AntiPhiMBS: A New Anti-phishing Model to Mitigate Phishing Attacks in Mobile Banking System at Application 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. A main challenge in the mobile banking system is to mitigate security risks such as phishing attacks, man in the middle attacks, replay attacks, etc. Verizon's 2019 Data Breach Investigations Report (DBIR) reveals that nearly one-third of all data breaches involved phishing attacks in many kinds of ways. The phishing attack is a type of social engineering attack to steal secret information from users. This paper proposes a new **anti**-**phi**shing model for **M**obile **B**anking **S**ystem (**AntiPhiMBS**) that prevents mobile users from phishing attacks in the mobile banking system at the application level. The model prevents mobile users from phishing app installation by using application id, token number, and a unique id for application received from the bank to operate the mobile banking system. The phisher does not know the application id, token number, and unique id and the relationship among them and is unable to install phishing apps on the user's mobile. This paper develops the new anti-phishing model **AntiPhiMBS** with system properties specified using Process meta language (PROMELA) that are successfully verified using Simple PROMELA Interpreter (SPIN). The SPIN verification results show that the proposed anti-phishing model is error-free, and the financial institutions can implement the verified model for mitigating phishing attacks in the mobile banking system at the application installation level.

Keywords: Mobile banking system · Phishing · Verification

1 Introduction

According to the forecast number of mobile users worldwide 2019-2023 (published by Statista O'Dea, Feb 28, 2020), the number of mobile users worldwide is forecast to grow to 7.26 billion for 2020. According to the Juniper research's digital transformation readiness index 2020 [29], it is found that the total number of digital banking users will exceed 3.6 billion by 2024, up from 2.4 billion in 2020 that is a 54% increase and mobile banking users are exceeded 1.75 billion by 2019, representing 32% of the global adult population. People have increased the use of the mobile banking system in the daily activities for financial transactions and cyber-attacks are increasing globally. Cybercriminals are targeting mobile banking users with different attacks for money and

N. T. Nguyen et al. (Eds.): ACIIDS 2021, LNAI 12672, pp. 399–412, 2021.
https://doi.org/10.1007/978-3-030-73280-6_32

are transferring millions of dollars from user accounts to their accounts. It has become necessary for the financial institution to use enhanced secure mobile banking system to perform financial transactions securely. The challenges in the mobile banking system are security risks. Users suffer from different kinds of attacks such as phishing attacks, man in the middle attack, replay attack, the man in the browser attack, denial of service (DoS) attack, distributed DoS (DDoS) attack, etc. Among them, a phishing attack is one of the main challenges for security among mobile banking users. Phishing is an attack that uses social engineering and technology to steal financial account credentials from users. According to the anti-phishing working group's (APWG et al. 2020) report [28], the number of phishing sites detected in the first quarter of 2020 was 165,772, up from the 162,155 observed in the fourth quarter of 2019. According to Verizon's 2019 Data Breach Investigations Report (DBIR) [30], nearly one-third of all data breaches involved are the type of phishing in many kinds of ways.

Phishers can use a phishing app for mobile banking users to install on their mobile and can accumulate vital data from the users. The phishers can use a phishing login interface to collect mobile banking account credentials. The phishers can try for transactions using login credentials in the mobile banking systems. Mobile users are not willing to use mobile banking systems for financial transactions because of fear of attacks. Phishing attacks have become one of the main problems for implementations of the mobile banking system globally. The first known phishing attack was reported in September 2003 after which researchers have proposed various anti-phishing models to mitigate phishing attacks, but variations in procedures of phishing attacks have not been stopped and an anti-phishing model built may not be effective with time.

Zahid Hasan, Sattar, Mahmud, and Talukder [1] proposed a multifactor authentication model to mitigate the phishing attack of e-service systems and the use of multifactor (user id, security image and one-time password) authentication will help the users for the prevention of the phishing attacks in e-service systems. An authentication protocol dealing with an Authentication Server (AS) is proposed in [3], which sends a nonce message to the mobile customer device to be signed to avoid phishing attacks. The use of authentication server in [3] is better suited for browsing safe Webpages in mobile device and prevents users from visiting the phishing Webpages. Megha, Ramesh babu, and Sherly [5] developed an intelligent system for phishing attack detection and prevention with the help of different agents such as monitoring, message passer, and decision-maker agents. The advantage of [5] is that the model can work well for the known phishing attacks using machine learning classifier, but it is difficult to detect and prevent the newly designed and variated phishing attacks. A phishing detection model with a multi-filter approach proposed in [6] can detect phishing attack with the help of filtering in different layers but disadvantage of this model is that phishing attack will be detected till the whitelist layer is updated frequently. Researchers discussed the social engineering attacks [15] utilizing bidirectional communication, unidirectional communication, or indirect communication but it is not easy in reality to detect the phishing attack because of the complex psychological behavior of the people participating in the attack. Cheves [15] and Aburrous, Hossain, Dahal, Thabtah [19] proposed models that can suit for the prevention of phishing attacks for Internet banking systems only. Moreover, Yeop, Kim and Lee [12] also presented anti-phishing model that seems to be effective for only Internet banking systems only by using server authentication schemes.

