Article

Not peer-reviewed version

Sectrabank Model to Mitigate Computer Fraud in Electronic Operations through Banking Applications on Android Devices

Jhon Melendez *, Jomark Noriega *, Jose Tiznado *, Paulo Calderon *, Yordy Benites *, Luis Rivera *, Jose Herrera *, Jorge Mayhuasca *

Posted Date: 3 April 2024

doi: 10.20944/preprints202404.0238.v1

Keywords: fake app; SIM swapping; cybercrime; computer fraud; security; authentication

Article

Sectrabank Model to Mitigate Computer Fraud in Electronic Operations through Banking Applications on Android Devices

Jhon Melendez [1,*,†], Jomark Noriega [1,†] Jose Tiznado [1,†] Paulo Calderón [1,†] Yordy Benites [1,†] Luis Rivera [1,2,†] José Herrera [1,3,†] and Jorge Mayhuasca [1,†]

[1] Universidad Nacional Mayor de San Marcos. Universidad del Perú. Decana de América. Lima, post code: 15081, Perú; jomark.noriega@unmsm.edu.pe (J.N.); jose.tiznado@unmsm.edu.pe (J.T.); paulocesar.calderon@unmsm.edu.pe (P.C.); yordy.benites@unmsm.edu.pe (Y.B.); lriverae@unmsm.edu.pe (L.R.); jherreraqu@unmsm.edu.pe (J.H.); jmayhuascag@unmsm.edu.pe (J.M.)

[2] Universidade Estadual do Norte Fluminense Darcy Ribeiro; Campos dos Goytacazes, post code: 28013-602, Brasil

[3] Universidad Pablo de Olavide; Sevilla, post code: 41013, España

* Correspondence: jhon.melendez@unmsm.edu.pe

† These authors contributed equally to this work.

Abstract: This research aims to introduce a model, SectraBank, designed to mitigate cyber fraud attacks, specifically targeting SIM Swapping and Fake App schemes in mobile banking users. A quantitative methodology with an experimental design was meticulously employed to examine the rise of cyber fraud within mobile banking. The study involved a sample of 100 professionals with advanced knowledge in Information and Communication Technologies (ICTs). Surveys were utilized to measure awareness of threats and perceptions of security before and after the implementation of the proposed model. SectraBank leverages unique user identifiers such as fingerprint authentication and the International Mobile Equipment Identity (IMEI) number, in addition to geolocation and One Time Passwords (OTP) for validating electronic transactions in mobile banking. The effectiveness of the proposed model was notable, achieving a 96.1% efficacy rate in mitigating Fake App attacks and a 90.2% success rate in countering SIM Swapping attacks. These findings underscore the potential of SectraBank as a robust solution to enhance cybersecurity measures in the realm of mobile banking.

Keywords: Fake App; SIM swapping; cybercrime; computer fraud; security; authentication

1. Introduction

While studies on cybercrime exist in other countries, there is a lack of research specifically focused on developing models for mitigating Computer Fraud against Subscriber Identify Module (SIM) swapping and fake apps, as can be evidenced by SMSPROTECT the proposed model in Nigeria [1], which consists of an application to combat smishing using machine learning. Similarly, the model SMISHING DETECTOR [2] focused on the detection of smishing using machine learning, and the model in Turkey suggests a real-time system to detect and stop phishing [3]. The aforementioned models, selected as references from the models studied, only mitigate phishing and its variants but do not focus on mitigating SIM swapping and fakeapp.

 doi:10.20944/preprints202404.0238.v1

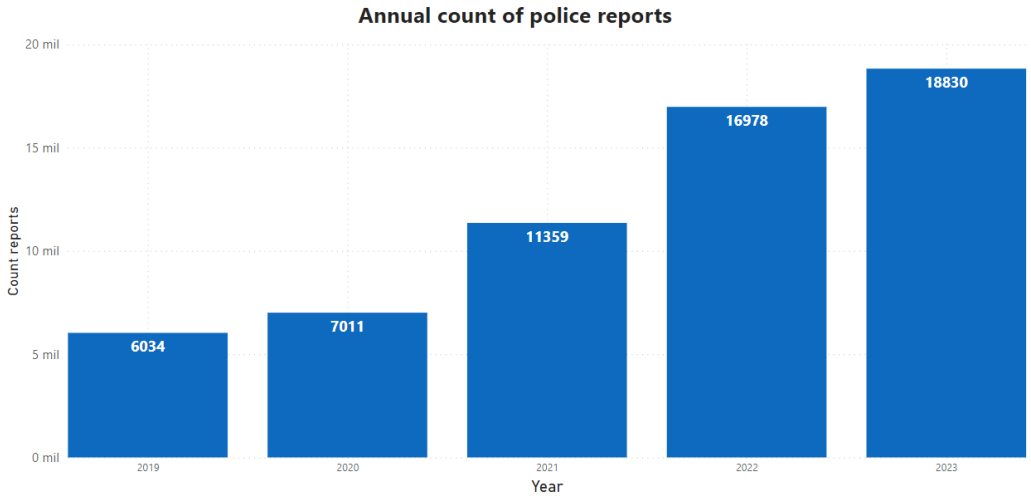


Figure 1. Bar graph showing the number of complaints in the last 5 years according to the Criminal Investigation Complaint Registration System in Peru.

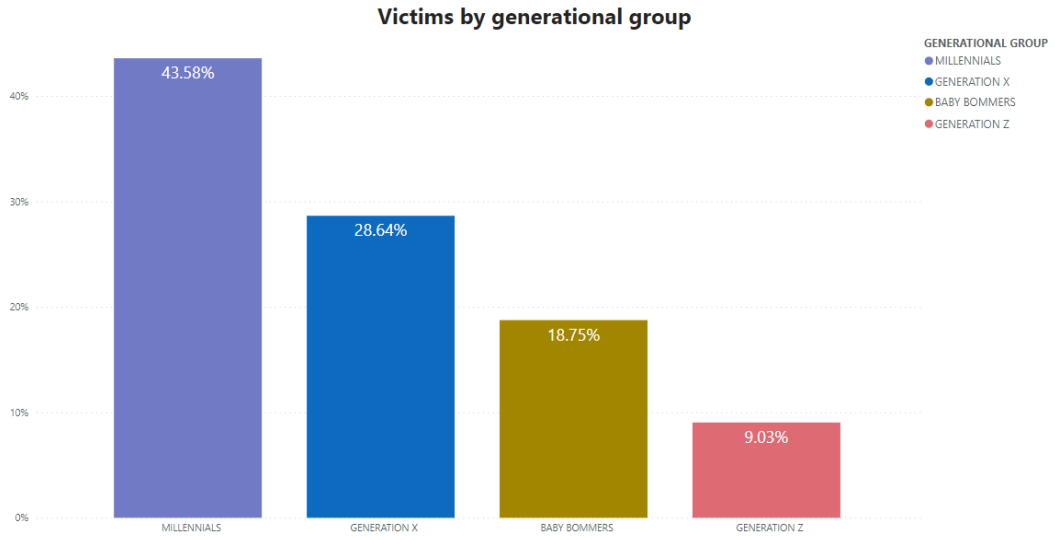


Figure 2. Bar graph showing the segmentation of victims according to their generational group in Peru.

This study proposes the SectraBank model to enhance security in electronic banking operations, specifically against SIM swapping and fake apps attacks. This innovative model utilizes the IMEI, fingerprint, and geolocation as preventive measures to mitigate vulnerabilities in transactions carried out via mobile applications. SectraBank aims to strengthen trust and security in digital banking operations, employing a layered security system to protect users from SIM swapping and fake app attacks [4].

 doi:10.20944/preprints202404.0238.v1

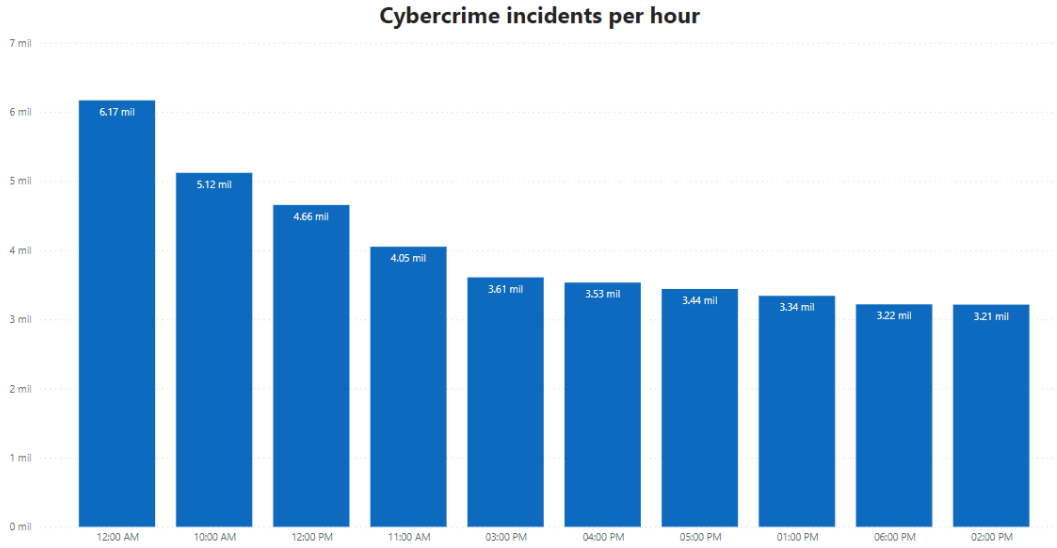


Figure 3. Time of highest incidence of cybercrime in Peru.

It is crucial to acknowledge that mobile systems face challenges regarding the lack of precise, real-time user signature verification systems robust against distortions and forgery attacks to secure electronic transactions on mobile devices [5]. One of the primary concerns is the lack of security in mobile commerce applications, as payments are conducted online via mobile devices. Despite meeting basic security requirements, the LPMP protocol exhibits several flaws: a) It requires the use of multiple secret keys between the client and issuer, necessitating synchronization and memory space. b) It allows the sending of certificates by unauthorized users. c) It lacks anonymity and transaction unlinkability. d) It is vulnerable to replay attacks by merchants [6].

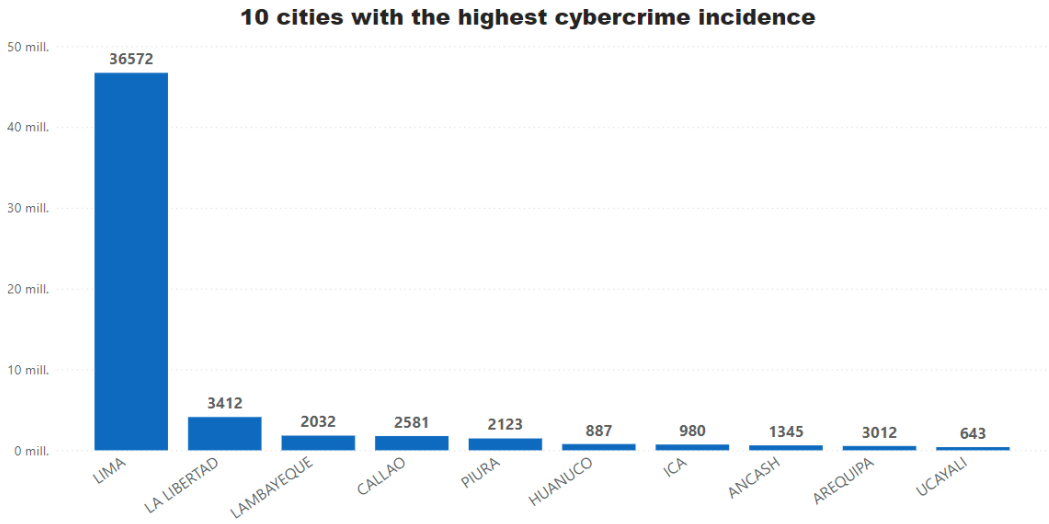


Figure 4. Peruvian cities with the highest incidences of cybercrime.

The continuous growth of electronic banking (E-Banking) and mobile banking (M-Banking) is driven by increased internet speed on mobile devices and banking apps, yet these services exhibit security deficiencies in various aspects, including wireless networks, exposing them to diverse types of attacks [7].

 doi:10.20944/preprints202404.0238.v1

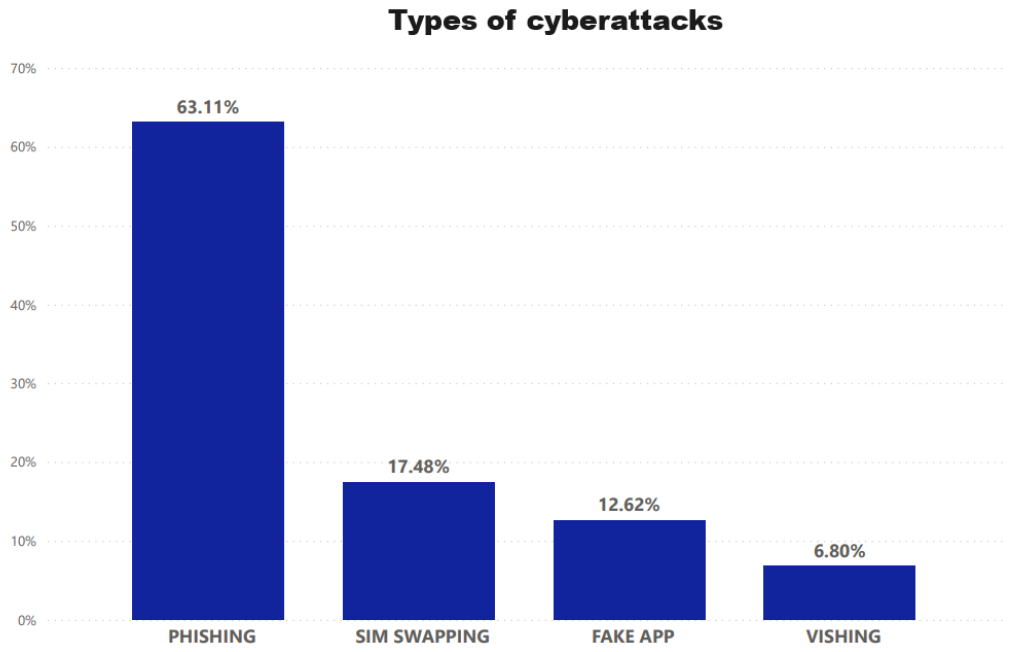


Figure 5. Bar graph showing the segmentation of attacks by modality, according to the complaint registry of the High Technology Crime Investigation Division.

