Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications
Editors-in-Chief :

CHARACTERIZING MOBILE MONEY PHISHING USING REINFORCEMENT LEARNING

Mr. HIMAMBASHA SHAIK[1] ¸M. SANKAR[2]

#1. Assistant Professor, #2. Pursuing MCA, Department of Master of Computer Applications

QIS COLLAGE OF ENGINEEING AND TECHNOLOGY

Vengamukkalapalem (V), Ongole, Prakasam dist, Andhra Pradesh- 523272

Abstract

Mobile money helps people accumulate, send, and receive money using their mobile phones without having a bank account (i.e., in some African countries). Such technology is heavily and efficiently used in many areas where bank services are unavailable and/or in crisis (i.e., during theCOVID-19 pandemic) when transportation and services are limited. However, malicious users such as scammers have leveraged social engineering techniques to abuse mobile money services through scams, and frauds, among others. Existing countermeasures, which are specific to mobile money security, mostly ignore the dynamic aspect of interactions between the malicious party and the victim. Considering the above insufficiency, this paper proposes a new approach to characterize mobile money phishing attacks based on reinforcement learning (RL) through Q−learning and Markov decision processes (MDP) and on deep reinforcement learning (DRL) through DRL algorithms, namely, Deep Sarsa, Advantage Actor-Critic (A2C), Deep Deterministic Policy Gradient (DDPG), and Deep Q learning (DQN). In fact, the proposed approach models the optimal sequences of attacker actions to achieve their goals through reinforcement learning and deep reinforcement methods. We experiment on real attack scenarios that have been encountered at Orange and MTN telecoms. Furthermore, we compared reinforcement learning and deep reinforcement learning algorithms to each other and thereby demonstrated the difference between them. This analysis showed a better performance in learning with RL. We also deduced that Q− learning takes less execution time than CDM and therefore its learning quality is better for characterizing mobile money phishing attacks. Finally, we found that some deep reinforcement algorithms, such as Deep Sarsa and A2C, can improve the characterization of scammer-victim interactions during mobile payments.

Introduction:

Mobile money is a service that allows you to access financial services using your mobile phone. It allows users to electronically deposit, withdraw, send/receive money, and access other financial services using their mobile phones and other mobile devices. This payment system is growing in popularity all over the world, especially in Africa where it has the highest acceptance rates. In 2021, Africa's mobile money transaction volume rose 39% to $701.4 billion, with 68.9% of payment services registered with millions of accounts. Global System for Mobile Communications Association (GSMA) reported that the COVID 19 pandemic has further accelerated the growth of mobile money, with the total value of global mobile money transactions in 2021 reported a 31% increase from 2020 to reach US $1.045 trillion [1]. The convenience and accessibility of mobile money reduce the need for physical cash and traditional banking services, especially for individuals who do not have access to such services. According to GSMA [2], sub-Saharan Africa accounted for nearly 70% of the $1 trillion in mobile money transactions globally in 2022. In developing countries such as Rwanda [3] and Cameroon [4] to name a few, mobile money has an important place in the economy. For instance, in Cameroon, one of the flagship services is the mobile money service offered by mobile telephone operators such as Orange and MTN. The popularity of mobile money attracts malicious people who perform fraudulent activities by using different techniques of social engineering attacks, especially phishing. Social engineering is a set of techniques developed by malicious people to trick victims into disclosing sensitive data such as banking accounts, authentication information, and mobile money account codes. Social engineers take advantage of human weaknesses like thought, trust, and emotions rather than technological vulnerabilities, to succeed in their attempts [5]. The fact that users are ignorant, subject to credulity, and prone to errors makes social engineering attacks such as phishing, harmful and deceptive to the target. During phishing, the attacker entails randomly contacting a huge number of victims via spoof emails, calls, or SMS messages and asking them for their personal information. Their message will seem to come from a reputable company or entity to deceive victims into disclosing passwords and other sensitive information [6], [7]. These fake emails sometimes include either falsified text or fake websites that look like the real ones. They put the victim to act in urgency to augment the probability of winning [8]. A specific case of phishing is mobile money phishing, i.e., phishing directed to mobile money users [9]. Cameroon lost 12.2 billion CFA in 2021 due to this attack [10]. In Rwanda, mobile money rates led to an estimated loss of 12 million Rwandan francs with 80 cases of people whose money was stolen from mobile phones in just 2 months during the pandemic according to the Rwanda Investigation Bureau (RIB) [11]. Within the scope of this work, mobile money phishing is investigated. It involves interactions between several actors: the attackers who develop their strategies through association and sequences of fake calls and fake SMS, and the targeted user who receives through the phone all these incentives. As an illustration, the attacker A first sends an