Banking users must install genuine banking application (app) on their mobile to use mobile banking system. Phishers have already started using phishing application to install on the users' mobile to perform phishing attacks. Such attacks can be mitigated only if some anti-phishing models are developed for application level in mobile banking system. Unfortunately, anti-phishing model has not been developed yet especially for mitigating phishing attacks at the application level in the mobile banking system. This paper presents a new anti-phishing model for Mobile Banking System (AntiPhiMBS) to overcome this gap, and the objective of this research is to build a new anti-phishing model to mitigate phishing attacks in the mobile banking system at application level.

This model can be implemented by the developers to mitigate the phishing attacks in the mobile banking system. Mobile users will be able to download only genuine bank apps on their mobile after the implementation of this model. The phisher will not be able to steal user credentials using a phishing app. The phisher will not be able to succeed in the transactions using the mobile banking system, either. This model can play a significant role in the enhancement of mobile commerce (M-commerce) globally.

The paper is further structured as follows: Sect. 2 describes the related studies, Sect. 3 presents the new anti-phishing model for the mobile banking system, Sect. 4 presents the results and discussion, and Sect. 5 describes conclusions and future work.

2 Background

Current researchers have mentioned different phishing attack techniques and have proposed various anti-phishing models to mitigate the phishing attacks in different environments. Zahid Hasan, Sattar, Mahmud, and Talukder [1] proposed a multifactor authentication model to mitigate the phishing attack of e-service systems from Bangladesh's perspective. The model uses user Id, a secured image with a caption, and a one-time password for authentication in e-service systems. Shankar, Shetty, and Badrinath [2] provided insight into phishing, the mechanism of the attack, the types of attacks and the possible solutions to overcome them. Bojjagani, Brabin, and Rao [3] proposed a novel authentication protocol that deals with an Authentication Server (AS), which sends a nonce message to the mobile customer device to be signed to avoid phishing attacks. Aribake and Aji [4] developed a conceptual model based on technology threat avoidance theory (TTAT) and modified TTAT to evaluate the phishing attack among Internet banking users in Nigeria and to enhance avoidance behavior. Megha, Ramesh babu, and Sherly [5] developed an intelligent system for phishing attack detection and prevention with agents in which the first agent is responsible for extracting URLs. Authors of [6, 7] proposed models for detection and prevention of phishing attacks. Khalid, Jalil, Khalid, Maryam, Shafique, and Rasheed [6] presented a detailed discussion on several anti-mobile phishing models based on various methods for preventing users to evade phishing attacks. Glavan, Racuciu, Moinescu, and Eftimie [7] proposed an anti-phishing model framework to detect phishing attacks by analyzing various anti-phishing methods. Doke, Khismatrao, Jambhale, and Marathe [8] proposed a system with an extension to a web browser that made use of a machine-learning algorithm to extract various features to help the users to distinguish between legitimate website and phishing website. Various phishing attacks and their mitigation techniques have been explained in [9–12]. Yeop Na, Kim and Lee [12] focused on prevention schemes against phishing attacks on Internet banking systems. Lacey, Salmon, and Glancy [13] applied work domain analysis (WDA) to understand the functional structure of phishing attacks and the online transactional environment which they target as a sociotechnical system. Bann, Singh, and Samsudin [14] addressed the advanced persistent threat (APT) issue via spear-phishing attacks within the bring your own device (BYOD) environment through the mediation provided by security policies.

Authors of [17, 21] proposed anti-phishing models to mitigate phishing attacks. Shashidhar, and Chen [17] proposed a model which makes a list of phishing sites and the model checks the messages accordingly for detection of phishing attacks. Cheves [15] proposed a research model that can be used to evaluate the significance of cybercrime in deterring the use of e-banking in the financial sector. Mouton, Leenen, and Venter [16] proposed a social engineering attack detection model: SEADMv2 to cater for social engineering attacks that use bidirectional communication, unidirectional communication, or indirect communication. Aburrous, Hossain, Dahal, and Thabtah [19] mentioned about the investigation of phishing techniques and attack strategies for E-banking. Oh, and Obi [20] discussed the identification of phishing threats in government web services. Authors of [23–25] discussed the securities of the online banking system. Similarly, Akinyede and Esese [26] pointed out the development of a secure mobile e-banking system.

