook Data Collection (Students' Platform)



Yakubu Bala Mohammedrossi ▶ UTM bazar 2014

Just now ·

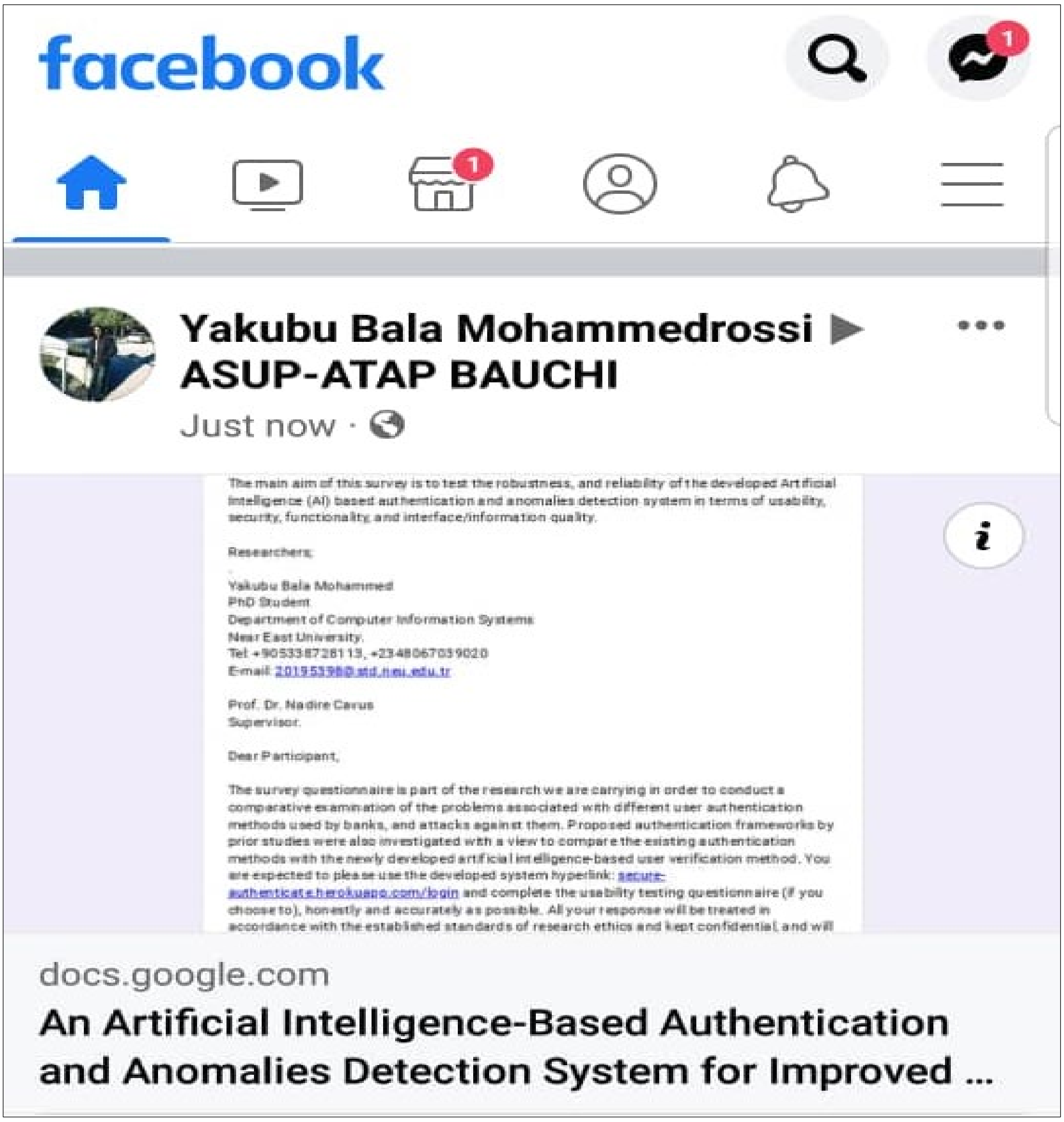
I am inviting you to participate in this survey, please. Your response will be treated confidential and only for research purposes

docs.google.com

An Artificial Intelligence-Based Authe...

Figure 9.

Facebook Data Collection (Academics Staff' Platform)



Yakubu Bala Mohammedrossi ▶ ASUP-ATAP BAUCHI

Just now ·

The main aim of this survey is to test the robustness, and reliability of the developed Artificial Intelligence (AI) based authentication and anomalies detection system in terms of usability, security, functionality and interface/information quality.

Researchers;

Yakubu Bala Mohammed
PhD Student
Department of Computer Information Systems
Near East University.
Tel: +905338728113, +2348067039020
E-mail: 20195398@std.neu.edu.tr

Prof. Dr. Nadire Cavus
Supervisor.

Dear Participant,

The survey questionnaire is part of the research we are carrying in order to conduct a comparative examination of the problems associated with different user authentication methods used by banks, and attacks against them. Proposed authentication frameworks by prior studies were also investigated with a view to compare the existing authentication methods with the newly developed artificial intelligence-based user verification method. You are expected to please use the developed system hyperlink: secure-authenticate.herokuapp.com/login and complete the usability testing questionnaire (if you choose to), honestly and accurately as possible. All your response will be treated in accordance with the established standards of research ethics and kept confidential, and will

docs.google.com

An Artificial Intelligence-Based Authentication and Anomalies Detection System for Improved ...

3.5 Data Analysis Methods

The study employed two data evaluation techniques, i.e., artificial intelligence-based approach, and structural equation modelling. The study data was processed and examined using “SPSS, and MATLAB” software’s. The SPSS package was used to analyzed participants’ characteristic details, and examined the uniformity levels of the study formulated theories. While MATLAB software was used to train and test the study employed AI based approaches so that effects of study input parameters on m-banking continuous patronage and advancement in the study locations can be estimated.

3.6 Structural Equation Modelling

A large number of studies in science, engineering, and social sciences uses “structural equation modeling” (SEM) approach for theories testing and advancement. For the purpose of this study, the method was used to analyzed the study sample characteristics profiles’ such as “nationality, gender, educational qualification, age, and employment status”. Also, the method was used to checked the reliability (i.e., internal consistencies) among the study formulated constructs of system security, and privacy in order to ensure that accepted level of consistency among the study formulated theories were attained using “Cronbach Alpha” (CA) and “composite reliability” (CR) due to the sensitivity nature of the study. CA and CR values greater than 0.90 indicate “an excellent level of uniformity among construct dimensions, while 0.90 very good, 0.80 good, 0.70 accepted, 0.60 questionable and 0.50 poor (Taber, 2018). Thus, the accepted level of uniformity amongst study constructs is 0.70 and above.

As shown in Table 6, only security and privacy dimensions items were checked using confirmatory (CA) and exploratory (CR) factors analysis, and the results clearly shows that the consistency level amongst the study formulated constructs were excellent signifying the uniformity of the items used in the study privacy and security constructs dimensions. Table 6 depicts the internal consistency results of the study formulated constructs.

Table 6.

Internal Consistency Results of the Study Formulated constructs (Security dimension)

Construct	Items	Load. (std.)	CA	CR
System Security	SysSeq1	0.902	0.912	0.963
	SysSeq2	0.901		
	SysSeq3	0.911		
	SysSeq4	0.878		
	SysSeq5	0.883		
System Security	SysPriv1	0.911	0.906	0.925
	SysPriv2	0.908		
	SysPriv3	0.966		
	SysPriv4	0.898		
	SysPriv5	0.914		

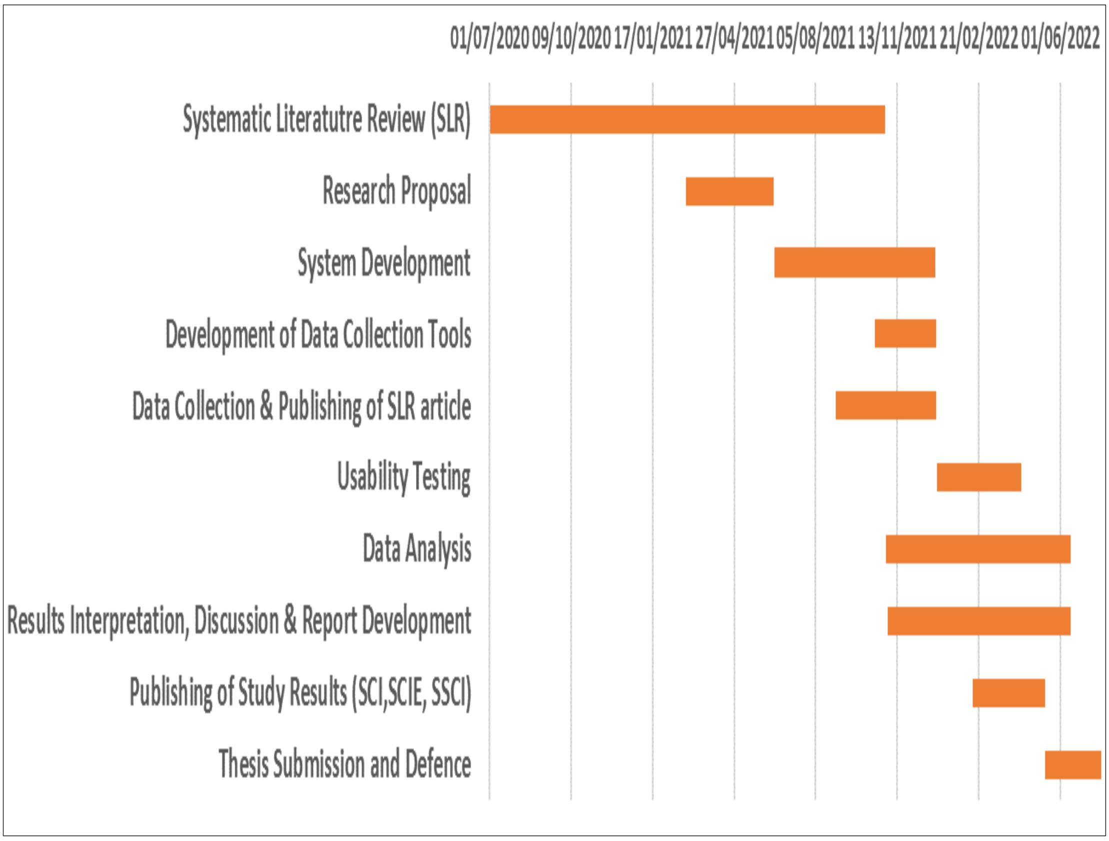
Notes: CR: Composite Reliability; CA: Cronbach's Alpha

3.7 Research Schedule

As shown in Figure 10, the research plan comprises of ten (10) major tasks; conducting “systematic literature review” (SLR), proposal, development of the proposed AI based system and data gathering tools, collation of the study data and publishing of SLR article. Also, in the agenda are; inspection of the study collated data using different approaches such as unit test, retesting, reliability testing and sensitivity check, followed by interpretation of results in a comparative manner and report development, publishing of results in high impact journals, thesis submission and defence. Figure 10 depicts the research plan with minimum start and maximum finished dates.

Figure 10.

Research Schedule



3.8 Methodology Phase I

3.8.1 System Development

Based on the study systematic literature review (SLR) findings, and remarks from prior m-banking studies which highlights the vulnerability of the present user authentication methods, and the need for more robust anomalies detection and authentication systems, the study proposed an artificial Intelligence-based anomalies and authentication system that is easy to use in terms of memorization, but more secured and robust compared to other authentication methods. The developed system can detect anomalies during login and take appropriate actions by considering certain parameters during the login process in order to differentiate legitimate users from attackers. The proposed system was deployed and tested in the study locations (i.e., Nigeria, Cyprus, and Iraq). Conceptual model, pseudocodes, and algorithms of the study proposed AI-based system is presented in the following subsections.

3.8.2 Conceptual Model of the Proposed System

As shown in Table 7, conceptual model of the study comprises of nine (9) stages ranging from login initiation to process termination.

Table 7.

Conceptual Model of the Proposed

Steps	Input – Process – Output Descriptions
Step: 1	Start login
Step: 2	Create a variable to count number of login (Login = login + 1)
Step: 3	Get user location, IP address, platform, and agent
Step: 4	Block and exit user IP address from login
Step: 5	Take user to second login in case user ID is not (modify 2 – way OTP)
Step: 6	Send/Re-send codes to users registered/alternate phone numbers
Step: 7	Codes not valid? Go back to step 4
Step: 8	Account access granted
Step: 9	End

3.8.3 Pseudocodes of the Proposed System

Pseudocodes of the study proposed AI-based system is presented in Table 8 consisting of five (5) key stages.

Table 8.

Pseudocodes of the Proposed

```
Begin the process:
          - The system begins the authentication process via the system interface.
          - Get user first login details (i.e., IP, Location, Platform, and Agent.
Initialize count total to zero:
          - Begin counting number of login (count = count + 1)
            If count is < = 3, and location, IP, platform, and agent are = first login, then
            grant account access,
            Else;
            Take user to second login (modify 2 – way OTP)
Initialize second login to zero:
            1st Step:   Send codes to Line1, & Line2
            2nd Step: Re-send codes to Line2, & Line1 (after 40 seconds in descending
order)
Compare codes:
             If codes are valid and supplied in their order, then grant access;
             Else; deny access
End process
```

3.8.4 Proposed System Algorithms

Based on comments from prior m-banking studies, the study proposed an AI-based anomalies detection and authentication system, with a modify - 2 - way OTP. As shown in Figure 6, the process begins with the user supplying his/her digital ID, via the "m-banking apps", after which the system verifies the digital ID, and number of failed login attempts. If number of failed attempts is fewer than or equal to three (3), the system obtained users' login information such as; device type, IP address, location, platform, and browser agent, before allowing the user to proceed to the next step. But where the number of failed attempts surpass the systems login limits (i.e., (failed login attempt), the system will redirect the process to the second login option i.e., the modified 2-way OTP. However, where users' login information is valid, the system grant access, else the system will take the user to the second login option in order to ensure that only legitimate users are granted access.

The novelty of the study proposed AI-based user verification scheme is that the proposed system can detect anomalies during login (i.e., velocity anomalies) as the system will artificially detect the usual location used by legitimate user to logon, detect any anomaly between first and subsequent logins, and prevent simultaneous login. For instance, where the proximity between the first login location and location where the second login attempt is made (in most cases attacks) are not near, and the time interval is not sufficient enough for the user to be in the second location, then the system blogs the login and direct the user to second login option. In the second login, the system will send OTP codes to two different phone numbers provided by the user i.e., users phone number and alternate phone number (i.e., Line1 and Line2) as against the one-way OTP presently used by banks where the OTP is sent to a single phone number or user email which may be compromise by attackers. The system will resent new codes after 40 seconds in reverse order i.e., to Line2 and Line1 instead of the first order. Account access can be granted only if the supplied codes are valid, else access will be denied. The reason behind this process (i.e., anomaly detection process) is that hackers usually used different locations other than the legitimate user location to carry out attacks during login or immediately after user logout. Figure 11, depicts the algorithm of the study proposed AI-based system.

Figure 11.

Proposed System Algorithms

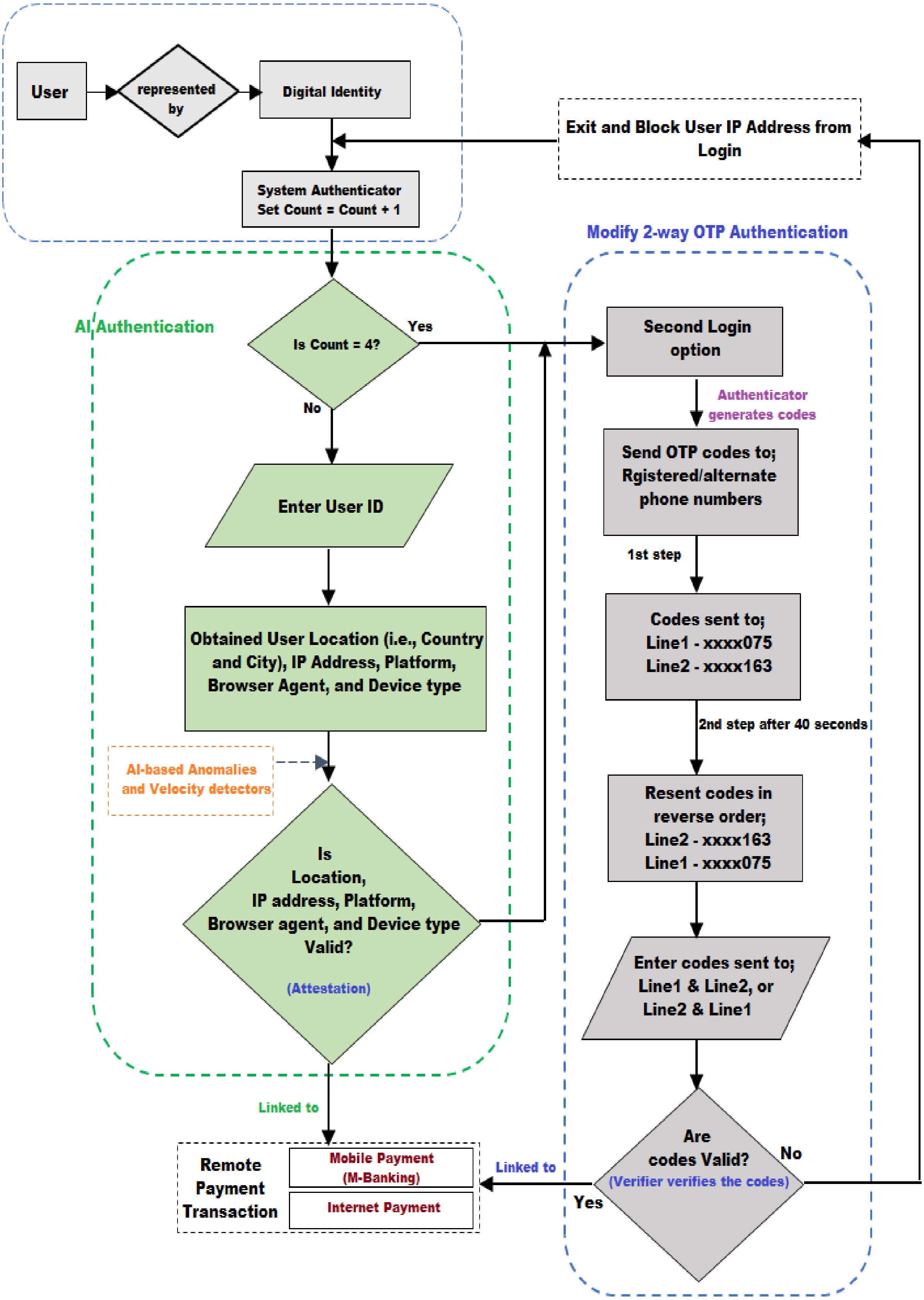
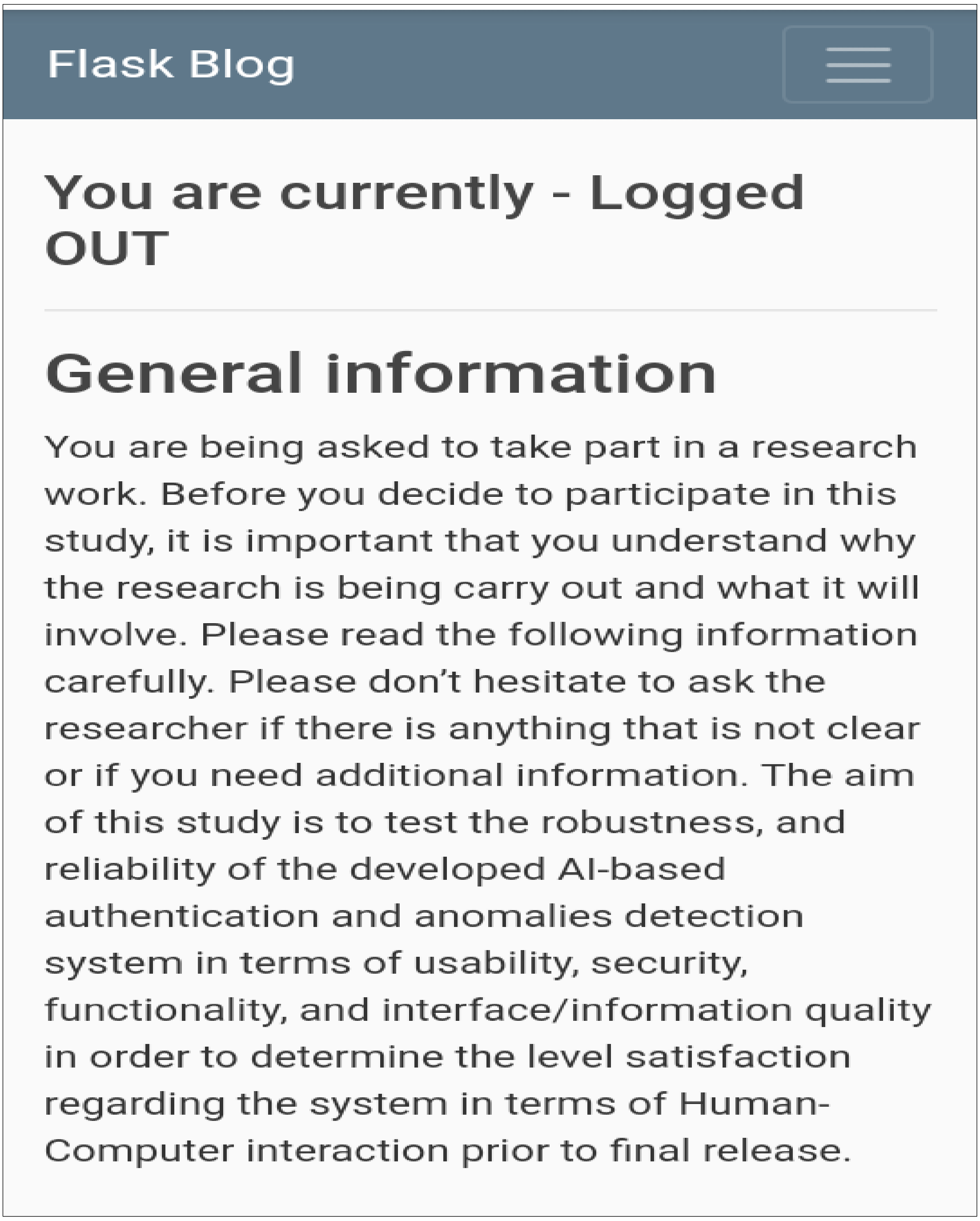

User
represented by
Digital Identity
Exit and Block User IP Address from Login
System Authenticator
Set Count = Count + 1
Modify 2-way OTP Authentication
AI Authentication
Is Count = 4?
Yes
No
Second Login option
Authenticator generates codes
Send OTP codes to; Rgistered/alternate phone numbers
1st step
Enter User ID
Codes sent to; Line1 - xxxx075 Line2 - xxxx163
Obtained User Location (i.e., Country and City), IP Address, Platform, Browser Agent, and Device type
2nd step after 40 seconds
AI-based Anomalies and Velocity detectors
Resent codes in reverse order; Line2 - xxxx163 Line1 - xxxx075
Is Location, IP address, Platform, Browser agent, and Device type Valid?
(Attestation)
Enter codes sent to; Line1 & Line2, or Line2 & Line1
Linked to
Are codes Valid?
(Verifier verifies the codes)
No
Yes
Linked to
Remote Payment Transaction
Mobile Payment (M-Banking)
Internet Payment

Figure 12.

Home Page of the Proposed System



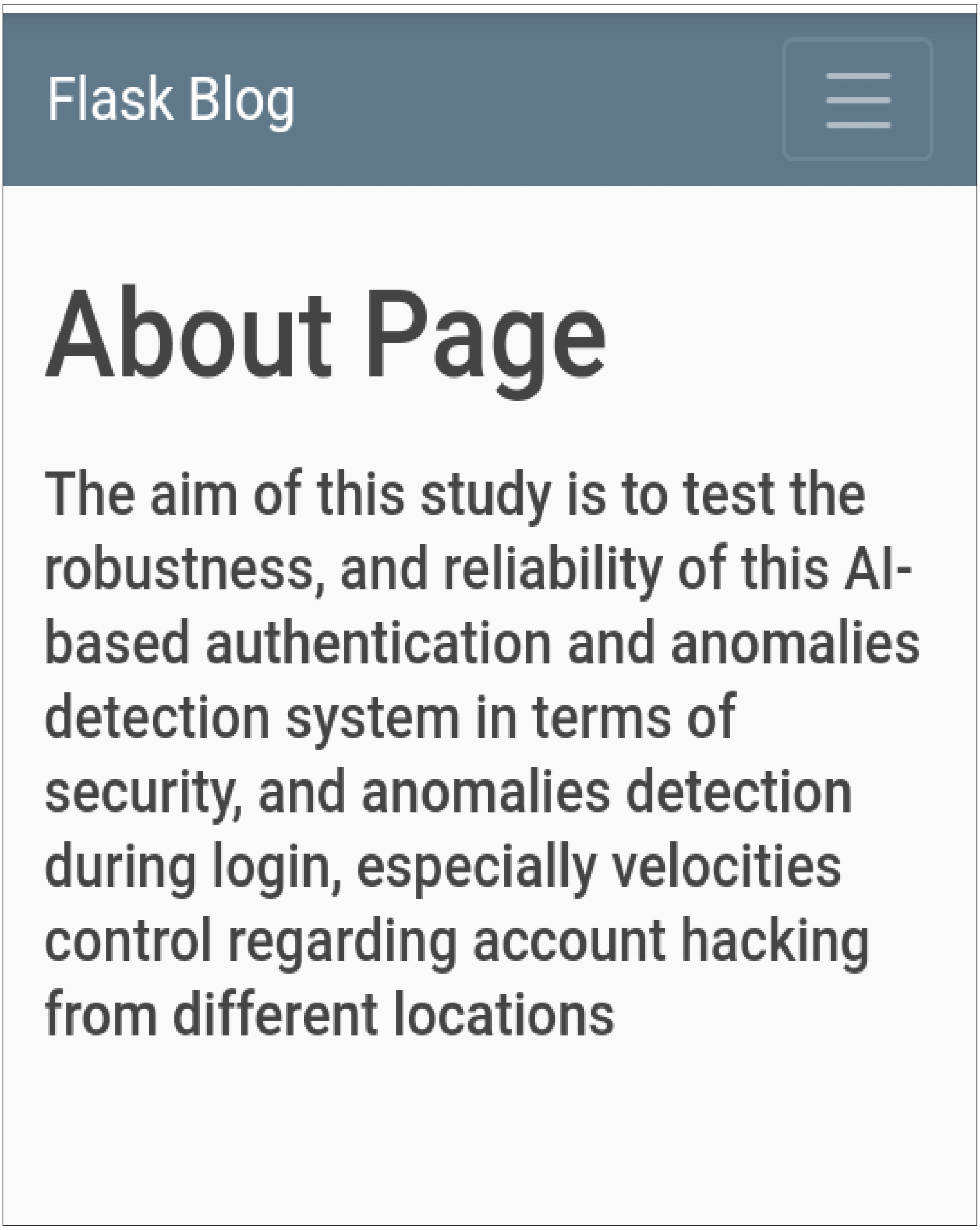
You are currently - Logged OUT

General information

You are being asked to take part in a research work. Before you decide to participate in this study, it is important that you understand why the research is being carry out and what it will involve. Please read the following information carefully. Please don’t hesitate to ask the researcher if there is anything that is not clear or if you need additional information. The aim of this study is to test the robustness, and reliability of the developed AI-based authentication and anomalies detection system in terms of usability, security, functionality, and interface/information quality in order to determine the level satisfaction regarding the system in terms of Human-Computer interaction prior to final release.