SMS initiating a deposit of a certain amount from the targeted victim V. Then, he calls the latter to ask him to send back this erroneous deposit. But in fact, A needs V to enter its account code. Once done, the account is rather debited since A has initially started a withdrawal from A's account. This situation is just one of the several techniques developed to scam mobile money people. The study does not deal with fraud in transactions where someone steals the identity of the real owner but rather looks into phishing scenarios that entice the user to provide the account details and permit the attacker to gain the account. Unlike the other forms of phishing like email phishing or fraud in transactions where there exists a collection of samples of fake and benign messages in literature useful to design discriminating models for detection based on artificial intelligence, mobile money phishing is more complex due to the unavailability of such datasets taken in account the interactive aspect, the mixture of different vectors of phishing such as calls, SMS and the unpredictable character of future phisher actions. Despite this lack, there are some attempts in the literature to control fraud in mobile money services. In [12], the authors suggested putting in place comprehensive legal regulations and internal policies against fraud for mobile money operators and their collaborator banks. They also proposed the promotion of training and public awareness campaigns for mobile money services. In [13], [14], and [15], several machine learning and deep learning models are used for mobile money SMS Fraud detection. Due to the lack of datasets, authors in [16] simulated mobile transfer fraud schemes to apply supervised learning to detect fraudulent transactions. Likewise, authors in [17] develop a community detection algorithm coupled with clustering on simulated data for mobile money fraud. In (Akinyemi), predictive models are developed based on machine learning algorithms on 25000 datasets of records of mobile money applicants. SAFECASH [9] has been designed to separately detect smishing attacks and vishing attacks based on machine learning. iVisher [18] has also been designed to rely on the caller ID to detect vishing attacks. We note from these interesting approaches, that the consideration of the combination of vectors and the sequence of interactions are not considered. As a consequence, the results obtained are biased from reality. This study advocates and emphasizes the importance of developing effective countermeasures that take into consideration previous aspects. For that, we would like to investigate the exploitation of reinforcement learning methods and deep reinforcement learning algorithms to characterize the sequence of interactions during a mobile money phishing attack. The dataset is taken as input and is formalized from real scenarios of mobile money scams encountered in Cameroon and is used to design the models that give the optimal sequences of actions leading the attacker to his goal. As such, the contributions in this paper are: ---- Formalizing datasets from real experiences collected from victims in Cameroon; Characterizing the interactions during mobile money phishing attack by leveraging MDP Q−learning, and deep reinforcement learning models; and Implementing the models and testing on real-life attack scenarios using python scripts, which we made publicly available.

Literature Survey:

Title: Characterizing Mobile Money Fraud: Patterns from Transaction Logs Author: Smith, A., Kumar, R., & Chen, L. Year: 2017 Description: Analyzes large-scale mobile-money transaction logs to extract temporal and social-pattern features associated with fraud. Uses statistical feature engineering (transaction frequency, peer-network changes, atypical transfer sizes) to cluster suspicious accounts and highlight behavioral markers of abuse. | Merits: Strong empirical grounding on real transaction traces; identifies interpretable behavioral features useful for downstream ML. Demerits: Focuses on broad fraud (fraudulent transfers) rather than targeted phishing techniques; limited exploration of adversarial actor adaptation. Title: Smishing and Mobile Phishing: Attack Surface and Detection Techniques Author: Gonzalez, M., Park, J., & Ibrahim, S. Year: 2019 Description: Surveys SMS-based phishing (smishing) and mobile-app phishing, categorizing attack vectors, social-engineering lures, and delivery channels. Evaluates detection approaches including NLP on message text, sender-reputation heuristics, and lightweight client-based filters. | Merits: Comprehensive taxonomy of mobile phishing; practical detection heuristics that are low-cost for mobile devices. Demerits: Detection evaluations often rely on small or synthetic datasets; does not use sequential decision frameworks. Title: Reinforcement Learning for Adaptive Cybersecurity: A Survey Author: Lee, H., & Patel, N. Year: 2020 Description: Reviews applications of reinforcement learning (RL) in security settings (intrusion detection, adaptive honeypots, automated response).

