AntiPhiMBS-TRN: A New Anti-phishing Model to Mitigate Phishing Attacks in Mobile Banking System at Transaction Level

Tej Narayan Thakur and Noriaki Yoshiura(✉)

Department of Information and Computer Sciences, Saitama University,
Saitama 338-8570, Japan
yoshiura@fmx.ics.saitama-u.ac.jp

Abstract. With the continuous improvement and growth at a rapid pace in the utility of mobile banking payment technologies, fraudulent mobile banking transactions are being multiplied using bleeding-edge technologies sharply and a significant economic loss is made every year around the world. Phishers seek new vulnerabilities with every advance in fraud prevention and have become an even more pressing issue of security challenges for banks and financial institutions. However, researchers have focused mainly on the prevention of fraudulent transactions on the online banking system. This paper proposes a new anti-phishing model for mobile banking systems at the transaction level (AntiPhiMBS-TRN) that mitigates fraudulent transactions in the mobile banking payment system. This model applies a unique id for the transactions and an application id for the bank application known to the bank, bank application, users, and the mobile banking system. In addition, AntiPhiMBS-TRN also utilizes the international mobile equipment identity (IMEI) number of the registered mobile device to prevent fraudulent transactions. Phishers cannot execute fraudulent transactions without knowing the unique id for the transaction, application id, and IMEI number of the mobile device. This paper employs a process meta language (PROMELA) to specify system descriptions and security properties and builds a verification model of AntiPhiMBS-TRN. Finally, AntiPhiMBS-TRN is successfully verified using a simple PROMELA interpreter (SPIN). The SPIN verification results prove that the proposed AntiPhiMBS-TRN is error-free, and banks can implement the verified model for mitigating fraudulent transactions in the mobile banking system globally.

Keywords: Mobile banking system · Fraudulent transaction · Anti-phishing model · Verification

1 Introduction

The “Mobile Banking System” in this paper referes to the concept of a mobile banking system in general. With the advancement of mobile technologies, most modern commerce payments depend on the mobile banking system that is always open 24/7, 365 days

N. T. Nguyen et al. (Eds.): ACIIDS 2022, LNAI 13758, pp. 595–607, 2022.
https://doi.org/10.1007/978-3-031-21967-2_48

a year for financial transactions. However, the unfortunate truth is that fraudulent transactions are also around-the-clock operations. With the continuous improvement and growth at a rapid pace in the utility of mobile banking payment technologies, fraudulent mobile banking transactions are being multiplied using bleeding-edge technologies sharply and a significant economic loss is made every year around the world. 2019 Iovation financial services fraud and consumer trust report [24] show that 61% of financial transactions originate from mobile and 50% of suspected fraudulent transactions seen by Iovation are from mobile devices. Fraudsters seek new vulnerabilities with every advance in fraud prevention and have become an even more pressing issue of security challenges for banks and financial institutions. Fraud-the Facts 2021 [25] revealed that mobile banking fraud losses increased by 41% in 2020 in the UK.

Mobile banking users download phishing apps unknowingly, install them on their mobile devices, and input login credentials (Username and password) in the phishing app unintentionally. They follow the links in the phishing emails/SMS and are redirected to the phishing login interface, and they input the login credentials in the phishing login interface. Thus, phishers steal login credentials using phishing apps or phishing login interfaces from mobile banking users and employ the stolen login credentials to login into the mobile banking system. As the login credentials are valid, phishers login into the mobile banking system. Phishers request a transaction, and MBS sends a one-time password (OTP) for the security of the transaction. However, phishers reply to the OTP, and they execute the fraudulent transactions as shown in the threat model in Fig. 1.

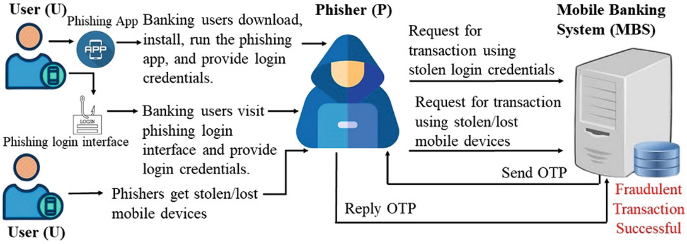
User (U)
Phishing App
APP
Banking users download, install, run the phishing app, and provide login credentials.
LOGIN
Phishing login interface
Banking users visit phishing login interface and provide login credentials.
User (U)
Phishers get stolen/lost mobile devices
Phisher (P)
Request for transaction using stolen login credentials
Request for transaction using stolen/lost mobile devices
Send OTP
Reply OTP
Mobile Banking System (MBS)
Fraudulent Transaction Successful