2. State of Art

In a study conducted in Turkey, researchers addressed the emerging issue of "Fake App" malware, particularly a type known as TrickBot. This modular malware is capable of stealing data, executing phishing attacks, and controlling infected devices. The team developed a machine learning model to identify network traffic associated with TrickBot. Using a quantitative approach and an experimental design, the study focused on collecting network traffic data, analyzing over 300 real TrickBot samples over a nine-month period. Algorithms such as Random Forest, Neural Networks, and Logistic Regression were used, finding that Random Forest offered the best performance with a precision of 99.95% and a true detection rate of 91.7%. This detection model is focused on analyzing network behavior to mitigate the impact of this type of banking malware [8].

Separately, in India, the issue of smishing, a phishing variant that uses SMS messages to deceive victims, was addressed. A security model called "Smishing Detector" was developed, which detects smishing by analyzing SMS content and Uniform Resource Locator (URL) behavior. With a quantitative and experimental approach, 5,858 messages, including both smishing and legitimate messages, were analyzed using the Naive Bayes algorithm for text classification. The model achieved high precision in detecting smishing messages, demonstrating its potential to mitigate banking fraud by identifying and blocking fraudulent messages [2].

In South Korea, an article was published on preventing telephone fraud using SIM boxes, based on the unique fingerprints of cellular device models. Employing a quantitative and experimental methodological design, the study focused on control messages from various devices. Analysis of 279 traces from 102 devices, including 85 smartphone models and 6 SIM boxes, utilized control messages like ATTACH Request and UECapabilityInformation. The results revealed that most smartphones possess unique fingerprints, and SIM boxes are clearly distinguishable. The developed system proved capable of effectively preventing most frauds associated with SIM boxes. These findings suggest that cellular device capability information can efficiently be used to prevent fraud in the telecommunications field [9].

 doi:10.20944/preprints202404.0238.v1

Researchers in Malaysia analyzed trends and mapping between criminology and cybercrime in Malaysia from 2008-2020. The unit of analysis was the cybercrime reports from Malaysia's computer emergency response team (MyCERT). The research, conducted from a quantitative approach with a non-experimental, cross-sectional descriptive design, used statistical analysis techniques to examine 109,034 reported cases. The results found an increase in cyberattacks, particularly frauds and malicious codes. In response, the authors propose an authentication and authorization model to protect critical applications as a mitigation measure. This study provides valuable understanding of cybercrime trends and possible technical strategies to combat banking fraud through robust authentication mechanisms [10].

A recent investigation in Canada addressed the analysis of the Fake App ANUBIS attack method, using a significant dataset comprising APT activities executed by a specialized team. This set was chosen for its relevance in renowned APT attacks. The study focused on using Bayesian neural networks for learning and function estimation, highlighting the system's ability to identify uncertainties in predictions and its high effectiveness in cyber threat detection, underscoring its value in corporate cyber defense [11].

Researchers in Indonesia focused on ANUBIS banking malware, specifically its impact on Android devices. Their study showed an increase in variants of banking trojans. ANUBIS, disguised in seemingly legitimate applications, revealed to be a significant threat once installed on devices. Through a controlled mobile security environment, the malware's behavior was simulated and analyzed, showing how it could access and operate discreetly. This quantitative analysis provided a detailed insight into the malware's capabilities, contributing to knowledge on Android device security and the importance of caution when downloading applications [12].

A team in Nigeria developed an innovative mobile application aimed at combating smishing attacks through SMS. They implemented an experimental design, analyzing thousands of SMS messages with advanced machine learning models. The application, developed in a popular programming language and supported by an API, was designed to intercept and evaluate SMS, providing alerts to users. The results showed high precision in spam identification, demonstrating the feasibility and effectiveness of this solution for preventing smishing on mobile devices [1]..

In a study conducted in China, researchers investigated vulnerabilities in biometric authentication systems on smartphones, focusing on an innovative method to compromise fingerprint authentication. The approach included the use of adversarial technology to manipulate the authentication process by exploiting system weaknesses. Although the method proved effective across several smartphone models, the study did not cover large-scale testing or fully explore implications on user privacy and payment applications, also assuming the need for physical access to conduct the attack [13].

This article proposes a precise, real-time, and forgery-resistant system to secure electronic transactions on mobile devices through effective user signature verification. One proposal comes from researchers studying mobile commerce, where they analyze protocols to identify specific security flaws and propose a fortified version that addresses the mitigations for the LPMP protocol's issues. An improved version of LPMP that is: a) more secure, b) more efficient in memory usage, c) resolves current version failures is proposed [6].

A study in Indian banks aimed to examine the continuous growth of electronic (E-Banking) and mobile banking (M-Banking) due to the increase in internet speed in relation to mobile devices and banking apps, showing security deficiencies in various aspects, including wireless networks in these M-Banking services, exposed to various types of attacks. They propose the implementation of multi-factor authentication to access applications and validate transactions. This would improve user identification, generating end-to-end encryption to protect confidential data and financial transactions using methods such as Secure Sockets Layer (SSL), Hyper Text Transfer Protocol Secure (HTTPS), or Transport Layer Security (TLS). Another method is to analyze malware threats in real-time on apps and mobile devices to identify attacks and protect the user. Also, maintain security control when making high-amount transfers with digital or biometric tokens, with the adoption of technical controls and

 doi:10.20944/preprints202404.0238.v1

policies aimed at improving security would reduce the risks associated with using M-Banking services to perform electronic financial transactions through mobile devices [7].

Banking applications, despite being virtual entities, constitute an essential part of the Internet of Things (IoT). Through digital interconnection, these applications establish a dynamic network by connecting with banking systems, servers, and online platforms to facilitate a wide range of financial services. In a study developed in China, a new method based on multidimensional similarity to detect fake IoT applications and mitigate the threats they pose was proposed, using IoT applications collected from different application markets. The research had an experimental methodological design, utilizing a reference dataset with 1,497 pairs of counterfeit and wild samples with 1,206 samples from 49 malware families. The main techniques were cryptographic hash-based similarity (TLSH) and application resource similarity techniques based on Minhash. The results showed an accuracy higher than 99.31% on the reference dataset and 97.43% on the wild set. It was concluded that multidimensional similarity is effective in detecting counterfeit IoT applications that pose a threat to the IoT ecosystem [14].

In Tanzania, a group of researchers looked at the issue of smishing and developed a machine learning algorithm to classify legitimate messages from Smishing messages (SMS phishing) targeting mobile money users. To train the model, they used legitimate SMS messages and Smishing messages in Swahili collected from mobile network operators and university students in Tanzania. The sample size was 31,962 legitimate messages and 302 unique Smishing messages. The research had a quantitative approach, with an experimental design, and they used supervised machine learning techniques like feature selection with the Extratree classifier and machine learning classifiers (Random Forest, Multinomial Naive Bayes, etc.). The hybrid model of feature selection with Extratree and Random Forest classifier using TFIDF vectorization achieved the best accuracy of 99.86%. It was compared with a baseline Multinomial Naive Bayes model. The proposed model had the lowest rate of false positives (2 Smishing messages that were classified as legitimate) and false negatives (4 legitimate messages that were incorrectly classified as Smishing), with a Log-Loss of 0.04 [15].

In research conducted in Indonesia, a solution was proposed to protect users of mobile financial applications from account takeover attacks by utilizing mobile network infrastructure. The study consists of using the mobile network infrastructure to add an additional factor of authentication and verify that the telephone number used for registration or login in the financial application matches the number installed on the mobile device. This aims to prevent cybercriminals from taking control of a mobile financial account even if they have obtained access credentials (username and password) through social engineering, phishing, or other methods. The research had a quantitative experimental approach and conducted 4 test scenarios with 10 attempts each in the processes of registration and login in the mobile app, for this they made a prototype of an Android mobile financial application integrated with a mobile network verification server through API, resulting in that the 4 test scenarios were successful 100% as expected. Registration and login could only be carried out when the telephone number matched between the device and the application [16].

In a study conducted in Saudi Arabia, a group of researchers proposed a phishing detection model based on Generative Adversarial Networks (GANs) that relies solely on website URLs to enhance performance. They analyzed both phishing and legitimate website URLs, with a sample size comprising 1,167,201 phishing URLs and 1,140,599 legitimate URLs gathered from PhishTank and DomCop. The research adopted a quantitative approach and experimental design, utilizing GAN neural networks. They employed a Long Short-Term Memory (LSTM) network as a generator for synthetic phishing URLs and a Convolutional Neural Network (CNN) as a discriminator for classifying URLs. The results showed that the proposed GAN model, named PDGAN, achieved a detection precision of 97.58% and an accuracy of 98.02%, outperforming state-of-the-art models by analyzing only the website URLs, without relying on third-party services [17].

In the United Kingdom, researchers explored the feasibility of using clustering to group phishing emails into significant campaigns, aiming to reduce the effort required by IT personnel to mitigate

 doi:10.20944/preprints202404.0238.v1

phishing. They analyzed 781,740 emails reported as phishing, distributed across two datasets of approximately 60,000 emails each over six-month periods. The study utilized a quantitative approach and employed clustering algorithms such as MeanShift and DBSCAN, along with seven sets of email features. The MeanShift algorithm, using email source and URL features, successfully clustered approximately 60,000 emails into fewer than 6,000 relatively homogeneous clusters with high expert agreement (precision 0.82, recall 0.57, F1 0.68), suggesting that unsupervised clustering is a promising technique for the automated identification of phishing campaigns based on user reports [18].

In China, researchers proposed an unsupervised feature learning algorithm called SPWalk to improve the detection of phishing web pages. They analyzed 78,368 malicious and 761,688 legitimate web page nodes from a network built by the authors, totaling 840,056 nodes. The study followed a quantitative approach and experimental design, using the SPWalk neural network embedding algorithm and logistic regression classifiers. The results demonstrated that the SPWalk model outperforms state-of-the-art network embeddings (DeepWalk, Node2vec) and traditional phishing detection methods in precision, recall, and F1-score, achieving over 95% accuracy in classifying web pages as phishing or legitimate through the robust and effective learning of URL features alone [19].

In India, a study titled "Phishing Attack Detection Using the Random Forest Algorithm" aimed to propose a machine learning-based protection system to detect malicious and phishing websites, preventing users from visiting them. The analysis units were website URLs, with a sample size of three subsets of 1,000 URLs each. The methodological approach was quantitative and experimental, using supervised learning algorithms Random Forest and Support Vector Machine (SVM). The classifier tested with the three datasets resulted in a detection accuracy of 98.38%, demonstrating the effectiveness of the proposed approach for phishing detection [20].

In Spain, a study titled "Banking Fraud Migration Using Artificial Intelligence Techniques" sought to develop a fraud detection model using AI approaches. Objectives included identifying features and patterns in fraudulent and legitimate transactions, comparing the performance of various machine learning algorithms, and creating a hybrid model integrating the best techniques for fraud detection. The analysis units were bank transactions labeled as fraudulent or legitimate, with a dataset of 1 million transactions split into training, validation, and testing sets. The methodology was quantitative and experimental, involving data preprocessing, feature selection, and various machine learning algorithms. The proposed hybrid model, combining SVM and neural networks, achieved high performance with an accuracy of 98% and a ROC curve of 0.99, outperforming other evaluated methods and identifying the most relevant variables in fraud detection [21].

The study "PhishHaven - An Efficient Real-Time Detection System for AI-Generated Phishing URLs" conducted in South Korea proposed PhishHaven, the first joint machine learning system to detect AI-generated phishing URLs using lexical feature analysis. With a sample of 100,000 URLs, including 50,000 AI phishing and 50,000 normal ones, divided 50%-50% for training and testing, it achieved 98% precision, 97% sensitivity, 99.17% specificity, and 98% F1 measure for AI-generated URLs, thus outperforming existing systems designed only for human-generated URLs [22].

The study "PhishHaven - An Efficient Real-Time Detection System for AI-Generated Phishing URLs" conducted in South Korea proposes PhishHaven, the first joint machine learning-based system for detecting phishing URLs generated by both humans and AI, utilizing lexical feature analysis. With a sample of 100,000 URLs, comprising 50,000 AI phishing and 50,000 normal URLs, split 50%-50% for training and testing, it achieved 98% precision, 97% sensitivity, 99.17% specificity, and 98% F1 measure for AI-generated URLs, thus surpassing existing systems designed solely for human-generated URLs [22].

In a 2022 study from India, a multi-layer stacked ensemble learning model for phishing website detection was proposed, applied across four datasets from India with sample sizes of 11K, 10K, 58K, and 88K instances. Through computational experiments, the proposed model was evaluated alongside machine learning algorithms using metrics such as precision, recall, F-score, and accuracy. The model achieved accuracies of 97.76%, 98.9%, 96.79%, and 98.43% across the datasets, outperforming baseline

 doi:10.20944/preprints202404.0238.v1

models. The results indicate that the proposed stacked ensemble learning-based model facilitates effective phishing website detection [23].

In Pakistan, a phishing attack protection tool called PhishCatcher was developed, implemented as a Chrome extension and based on supervised machine learning techniques for detecting fake login web pages. Utilizing a dataset of 800 URLs, split evenly between phishing and legitimate, a random forest classifier was trained and tested in the PhishCatcher extension, exhibiting excellent performance with 98.5% precision, recall, and accuracy in identifying phishing URLs. Additionally, PhishCatcher demonstrated a very low average response time of 62.5 milliseconds across 40 evaluated phishing URLs [4].