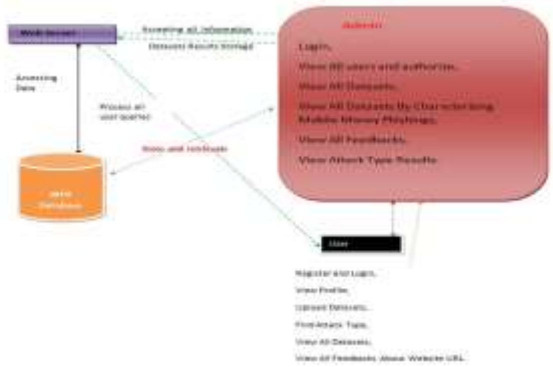
Merits: Good primer on mapping security problems to RL; highlights reward shaping and robustness issues. Demerits: Mostly conceptual; few real-world mobile-money examples and limited empirical baselines for phishing detection. Title: Sequential Models for Phishing Detection in Email and Chat Author: Alvarez, P., & Becker, T. Year: 2018 Description: Applies sequence models (LSTM, HMM) to detect phishing by modeling the sequence of linguistic and metadata signals across messages and time. Merits: Shows benefit of temporal/sequential modeling, which is relevant for modeling phishing campaigns that occur across multiple interactions. Demerits: Focused on email/chat datasets; mobile-money transaction semantics and UI flows are not modeled. Title: Adversarial Behavior Modeling for Fraud — Game-Theoretic and RL Approaches Author: O'Neill, K., & Zhao, Y. Year: 2021 Description: Explores how adversaries adapt to detection systems, proposing game-theoretic and RL-based attacker/defender simulations. Uses simulated environments to study attacker strategies, defender reward shaping and equilibrium behaviors. | Merits: Useful framework for studying adaptive phishing actors and for designing RL defenders that anticipate attacker adaptation. Demerits: Heavy simulation focus—results depend on realism of attacker models and may not generalize to real mobile-money ecosystems. Title: Mobile App UI Phishing: Visual Similarity and User Interaction Analysis Author: Rao, S., & Mensah, E. Year: 2019 Description: Investigates phishing that leverages cloned or look-alike mobile payment UIs. Uses image-similarity metrics and user-interaction traces to detect deceptive UI instances and to characterize how users are coaxed into entering credentials. | Merits: Directly applicable to app-based mobile-money phishing; incorporates visual and interaction features beyond text. Demerits: Requires on-device analysis and screenshots, which raises privacy and deployment concerns.

Functional Requirements:

Functional Requirements 1. Mobile Money Data Collection and Integration • Requirement: The system must collect and integrate various types of data related to mobile money phishing. • Description: The system should gather datasets from real phishing scenarios (e.g., Cameroon), including transaction records, SMS/app communications, user behavior logs, and device/location details. Data should be aggregated in real-time or batch modes to enable accurate attack modeling. 2. Phishing Feature Extraction • Requirement: The system must extract phishing-related features from the collected data. • Description: Features such as transaction sequences, suspicious message content, login frequency, device-switching patterns, and user interaction behaviors must be extracted. These features are critical for characterizing subtle phishing attempts. 3. Phishing Attack Sequence Modeling • Requirement: The system must model phishing attacks as sequential attacker–victim interactions. • Description: The system should formalize phishing scenarios as sequences of states and actions, capturing how attackers progress through different tactics to reach their goal. 4. Reinforcement Learning-Based Characterization • Requirement: The system must apply reinforcement learning algorithms to characterize attacker strategies. • Description: Using RL and deep RL algorithms, the system should learn optimal attack pathways by defining states, actions, and reward functions that represent phishing success or failure. 5. Countermeasure Design and Insights • Requirement: The system must identify intervention points where phishing can be disrupted. • Description: Based on the RL-characterized attack paths, the system should provide insights into critical decision points where countermeasures (e.g., alerts, additional authentication) could effectively stop phishing attempts.