Fig. 1. Threat model for phishing in mobile banking system at transaction level

Generally, mobile banking users provide usernames and passwords only once on their mobile devices for MBS and MBS do not ask for a password each time they use the MBS. MBS use OTP for security when they request a transaction. Phishers get stolen/lost users' mobile devices and they do not have to enter the username and password to use the MBS. They request fraudulent transactions using the stolen/lost mobile devices. Currently, security is maintained in the MBS at the transaction level using login credentials and the OTP mechanism (Two-factor authentication). Phishers do not have to input login credentials (Username and password) on mobile devices. MBS sends OTP to the phishers for security and asks to reply to the OTP. Phishers have physical access to mobile devices and reply to OTP easily and execute fraudulent transactions. Hence, only two-factor authentication (Login credentials, and OTP) mechanism cannot stop phishers from executing fraudulent transactions, and there is a need for multi-factor authentication to stop the fraudulent transactions in the mobile banking system.

Researchers have worked to prevent these frauds and enhance the security measures for fraudulent transactions. Researchers developed a layered approach for near-field communication (NFC) enabled mobile payment systems [1] and used machine learning algorithms for the mobile fraud detection system [2, 3]. However, machine learning can solve simple fraud cases, and more complex frauds require human intervention. Fraudsters also use emerging technologies to mimic the transaction behavior of genuine customers. They also keep changing their methods so that it is difficult to detect fraud using machine learning methods. Authors of [4–8] presented a fraud detection system for electronic banking systems in which [4] proposed biometric security and systems, and [5–8] employed machine learning for fraud detection in electronic banking transactions. Authors of [9–20] used machine learning, deep learning, and neural networks for fraud detection in online transactions and banking transactions. Authors of [21–23] developed fraud detection systems for financial databases.

The above research adopted machine learning models to mitigate fraudulent transactions in online transactions. However, these approaches are inefficient and insufficient to account for fraudulent transactions in the mobile banking system. To overcome this gap, this paper presents a new anti-phishing model for mobile banking systems at the transaction level (AntiPhiMBS-TRN), and the objective of this research is to mitigate fraudulent transactions executed using stolen login credentials and stolen/lost mobile devices. Banks and financial institutions can implement AntiPhiMBS-TRN to mitigate fraudulent transactions in the mobile banking industry. The paper is further structured as follows: Sect. 2 describes the related works, Sect. 3 presents the novel anti-phishing model to mitigate fraudulent transactions in the mobile banking system, Sect. 4 describes the results and discussion, and Sect. 5 presents conclusions and future work.

2 Related Works

Researchers have worked on the prevention of fraudulent transactions in digital banking. Vishwakarma, Tripathy, and Vemuru [1] proposed a layered approach for near field communication (NFC) enabled mobile payment system to prevent fraudulent transactions. Delecourt and Guo [2] utilized potential reactions of fraudsters into consideration to build a robust mobile fraud detection system using adversarial examples. Zhou, Chai, and Qiu [3] introduced several traditional machine learning algorithms for fraud detection in the mobile payment system. Eneji, Angib, Ibe, and Ekwegh [4] focused on the integration of biometric security to mitigate and combat electronic banking frauds. Ali, Hussin, and Abed [5] reviewed various attack detection systems and identified transaction monitoring as the most effective model for electronic banking (e-banking). Pracidelli, and Lopes [6] proposed the artifacts capable of minimizing electronic payment fraud problems using unsupervised and supervised algorithms. Guo,Wang,Dai,Cheng, and Wang [7] proposed a novel fraud risk monitoring system for e-banking transactions. Seo and Choi [8] used machine learning techniques for predicting abusers in electronic transactions.