In China, the development of an effective phishing detection model based on a character-level CNN, focusing exclusively on website URL features, is presented. Aiming to provide a fast and accurate solution, it forgoes content extraction and the use of third-party services. The study employs a robust sample including a proprietary database of 318,642 URLs and benchmark databases of 73,575; 83,857, and 82,888 URLs. The study's design involves comparing various deep learning and machine models, evaluating different features extracted from URLs. Instruments used include character-level URL vectorization, vector counts, character-level TF-IDF, and manually constructed features. Various classification algorithms were applied, such as logistic regression, random forest, XGBoost, Recurrent neural network (RNN), RCNN, Deep Neural Network (DNN), and a character-level CNN, with the latter being the proposed model. The results highlight the superior performance of the proposed model, achieving a precision of 95.02% on the proprietary base and 98.58%, 95.46%, and 95.22% on the benchmark bases, surpassing existing phishing URL detection models [24].

A study titled "Enhancing Cybersecurity in the Banking Sector through the Detection of Malicious Attacks Using the Wrapper Stepwise Resnet Classifier" conducted in India aimed primarily at mitigating banking fraud. The study's purpose was to develop an innovative approach for identifying and preventing malicious attacks in the banking sector, utilizing the Wrapper Stepwise Resnet classifier. The units of analysis include cybersecurity data collected from banking institutions. The study employs an experimental research methodology, with a significant sample size of cybersecurity data from multiple sources. Data preprocessing techniques and feature extraction, along with the Wrapper Stepwise Resnet classifier, were used to analyze and classify malicious attacks. The results indicate that the proposed approach achieves a 98.642% accuracy rate in detecting malicious attacks, outperforming existing techniques. These findings support the effectiveness of the proposed approach in enhancing cybersecurity in the banking sector and mitigating fraud [25].

The research "Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment" carried out in Poland aimed to design a machine learning-based scoring system to introduce early fraud warnings in banking. It utilized a sample of 1.9 million records of banking login attempts collected over 2 months. The methodological design consisted of developing a machine learning extension scoring module that analyzes client logins and complements the existing rule-based antifraud system. Two autoencoder models were implemented to classify transactions into risk categories. The results show that autoencoders efficiently discriminated between legitimate, suspicious, and fraudulent events, reducing the manual burden of detecting potentially fraudulent actions [26].

A study titled "Combine Correlation Features Selection for Detecting Phishing Websites Using Machine Learning" conducted in Indonesia aimed to propose an optimal feature selection scenario for detecting phishing websites using machine learning. The units of analysis were phishing websites, using a dataset of 2450 websites. The research methodological design included feature selection and recursive feature elimination, as well as combining three correlation methods with a machine learning algorithm. Four machine learning algorithms were evaluated: Random Forest, SVM, Decision Tree, and AdaBoost. The results showed that CCrFS significantly improved the accuracy of phishing website detection compared to other methods. This study may be relevant for banking fraud mitigation, as phishing websites are one of the primary tools used by criminals to obtain confidential financial information [27].

 doi:10.20944/preprints202404.0238.v1

The study titled "A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks," published in Zambia, presents a modeling technique using Bayesian networks to represent financial cyberattacks perpetrated through malware, specifically GameOver Zeus. It uses Common Vulnerabilities and Exposures (CVE) to calculate conditional probabilities and generate attack paths, later used to create probability density curves reflecting the malware's behavior seeking to capture banking credentials swiftly. Four attack scenarios were identified with varying probability, complexity, and step count. The probability curves' results allow characterizing each path and prioritizing mitigation actions on the most relevant nodes and edges [28].

The study "Hunger Search Optimization with Hybrid Deep Learning Enabled Phishing Detection and Classification Model" conducted in Saudi Arabia and Egypt aimed to develop an effective model for phishing attack detection and classification, with potential applications in banking fraud mitigation. The units of analysis consisted of website URL datasets, employing a methodological design that integrated hyperparameter optimization techniques and hybrid deep learning. The results demonstrated the proposed model's superiority over previous approaches, with significant improvements in accuracy and efficacy in detecting and classifying phishing attacks, suggesting its viability for banking fraud mitigation in cybersecurity environments [29].

This study from Saudi Arabia introduces a hybrid CNN-LSTM model for detecting SMS spam in both Arabic and English messages. The goal is to propose a deep learning architecture that combines Convolutional Neural Networks (CNN), LSTM networks for classifying mixed text messages. The sample includes 2730 Arabic SMS messages collected locally and 5574 English SMS messages from a public dataset. The model's design relies on integrating CNN and LSTM, using word embedding to represent words as numerical vector inputs. Evaluation metrics include accuracy, sensitivity, F1 score, ROC curve, and Area Under the Curve (AUC). The results highlight the proposed model's outstanding performance, with an accuracy of 98.37%, sensitivity of 95.39%, F1 score of 91.48%, and AUC of 93.7%, surpassing other machine learning algorithms in detecting SMS spam [30].

A study in India aimed to develop a model for detecting phishing messages via SMS using multiple correlation algorithms and machine learning techniques. The research uses a sample of 5578 SMS messages, with 747 identified as phishing and 4831 as legitimate. The experimental design methodology evaluates correlation algorithms like Pearson, Spearman, Kendall, and Point-biserial in combination with machine learning classifiers such as AdaBoost, Random Forest, Decision Trees, and SVM. Fifty-two features extracted from the SMS messages served as input for the algorithms, employing feature selection techniques and supervised classification. The results reveal that the AdaBoost classifier, coupled with the Kendall correlation algorithm, achieved the best accuracy of 98.4%, reducing the feature dimensionality by 61.53%, thus outperforming previous methods in detecting Smishing messages [31].

In India, a study titled "Phishing Email Detection Based on Binary Search Feature Selection" aimed at detecting phishing emails through an innovative approach based on binary search feature selection. Analyzing a set of 1,824 phishing emails and 1,604 legitimate ones, the total sample consists of 3,428 emails. The methodology involves email feature extraction, feature selection using ranking algorithms like PCC and binary search, and classification through Random Forest. The applied instruments and techniques cover text processing, readability measures, and URL analysis. The proposed method, named BSFS, achieved an accuracy of 97.41%, surpassing other feature selection approaches like SFFS at 95.63%, and without feature selection at 915.56%. Notably, BSFS identified an optimal subset of 37 features in just six iterations, achieving an efficient balance between accuracy and execution time [32].

A study titled "Particle Swarm Optimization-Based Feature Weighting for Intelligent Phishing Website Detection" conducted in Saudi Arabia presents a proposal to enhance phishing website detection using machine learning techniques. The primary goal is to address the limitations of current phishing detection methods and provide an early warning to users. The analysis unit is phishing websites, utilizing a sample of 245 websites. The quantitative research design employed particle swarm

 doi:10.20944/preprints202404.0238.v1

optimization technique to improve phishing website detection. The authors' proposal significantly enhances phishing website detection compared to current methods [33].

In Greece, researchers embarked on a novel approach to detect persuasion in chat-based social engineering attacks, aiming to enhance cybersecurity in digital work environments by identifying early-stage persuasion tactics used in social engineering attacks. They analyzed chat-based conversations. The experimental research design used CNN and Natural Language Processing (NLP) techniques, along with a chat-based social engineering (CSE Corpus) corpus to train the neural network, specifically annotating Cialdini's principles of persuasion. The proposed persuasion classification model, named CSE-PUC, can determine whether a sentence carries a persuasive message by producing a probability distribution over sentence classes as persuasion containers. The results show promising performance in detecting persuasion tactics in chat-based social engineering attacks [34].

In a study conducted in the United Arab Emirates, researchers proposed an optimized email spam detection algorithm with significant improvements to the Dandelion Optimizer (DO) algorithm. Emails labeled as spam and non-spam from the Spam base dataset were analyzed, with the sample size comprising 4601 instances and 57 features. The research adopted a quantitative approach with an experimental design and compared the performance of the proposed Enhanced DO (IDO) algorithm against established algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and others, based on metrics like accuracy, fitness value, and execution time. K-fold cross-validation and the Wilcoxon test were used for model validation. The results show that the proposed IDO algorithm outperforms the other algorithms, achieving an average classification accuracy of 0.9468, the best average fitness value of 0.0565, and the shortest average execution time of 30.36 seconds. The Wilcoxon test confirms the statistical significance of IDO's performance improvements over other algorithms [35].

In Serbia, a study titled "Character and Word Embeddings for Phishing Email Detection" proposes a neural network model for phishing email detection. For the experimental stage, a sample of 4150 legitimate emails and 2279 phishing emails underwent 10-fold cross-validation. The model extracts vector representations of characters and words directly from email texts through embedding layers and then uses convolutional and LSTM recurrent layers to extract features and classify them. The results show an accuracy of 99.81%, recall of 99.65%, and F1-score of 99.74%, outperforming other state-of-the-art methods. This model represents an advancement in automatic phishing email detection through the learning of textual vector representations [36].

In Brazil, machine learning-based methods were proposed to improve phishing email detection rates using a sample of 6,429 emails from the Phishing Corpus and SpamAssassin PublicCorpus datasets. The approach consisted of generating more expressive feature attributes using natural language processing techniques, lemmatization with WordNet, bag-of-words model, document-term matrix, and Latent Dirichlet Allocation (LDA). Various classification algorithms were trained with these features using enhanced resampling and cross-validation techniques. An F1-Score success rate of 99.95% was achieved with the XGBoost algorithm, surpassing previous state-of-the-art results in this area [37].

The study "Life-long phishing attack detection using continual learning" carried out in Pakistan aimed to identify and mitigate performance degradation in machine learning models for phishing attack detection. A sample of 90k phishing web pages and 80k benign pages from 2018-2020 was used, with an experimental design comparing traditional neural network models, transfer learning, and continual learning models. Feature vector analysis with FastText and neural network models was the instrumentation used. The results show that continual learning models maintain high performance over time, with a tolerable performance drop of only 2.45%, while traditional and transfer learning models suffer performance deteriorations of 8-20% [38].

The study titled "A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning" conducted in Pakistan aimed to introduce a layered phishing attack detection approach through the analysis of URL features, text content, and images. A sample set comprised of 20,000

 doi:10.20944/preprints202404.0238.v1

phishing URLs and 20,000 legitimate URLs, as well as a dataset of spam and non-spam text messages, was analyzed. The quantitative methodology employed a comparison of machine learning classification models. Various algorithms such as SVM, XGBoost, random forest, multilayer perceptron, logistic regression, and decision tree were utilized. The results highlight that the XGBoost algorithm showed superior performance, achieving maximum training phase precision and accuracy of 94% and testing phase precision of 91%. The multilayer perceptron also demonstrated good performance with a testing phase precision of 91%. Additionally, random forest and decision tree achieved precisions of 91% and 90%, respectively. Text classification was conducted using logistic regression and SVM, with precisions of 87% and 88%, respectively. These results suggest that the proposed hybrid approach, backed by the XGBoost algorithm, is effective in detecting phishing attacks in alluring ads [39].

In a study conducted in the United Arab Emirates, researchers presented a classifier based on the DDQN (Double Deep Q-Network) to address web phishing detection without utilizing previous data sampling techniques for class balancing. They analyzed both malicious and legitimate URLs from the Mendeley web phishing dataset, consisting of 30,647 malicious URLs and 58,000 legitimate ones. The research took a quantitative approach with an experimental design, comparing the performance of the proposed DDQN against established deep learning algorithms combined with data sampling techniques. The model employed K-fold cross-validation and metrics specific to unbalanced classification problems. The conclusion was that the proposed DDQN surpassed other algorithms in metrics like geometric mean, balanced accuracy index, F1 score, and area under the ROC curve in all test cases, without prior data manipulation [40].

In China, a study aimed to develop a phishing detection model capable of identifying bank fraud attacks. The unit of analysis was web page URLs, using a dataset of 50,000 URLs, divided into three subsets for training, testing, and validation. The quantitative research approach involved extracting URL features through a deep learning model that combines a convolutional neural network and a Transformer encoder. The results showed that the proposed model achieved an F1 score of 99%, precision of 99%, and recall of 99%, suggesting that PhishTransformer is a promising new approach for phishing detection and banking fraud mitigation [41].

A study at the Ming Chuan University's Department of Computer Science and Engineering in Taoyuan, Taiwan, developed a BERT-based approach to improve the detection of malicious URLs. This experimental research utilized three public datasets for evaluation: a Kaggle dataset containing only URL strings, a GitHub dataset with only URL features, and an ISCX 2016 dataset containing both. The proposed method achieved accuracy rates of 98.78%, 96.71%, and 99.98% on these datasets, respectively. It was also tested on two datasets from different domains, IoT and DNS over HTTPS (DoH), demonstrating its versatility. The results show that the BERT-based approach performs excellently in detecting malicious URLs compared to other methods [42].

In Mexico, researchers proposed a methodology aimed at detecting cyberattack messages on social networks. The quantitative research with an experimental design analyzed social media messages using natural language processing and convolutional neural networks. The sample consisted of real messages, achieving an accuracy of 0.91 in detecting cyberattacks and 0.82 in classifying them into four categories. The findings demonstrate the effectiveness of the proposed methodology for detecting cyberattacks in social media messages, potentially useful for banking fraud mitigation in the context of social networks [43].

In China, enhanced phishing email detection through ensemble learning and subsampling was proposed to mitigate the impact of data imbalance on classifier performance and improve the phishing email detection rate. The analysis unit was legitimate and phishing emails, with the sample size consisting of 32,046 legitimate emails and 3,465 phishing emails. The experimental design included a training set and a test set. Two new algorithms, FMPED and FMMPED, involving the subsampling of legitimate emails and ensemble learning for classification, were proposed. Results showed improvements in AUC up to 47.50%, G-mean value up to 90.63%, and MCC coefficient up to 95.99% compared

 doi:10.20944/preprints202404.0238.v1

to other algorithms. The FMMPED algorithm achieved an F1-score of 0.9941, precision of 0.9941, AUC of 0.9797, and G-mean of 0.9795 [44].

In South Korea, a hybrid model based on 1D-CNN with enhanced attention using FastText word embedding was developed for the detection of banking voice phishing. The main goal was to mitigate banking fraud by implementing a sophisticated detection model, analyzing transcripts of fraudulent phone calls with a significant amount of Korean voice data. The quantitative research approach employed NLP and machine learning (ML) techniques, with the implementation of a hybrid 1D-CNN and BiLSTM model enhanced with FastText word embedding. The results revealed improved performance in banking fraud detection, with superior accuracy and F1 scores, suggesting the efficacy of the proposed model in addressing this specific vishing issue in the Korean banking context [45].