Our paper proposes a new anti-phishing model for the mobile banking system that prevents phishing attacks in the mobile banking systems at the application installation level. The model will be useful for banks and financial institutions globally for security in Electronic banking (E-Banking).

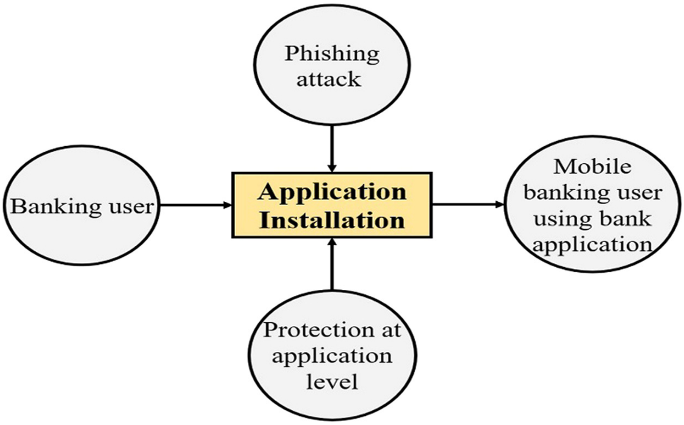
Phishing attack
Banking user
Application Installation
Mobile banking user using bank application
Protection at application level

Fig. 1. Phishing attack protection at application level

3 Proposed Anti-phishing Model For Mobile Banking System

The proposed model is an **anti-phi**shing model for **M**obile **B**anking **S**ystem (**AntiPhiMBS**). AntiPhiMBS aims to mitigate phishing attacks in the mobile banking system at the application level. Banking users install mobile applications and may install phishing apps instead of genuine bank mobile applications by phishing attacks. AntiPhiMBS protects the banking users from installing phishing apps in their mobile phones and helps to use genuine bank applications in their mobile as shown in Fig. 1.

This paper proposes AntiPhiMBS and verifies that AntiPhiMBS satisfies the security properties.

3.1 Architecture of Anti-phishing Model AntiPhiMBS

The architecture of the anti-phishing model AntiPhiMBS consists of the model for defending against phishing attacks at the mobile application level. Participating entities in the model are mobile user, bank, bank application website, mobile banking system, and phishing application website. A mobile customer user opens an account in a bank and receives application installation parameters for the operation of the mobile banking system. The bank maintains a bank application website which offers users services of downloading bank applications for the mobile banking system. The bank shares application installation parameters with the mobile banking system. The phisher might make a phishing application website similar to that of the bank application website and might develop a phishing app for phishing attacks in the mobile banking system. The model uses various parameters for the operation of this model. Table 1 shows the notations for entities and parameters used in AntiPhiMBS.

Table 1. Notations used in AntiPhiMBS

Notation	Description	Notation	Description
U	Mobile User	app	Application
B	Bank	appId	Application Id
MBS	Mobile Banking System	tktNo	Ticket Number
BAW	Bank App Website	unqIdApp	Unique Id Application
PAW	Phishing App Website	mobNo	Mobile Number

Entities and Initial Conditions for Working of AntiPhiMBS

- A mobile user (U) opens an account in the Bank (B).
- Bank provides appId, tktNo and unqIdApp to the user for the operation of Mobile Banking System (MBS).
- Bank shares appId, tktNo, unqIdApp and mobNo of each user to MBS.

- Bank maintains an application website for users to download genuine mobile banking application. Each of the applications is identified by appId. Bank, bank app website and MBS only know the relationship of tktNo, appId, and unqIdApp.
- Users do not share information provided by the bank with any other entities.

Model for Defending Against Phishing Attacks in Mobile Banking System At Application Level

Generally, a bank should conduct phishing awareness training for mobile users when they open an account in the bank. Phishing training should be a part of the bank's cyber security business plan. The bank should give training to mobile users about the procedure of the installation of the mobile app and the use of the system. The application level of prevention against a phishing attack is for all the users who download the mobile app to use the mobile banking system. This method proposes a novel application id (appId), ticket number (tktNo), and a unique id for application (unqIdApp) system to prevent phishing app installation in the user's mobile. Correct steps are necessary for the successful operation of AntiPhiMBS and the bank, user, bank application website, and the mobile banking system should follow all the steps to mitigate the phishing attacks at application level. The scenario of bank app installation is shown in Fig. 2.