Minastireanu and Mesnita [9] reviewed the existing research in fraud detection and found that the best results were achieved in terms of accuracy and coverage by the supervised learning techniques. Zhou, Zhang, Wang, and Wang [10] used the siamese neural network structure to solve the problem of sample imbalance in online transactions. Khattri and Singh [11] proposed a new distance authentication mechanism for committing a valid and secure online transaction using a credit card or debit card. Kanika and Singla [12] reviewed the use of deep learning techniques for online transaction fraud detection. Hartl and Schmuntzsch [13] focused on the user-end fraud detection and protection for online banking in social engineering. Kataria and Nafis [14] compared the hidden Markov model, deep learning, and neural network to detect fraud in online banking transactions. Masoud and Mehdi [15] used the k nearest neighbor technique with association rules to improve the algorithms for detecting outliers in credit card transactions for electronic banking. Eshghi and Kargari [16] proposed a multi-criteria decision method, intuitionistic fuzzy set, and evidential reasoning of a transaction concerning the effects of uncertainty for them. Kargari and Eshghi [17] proposed a semi-supervised combined model based on clustering algorithms and association rule mining for detecting frauds and suspicious behaviors in banking transactions. Sarma, Alam, Saha, Alam, Alam, and Hossain [18] proposed a system to detect bank fraud using a community detection algorithm that identifies the patterns that can lead to fraud occurrences. Gyamfi and Abdulai [19] used supervised learning methods to support vector machines with spark (SVMS) to build models representing normal and abnormal customer behavior for detecting fraud in new transactions. Shaji and Panchal [20] used an adaptive neuro-fuzzy inference system for detecting fraudulent transactions. Susto, Terzi, Masiero, Pampuri, and Schirru [21] proposed a machine learning-based decision support system for fraud detection in online/mobile banking system. Sapozhnikova, Nikonov, Vulfin, Gayanova, Mironov, and Kurennov [22] employed three classifiers and developed an algorithm for analyzing the information about the user environment to monitor the transactions. Mubalaike and Adali [23] emphasized deep learning (DL) models to detect fraudulent transactions with high accuracy.

Above mentioned works do not mitigate fraudulent transactions using stolen login credentials and phishing apps in the mobile banking system. Our paper proposes a new anti-phishing model to mitigate fraudulent transactions in the mobile banking system in the world of mobile payment transactions. Banks and financial institutions can implement this model to mitigate phishing attacks in the mobile banking system.

3 Proposed Anti-phishing Model AntiPhiMBS-TRN

This paper proposes an anti-phishing model for mobile banking systems at the transaction level (AntiPhiMBS-TRN). AntiPhiMBS-TRN aims to mitigate phishing attacks in the mobile banking system for three categories of users. The first category is the users who download phishing apps mistakenly and provide login credentials in phishing apps. The second category is the users who visit the phishing login interface mistakenly and provide login credentials in the phishing login interface. Phishers steal login credentials from banking users using phishing apps or phishing login interfaces and exploit them to request fraudulent transactions. The third category is the users whose mobile devices are stolen by the phishers or lost somewhere unknownigly. When phishers get such stolen/lost mobile devices, they do not have to enter the login credentials to use the mobile banking system. Phishers request transactions using the stolen/lost mobile devices.

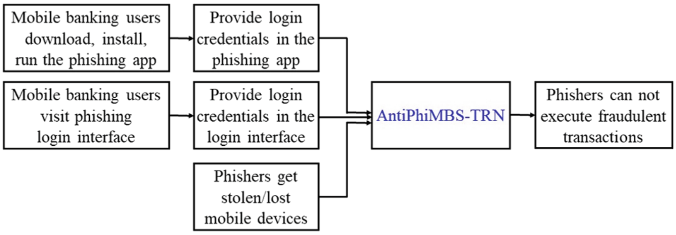
Mobile banking users download, install, run the phishing app
Provide login credentials in the phishing app
Mobile banking users visit phishing login interface
Provide login credentials in the login interface
Phishers get stolen/lost mobile devices
AntiPhiMBS-TRN
Phishers can not execute fraudulent transactions

Fig. 2. Fraudulent transaction protection in the mobile banking system using AntiPhiMBS-TRN

In all of the above cases, the mobile banking system sends OTP to the phishers for the security of the transactions. However, phishers reply to OTP using mobile devices as they have physical access to them and execute fraudulent transactions. Our proposed model AntiPhiMBS-TRN protects mobile banking users from phishers' fraudulent transactions as shown in Fig. 2. We propose the architecture of the anti-phishing model AntiPhiMBS-TRN to describe the detailed working mechanism of AntiPhiMBS-TRN.

3.1 Architecture of Anti-phishing Model AntiPhiMBS-TRN

The architecture of the anti-phishing model AntiPhiMBS-TRN consists of the model for defending against phishing attacks in the mobile banking system at the transaction level. The participating agents in our proposed model AntiPhiMBS-TRN are mobile user, bank, bank application, mobile banking system, phishing application, and phisher.

We specify the following agents and initial conditions for working of AntiPhiMBS-TRN.