In a study conducted in Saudi Arabia, researchers proposed mitigating bank fraud through phishing detection using the Chaotic Dragonfly Algorithm. The primary aim was to enhance security in banking transactions by developing an effective phishing detection method utilizing the chaotic behavior of the dragonfly algorithm. The research was carried out across various financial institutions in Saudi Arabia, focusing on analyzing suspicious banking transactions and user behavior patterns. The sample consisted of real banking transaction data, with a sample size of 100,000 transactions. The Chaotic Dragonfly Algorithm was applied for the automated selection of features, along with K-nearest neighbors (KNN), SVM, and decision tree classifiers. The results showed a 20% improvement in phishing detection accuracy compared to traditional methods, demonstrating the efficacy of the proposed approach in mitigating bank fraud [46].

In another group of researchers in Saudi Arabia, a phishing website detection system was proposed using deep learning techniques LSTM, CNN, and LSTM-CNN. This system analyzed web URLs, with the sample consisting of 20,000 URLs, of which 9,800 were phishing and 10,200 legitimate. The research adopted a quantitative approach with an experimental design. Performance measures such as precision, recall, confusion matrix, and accuracy were used, indicating that the CNN algorithm surpasses LSTM and LSTM-CNN in phishing detection, achieving an accuracy of 99.2%, while LSTM-CNN and LSTM achieved 97.6% and 96.8%, respectively. The proposed CNN system demonstrates superiority in the effective classification of phishing URLs [47].

In Saudi Arabia, a study titled: Cyber Threats Classifications and Countermeasures in the Banking and Financial Sector aimed to analyze cyber threats facing the banking and finance sector, with the goal of developing a comprehensive strategy to mitigate bank fraud. The units of analysis include financial institutions, banks, regulatory entities, and cybersecurity companies. The research methodology is a mix of qualitative and quantitative methods, with a sample study comprising 50 financial institutions from different geographical regions, including commercial banks, investment banks, and credit unions. Instruments and techniques used include questionnaires, semi-structured interviews, participant observation, and analysis of cyber incident data. The results show that the most common cyber threats in the banking and finance sector are malware, phishing, distributed denial-of-service (DDoS) attacks, and insider threats. These attacks have led to significant financial losses, with the average cost amounting to $3.86 million in 2020, and the number of global ransomware attacks increasing by 148% between February and March 2020. To mitigate these threats, the study proposes a comprehensive strategy combining technical controls such as encryption, multi-factor authentication, and network segmentation [48].

In India, researchers developed a malicious URL detection mechanism using recurrent deep learning models. The study aimed to propose a detection mechanism to identify malicious URLs using recurrent neural networks like LSTM, Bi-LSTM, and Gated Recurrent Unit (GRU). A Kaggle dataset with 450,176 URLs, including 345,738 legitimate URLs and 104,438 phishing URLs, was used. 70% of the data was used for training the models and the remaining 30% for evaluation. The research adopted a quantitative approach with an experimental design. LSTM, Bi-LSTM, and GRU deep learning models were applied and evaluated using confusion matrices, precision, recall, F1 score, and accuracy. The results showed that the Bi-LSTM model achieved the highest precision of 99%, compared to 97% for

 doi:10.20944/preprints202404.0238.v1

LSTM and 97.5% for GRU. Bi-LSTM also obtained the highest F1 score and recall among the evaluated models. In conclusion, the proposed recurrent Bi-LSTM model demonstrated the best performance for detecting malicious URLs [49].

In Saudi Arabia, a group of researchers developed an intelligent phishing URL detection method based on BERT feature extraction and deep learning algorithms, aiming to mitigate this type of fraud. The research adopted a quantitative approach with an experimental design. Using a sample of 549,346 URLs from a public dataset, they applied natural language processing techniques using BERT to extract semantic features from the URL text. They then trained a classification model based on a convolutional neural network on these extracted features and evaluated its accuracy on a test set, achieving an accuracy of 96.66% in detecting fraudulent URLs. The authors conclude that the proposed combination of textual feature extraction using BERT and classification with neural networks is effective for detecting this type of bank fraud [50].

In Saudi Arabia, researchers proposed a model to detect homographic attacks by combining a hash function and machine learning. The goal was to enhance accuracy in identifying fraudulent websites using visually similar characters. The quantitative research approach analyzed a sample of 70,000 URLs (35,000 legitimate and 35,000 fraudulent) to train classification models. Features were extracted from URLs, and classifiers such as SVM, decision trees, and random forests were tested. The model achieved a 99.8% accuracy with Random Forest, concluding that using a hash function improves the detection of homographic attacks. This detector can be implemented as standalone software to enhance web browser security [51].

A novel logo identification technique for logo-based phishing detection in cyber-physical systems was proposed in India. The study aimed to propose a phishing detection mechanism based on logos, using hue values and the density distribution of hue values, uniquely defining each logo's characteristics and identifying known brands. The study's units of analysis were logos from 21 popular brands prone to phishing, totaling 538 logos. The methodology involved a training phase to prepare the dataset with logo characteristics and a detection phase to classify new logos as phishing or genuine. Machine learning algorithms (decision tree, random forest, SVM, KNN, naive bayes) trained with the data showed that the ensemble random forest classifier achieved an 87% accuracy in correctly detecting genuine logos [52].

In the UK, researchers developed a detection solution called Phish Responder, using a hybrid machine learning approach combining natural language processing and deep learning to detect phishing and spam emails. Email datasets containing phishing, spam, and benign emails from various public Kaggle datasets were analyzed. Experimental experiments determined the most suitable machine learning techniques, including natural language processing (tokenization, TF-IDF) and deep learning algorithms: LSTM, Multi Layer Perceptron (MLP). Phish Responder achieved an average accuracy of 99% with the LSTM model for text-based datasets and 94% with the MLP model for numerical datasets. An independent T-test proved the numerical technique significantly better than existing approaches [53].

In Saudi Arabia, researchers introduced an Optimal Deep Autoencoder Network (ODAE-WPDC) for phishing website detection and classification to achieve cybersecurity. The quantitative, experimental approach utilized a sample of 11,055 URLs (4,898 legitimate and 6,157 phishing) from the Kaggle repository. Data preprocessing, feature extraction, feature selection with the Artificial Algae Algorithm (AAA), and classification with a Deep Autoencoder (DAE) optimized with Invasive Weed Optimization (IWO) were applied. The ODAE-WPDC model achieved an average precision of 99.29%, recall of 99.24%, F-score of 99.27%, and accuracy of 99.28%, outperforming state-of-the-art deep learning methods [54].

An experimental study in India proposed a three-phase phishing detection mechanism (Domain Name System [DNS] blacklist, heuristic-based, and web crawler) for accurately detecting phishing websites. URLs, website content, and web traffic were analyzed using 200 samples with features and labels, split into training (70%) and testing (30%) sets. Three classifiers (neural network, SVM, and

 doi:10.20944/preprints202404.0238.v1

random forest) were utilized. Classification accuracy results were 95.18%, 85.45%, and 78.89% for neural network, SVM, and random forest, respectively, with the neural network performing best in phishing detection [55].

Research in Jordan aimed to propose a method for detecting phishing website attacks using Fuzzy Rule Interpolation (FRI) to enhance the robustness of fuzzy systems and effectively reduce their complexity. Phishing and legitimate websites were analyzed using a sample of 5,000 sites from PhishTank and OpenPhish and 5,000 legitimate sites from Alexa and Common Crawl. The experimental design used a public dataset of phishing websites. The proposed FRI-Incircle method achieved a detection rate of 97.58% and effectively reduced false alerts, smoothing the boundaries between normal and attack traffic due to its fuzzy nature. The results were competitive compared to other methods in the literature [56].

In a study conducted in Turkey, researchers introduced a novel hybrid classification algorithm named the Core Classifier Algorithm (CCA), which is based on class cores and clustering to enhance accuracy in nonlinear classification. Five datasets from two different domains (phishing URLs and healthcare) were analyzed, with sample sizes ranging from 1,000 to 36,569 observations. The research took a quantitative approach with an experimental design, employing classification algorithms and clustering (K-means). The proposed CCA algorithm achieved up to 100% accuracy in linear classification, surpassing well-known algorithms like Random Forest and SVM in various nonlinear classification cases; by hybridizing with clustering, the model's accuracy increases for each dataset with an appropriate number of clusters [57].

Researchers in South Korea proposed a method to enhance phishing attack detection by optimizing URL feature selection using Genetic Algorithms integrated into deep Convolutional-Recurrent neural networks. The aim was to improve performance metrics such as precision and recall. A total of 222,541 URLs from 3 public datasets were analyzed, consisting of 95,541 benign and 126,547 malicious URLs. The study adopted a quantitative approach with an experimental design, developing a deep learning model combined with Genetic Algorithms to optimize the search for relevant URL features for phishing detection. Techniques used included feature extraction and selection based on the evolutionary rules of Genetic Algorithms and deep learning models such as convolutional and LSTM neural networks. Results showed improvements of 4.13% in precision and 7.07% in recall compared to previous deep learning methods for phishing URL classification [58].

The study "Machine learning-based phishing detection from URLs" conducted in Turkey aimed to propose a real-time system against phishing using seven different machine learning classification algorithms and features based on NLP to detect phishing web pages from URLs. The sample consisted of 73,575 URLs, of which 36,400 were legitimate URLs and 37,175 were phishing URLs. The methodological design was experimental, testing three types of feature sets, word vectors, NLP-based, and hybrids, with seven classification algorithms. The instruments were machine learning classification algorithms. Results show that the Random Forest algorithm with only NLP-based features gives the best performance with a precision rate of 97.98% for phishing URL detection [3].

3. Methodology

This research is designed within a quantitative approach framework and utilizes an experimental design. The objective is to propose a model aimed at mitigating Computer Fraud attacks specifically in the forms of Fakeapp and SIM Swapping on Android mobile phones. To achieve this, the IMEI, geolocation, fingerprint recognition, and One Time Password (OTP) messaging will be utilized as core components of the proposed model. A field test will be conducted to simulate FakeApp and SIM Swapping attacks on a group of 50 professionals with advanced knowledge in Information and Communication Technologies (ICTs). Data collected from this exercise will be used to assess the model's effectiveness in mitigating fraud, with particular focus on the mentioned attack vectors.

The process of a computer fraud attack targeting banking system customers is depicted in Figure 6 and unfolds in three stages.

 doi:10.20944/preprints202404.0238.v1

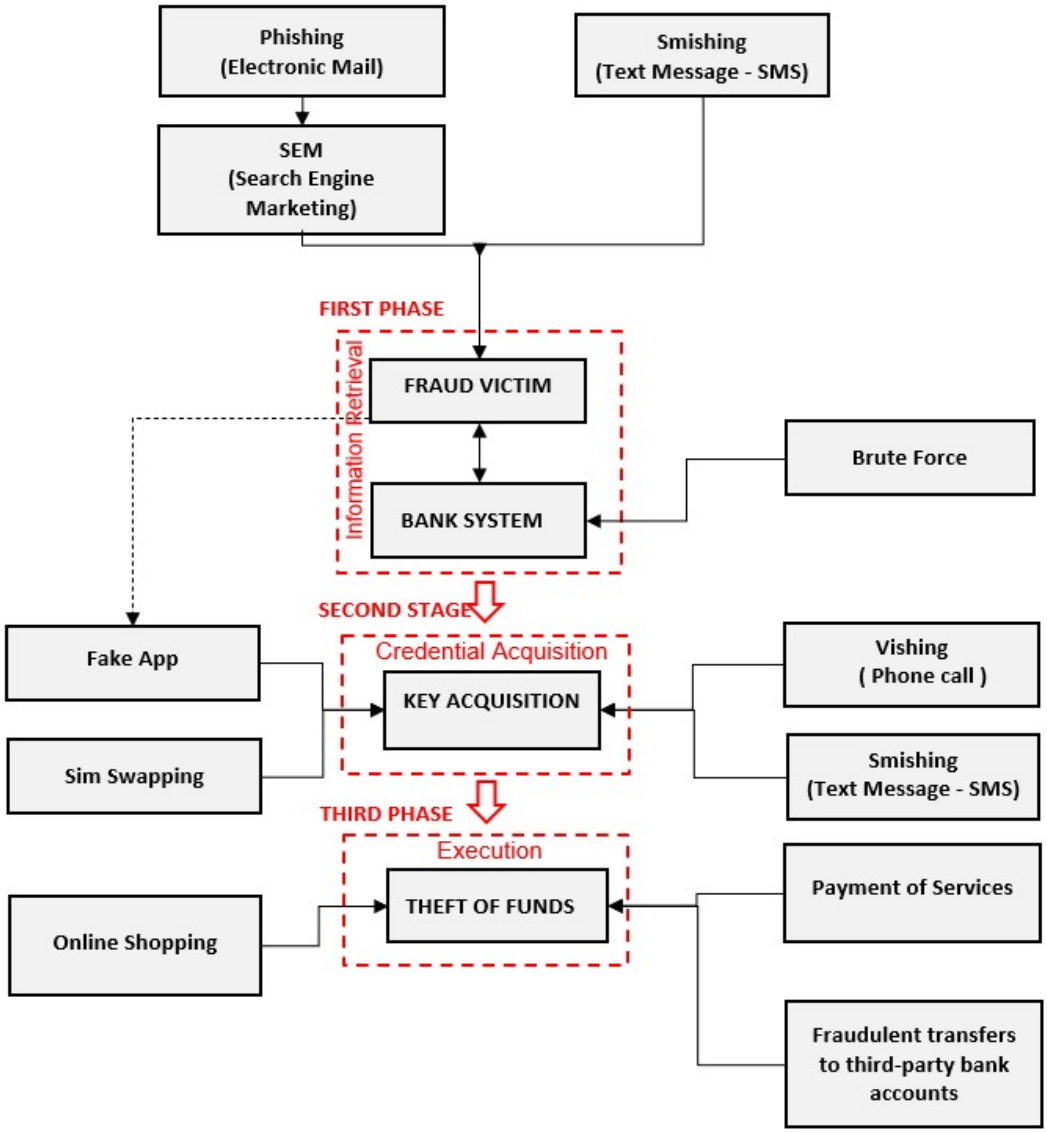


Figure 6. Fraud process map.