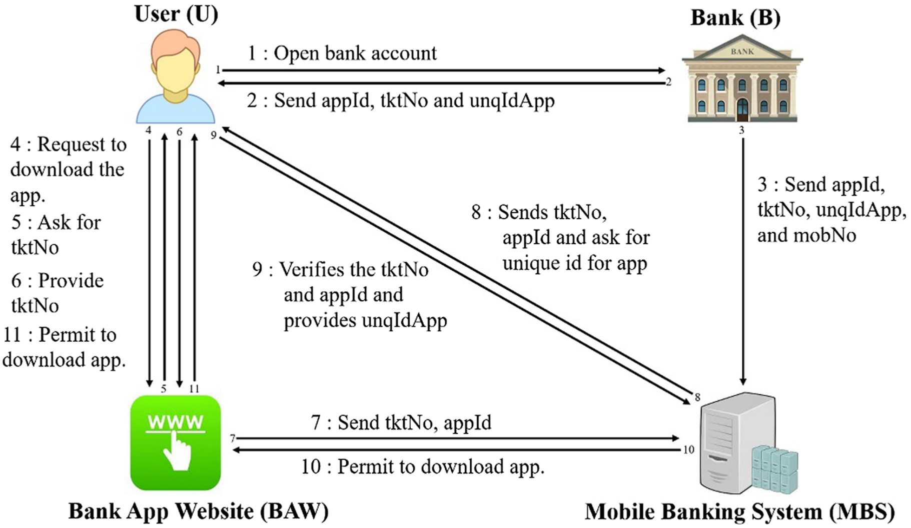
User (U)
Bank (B)
BANK
1 : Open bank account
2 : Send appId, tktNo and unqIdApp
3 : Send appId, tktNo, unqIdApp, and mobNo
4 : Request to download the app.
5 : Ask for tktNo
6 : Provide tktNo
11 : Permit to download app.
8 : Sends tktNo, appId and ask for unique id for app
9 : Verifies the tktNo and appId and provides unqIdApp
7 : Send tktNo, appId
10 : Permit to download app.
WWW
Bank App Website (BAW)
Mobile Banking System (MBS)
1
2
3
4
5
6
7
8
9
10
11

Fig. 2. Scenario of bank app installation

Scenario of Bank Mobile App Installation

The following steps are necessary for a user to install bank mobile app successfully.

- Step 1. A mobile user (U) opens a bank account in the Bank (B).

- Step 2. Bank sends application id (appId), ticket number (tktNo), and unique id for application installation (unqIdApp) to the user for the operation of Mobile Banking System (MBS).
- Step 3. Bank sends appId, tktNo, unqIdApp, and mobile number (mobNo) to MBS.
- Step 4. User visits bank's app website (BAW) and requests to download the app.
- Step 5. Bank's app website asks for ticket number to the user.
- Step 6. The user provides ticketNo to BAW.
- Step 7. BAW knows the relationship between tktNo and appId. BAW searches the appId based on ticketNo and sends both tktNo and appId to MBS.
- Step 8. MBS verifies the tktNo and appId, sends both to the user and asks for a unique Id for app.
- Step 9. User verifies tktNo and appId, and provides a unqIdApp to MBS.
- Step 10. If the unqIdApp from the user is valid, MBS informs the BAW that the user can download the app.
- Step 11. BAW permits the user to download the app.

Bank manages ticket number, application id, and a unique id for each user for the operation of the mobile banking system. Bank also manages the bank application website (BAW) for the management of downloading of a genuine app to the mobile banking system users. Bank communicates with the mobile banking system for the proper installation of the mobile application. BAW maintains the banking apps which are identified by the application id. Bank, BAW and MBS know the relationship between the ticket number, the application id, and the unique id for application allocated for each user in the bank. A mobile user opens an account in the bank and receives an application id, ticket number, and unique id from the bank. The user visits the bank application website and requests to download the app. BAW asks the user to input the correct ticket number and searches the application id based on the ticket number received from the user. BAW sends the ticket number and application id of that user together to the mobile banking system for verification of the application installation. The mobile banking system verifies the ticket number and application id with the help of the database already received from the bank. MBS shows the ticket number and application id to the user and asks to enter the valid unique id for the application. Users can verify the MBS supplied ticket number and application id and have the option of downloading the application or not. The user enters the unique id for the application if both of the ticket number and application id are correct. MBS verifies the unique id and sends permission to BAW to allow users to download the app if the unique id supplied by the user is valid. Finally, BAW allows users to download the app after getting a positive response from the mobile banking system.

Scenario of Phishing App Installation

Even though users know the correct procedure for downloading the app from the bank application website, they may receive phishing emails or SMS from the phishers. Phishers might develop a phisher application website (PAW) similar to that of the bank application website (BAW) and phisher mobile banking system. Users may visit PAW and may click the link unknowingly to download the mobile application on their mobile.