- A mobile user (U) opens an account in the Bank (B) and provides an international mobile equipment identity number (imeiNo) of mobile devices for the Mobile Banking System (MBS).
- Bank provides application id (appId), user id (uId), login password (lgnPwd), transaction password (trnPwd), and a unique id for transaction (unqIdTrn) to the user for transaction in MBS. Bank generates unqIdTrn once when a new bank account is opened. New unqIdTrn is not needed for each transaction.
- Bank shares imeiNo, appId, uId, lgnPwd, trnPwd, unqIdTrn, and mobNo of each user with MBS.
- Each of the banking applications is identified by an appId and know the relationship among uId, appId, imeiNo, and unqIdTrn for each user.
- Bank and MBS know the relationship among uId, lgnPwd, trnPwd, appId, imeiNo, and unqIdTrn for each user.
- Users download mobile banking app (BA), install, run and provide login credentials (Username and password) to log on to the mobile banking system.
- Users always share the IMEI number of the mobile device with the MBS. MBS verifies the IMEI number of the mobile device during the transaction.
- Users do not reveal the information provided by the bank to others.

Model for Preventing Fraudulent Transactions in the Mobile Banking System

We consider that banks provide training to mobile users about the detailed procedure to execute transactions using the mobile banking system. This paper presents the scenario of transactions in the mobile banking system using the mobile banking app and the scenario of fraudulent transactions.

Scenario of Transaction in the Mobile Banking System Using Mobile Banking App

All the participating agents (user, bank, bank app, and mobile banking system) of the model must follow the following steps to mitigate the phishing attacks at the transaction level.

- Step 1. A mobile user (U) opens a bank account in the Bank (B) and provides an imeiNo as security parameters to the bank.
- Step 2. Bank sends uId, lgnPwd, trnPwd, and a unqIdTrn to the user for transactions in the MBS.
- Step 3. Bank sends appId, uId, lgnPwd, trnPwd, unqIdTrn, and mobile number (mobNo) of each user to the MBS.
- Step 4. A mobile user downloads the app, logins and is authenticated in MBS, and requests for transactions.
- Step 5. Bank app (BA) asks for a unique id for the transaction to the user.
- Step 6. The user provides unqIdTrn to BA.
- Step 7. BA sends uId, lgnPwd, and unqIdTrn to MBS and requests for the transaction.
- Step 8. MBS asks BA for its appId.
- Step 9. BA provides appId to MBS.
- Step 10. MBS asks for a transaction password to the BA if the application id is the same as in the stored database of MBS for that user id.
- Step 11. BA asks for the transaction password to the user.
- Step 12. The user provides trnPwd to BA.
- Step 13. BA sends trnPwd to the MBS.
- Step 14. MBS verifies the transaction password and sends OTP to the user.
- Step 15. The user replies with the OTP to the MBS. MBS verifies the OTP and IMEI number of the mobile device.

The scenario of transactions in the mobile banking system is shown in Fig. 3. Mobile banking users request transactions and the bank app asks the user to input the unique id for the transaction. The user inputs in the bank app of the mobile banking system.

The bank app already knows the login credentials (User id and password) as they are inputted by the users for authentication in the mobile banking system before requesting the transactions. The bank app sends the login credentials and unique id for the transaction to the MBS. MBS wants to verify the identity of the bank app and asks it to provide the application id. The bank app supplies the app id to MBS. MBS verifies the application id of the bank app within its database. If the application id is not valid, MBS knows that the app is a phishing app. If the application id is valid, then MBS asks the bank app to provide a transaction password. After that, the bank app asks the user to provide the transaction password. The user provides the transaction password to the bank app. The bank app provides the transaction password to the MBS. MBS verifies the two-factor

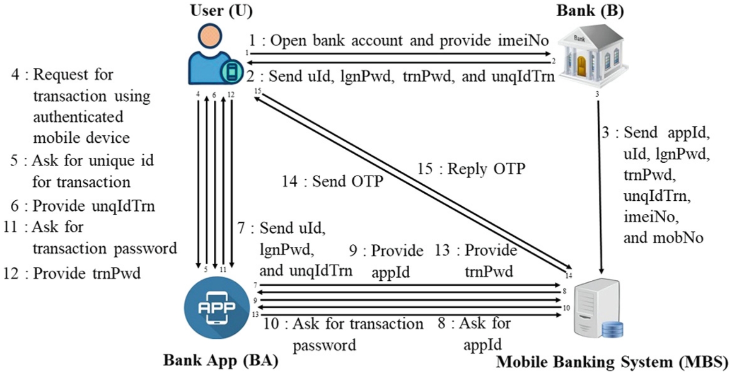
User (U)
Bank (B)
1 : Open bank account and provide imeiNo
2 : Send uId, lgnPwd, trnPwd, and unqIdTrn
4 : Request for transaction using authenticated mobile device
5 : Ask for unique id for transaction
6 : Provide unqIdTrn
11 : Ask for transaction password
12 : Provide trnPwd
3 : Send appId, uId, lgnPwd, trnPwd, unqIdTrn, imeiNo, and mobNo
14 : Send OTP
15 : Reply OTP
7 : Send uId, lgnPwd, and unqIdTrn
9 : Provide appId
13 : Provide trnPwd
APP
10 : Ask for transaction password
8 : Ask for appId
Bank App (BA)
Mobile Banking System (MBS)