Figure 13.

About Page of the Proposed System

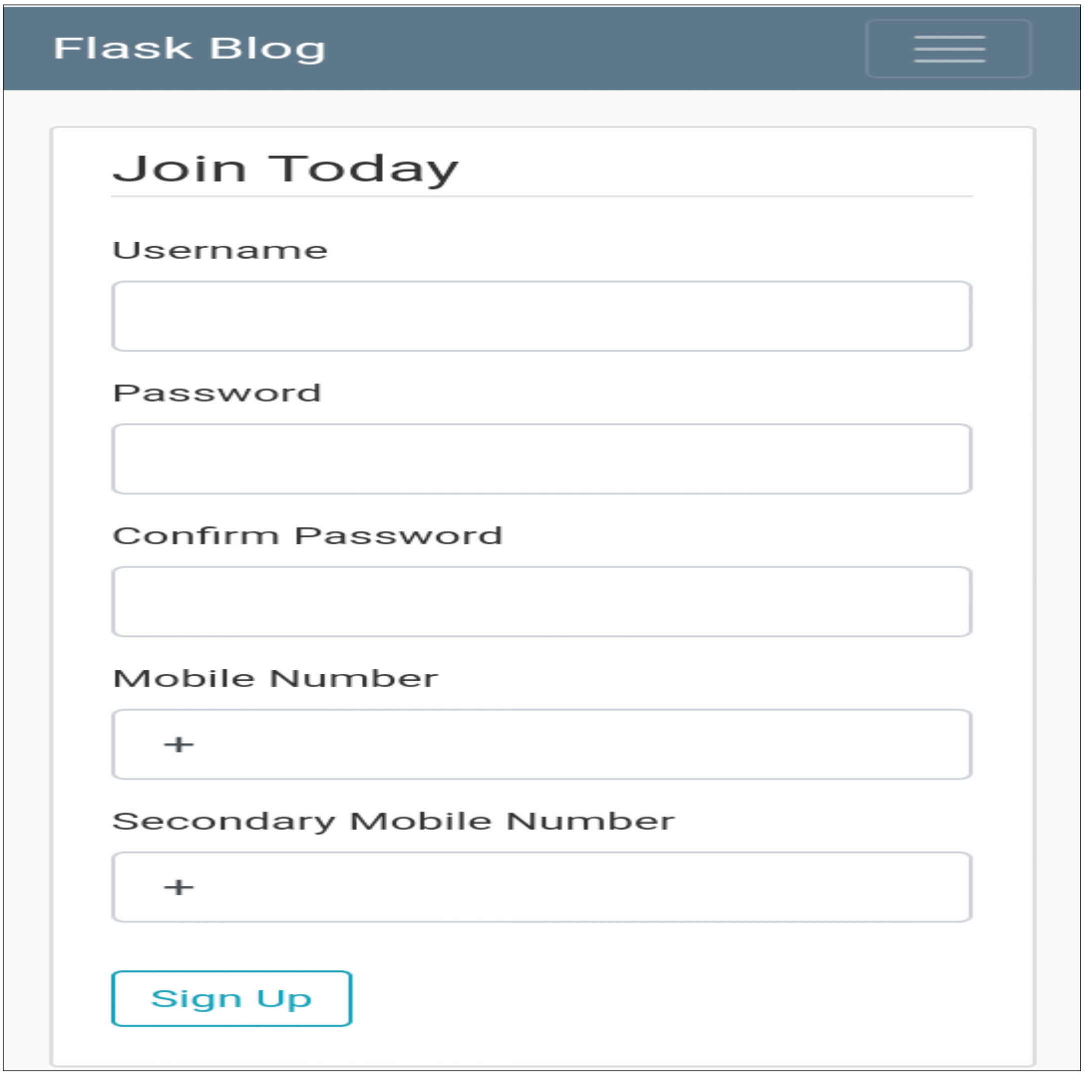


About Page

The aim of this study is to test the robustness, and reliability of this AI-based authentication and anomalies detection system in terms of security, and anomalies detection during login, especially velocities control regarding account hacking from different locations

Figure 14.

Sign Up Page of the Proposed System



Flask Blog

Join Today

Username

Password

Confirm Password

Mobile Number

+

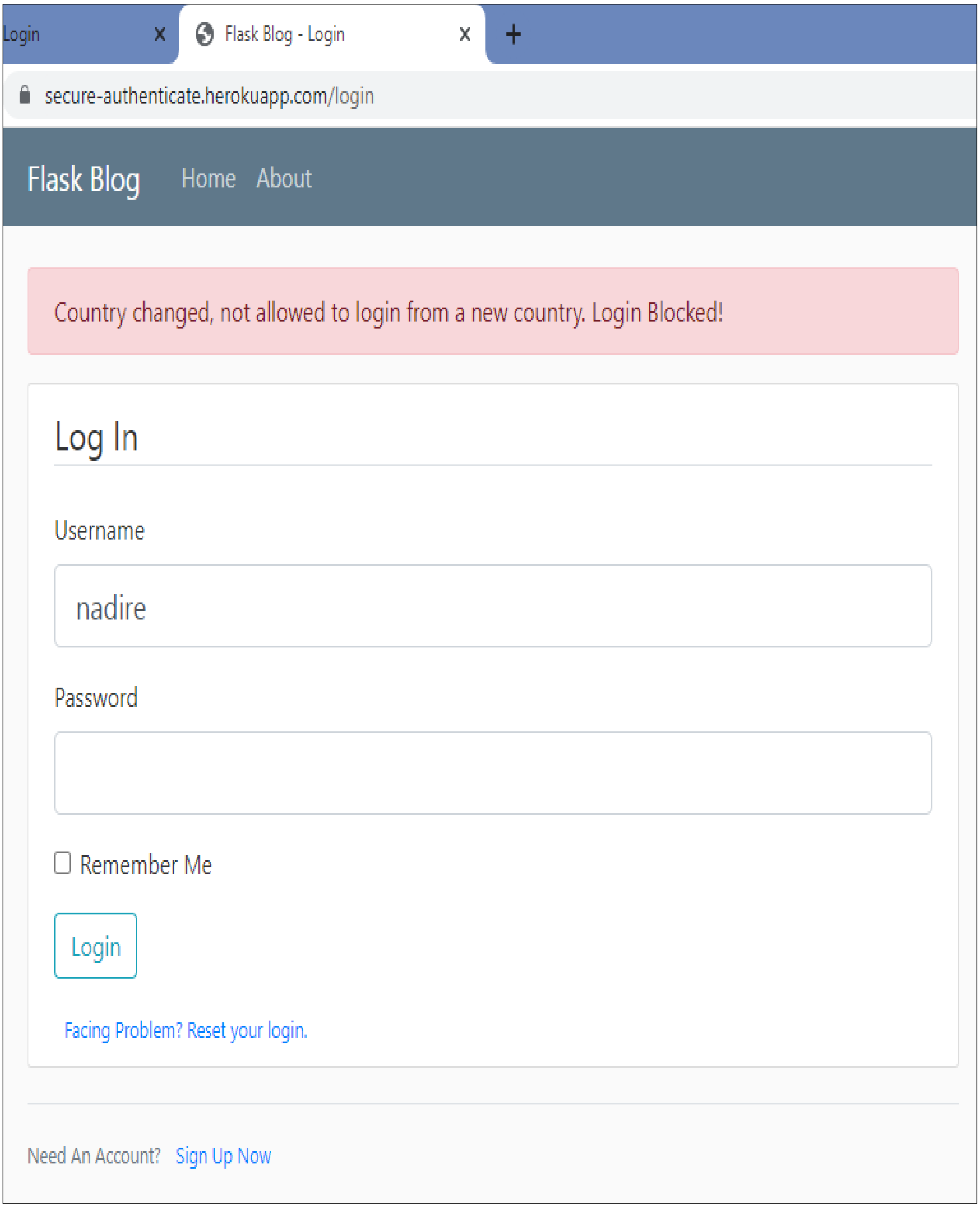
Secondary Mobile Number

+

Sign Up

Figure 15.

Country/Device Changes Detection



Country changed, not allowed to login from a new country. Login Blocked!

Log In

Username

nadire

Password

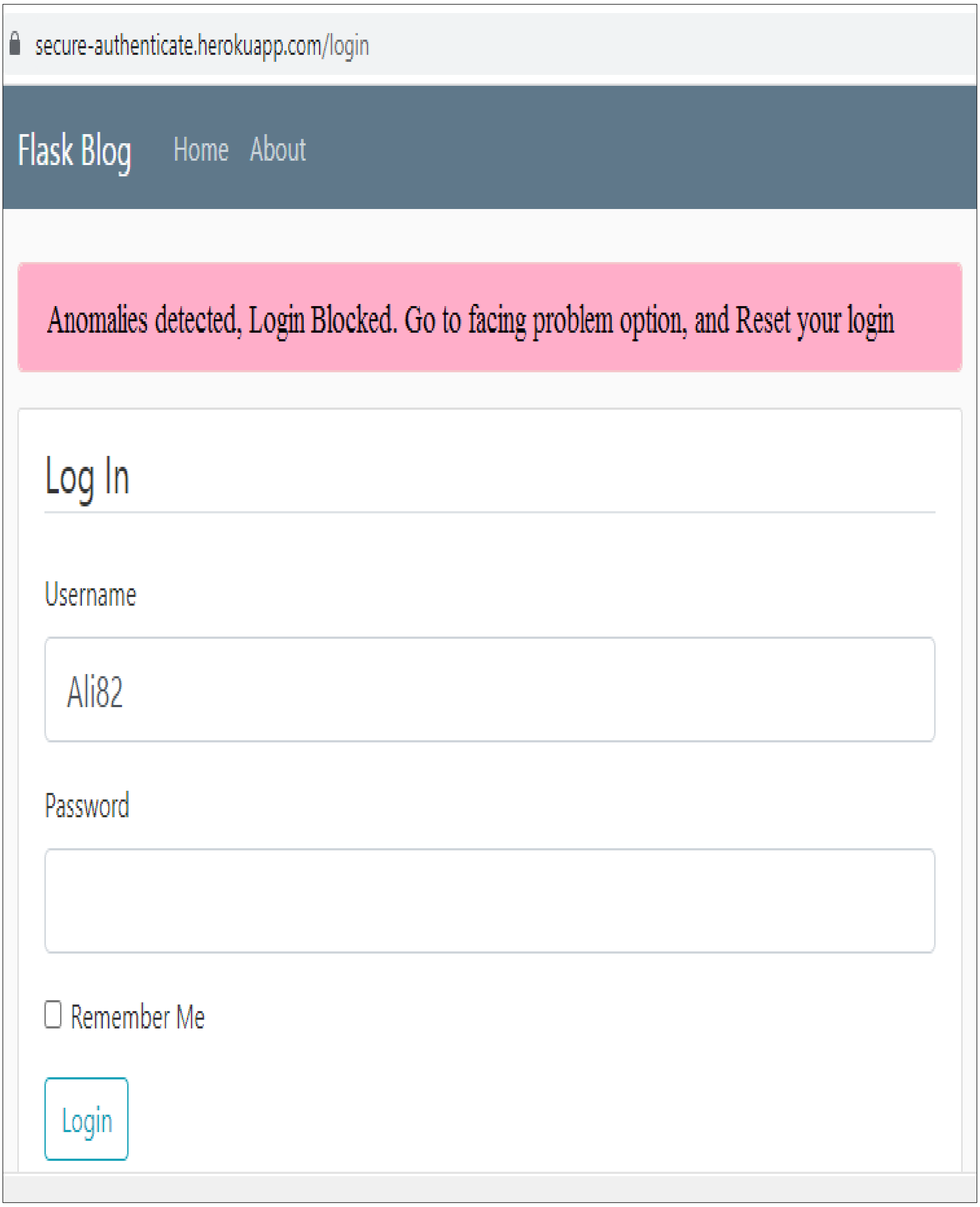
☐ Remember Me

Facing Problem? Reset your login.

Need An Account? Sign Up Now

Figure 16.

Velocity Anomalies Detection



secure-authenticate.herokuapp.com/login

Anomalies detected, Login Blocked. Go to facing problem option, and Reset your login

Log In

Username

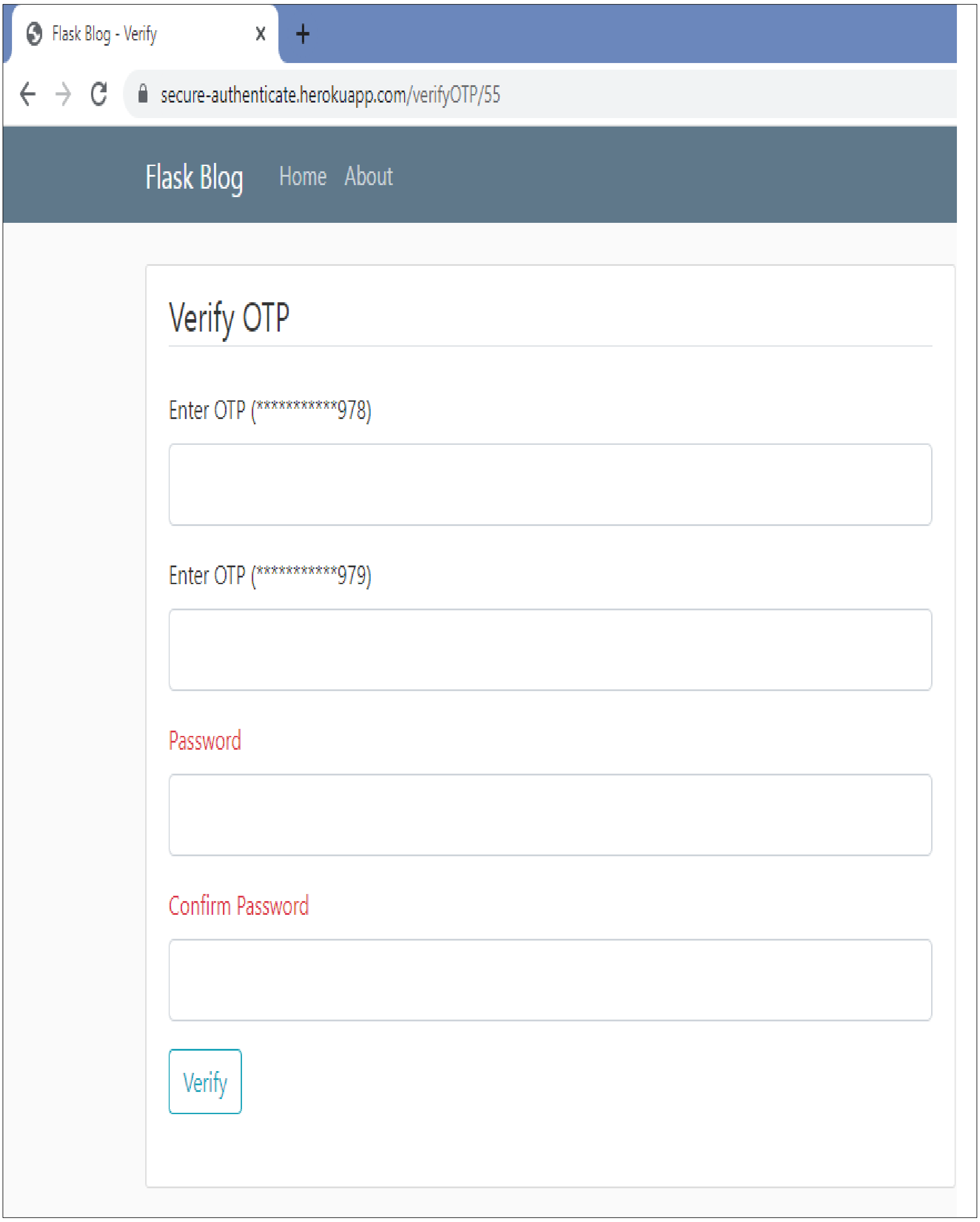
Ali82

Password

□ Remember Me

Figure 17.

Modify 2 - way OTP



Flask Blog - Verify

secure-authenticate.herokuapp.com/verifyOTP/55

Verify OTP

Enter OTP (***********978)

Enter OTP (***********979)

Password

Confirm Password

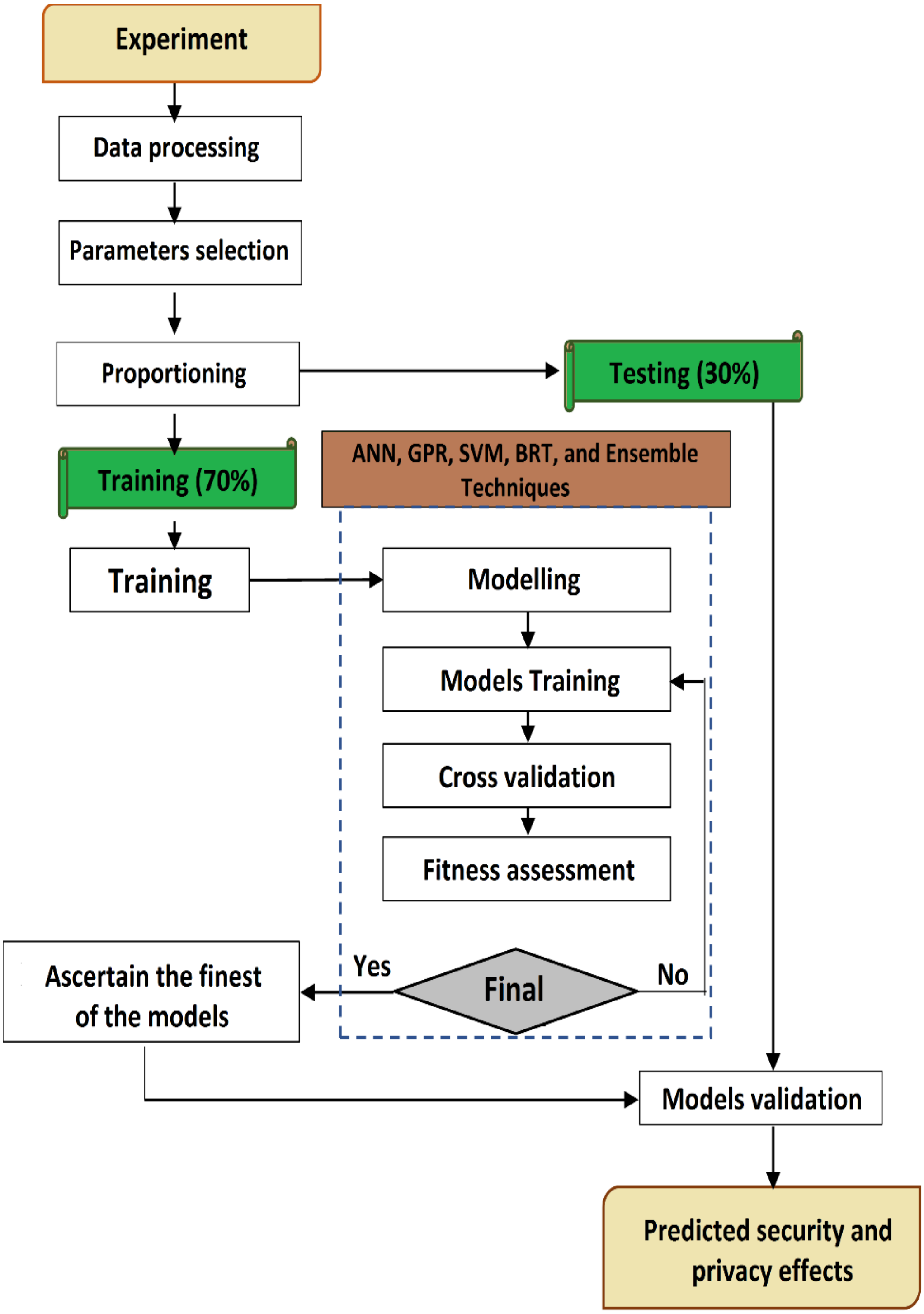
3.9 Methodology Phase II

In the second phase of the study process, effects of the study input parameters (i.e., security, privacy, usability, interface and information qualities) on the study dependent variable of m-banking patronage and progress were investigated and evaluated using 4 artificial intelligence (AI) based methods in order to determine the correlation between the variables.

The study phase methodology comprises of four key stages; stage I) data pre-processing and relevant parameters selection, stage II) models' development and validation, stage III) predictions of parameters influence on innovative financial and banking technologies, in this case m-banking from the study developed AI models were obtained and compared in the third stage. Lastly, in the fourth stage of the study process, a hybrid (i.e., ensemble) machine learning model was developed to enhance the performance of the single models using prediction outcomes of the study four AI models as inputs of the model using "Feed-Forward Neural Network" ensemble approach. Figure 18 portrays the structure of the study soft computing process (methodology phase II).

Figure 18.

Study Proposed Soft Computing Flow diagram (Methodology Phase II)



3.9.1 Artificial Intelligence Techniques

Literature (Merhi et al., 2019) have shown that factors affecting "innovative banking and financial technologies usage", specifically, m-banking systems growth in developing countries and few developed states are normally measured using classical models such as revised "DeLone and McLean (2003) model of Information Systems Success" that stressed the importance of autonomous parameter in computer-based system studies; Fishbein et al. (2007) updated "Theory of Reasoned Action" (TRA), which explained people's action from emotional stand point; Davis (1989) reviewed "Technology Acceptance Model" (TAM), Ajzen (1991) "Theory of Planned Behaviour" (TPB), Smith and McSweeney (2007) updated "Innovation Diffusion Theory" (IDT) for innovations adoption and use, and Venkatesh et al. (2012) lengthy "Unified Theory of Acceptance and Use of Technology" (UTAUT2). However, Cavus et al. (2021a) and Leitner-Hanetseder et al. (2021) in their studies argued that predictions based on conventional approaches (i.e., classical models) are generally "time consuming, bias-based, and sometimes produced inaccurate and unreliable results". Thus, the need for computer and engineering researchers to employs different AI-based methods (AI-based linear and non-linear models) such as "Artificial neural network" (ANN), "Support vector machine" (SVM), "Gaussian process regression" (GPR), and "Boosted regression tree" (BRT) to overcome the deficiencies of the classical models (Gezici & Tarhan, 2022; Nourani, Gökçekuş, et al., 2020; Parveen et al., 2020).

Bogner et al. (2021) and (Deepa et al., 2021) in their works argued that AI-based methods provide a window for computer scientists, engineering, and social sciences scholars to validate study models so that precise and consistent results can be obtained. Furthermore, Deepa et al. (2021) stressed that "AI-based approaches such as EANN, GPR, ANFIS, BRT, ANN and SVM, has proven to have greater performances in studies that involves investigation of human attitudes, emotions, and interaction with computer-based systems, especially newly developed system due to their suppleness, robustness, and predictions capabilities" (p.16). Thus, in this study, four (4) different AI-based models i.e., ANN, BRT, SVM, and GPR were used to train and test the study collected data so that accurate and reliable results regarding the effects of security parameter on "m-banking" continuous patronage, and robustness of the study proposed AI-based systems can be obtained. Structures of the study AI-based models are presented in the following subsections.

3.9.2 Data Normalization

Data used in AI-based "modelling and simulations" are usually normalized before imputed into the simulation and modelling packages. Data sets were normalized to avoid sets with greater numerical values overwhelming those sets with lesser numerical values by setting the same values range for all the study input variables (Singh & Singh, 2020). There are different machine learning (ML) methods e.g., "Pareto Scaling" (PS) approach which uses "square root of standard deviation as the scaling factor for the dataset, while the new features of all the dataset are to have a variance equal to the standard deviation of the un-normalized features", Mean Centered (MC) method which removes any offset from the dataset by "subtracting the mean of a feature from each instance of that feat", Variable Stability Scaling (VSS) method which extends the PS method by presenting variation coefficient (CV) as the scaling parameter, and the Min–Max Normalization (MMN) method which "scales the un-normalized data to a predefined lower and upper bound linearly" (Ambarwari et al., 2020: p.3) etc. Additionally, data calibration simplified arithmetic calculation in "artificial intelligence (AI) modelling and simulations procedures which in turn increased models' precision, and lessened results processing time" (Ferreira et al., 2019: p.3). Consequently, data collected for this study were regularized using the "Min–Max Normalization" (MMN) method by rescaling the dataset within the range of 0 – to – 1, or 1 – to – 1 using Equation 1.

$$N_{norm} = \frac{N - N_{min}}{N_{max} - N_{min}} \tag{1}$$

Where N represents the number parameters used in the research, while the stabilized values for all the study parameters were denoted as "Nnorm", and the experimental minimum and maximum values regarding the study parameters level of significant effects on m-payment systems usage and continued growth were denoted as Nmin and Nmax in the formular. Volaka et al. (2019) argued that MMN normalization method is more suitable for studies with large dataset, and different scaling factor due to its rescaling ability.

3.9.3 Sensitivity Analysis

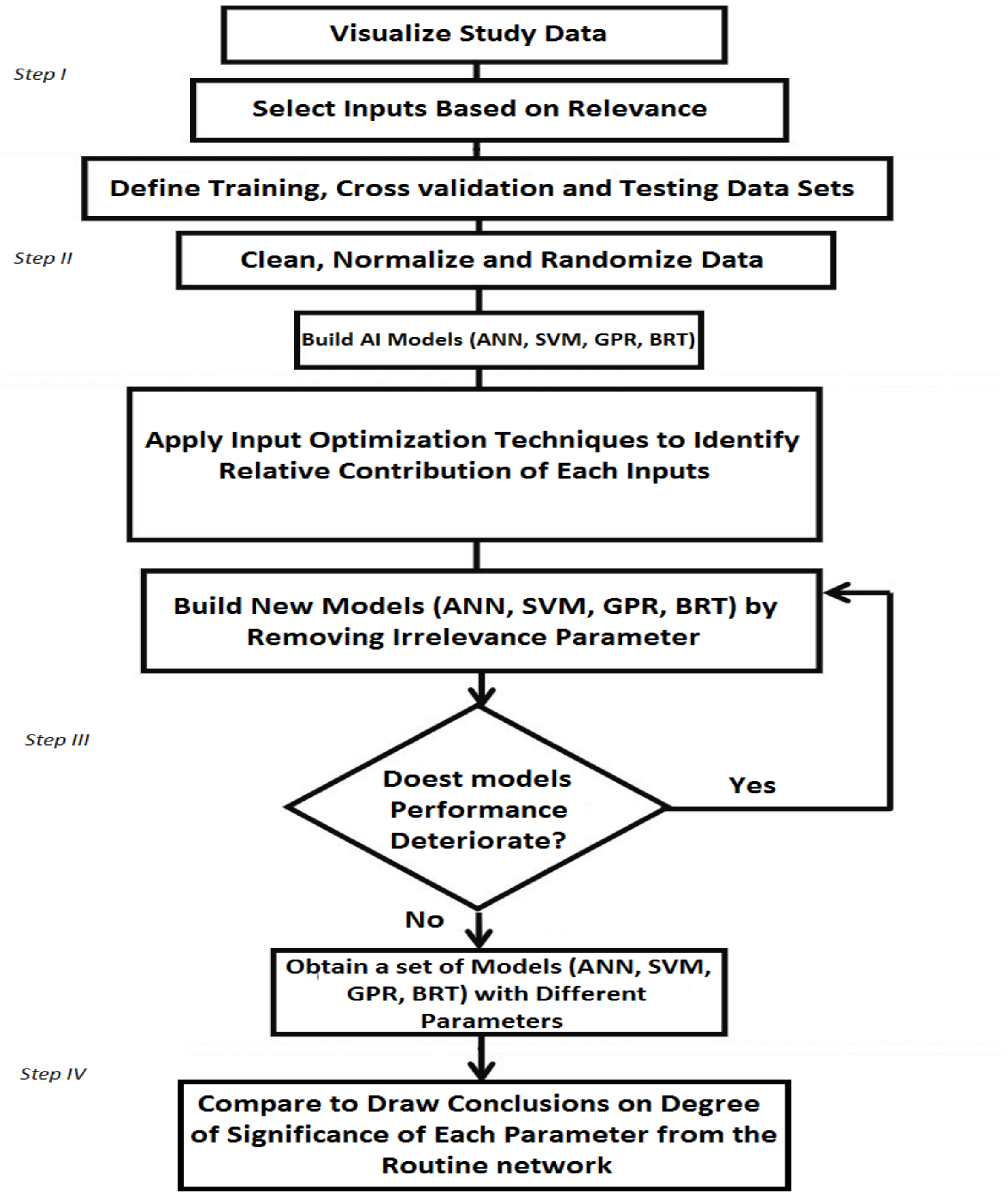
Selection of most relevant input parameters in artificial intelligence (AI) modelling is one of the most crucial steps for attaining reliable and accurate results. For this purpose, the study employed a nonlinear sensitivity examination method in order to determine the ranking and relevancy of each of the study predictors (i.e., security, usability, privacy, interface and information qualities) in predicting "m-banking" continuous patronage and advancement. Also, the method was used to examined the correlation between the study predictors (i.e., input parameters) and innovative financial banking technologies, in this case m-banking in the study locations using coefficient of determination (*DC*). The study sensitivity examination processes were offered in the following subsections.

