Unveiling Moblie Money Phishing Scam Employing Reinforcement Learning Strategies

T Sundararajulu [1], Y Ujiviutha[2], P Lakshman sai kiran[3], E Arun[4], K lokesh[5], L.G.Kavitha[6]

[1] *Research Scholar, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India*
[2] *Assistant Professor, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India*

ABSTRACT

This abstract explores the widespread use of mobile money in regions lacking traditional banking infrastructure. Despite its efficiency, the technology faces challenges from malicious actors who exploit social engineering for scams and frauds in the absence of robust security measures. Addressing this gap, the paper introduces a fresh approach employing reinforcement learning techniques like Q-learning and Markov decision processes, along with deep reinforcement learning algorithms such as deep Q-learningThe proposed method aims to create models that understands and counteract phishing attacks by identifying optimal sequences of attacker actions through reinforcement learning and deep reinforcement methods. Real-world attack scenarios encountered at Orange and MTN telecoms are used for experimentation, comparing the effectiveness of reinforcement learning and deep reinforcement learning algorithms. RL exhibited better learning performance compared to DRL.Q-learning was found to have superior learning quality and faster execution time than certain DRL algorithms. Also, Some DRL algorithms were identified as beneficial in improving the understanding of scammer-victim interactions during mobile payments..

Keyword: -*Moblie,Money,Publishing, Frauds*

1. INTRODUCTION

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 . 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 . These fake emails sometimes include either falsified text or fake websites that look like the real ones 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. 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 of road situation

2. LITERATURE SURVEY

Authors: Sourabh singh and J Wang. Tittle: "S-detector : an enhanced security model for detecting smishing attack for mobile computing": Naive Bayes classifier Approach.Published in 2018.S-detector : an enhanced security model for detecting smishing attack for mobile computingThis paper proposed model is applied to a Naive Bayes classifier to improve the Smishing attack detection in smart devices[1]
Authors: F Micheal and Iddi S. Tittle: "Classifying swahili smishing attacks for mobile money users ": A machine-learning approach.Published in 2022.Classifying swahili smishing attacks for mobile money users : A machine-learning approach. This study proposes a machine-learning based model to classify Swahili Smishing text messages targeting mobile money users..[2]
Authors: Safa Ayeb. Tittle: "Community detection for mobile money fraud detection."Published in 2021Community detection for mobile money fraud detection. The main idea can be expressed as a community detection issue in a real network containing data from a telecommu- nications operator. More precisely, mobile money transactions will be studied.[3]
Authors: Kuldeep Yadav and Atul Goyal. Tittle: "Smsassassin : Crowdsourcing driven mobile-based system for sms spam filtering". Published in 2019 Smsassassin : Crowdsourcing driven mobile-based system for sms spam filtering. A mobile-based system SMSAssassin that can filter SMS spam messages based on bayesian learning and sender blacklisting mechanism and uses crowd sourcing to keep itself updated is developed.

.[4]

Authors: Sandeep Roy and Ashok Das. Tittle: "Aspa-mosn : An efficient user authentication scheme for phishing attack detection in mobile online social network."Published in 2022.Aspa-mosn : An efficient user authentication scheme for phishing attack detection in mobile online social network. propose a secure and lightweight cryptography-based authentication scheme, called authentication scheme for phishing attack (ASPA)-mobile online social network that provides resistance to phishing and other related attacks in OSNs.
.[5]

3. METHODOLOGY

3.1EXISTING SYSTEM

In Existing system, Deep learning techniques were used by to implement them on the CSE-CIC-IDS2018 and Bot-IoT datasets. These techniques included recurrent neural networks (RNN), deep neural networks (DNN), restricted Boltzmann machines (RBM), deep belief networks (DBN), convoluted neural networks (CNN), deep Boltzmann machines (DBM), and deep autoencoders (DA). Then, the classification times of various data sets and the classification success of deep learning are contrasted. Also, 35 attack detection data sets that were used in the literature were categorized as part of their study's examination of intrusion detection systems based on deep learning techniques. Furthermore, proposed S-Detector, a security model to detect and block smishing messages. The Naive Bayesian Classifier was used to differentiate smishing messages from benign ones by retrieving keywords that are most often used in smishing messages. Moreover, proposed SMSAssassin, a mobile application for filtering spam messages based on Bayesian learning. This SVM technique is leveraged with Bayesian learning to achieve greater results (i.e., precision). Users with the SMSAssassin app on their mobile phones can share the reported spam list.

.