Fig. 3. Scenario of transaction by using bank app

authentication (login credentials and unique id for transactions). If both of them are correct, then MBS sends OTP to the user as third-factor authentication. The user replies with the OTP. MBS always detects the IMEI number of the transaction originating mobile devices. Finally, MBS verifies the OTP and the IMEI number of the mobile devices. If both the OTP reply and IMEI number of the mobile devices are valid, then MBS executes the transactions. Generally, the execution of the transaction depends on the two-factor authentication (login credentials and OTP) only. In AntiPhiMBS-TRN, the execution of the transaction depends on the multi-factor authentication (login credentials, unique id for transaction, OTP, and IMEI number of mobile devices).

Scenario of Fraudulent Transaction by Phisher

The fraudulent transactions can be executed in the mobile banking system using the following methods.

- Fraudulent transaction using stolen login credentials and phishing apps
- Fraudulent transaction using stolen/lost mobile devices.

Fraudulent Transaction Using Stolen Login Credentials and Phishing Apps

When the phishers request transactions using stolen login credentials, MBS detects the new mobile devices with the help of the registered IMEI number for that user. The bank app asks for a valid IMEI number of the registered mobile devices to the phisher as shown in Fig. 4. The phisher cannot provide the IMEI number of the old mobile device, and the new mobile device is not allowed for the fraudulent transaction. Generally, MBS does not notice the change of mobile devices for financial transactions. This paper uses an IMEI number of mobile devices in AntiPhiMBS-TRN for the security of change of mobile devices. If the phishers reply with the valid IMEI number anyway and request the transaction, the bank app asks for a unique id for the transaction and the phishers cannot provide a unique id for the transaction to the bank app.

If phishers use phishing apps (PA), phishing app requests a fraudulent transaction, the mobile banking system asks for an application id to the phishing app to identify the

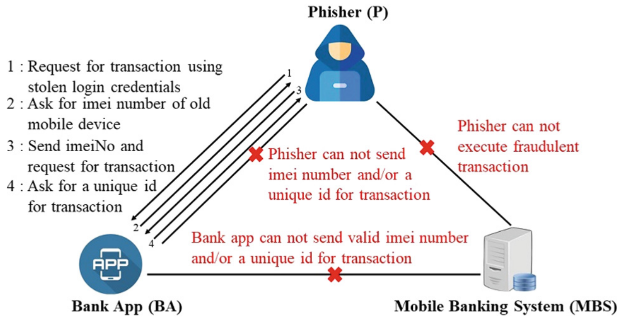
Phisher (P)
1 : Request for transaction using stolen login credentials
2 : Ask for imei number of old mobile device
3 : Send imeiNo and request for transaction
4 : Ask for a unique id for transaction
1
2
3
4
Phisher can not send imei number and/or a unique id for transaction
Phisher can not execute fraudulent transaction
Bank app can not send valid imei number and/or a unique id for transaction
APP
Bank App (BA)
Mobile Banking System (MBS)

Fig. 4. Scenario of fraudulent transaction using stolen login credentials

phishing apps. The phishing app provides a fake app id to the MBS. However, MBS detects the phishing app as a fake app that differs from the registered app id. Thus, the phishers cannot execute the fraudulent transaction using phishing apps.

Fraudulent Transaction Using Stolen/Lost Mobile Devices

Practically, mobile banking users input login credentials (username and password) in the mobile banking system only once, and they are saved on those mobile devices. They do not have to input first-factor authentication (Login credentials) each time when they request transactions. MBS uses OTP as the second-factor authentication for the security of the transactions. The phishers get stolen/lost mobile devices and request a fraudulent transaction using the mobile banking system running on those mobile devices as shown in Fig. 5. If AntiPhiMBS-TRN is not used, MBS asks for OTP only to the phishers and they can reply to OTP easily using the stolen/lost mobile devices and the fraudulent transactions can be successful. However, in AntiPhiMBS-TRN, the bank app asks for a unique id for a transaction for multifactor authentication. The phishers cannot provide a unique id for the transactions to the bank app, and fraudulent transactions are not executed using those stolen/lost mobile devices. The advantage of AntiPhiMBS-TRN is