3.9.4 Removals of Irrelevant Parameters

Removing unimportant parameters from study inputs helps to "reduce the dimension of the input space, and model running time which in turn significantly improves the performance of the AI models" (Pham et al., 2019: p.6). There are many AI sensitivity investigations techniques such as "Monte Carlo (MC) sensitivity analysis, Feed-Forward Neural Network (FFNN) sensitivity analysis, Laban Movement (LM) Analysis" etc., (Gosselin et al., 2016: p.4). Thus, a "Feed-forward neural network (FFNN) sensitivity analysis method was used instead of the usual classic techniques employed by majority of researchers due to its correctness, and robustness in selecting relevant parameters in regression problems" (Ranković et al., 2010: p.11). Coefficient of determination (*DC*) technique was used in assessing and ranking the influence of each of the inputs on "m-banking" continuous patronage and growth in the three study locations i.e., Cyprus, Iraq, and Nigeria. The higher the *DC* values the higher the effects of such parameters on m-banking patronage. In other words, the nearer the *DC* values to 1, the higher the influence and vice versa. The study ANN-based irrelevant parameters removal comprises of four key stages. The study data were visualized and input parameters selection were done based on relevance in the first stage, while training, validation, testing of defined data sets, cleaning, normalization, and models building were done in the second stage. In the third stage, relevance of each parameter was determined using optimization techniques (*DC*), and building of new models with all the parameters, or after removal of irrelevant parameters in case of performance deterioration. Lastly, significance of each of the parameters were compared and conclusions drawn regarding the significance of each parameter was carried out in the fourth stage as shown in Figure 19.

Figure 19.

Flow Diagram of the ANN-based Removal of Irrelevance Parameters (Elangasinghe et al., 2014)


Step I
Visualize Study Data
Select Inputs Based on Relevance
Define Training, Cross validation and Testing Data Sets
Step II
Clean, Normalize and Randomize Data
Build AI Models (ANN, SVM, GPR, BRT)
Apply Input Optimization Techniques to Identify Relative Contribution of Each Inputs
Build New Models (ANN, SVM, GPR, BRT) by Removing Irrelevance Parameter
Step III
Doest models Performance Deteriorate?
Yes
No
Obtain a set of Models (ANN, SVM, GPR, BRT) with Different Parameters
Step IV
Compare to Draw Conclusions on Degree of Significance of Each Parameter from the Routine network

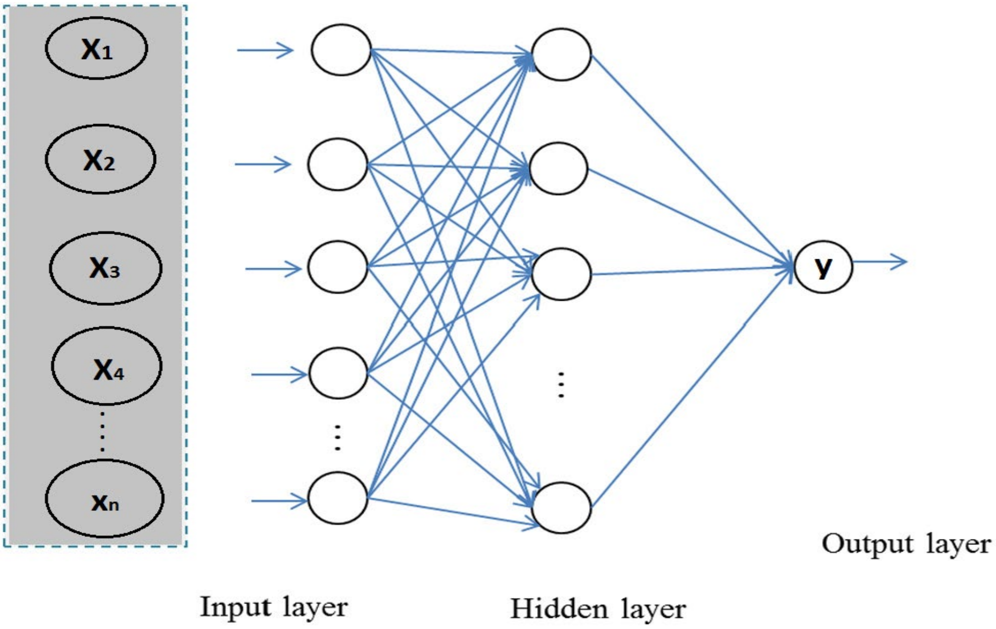
3.10 Artificial Intelligence Models

3.10.1 Artificial Neural Network Model

Nowadays, application of "artificial neural networks (ANN) is undergoing a rebirth that do not only changes artificial intelligence (AI) field, but also offers new ideas regarding neural computing opportunities for scholars in computer related discipline" (Abiodun et al., 2018: p.6) Furthermore, scholars in other fields such as "social sciences now use ANN to validate and measure the performance of studies model" (Aydin & Cavdar, 2015: p.7). These and other contributions signify the effectiveness of ANN in both social and natural science studies. The study ANN model comprises of three (3) layers i.e., "input layer, hidden layer, and output layer" as shown in Figure 20. The study independent variables were represented in the model input layers from x_1 to x_n (i.e., system security, usability, privacy, information and interface qualities), while the model hidden layers which are at the middle neutralized the synopsis weights of the variables inputted into the input layers in order to "abridge the error between desired and computed outputs" (Aydin & Cavdar, 2015: p.8). While the output layer represents the study target which i.e., m-banking patronage and progress represented as y.

Figure 20.

Flow diagram of the study ANN algorithm

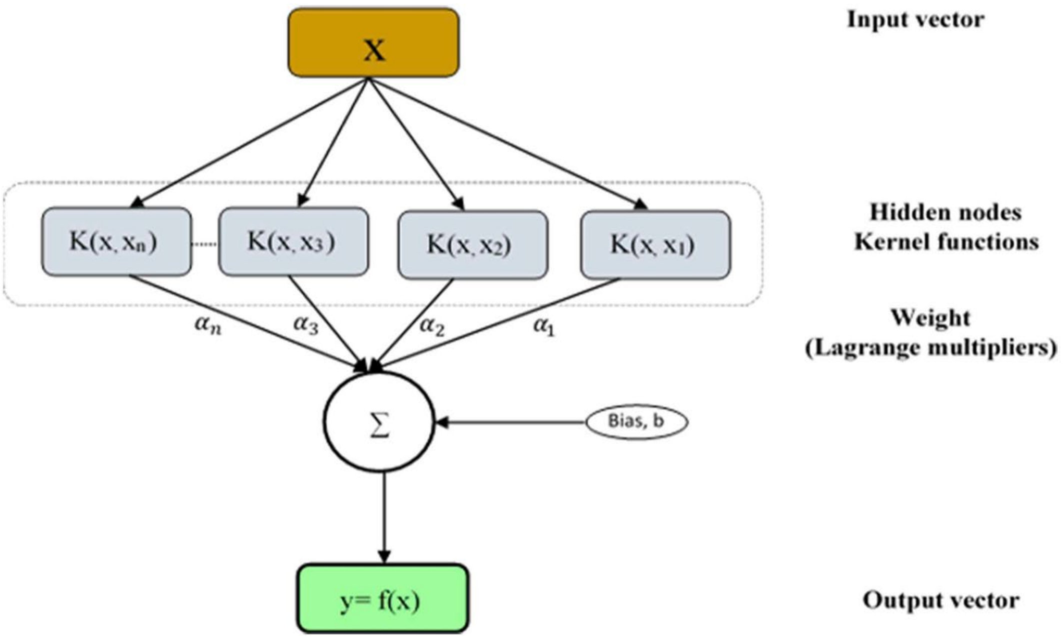


3.10.2 Support Vector Machine Model

Another AI-based technique used by scholars to validate experimental results is "support vector machine" (SVM). The method is one of the finest AI techniques in terms of accuracy in prediction (Cavus et al., 2021b). The study SVM model comprises of four (4) vector nodes. The input vector which confined the study independent parameters, denoted as x, the unseen nodes which contained the seed functions, the weighted Lagrange multipliers node which regulate the "network synopsis weight and determine the percentage of Bias, and the output vector note denoted as y which normalize the correlation coefficient between the study inputs and targeted output" (Demertzis & Iliadis, 2017: p.7). There are different SVM kernel such as; "Linear kernel, Radial basis function (RBF) kernel, Polynomial kernel, Gaussian kernel, Nonlinear kernel, Sigmoid kernel" etc., (Otchere et al., 2021: p. 13). However, for the purposed of this study the Linear kernel was used due to its generality, and robustness in transforming inputs data into a required form, especially in studies with large volume of data set, and uses both linear and nonlinear machine learning (MI) approaches without prior knowledge of the collected data set (Nourani et al., 2020). Diagram of the study SVM model is offered in Figure 21.

Figure 21.

Architecture of the SVM Model (Nourani et al., 2020)

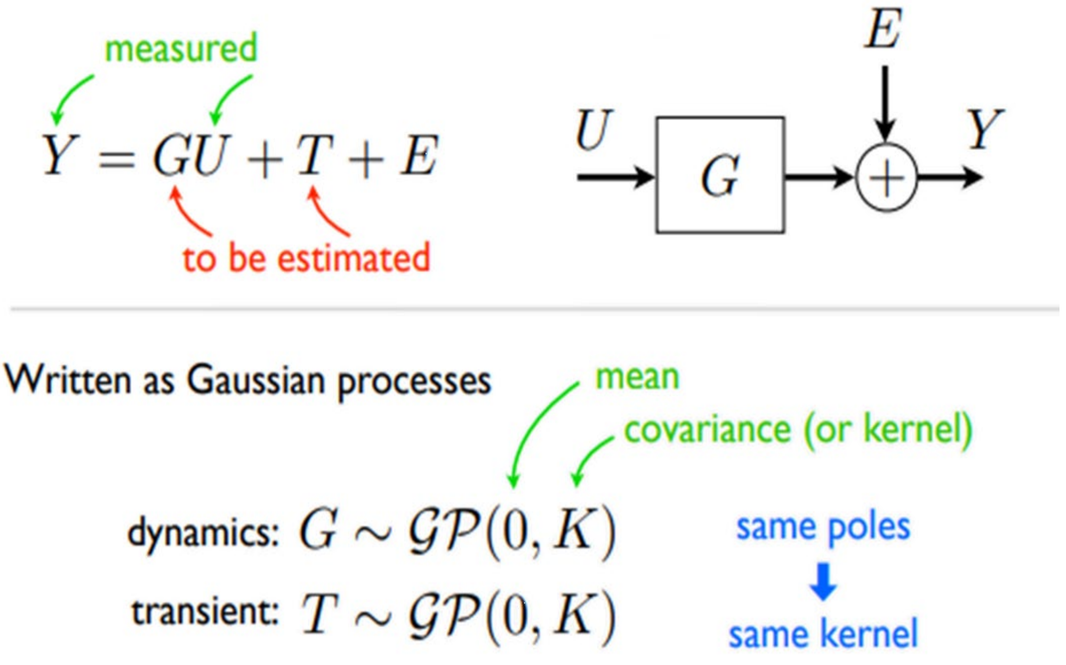


3.10.3 Gaussian Process Regression Model

GPR is another AI-based model used by researchers. For this study, the technique was used to validate the study collated data. The research GPR model has five different notes as shown in in Figure 22, where " u represent the gaussian units (GU), and the y components measured the targeted output values, while k and o represent the kernel (covariance) and mean" respectively (Da et al., 2019: p.6). GPR has the advantage of not requiring accurate data as usually required by other AI models. It enables "improved tracking accuracy compared to other AI models, and degrades gracefully with increased model uncertainty in studies with large data sets" (Yang et al., 2018: p.5). Additionally, the technique has the advantage of handling noise and data uncertainty.

Figure 22.

Structure of GPR Algorithm


measured
$Y = GU + T + E$
to be estimated
E
U
G
Y
Written as Gaussian processes
mean
covariance (or kernel)
dynamics: $G \sim \mathcal{GP}(0, K)$
transient: $T \sim \mathcal{GP}(0, K)$
same poles
same kernel

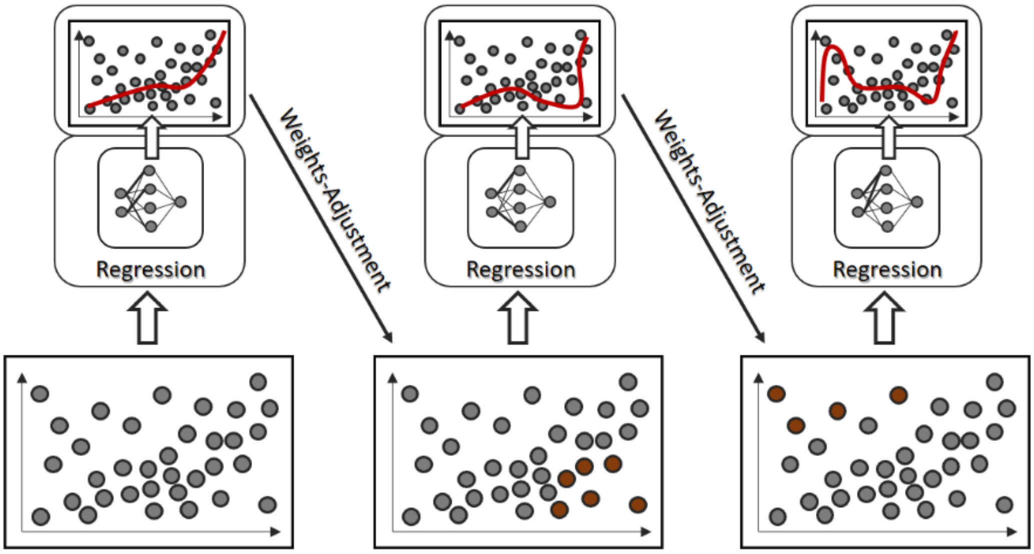
3.10.4 Boosted Regression Tree Model

The BRT method was developed by "computational learning theorist and later re-explained and generalized by machine learning researchers and statisticians" (Delen, 2010: p.4). Researchers from computer related fields think of BRT as an ensemble technique i.e., "a weighted average of predictions of individual classifiers, while mathematicians on the other hand think of BRT as a sequential regression method" (Chen et al., 2011: p.2). The technique enhances model precision, by "searching for different rough prediction rules rather than the single most accurate prediction rule" (Schapire, 2003: p.13). Thus, for this study being an AI based study, the approach is employed to combine prediction results of the different models used so that accurate prediction can be obtained.

Investigation using BRT technique involves adjustment of two vital parameters; i) learning rate which determines the contribution made by each tree toward the development of the final model, and ii) tree complexity which controls the flow of interactions between choosing sets in order to ensure that fitted collaborations are achieved. As shown in Figure 23, edifice of the study BRT model comprises of three hierarchies. The study regularized data were inputted into the model, while the anticipated output was calculated from the independent parameters by adjusting the network weights until fitted outcome (prediction) were obtained.

Figure 23.

Conceptual Diagram of the BRT Model



3.11 Validation of the Study Models

The main purpose of using machine learning (ML) approaches for multifaceted regression issues is to obtain an accurate and reliable outcome which are difficult to attain via empirical methods without profound and prior understanding of the concept. Nonetheless, due to underfitting and overfitting problems encountered in many ML models, training phase performance of ML models are not always in coherent with the performance at the calibration stage (i.e., testing phase), making it difficult to scholars to get correct predictions, especially in studies with unseen data sets. This and other reasons make it compulsory for researchers to validate study models in order to overcome the problems of underestimation and overestimation in ML models. Different types of validation exist which are used to address this problem such as holdout, leave-one-out, and k-fold cross validations" etc. For this study, the k-fold validation was used due to its ability to portion the dataset into an equal subset of k-numbers.

For data proportions to be used in training and calibration phases, some studies use 80% - 20% proportion for training and calibration, while others use 75% - 25% proportion, or 70% - 30% proportion (Abd Jalil et al., 2010). This study employed the 70% - 30% (see, Figure 18) proportioning approach due to its ability to improve models' performance via its data optimization techniques of k-numbers (Ahmad & Aftab, 2017).

3.12 Models Performance Evaluation

Efficacy and performance of the four proposed AI models in forecasting the effects of the study autonomous parameters (i.e., security, usability, privacy, interface and information qualities) on "m-banking" continuous patronage and advancement in the study locations i.e., Cyprus, Iraq, and Nigeria were assessed using five statistical assessment criteria; "Mean absolute percentage error" (MAPE), "Nash-Sutcliffe efficiency" (NSE), "Root mean square error" (RMSE), "Percentage bias" (PBIAS), "Correlation coefficient" (R). The above-mentioned arithmetic performance and efficiency measurements indices were explained using Equations 2 - 6.

$$NSE = 1 - \frac{\sum_{i=1}^{n} \left(N_{obs_i} - N_{pre_i}\right)^2}{\sum_{i=1}^{n} \left(N_{obs_i} - \overline{N_{obs_i}}\right)^2} \tag{2}$$

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n} \left(N_{obs_i} - N_{pre_i}\right)^2}{n}} \tag{3}$$

$$MAE = \frac{\sum_{i=1}^{n} \left| N_{obs_i} - N_{pre_i} \right|}{n} \tag{4}$$

$$PBIAS = \sum_{i=1}^{n} \frac{\left| X_{obs_i} - X_{pre_i} \right|}{X_{pre_i}} \tag{5}$$

$$R = \frac{\sqrt{\frac{\sum_{i=1}^{n} \left(N_{obs_i} - N_{pre_i}\right)^2}{n}}}{\frac{1}{N}\sum_{i=1}^{n} \left(N_{obs_i}\right)} \tag{6}$$

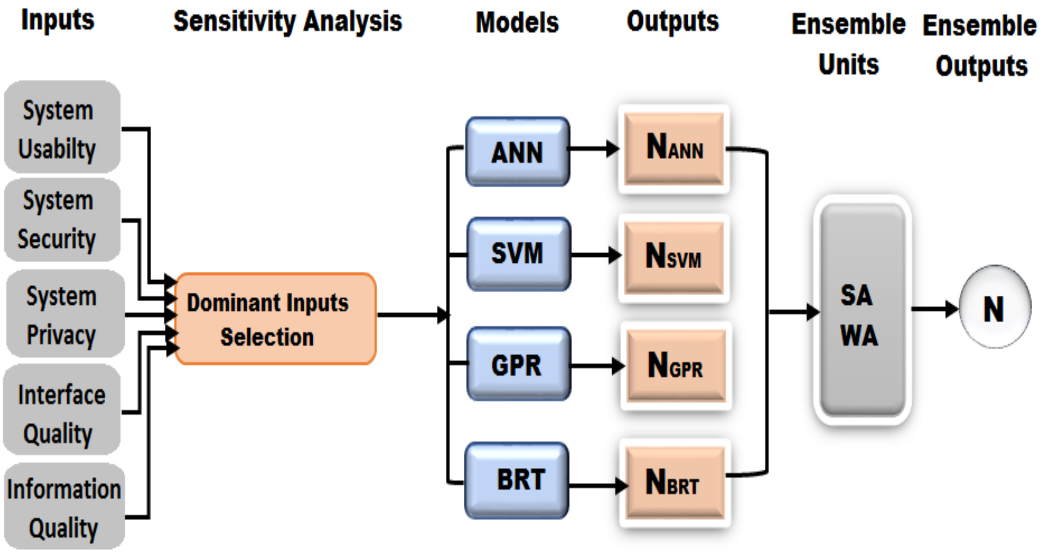
Where, obs represents observed mean effects of the autonomous parameters on "m-banking", and N denotes the observations sum, while N_{pre} represents the projected parameters influence level.

3.13 Ensemble Techniques

Ensemble technique is a "machine learning (ML) approach normally used by scholars to bring together different prediction results obtained from dissimilar models in order to "boost the performance of an experimental model (i.e., reported model) so that accurate and consistent results can be obtained" (Demertzis & Iliadis, 2017: p.8). Also, Abdullah et al. (2018) and Nourani, et al. (2020) in their works stressed that there are two major categories of collaborative approaches; i) linear ensemble approach, which involves the use of linear collaborative such as "simple averaging, weighted averaging, and median weighted averaging" etc, and ii) nonlinear ensemble approach such as SVM, ANN, BRT and GPR, and ANFIS, etc, which are used for nonlinear collaborative (Lu et al., 2020). Nowadays, application of ensemble methods in the different fields of computing research such as digital payment systems, internet banking, e-Learning systems, m-banking, and other modelling and simulation tasks has "proven to be effective, and delivered better prediction results than the use of single models" (Cavus et al., 2021b; Nourani et al., 2020). Thus, this research employed four (4) nonlinear i.e., ANN, SVM, GPR, and BRT, and two (2) linear i.e., simple and weighted averaging ensemble approaches in order to increase the concert of distinct models employed in a particular study. Structure of the study ensemble approach is presented in Figure 24**.**

Figure 24.

Structure of the Developed Ensemble Methods



As seen in Figure 24, the study collaborative method contains six stages namely; i) input unit which contained the study independent parameters of system security, usability, privacy, interface and information qualities, ii) sensitivity analysis phase which aim at finding the significant or effects of each of the study input parameters on m-payment systems, iii) models phase which contained four different AI-based models used in the study, iv) outputs unit which determine the output produced by each of the four AI-based developed models, v) ensemble unit which contained the two "linear ensemble techniques" employed in the study i.e., "simple averaging, and weighted averaging", and vi) the ensemble output phase that determines the results produced by the two ensemble techniques.

3.13.1 Linear Ensemble

The two employed linear ensembles used in this study are the simple averaging (SA), and weighted averaging (WA) collaboratives. In the SA, average of all the outputs (i.e., parameters effects) produced by study developed models of ANN, GPR, SVM and BRT were taken as the forecasted effects values using Equations 7.

$$\bar{N} = \sum_{i-1}^{nm} w_i \, N_i \tag{7}$$

The w_i represents the weights applied on the output of the i^{th} model, which can be ascertained on the basis of performance produced by the models using Equations 8.

$$w_i = \frac{DC_i}{\sum_{i=1}^{nm} DC_i} \tag{8}$$

Where, DC_i represent the optimum performance of the i^{th} sole model.

3.13.2 Nonlinear Ensemble

The "Feed-Forward Neural network" (FFNN), was employed in the study nonlinear ensemble approach. The FFNN was first trained to execute the averaging effects of each parameter on m-banking in a non-linearized manner. While, outputs of each of the study developed models are considered as one parameter each, and inputted into the first layer (i.e., input layer) of the ensemble model as inputs. Lastly, the FFNN was trained with outputs of the study sole models as inputs, for prediction which can be reported in a hybrid manner.

CHAPTER IV

RESULTS AND FINDINGS

In this chapter, findings regarding the effects of security and confidentiality on "m-banking" continuous patronage and advancement, vulnerability of m-banking authentication methods, and study proposed system usability testing results in the study areas (i.e., Nigerian, Cyprus, and Iraq) were presented. Also, sensitivity examination, sole models, and hybrid model results were offered in the following sections.

4.1 M-banking Security Issues in the Study Areas

The security dataset of the study consists of 978 samples comprising of four major dimensions; Authentication methods, Distributed denial of service (DDoS), Risk, and Velocity anomalies issues. The normalized security dataset was separately processed using ANN model due to its weights' adjustment capabilities. The data were fed into the network input layer, while the hidden layer continued to adjust the synopsis weights until best performance was achieved. In training the separate ANN models, MSE and TANSIG were used as performance and transfer functions, while Feed-forward backward propagation and TRAINLM were used as network category and training functions respectively.

For safety and secrecy issues in the study locations i.e., Cyprus, Iraq, and Nigeria. The study found customers fear of third-party intrusion (e.g., device intrusion, network vulnerability, intrusion, malicious insider attacks, and financial malware attacks) through other applications that are stuffed in mobile devices, and absence of classy security apparatus to be the key protection and privacy issues upsetting the expansion of m-banking, especially in Nigeria. It was discovered that customers' concern for security negatively affects m-banking continued patronage among those already using the services, and harmfully influenced non-adopters' intent to accept and use the services in both evolving and advanced countries. Furthermore, the study exposed other aspects of m-banking security such as economic risk, privacy risk, functional risk, and time risk which merit distinct investigation as opposed to the general examination of risk concept by prior research. This clearly shows that individual's perception of what constitutes m-banking security and secrecy varies.

Other security issues affecting “m-banking” continuous patronage and advancement in the study locations are; failures of payment institutions to prevent their network or server from different forms of threats, and attacks e.g., distributed denial of service (DDoS) or intrusion by unauthorized persons even in applications where security is paramount such as password manager, m-banking, and mobile-Health applications. Also, majority of the verification techniques employed by banks were discovered to be week in terms of velocities anomalies detection, as the study findings found user confirmation process and velocity anomalies issues to be the main reasons why successful cyber-attacks were carried out on m-payments platforms such as m-banking. Table 9 displays the performance of the separate ANN security model, while Figure 25 depicts the distributions of security concern for each of the dimensions.

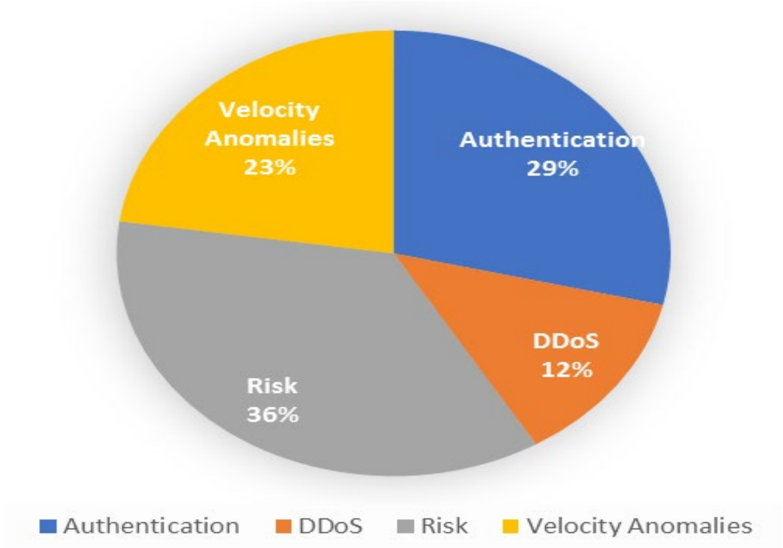
Table 9.