Thus, users may start phishing app installation unknowingly. Scenario of phishing app installation is shown in Fig. 3.

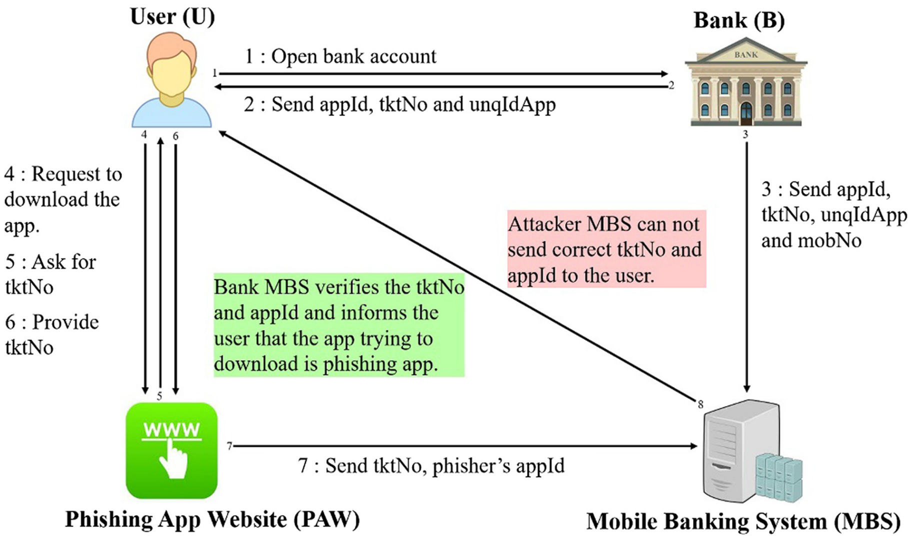
User (U)
Bank (B)
1 : Open bank account
2 : Send appId, tktNo and unqIdApp
3 : Send appId, tktNo, unqIdApp and mobNo
4 : Request to download the app.
5 : Ask for tktNo
6 : Provide tktNo
Attacker MBS can not send correct tktNo and appId to the user.
Bank MBS verifies the tktNo and appId and informs the user that the app trying to download is phishing app.
7 : Send tktNo, phisher's appId
1
2
3
4
5
6
7
8
BANK
WWW
Phishing App Website (PAW)
Mobile Banking System (MBS)

Fig. 3. Scenario of phishing app installation

The following steps may be executed during phishing app installation.

- Step 1. A mobile user (U) opens a bank account in the Bank (B).
- Step 2. Bank sends application id (appId), ticket number (tktNo), and unique id for application installation (unqIdApp) to the user for the operation of Mobile Banking System (MBS).
- Step 3. Bank sends appId, tktNo, unqIdApp, and mobile number (mobNo) to MBS.
- Step 4. User may receive phishing email or phishing SMS with links to download the app. User may click the provided links to download the app.
- Step 5. Phisher's website asks for ticket number to user.
- Step 6. User may provide tktNo to the Phisher's website.
- Step 7. Phisher's website sends tktNo and phisher's appId to MBS. MBS verifies the tktNo and appId and informs the user that the app trying to download is not bank's app. If the phisher act as MBS too, fake MBS cannot send the correct tktNo and appId to the user.

User may click phishing app download links unknowingly. PAW asks for the ticket number to the user and the user may input the ticket number to PAW. PAW does not know the true application id for that ticket number and sends a fake application id along with the ticket number to MBS. MBS verifies the ticket number and phisher application id and detects that the application download request is from the phisher application website. After that, MBS informs the user about the phishing app and prevents the user from downloading the phishing app. If the phisher uses fake MBS, fake MBS does not know the application id for the ticket number and cannot send it to the user. Fake MBS may send ticket number and fake application id to the user, but user verifies the ticket number and fake application id and knows about the phishing attack. Users do not provide a unique id and do not download the app until they receive the correct ticket number and the application id from MBS. Users have the option to continue downloading the app or cancel the process and are prevented from phishing attacks. Even though phishers collect ticket numbers using the phisher application website and try to download the bank app using the genuine ticket number, they fail in downloading the application because they do not know the unique id for the application. Hence, AntiPhiMBS prevents the users from installing phishing apps on their mobile and forbids the phishers from downloading the bank app on their mobile. Thus, the model prevents phishing attacks in the mobile banking system at the application level.

3.2 Verification of Proposed Anti-phishing Model AntiPhiMBS

We chose SPIN to verify the proposed model AntiPhiMBS because of its graphical user interface and counterexample generation during the verification and developed the verification model of AntiPhiMBS using PROMELA. This paper does not show the PROMELA codes because of space limitations. The PROMELA code in this paper has 201 lines. The PROMELA verification model of AntiPhiMBS consists of the processes, message channels, and data types. This paper explains the overview of the codes. The verification model of AntiPhiMBS consists of the following processes.