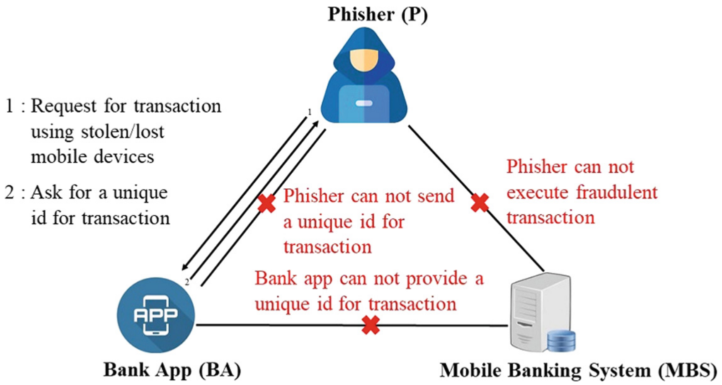
Phisher (P)
1 : Request for transaction using stolen/lost mobile devices
2 : Ask for a unique id for transaction
1
2
Phisher can not send a unique id for transaction
Phisher can not execute fraudulent transaction
Bank app can not provide a unique id for transaction
APP
Bank App (BA)
Mobile Banking System (MBS)

Fig. 5. Scenario of fraudulent transaction using stolen/lost mobile devices

that phishers cannot execute fraudulent transactions using stolen login credentials and stolen/lost mobile devices.

3.2 Verification of Proposed Anti-phishing Model AntiPhiMBS-TRN

We develop a verification model of AntiPhiMBS-TRN by specifying system properties and safety properties using PROMELA. The verification model of AntiPhiMBS-TRN consists of the processes, message channels, and data types. The processes (mobileUser, bank, mobileBankingSystem, bankApp, phisher, and phishing app) in AntiPhiMBS-TRN communicate with each other using defined message channels. We specify the following temporal property using linear temporal logic (LTL) in the verification model of AntiPhiMBS-TRN.

[](((usrId==bankUsrId)&&(lgnPwd==bankLgnPwd)&&usrTrnPwd==bankTrn
Pwd)&&(usrUnqIdTrn==bankUnqIdTrn)&&(usrOTP==bankOTP))-
><>(transactionSuccess==true))

The LTL property states that the transaction of the banking user in the mobile banking system will succeed if (i) the user id provided by the user and received by MBS from the bank is equal, (ii) the login password provided by the user and received by MBS from the bank is equal, (iii) the transaction password provided by the user and received by MBS from the bank is equal, (iv) the unique id for the transaction provided by the user and received by MBS from the bank is equal, and (v) OTP provided by the user and sent by MBS to the user is equal.

4 Results and Discussion

This paper verifies the safety properties and the LTL property of the proposed model AntiPhiMBS-TRN. We accomplished experiments using SPIN Version 6.4.9 running on a computer with the following specifications: Intel® Core(TM) i5-6500 CPU@3.20 GHz, RAM 16 GB, and windows10 64 bit. We ran SPIN to verify the safety properties of AntiPhiMBS-TRN for up to 50 users. SPIN checked the state space for deadlocks during the verification of safety properties. The SPIN verification results for safety properties are in Table 1.

Table 1 shows the results obtained from SPIN illustrating the elapsed time, total memory usage, states transitioned, states stored, depth reached, and verification status for safety properties for various users. The SPIN verification results show a continuous rise in the verification time, transitions, and depth with an increase in the number of users during the verification of AntiPhiMBS-TRN. Besides, the SPIN verification did not detect any deadlock or errors during the execution of the AntiPhiMBS-TRN model. After that, we executed SPIN in the same computing environment to verify the LTL property for up to 50 users. The SPIN verification result for LTL property is in Table 2.

SPIN checked the statespace for never claim and assertion violations in the run of LTL property. The SPIN verification results show a continuous rise in the verification time and depth with the increase in the banking users during the verification of LTL property. The SPIN verified the LTL property successfully. Moreover, the SPIN verification did not detect any deadlock or errors during the execution of the AntiPhiMBS-TRN model.