Results of the Study Separate ANN Security Models

Security Parameters	Model	Target	Proportioning	Training	Testing	Prediction
M-banking Risk	1	1.0	70% - 30%	0.9981	1.0000	0.9820
Authentication Methods	2	1.0	70% - 30%	0.9826	0.9893	0.9764
Velocity Anomalies	3	1.0	70% - 30%	0.9247	0.9311	0.9633
DDoS	4	1.0	70% - 30%	0.9011	0.9132	0.9479

Figure 25.

Distributions of Security Parameters



4.2 Vulnerability of Present Authentication Methods

For authentication methods, the study results found traditional password to be the most widely used means of verification method employed by banks and other payment institutions despites its safety and memorability challenges, as users find it difficult to memorized strong passwords. Also, it was discovered that even the multi-factor authentication (MFA) methods which are considered to be more secure than the usual single and double factors authentication approaches are not as highly as anticipated in terms of complexity, laws compliance, and robustness against well-established attacks. Furthermore, the study's findings exposed the security defects of the five most foremost two-factor authentication methods in multi-server surroundings, as it highlights some of the new security challenges affecting both two-factor and MFA schemes such as; session-specific and malicious insiders attacks. Thus, nullify future use of these schemes without further enhancement. In terms of preference regarding authentication approaches employed by banks, findings of the study discovered that password and fingerprint verification methods were the most preferred authentication methods for majority of m-banking users due to its ease of usage, but not in terms of security viability.

Another result that emerges from the study is inadequate analysis of users' cognitive capacity and other details. The study found insufficient analysis of user reliability, intellectual capacity, actions, other m-banking essentials, and lack of user involvement in the design process of different verification methods to have negative effects on present verification techniques used by banks and other payments institutions which in turn negatively affects the patronage and progress of all innovative banking and financial technologies such as m-banking. Though, authentication using "Near Field Communication" (NFC) is more secured than single, double, and MFA authentication methods. However, the study found NFC method to be complex and difficult as attackers can take advantage of the card susceptibilities to intercept payment dealings during the authentication process between user device, NFC-enabled and brokers. Thus, resulting in financial losses not only on the side of the customers, but also on payment institutions.

4.3 Usability Testing Results

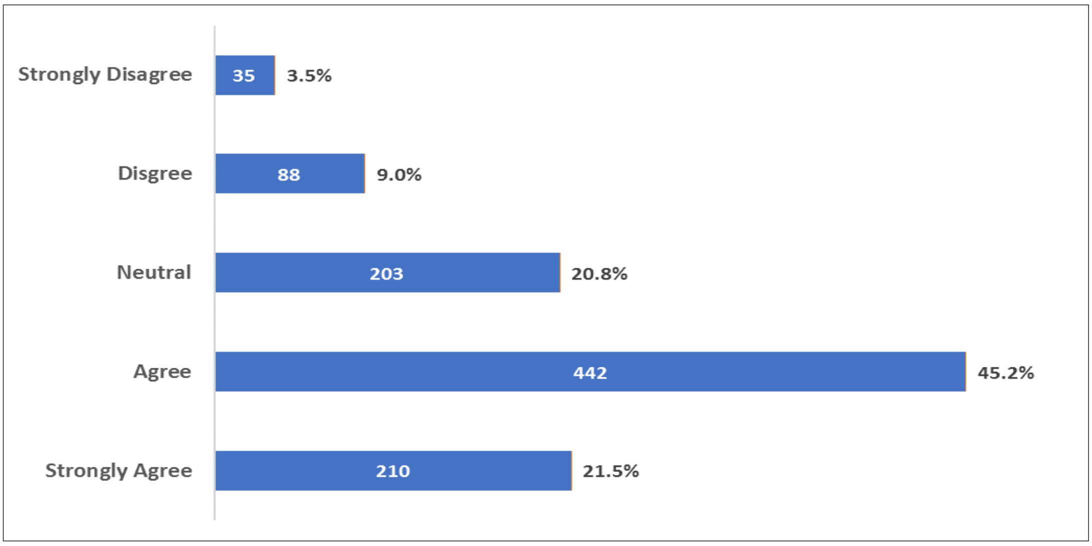
The study developed an AI-based anomalies detection and authentication system for improved m-banking security, and tested using a usability testing approach. Results concerning the robustness of the study proposed system in terms of security, usability, privacy, interface and information qualities using 5 points Likert Scale (see Appendix - C) are offered in the following subsections.

4.3.1 System Security

Results regarding the security features of the proposed system clearly shows that participants who used the system expressed satisfaction with the system, signifying the system ability to detect and handle velocity anomalies during login, and prevent different forms of attack such as DDoS attack. With regards to security components of the proposed AI-based anomalies detection and verification system, 45.2% and 21.5% of those who tested the system believed that the proposed system is capable of handling DDoS attacks against banks' networks, and can detect and handle velocity anomalies which present verification methods failed to achieve. Thus, the system can assist in reducing some of the m-banking security challenges. Figure 26 depicts distributions of participant feeling about the security features of the system.

Figure 26.

Participants Security Feelings

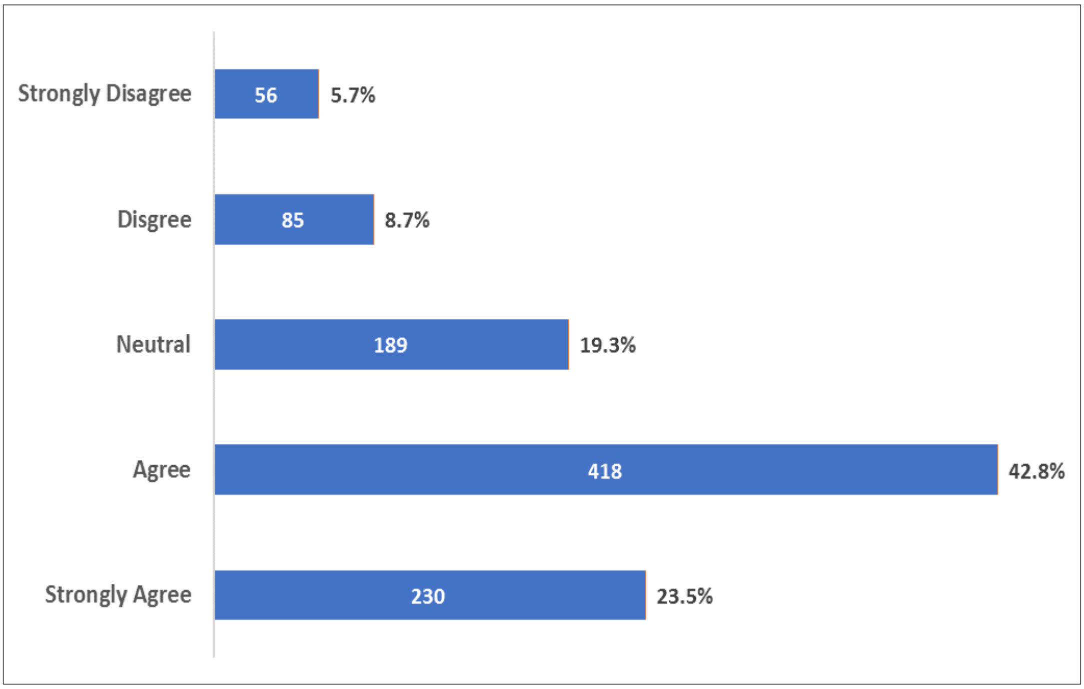


4.3.2 System Usability

Result regarding the simplicity (i.e., ease of use) of the study proposed AI-based system shows that majority of the participants expressed satisfaction on how simple and easy it was to use the proposed system as the participants were able to complete intended tasks and scenarios so quickly via the system compared to other systems deployed by payment institutions. This clearly shows that the participants found the proposed system suitable in terms of ease of use. Also, the results indicate that authentication methods presently used by banks may be are not as easy as people may think. Based on the usability testing result, 42.8% and 23.5% of the study sample agreed and strongly agreed respectively that it is much easier to operate the study proposed AI-based authentication system compared to other verification systems used by banks, as only 8.7% and 5.7% of the participants who tested the system disapproved or strongly disapproved usability features of the proposed system, while 19% remain neutral i.e., they neither disapproved nor approved the proposed system ease of usage. Participants' feelings regarding the proposed system ease of usage is presented in Figure 27.

Figure 27.

System Usability

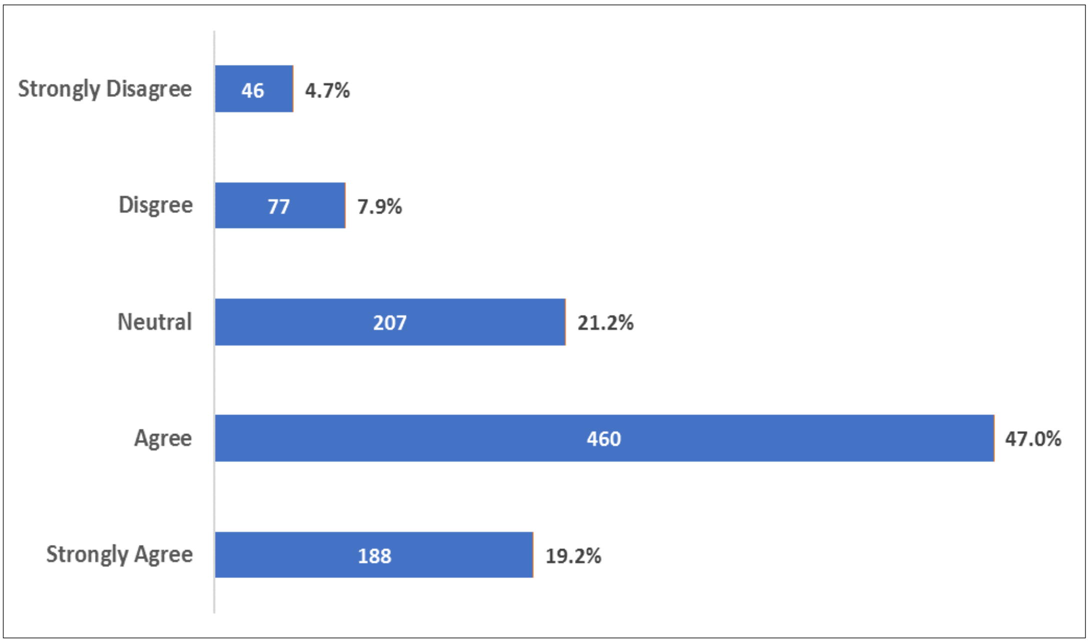


4.3.3 System Privacy

Regarding how the study proposed AI based system handle users' privacy such as login and other sensitive information stored on the app. The result indicates that more than 66% of the participants that participated in the usability testing process expressed optimism that the proposed system has the required features to protect customers funds convey via bank externalized networks which are increasingly becoming more vulnerable than before due to increase in the number of cyber-crimes, and accessing of other sensitive information stored on m-banking apps. The result clearly indicates that privacy is one most influential drivers of m-banking, and that externalization of bank networks via m-banking platforms makes the networks susceptible to attacks by unauthorized persons. Participants' opinion regarding the proposed system's ability to handle secrecy issues is presented in Figure 28.

Figure 28.

System Privacy

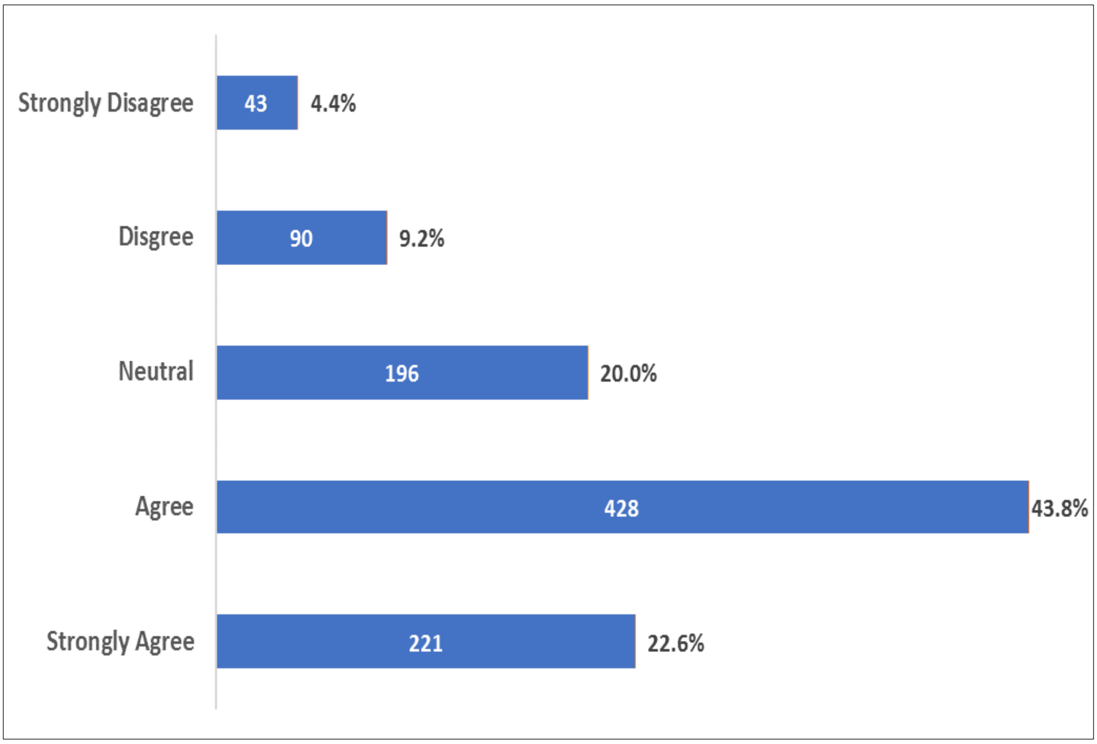


4.3.4 Interface Quality

Participants opinion regarding the quality of interfaces provided in the study proposed system were also assessed and determined, and the result clearly shows that the quality of interface supplied in the proposed system are of high quality and capable of meeting user needs in terms of functionality, flexibility, and protection as only 4.4% and 9.2% of those who used the system expressed doubt about the excellent level of the system interface which are insignificant compared to the 43.8% and 22.6% who are satisfied with the quality of the interfaces integrated in the proposed system. The result signifies the importance of interface quality in computer-based systems like that of m-banking systems. Figure 29 displays the usability testing outcome for the proposed system in terms of interface quality.

Figure 29.

Interface Quality

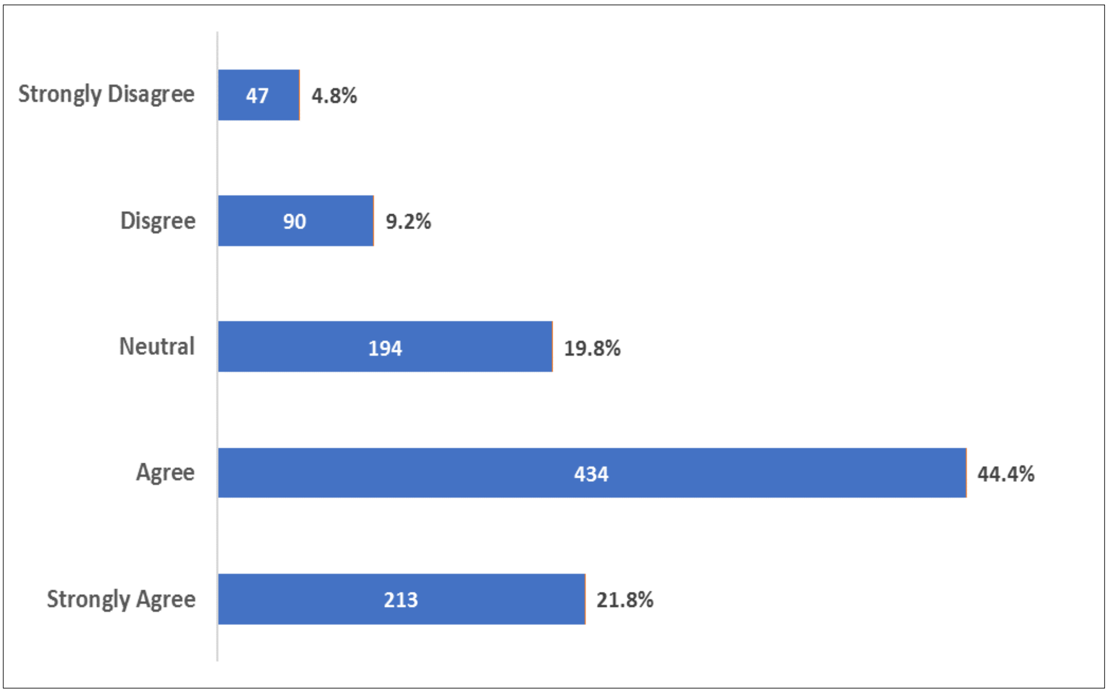


4.3.5 Information Quality

The quality of information provided in any computer-based system determined its efficacy. Organization and quality of information provided in a system allows the system to display clear error messages which enable users to fix any problem that the user may encounter, and recover quickly and easily whenever they make mistakes while using the system. Thus, it is an integral component of any system development. For the quality of information provided in the proposed system, it was discovered that the information supplied in the proposed system allows users to recover quickly and easily from mistakes made, which allows them to fix all problems encountered while using the system as a large number of the participants that partake in the testing process express satisfaction with the quality and arrangement of information in the proposed study. This is because more than 66% of the participants believe that the information provided in the proposed system is adequate, well arranged, and will guide the user on how to use the system, and resolve majority of problems that may be encountered. Figure 30 depicts participants' sentiments regarding the quality of information provided in the proposed system.

Figure 30.

Information Quality



4.4 Sensitivity Analysis Results

Literature have shown that the efficacy of any AI-based model relies on the number of input parameters (i.e., independent variables) used (Akhavian & Behzadan, 2015; Vom Lehn et al., 2020). Selection of key inputs is the most important step in the development of any AI model, and process of communicating study findings. For instance, essential insights on model structure, behaviour, and reactions to input changes were all gained via sensitivity analysis (Borgonovo & Plischke, 2016). Also, it has been argued that use of so many input parameters will increase the intricacy of the model which in turn lead to overfitting. While, the use of little inputs can affect the model forecasting ability. The implication of model overfit is that the model will look pretty good at the first instance with too many parameters (i.e., good fit with the sample data) but have a poor fit whenever new dataset are fed. As shown in Table 10, parameters used in the study are neither too little nor are they so many in order to avoid having overfitted model or model with deflated prediction capability so that consistent and precise results can be achieved regarding security effects on "m-banking" continuous patronage and advancement in the three study locations.

For effects classification of each of the input parameters, a "Feed-forward neural network" (FFNN) sensitivity investigation methods was used to determine the relative contribution as well as the effects (i.e., correlation) of each of the choosing variables on "m-banking" continuous patronage and advancement (target) instead of the usual conventional correlation approaches previously used in choosing key determinants of m-banking such as "Pearson's product moment correlation, Kendal, and spearman's rank correlations coefficients" etc. Some scholars criticized the use of these and other classical correlation approaches in selecting key inputs in m-banking determinants prediction e.g., see (Cavus et al., 2021a). Furthermore, AI-based models such as EANN, ANN, CNN, SVR, and GPR have the capability to handle data uncertainty e.g., see (Ning & You, 2019). Thus, it offered reliable and accurate outcomes than conventional methods. For this study, coefficient of determination (*DC*) technique was employed to assess and rank the effects of each of the choosing inputs on m-banking continuous patronage and growth in the study locations i.e., Cyprus, Iraq, and Nigeria. The higher the *DC* values of an input parameter, the higher the effects of such a parameter on dependent variables, in this case m-banking systems. In other words, the closer the parameter values to 1, the higher the influence of such parameter on the study dependent variables. The study input parameters were assessed and ranked using Equation 9.

$$DC = 1 - \frac{\sum_{i=1}^{n}(N_{obsi} - Nprei)2}{\sum_{i=1}^{n}(N_{obsi} - N_{obsi})2} \qquad (9).$$

Where N_s represents the m-banking observed mean values, n represents the total number of observations, while N_{obsi} stands for m-banking determinants effects observed, and N_{prei} is the forecasted effects of the study inputs on m-banking. Parameters *DC* values, and ranking results are presented in Table 10.

Table 10.

Study Sensitivity Analysis Results

Input Parameters (X_1 - X_n)	*DC* (Average)	Rank
X_1 = System security (SysSeq)	0.9821	1
X_2 = System privacy (SysPriv)	0.9610	2
X_3 = System ease of use (Syseus)	0.9360	3
X_4 = Interface quality (IntQual)	0.9236	4
X_5 = Information quality (InfoQua)	0.8917	5

As seen in the sensitivity examination results (Table 10), the *DC* values for all the parameters are > 0.9, except for information quality which has a *DC* value of < 0.9 which is also considered as good results (Borgonovo & Plischke, 2016). Thus, it can be said that all the study inputs are relevant in modelling security effects on m-banking patronage and progress.

4.5 Single Models Results

Having assessed and selected the most foremost input parameters (i.e., X_1, X_2, X_3, X_4, X_5) affecting m-banking and other innovative banking and financial technologies continued patronage and progress four non-linear artificial intelligence (AI) based models (ANN, BRT, SVM, GPR) were developed in order to forecast the influence of security on “m-banking” continuous patronage and advancement in Nigerian, Iraq, and Cyprus.

Feed-forward neural network (FFNN) approach was employed with one input, hidden, and output layers respectively. Levenberg-Marquard algorithm was used to trained the FFNN model with five input factors for prediction of security influence on m-banking in the research areas. To choose the best structure for the FFNN model, which is very vital for getting better results in any FFNN modeling, a repetitive method was used by assessing the performance of different models which are modelled using different number of neurons. Different FFNN models were created and trained with three different structures; 5-6-1, 5-8-1, and 5-10-1, structures using Levenberg Marquardt algorithm and tan-sigmoid activation function.

Model with 10 numbers of hidden neurons 5-10-1 (i.e., 10 hidden neurons) produced the best result compared to 5-6-1 and 5-8-1 structures respectively. ANN model is widely recognised as one the best approach for modelling non-linear associations with regards to human emotions toward computer-based systems like that of m-banking. TANSIG and Feed-forward backward prop were used as transfer function and network type, while tan-sigmoid and the Levenberg- Marquardt algorithm was used as activation and training functions respectively. The best performance was achieved at epoch 11. The second non-linear model used in this research was SVM model which is generally regarded as one of the most robust among AI techniques in terms of accuracy, and handling of hidden dataset. The models were also used to determine the influence of the study inputs on the reliant variable (i.e., m-banking). While the third and fourth non-linear models used are BRT and GPR which are also considered to be among the best AI approaches for solving regression problems that involve large volume of dataset with different dimensions.

For the BRT, GPR, and SVM models, optimum models were achieved using squared exponential kernel, least square boost algorithm, and RBF kernel respectively which are the most widely employed kernels for regression models (Zhang et al., 2019).

Performance of the four developed non-linear AI models (ANN, BRT, SVM, and GPR) in forecasting the influence of security on “m-banking” advancement in Nigeria, Iraq, and Cyprus was measured and evaluated using five arithmetic indices of; i) “Root mean square error” (RMSE), ii) “Nash-Sutcliffe efficiency” (NSE), iii) “Mean absolute error” (MAE), iv) “Percentage bias” (PBIAS), and “Correlation coefficient” (R) respectively. Performance of the non-linear models are presented in Table 11.

Table 11.

Single Modelling Results

Models	Training					Testing				
	RMSE	NSE	MAE	PBIAS	R	RMSE	NSE	MAE	PBIAS	R
ANN	0.0011	0.9951	0.0006	0.0010	0.9823	0.0013	0.9962	0.0008	0.0012	0.9880
SVM	0.0000	0.9999	0.0000	0.0000	1.0000	0.0000	1.0000	0.0000	0.0000	1.0000
GPR	0.0007	0.9999	0.0000	0.0009	1.0000	0.0008	0.9999	0.0000	0.0013	0.9998
BRT	0.0033	0.9773	0.0009	0.0501	0.9961	0.0059	0.9826	0.0009	0.0651	0.9970

4.6 Ensemble Model Result

In the final stage of the modelling process, two linear ensembles approach i.e., simple averaging (SA), and weighted averaging were developed in order to improve the efficacy of the four non-linear models. Outputs of each of the four different non-linear models (ANN, GPR, SVM, and BRT) were entered into the ensemble first layers (input layers) as input variables. The two employed linear collaborative approach (i.e., WA and SA). Table 12 displays the results of the two linear collaborative methods.

Table 12.

Ensemble Methods Results

Ensemble	Calibration		Verification	
	DC	RMSE	DC	RMSE
SA	0.8936	0.1208	0.8103	0.1724
WA	0.8642	0.1187	0.8395	0.1325

CHAPTER V

DISCUSSION

In this chapter, the study results presented in previous section (chapter four) were debated, and compared with the findings of prior m-payment, machine learning, m-banking, and other relevant related studies.

5.1 Sensitivity Analysis Results

Selection of relevant input parameters is the most important task in any AI modelling process. For instance, essential insights on model structure, performance, and reactions to input changes were all gained via sensitivity analysis (Borgonovo & Plischke, 2016). Furthermore, Tunkiel et al. (2020) and Linardatos et al. (2020) in their studies argued that use of so many input parameters will increase the intricacy of the model which in turn leads to overfitting the model. While, use of little parameters can affect the model forecasting ability. The implication of model overfit is that the model will look pretty good at the first instance with too many parameters (i.e., good fit with the sample data) but have a poor fit whenever new data set are fed into the model. As shown in Figure 24, parameters used in this study are neither too little nor are they so many in order to avoid having overfitted model, or model with deflated prediction capability so that precise and consistent results can be attained regarding the impacts of protection on "m-banking" continuous patronage and advancement in the study locations, and in assessing the robustness of the proposed AI-based anomalies detection and authentication system.

For determining the importance, and contribution of each of the input parameters, a "Feed-forward neural network" (FFNN) relevancy investigation methods was used as an alternative to the usual classic procedures used by majority of researchers due to its' correctness and robustness in selecting relevant parameters. Use of classical measurement approach (e.g., Pearson correlation) has been faulted by quite a number of computing and engineering studies (e.g., Bermudez-Edo et al., 2018; Cavus et al., 2021a; Umar et al., 2021). The authors argued that used of "conventional linear measurement techniques such as Pearson correlation are time consuming, bias-based in nature, and produce inaccurate results in most cases". Thus, the need for artificial intelligence (AI) based approach such as “sensitivity analysis” in order to choose the most relevant parameters.

As seen in Table 10, the nearer the DC values to 1, the higher the effects such parameter may have on the study dependent variable and vice versa. Based on the study sensitivity evaluation results (Table 10), it can be seen that security (X_1) is ranked first with *DC* values of 0.9821, and followed by privacy (X_2) with *DC* values of 0.9610 respectively. The two results clearly shows that protection (X_1) and secrecy (X_2) issues are the two most relevant parameters among the study inputs. Furthermore, the results signify the importance of customer protection in m-banking, and other internet related banking platforms, as people concern for safety of their funds and other valuable information negatively influence their intent to use or continued patronage of the service platforms. The result is supported by the findings Jebarajakirthy and Shankar (2021) who stressed that in the near future, “security may likely become the key moderator of m-payment systems, especially m-banking service due to its complexity” (Jebarajakirthy & Shankar 2021: p.3), and if not carefully handle by the payment institutions it may affects the future prospects of not only m-banking platforms, but also other e-Payments services globally.

The sensitivity analysis results, also shows that system ease of use (X_3), and interface quality (X_4)with *DC* values of 0.9360 and 0.9236 were ranked third and fourth respectively, signifying the importance of interface excellence and ease of usage in computer-based applications such as m-payment systems, in this case m-banking applications. The result is reinforced by the findings of Mohammed and Karagozlu (2021) who argued that “information systems designers should tailor their efforts toward designing a user-friendly systems’ which are free from anxiety and tense, so that users can use it without requiring any form of special training” (Mohammed & Karagozla 2021: pp. 243) before usage. While, information quality (X_5) is ranked fifth with *DC* value of 0.8917.