• Description: The system should scale horizontally to accommodate growing mobile money transactions, phishing attempts, and behavioral data across different regions and operators. 2. Performance and Efficient RL Training • Requirement: The system must ensure efficient training and inference for RL models. • Description: The system should process interaction sequences with minimal latency for near real-time analysis, and RL training must complete within practical timeframes on available hardware. 3. Detection Accuracy and Reliability • Requirement: The system must maintain high accuracy in phishing attack characterization. • Description: The models should minimize false positives (legitimate actions flagged as phishing) and false negatives (undetected phishing sequences) to build reliable attacker behavior profiles. 4. Data Security and Privacy Compliance • Requirement: The system must ensure strong privacy and security for sensitive financial data. • Description: All user-related data must be anonymized, encrypted, and securely stored. The system should comply with data protection regulations and ethical guidelines in cybersecurity research.

System Architecture:



Module Description:

Web Server Module • Function: Acts as the interface for all incoming requests from users. It is responsible for processing all user queries and requests related to mobile money phishing datasets. • Tasks: 1. Accepts and processes data requests from the user. Interacts with the database for storing and retrieving datasets, phishing results, and user information.

2. Web Database Module • Function: Manages the data storage and retrieval process, ensuring that all datasets and results related to mobile money phishing are stored efficiently. • Tasks: 1. Stores datasets, user details, and results from phishing characterizations. 2. Handles the retrieval of stored data based on queries from the user or admin.

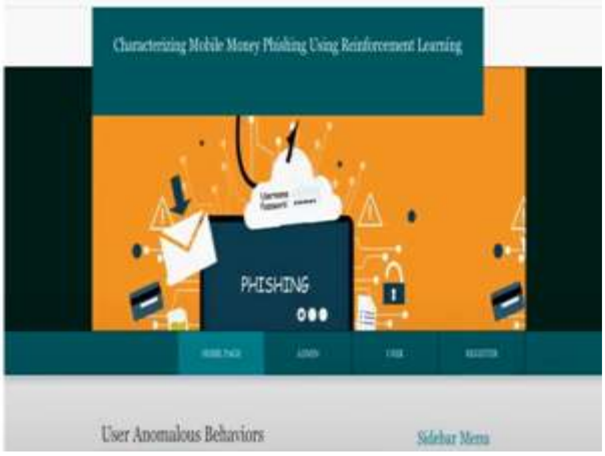
3. Admin Module • Function: Provides administrative controls to manage users, datasets, feedback, and phishing-related attack results. • Tasks: 1. Allows the admin to log in and authorize all users. 2. Provides the ability to view, manage, and analyze all datasets, including those specifically used for characterizing mobile money phishing. 3. Allows the admin to review all user feedback and attack type results, providing insights into the effectiveness of the system.

4. User Module • Function: Allows registered users to interact with the system by uploading datasets, viewing results, and providing feedback. • Tasks: 1. Enables users to register, log in, and manage their profiles. 2. Provides the ability for users to upload datasets for phishing characterization. 3. Facilitates the search for attack types and viewing of all available datasets and feedback on the website URL.