In the first stage, cybercriminals obtain banking details such as account holder name, account number, card number, internet banking password, and affiliated phone number. These details are acquired through phishing, smishing, or vishing attacks directed at customers, or via brute force attacks on the banking systems.

The second stage, known as credential acquisition, involves obtaining the dynamic key or operation validation code. Here, the cybercriminal, employing vishing techniques, impersonates a bank official to gain possession of the dynamic key or validation code sent to the victim's mobile phone or through a token. This information can also be obtained via smishing, Fake APP, or Sim Swapping techniques.

The third stage, execution, entails the theft of funds from victims' bank accounts through fraudulent transfers to third-party accounts (money mules), payments for services, or online purchases.

This methodology outlines a structured approach to simulate and analyze the effectiveness of the proposed model against sophisticated cyber-attacks in the banking sector, providing valuable insights into the development of more secure mobile banking environments.

The proposed model is operationalized through a mobile application, harnessing unique user and device features such as fingerprint recognition and the IMEI, along with geolocation, to authenticate electronic transactions via mobile banking.

 doi:10.20944/preprints202404.0238.v1

3.1. Mobile Banking Fraud Typologies

Mobile banking fraud typologies encompass a range of malicious techniques deployed by cybercriminals to compromise users' security and financial information via mobile phones. These typologies present significant challenges to mobile banking security, necessitating stronger preventive and security measures to shield users from these burgeoning threats. Various studies have delineated the techniques utilized by cybercriminals:

3.1.1. Phishing

Phishing, an increasingly sophisticated cybercrime, involves deceptive communications sent by attackers aiming to extract confidential information from victims. This phenomenon is marked by the use of fake websites and messages designed to harvest personal data for malicious purposes. Given the rising complexity and prevalence of these attacks, there is a pressing need for more advanced detection systems, integrating artificial intelligence and machine learning technologies [59].

Recent research advocates for the implementation of NLP and Deep Learning (DL) algorithms for the effective identification of phishing attempts, analyzing text on suspicious websites. These algorithms, including LSTM (Long Short-Term Memory), BiLSTM (Bidirectional Long Short-Term Memory), GRU, and BigRu, are recognized for their ability to meticulously examine the semantic and syntactic features of web content. Their application in this domain promises to achieve significant accuracy levels in fraud activity detection [59]..

3.1.2. Smishing

Smishing refers to a specific type of communication fraud where attackers use SMS messages to coax users into disclosing sensitive information or carrying out malicious actions. This social engineering technique primarily aims to acquire user credentials, install malware, or lay the groundwork for more sophisticated spoofing attacks. Recent studies have delved into the dynamics and impact of these phishing attacks while concurrently developing methods to counter them. These investigations reveal that a substantial portion of users is vulnerable to smishing attacks, highlighting the need to bolster security strategies.

In this vein, experts have examined various approaches to enhance the detection and prevention of such attacks. Among the most promising proposals are the deployment of advanced classifiers analyzing texts and URLs to identify phishing attempts, and the application of neural networks. These technologies, specifically tailored to discern subtle patterns in message content, promise high accuracy in identifying and neutralizing smishing attempts. The collective approach of these methodologies indicates a significant advancement in combating digital impersonation [60–62].

3.1.3. Vishing

Vishing, a portmanteau of "voice" and "phishing," refers to a social engineering technique wherein the attacker, through phone calls, seeks to persuade targeted individuals to disclose confidential information such as usernames and passwords, or information about roles and responsibilities of other employees. During these interactions, the "visher" employs manipulation and persuasion tactics to extract information that can be used for immediate financial gain or to facilitate subsequent vishing attacks. This method is characterized by its direct and personalized approach, potentially increasing its effectiveness compared to other forms of phishing attacks. The nature of these tactics underscores the necessity for heightened cybersecurity awareness and training to prevent the inadvertent disclosure of sensitive information [63].

3.1.4. SIM Swapping

The criminal technique known as SIM card cloning involves the unauthorized reproduction of SIM cards to illegitimately access mobile services and obtain sensitive personal and financial data from the line holder. This practice has seen a notable increase globally, particularly during the COVID-19

 doi:10.20944/preprints202404.0238.v1

pandemic, a period marked by a significant rise in reliance on virtual communications and transactions. Criminals have exploited this situation to intensify their illicit activities [64].

The process of SIM card cloning typically unfolds in three key stages: first, the illicit acquisition of the user's personal data; second, the fraudulent reproduction of the SIM card using sophisticated techniques; and third, the utilization of the usurped mobile services to conduct illicit activities. This method poses a serious risk to information security and user privacy, highlighting the need for the implementation of more robust security measures both at the mobile service operator level and by the users themselves [64].

3.1.5. Fake App

A fake app is one that pretends to be legitimate but is actually malicious, aiming to deceive or harm users.

Fake apps and scams within the banking sector are two distinct areas of concern. Fake apps, belonging to the underground mobile industry, have been subject to limited discussions and investigations. Tang et al. conducted an exhaustive study on fake apps and collected over 150,000 samples related to popular apps [65].

3.1.6. Brute Force

Brute Force is a malicious method employed by cybercriminals to infiltrate computer systems by making numerous login attempts with different password combinations [25]. This approach relies on the premise that the correct password will eventually be found due to the exhaustive testing of all possible combinations. Hackers use a program designed to decrypt encrypted passwords using specific algorithms to automate this process and increase the efficiency of the attack [66].

3.1.7. Cybercrime

Cybercrime refers to criminal activities that are committed using computers or targeting computer systems. It encompasses various types of crimes, such as identity theft, hacking, and fraud. Cybercrimes pose a high risk to businesses, especially in the banking sector, and can range from hacking to cyberterrorism. The challenges faced by the banking sector in combating cybercrime are significant, and various countries have adopted measures to address this issue. Law enforcement and the criminal justice system face challenges in dealing with cybercrime due to the disruptive effects of digital innovation. Private entities have played a significant role in developing technical measures for crime prevention, while public perception of the role of law enforcement in preventing cybercrime remains weak. The impact of cybercrime on trials has necessitated legal professionals to understand the challenges and limits of digital evidence. Efforts are being made to classify cybercriminals and cyberattacks and develop strategies to combat cybercrime and strengthen cybersecurity [67].

3.1.8. Search Engine Marketing (SEM)

In recent years, it has been observed that an increasing proportion of internet users access websites they visit using search engines rather than direct links from another online page. Clearly, search engines play a significant role in the online world. They are used to find a variety of information, such as objects, events, people, and locations. Consumers frequently use web search engines to gather information about e-commerce [68].

3.2. Capturing Unique User and Mobile Features, and Application Permissions

The proposed model, as illustrated in Figure 7, outlines the application process for capturing unique user and mobile features, and access permissions by the application. The diagram begins with the user opening a bank account, followed by the installation and entry into the application, data capture, and concluding with storage in the entity's database. The steps are described as follows:

 doi:10.20944/preprints202404.0238.v1

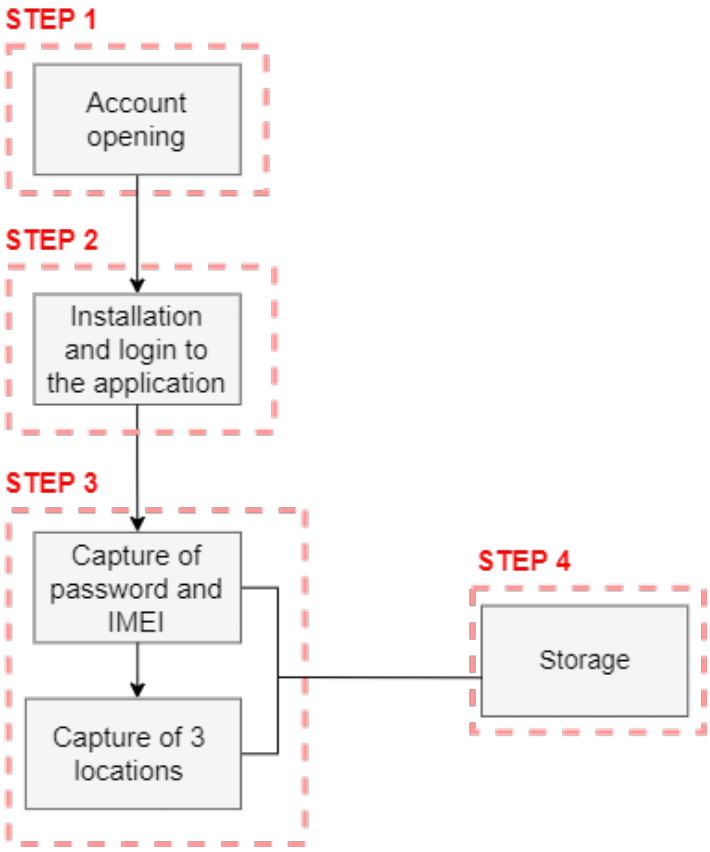


Figure 7. Data capture diagram.

- Step 1: Opening a Bank Account

  The user must personally visit the bank branch to register their personal data, which includes names, identity document number, address, and telephone number along with the operator.
- Step 2: Application Installation

  After opening the bank account, the user will download and install the application and then register their credentials.
- Step 3: Capturing the Password and IMEI

  This step is divided into two phases, initial and final. In the initial phase, the user sets their password to access mobile banking. The application verifies the accuracy of the entered data to allow the registration of the new user. Additionally, the IMEI is registered in the bank's database for future validations. As an additional security measure, the application also uses the user's fingerprint as an authentication factor.

  In the final phase, the application will ask the user to define three safe location points using the integrated Google Maps services, adding an extra layer of protection.
- Step 4: Storage

  Finally, the application stores the IMEI in the database, so that in the next login, the system will verify the correspondence of the mobile device's IMEI with the IMEI registered in the database before allowing access to the application menu.

3.3. Execution of the Sectrabank Model

The proposed model has been developed following a comprehensive study of fraud attack methods, detailed in Figure 6, which illustrates a model designed to counteract attacks such as phishing, smishing, fake apps, and SIM card spoofing, as depicted in Figure 8.

 doi:10.20944/preprints202404.0238.v1

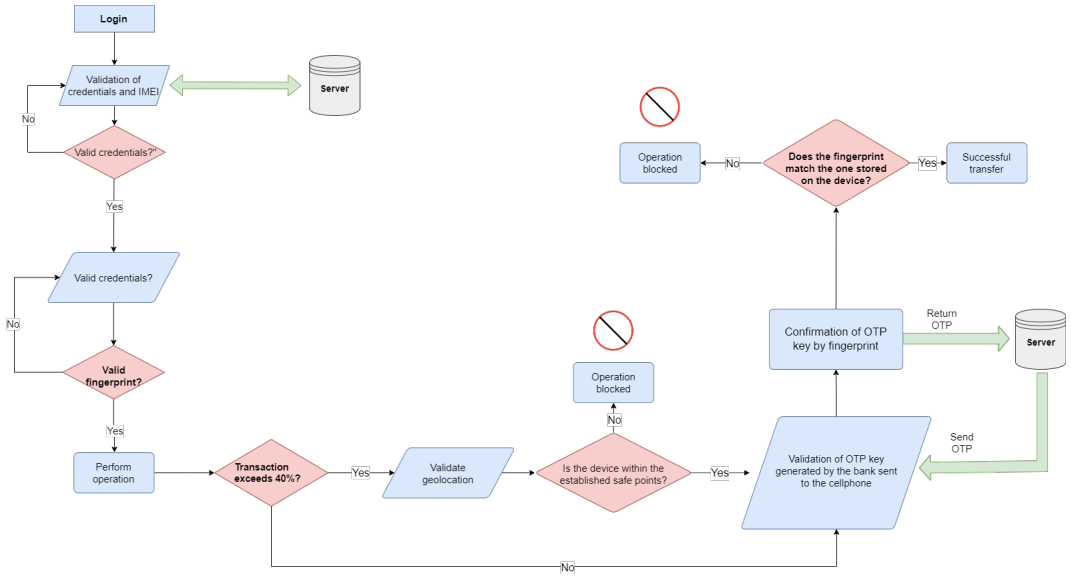


Figure 8. Sectrabank model flow map.

- First Layer of Security:

  This phase involves the validation of security credentials, account number, password, and IMEI. It constitutes the initial process, during which the user launches the application to enter their credentials. These credentials are validated by comparison with the information stored on the financial entity's server; additionally, the user's fingerprint is also validated. In this stage, Sectrabank focuses on mitigating cyberattacks in their various forms by validating the IMEI and the user's fingerprint registered on the mobile device. If all requirements match, it is inferred that the user is attempting to carry out operations from the validated device; otherwise, the operation will be blocked.
- Second Layer of Security:

  The effectiveness of this layer is based on the principle of geolocation. In other words, to conduct transfers that exceed 40% of the total amount in the account, it is necessary to be in a pre-established location designated as a safe zone, delimited by a geofence. Failure to meet this condition will result in the inhibition of any banking transaction. This approach ensures that individuals with malicious intentions cannot use our credentials to carry out fraudulent transactions. The first two security barriers have been designed to reduce the risk associated with cyber fraud, especially in modalities such as SIM swapping and fakeapp. In the scenario that these measures are bypassed, the third layer of security will be activated.
- Third Layer of Security:

  The system integrates an additional layer of security consisting of the implementation of a OTP, which can only be validated through the user's fingerprint authentication. In the event that the user does not comply with this validation process, the operation will be blocked. This measure significantly strengthens the system's integrity, providing an additional layer of protection against potential unauthorized access attempts.

4. Discussions

The "SMISHING DETECTOR" model demonstrated a 96.29% accuracy rate in detecting fraudulent smishing messages. This study analyzed 5,858 SMS messages, including 538 smishing and 5,320 legitimate messages, and developed the model with four modules: SMS Content Analyzer, URL Filter, Source Code Analyzer, and APK Download Detector. Utilizing multiple approaches for content and behavior analysis allowed for effective fraud detection while minimizing false positives [2].

 doi:10.20944/preprints202404.0238.v1

On the other hand, the HearMeOut model for detecting phishing activities via voice on Android achieved a 100% accuracy rate with an additional average latency of only 0.36 ms. This quantitative study with an experimental design analyzed 1,017 voice phishing applications obtained from an antivirus corporation and the Financial Security Institute of South Korea. Through static and dynamic analysis, the study identified three new phishing functionalities: outbound call redirection, call screen overlay, and fake call voice [69].