- mobileUser: The process represents the end user of the mobile banking system.
- bank: The process represents the bank where the user opens the bank account, and the bank manages the mobile banking system for the user.
- mobileBankingSystem: The process represents the mobile banking system which offers the services of banking operations in the mobile.
- bankAppWebsite: The process represents the bank's authorized application website which manages the downloading of mobile application for the user.
- phisherAppWebsite: The process represents the phisher's phishing website which imitates the bank application website and tries to fool the users to install a phishing app on their mobile.

Above mentioned processes communicate using message channels that are specified in the PROMELA code of AntiPhiMBS.

We also specified the following security properties using linear temporal logic (LTL) in the verification model of AntiPhiMBS.

[](((usrTktNo ==bankTktNo)&&(websiteAppId ==bankAppId)&&(usrUnqIdApp ==bankUnqIdApp))- > <>(appDownloadSuccess ==true))

Download of mobile banking application is successful only if (i) the ticket number provided by the user and received from bank is equal (ii) the application id provided by the bank application website and received from bank is equal (iii) the unique id for application provided by the user and received from the bank is equal.

4 Results and Discussion

This paper verifies the safety properties and LTL properties of the proposed model AntiPhiMBS. Safety properties include the checking of deadlocks and assertion violations in AntiPhiMBS and ensure that nothing bad ever happens in the proper functioning of the model. 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 64bit. We applied bitstate to save memory during the verification of the model. We set the advanced parameters in the SPIN for the verification of AntiPhiMBS and made physical memory available as 4096 (in Mbytes), maximum search depths (steps) as 1000000, and estimated state space size as 1000 for the experiments. Besides, we set extra compile-time directives to DVECTORSZ as 9216 to avoid the memory error during the experiments. After that, we ran SPIN to verify the safety properties of AntiPhiMBS for various users. SPIN checked the state space for invalid end states, assertion violations, and acceptance cycles. The SPIN verification results for safety properties are in Table 2.

Table 2. Verification results for safety properties

No. of users	Time (in seconds)	Memory (in Mbytes)	Transitions	States stored	Depth	Safety property verification status
1	1.43	39.026	2634164	196203	65223	Verified
5	4.26	39.026	4177108	283820	112921	Verified
10	24.1	156.799	6537677	431452	197962	Verified
20	49.6	320.276	8058943	511312	273755	Verified
50	126	788.733	9324748	574242	322689	Verified
80	201	1235.217	9578183	582609	324933	Verified
100	255	1549.866	9723016	588837	330954	Verified

The results in Table 2 shows the elapsed time, total memory usage, states transitioned, states stored, depth reached, and verification status for different numbers of users. The SPIN verification results show that the verification time has been increased consistently with the rise in the number of users during the verification of AntiPhiMBS. However, the memory required for the verification remained approximately equivalent for up to 5 users followed by an increment with the increase in the number of users. Moreover, the states stored, depth reached and transitions for various users increased significantly for up to 10 users and afterwards slightly for the rest of the users. The safety property is satisfied in each run of the SPIN and neither any deadlock nor any errors are detected during the verification of AntiPhiMBS.

After verification of the safety properties, we ran SPIN in the same computing environment to verify the LTL properties for various users. SPIN checked the statespace for never claim and assertion violations in run of LTL property. The SPIN verification result for LTL properties is in Table 3. Table 3 shows the results obtained from SPIN showing the elapsed time, total memory usage, states transitioned, states stored and verification status for various users. The LTL property of AntiPhiMBS is verified by the SPIN. The memory required for LTL property for all the users are same. The verification time has been increased proportionally with the rise in the number of users during the verification of AntiPhiMBS. Furthermore, the states stored, and elapsed time increased with the increase in the number of users.

Table 3. Verification results for LTL properties

No. of users	Time (in seconds)	Memory (in Mbytes)	Transitions	States stored	Depth	LTL property verification status
1	0.522	39.026	954795	78200	6525	Verified
5	1.96	39.026	1913065	139316	13532	Verified
10	5.83	39.026	3411072	245312	22076	Verified
20	16.1	39.026	5629439	402333	29722	Verified
50	45	39.026	7054808	525783	29214	Verified
80	68	39.026	6919770	541326	45642	Verified
100	83.1	39.026	6819757	551746	54444	Verified

SPIN displays execution paths as counterexamples if some situations do not meet the properties specified in the design of the model. In our case, SPIN did not generate any counterexample during the verification of AntiPhiMBS in any of the experiments. Hence, the verified AntiPhiMBS seems to be applicable for the development and implementation of the anti-phishing system within the banks and financial institutions globally to countermeasure the continued phishing attacks in Electronic Banking (E-Banking).