3.1.1DISADVANTAGES OF EXISTING SYSTEM

- An existing system doesn't have particular form of spear phishing which is unique. When the attacker has enough information about the target, he or she uses it to launch the attack after spending a lot of time and effort to obtain it.
- Before launching the attack, it may take some time to gain the trust of the victim

3.2 PROPOSED METHODOLOGY

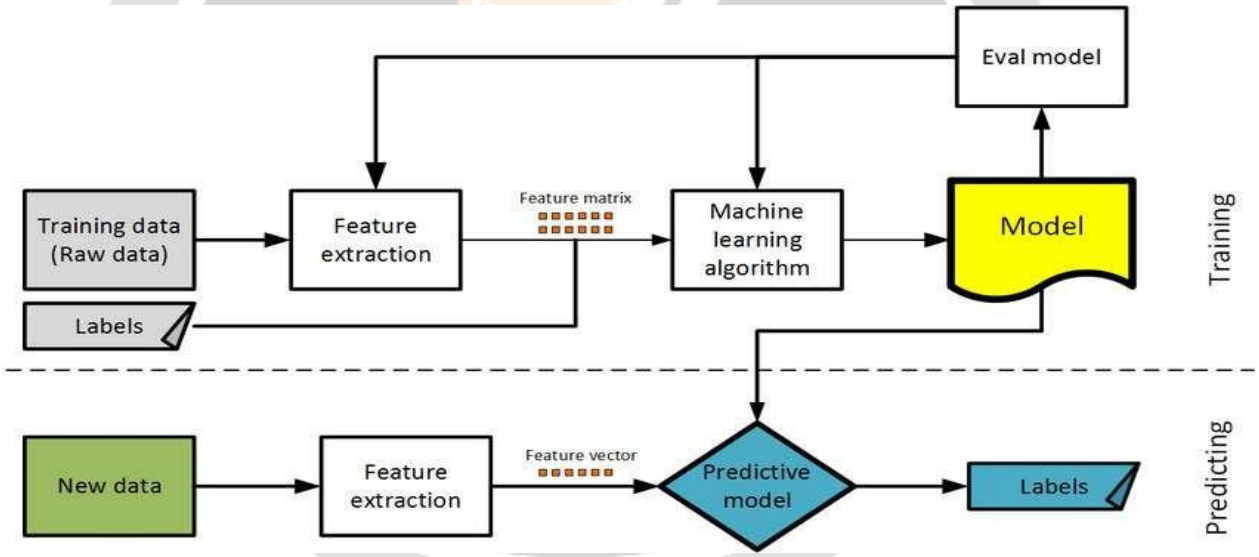
Formalizing datasets from real experiences collected from victims in CameroonCharacterizing the interactions during mobile money phishing attack by leveraging MDP Q−learning, and deep reinforcement learning modelImplementing the models and testing on real-life attack scenarios

.

4. SYSTEM DESIGN

It is a process of planning a new business system or replacing an existing system by defining its components or modules to satisfy the specific requirements. Before planning, you need to understand the old system thoroughly and determine how computers can best be used in order to operate efficiently.

4.1 SYSTEM ARCHITECTURE



4.2 MODULES

In this Proposed System, There are two Modules. They are:

1. Admin
2. Remote User

4.2.1 ADMIN

This system should provide the admikn with the convenience of providing trainingand testing of dataset

- Login
- View all user and authorize
- View all data sets

- View all data sets by characterizing mobile money
- View all feedback
- View attack type result
- Logout

4.2.2 REMOTE USER

This system should help the user by registering with his basic details that can be stored inthe database and it provides the following such as

- Register
- Login
- View profile
- Upload datasets
- View all datasets
- View all feedbacks about website
- Logout

5. RESULTS AND PERFORMANCE

EXECUTION PROCEDURE

The Execution procedure is as follows:

1. In this research work with data with attributes are observable and then all of them are floating data. And there's a decision class/class variable. This data was collected from Kaggle machine learning repository.
2. In this research 70% data use for train model and 30% data use for testing purpose.
3. RF is used as Classifier.
4. In the classification report we were able to find out the desired result
5. In this analysis the result depends on some part of this research. However, which algorithm gives the best true positive, false positive, true negative, and false negative are the best algorithms in this analysis.

Fig. Home page

Fig. Admin login page

Fig. Admin home page

Fig. Veiw all user

Fig.Veiw all datasets

Fig. Find attack type results

6. 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. Our choice of reinforcement learning method is ultimately oriented towards 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.

.

7. REFERENCE

[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