Though, the *DC* values of the study input parameters (i.e., X_1, X_2, X_3, X_4, X_5) varies. However, all the parameters were used in the confirmation and calibration steps of the study proposed AI-based models (GPR, ANN, SVM, and BRT) as the parameters *DC* values were all > 0.9 except for information quality which has a *DC* value of < 0.9 which is also considered as good result (Zainab et al., 2021). Having, choosing the foremost parameters among the study inputs (i.e., security, privacy, ease of use, interface, and information qualities). The study proposed models were developed, trained, and tested for predictions of security impacts on “m-banking” continuous patronage, and advancement in Nigerian, Iraq, and Cyprus. Performance of the four different AI models is presented in the following section.

5.2 Single Model Results

Based on the study single modelling results (Table 11), it can be seen that predictions’ ability of the study proposed models were interpreted based on five arithmetic measurement metrics; NSE, RMSE, MAE, R, PBIAS. Usually, models’ accuracy is measured based on NSE values. An NSE value is considered unsatisfactory if it stood at (< 0.50), satisfactory (> 0.50), good (> 0.65), very good (> 0.75), and excellent (> 0.90) (Gupta et al., 2009). While the RMSE metric was used to measure the average mistake produced by each of the modes. The lower the RMSE values the better the performance of a model vice versa (Wang et al., 2016). Another measurement metric used in the study is Mean absolute error (MAE). The MAE metric was used to measure error between predicted values of security influence and observed values of security effects on m-banking. Just like the RMSE, the MAE was employed in this study to measure the goodness-of-fit level by assessing the deviations between the observed security influence and forecasted security influence levels in the same way irrespective of signs. Also, the PBIAS metric was used to evaluate the percentage of preconception produced by each of the models in estimating the impacts of protection (security) on “m-banking platforms” in the study areas. The closer the PBIAS and MAE values to 0, the healthier the model’s forecasting precision. Lastly, correlation coefficient (R) was used to measure the level of association between security and m-banking continued patronage and progress. The nearer the R values to the target (1), the stronger the relationship between the parameters and vice versa. In other words, higher R values indicate a strong correlation between the dependent and input parameters (Ratner, 2009).

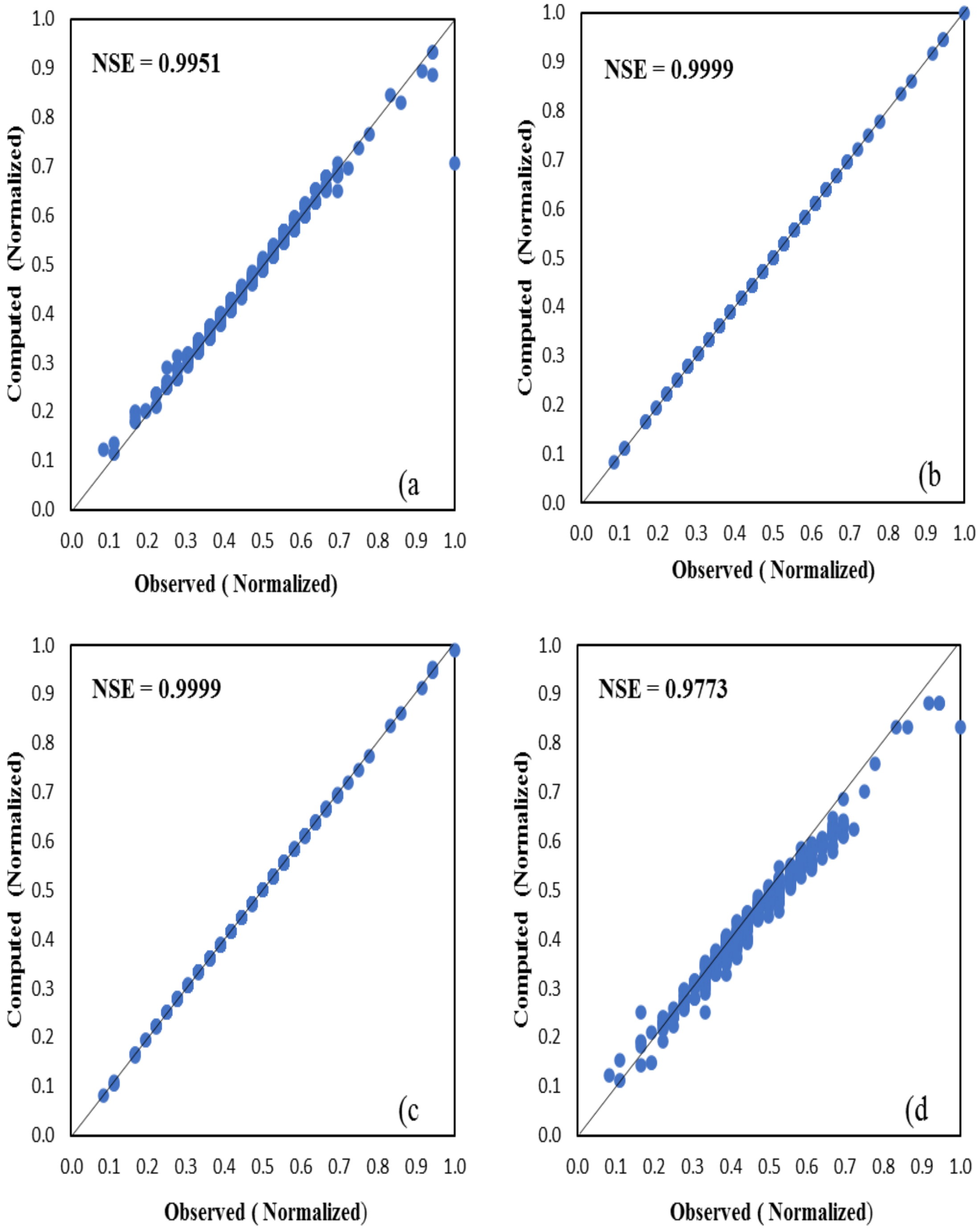
Based on the study single modelling results (Table 11), it can be said that the SVM model has the topmost testing and training values compared to other models. The model has RMSE and MAE values of 0.0000 in both verification and calibration steps respectively, signifying the model’s precision level in terms of error compared to other AI-based models. The results justify the argument of Latchoumi et al. (2019) that “SVM in most cases outperformed other AI-based models not only in prediction, but also in training and testing of study dataset" (Latchoumi et al., 2019: p.6). Furthermore, the model NSE figures of 0.9999, and 1.0000 in verification and calibration stages further justify the model prediction ability as both values are very close to 1(i.e., targeted output). While the model R values of 1.0000 in both verification and calibration indicates a strong correlation between the study variables (i.e., security, ease of use, privacy, information and interface qualities, and dependent variable of m-banking). Furthermore, optimum percentage of bias (PBIAS) values required in any scientific research was attained in the SVM model as the figures stood at 0.0000 in both testing and training.

Another model that performs pretty well in training and testing is the GPR model. For instance, in terms of error, the finest percentage rate was attained in the GPR Model. This is because the model has an RMSE values of 0.0007 in training, and 0.0008 in testing, and MAE values of 0.0000 in both verification and calibration. While in terms of bias, the GPR PBIAS values stood at 0.0009 and 0.0013 in testing and training signifying the accuracy level of the model (Latchoumi et al., 2019). For correlation amongst the parameters (i.e., dependent and independent variables), and prediction skill, the GPR replica has an NSE figures of 0.9999 in both verification and calibration stages which are very near to 1 (i.e., the targeted output). Similarly, the replica R figures of 1.0000 and 0.9998 in verification and calibration stages clearly indicate a strong correlation between security and "m-banking" continuous patronage, and advancement in the three locations that made up the study sample.

For the study ANN model as seen in Table 11, it can be said that the model also performed well in the calibration and verification process, as the model has RMSE figures of (0.0011 and 0.0013), NSE (0.9951 and 0.9962), MAE (0.0006 and 0.0008), PBIAS (0.0010 and 0.0012), and R values of (0.9823 and 0.9880) in calibration and verification stages. Signifying the model precision in estimating the impacts of security on "m-banking" advancement and continuous usage in the study areas. ANN is another machine learning model with higher forecasting ability due to its forward-back-propagated function which adjusts the synopsis weights from the superior layers to the subordinate layers (Dao et al., 2020; Yang & Kim, 2004). Finanly, based on the single modelling results (Table 11), it can be seen that the BRT model has the highest percentage of bias (i.e., PBIAS), and errors rate (i.e., MAE and RMSE) in the sole modelling process compare to other three models, as the model PBIAS figures stood at (0.0501 and 0.0651), MAE (0.0009), and RMSE (0.0033 and 0.0059) in both testing and training steps. Based on the results in Table 11, and the interpretations of the study employed performance measurement metrics given above, results of all the four proposed AI models can be accepted as all the models achieved the optimum performance level required in any machine learning techniques (Otchere et al., 2021). Thus, included in the study scatter plots, and predictions computational activities. Scatter plots of the four study proposed AI models in testing and training phases are offered in Figure 31, and Figure 32.

Figure 31.

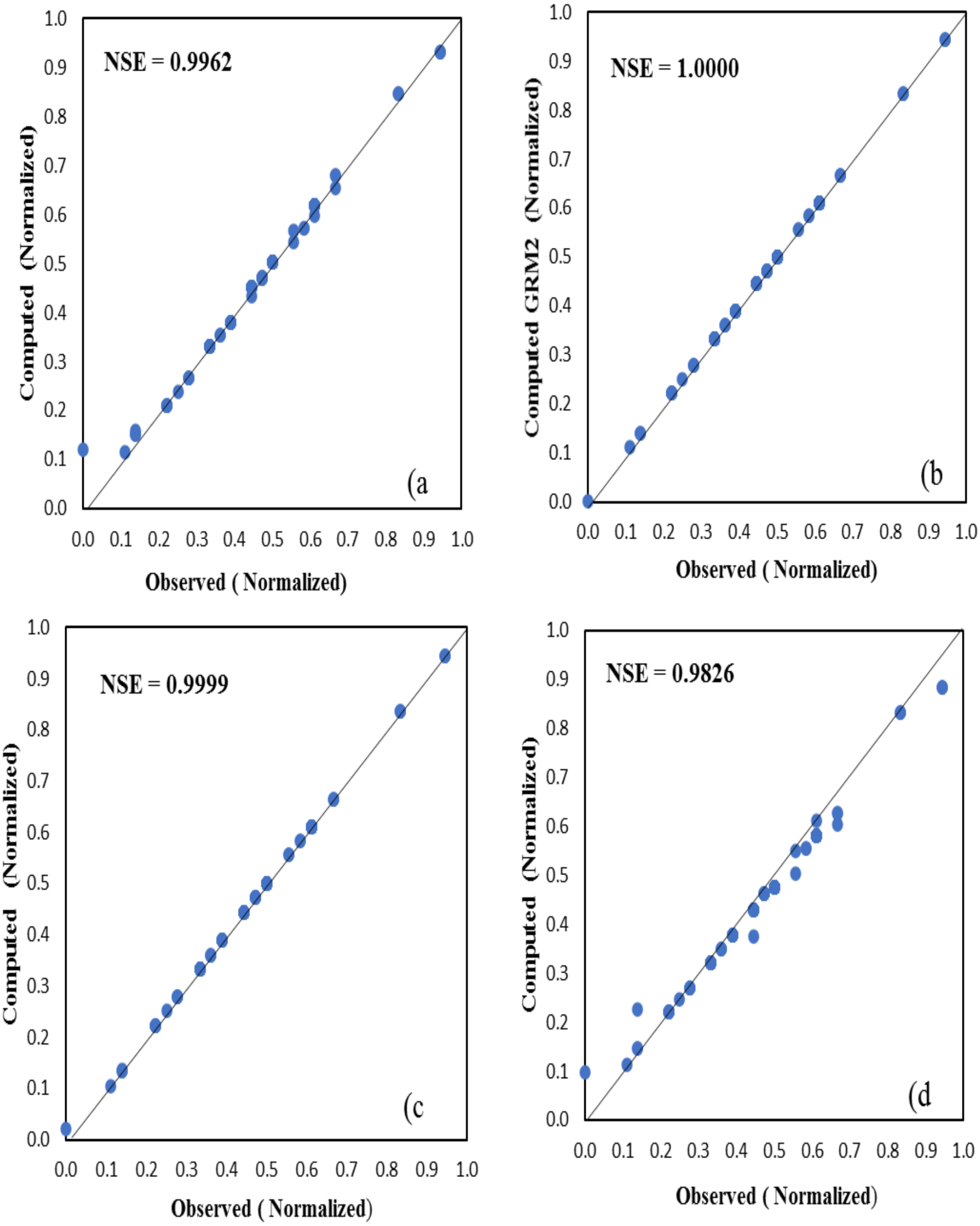
Calibration Strew Plots Between Calculated and Experimental Effects of Security on M-banking Continued Patronage and Progress by a) ANN, b) SVM, c) GPR, and d) BRT Models



As shown in Figure 31, the NSE metric results obtained in the calibration strew plots of the four AI models (i.e., ANN, SVM, GPR, and BRT) employed in the study signify the projection ability of AI-based methods in terms of precision, reliability, and robustness. The result (i.e., (i.e., $X_1, - X_n$ precisions results) is supported by the arguments of Ahmad and Aftab (2017). The authors stressed that estimation ability of machine learning (ML) models are normally influenced by calibration outcomes of the models, as plots with fitted data lines indicate good calibration performance which in turn increase models estimation ability and vice versa. Furthermore, the model’s NSE values in calibration clearly shows how pretty well the study simulated and observed data fits the plots line indicating a strong correlation between security and “m-banking” continuous patronage and advancement in the study locations. Also, this result is strengthened by the findings of Ambarwari et al. (2020) who argued that hiher NSE values in ML modelling indicates strong connection between parameters under investigation. Likewise, the results further confirm the performance outcomes of the separate models obtained in sole modelling process as shown in Table 11. The testing scatter plots of the study separate models are presented in Figure 32.

Figure 32.

Verification Strew Plots Between Calculated and Experimental Effects of Security on M-banking Continued Patronage and Progress by a) ANN, b) SVM, c) GPR, and d) BRT Models



As seen in Figure 32, the verification strews plots results show similar signs like that of the training scatter plots with little variance, signifying how good the computed and observed datasets fit well in the line plots. Similarly, the testing scatter plots results reaffirm the prediction skills of the study AI based replicas i.e., BRT, GPR, SVM, and ANN. The verification results (i.e., $X_1, - X_n$ precisions results) clearly shows that performance of the research proposed AI models at the verification phase is higher compared to the calibration performance signifying the estimation ability of the models. This outcome is strengthened by the sentiments of Dao et al. (2020) who argued that verification phase performance of any reliable ML models are usually higher than the performance obtained in the calibration phase. Also, the findings evidently shows that the research inputs parameters i.e., system security, ease of use, privacy, information, and interface qualities were the main issues affecting "m-banking" continuous patronage and advancement in the study locations i.e., Cyprus, Iraq, and Nigeria. This result also supported the verdicts of Deepa et al. (2021) who argued that ML methods such as ANN, and SVM have proven to be effectual, and robust in studies that involves investigation of emotions. Thus, the need for m-banking stakeholders to do more in the areas of m-banking security. Results concerning the security effects on "m-banking" continuous patronage and advancement in Nigeria, Iraq, and Cyprus as predicted by the study four AI proposed models were offered in the next section.

5.3 Security Effects on M-banking Continues Patronage and Advancement in the Study Areas

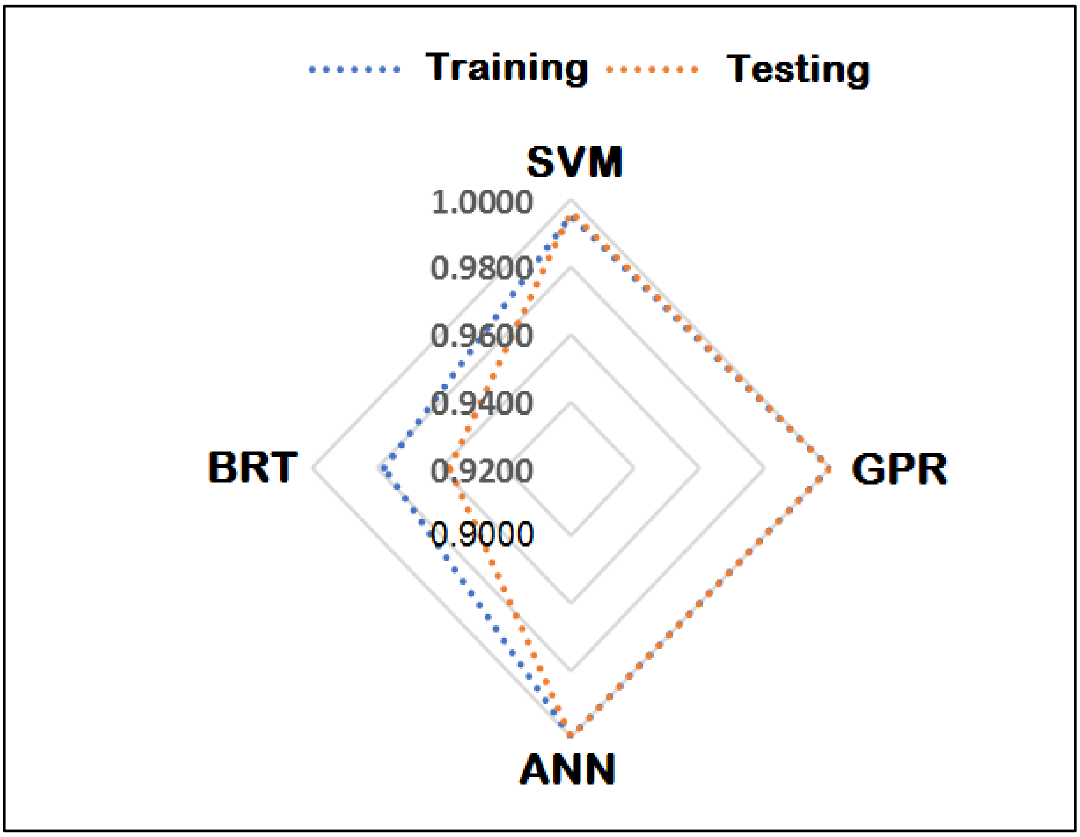
Based on the prediction results obtained from the study proposed non-linear models (GPR, ANN, SVM, and BRT), and the ensemble model as shown in Figure 33, it can be seen that all the study AI models, estimated the influence of security (X_1) on the output parameter y i.e., "m-banking" continuous patronage and advancement in Nigeria, Iraq, and Cyprus with higher precision. Thus, it can be said that security (X_1) is the main reasons for Nigerians, Iraqis, and Cypriots lack of continued interest in m-banking services which in turn affects its progress. The result is reinforced by the results of Kasiyanto (2016) and Williams (2021) who stressed that security may likely become the key determinant of m-payment systems (m-banking) in the near future. The authors' argued that people are increasingly becoming worried about the security of coffers and other sensitive data conveyed via "m-banking" platforms, and that if the issue is not properly addressed by payment institutions it may likely affect the future prospects of all m-payment platforms not only developing markets, but also developed markets. But the result contradicts the verdicts of Giovanis et al. (2018) who found "social influnce to be the key determinants of innovative retail banking platforms such as m-banking" amongst young people (Giovanis et al., 2018: p.13).

For the ensemble model prediction result, the result was obtained via ensemble techniques where output (y) of each of the study AI models (i.e., ANN, BRT, SVM, GPR, BRT) were assembled to form the inputs of the study ensemble model in order to enhance the concert of the reported model. The collaborative activities were carried out with 70-30 data proportion for training and testing as suggested by (Abd Jalil et al., 2010). The results produced by all the four AI developed models (i.e., ANN, SVM, GPR, and BRT) were pretty good as all the predicted values were very close to the targeted value of 1. Also, the models' estimation results (Figure 33) clearly indicates that there is a significant relationship between "m-banking" continued patronage and development, and security and other experimental variables in the study areas. The result is supported by the results of Vom Lehn et al. (2020) who stressed that AI based studies with moderate parameters (i.e., not too many nor little) usually produced better results. Furthermore, the results confirm the robustness and reliability of the study developed AI based anomalies and authentication system in terms of detecting and handling velocity anomalies during login, and highlights the proposed system ability to differentiate authentic user from unauthorize user.

As shown in Figure 33, the 1.0000 values at the left top corner of the study reported model radar plots represent the target value, while 0.9800 represent the ensemble model estimation result, and the remaining values of 0.9600, 0.9400, 0.9200, and 0.9000 represents the forecasted effects of protection on m-banking advancement made by the separate models (i.e., SVM, GPR, ANN, and BRT). The ensemble model estimation result of 0.9800 clearly shows that the approach enhanced the research proposed non-linear models' concert. The result is strengthened by the results of Nourani et al. (2020) and Cavus et al. (2021b) who stressed that collaborative (ensemble) methods usually enhance the concert of AI based single models. Though, based on the models' estimation results (Figure 33), all the proposed AI models performed well. However, it can be seen that the SVM model outperformed the other three non-linear models (GPR, ANN, and BRT) in terms of predicting security effects on "m-banking" continues attractiveness and advancement in the three study locations, as the model has an estimation value of 0.9600 which is closer to the study target values of 1.0000 compare to GPR = 0.9400, ANN = 0.9200, and BRT = 0.90000 respectively. Possibly the high performance of the SVM model was achieved due to the model's ability to detect and treat unseen data in the study dataset. The result is supported by the results of Pourghasemi and Rahmati (2018) who claimed that “SVM technique has the ability to handle input-output data uncertainties compared to other AI-based techniques e.g., BRT, ANN, and GPR” (Pourghasemi & Rahmati 2018: p.9), thus, increase the model predictions abilities above others. Furthermore, based on the estimation outcomes, it can be seen that the estimation (0.9800) made by the study ensemble model increased the performance of the study final model by 2% in the case of SVM model, 4% for GPR model, 6% for ANN model, and 8% for the study BRT model. This is because ensemble approach usually improves the performance of AI based models (Madisetty & Desarkar, 2018). Predictions results of the separate AI models and the ensemble model are offered in Figure 33.

Figure 33.

The Study Model Prediction Outcomes by a) Ensemble, b) SVM, c) GPR, d) ANN, and e) BRT Models.



Performance of the models were further verified using Taylor diagram. Taylor diagram is used by scholars to measure models' goodness-of-fit, and grading of study autonomous parameters. Thus, the diagram was used in this study to rank the study proposed AI models, and determine the effects level of each of the study choosing parameters on "m-banking" continuous attractiveness and advancement in the three study locations. Taylor diagram offers precise means of measuring the correctness of different study models, and grading of study parameters via comparation of three arithmetic indices; standard deviation, correlation coefficient, and RMSE in a pictorial way in order to evaluate models' relative concert (Taylor, 2001). As shown in Figure 34, and Figure 35, the correlation amongst the different arenas is signified by the horizontal spot of the assessment arena, measuring the deviation standard pattern from the derivation in a radius manner, while the RMSE values are proportioned between the forecasted and actual fields with similar units as the standard deviation. The RMSE values reduce, when the correlation value increases, and increase when correlation value decreases. Therefore, a faultless model is the one that is divided by the orientation points with the "correlation coefficient that is equal to 1, and similar abundancy of varieties contrasted with the observation" (Gleckler et al., 2008: p.6).

Just like the radar plot Figure 33, and scatter plots Figure 31, and Figure 32, the "Taylor diagram" results also shows that the study proposed AI models (ANN, BRT, GPR, SVM) forecasted the influence of security on m-banking with higher precision, as the models' correlation coefficient stood at > 0.95 in confirmation phase, and > 0.9 in the calibration phase signifying the levels of security effects on "m-banking" continuous demand and development in the study areas. Also, the models' "standard deviation" values obtained are smaller than that of the real dataset with little difference indicating that the model's excessive estimation (i.e., prediction outcomes) does not in any way affect the models' concert. The study Taylor result is supported by the findings of Cavus et al. (2022) who argued that Taylor diagram offers an efficient means of correlations measurement between two or more study variables via its derivation and deviation patterns.

Based on the "Taylor diagram", the study developed models were graded as; first = SVM, second = GPR, third = ANN, and fourth = BRT as shown in Figure 34, and Figure 35.

Figure 34.