Table 1. Verification results for safety properties

Users	Time (seconds)	Memory (Mbytes)	Transitions	States stored	Depth	Verification status
1	4.62	39.026	8291118	572263	3737	Verified
2	6.93	39.026	8922211	580992	3777	Verified
5	10.3	39.026	9317685	585438	6411	Verified
10	15.8	39.026	9624342	585278	10054	Verified
20	28.8	39.026	10183740	590008	19795	Verified
30	41.2	39.026	10400937	586723	24735	Verified
40	53.6	39.026	10529304	587235	37421	Verified
50	66.6	39.026	10552524	587991	45013	Verified

Table 2. Verification results for LTL property

Users	Time (seconds)	Memory (Mbytes)	Transitions	States stored	Depth	Verification status
1	4.12	39.026	7134189	572388	684	Verified
2	6.14	39.026	7856907	579632	967	Verified
5	8.23	39.026	7913480	585144	1607	Verified
10	12.9	39.026	7647999	585217	2564	Verified
20	22.9	39.026	8152402	581929	4063	Verified
30	33.3	39.026	8443322	585684	5408	Verified
40	43.4	39.026	8582050	586992	6504	Verified
50	54.8	39.026	8859879	586604	8056	Verified

SPIN did not generate any counterexample during these experiments, and we concluded that there is no error in the design of the AntiPhiMBS-TRN model.

5 Conclusion and Future Work

In this digital era, fraudulent transactions are escalating sharply with the rise in mobile banking transactions in banks and financial institutions. Phishers utilize phishing apps or phishing login interfaces to accumulate login credentials and employ them to perform fraudulent transactions within the mobile banking industry. Moreover, phishers exploit stolen/lost mobile banking users' mobile devices to execute fraudulent transactions. Even though fraudulent transactions are ascending progressively, any anti-phishing model for fraudulent transactions has not been developed so far for the mobile banking system. Therefore, this paper developed a new anti-phishing for mobile banking system at the transaction level (AntiPhiMBS-TRN) to mitigate fraudulent transactions globally.

Phishers exploit stolen login credentials for fraudulent transactions using a new mobile device. However, AntiPhiMBS-TRN detects the new mobile device and queries the IMEI number of the old mobile device to execute the transaction. The phishers cannot deliver an IMEI number, a unique id for the transactions and cannot succeed in the fraudulent transactions in the mobile banking system. The phishing apps cannot provide a valid application id to the mobile banking system, and phishers fail to execute the fraudulent transactions in the mobile banking system using phishing apps. Phishers get stolen/lost mobile devices and request transactions using mobile banking systems installed in those devices. However, AntiPhiMBS-TRN employs a unique id for the transaction system, and phishers cannot provide a unique id for transactions. Hence, phishers fail to execute the fraudulent transactions using stolen/lost mobile devices.

We observed from our experimental SPIN results of the PROMELA model of the AntiPhiMBS-TRN program that the AntiPhiMBS-TRN does not include any deadlocks or errors within the model. Moreover, SPIN verified safety properties and LTL property within the PROMELA model of AntiPhiMBS-TRN. Hence, banks and financial institutions can implement this verified AntiPhiMBS-TRN model to mitigate the ongoing fraudulent transactions and increase the mobile banking users to transform into a cashless society in this digital era of digital banking. In future research, we will propose a new secured model to detect the change of locations and mitigate other probable attacks such as man in the middle (MITM) attack, SQL injection attack, man in the browser (MITB) attack, replay attack in the mobile banking system.

References

1. Vishwakarma, P.P., Tripathy, A.K., Vemuru, S.: A Layered approach to fraud analytics for nfc-enabled mobile payment system. In: Negi, A., Bhatnagar, R., Parida, L. (eds.) ICDCIT 2018. LNCS, vol. 10722, pp. 127–131. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-72344-0_9
2. Delecourt, S., Guo, L.: Building a robust mobile payment fraud detection system with adversarial examples. In: 2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), pp. 103–106. IEEE. Sardinia (2019). https://doi.org/10.1109/AIKE.2019.00026
3. Zhou, H., Chai, H.F., Qiu, M.I.: Fraud detection within bankcard enrollment on mobile device based payment using machine learning. Front. Inf. Technol. Electron. Eng. **19**(12), 1537–1545 (2018). https://doi.org/10.1631/FITEE.1800580
4. Eneji, S.E., Angib, M.U., Ibe, W.E., Ekwegh, K.C.: A study of electronic banking fraud, fraud detection and control. Int. J. Innov. Sci. Res. Technol. **4**(3), 708–711 (2019)
5. Ali, M., Hussin, N., Abed, I.: E-banking fraud detection: a short review. Int. J. Innov. Creat. Change **6**(8), 67–87 (2019)
6. Pracidelli, L.P., Lopes, F.S.: Electronic payment fraud detection using supervised and unsupervised learning. In: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S., Orovic, I., Moreira, F. (eds.) WorldCIST 2020. AISC, vol. 1160, pp. 88–101. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45691-7_9
7. Guo, C., Wang, H., Dai, H., Cheng, S., Wang, T.: Fraud risk monitoring system for e-banking transactions. In: 2018 IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and