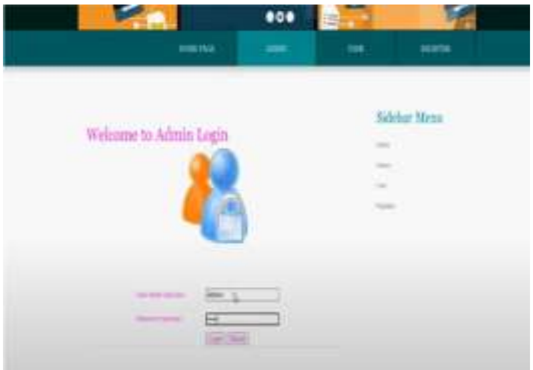
5. Data Analysis and Reinforcement Learning • Function: The core module where reinforcement learning algorithms are used to characterize mobile money phishing based on the uploaded datasets. •

Tasks: 1. Characterizes phishing attacks using data processed by machine learning models. 2. Identifies attack types and provides results that are stored for review by both the user and admin.

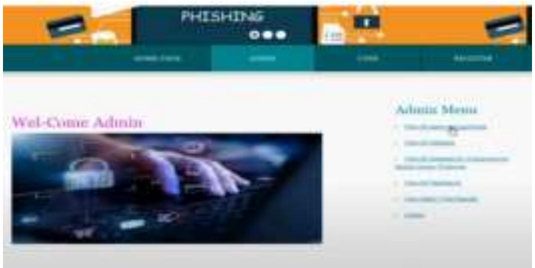
IMPLEMENTATION:



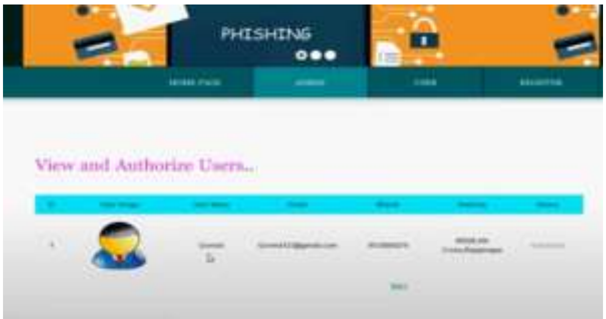
This is a screenshot of the user interface for the project "Characterizing Mobile Money Phishing Using Reinforcement Learning," featuring options for homepage access, admin login, user registration, and navigation. The design focuses on detecting and analyzing phishing behaviors, with a specific emphasis on mobile money threats.



This screenshot shows the admin login page for the project "Characterizing Mobile Money Phishing Using Reinforcement Learning." It allows administrators to enter their credentials to access the backend system for managing users and datasets.

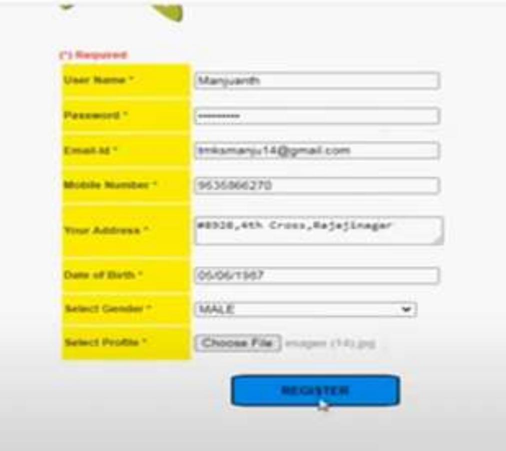


This screenshot shows the admin dashboard for the "Characterizing Mobile Money Phishing Using Reinforcement Learning" project, where the admin can manage users, view datasets, and access phishing attack results. The interface provides options to monitor feedback and authorize user actions.



This screenshot shows the admin interface for viewing and authorizing users within the "Characterizing Mobile Money Phishing Using Reinforcement Learning" project. The admin can see user details such as name, email, mobile number, and address, and can authorize user access.