Taylor Diagram Comparing the Performance of the Study Proposed Models in the Calibration Phase

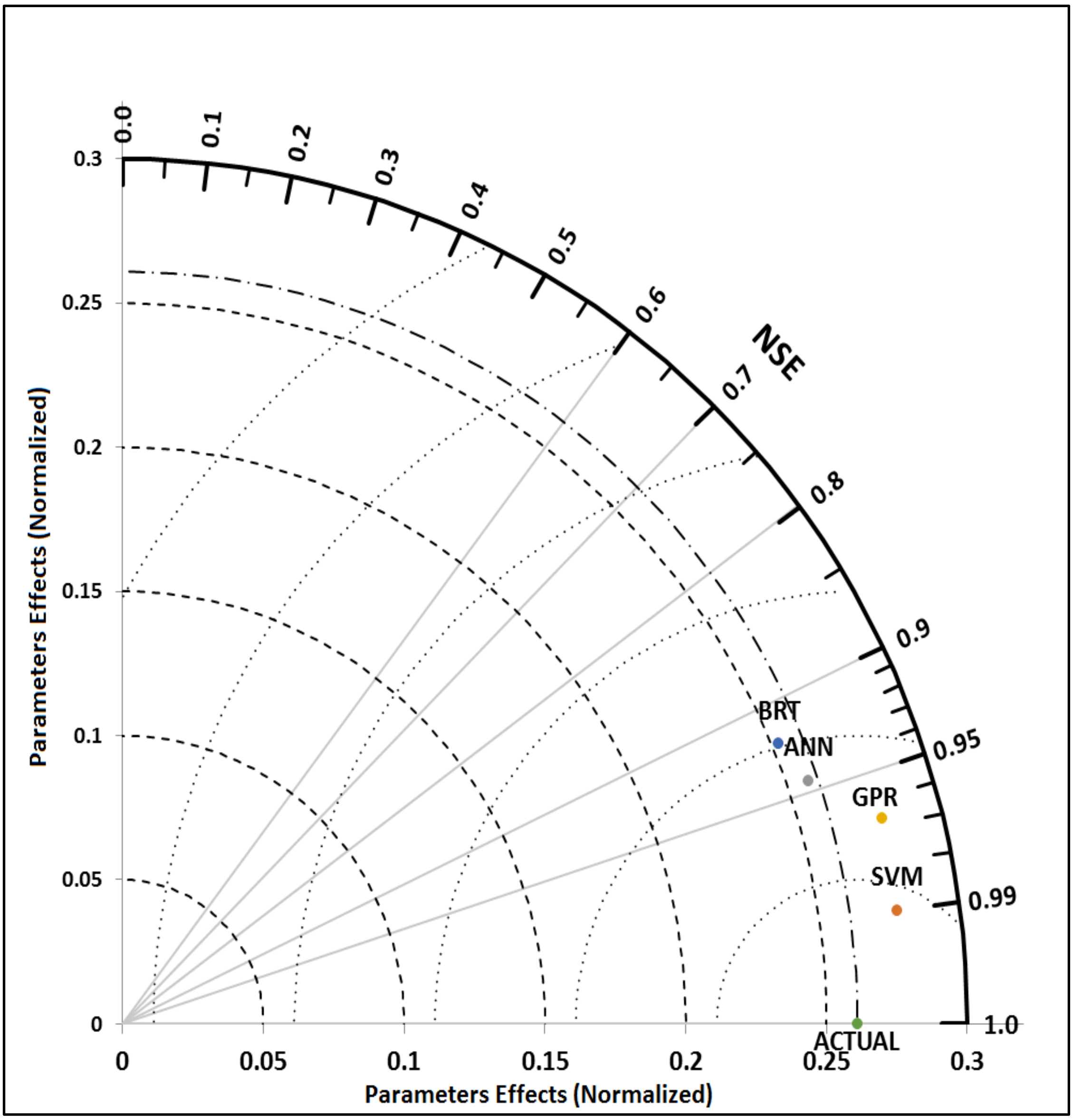
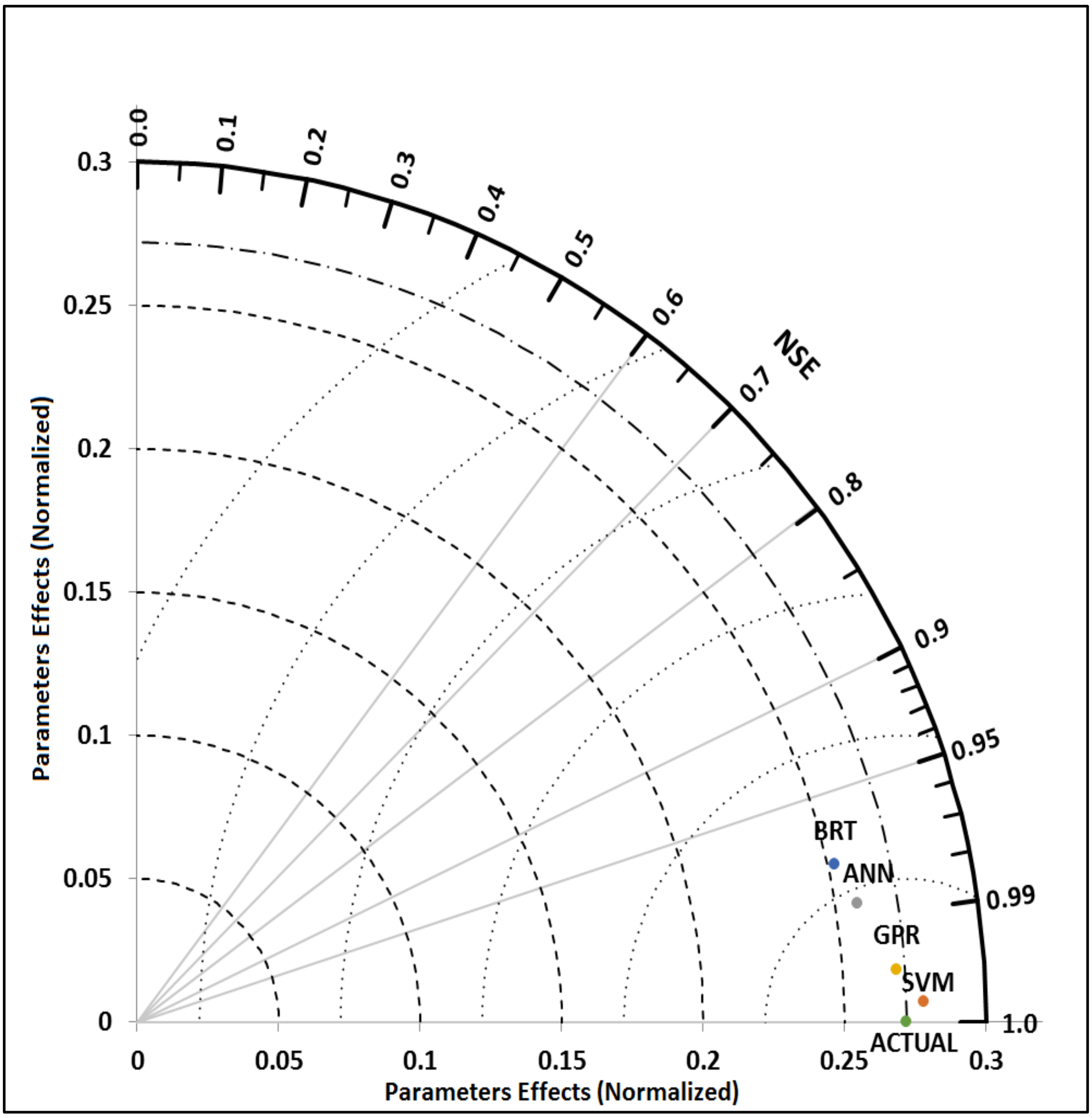


Figure 35.

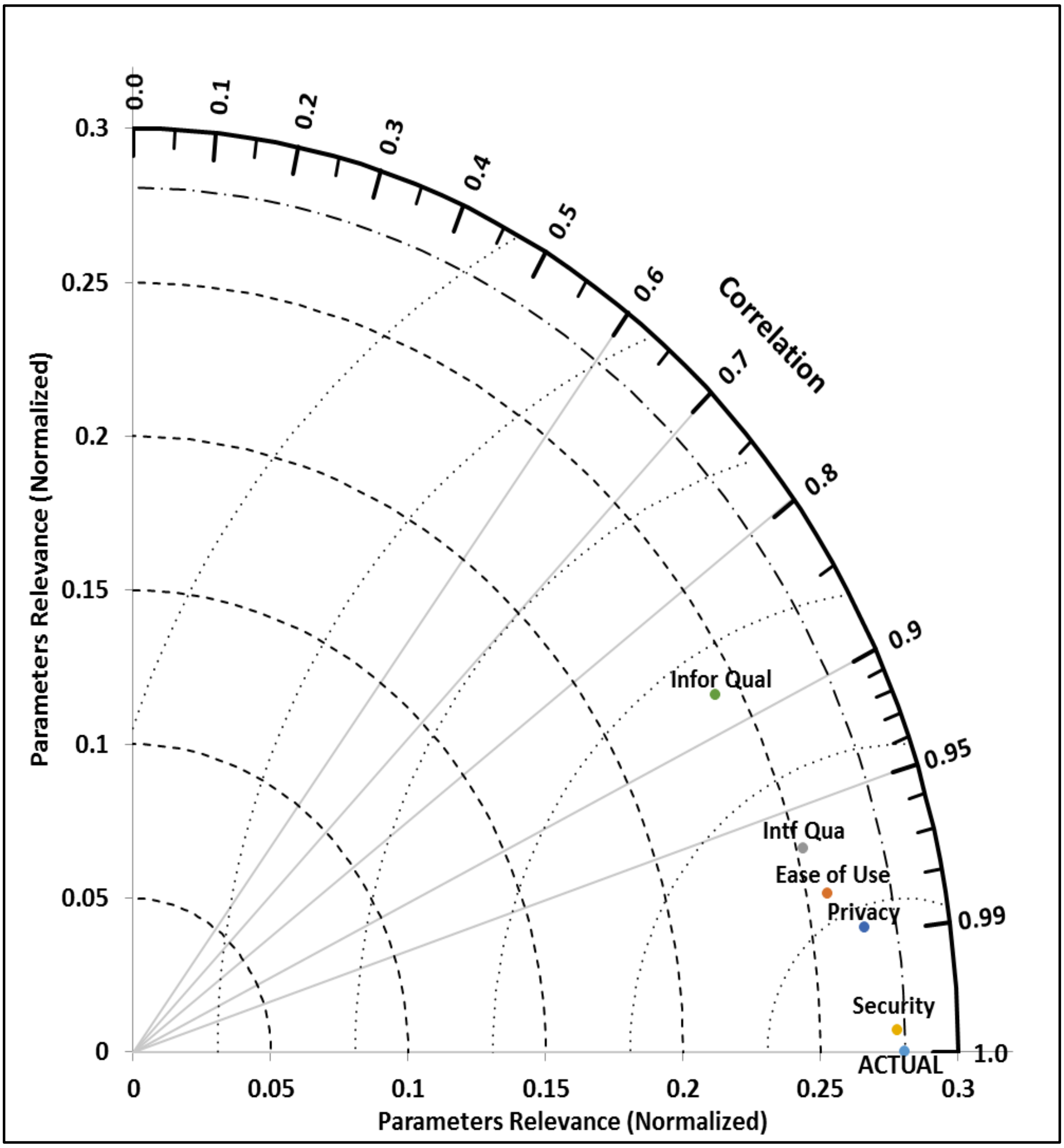
Taylor Diagram Comparing the Performance of the Study proposed Models in the Verification Phase.



Having compared the study proposed AI models concert using Taylor diagram, relevance of each of the study input parameters were further checked using the "Taylor diagram" in order to reaffirm the study relevancy investigation results or otherwise. As shown in Figure 36, people concern for safety in m-banking (X_1) is the most important parameter amongst study input variables, followed by people needs for secrecy (X_2). These results contradict the findings of Baabdullah et al. (2019) and Khan et al. (2021) who stressed that cultural differences and excellence of m-banking service offered were the main determinants of "m-banking" patronage and continual usage, but is supported by the findings of Cavus et al. (2021a) who argued that “safety and secrecy are likely to be the key determinants of m-banking continuance usage and progress not only in developing nations, but also in developed states” (Cavus et al., 2021a: p.11). While system ease of usage (X_3), and interface quality (X_4) were ranked third and fourth respectively. Also, the diagram clearly shows that quality of information provided (X_5) in m-banking channels is the least important parameter amongst the study inputs. This result contradicts the findings of Sharma and Sharma (2019) who stated that “quality of information provided in m-banking platforms by the servicing institutions influence customers’ intent to use the service channel” (Sharma & Sharma 2019: p.6), as adequate and excellence information provision enhanced patronage and continuance usage, while poor information negatively affects advancement. Effects of each of the study choosing parameters on m-banking patronage and progress in the study locations is presented Figure 36.

Figure 36.

Ranking of the Study Parameters Relevance Using Taylor Diagram



5.4 Confusion Matrix and ROC Curves Results

As seen in Figure 36, and Figure 33 (single model precision results), it can be said that all the study input parameters i.e., $X_1,\ X_2, X_3, X_4, X_5$ were found to have significant effects on the study output parameter y (i.e., m-banking continued patronage and development) in the three study areas of Nigeria, Iraq, and Cyprus. Results regarding effects of the study input parameters i.e., $X_1,\ X_2, X_3, X_4, X_5$ were classified using ROC arcs and confusion matrix as shown in Figure 37, and Figure 38. The inputs were categorized into two classes, the first class comprises of $X_1,\ and\ X_2,$ while second class consisted of X_3, X_4, X_5 in order to determine which class was predicted correctly, and has the most significance effects on the study output variable y (i.e., m-banking continues patronage and development) in the study areas. The confusion matrix results clearly indicate that both classes were predicted correctly signifying the effects of X results on the study output y as shown in Figure 37. Furthermore, the ROC arcs results shows that SVM, GPR, and ANN models has the highest classification precision in terms of classifying the effects of protection, privacy, ease of use, interface and information quality (i.e., $X_1,\ X_2, X_3$, X_4, X_5) on “m-banking patronage and continual usage” (i.e., y) in the study areas with 99% precision compared to BRT model that has classified the effects with 96% accuracy. The ROC arcs and confusion matrix diagrams were presented in Figure 37, and Figure 38.

Figure 37.

Study Confusion Matrix by (a) SVM, (b) GPR, (c) ANN, (d) BRT

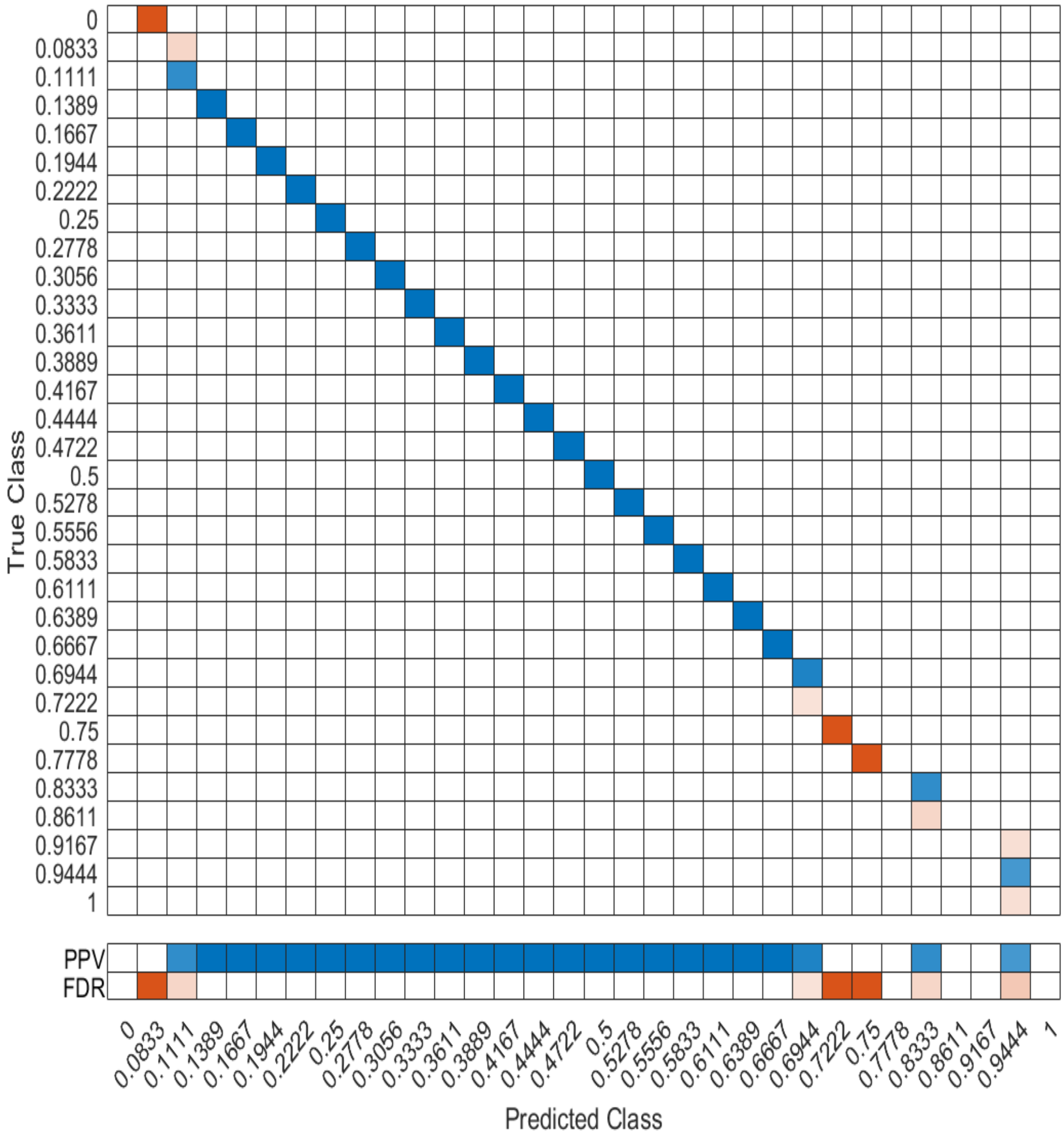
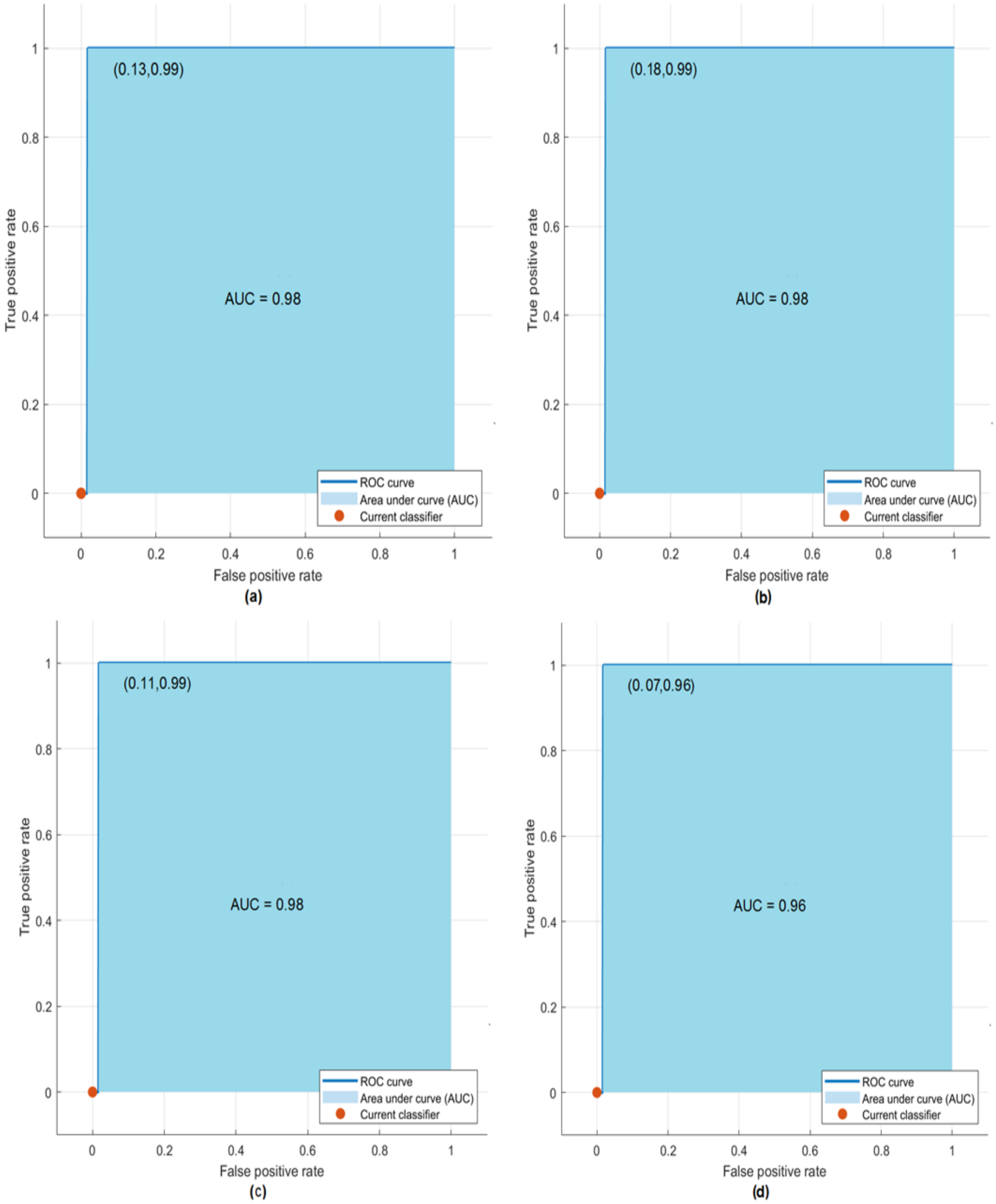


Figure 38.

Models ROC Curves Results by (a) SVM, (b) GPR, (c) ANN, (d) BRT



5.5 Vulnerability of Present M-banking Authentication Methods

Based on the study systematic literature review (SLR) findings, the study found majority if not all the user authentication methods employed by banks and other payment institutions to be susceptible to various attacks and threats due to rise in online frauds, particularly during COVID-19 lockdown. For instance, the study discovered that both single and two factors authentication approaches are increasingly becoming weak, and subjected to different forms of attacks due to their feebleness. This outcome is supported by the results of Parker et al. (2015) and Bani-Hani et al. (2019) who stressed that both "single and two factors verification schemes are becoming frail and exposed to various threats as hackers can access client login information such as username, pin and password" through other applications that are stuffed on moveable devices.

For multi-factor verification (MFA), though, the technique is more secure and robust compared to single and two factors verification methods. However, the study discovered that in addition to feebleness and susceptibility issues, memorability is another factor affecting the robustness of different multi-factor verification methods used by payment institutions, as clients find it hard to continue memorizing the multiple login particulars, particularly the ageing clients. Also, the technique (MFA) is complicated as it involves a lot of risk, and makes maintenance of regional privacy, information laws, protection standards, and banking governance difficult. This result is reinforced by the outcomes of Choi et al. (2020) who stressed that "multi-factor authentication" is the most complex verification approach as it makes banking management difficult, as imbursement institutions find it hard to manage safety protocols via multi-factor verification method.

For the Biometric verification approach, this study found the newly introduced "Biometric authentication schemes" to be susceptible, as surface utilized by legitimate user can be used to compromise the security apparatus in order to gain access to the system which may lead to identity theft, data theft, or financial loses. Also, this result is in agreement with the results of Wang et al. (2020) who argued that just like the multi-factors approaches, the biometric approaches also are not secured in "an environment where there are multiple-servers like that of m-payment systems e.g., m-banking platforms". Thus, the need for a more robust approach.

For the study proposed AI based authentication and anomalies detection system, based the usability testing results Figure 26 – 30, it can be seen that the proposed AI based system is more robust and secured compared to other verification methods recently used by banks and other payment institutions, as majority of the participants that used the system expressed satisfaction regarding the safety and secrecy features of the system, qualities of information and interfaces provided in the system, and how easy it was to use the system. Thus, based on the testing results it can be said that the study proposed AI based system is more flexible in terms of memorability, but more secure than single, double, and multi-factors' approaches. Additionally, it was discovered that the proposed has the ability to detect and handle any anomalies during login which make the system more unique, and secured than the biometric methods. Thus, it can be said that the proposed AI based system is more robust and secured compared to other verification methods used by banks.

CHAPTER VI

CONCLUSION AND RECOMMENDATIONS

In this chapter, conclusions regarding the study key findings were made. Also, importance and limitations of the research were stated. Likewise, suggestions for various m-banking stakeholders, software developers, and researchers were also offered in the chapter.

6.1 Conclusion

In this study, influence of security on "m-banking" continuous patronage and advancement in three different countries i.e., Cyprus, Iraq, and Nigeria was investigated and simulated using 4 separate "artificial intelligence" (AI) models; ANN, BRT, GPR, BRT, and one ensemble model. t was discovered that the level of security effects on m-banking continues advancement in the research areas are highly significance, as the research proposed AI models forecasted the effects of protection on m-banking with higher precisions, with correlation coefficient of > 0.95, especially in Nigeria, and Iraq. The result may not be unconnected with the countries (Nigeria, Iraq) level of underdevelopment in terms of technological advancement compared to Cyprus. Appropriate actions are therefore needed to lessen the effects of security parameter on "m-banking" continued patronage and progress in study locations. Thus, it can be said that the results provided support for the study objectives, as the results evidently and concisely answered the main research questions of the study.

Prior to the development of the AI based security models (GPR, ANN, SVM, BRT), a non-linear sensitivity examination was carried out in order to select the most influential predictors of "m-banking" continuous advancement in the research areas. Security, privacy, ease of use, and interface quality were found to be the most pertinent parameters contributing to the slow growth, and people lack of continual usage of m-banking in the study locations. While, information quality was found to have little effects on m-banking advancement in the study locations. Consequently, it can be said that all the study proposed sole non-linear AI based models (GPR, ANN, SVM, BRT) produced an estimation value of > 0.9 signifying the precision of the results obtained, and robustness of AI based models in terms of estimation ability. Though, all the study proposed single AI models performed well. However, it can be seen that the SVM model outperform the other three non-linear models (GPR, ANN, and BRT) in terms of predicting the security effects on “m-banking” attractiveness, and advancement in the research areas, as the model has an estimation value of > 0.95 which is closer to the study target value of 1.0000 compared to other models’ estimation values of > 0.9. also, the novel model (ensemble model) was developed using outputs of the single models as inputs to the ensemble method, and the approach was found to be effective by enhancing the concert of the sole models (SVM, GPR, ANN, BRT) in confirmation phase by 2%, 4%, 6%, and 8% respectively. Thus, it can be said that findings of the study provide support for the study proposed AI models, and the developed AI based authentication and anomalies detection system in terms of security effects on m-banking in the study locations, and robustness of the proposed AI based system.

Based on the study results, it can be seen that employing the use of robust user verification, and anomalies detection procedures like that of the study proposed AI based authentication and anomalies detection system could improve m-banking security which in turn may decrease the effects of security on m-banking, and increase customers patronage of the services conduit. Therefore, it can be said that the research contributes to the existing body of knowledge by highlighting the robustness of AI methods, main forecasters of m-payment systems, and level of security effects on m-banking advancements.

6.2 Recommendations

Suggestions to various m-payments stakeholders such as customers, banks, software developers, and researchers were offered in following subsections.

6.2.1 Recommendations for Banks

Based on the findings obtained in this study using different AI based modelling, the following suggestions were offered:

- Influence of security of m-banking advancement in the study locations are high. Therefore, appropriate actions are needed from the sides of banks, and other imbursement organizations to lessen the influence of security on m-banking advancement such as deployment of modify - 2 - way OTP proposed in this study.
- Imbursement institutions and other relevant government agencies responsible for the implementation of cashless policies via m-payment platforms could use the

study AI based approach for forecasting key determinants of m-payments advancement as the approach offers precise and reliable results.

- In assessing and forecasting key determinants of m-banking acceptance and continuous usage, customers concern for safety and secrecy should be included as findings of the study highlights their relevance.

6.2.2 Recommendations for Customers

- Customers can use the study results to understand the complexity, and problems associated with the different user authentication techniques employed by banks and other imbursement institutions.
- Results of the study can also assist customers in understanding the importance of protecting login details such as PIN, user ID, Password, and other sensitive information from being exposed.
- Customers can use the study findings to understand the benefits of using m-banking platforms in conducting their financial dealings as the results highlights the flexibility, and efficacy of m-banking podiums.

6.2.3 Recommendations for Software Developers

- Software developers can use the study iterative approach which is more of user, device, and location-based cantered due to its anomalies detection capability to develop more flexible, and robust online user verification systems that can reduce the rate of internet crimes, especially in m-payment systems platforms.

6.2.4 Recommendations for Future Researchers

- Upcoming studies should use other machine learning methods such as “gradient boosting approach e.g., Leas-Square Boosting” (LSBoost), emotional artificial neural network (EANN) ensemble, and manifold linear regression (MLR) to further assess the influence of safety and privacy on m-banking advancement in both advance and developing digital markets.
- This study is limited to the approach used (i.e., AI based approach), and dataset used. Thus, future research should use a combination of empirical methods such as Pearson correlation and leas square methods, and AI based procedures such as ANFIS so that performance of the two approaches can be compared.

- Future research should also use the study proposed AI based system as benchmark for developing future user verification systems for online platforms.