Technology Congress, pp. 100–105. IEEE, Athens (2018). https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00030

8. Seo, J.H., Choi, D.: Feature selection for chargeback fraud detection based on machine learning algorithms. Int. J. Appl. Eng. Res. **11**(22), 10960–10966 (2016)
9. Minastireanu, E., Mesnita, G.: An analysis of the most used machine learning algorithms for online fraud detection. Informatica Economica **23**(1), 5–16 (2019). https://doi.org/10.12948/issn14531305/23.1.2019.01
10. Zhou, X., Zhang, Z., Wang, L., Wang, P.: A model based on Siamese neural network for online transaction fraud detection. In: 2019 International Joint Conference on Neural Networks (IJCNN), pp. 1–7, IEEE, Budapest (2019). https://doi.org/10.1109/IJCNN.2019.8852295
11. Khattri, V., Singh, D.K.: A novel distance authentication mechanism to prevent the online transaction fraud. In: Siddiqui, N.A., Tauseef, S.M., Abbasi, S.A., Rangwala, A.S. (eds.) Advances in Fire and Process Safety. STCEE, pp. 157–169. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7281-9_13
12. Kanika, Singla, J.: A survey of deep learning based online transactions fraud detection systems. In: 2020 International Conference on Intelligent Engineering and Management (ICIEM), pp. 130–136. IEEE, London (2020). https://doi.org/10.1109/ICIEM48762.2020.9160200
13. Hartl, V.M.I.A., Schmuntzsch, U.: Fraud protection for online banking. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 37–47. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39381-0_4
14. Kataria, S., Nafis, M.T.: Internet banking fraud detection using deep learning based on decision tree and multilayer perceptron. In: 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1298–1302. IEEE, New Delhi (2019)
15. Masoud, K., Mehdi, F.: Fraud detection in banking using kNN (k-nearest neighbor) algorithm. In: International Conference on Research in Science and Technology, vol. 5, pp. 26–34. Scientific Information Database, London (2016)
16. Eshghi, A., Kargari, M.: Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty. Expert Syst. Appl. **121**, 382–392 (2019). https://doi.org/10.1016/J.ESWA.2018.11.039
17. Kargari, M., Eshghi, A.: A model based on clustering and association rules for detection of fraud in banking transactions. In: Proceedings of the 4th World Congress on Electrical Engineering and Computer Systems and Sciences EECSS, vol. MVML 104, Madrid, Spain (2018). https://doi.org/10.11159/MVML18.104
18. Sarma, D., Alam, W., Saha, I., Alam, M.N., Alam, M.J., Hossain, S.: Bank fraud detection using community detection algorithm. In: 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 642–646. IEEE, Coimbatore (2020). https://doi.org/10.1109/ICIRCA48905.2020.9182954
19. Gyamfi, N.K., Abdulai, J.: Bank fraud detection using support vector machine. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 37–41. IEEE, Vancouver (2018). https://doi.org/10.1109/IEMCON.2018.8614994
20. Shaji, J., Panchal, D.: Improved fraud detection in e-commerce transactions. In: 2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA), pp. 121–126. IEEE, Mumbai (2017). https://doi.org/10.1109/CSCITA.2017.8066537
21. Susto, G.A., Terzi, M., Masiero, C., Pampuri, S., Schirru, A.: A fraud detection decision support system via human on-line behavior characterization and machine learning. In: 2018 First International Conference on Artificial Intelligence for Industries (AI4I), pp. 9–14. IEEE, Laguna Hills (2018). https://doi.org/10.1109/AI4I.2018.8665694

22. Sapozhnikova, M.U., Nikonov, A.V., Vulfin, A.M., Gayanova, M.M., Mironov, K.V., Kurennov, D.V.: Anti-fraud system on the basis of data mining technologies. In: 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp. 243–248. IEEE, Bilbao (2017). https://doi.org/10.1109/ISSPIT.2017.8388649
23. Mubalaike, A.M., Adali, E.: Deep learning approach for intelligent financial fraud detection system. In: 2018 3rd International Conference on Computer Science and Engineering (UBMK), pp. 598–603. IEEE, Sarajevo (2018). https://doi.org/10.1109/UBMK.2018.8566574
24. 2019 Iovation financial services fraud and consumer trust report. https://content.iovation.com/resources/2019-iovation-Financial-Services-Fraud-and-Consumer-Trust-Report.pdf. Accessed 14 Dec 2021
25. Fraud-The Facts 2021: the definitive overview of payment industry fraud report. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021. Accessed 14 Apr 2022