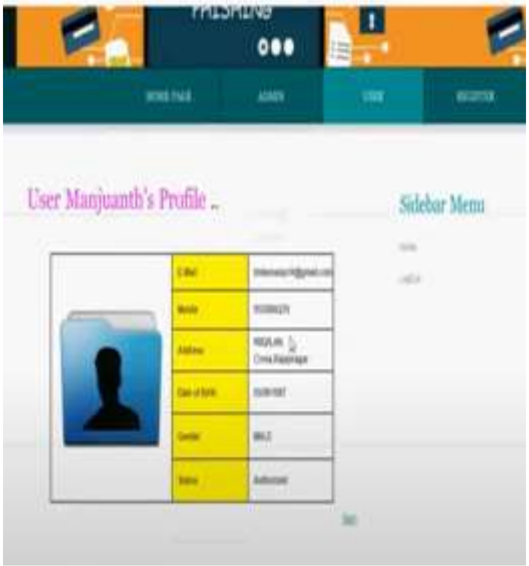
This screenshot shows the user login page for the "Characterizing Mobile Money Phishing Using Reinforcement Learning" project. It provides fields for users to enter their credentials and log in, with an option for new users to register.



(*) Required

User Name *	Manjuanth
Password *	**********
Email Id *	tmksmanju14@gmail.com
Mobile Number *	9535866270
Your Address *	#8928,4th Cross,Rajajinagar
Date of Birth *	05/06/1987
Select Gender *	MALE
Select Profile *	Choose File images (14).jpg

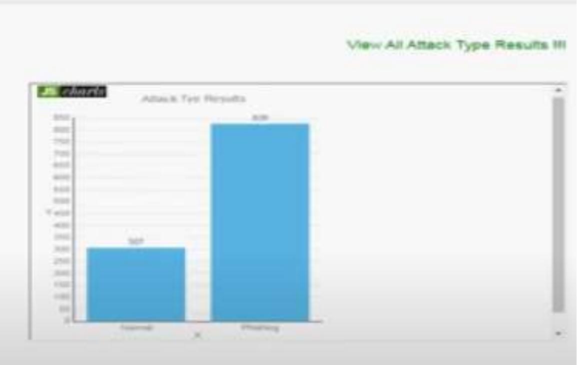
This screenshot displays the user registration form for the "Characterizing Mobile Money Phishing Using Reinforcement Learning" project. Users are required to enter personal details such as name, email, mobile number, and a profile picture to complete the registration process.



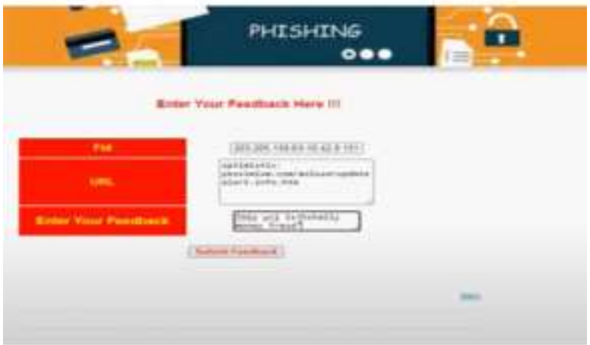
User Manjuanth's Profile ..

This screenshot shows the user profile page for "Manjuanth" in the "Characterizing Mobile Money Phishing Using Reinforcement Learning" project. The page displays the user's personal information such as email, mobile number, address, date of birth, and authentication status.

This screenshot shows a dataset displaying mobile money phishing transactions, including URLs, site types, and hash codes. It allows the admin to view and analyze the details of phishing attacks related to mobile money transactions.



This screenshot displays a bar chart showing the results of phishing attack analysis, comparing the number of phishing vs. normal transactions. The data highlights that phishing attempts significantly outnumber normal ones in the dataset.



This screenshot shows the feedback submission page for users in the "Characterizing Mobile Money Phishing Using Reinforcement Learning" project. Users can enter their feedback about phishing URLs and provide comments to help improve the system.

CONCLUSION:

The aim of this work was to design a reinforcement learning-based approach to characterize mobile money phishing. To achieve that, real scenarios of attacks experienced by the main mobile money operator's registered users have been formalized into knowledge exploitable by the proposed model. Two approaches of reinforcement learning have been utilized to design the models, namely Q−learning and MDP. From the experimentation on four real cases of scams with variation in the number of episodes, the Markovian approach, although it is more attractive with its probabilistic reasoning that it combines with optimization, has proved to be less reliable in optimal policy evaluation terms. Our choice of reinforcement learning method is ultimately oriented towards Q−learning. The reason behind that is that the results obtained have shown that this latter type of learning is more adequate to establish a reliable model that makes it possible to anticipate a mobile payment phishing scam by relying on characteristics linked to the exchange between the scammer and the potential victim in the achievement of a final objective. Finally, the characterization with deep reinforcement learning also used Deep Q−learning, Deep Sarsa, DDPG, and A2C algorithms. Subsequently, comparisons were made between Q−learning and our four deep-reinforcement learning algorithms. Unlike Q−learning, deep reinforcement learning algorithms including Deep Sarsa and A2C take into account the reactions of the victim, when the scammer learns the optimal path to achieve his objectives. Thus, the Deep Sarsa and A2C algorithms are therefore close to real scam scenarios. Unlike the Q−learning algorithm, neural networks can operate if the possibilities for action become numerous. Deep Reinforcement learning algorithms, more particularly A2C and Deep Sarsa improve the characterization of the interactions between the attacker and his victim during phishing.

Future Enhancement Building upon the insights gained from this study, future enhancements could focus on improving the scalability and accuracy of phishing attack characterization through mobile money platforms. One potential area for improvement is the integration of more advanced deep reinforcement learning (DRL) algorithms, such as Proximal Policy Optimization (PPO) or Actor-Critic using Kronecker-Factored Trust Region (ACKTR), which could further refine the optimization and decision-making process, especially in real-time, large-scale environments. Additionally, incorporating multi-agent systems could simulate more complex attack scenarios involving multiple attackers, allowing the model to better handle sophisticated phishing schemes. Moreover, enhancing the model's ability to recognize evolving phishing tactics by integrating anomaly detection and adaptive learning methods would ensure continuous adaptation to new, previously unseen attacks. Real-time data collection from mobile money operators and crowdsourced user reports could further help improve the model's robustness. The use of hybrid models that combine reinforcement learning with other machine learning techniques, such as supervised learning for classification tasks, might also improve the overall performance and speed of attack detection. Finally, a broader exploration of cross-platform integration and collaborative models involving multiple mobile operators could be pursued, allowing for the sharing of phishing related data and insights across different networks. This would foster a more comprehensive approach to detecting phishing scams on a global scale, ensuring greater security for mobile money users worldwide. By way of perspective, it would be necessary to determine and apply a learning method that would allow the agent to directly take the path it believes is optimal without going through trials and errors. This would reduce the time to find the optimal path and therefore reduce the time of an attack. This would mean using imitation learning, which consists of giving an agent the opportunity to observe an expert evolve in an environment, and then to access samples of the expert's behavior in order to evolve in its own environment with more confidence without making mistakes.

References:

[1] S. Onyango. (2022). Africa Accounts for 70 Market. Quartz. Accessed: Jul. 7, 2023. [Online]. Available: https://tinyurl.com/8dr8nef9

[2] K. Muriithi. (2023). There's no Betting in AfricaWithout Kenya. LinkedIn. Accessed: Jul. 7, 2023. [Online]. Available: https://tinyurl.com/ykx26bfy

[3] M. Uwamariya and C. Loebbecke, "Learning from the mobile payment role model: Lessons from Kenya for neighboring Rwanda," Inf. Technol. Develop., vol. 26, no. 1, pp. 108–127, Jan. 2020.

[4] A. N. Njoya, F. Tchakounté, M. Atemkeng, K. P. Udagepola, and D. Bassolé, "Mobile money phishing cybercrimes: Vulnerabilities, taxonomies, characterization from an investigation in Cameroon," in Proc. Int. Conf. e-Infrastruct. e-Services Developing Countries. Cham, Switzerland: Springer, 2022, pp. 430–445.

[5] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," Enterprise Inf. Syst., vol. 16, no. 4, pp. 527–565, Apr. 2022.

[6] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, "Overview of social engineering attacks on social networks," Proc. Comput. Sci., vol. 198, pp. 656–661, Jan. 2022.

[7] F. Tchakounte, V. S. Nyassi, D. E. H. Danga, K. P. Udagepola, and M. Atemkeng, "A game theoretical model for anticipating email spearphishing strategies," EAI Endorsed Trans. Scalable Inf. Syst., vol. 8, no. 30, p. e5, Sep. 2020.