References

Abd Jalil, K., Kamarudin, M. H., & Masrek, M. N. (2010). Comparison of machine learning algorithms performance in detecting network intrusion. In *Proceedings of the International Conference on Networking and Information Technology*, (pp. 221-226). EEE. https://doi.org/10.1109/icnit.2010.5508526

Abdullah, M., Alshannaq, A., Balamash, A., & Almabdy, S. (2018). Enhanced intrusion detection system using feature selection method and ensemble learning algorithms. *International Journal of Computer Science and Information Security (IJCSIS), 16*(2), 48-55. https://doi.org/10.1016/j.procs.2018.10.416

Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. *Heliyon, 4*(11), e00938. https://doi.org/10.1016/j.heliyon.2018.e00938

Abo-Zahhad, M., Ahmed, S. M., & Abbas, S. N. (2014). Biometric authentication based on PCG and ECG signals: present status and future directions. *Signal, Image and Video Processing, 8*(4), 739-751. https://doi.org/10.1007/s11760-013-0593-4

Agarwal, N. K. (2011). Verifying survey items for construct validity: A two-stage sorting procedure for questionnaire design in information behavior research. *proceedings of the American Society for Information Science and Technology, 48*(1), 1-8. https://doi.org/10.1002/meet.2011.14504801166

Ahmad, M., & Aftab, S. (2017). Analyzing the Performance of SVM for Polarity Detection with Different Datasets. *International Journal of Modern Education & Computer Science, 9*(10). https://doi.org/10.5815/ijmecs.2017.10.04

Aithal, P. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. *International Journal of Management, IT and Engineering, 5*(7), 455-464. https://doi.org/77.9027ssrn. 2015.11.03.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-t

Akhavian, R., & Behzadan, A. H. (2015). Construction equipment activity recognition for simulation input modeling using mobile sensors and machine learning classifiers. *Advanced Engineering Informatics, 29*(4), 867-877. https://doi.org/10.1016/j.aei.2015.03.001

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Algharabat, R. (2018). Examining factors influencing Jordanian customers' intentions and adoption of internet banking: Extending UTAUT2 with risk. *Journal of Retailing and Consumer Services, 40*, 125-138. https://doi.org/10.1016/j.jretconser.2017.08.026

Albashrawi, M., & Motiwalla, L. (2019). Privacy and personalization in continued usage intention of mobile banking: An integrative perspective. *Information Systems Frontiers, 21*(5), 1031-1043. https://doi.org/10.1007/s10796-017-9814-7

Alhothaily, A., Alrawais, A., Hu, C., & Li, W. (2018). One-time-username: A threshold-based authentication system. *Procedia Computer Science, 129*, 426-432. https://doi.org/10.1007/s10796-017-9814-7

Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. *International Journal of Information Management, 53*, 102102. https://doi.org/10.1016/j.ijinfomgt.2020.102102

Ambarwari, A., Adrian, Q. J., & Herdiyeni, Y. (2020). Analysis of the effect of data scaling on the performance of the machine learning algorithm for plant identification. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4*(1), 117-122. https://doi.org/10.29207/resti.v4i1.1517

Ammar, A., & Ahmed, E. M. (2016). Factors influencing Sudanese microfinance intention to adopt mobile banking. *Cogent Business & Management, 3*(1), 1154257. https://doi.org/10.1080/23311975.2016.1154257

Andaryani, S., Nourani, V., Haghighi, A. T., & Keesstra, S. (2021). Integration of hard and soft supervised machine learning for flood susceptibility mapping. *Journal of Environmental Management, 291,* 112731. https://doi.org/10.1016/j.jenvman.2021.112731

Apostolopoulos, D., Marinakis, G., Ntantogian, C., & Xenakis, C. (2013). Discovering authentication credentials in volatile memory of android mobile devices. In *Proceedings of the International Conference on e-Business, e-Services and e-Society,* (pp. 178-185). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37437-1_15

Asastani, H. L., Kusumawardhana, V. H., & Warnars, H. L. H. S. (2018). Factors affecting the usage of mobile commerce using technology acceptance model (TAM) and unified theory of acceptance and use of technology (UTAUT). In *Proceedings of the Indonesian Association for Pattern Recognition International Conference (INAPR),* (pp. 322-328). IEEE. https://doi.org/10.1109/inapr.2018.8627003

Asnakew, Z. S. (2020). Customers' continuance intention to use mobile banking: development and testing of an integrated model. *The Review of Socionetwork Strategies, 14*(1), 123-146. https://doi.org/10.1007/s12626-020-00060-7

Asongu, S. A. (2018). Conditional determinants of mobile phones penetration and mobile banking in Sub-Saharan Africa. *Journal of the Knowledge Economy, 9*(1), 81-135. https://doi.org/10.1007/s13132-015-0322-z

Aydin, A. D., & Cavdar, S. C. (2015). Comparison of prediction performances of artificial neural network (ANN) and vector autoregressive (VAR) Models by using the macroeconomic variables of gold prices, Borsa Istanbul (BIST) 100 index and US Dollar-Turkish Lira (USD/TRY) exchange rates. *Procedia Economics and Finance, 30*, 3-14. https://doi.org/10.1016/s2212-5671(15)01249-6

Baabdullah, A. M., Alalwan, A. A., Rana, N. P., Kizgin, H., & Patil, P. (2019). Consumer use of mobile banking (M-Banking) in Saudi Arabia: Towards an integrated model. *International Journal of Information Management, 44*, 38-52. https://doi.org/10.1016/j.ijinfomgt.2018.09.002

Bahrammirzaee, A. (2010). A comparative survey of artificial intelligence applications in finance: artificial neural networks, expert system and hybrid intelligent systems. *Neural Computing and Applications, 19*(8), 1165-1195. https://doi.org/10.1007/s00521-010-0362-z

Bani-Hani, A., Majdalweieh, M., & AlShamsi, A. (2019). Online authentication methods used in banks and attacks against these methods. *Procedia Computer Science, 151*, 1052-1059. https://doi.org/10.1016/j.procs.2019.04.149

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and informatics, 35*(5), 1491-1511. https://doi.org/10.1016/j.tele.2018.03.018

Barkhordari, M., Nourollah, Z., Mashayekhi, H., Mashayekhi, Y., & Ahangar, M. S. (2017). Factors influencing adoption of e-payment systems: an empirical study on Iranian customers. *Information Systems and e-Business Management, 15*(1), 89-116. https://doi.org/10.1007/s10257-016-0311-1

Basar, O. E., Alptekin, G., Volaka, H. C., Isbilen, M., & Incel, O. D. (2019). Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication. *Procedia Computer Science, 155*, 185-192. https://doi.org/10.1016/j.procs.2019.08.028

Bermudez-Edo, M., Barnaghi, P., & Moessner, K. (2018). Analysing real world data streams with spatio-temporal correlations: Entropy vs. Pearson correlation. *Automation in Construction, 88*, 87-100. https://doi.org/10.1016/j.autcon.2017.12.036

Bhaskar, H., Hoyle, D. C., & Singh, S. (2006). Machine learning in bioinformatics: A brief survey and recommendations for practitioners. *Computers in biology and medicine, 36*(10), 1104-1125. https://doi.org/10.1016/j.compbiomed.2005.09.002

Boateng, H., Adam, D. R., Okoe, A. F., & Anning-Dorson, T. (2016). Assessing the determinants of internet banking adoption intentions: A social cognitive theory perspective. *Computers in human behavior, 65*, 468-478. https://doi.org/10.1016/j.chb.2016.09.017

Bogner, J., Verdecchia, R., & Gerostathopoulos, I. (2021). Characterizing technical debt and antipatterns in ai-based systems: A systematic mapping study. A systematic mapping study. In *Proceedings of the IEEE/ACM International Conference on Technical Debt (TechDebt)* (pp. 64-73). IEEE. https://doi.org/10.1109/techdebt52882.2021.00016

Borgonovo, E., & Plischke, E. (2016). Sensitivity analysis: a review of recent advances. *European Journal of Operational Research, 248*(3), 869-887. https://doi.org/10.1016/j.ejor.2015.06.032

Brody, R. G., Kern, S., & Ogunade, K. (2020). An insider's look at the rise of Nigerian 419 scams. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-12-2019-0162

Cavus, N., Mohammed, Y. B., Gital, A. Y. u., Bulama, M., Tukur, A. M., Mohammed, D., Isah, M. L., & Hassan, A. (2022). Emotional Artificial Neural Networks and Gaussian Process-Regression-Based Hybrid Machine-Learning Model for Prediction of Security and Privacy Effects on M-Banking Attractiveness. Sustainability, 14(10), 5826. https://doi.org/10.3390/su14105826

Cavus, N., Mohammed, Y. B., & Yakubu, M. N. (2021a). An Artificial Intelligence-Based Model for Prediction of Parameters Affecting Sustainable Growth of Mobile Banking Apps. *Sustainability, 13*(11), 6206. https://doi.org/10.3390/su13116206

Cavus, N., Mohammed, Y. B., & Yakubu, M. N. (2021b). Determinants of learning management systems during covid-19 pandemic for sustainable education. *Sustainability, 13*(9), 5189. https://doi.org/10.3390/su13095189

Chaimaa, B., Najib, E., & Rachid, H. (2021). E-banking Overview: Concepts, Challenges and Solutions. *Wireless personal communications, 117*(2), 1059-1078. https://doi.org/10.1007/s11277-020-07911-0

Chanajitt, R., Viriyasitavat, W., & Choo, K.-K. R. (2018). Forensic analysis and security assessment of Android m-banking apps. *Australian Journal of Forensic Sciences, 50*(1), 3-19. https://doi.org/10.1080/00450618.2016.1182589

Chen, C.-M., Hsu, C.-Y., Chiu, H.-W., & Rau, H.-H. (2011). Prediction of survival in patients with liver cancer using artificial neural networks and classification and regression trees. In *Proceedings of the Seventh International Conference on Natural Computation*, (Vol. 2, pp. 811-815). IEEE. https://doi.org/10.1109/icnc.2011.6022187

Chen, X., Choi, K., & Chae, K. (2017). A secure and efficient key authentication using bilinear pairing for NFC mobile payment service. *Wireless personal communications, 97*(1), 1-17. https://doi.org/10.1007/s11277-017-4261-9

Choi, H., Park, J., Kim, J., & Jung, Y. (2020). Consumer preferences of attributes of mobile payment services in South Korea. *Telematics and informatics, 51*, 101397. https://doi.org/10.1016/j.tele.2020.101397

Da, B., Ong, Y.-S., Gupta, A., Feng, L., & Liu, H. (2019). Fast transfer Gaussian process regression with large-scale sources. *Knowledge-Based Systems, 165*, 208-218. https://doi.org/10.1016/j.knosys.2018.11.029

Dao, D. V., Adeli, H., Ly, H.-B., Le, L. M., Le, V. M., Le, T.-T., & Pham, B. T. (2020). A sensitivity and robustness analysis of GPR and ANN for high-performance concrete compressive strength prediction using a Monte Carlo simulation. *Sustainability, 12*(3), 830. https://doi.org/10.3390/su12030830

Dauda, S. Y., & Lee, J. (2015). Technology adoption: A conjoint analysis of consumers′ preference on future online banking services. *Information Systems, 53*, 1-15. https://doi.org/10.1016/j.is.2015.04.006

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340. https://doi.org/10.2307/249008

De Reuver, M., & Ondrus, J. (2017). When technological superiority is not enough: The struggle to impose the SIM card as the NFC Secure Element for mobile payment platforms. *Telecommunications Policy, 41*(4), 253-262. https://doi.org/10.1016/j.telpol.2017.01.004

Deepa, N., Prabadevi, B., Maddikunta, P. K., Gadekallu, T. R., Baker, T., Khan, M. A., & Tariq, U. (2021). An AI-based intelligent system for healthcare analysis using Ridge-Adaline Stochastic Gradient Descent Classifier. *The Journal of Supercomputing, 77*(2), 1998-2017. https://doi.org/10.1007/s11227-020-03347-2

Delen, D. (2010). A comparative analysis of machine learning techniques for student retention management. *Decision Support Systems, 49*(4), 498-506. https://doi.org/10.1016/j.dss.2010.06.003

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of management information systems, 19*(4), 9-30. https://doi.org/10.1080/07421222.2003.11045748

Demertzis, K., & Iliadis, L. (2017). Computational intelligence anti-malware framework for android OS. *Vietnam Journal of Computer Science, 4*(4), 245-259. https://doi.org/10.1007/s40595-017-0095-3

Elangasinghe, M. A., Singhal, N., Dirks, K. N., & Salmond, J. A. (2014). Development of an ANN–based air pollution forecasting system with explicit knowledge through sensitivity analysis. *Atmospheric pollution research, 5*(4), 696-708. https://doi.org/10.5094/apr.2014.079

Emeka, B. O., & Liu, S. (2017). Security requirement engineering using structured object-oriented formal language for m-banking applications. In *Proceedings of the IEEE International Conference on Software Quality, Reliability and Security (QRS)*, (pp. 176-183). IEEE. https://doi.org/10.1109/qrs.2017.28

Fadlelmula, F. K., Cakiroglu, E., & Sungur, S. (2015). Developing a structural model on the relationship among motivational beliefs, self-regulated learning strategies, and achievement in mathematics. *International journal of science* *and mathematics education, 13*(6), 1355-1375. https://doi.org/10.1007/s10763-013-9499-4

Ferreira, P., Le, D. C., & Zincir-Heywood, N. (2019). Exploring feature normalization and temporal information for machine learning based insider threat detection. In *2019 15th International Conference on Network and Service Management (CNSM)*, (pp. 1-7). IEEE. https://doi.org/10.23919/cnsm46954.2019.9012708

Fishbein, M., Ajzen, I., Albarracin, D., & Hornik, R. (2007). A reasoned action approach: Some issues, questions, and clarifications. *Prediction and change of health behavior:* Lawrence Erlbaum Associates, Inc.: Mahwah, NJ, YSA, 2007; pp. 281-295. https://doi.org/10.4324/9780203937082

Gezici, B., & Tarhan, A. K. (2022). Systematic literature review on software quality for AI-based software. *Empirical Software Engineering, 27*(3), 1-65. https://doi.org/10.1007/s10664-021-10105-2

Giovanis, A., Assimakopoulos, C., & Sarmaniotis, C. (2018). Adoption of mobile self-service retail banking technologies: The role of technology, social, channel and personal factors. *International Journal of Retail & Distribution Management, 47* (9), 894-914. https://doi.org/10.1108/ijrdm-05-2018-0089

Glavee-Geo, R., Shaikh, A. A., & Karjaluoto, H. (2017). Mobile banking services adoption in Pakistan: are there gender differences? *International Journal of bank marketing*, 35 (7), 1090-1114. https://doi.org/10.1108/ijbm-09-2015-0142

Gleckler, P. J., Taylor, K. E., & Doutriaux, C. (2008). Performance metrics for climate models. *Journal of Geophysical Research: Atmospheres, 113*(D6). https://doi.org/10.1029/2007jd008972

Gosselin, C., Isaksson, M., Marlow, K., & Laliberté, T. (2016). Workspace and sensitivity analysis of a novel nonredundant parallel SCARA robot featuring infinite tool rotation. *IEEE Robotics and Automation Letters, 1*(2), 776-783. https://doi.org/10.1109/lra.2016.2527064

Gupta, H. V., Kling, H., Yilmaz, K. K., & Martinez, G. F. (2009). Decomposition of the mean squared error and NSE performance criteria: Implications for improving hydrological modelling. *Journal of hydrology, 377*(1-2), 80-91. https://doi.org/10.1016/j.jhydrol.2009.08.003

Gupta, S., Yun, H., Xu, H., & Kim, H.-W. (2017). An exploratory study on mobile banking adoption in Indian metropolitan and urban areas: A scenario-based experiment. *Information Technology for Development, 23*(1), 127-152. https://doi.org/10.1080/02681102.2016.1233855

Ha, K.-H., Canedoli, A., Baur, A. W., & Bick, M. (2012). Mobile banking—insights on its increasing relevance and most common drivers of adoption. *Electronic Markets, 22*(4), 217-227. https://doi.org/10.1007/s12525-012-0107-1

Jebarajakirthy, C., & Shankar, A. (2021). Impact of online convenience on mobile banking adoption intention: A moderated mediation approach. *Journal of Retailing and Consumer Services, 58*, 102323. https://doi.org/10.1016/j.jretconser.2020.102323

Kamdjoug, J. R. K., Wamba-Taguimdje, S.-L., Wamba, S. F., & Kake, I. B. e. (2021). Determining factors and impacts of the intention to adopt mobile banking app in Cameroon: Case of SARA by afriland First Bank. *Journal of Retailing and Consumer Services, 61*, 102509. https://doi.org/10.1016/j.jretconser.2021.102509

Karim, N. A., Shukur, Z., & AL-banna, A. M. (2020). UIPA: User authentication method based on user interface preferences for account recovery process.

Journal of Information Security and Applications, 52, 102466. https://doi.org/10.1016/j.jisa.2020.102466

Kasiyanto, S. (2016). Security issues of new innovative payments and their regulatory challenges. In *Bitcoin and Mobile Payments* (pp. 145-179). Springer. https://doi.org/10.1057/978-1-137-57512-8_7

Kemal, A. A. (2019). Mobile banking in the government-to-person payment sector for financial inclusion in Pakistan. *Information Technology for Development, 25*(3), 475-502. https://doi.org/10.1080/02681102.2017.1422105

Khan, A. G., Lima, R. P., & Mahmud, M. S. (2021). Understanding the service quality and customer satisfaction of mobile banking in Bangladesh: Using a structural equation model. *Global Business Review, 22*(1), 85-100. https://doi.org/10.1177/0972150918795551

Khattak, S., Jan, S., Ahmad, I., Wadud, Z., & Khan, F. Q. (2021). An effective security assessment approach for Internet banking services via deep analysis of multimedia data. *Multimedia Systems, 27*(4), 733-751. https://doi.org/10.1007/s00530-020-00680-7

Kiljan, S., Vranken, H., & van Eekelen, M. (2018). Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems, 80*, 430-447. https://doi.org/10.1016/j.future.2016.05.024

Kumar, V., Lai, K.-K., Chang, Y.-H., Bhatt, P. C., & Su, F.-P. (2020). A structural analysis approach to identify technology innovation and evolution path: a case of m-payment technology ecosystem. *Journal of Knowledge Management*,25 (2), 477-499. https://doi.org/10.1108/jkm-01-2020-0080

Latchoumi, T., Ezhilarasi, T., & Balamurugan, K. (2019). Bio-inspired weighed quantum particle swarm optimization and smooth support vector machine ensembles for identification of abnormalities in medical data. *SN Applied Sciences, 1*(10), 1-10. https://doi.org/10.1007/s42452-019-1179-8

Laukkanen, T. (2016). Consumer adoption versus rejection decisions in seemingly similar service innovations: The case of the Internet and mobile banking. *Journal of Business Research, 69*(7), 2432-2439. https://doi.org/10.1016/j.jbusres.2016.01.013

Leitner-Hanetseder, S., Lehner, O. M., Eisl, C., & Forstenlechner, C. (2021). A profession in transition: actors, tasks and roles in AI-based accounting. *Journal of Applied Accounting Research*, *22*(3), 539-556. https://doi.org/10.1108/jaar-10-2020-0201

Lewis, J. R. (2006). Sample sizes for usability tests: mostly math, not magic. *interactions, 13*(6), 29-33. https://doi.org/10.1145/1167948.1167973

Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. U. (2020). Security analysis of IoT devices by using mobile computing: a systematic literature review. *IEEE Access, 8*, 120331-120350. https://doi.org/10.1109/access.2020.3006358

Linardatos, P., Papastefanopoulos, V., & Kotsiantis, S. (2020). Explainable ai: A review of machine learning interpretability methods. *Entropy, 23*(1), 18. https://doi.org/10.3390/e23010018

Lu, J., Song, E., Ghoneim, A., & Alrashoud, M. (2020). Machine learning for assisting cervical cancer diagnosis: An ensemble approach. *Future Generation Computer Systems, 106*, 199-205. https://doi.org/10.1016/j.future.2019.12.033

Lu, J., Wei, J., Yu, C.-S., & Liu, C. (2017). How do post-usage factors and espoused cultural values impact mobile payment continuation? *Behaviour & information technology, 36*(2), 140-164. https://doi.org/10.1080/0144929x.2016.1208773

Madisetty, S., & Desarkar, M. S. (2018). A neural network-based ensemble approach for spam detection in Twitter. *IEEE Transactions on Computational Social Systems, 5*(4), 973-984. https://doi.org/10.1109/tcss.2018.2878852

Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. *Computers in human behavior, 54*, 453-461. https://doi.org/10.1016/j.chb.2015.08.039

Malaquias, R. F., & Hwang, Y. (2019). Mobile banking use: A comparative study with Brazilian and US participants. *International Journal of Information Management, 44*, 132-140. https://doi.org/10.1016/j.ijinfomgt.2018.10.004

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics, 10*(10), 2823-2836. https://doi.org/10.1007/s13042-018-00906-1

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society, 59*, 101151. https://doi.org/10.1016/j.techsoc.2019.101151

Mohammed, Y. B., & Karagozlu, D. (2021). A Review of Human-Computer Interaction Design Approaches towards Information Systems Development. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 12*(1), 229-250. https://doi.org/10.18662/brain/12.1/180

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International journal of surgery (London, England), 8*(5), 336-341. https://doi.org/10.1016/j.ijsu.2010.02.007

Montazemi, A. R., & Qahri-Saremi, H. (2015). Factors affecting adoption of online banking: A meta-analytic structural equation modeling study. *Information & management, 52*(2), 210-226. https://doi.org/10.1016/j.im.2014.11.002

Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of Cloud Computing, 4*(1), 1-23. https://doi.org/10.1186/s13677-015-0046-4

Nguyen, O. T. (2020). Factors affecting the intention to use digital banking in Vietnam. *The Journal of Asian Finance, Economics and Business, 7*(3), 303-310. https://doi.org/10.13106/jafeb.2020.vol7.no3.303

Ning, C., & You, F. (2019). Optimization under uncertainty in the era of big data and deep learning: When machine learning meets mathematical programming. *Computers & Chemical Engineering, 125*, 434-448. https://doi.org/10.1016/j.compchemeng.2019.03.034

Nourani, V., Behfar, N., Uzelaltinbulat, S., & Sadikoglu, F. (2020). Spatiotemporal precipitation modeling by artificial intelligence-based ensemble approach. *Environmental Earth Sciences, 79*(1), 1-20. https://doi.org/10.1007/s12665-019-8755-5

Nourani, V., Gökçekuş, H., & Umar, I. K. (2020). Artificial intelligence based ensemble model for prediction of vehicular traffic noise. *Environmental research, 180*, 108852. https://doi.org/10.1016/j.envres.2019.108852

Ofori, M., & El-Gayar, O. (2021). Drivers and challenges of precision agriculture: a social media perspective. *Precision Agriculture, 22*(3), 1019-1044. https://doi.org/10.1007/s11119-020-09760-0

Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems, 106*, 1-14. https://doi.org/10.1016/j.dss.2017.11.003

Osisanwo, F., Akinsola, J., Awodele, O., Hinmikaiye, J., Olakanmi, O., & Akinjobi, J. (2017). Supervised machine learning algorithms: classification and comparison. *International Journal of Computer Trends and Technology (IJCTT), 48*(3), 128-138. https://doi.org/10.14445/22312803/ijctt-v48p126

Otchere, D. A., Ganat, T. O. A., Gholami, R., & Ridha, S. (2021). Application of supervised machine learning paradigms in the prediction of petroleum reservoir properties: Comparative analysis of ANN and SVM models. *Journal of Petroleum Science and Engineering, 200*, 108182. https://doi.org/10.1016/j.petrol.2020.108182

Parker, F., Ophoff, J., Van Belle, J.-P., & Karia, R. (2015). Security awareness and adoption of security controls by smartphone users. In *Proceedingss of the Second International Conference on Information Security and Cyber Forensics (InfoSec),* (pp. 99-104). IEEE. https://doi.org/10.1109/infosec.2015.7435513

Parveen, N., Zaidi, S., & Danish, M. (2020). Comparative analysis for the prediction of boiling heat transfer coefficient of R134a in micro/mini channels using artificial intelligence (AI)-based techniques. *International Journal of Modelling and Simulation, 40*(2), 114-129. https://doi.org/10.1080/02286203.2018.1564809

Petropoulos, A., Siakoulis, V., Stavroulakis, E., & Vlachogiannakis, N. E. (2020). Predicting bank insolvencies using machine learning techniques. *International Journal of Forecasting, 36*(3), 1092-1113. https://doi.org/10.1016/j.ijforecast.2019.11.005

Pham, B. T., Nguyen, M. D., Van Dao, D., Prakash, I., Ly, H.-B., Le, T.-T., Ho, L. S., Nguyen, K. T., Ngo, T. Q., & Hoang, V. (2019). Development of artificial intelligence models for the prediction of Compression Coefficient of soil: An application of Monte Carlo sensitivity analysis. *Science of The Total Environment, 679*, 172-184. https://doi.org/10.1016/j.scitotenv.2019.05.061

Pourghasemi, H. R., & Rahmati, O. (2018). Prediction of the landslide susceptibility: Which algorithm, which precision? *Catena, 162*, 177-192. https://doi.org/10.1016/j.catena.2017.11.022

Qasim, H., & Abu-Shanab, E. (2016). Drivers of mobile payment acceptance: The impact of network externalities. *Information Systems Frontiers, 18*(5), 1021-1034. https://doi.org/10.1007/s10796-015-9598-6

Rabaa'i, A. A., & AlMaati, S. (2021). Exploring the determinants of users' continuance intention to use mobile banking services in Kuwait: Extending the expectation-confirmation model. *Asia Pacific Journal of Information Systems, 31*(2), 141-184. https://doi.org/10.14329/apjis.2021.31.2.141

Ranković, V., Radulović, J., Radojević, I., Ostojić, A., & Čomić, L. (2010). Neural network modeling of dissolved oxygen in the Gruža reservoir, Serbia. *Ecological Modelling, 221*(8), 1239-1244. https://doi.org/10.1016/j.ecolmodel.2009.12.023

Ratner, B. (2009). The correlation coefficient: Its values range between+ 1/− 1, or do they? *Journal of targeting, measurement and analysis for marketing, 17*(2), 139-142. https://doi.org/10.1057/jt.2009.5

Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020). Machine learning and deep learning techniques for cybersecurity: a review. In *The 2020 International Conference on Artificial Intelligence and Computer Vision,* (pp. 50-57). Springer, Cham. https://doi.org/10.1007/978-3-030-44289-7_5

Schapire, R. E. (2003). The boosting approach to machine learning: An overview. *Nonlinear estimation and classification*, 149-171. https://doi.org/10.1007/978-0-387-21579-2_9

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and informatics, 32*(1), 129-142. https://doi.org/10.1016/j.tele.2014.05.003

Shaikh, A. A., Karjaluoto, H., & Chinje, N. B. (2015). Continuous mobile banking usage and relationship commitment–A multi-country assessment. *Journal of Financial Services Marketing, 20*(3), 208-219. https://doi.org/10.1057/fsm.2015.14

Sharma, S. K. (2019). Integrating cognitive antecedents into TAM to explain mobile banking behavioral intention: A SEM-neural network modeling. *Information Systems Frontiers, 21*(4), 815-827. https://doi.org/10.1007/s10796-017-9775-x

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. *International Journal of Information Management, 44*, 65-75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

Singh, D., & Singh, B. (2020). Investigating the impact of data normalization on classification performance. *Applied Soft Computing, 97*, 105524. https://doi.org/10.1016/j.asoc.2019.105524

Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. *Computers & Security, 95*, 101745. https://doi.org/10.1016/j.cose.2020.101745

Smith, J. R., & McSweeney, A. (2007). Charitable giving: The effectiveness of a revised theory of planned behaviour model in predicting donating intentions and behaviour. *Journal of Community & Applied Social Psychology, 17*(5), 363-386. https://doi.org/10.1002/casp.906

Soviany, S., Săndulescu, V., & Puşcoci, S. (2016). A multimodal biometric identification method for mobile applications security. In *2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, (pp. 1-6). IEEE. https://doi.org/10.1109/ecai.2016.7861102

Szumski, O. (2020). Digital payment methods within Polish students-leading decision characteristics. *Procedia Computer Science, 176*, 3456-3465. https://doi.org/10.1016/j.procs.2020.09.051

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*(6), 1273-1296. https://doi.org/10.1007/s11165-016-9602-2

Tandon, U., Kiran, R., & Sah, A. N. (2018). The influence of website functionality, drivers and perceived risk on customer satisfaction in online shopping: an emerging economy case. *Information Systems and e-Business Management, 16*(1), 57-91. https://doi.org/10.1007/s10257-017-0341-3

Tavera-Mesias, J. F., van Klyton, A., & Zuñiga Collazos, A. (2021). Social Stratification, Self-Image Congruence, and Mobile Banking in Colombian Cities. *Journal of International Consumer Marketing*, 1-20. https://doi.org/10.1080/08961530.2021.1955426

Taylor, K. E. (2001). Summarizing multiple aspects of model performance in a single diagram. *Journal of Geophysical Research: Atmospheres, 106*(D7), 7183-7192. https://doi.org/10.1029/2000jd900719

