






AntiPhiMBS-Auth: A New Anti-phishing Model to Mitigate Phishing Attacks in Mobile Banking System at Authentication 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. In the era of digital banking, the advent of the latest technologies, utilization of social media, and mobile technologies became prime parts of our digital lives. Unfortunately, phishers exploit digital channels to collect login credentials from users and impersonate them to log on to the victim systems to accomplish phishing attacks. This paper proposes a novel anti-phishing model for Mobile Banking System at the authentication level (AntiPhiMBS-Auth) that averts phishing attacks in the mobile banking system. This model employs a novel concept of a unique id for authentication and application id that is known to users, banking app, and mobile banking system only. Phishers and phishing apps do not know the unique id or the application id, and consequently, this model mitigates the phishing attack in the mobile banking system. This paper utilized a process meta language (PROMELA) to specify system descriptions and security properties and built a verification model of **AntiPhiMBS-Auth**. The verification model of **AntiPhiMBS-Auth** is successfully verified using a simple PROMELA interpreter (SPIN). The SPIN verification results prove that the proposed **AntiPhiMBS-Auth** is error-free, and financial institutions can implement the verified model for mitigating the phishing attacks in the mobile banking system at the authentication level.

Keywords: Mobile banking system · Authentication · Anti-phishing model · Verification · Model checking

1 Introduction

Phishing is a growing social engineering asynchronous attack in which phishers exploit digital channels such as mobile banking, Internet banking, ATM (Automated Teller Machine), social media platform (such as Facebook, Line, Viber, WhatsApp, etc.) for the attacks. Phishers craft an email, SMS (Short Messaging Service), or voicemail and wait for the victims to log onto their phishing site or phishing application. Subsequently, phishers collect the stolen credentials and impersonate them to log onto the digital channels. Attackers have a list of validated banking credentials for manual account takeover on the banking site and banking applications. Shape Security's 2018 credential

spill report [28] shows 2.3 billion credentials breaches in 2017, and online retail loses about \$6 billion per year while the US consumer banking industry faces over \$50 million per day in potential losses from the attacks.

In the era of digital banking, the advent of the latest technologies, the utilization of social media, and mobile technologies have become prime parts of our digital lives. People use mobile applications, email, SMS, web, and social media every day, but unfortunately, they are all abused for phishing attacks. Phishers employ all of these platforms to exploit information, harm society, and globally dispute attacker activities, thus leading to financial loss and cybercrime. According to the findings of Phishlab's 2019 phishing trends and intelligence report [29], phishing attack volume raised to 40.9% in 2018, and 83.9% of attacks targeted credentials for financial, email, cloud, payment, and SaaS services. The financial institutions, being on top as the single most targeted industry, accounted for 28.9% of all phishing websites in 2018, and the most credential theft achieved using phishing-based links accounted for 88% [29]. According to F5 Labs' 2020 phishing and fraud report [30], phishing incidents rose by a staggering 220% compared to the yearly average during the height of global pandemic fears.

The phishing attack is the main challenge all around the world, and it has become one of the main burdens for the full-fledged implementation of mobile banking in financial institutions. Researchers have been working for the mitigation of such attacks universally. Some of the researchers have focused on machine learning models. Machine learning models [1–6] and artificial neural networks [7] can mitigate the known phishing attacks up to some extent. The advantages of these models are that they can be suitable for the known phishing websites but may not work for newly conceived phishing attacks. Besides, algorithms [8, 9] can mitigate only the specified pattern of phishing attacks. Drury and Meyer [10] proposed an email account separation for the detection of phishing emails but the proposed method can detect phishing emails in an organization where the mail server is configured securely for operation. Miller, Miller, Zhang, and Terwilliger [13] presented a three-pillared strategy for the prevention of phishing attacks using one-time passwords, multi-level desktop barrier applications, and behavior modification which can be advantageous for the organization where employees do not misconduct the information technology policy and guidelines of the organization.

Some of the researchers focused on multifactor authentication for the mitigation of phishing attacks. The advantage of using the counter challenge authentication method in [17] is that the phisher cannot provide the challenge enforced by the web application and thus, mitigates the phishing attacks. The use of various multifactor authentication methods in [18–27] can help in mitigating phishing attacks in online banking systems.

Generally, banking users install banking applications on their mobile to get banking services using mobile. The users might install a phishing app on their mobile misguidedly and enter the login credentials for the mobile banking system. Moreover, the users might follow the links of a phishing email or phishing SMS and enter the login credentials unknowingly about the phishing. In this way, phishers collect the login credentials from banking users and exploit them for phishing attacks in the mobile banking system. Some of the above research adopted machine learning models for the mitigation of phishing attacks using web pages and some employed multifactor authentication methods for the prevention of phishing attacks within the Internet banking systems. However,

these approaches are inefficient for mitigating phishing attacks within the mobile banking system. According to the above studies, we found that the existing approaches are insufficient to account for the phishing attacks in the mobile banking system at the authentication level. A phishing attack can be pandemic in the future if proper actions are not taken in time by the financial institutions. This paper presents a new anti-phishing model for mobile banking system at the authentication level (AntiPhiMBS-Auth) to beat this gap, and the objective of this research is to build a new anti-phishing model, to the best of our knowledge, is the first attempt to mitigate phishing attacks in the mobile banking system at the authentication level.