The "FINGERPRINTING" model was successful in preventing most cases of fraud involving SIM boxes by analyzing 102 commercial devices, including 85 smartphone models, 6 SIM boxes, and 11 IoT devices. Device fingerprints were constructed from control plane signaling messages, proving smartphones have virtually unique fingerprints. A fraud prevention system was proposed using an access control list that leverages these fingerprints to validate reported IMEIs.

Similarly, the proposed Sectrabank model focuses on detecting malicious attacks in the banking sector, akin to the "PHISHING DETECTION" study. However, while the Chinese study concentrates on phishing detection using a Character-Level Convolutional Neural Network, Sectrabank distinguishes itself by employing the device's fingerprint and IMEI to validate electronic transactions and prevent attacks such as phishing, vishing, smishing, and SIM swapping [9].

This comparative discussion emphasizes the diverse methodologies and technologies employed in the battle against cyber threats within the banking sector. The Sectrabank model illustrates an innovative approach by integrating unique device identifiers and user biometrics, offering a personalized and secure method for thwarting cybercriminal activities. The success of these models underscores the potential for further research and development in enhancing cybersecurity measures to combat the evolving landscape of cyber threats effectively [24].

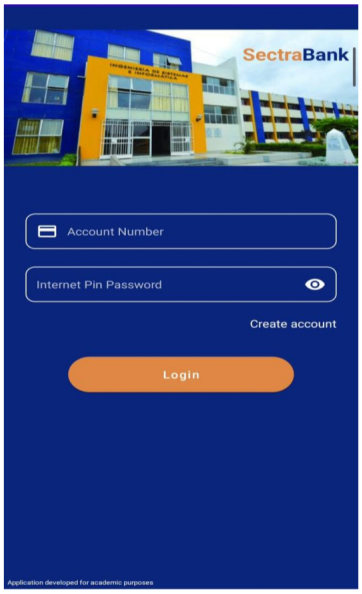
5. Results

In the current context of rising cybercrime, ensuring the security of electronic banking operations has emerged as a critical priority. Following a comprehensive systematic literature review and a detailed analysis of the cyberattack process depicted in Figure 6, a model named Sectrabank was developed. This model incorporates multiple security layers to mitigate cyberattacks, specifically targeting SIM Swapping and Fake App scenarios. Designed for the Android platform for research purposes, Sectrabank integrates three security layers to validate the device's IMEI, the user's fingerprint, geolocation, and OTP message verification, leading to the final prototype of the system.

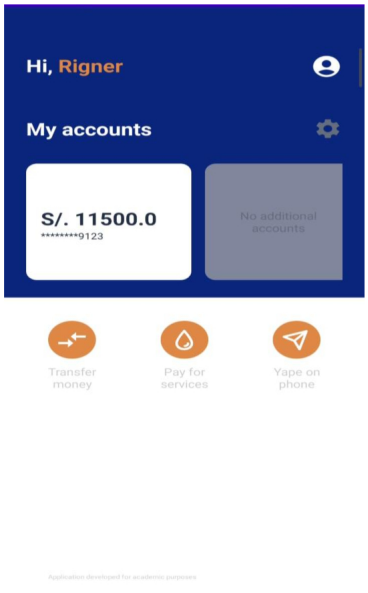
For validation, the Sectrabank model underwent evaluation by subject matter experts through field testing. An experimental group and a control group were considered, and data were collected from 100 experts, including students from the Faculty of Software Engineering at the National University of San Marcos, police officers from the High Technology Crime Investigation Division of Peru (DIVINDAT), and prosecutors specialized in cybercrime investigation.

Sectrabank presents four main interfaces as observed in Figure 9, which are the Login Interface, Dashboard Interface, Geolocation Interface, and Transfer Interface.

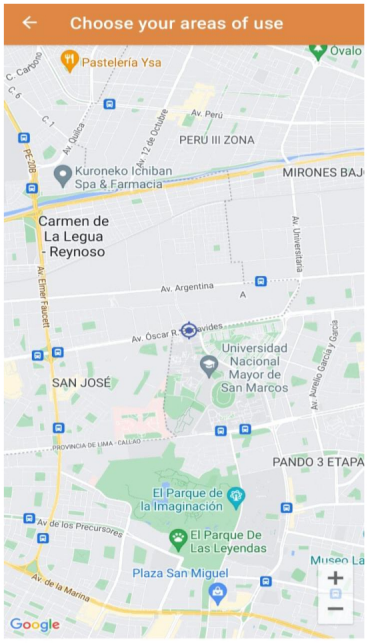
Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 April 2024 doi:10.20944/preprints202404.0238.v1



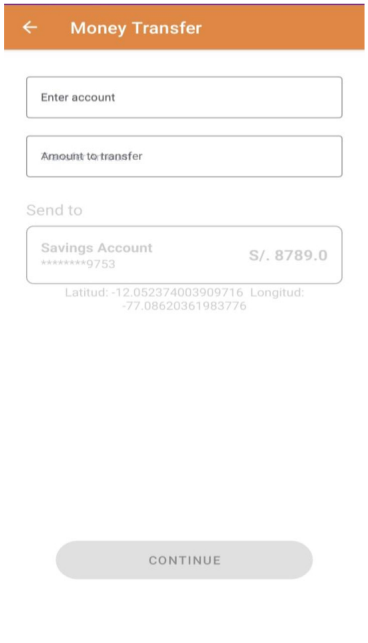
(a) : Login Interface



(b) : Dashboard Interface



(c) : Geolocation Interface



(d) : Transfer Interface

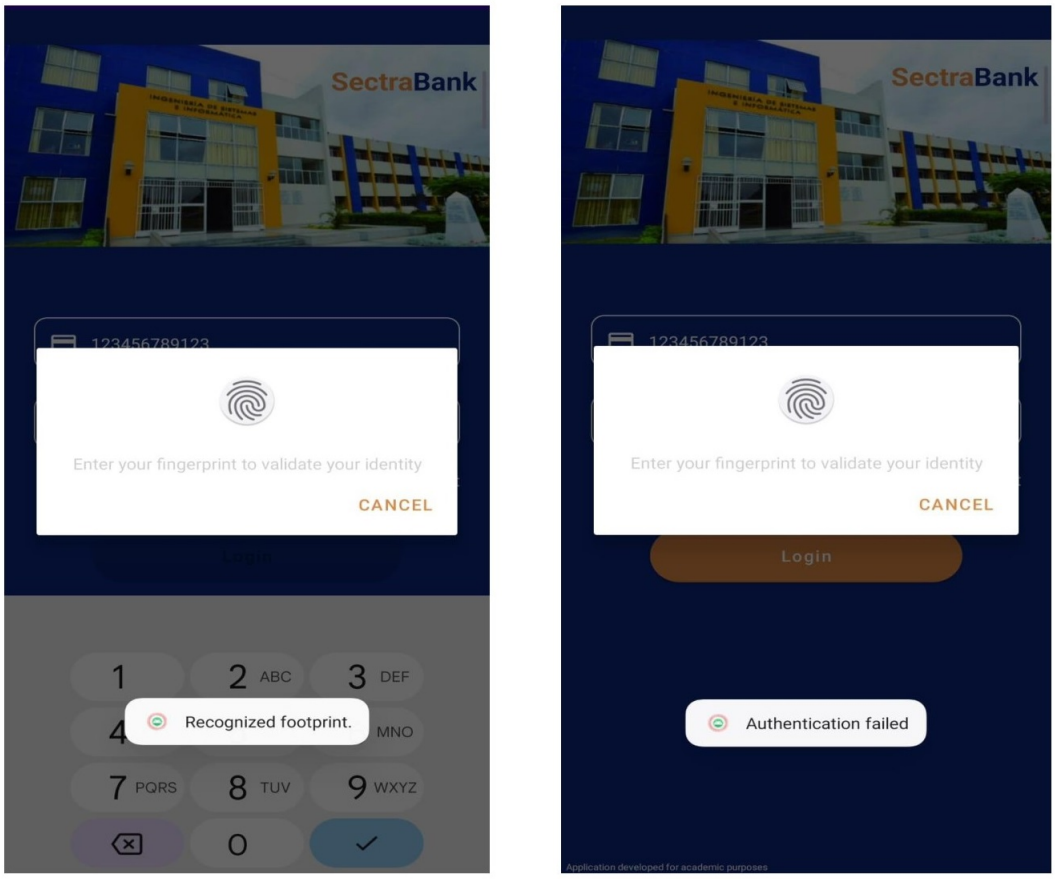
Figure 9. Sectrabank application user interfaces.

Figure 10 illustrates the operation of the first security layer, allowing login only by validating the correct credentials, such as the registered IMEI and the fingerprint. The model displays a message of successful authentication, as shown in Figure 10(a).

 doi:10.20944/preprints202404.0238.v1

If the IMEI, password, or fingerprint is incorrect, the system will not allow login, displaying an error message in user verification, as observed in Figure 10(b). This mechanism effectively mitigates the risk of SIM Swapping attacks.

Upon successful verification of user credentials, the model reveals the main menu interface, as seen in Figure 9(b). The top part displays the user's name and account balance, while the bottom part presents the banking operation panel.

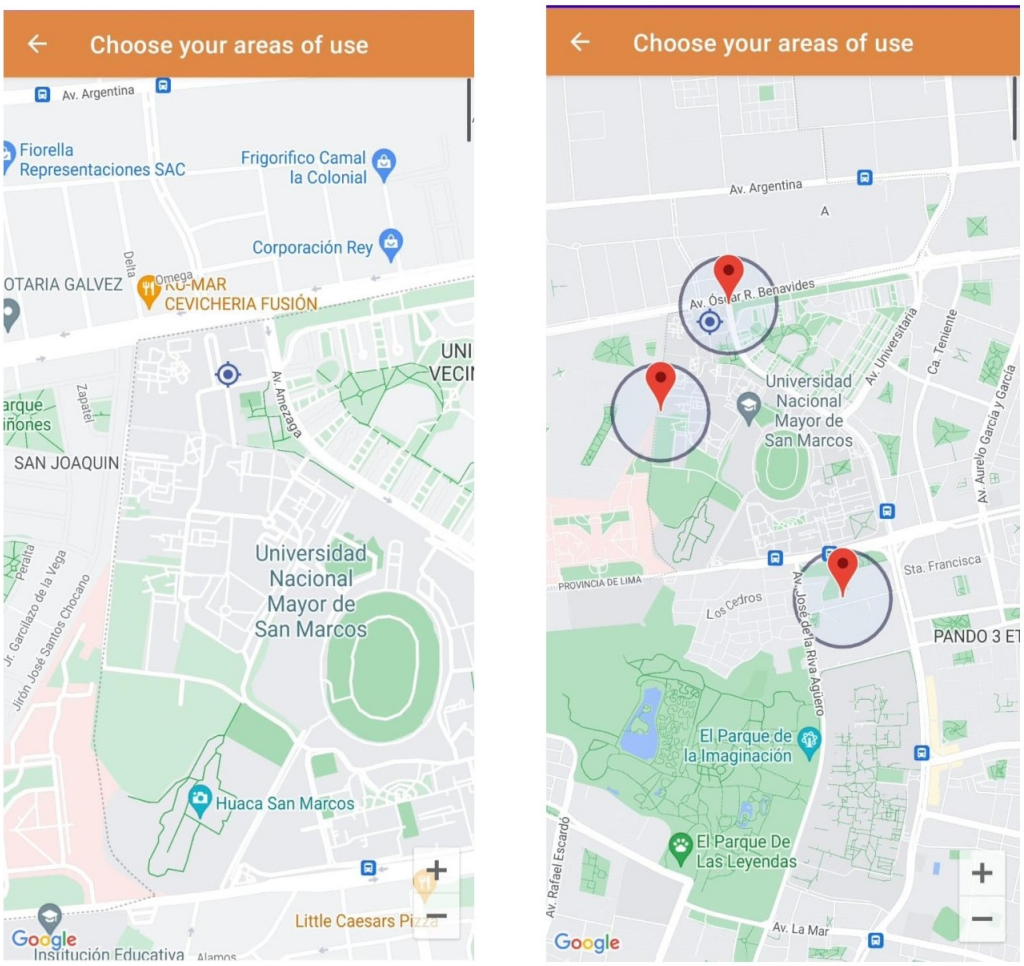


(a) Succesful Authentication (b) Failed Authentication

Figure 10. First layer of security.

Figure 11 illustrates the functionality of the second security layer, which allows users to select three geolocation points for validating transactions exceeding 40% of the total account balance. This process is implemented as a defense mechanism against potential cyberattacks enabling unauthorized geographical locations to conduct transfers, as exemplified in Figure 13(a). If a transfer attempt is detected originating from a geolocation outside the established geofence, the transaction will be invalidated, as depicted in Figure 13(b). This measure effectively mitigates the risk of cyber fraud in the form of FakeApp attacks.

 doi:10.20944/preprints202404.0238.v1



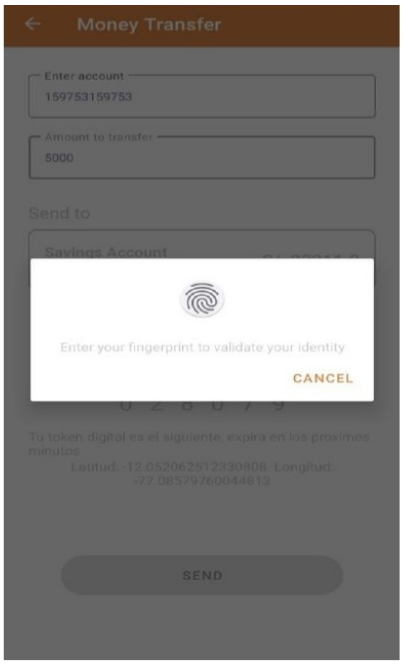
(a) Location Detection (b) Geogrid Points

Figure 11. Second layer of security.