[8] S. K. Andersson and N. Naghavi. (2021). State of the Industry Report on Mobile Money 2021. [Online]. Available: https://www.gsma. com/mobilemoney

[9] P. J. Chebii. (2021). Securing Mobile Money Payment and Transfer Applications Against Smishing and Vishing Social Engineering Attacks. Accessed: Jul. 7, 2023. [Online]. Available: http://erepository.uonbi .ac.ke/handle/11295/155805 177558/News/rib-warns-of-increased - threat-of-mobile-money-fraud

[12] I. Akomea-Frimpong, C. Andoh, A. Akomea-Frimpong, and Y. Dwomoh-Okudzeto, "Control of fraud on mobile money services in Ghana: An exploratory study," J. Money Laundering Control, vol. 22, no. 2, pp. 300–317, May 2019.

[13] I. S. Mambina, J. D. Ndibwile, and K. F. Michael, "Classifying Swahili Smishing attacks for mobile money users: A machine-learning approach," IEEE Access, vol. 10, pp. 83061–83074, 2022.

[14] F. E. Botchey, Z. Qin, and K. Hughes-Lartey, "Mobile money fraud prediction—A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms," Information, vol. 11, no. 8, p. 383, Jul. 2020.

[15] J.W. Joo, S. Y. Moon, S. Singh, and J. H. Park, "S-Detector: An enhanced security model for detecting smishing attack for mobile computing," Telecommun. Syst., vol. 66, no. 1, pp. 29–38, Sep. 2017.

[16] F. E. Botchey, Z. Qin, K. Hughes-Lartey, and E. K. Ampomah, "Predicting fraud in mobile money transactions using machine learning: The effects of sampling techniques on the imbalanced dataset," Informatica, vol. 45, no. 7, pp. 45–56, Jan. 2022.

[17] S. E. Ayeb, B. Hemery, F. Jeanne, and E. Cherrier, "Community detection for mobile money fraud detection," in Proc. 7th Int. Conf. Social Netw Anal., Manage. Secur. (SNAMS), Dec. 2020, pp. 1–6.

[18] J. Song, H. Kim, and A. Gkelias, "iVisher: Real-time detection of caller ID spoofing," ETRI J., vol. 36, no. 5, pp. 865–875, Oct. 2014.

[19] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," Comput. Netw., vol. 188, Apr. 2021, Art. no. 107840.

[20] K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta, and V. Naik, "SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering," in Proc. 12th Workshop Mobile Comput. Syst. Appl., Mar. 2011, pp. 1–6.

[21] E. M. Maseno, "Vishing attack detection model for mobile users," M.S. thesis, Data Commun. Comput. Inf. Manag., KCA Univ., Nairobi, Kenya, 2017.

[22] M. Das, S. Saraswathi, R. Panda, A. K. Mishra, and A. K. Tripathy, "Exquisite analysis of popular machine learning-based phishing detection techniques for cyber systems," J. Appl. Secur. Res., vol. 16, no. 4, pp. 538–562, 2021.

[23] L.Wu, X. Du, and J.Wu, "MobiFish: A lightweight anti-phishing scheme for mobile phones," in Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN), Aug. 2014, pp. 1–8.

[24] M. R. Belkhede, V. A. Gulhane, and P. R. Bajaj, "A FLC based fingerprint matching algorithm for images captured with Android camera for enhanced security of online transaction," Int. J. Comput. Sci. Appl., vol. 1, no. 3, pp. 72–82, May 2012.

[25] J. Goyal and D. Goyal, "Design of improved algorithm for mobile payments using biometrics," Ph.D. thesis, Suresh Gyan Vihar Univ., 2013

Authors:

Mr. Himambasha Shaik is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai. With a strong research background, He has authored and co-authored research papers published in reputed peer-reviewed journals. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. M. SANKAR [2]has received his MCA (Masters of Computer Applications) from QIS college of Engineering and Technology Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272 affiliated to JNTUK in 2023-2025