5 Conclusion and Future Work

Since phishing attack creates a negative impact on the E-banking, establishes relationships with other attacks, and creates financial risks for emerging digital era at the national and international level, this paper chose to develop a new anti-phishing model for Mobile Banking System (AntiPhiMBS) to mitigate phishing attacks in the mobile banking system at the application level. Our experimental results showed that the proposed AntiPhiMBS is free from errors and deadlocks. Furthermore, AntiPhiMBS is verified using SPIN for different numbers of users to assure the practical implementation of the model in the financial institutions. Moreover, the study presented the mitigation of phishing attacks at the application level in AntiPhiMBS. Phisher may send phishing emails or SMS (Short Messaging Service) to the users and may redirect them to download the phishing app. Phishers might use the phishing app to install it on the user's mobile to steal login credentials from the user. However, AntiPhiMBS uses the ticket number, application id, and a unique id for the application installation and prevents the user from installing the phishing app. Hence, financial institutions can implement this verified AntiPhiMBS model to mitigate the ongoing phishing attacks in the world of E-Banking and can save millions of dollars annually globally. Our research will also be beneficial to mobile app developers, end users, researchers, and bankers.

AntiPhiMBS model mitigates the phishing attacks in the mobile banking system at the application level only. In our future research, we will propose new anti-phishing models to mitigate phishing attacks in the mobile banking system at the authentication level and transaction level. Furthermore, this research could be further extended through the verification of new models to mitigate man in the middle (MITM) attack, man in the browser (MITB) attack, replay attack, SQL injection attack, and other probable attacks in E-Banking.

References

1. Zahid Hasan, M., Sattar, A., Mahmud, A., Talukder, K.H.: A multifactor authentication model to mitigate the phishing attack of e-service systems from Bangladesh perspective. In: Shetty, N.R., Patnaik, L.M., Nagaraj, H.C., Hamsavath, P.N., Nalini, N. (eds.) Emerging Research in Computing, Information, Communication and Applications. AISC, vol. 882, pp. 75–86. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-5953-8_7
2. Shankar, A., Shetty, R., Badrinath, K.: A review on phishing attacks. Int. J. Appl. Eng. Res. **14**(9), 2171–2175 (2019)
3. Bojjagani, S., Brabin, D., Rao, V.: PhishPreventer: a secure authentication protocol for prevention of phishing attacks in mobile environment with formal verification. In: Thampi, S., Madria, S., Fernando, X., Doss, R., Mehta, S., Ciuonzo, D. (eds.) Third International Conference on Computing and Network Communications 2019, vol. 171, pp. 1110–1119. Elsevier B.V, Heidelberg (2020)
4. Aribake, F.O., Aji, Z.M.: Modelling the phishing avoidance behavior among internet banking users in Nigeria: the initial investigation. J. Comput. Eng. Technol. **4**(1), 1–17 (2020)
5. Megha, N., Ramesh babu, K.R., Sherly, E.: An intelligent system for phishing attack detection and prevention. In: Proceedings of the Fourth International Conference on Communication and Electronics Systems, pp. 1577–1582. IEEE Xplore, Coimbatore, India (2019). https://doi.org/10.1109/icces45898.2019.9002204
6. Khalid, J., Jalil, R., Khalid, M., Maryam, M., Shafique, M.A., Rasheed, W.: Anti-phishing models for mobile application development: a review paper. In: Bajwa, I.S., Kamareddine, F., Costa, A. (eds.) INTAP 2018. CCIS, vol. 932, pp. 168–181. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-6052-7_15
7. Glavan, D., Racuciu, C., Moinescu, R., Eftimie, S.: Detection of phishing attacks using the anti-phishing framework. Sci. Bull. Naval Acad. **13**(1), 208–212 (2020)
8. Doke, T., Khismatrao, P., Jambhale, V., Marathe, N.: Phishing-inspector: detection & prevention of phishing websites. In: Patil, D.Y. (ed.) International Conference on Automation, Computing and Communication 2019, vol. 32, pp. 1–6. EDP Sciences, India (2020). https://doi.org/10.1051/itmconf/20203203004
9. Meena, K., Kanti, T.: A review of exposure and avoidance techniques for phishing attack. Int. J. Comput. Appl. **107**(5), 27–31 (2014)
10. Naidu, G.: A survey on various phishing detection and prevention techniques. Int. J. Eng. Comput. Sci. **5**(9), 17823–17826 (2016)