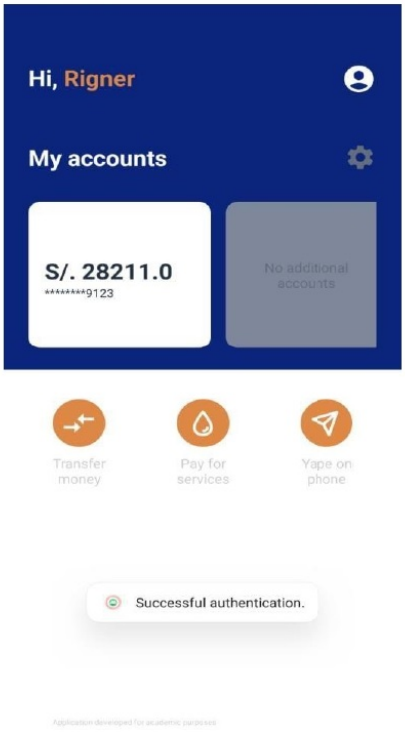
Figure 12 displays the operation of the third layer of security, which requires the user to input the bank account number and the transaction amount. To proceed with the transfer, authentication through a OTP message is necessary, as illustrated in Figure 12(a). This OTP is sent to the mobile device linked to the bank account via the registered SIM card. Additionally, fingerprint validation is conducted, as shown in Figure 12(b). The process concludes with a transfer confirmation message, exemplified in Figure 12(c). This layer effectively ensures secure transactions, incorporating both OTP and biometric verification to mitigate potential cyber fraud risks.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 3 April 2024 doi:10.20944/preprints202404.0238.v1

(a) OTP Message



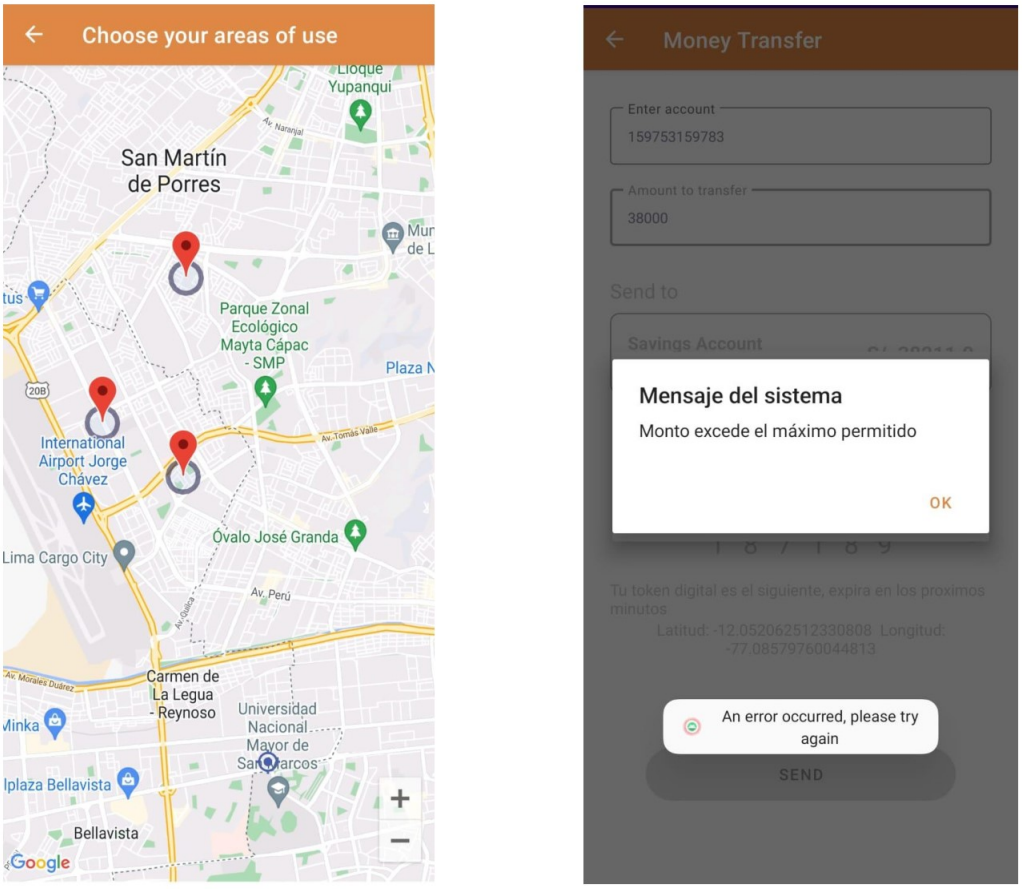
(b) Fingerprint Validation



(c) Succesful Transfer

Figure 12. Third layer of security

 doi:10.20944/preprints202404.0238.v1



(a) Far Geogrid Location (b) Invalid transfer

Figure 13. Transfer canceled by the second layer of security.

To assess the effectiveness of the proposed model, a prototype was developed for educational purposes. The integration of these security layers marks a significant advancement in safeguarding sensitive information and thwarting cyberattacks in the financial sector.

Subsequently, a field test was conducted with the participation of 50 professionals highly skilled in ICTs, as depicted in Figure 16. The application was installed on the participants' mobile devices, and attacks simulating FakeApp and SIM Swapping were executed. Following the attack, the model's ability to mitigate the attacks was evaluated through a survey administered to the participants.

The data gathered from the field survey conclusively determined the proposed model's effectiveness in mitigating two specific types of cyber fraud: FakeApp and SIM Swapping.

Firstly, the results indicated that 96.1% of the participants confirmed the model successfully mitigated a simulated FakeApp attack on their mobile devices, as illustrated in Figure 14. This high percentage of affirmative responses signifies that the implemented model was effectively able to identify and counter the threat posed by this form of cyber fraud, providing users with an additional layer of protection for their online banking operations.

 doi:10.20944/preprints202404.0238.v1

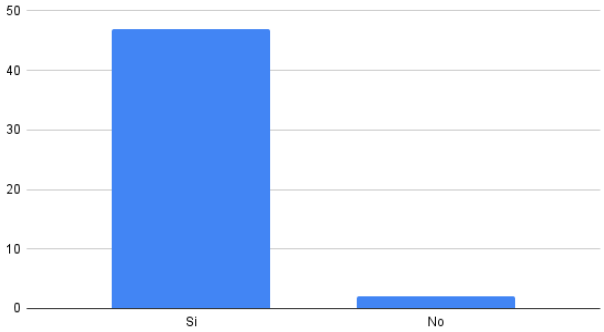


Figure 14. Survey Results About FakeApp Mitigation.

Secondly, the study revealed that 90.2% of the respondents observed the model was also effective in mitigating a simulated attack of SIM Swapping, as illustrated in Figure **??**. This figure suggests that the model is not only efficient in detecting and preventing FakeApp attacks but also can adapt and respond appropriately to other forms of cyber fraud, such as the fraudulent swapping of SIM cards, which is an increasingly common tactic among cybercriminals.

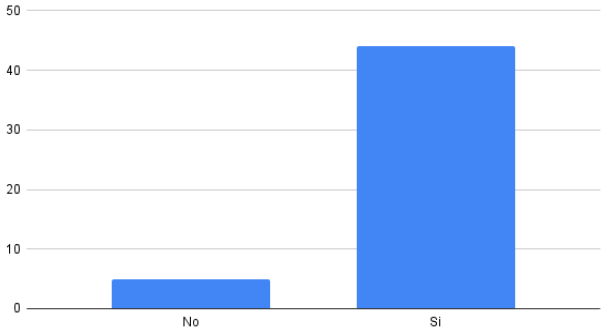


Figure 15. Survey Results on SIM Swapping Mitigation

These findings reinforce the validity and usefulness of the proposed model as an effective tool for protecting users against a variety of cyber fraud threats in the digital environment.

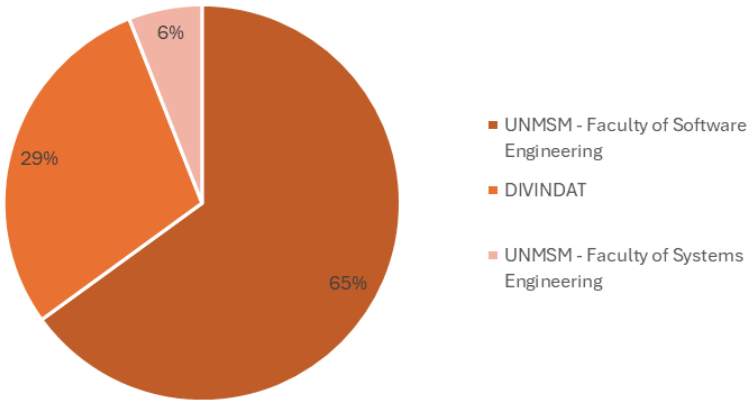


Figure 16. Survey Participants.

6. Conclusions and Future Research

Following thorough research, it has been determined that the SectraBank model represents a new alternative for reducing the increasing rate of cybercrime recorded in Peru, showcasing an efficacy of 96.1% in mitigating the cyberattack known as Fake App, and 90.2% in mitigating the cyberattack known as SIM Swapping.

 doi:10.20944/preprints202404.0238.v1

An additional contribution to the scientific community has been the establishment of the cyber fraud process as shown in Figure 6, along with the finding that Phishing is the most utilized modality by cybercriminals, with Millennials being the most prone to becoming victims of cyber fraud.

Given the demonstrated benefits of the SectraBank model in reducing cyber vulnerabilities and effectively preventing high-complexity electronic frauds in the financial system environment, a strong recommendation is made for its adoption as an additional layer of cybersecurity in the digital services offered by banking entities in the Peruvian context.

Moreover, to ensure that bank customers optimally benefit from this innovative solution, it is suggested to establish awareness, education, and training campaigns about its proper use, functionalities, and advantages in terms of privacy and financial asset protection.

Similarly, it is recommended to issue policies and guidelines for financial entities to adequately integrate the SectraBank model into their mobile applications and strengthen their authentication, monitoring, and response schemes against cyber threats.

The comprehensive adoption of this model would represent a tangible step toward a more secure and trustworthy financial system in the face of the growing risks of cybercrime reflected in the complaint records mentioned earlier.

While the SectraBank model constitutes a concrete advancement in bolstering cybersecurity within Peru's financial system, there is room for further research and expansion of this line of work, and its adaptation to financial systems in other latitudes.

It is crucial to note that the proposed model is designed with development limitations that restrict it exclusively to mobile devices operating under the Android OS, except for HUAWEI brand phones. This restriction stems from Google's sanctions against HUAWEI manufacturer, impacting the model's compatibility with such devices.

Future studies should consider integrating new biometric and artificial intelligence technologies to strengthen authentication schemes and fraud prevention, ensuring differential data privacy.

Another area for future work is to expand the model's capabilities to additionally protect transactions and operations carried out from computers and other devices, aiming to provide integral multi-platform security to financial customers.

Finally, research into the applicability of the SectraBank model, with necessary adaptations, in the context of related sectors such as fintech, digital payment methods, and governmental institutions is proposed, thereby contributing to a secure ecosystem against cybercrime.

Funding: No Aplica.

Institutional Review Board Statement: No Aplica.

Informed Consent Statement: No Aplica.

Data Availability Statement: No Aplica.

Acknowledgments: We extend our heartfelt gratitude to the creators of Google for making available a variety of functionalities that have significantly contributed to the development of our application. We also thank the diligent students of the eighth cycle of 2023 from the Universidad Nacional Mayor de San Marcos (UNMSM), whose commitment and enthusiasm have enriched this project. Our deep appreciation goes to the law enforcement officers of the DIVINDAT of the Policía Nacional del Perú for their invaluable insights and support. Their expertise and dedication to safeguarding digital integrity have been an inspiration for our work. We extend our thanks to everyone who has, in one way or another, contributed to this research. A special mention to Tomás Campana Segovia, David Morillo Acuña and Piero Paguada Tavares, whose technical skill and commitment have been pivotal in the realization of this project.

Conflicts of Interest: No Aplica.