Thomas, J., & Goudar, R. (2018). Multilevel Authentication using QR code based watermarking with mobile OTP and Hadamard transformation. In *Proceedings* *of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, (pp. 2421-2425). IEEE. https://doi.org/10.1109/icacci.2018.8554891

Tunkiel, A. T., Sui, D., & Wiktorski, T. (2020). Data-driven sensitivity analysis of complex machine learning models: A case study of directional drilling. *Journal of Petroleum Science and Engineering, 195*, 107630. https://doi.org/10.1016/j.petrol.2020.107630

Umar, I. K., Nourani, V., & Gökçekuş, H. (2021). A novel multi-model data-driven ensemble approach for the prediction of particulate matter concentration. *Environmental Science and Pollution Research, 28*(36), 49663-49677. https://doi.org/10.1007/s11356-021-14133-9

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157-178. https://doi.org/10.2307/41410412

Vishnuvardhan, B., Manjula, B., & Lakshman Naik, R. (2020). A study of digital banking: Security issues and challenges. In *Proceedings of the Third International Conference on Computational Intelligence and Informatics,* (pp. 163-185). Springer, Singapore. https://doi.org/10.1007/978-981-15-1480-7_14

Volaka, H. C., Alptekin, G., Basar, O. E., Isbilen, M., & Incel, O. D. (2019). Towards continuous authentication on mobile phones using deep learning models. *Procedia Computer Science, 155*, 177-184. https://doi.org/10.1016/j.procs.2019.08.027

Vom Lehn, F., Brosius, B., Broda, R., Cai, L., & Pitsch, H. (2020). Using machine learning with target-specific feature sets for structure-property relationship modeling of octane numbers and octane sensitivity. *Fuel, 281*, 118772. https://doi.org/10.1016/j.fuel.2020.118772

Wang, D., Zhang, X., Zhang, Z., & Wang, P. (2020). Understanding security failures of multi-factor authentication schemes for multi-server environments. *Computers & Security, 88*, 101619. https://doi.org/10.1016/j.cose.2019.101619

Wang, L., Kisi, O., Zounemat-Kermani, M., Salazar, G. A., Zhu, Z., & Gong, W. (2016). Solar radiation prediction using different techniques: model evaluation and comparison. *Renewable and Sustainable Energy Reviews, 61*, 384-397. https://doi.org/10.1016/j.rser.2016.04.024

Wang, X., Butt, A. H., Zhang, Q., Ahmad, H., & Shafique, M. N. (2021). Intention to Use AI-Powered Financial Investment Robo-Advisors in the M-Banking Sector of Pakistan. *Information Resources Management Journal (IRMJ), 34*(4), 1-27. https://doi.org/10.4018/irmj.2021100101

Wang, Y., Hahn, C., & Sutrave, K. (2016). Mobile payment security, threats, and challenges. In *Proceedings of the Second International Conference on Mobile and Secure Services (MobiSecServ),* (pp. 1-5). IEEE. https://doi.org/10.1109/mobisecserv.2016.7440226

Wei, Z., Wang, W., Bradfield, J., Li, J., Cardinale, C., Frackelton, E., Kim, C., Mentch, F., Van Steen, K., & Visscher, P. M. (2013). Large sample size, wide variant spectrum, and advanced machine-learning technique boost risk prediction for inflammatory bowel disease. *The American Journal of Human Genetics, 92*(6), 1008-1012. https://doi.org/10.1016/j.ajhg.2013.05.002

Welch, V., Petticrew, M., Petkovic, J., Moher, D., Waters, E., White, H., Tugwell, P., Atun, R., Awasthi, S., & Barbour, V. (2016). Extending the PRISMA statement to equity-focused systematic reviews (PRISMA-E 2012): explanation and elaboration. *Journal of Clinical Epidemiology, 70*, 68-89. https://doi.org/10.1016/j.jclinepi.2015.09.001

Wessels, L., & Drennan, J. (2010). An investigation of consumer acceptance of M-banking. *International Journal of bank marketing*, *28*(7), 547-568. https://doi.org/10.1108/02652321011085194

Williams, M. D. (2021). Social commerce and the mobile platform: Payment and security perceptions of potential users. *Computers in human behavior, 115*, 105557. https://doi.org/10.1016/j.chb.2018.06.005

Wu, H., & Leung, S.-O. (2017). Can Likert scales be treated as interval scales?—A Simulation study. *Journal of Social Service Research, 43*(4), 527-532. https://doi.org/10.1080/01488376.2017.1329775

Yang, I.-H., & Kim, K.-W. (2004). Prediction of the time of room air temperature descending for heating systems in buildings. *Building and Environment, 39*(1), 19-29. https://doi.org/10.1016/j.buildenv.2003.08.003

Yang, Q., Pang, C., Liu, L., Yen, D. C., & Tarn, J. M. (2015). Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. *Computers in human behavior, 50*, 9-24. https://doi.org/10.1016/j.chb.2015.03.058

Yang, Y., Li, S., Li, W., & Qu, M. (2018). Power load probability density forecasting using Gaussian process quantile regression. *Applied Energy, 213*, 499-509. https://doi.org/10.1016/j.apenergy.2017.11.035

Yin, H. S., & Vatrapu, R. (2017). A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In *Proceedings of the IEEE International Conference on Big Data (Big Data)*, (pp. 3690-3699). IEEE. https://doi.org/10.1109/bigdata.2017.8258365

Zainab, A., Syed, D., Ghrayeb, A., Abu-Rub, H., Refaat, S. S., Houchati, M., Bouhali, O., & Lopez, S. B. (2021). A multiprocessing-based sensitivity analysis of machine learning algorithms for load forecasting of electric power distribution system. *IEEE Access, 9*, 31684-31694. https://doi.org/10.1109/access.2021.3059730

Zefferer, T., & Teufl, P. (2013). Policy-based security assessment of mobile end-user devices an alternative to mobile device management solutions for Android smartphones. In *Proceedings International Conference on Security and Cryptography (SECRYPT)*, (pp. 1-8). IEEE. https://doi.org/10.5220/0004509903470354

Zhang, X., Kano, M., & Matsuzaki, S. (2019). A comparative study of deep and shallow predictive techniques for hot metal temperature prediction in blast furnace ironmaking. *Computers & Chemical Engineering, 130*, 106575. https://doi.org/10.1016/j.compchemeng.2019.106575

Zhao, L., Wang, Q., Wang, C., Li, Q., Shen, C., & Feng, B. (2021). Veriml: Enabling integrity assurances and fair payments for machine learning as a service. *IEEE Transactions on Parallel and Distributed Systems, 32*(10), 2524-2540. https://doi.org/10.1109/tpds.2021.3068195

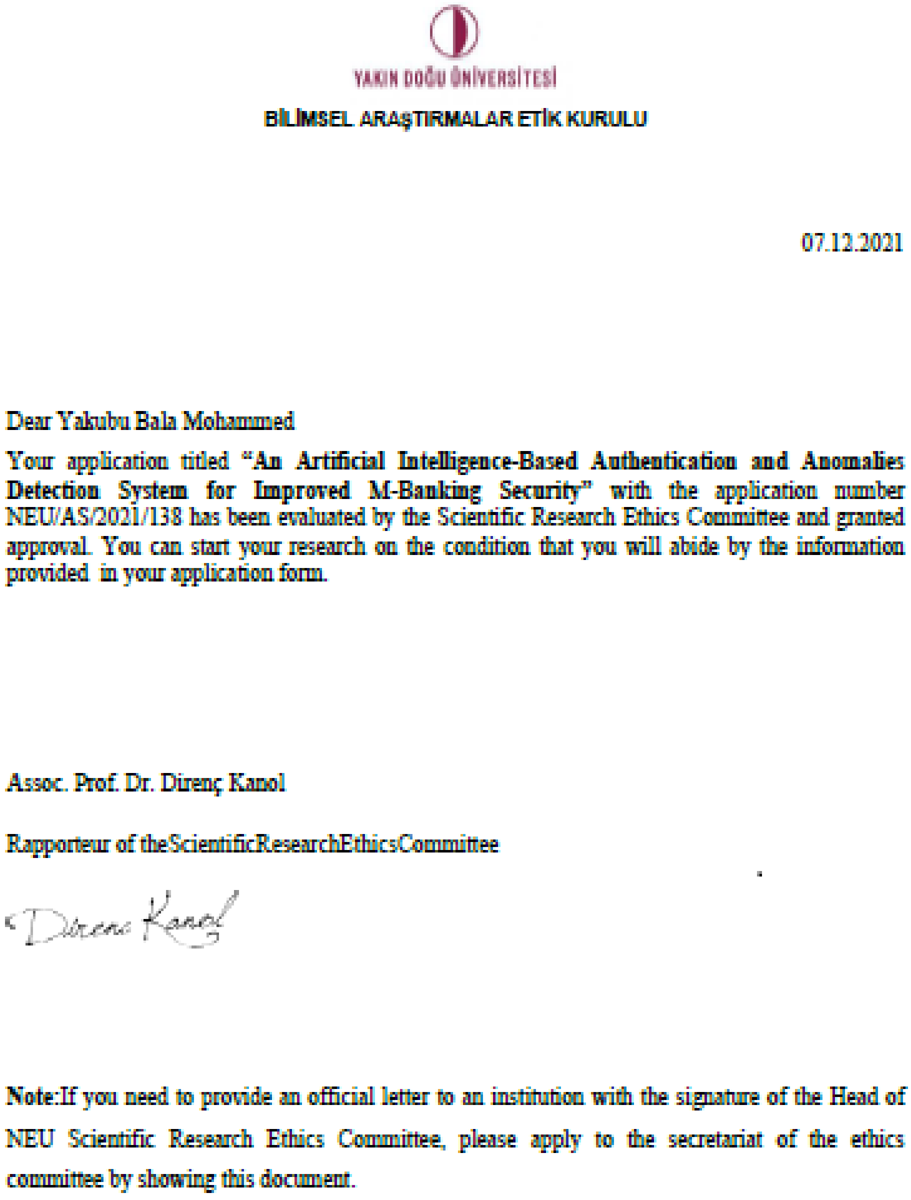
Zhou, Q., Lim, F. J., Yu, H., Xu, G., Ren, X., Liu, D., Wang, X., Mai, X., & Xu, H. (2021). A study on factors affecting service quality and loyalty intention in mobile banking. *Journal of Retailing and Consumer Services, 60*, 102424. https://doi.org/10.1016/j.jretconser.2020.102424

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password– A laboratory study on user perceptions of authentication schemes. *International*

Journal of Human-Computer Studies, 133, 26-44. https://doi.org/10.1016/j.ijhcs.2019.08.006

APPENDICES

Appendix A: Ethics Committee Permission



YAKIN DOĞU ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMALAR ETİK KURULU

07.12.2021

Dear Yakubu Bala Mohammed

Your application titled **"An Artificial Intelligence-Based Authentication and Anomalies Detection System for Improved M-Banking Security"** with the application number NEU/AS/2021/138 has been evaluated by the Scientific Research Ethics Committee and granted approval. You can start your research on the condition that you will abide by the information provided in your application form.

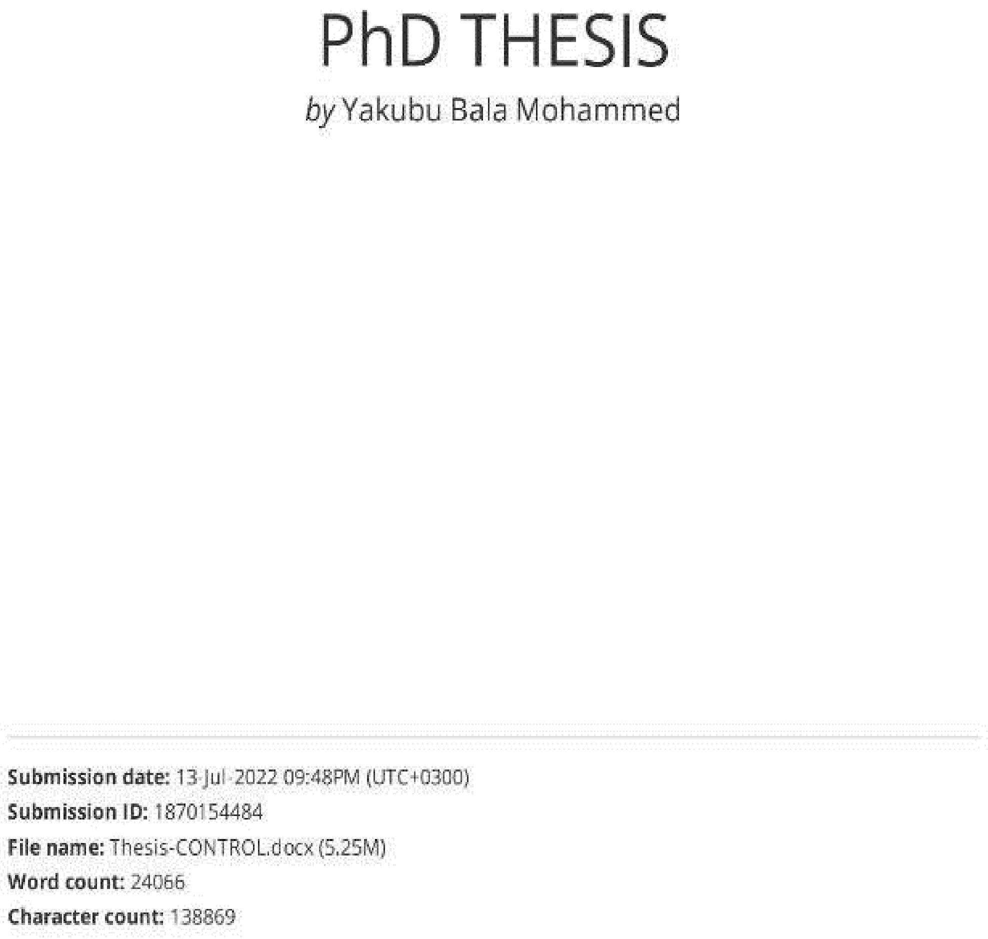
Assoc. Prof. Dr. Direnç Kanol

Rapporteur of theScientificResearchEthicsCommittee

Direnç Kanol

Note: If you need to provide an official letter to an institution with the signature of the Head of NEU Scientific Research Ethics Committee, please apply to the secretariat of the ethics committee by showing this document.

Appendix B: Turnitin Similarity Report



PhD THESIS

by Yakubu Bala Mohammed

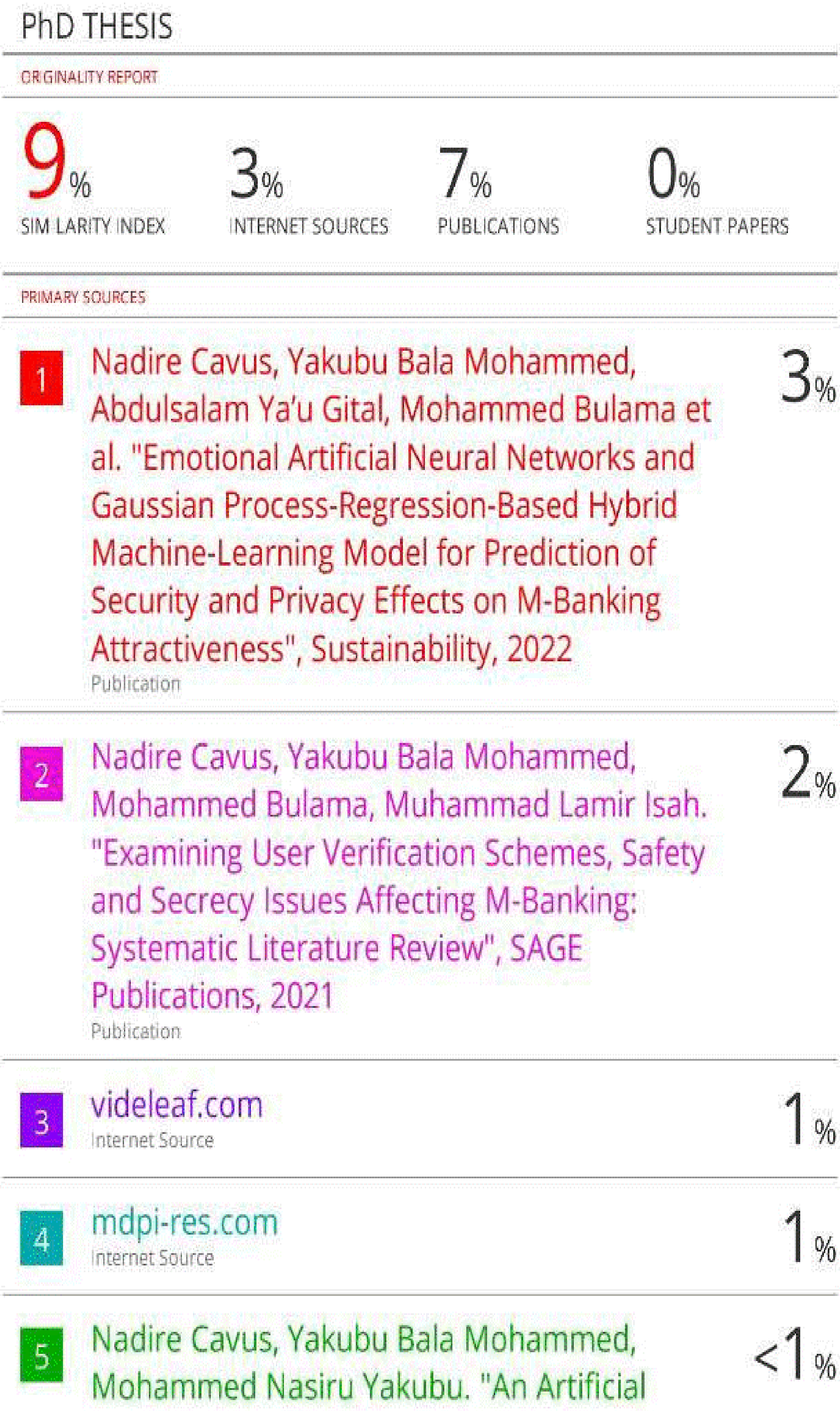
Submission date: 13-Jul-2022 09:48PM (UTC+0300)

Submission ID: 1870154484

File name: Thesis-CONTROL.docx (5.25M)

Word count: 24066

Character count: 138869



PhD THESIS

ORIGINALITY REPORT

9%	3%	7%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Nadire Cavus, Yakubu Bala Mohammed, Abdulsalam Ya'u Gital, Mohammed Bulama et al. "Emotional Artificial Neural Networks and Gaussian Process-Regression-Based Hybrid Machine-Learning Model for Prediction of Security and Privacy Effects on M-Banking Attractiveness", Sustainability, 2022 Publication	3%
2	Nadire Cavus, Yakubu Bala Mohammed, Mohammed Bulama, Muhammad Lamir Isah. "Examining User Verification Schemes, Safety and Secrecy Issues Affecting M-Banking: Systematic Literature Review", SAGE Publications, 2021 Publication	2%
3	videleaf.com Internet Source	1%
4	mdpi-res.com Internet Source	1%
5	Nadire Cavus, Yakubu Bala Mohammed, Mohammed Nasiru Yakubu. "An Artificial	<1%

Appendix C: Data Collection Tools

Section (A) – General Information

Kindly tick (√) the following answer concerning your demographic information.

1. Gender	( ) Male	( ) Female		
2. Age group	( ) 18 -25	( ) 26 - 35	( ) 36 and above	
3. Education level	( ) SSCE	( ) ND	( ) Barchelor/HND	( ) Masters or higher
4. Employment Status	( ) Academics	( ) Students	( ) Banking Staff	( ) Security expert
5. Nationality	( ) Nigeria	( ) Others		

Note: SSCE = Senior School Certificate; ND = National Diploma; HND = Higher National Diploma

Section (B) – Responses

Please use the following system link ***https://secure-authy.herokuapp.com/login****, and kindly tick (√) the response that best reflects your beliefs with respect to the developed user-authentication mobile apps for m-banking 1 to 5 Likert scale ranging from (1) strongly disagree, (2) disagree, (3) neutral, (4) agree and (5) strongly agree.* Using - (Usability Testing questions**)**

	Items	Sd	D	N	A	Sa
H_1	System Usability (Lewis, 2006)	1	2	3	4	5
SysUse1	Overall, I am satisfied with how easy it is to use this System					
SysUse2	It was simple to use this system					
SysUse3	I was able to complete the tasks and scenarios quickly using this system.					
SysUse4	I felt comfortable using this system.					
SysUse5	It was easy to learn to use this system.					
SysUse6	I believe I could be protected using this system.					
H_2	Information quality (Lewis, 2006)	1	2	3	4	5
InfoQual1	The system gave error messages that clearly told me how to fix problems.					
InfoQual2	Whenever I made a mistake using the system, I could recover easily and quickly.					

InfoQual3	The information (such as on-line help, on-screen messages and other documentation) provided with this system was clear.					
InfoQual4	It was easy to find the information I needed.					
InfoQual5	The information was effective in helping me complete the tasks and scenarios.					
InfoQual6	The organization of information on the system screens was clear.					
H_3	Interface quality (Lewis, 2006)	1	2	3	4	5
IntQual1	The interface of this system was pleasant.					
IntQual2	I liked using the interface of this system.					
IntQual3	This system has all the functions and capabilities I expect it to have.					
IntQual4	Overall, I am satisfied with this system.					
H_4	System Security (Authors of this study)	1	2	3	4	5
SysSq1	The security features of the system are pleasant to me					
SysSq2	Velocity anomalies during login can be handle by the system					
SysSq3	The authentication process provided in the system is more reliable, robust, and can help safeguard customers funds					
SysSq4	The system is capable of handling DDoS attacks					
SysSq5	In general, I am satisfied with the level of security provided in the systems					
H_5	System Privacy (Authors of this study)	1	2	3	4	5
SysPriv1	I fear that while I am paying a bill by mobile phone, I might make mistakes since the correctness of the inputted information is difficult to check from the screen					
SysPriv2	I fear that while I am using mobile banking services, the Government can inter-cept my personal information					
SysPriv3	I fear that while I am using mobile banking services, third parties can access my account or see my account information					
SysPriv4	I fear that the list of PIN codes may be lost and end up in the wrong hands					
SysPriv5	Generally, I fear that my personal information can be accessed through m-banking platform					

Appendix D: Curriculum Vitae CV

PERSONAL INFORMATION

Surname, Name: Yakubu Bala MOHAMMED

Nationality: Nigerian

Date and Place of Birth: 04 January, 1979, Bauchi-Nigeria

Marital Status: Married

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Universiti Teknologi Malaysia (UTM)	2015
B.Tech.	ATBU Department of Computer and Information Technology	2010

WORK EXPERIENCE

Year	Place	Enrollment
2020 - Present	Computer Information Systems Research and Technology Center (CISRTC).	Researcher
2011 – Present	Tatari Ali Polytechnic, Bauchi.	Lecturer I
2007 – 2011	Bauchi State Ministry Education, Nigeria.	Higher Instructor
2004 – 2007	Bauchi State Board of Internal Revenue, Nigeria.	Data Processing Officer

LANGUAGES

- Hausa and English.

MEMBERSHIP OF PROFESSIONAL ORGANISATIONS

- *Member*, Nigerian Computer Society of (NCS), Nigeria.
- *Member,* Computer Professionals (Registration Council of Nigeria) CPN, Nigeria.

PUBLICATIONS IN INTERNATIONAL REFEREED JOURNALS (IN COVERAGE OF SCI/SCIE/SSCI)

- Cavus, N., **Mohammed, Y. B.,** & Yakubu, M. N. (2022). Emotional Artificial Neural Networks and Guassian Process Regression-Based Hybrid Machine Learning Model for Prediction of Security and Privacy Effects on M-Banking Attractiveness. *Sustainability, 14*, 5826. **(Q1).**
- Cavus, N., **Mohammed, Y. B.,** Bulama, M., & Isah, M. L. (2022). Examining User Verification Schemes, Safety and Secrecy Issues Affecting M-Banking: Systematic Literature Review. *Sage Open, 12*(2), 211-220. **(Q2).**
- Cavus, N., **Mohammed, Y. B**., & Yakubu, M. N. (2021). An Artificial Intelligence-Based Model for Prediction of Parameters Affecting Sustainable Growth of Mobile Banking Apps. *Sustainability, 13*(11), 6206. **(Q1)**.
- Cavus, N., **Mohammed, Y. B.,** & Yakubu, M. N. (2021). Determinants of Learning Management Systems during COVID-19 Pandemic for Sustainable Education. *Sustainability, 13*(9), 5189. **(Q1).**
- **Mohammed, Y. B.,** Nourani, V., Hassan, A., & Mohammed, B. (2020). Analyzing & Modelling Energy Consumption Logs. *Soft Computing Research, 9*(1), 1-9. **(Q1).**

PUBLICATIONS IN INTERNATIONAL REFEREED JOURNALS (IN COVERAGE OF ESCI)

- **Mohammed, Y. B.,** & Karagozlu, D. (2021). A Review of Human-Computer Interaction Design Approaches towards Information Systems Development. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 12*(1), 229-250.
- **Mohammed, Y. B.,** & Ozdamli, F. (2021). Motivational Effects of Gamification Apps in Education: A Systematic Literature Review. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 12*(2), 122-138.
- Mohammed, B., **Mohammed, B. Y**. M. A. H., & Isah, L. (2020). Holistic Approach to Mobile Cash Transaction. *International Journal of Computing, 9*(3), 16-22.

PAPERS PUBLISHED IN OTHER INTERNATIONAL INDEXED JOURNALS

- Hassan, A., **Yakubu, M. B., Bulama,** M., & Shitu, A. A. (2018). A customer perspective on infrastructure & legislative effects to use mobile banking app in Nigeria. *Global Journal of Information Technology: Emerging Technologies, 8*(3), 102-113.
- **Yakubu, M. B.,** DanAzumi, H., Bulama, M., & Hassan, A. (2019). Intrusion tolerance model against higher institution database. *Global Journal of Information Technology: Emerging Technologies, 9*(1), 20-28.
- **Yakubu, M. B.,** Hassan, A., Ahmad, A., Musa, K. I., & Gital, A. (2018). Mobile learning stimulus in Nigeria. *Global Journal of Information Technology: Emerging Technologies, 8*(3), 95-101.

BOOK AND BOOK CHAPTER PUBLISHED

- Cavus, N., **Mohammed, Y. B.,** & Yakubu, M. N. (2021). AI-Based Models for Prediction of Parameters Affecting Sustainable Growth of Mobile Banking Apps. *Resource Management and Sustainable Development. 114523.*

THESIS

Master

- Yakubu, M. B., (2014). *Reputation and Credit-Based Incentives Mechanism for Data-Centric Message Delivery in M-Payment Systems.* Unpublished Master Thesis, Universiti Teknologi Malaysia (UTM), Department of Information Systems, Faculty of Computing.

Undergraduate Project

- Yakubu, M. B., (2010). *Computer-Based Network Security and Firewalls in Banking Sector. (A case Study of Guaranty Trust Bank).* Unpublished Undergraduate project (B.Tech.), Abubakar Tafawa Balewa University, Bauchi, Department of Information Technology, Faculty of Management Sciences,

UNDERTAKING PROJECTS

- Networking and Installation of Computer Based Test (CBT) Centres in Abubakar Tatari Ali Polytechnic, Bauchi. 2016.
- Design and Implementation of An Online Campus Car Hiring Service, for Universiti Teknologi Malaysia (UTM), Students and Gues – 2014.
- Design and Implementation of Abubakar Tatari Ali Polytechnic, Bauchi Students Portal. 2018.

SPORTS

- Football, Basketball.

HOBBIES

- Reading, Research, Movies.