11. Akinyede, R.O., Adelakun, O.R., Olatunde, K.V.: Detection and prevention of phishing attack using linkguard algorithm. J. Inf. **4**(1), 10–23 (2018). https://doi.org/10.18488/journal.104.2018.41.10.23
12. Yeop Na, S., Kim, H., Lee, D.H.: Prevention schemes against phishing attacks on internet banking systems. Int. J. Adv. Soft Comput. Appl. **6**(1), 1–15 (2014)
13. Lacey, D., Salmon, P., Glancy, P.: Taking the bait: a systems analysis of phishing attacks. In: 6th International Conference on Applied Human Factors and Ergonomics and the Affiliated Conferences, vol. 3, pp. 1109–1116. Elsevier, Australia (2015). https://doi.org/10.1016/j.promfg.2015.07.185
14. Bann, L.L., Singh, M.M., Samsudin, A.: Trusted security policies for tackling advanced persistent threat via spear phishing in BYOD environment. In: The Third Information Systems International Conference, vol. 72, pp. 129–136. Elsevier ScienceDirect, Penang Malaysia (2015). https://doi.org/10.1016/j.procs.2015.12.113
15. Cheves, D.A.: The impact of cybercrime on e-banking: a proposed model. In: International Conference on Information Resources Management, pp. 1–10. Association for Information Systems AIS Electronic Library, West Indies (2019)
16. Mouton, F., Leenen, L., Venter, H.S.: Social engineering attack detection model: SEADMv2. In: International Conference on Cyberworlds, pp. 216–223. IEEE, Pretoria, South Africa (2015). https://doi.org/10.1109/cw.2015.52
17. Shashidhar, N., Chen, L.: A phishing model and its applications to evaluating phishing attacks. In: Proceedings of the 2nd International Cyber Resilience Conference, pp. 63–69. Edith Cowan University, Perth Western Australia (2011)
18. Rajalingam, M., Alomari, S.A., Sumari, P.: Prevention of phishing attacks based on discriminative key point features of webpages phishing attacks. Int. J. Comput. Sci. Secur. **6**(1), 1–18 (2012)
19. Aburrous, M., Hossain, M.A., Dahal, K., Thabtah, F.: Experimental case studies for investigating e-banking phishing techniques and attack strategies. Cogn. Comput. **2**, 242–253 (2010). https://doi.org/10.1007/s12559-010-9042-7
20. Oh, Y., Obi, T.: Identifying phishing threats in government web services. Int. J. Inf. Netw. Secur. **2**(1), 32–42 (2013)
21. Jakobsson, M.: Modeling and Preventing Phishing Attacks. In: Patrick, Andrew S., Yung, M. (eds.) FC 2005. LNCS, vol. 3570, p. 89. Springer, Heidelberg (2005). https://doi.org/10.1007/11507840_9
22. Jagadeesh Kumar, P.S., Nedumaan, J., Tisa, J., Lepika, J., Wenli, H., Xianpei, L.: New malicious attacks on mobile banking applications. Mob. Netw. Appl. **21**(3), 561–572 (2016). Special Issue on Mobile Reliability, Security and Robustness, Springer
23. Yildirim, N., Varol, A.: A research on security vulnerabilities in online and mobile banking systems. In: 7th International Symposium on Digital Forensics and Security, pp. 1–5. IEEE, Barcelos, Potugal (2019)
24. Hammood, W.A., Abdulla, R., Hammood, O.A., Asmara, S.M., Al-Sharafi, M.A., Hasan, A.M.: A review of user authentication model for online banking system based on mobile imei number. In: The 6th International Conference on Software Engineering & Computer Systems, IOP Conf. Series: Materials Science and Engineering 769, Kuantan, Pahang, Malaysia (2020). https://doi.org/10.1088/1757-899x/769/1/012061
25. Dhoot, A., Nazarov, A.N., Koupaei, A.N.A.: A security risk model for online banking system. In: 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, pp. 1–4. IEEE, Moscow, Russia (2020)
26. Akinyede, R.O., Esese, O.A.: Development of a secure mobile e-banking system. Int. J. Comput. **26**(1), 23–42 (2017)

27. Ahmed, A.A., Adullah, A.N.: Real time detection of phishing websites. In: 7th Annual Information Technology, Electronics and Mobile Communication Conference, pp. 1–6. IEEE, Vancouver, Canada(2016)
28. APWG Homepage. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf. Accessed 11 Nov 2020
29. JUNIPER Research. https://www.juniperresearch.com/press/press-releases/digital-banking-users-to-exceed-3-6-billion. Accessed 12 Nov 2020
30. VERIZON data breach investigation report. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf. Accessed 11 Nov 2020