References

1. Akande, O.N.; Gbenle, O.; Abikoye, O.C.; Jimoh, R.G.; Akande, H.B.; Balogun, A.O.; Fatokun, A. SMSPROTECT: An automatic smishing detection mobile application. *ICT Express* **2023**, *9*, 168–176. doi:https://doi.org/10.1016/j.icte.2022.05.009.
2. Mishra, S.; Soni, D. Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems* **2020**, *108*, 803–815.
3. Sahingoz, O.K.; Buber, E.; Demir, O.; Diri, B. Machine learning based phishing detection from URLs. *Expert Systems with Applications* **2019**, *117*, 345–357.
4. Ahmed, M.; Altamimi, A.B.; Khan, W.; Alsaffar, M.; Ahmad, A.; Khan, Z.H.; Alreshidi, A. PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using Machine Learning. *IEEE Access* **2023**, *11*, 61249–61263. doi:10.1109/ACCESS.2023.3287226.
5. Ren, Y.; Wang, C.; Chen, Y.; Chuah, M.C.; Yang, J. Signature Verification Using Critical Segments for Securing Mobile Transactions. *IEEE Transactions on Mobile Computing* **2020**, *19*, 724–739. doi:https://doi.org/10.1109/TMC.2019.2897657.
6. Sharma, G.; Ghosh, M. A Secure Lightweight Authentication Protocol for Mobile Payment. *Lecture Notes in Networks and Systems* **2021**, *164*, 515 – 527. Cited by: 0, doi:10.1007/978-981-15-9774-9_48.
7. Vishnuvardhan, B.; Manjula, B.; Naik, R.L. A study of digital banking: Security issues and challenges. *Advances in Intelligent Systems and Computing* **2020**, *1090*, 163 – 185. Cited by: 4, doi:10.1007/978-981-15-1480-7_14.
8. Gezer, A.; Warner, G.; Wilson, C.; Shrestha, P. A flow-based approach for Trickbot banking trojan detection. *Computers & Security* **2019**, *84*, 179–192. doi:10.1016/j.cose.2019.03.013.
9. Oh, B.; Ahn, J.; Bae, S.; Son, M.; Lee, Y.; Kang, M.S.; Kim, Y. Preventing SIM Box Fraud Using Device Model Fingerprinting. Proceedings 2023 Network and Distributed System Security Symposium. Internet Society, 2023, NDSS 2023. doi:10.14722/ndss.2023.24416.
10. Singh, M.M.; Frank, R.; Zainon, W.M.N.W. Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics* **2021**, *10*, 1658–1668.
11. Anjum, M.M.; Iqbal, S.; Hamelin, B. ANUBIS: a provenance graph-based framework for advanced persistent threat detection. Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing. ACM, 2022, SAC '22. doi:10.1145/3477314.3507097.
12. Riadi, I.; Sunardi.; Aprilliansyah, D. Analysis of Anubis Trojan Attack on Android Banking Application Using Mobile Security Labware. *International Journal of Safety and Security Engineering* **2023**, *13*, 31–38. doi:10.18280/ijsse.130104.
13. Chen, Y.; He, Y. BrutePrint: Expose Smartphone Fingerprint Authentication to Brute-force Attack, 2023. doi:10.48550/ARXIV.2305.10791.
14. Wu, P.; Liu, D.; Wang, J.; Yuan, B.; Kuang, W. Detection of fake IoT app based on multidimensional similarity. *IEEE Internet of Things Journal* **2020**, *7*, 7021–7031.
15. Mambina, I.S.; Ndibwile, J.D.; Michael, K.F. Classifying Swahili Smishing Attacks for Mobile Money Users: A Machine-Learning Approach. *IEEE Access* **2022**, *10*, 83061–83074.
16. Prayogi, A.; Aji, R.F.; others. Utilization of Mobile Network Infrastructure to Prevent Financial Mobile Application Account Takeover. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* **2023**, *7*, 797–808.
17. Al-Ahmadi, S.; Alotaibi, A.; Alsaleh, O. PDGAN: Phishing detection with generative adversarial networks. *IEEE Access* **2022**, *10*, 42459–42468.
18. Althobaiti, K.; Vaniea, K.; Wolters, M.K.; Alsufyani, N. Using Clustering Algorithms to Automatically Identify Phishing Campaigns. *IEEE Access* **2023**.
19. Liu, X.; Fu, J. SPWalk: Similar property oriented feature learning for phishing detection. *Ieee Access* **2020**, *8*, 87031–87045.
20. Sathya, R.; Kiran, U.; Chowdary, J.; Kasi, B.; Reddy, K.; Student. Detection of Phishing Attacks using Random Forest Algorithm. *International Journal of Advanced Science and Technology* **2020**, *6*, 6483–6490.
21. Castaño, F.; Fernañdez, E.F.; Alaiz-Rodríguez, R.; Alegre, E. PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification. *IEEE Access* **2023**, *11*, 40779–40789. doi:10.1109/ACCESS.2023.3268027.
22. Sameen, M.; Han, K.; Hwang, S.O. PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System. *IEEE Access* **2020**, *8*, 83425–83443. doi:10.1109/ACCESS.2020.2991403.

23. Kalabarige, L.R.; Rao, R.S.; Abraham, A.; Gabralla, L.A. Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites. *IEEE Access* **2022**, *10*, 79543–79552. doi:10.1109/ACCESS.2022.3194672.
24. Aljofey, A.; Jiang, Q.; Qu, Q.; Huang, M.; Niyigena, J.P. An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL. *Electronics* **2020**, *9*. doi:10.3390/electronics9091514.
25. *KSII Transactions on Internet and Information Systems* **2023**, *17*. doi:10.3837/tiis.2023.06.007.
26. Srokosz, M.; Bobyk, A.; Ksiezopolski, B.; Wydra, M. Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment. *Electronics* **2023**, *12*, 251. doi:10.3390/electronics12010251.
27. Moedjahedy, J.; Setyanto, A.; Alarfaj, F.K.; Alreshoodi, M. CCrFS: Combine Correlation Features Selection for Detecting Phishing Websites Using Machine Learning. *Future Internet* **2022**, *14*, 229. doi:10.3390/fi14080229.
28. Zimba, A. A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks. *International Journal of Computer Network and Information Security* **2021**, *14*, 25–39. doi:10.5815/ijcnis.2022.01.03.
29. Shaiba, H.; S. Alzahrani, J.; M. Eltahir, M.; Marzouk, R.; Mohsen, H.; Ahmed Hamza, M. Hunger Search Optimization with Hybrid Deep Learning Enabled Phishing Detection and Classification Model. *Computers, Materials & Continua* **2022**, *73*, 6425–6441. doi:10.32604/cmc.2022.031625.
30. Ghourabi, A.; Mahmood, M.A.; Alzubi, Q.M. A Hybrid CNN-LSTM Model for SMS Spam Detection in Arabic and English Messages. *Future Internet* **2020**, *12*, 156. doi:10.3390/fi12090156.
31. Sonowal, G. Detecting Phishing SMS Based on Multiple Correlation Algorithms. *SN Computer Science* **2020**, *1*. doi:10.1007/s42979-020-00377-8.
32. Sonowal, G. Phishing Email Detection Based on Binary Search Feature Selection. *SN Computer Science* **2020**, *1*. doi:10.1007/s42979-020-00194-z.
33. Ali, W.; Malebary, S. Particle Swarm Optimization-Based Feature Weighting for Improving Intelligent Phishing Website Detection. *IEEE Access* **2020**, *8*, 116766–116780. doi:10.1109/ACCESS.2020.3003569.
34. Tsinganos, N.; Mavridis, I.; Gritzalis, D. Utilizing Convolutional Neural Networks and Word Embeddings for Early-Stage Recognition of Persuasion in Chat-Based Social Engineering Attacks. *IEEE Access* **2022**, *10*, 108517–108529.
35. Tubishat, M.; Al-Obeidat, F.; Sadiq, A.S.; Mirjalili, S. An Improved Dandelion Optimizer Algorithm for Spam Detection: Next-Generation Email Filtering System. *Computers* **2023**, *12*, 196. doi:10.3390/computers12100196.
36. Stevanović, N. Character and Word Embeddings for Phishing Email Detection. *Computing and Informatics* **2022**, *41*, 1337–1357. doi:10.31577/cai_2022_5_1337.
37. Gualberto, E.S.; De Sousa, R.T.; De B. Vieira, T.P.; Da Costa, J.P.C.L.; Duque, C.G. From Feature Engineering and Topics Models to Enhanced Prediction Rates in Phishing Detection. *IEEE Access* **2020**, *8*, 76368–76385. doi:10.1109/access.2020.2989126.
38. Ejaz, A.; Mian, A.N.; Manzoor, S. Life-long phishing attack detection using continual learning. *Scientific Reports* **2023**, *13*. doi:10.1038/s41598-023-37552-9.
39. Shaukat, M.W.; Amin, R.; Muslam, M.M.A.; Alshehri, A.H.; Xie, J. A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning. *Sensors* **2023**, *23*, 8070. doi:10.3390/s23198070.
40. Maci, A.; Santorsola, A.; Coscia, A.; Iannacone, A. Unbalanced Web Phishing Classification through Deep Reinforcement Learning. *Computers* **2023**, *12*, 118.
41. Asiri, S.; Xiao, Y.; Li, T. PhishTransformer: A Novel Approach to Detect Phishing Attacks Using URL Collection and Transformer. *Electronics* **2023**, *13*, 30.
42. Su, M.Y.; Su, K.L. BERT-Based Approaches to Identifying Malicious URLs. *Sensors* **2023**, *23*, 8499.
43. Coyac-Torres, J.E.; Sidorov, G.; Aguirre-Anaya, E.; Hernández-Oregón, G. Cyberattack Detection in Social Network Messages Based on Convolutional Neural Networks and NLP Techniques. *Machine Learning and Knowledge Extraction* **2023**, *5*, 1132–1148.
44. Qi, Q.; Wang, Z.; Xu, Y.; Fang, Y.; Wang, C. Enhancing Phishing Email Detection through Ensemble Learning and Undersampling. *Applied Sciences* **2023**, *13*, 8756.
45. Moussavou Boussougou, M.K.; Park, D.J. Attention-Based 1D CNN-BiLSTM Hybrid Model Enhanced with FastText Word Embedding for Korean Voice Phishing Detection. *Mathematics* **2023**, *11*, 3217.
46. Alshammari, G.; Alshammari, M.; Almurayziq, T.S.; Alshammari, A.; Alsaffar, M. Hybrid Phishing Detection Based on Automated Feature Selection Using the Chaotic Dragonfly Algorithm. *Electronics* **2023**, *12*, 2823.
47. Alshingiti, Z.; Alaqel, R.; Al-Muhtadi, J.; Haq, Q.E.U.; Saleem, K.; Faheem, M.H. A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN. *Electronics* **2023**, *12*, 232.

48. Darem, A.A.; Alhashmi, A.A.; Alkhaldi, T.M.; Alashjaee, A.M.; Alanazi, S.M.; Ebad, S.A. Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. *IEEE Access* **2023**, *11*, 125138–125158. doi:10.1109/ACCESS.2023.3327016.
49. Roy, S.S.; Awad, A.I.; Amare, L.A.; Erkihun, M.T.; Anas, M. Multimodel phishing url detection using lstm, bidirectional lstm, and gru models. *Future Internet* **2022**, *14*, 340.
50. Elsadig, M.; Ibrahim, A.O.; Basheer, S.; Alohali, M.A.; Alshunaifi, S.; Alqahtani, H.; Alharbi, N.; Nagmeldin, W. Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction. *Electronics* **2022**, *11*, 3647.
51. Almuhaideb, A.M.; Aslam, N.; Alabdullatif, A.; Altamimi, S.; Alothman, S.; Alhussain, A.; Aldosari, W.; Alsunaidi, S.J.; Alissa, K.A. Homoglyph Attack Detection Model Using Machine Learning and Hash Function. *Journal of Sensor and Actuator Networks* **2022**, *11*, 54.
52. Panda, P.; Mishra, A.K.; Puthal, D. A Novel Logo Identification Technique for Logo-Based Phishing Detection in Cyber-Physical Systems. *Future Internet* **2022**, *14*, 241.
53. Dewis, M.; Viana, T. Phish responder: A Hybrid machine learning approach to detect phishing and spam emails, 2022. doi:https://doi.org/10.3390/asi5040073.
54. Alqahtani, H.; Alotaibi, S.S.; Alrayes, F.S.; Al-Turaiki, I.; Alissa, K.A.; Aziz, A.S.A.; Maray, M.; Al Duhayyim, M. Evolutionary Algorithm with Deep Auto Encoder Network Based Website Phishing Detection and Classification. *Applied Sciences* **2022**, *12*, 7441.
55. Mohamed, G.; Visumathi, J.; Mahdal, M.; Anand, J.; Elangovan, M. An effective and secure mechanism for phishing attacks using a machine learning approach. *Processes* **2022**, *10*, 1356.
56. Almseidin, M.; Alkasassbeh, M.; Alzubi, M.; Al-Sawwa, J. Cyber-Phishing Website Detection Using Fuzzy Rule Interpolation. *Cryptography* **2022**, *6*, 24.
57. Alarbi, A.; Albayrak, Z. Core Classifier Algorithm: A Hybrid Classification Algorithm Based on Class Core and Clustering. *Applied Sciences* **2022**, *12*, 3524.
58. Bu, S.J.; Kim, H.J. Optimized URL feature selection based on genetic-algorithm-embedded deep learning for phishing website detection. *Electronics* **2022**, *11*, 1090.
59. Seth, P.; Damle, M. A Comprehensive Study of Classification of Phishing Attacks with its AI/I Detection. 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), 2022, pp. 370–375. doi:10.1109/IIHC55949.2022.10060305.
60. Timko, D.; Rahman, M.L. Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats. Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks; Association for Computing Machinery: New York, NY, USA, 2023; WiSec '23, p. 1–12. doi:10.1145/3558482.3590173.
61. Rahman, M.L.; Timko, D.; Wali, H.; Neupane, A. Users Really Do Respond To Smishing. Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy; Association for Computing Machinery: New York, NY, USA, 2023; CODASPY '23, p. 49–60. doi:10.1145/3577923.3583640.
62. Jain, A.K.; Gupta, B.B.; Kaur, K.; Bhutani, P.; Alhalabi, W.; Almomani, A. A content and URL analysis-based efficient approach to detect smishing SMS in intelligent systems. *International Journal of Intelligent Systems* **2022**, *37*, 11117–11141, [https://onlinelibrary.wiley.com/doi/pdf/10.1002/int.23035]. doi:https://doi.org/10.1002/int.23035.
63. Armstrong, M.E.; Jones, K.S.; Namin, A.S. How Perceptions of Caller Honesty Vary During Vishing Attacks That Include Highly Sensitive or Seemingly Innocuous Requests. *Human Factors: The Journal of the Human Factors and Ergonomics Society* **2021**, *65*, 275–287. doi:10.1177/00187208211012818.
64. Park, H.; Lee, S. Countermeasures against 'SIM-Swapping' Crime through Criminal Script Analysis. *Criminal Investigation Studies* **2023**, *9*, 87–110. doi:10.46225/cis.2023.04.9.1.87.
65. Tang, C.; Chen, S.; Fan, L.; Xu, L.; Liu, Y.; Tang, Z.; Dou, L. A Large-Scale Empirical Study on Industrial Fake Apps. 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP), 2019, pp. 183–192. doi:10.1109/ICSE-SEIP.2019.00028.
66. BRĂSLAȘU, I.I.; ANDRONESCU, A.D.; NĂSTAC, D.I. Easy to Remember, Hard to Guess: A Password Generation Tool for the Digital Age. *International Conference on Cybersecurity and Cybercrime* **2023**, *10*, 113–119. doi:10.19107/CYBERCON.2023.15.

67. Tok, Y.C.; Chattopadhyay, S. Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. *Forensic Science International: Digital Investigation* **2023**, *45*, 301540. doi:10.1016/j.fsidi.2023.301540.
68. Caneppele, S.; da Silva, A., Cybercrime. In *Research Handbook of Comparative Criminal Justice*; Edward Elgar Publishing, 2022; p. 243–260. doi:10.4337/9781839106385.00024.
69. Kim, J.; Kim, J.; Wi, S.; Kim, Y.; Son, S. HearMeOut: detecting voice phishing activities in Android. Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, 2022, pp. 422–435.