Financial institutions can implement this model globally to mitigate phishing attacks in the mobile banking industry. Phishers might succeed in collecting the login credentials using phishing apps, phishing email, phishing SMS, or social media platform but could not complete the authentication process of the mobile banking system if this model is implemented in the financial institutions correctly. Henceforth, phishers could not succeed in executing the transactions in the mobile banking system using stolen login credentials, and financial institutions can save millions of dollars globally. The model will play a significant role in increasing mobile banking transactions and will contribute to the transformation towards a cashless society in the era of digital banking. 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 at the authentication level, Sect. 4 presents the results and discussion, and Sect. 5 describes conclusions and future work.

2 Background

Phishing has become one of the foremost attacks nowadays and many researchers have been proposing different solutions to mitigate the ongoing phishing attacks in cyberspace. Authors of [1–7] employed different machine learning models and artificial neural networks to classify websites as legitimate or phishing using the knowledge base of the phishing attacks. Tchakounte, Molengar, and Ngossaha [1] employed a formal description logic to prepare the knowledge base of phishing attacks and designed an ontology-oriented approach to add semantics in the knowledge base of phishing attacks. Subasi and Kremic [2] presented an intelligent phishing website detection framework where different machine learning models such as AdaBoost and Multiboost are employed to classify websites as legitimate or phishing websites. Ozker and Sahingoz [3] proposed a machine learning model and implemented a content-based phishing detection system that analyzes the text and additional properties of the web page and tries to understand whether there is a fraudulent web page or not on the websites. Priya, Selvakumar, and Velusamy [4] proposed a radial basis function (RBF) network with enhanced hyper parameters for classifying and predicting the phishing websites. K-modes clustering algorithm along with the proposed dissimilarity evaluation is used in [4] to select the RBF centers and spread constant of the network for better learning. Odeh, Alarbi, Keshta, and Abdelfattah [5] presented an intelligent model for detecting phishing websites on the Internet that applies multilayer perceptron to the system which classifies the inputted URL and applies the single attribute evaluator to eliminate irrelevant attributes to detect the phishing attacks.

Hossain, Sarma, and Chakma [6] analyzed different machine learning techniques that can be implemented over a dataset of features regarding websites and their corresponding details to detect a possible phishing website. Su [7] adopted long short-term memory (LSTM) and optimized the training method of the model in combination with the characteristics of recurrent neural networks (RNN) for the detection of phishing websites. Authors of [8, 9] used algorithms to classify the incoming URL (Uniform Resource Locator) into a phishing site or non-phishing site. Abiodun, Sodiya, and Kareem [8] employed an algorithm design to extract link characteristics from loading URLs to determine their legitimacy. Sharathkumar, Shetty, Prakyath, and Supriya [9] proposed a system that extracts features of the inputted URL and classifies them as a phishing site or a non-phished site using the random forest algorithm. Drury and Meyer [10] proposed email account separation as a possible approach to detect phishing emails by analyzing the collection process of email addresses. Awan [11] discussed different types of phishing attacks and various defenses against the attacks. Alabdan [12] presented a review of the approaches used during the phishing attacks and analyzed the characteristics of the existing classic, modern, and cutting-edge phishing attack techniques. Miller, Miller, Zhang, and Terwilliger [13] presented a three-pillared strategy for the prevention of phishing attacks in which the strategy is based on one-time passwords, multi-level desktop barrier applications, and behavior modification. Ustundag Soykan and Bagriyanik [14] implemented deterministic and randomized attack scenarios to demonstrate the success of the attack using a state-of-the-art simulator on the IEEE (Institute of Electrical and Electronics Engineers) European low voltage feeder test system in which authors identified threats, conducted impact analysis and estimated the likelihood of the attacks for various attacker types and motivations. Natadimadja, Abdurohman, and Nuha [15] used Hadoop (A Java-based open-source platform under apache to support applications that run on big data) and MapReduce (A programming model aimed at processing large datasets) for the detection of phishing websites. Chaudhry, Chaudhry, and Rittenhouse [16] explained various methods used in phishing attacks and pointed out the prevention from such attacks using a combination of client-side tools and server-side protection. Shaik [17] presented a counter challenge authentication method that uses a counter challenge from a user to a web application asking to provide certain information from one or more user details recorded at the time of registration.

Different authentication methods are suggested in [18–22] for additional security during the authentication in the banking systems. Aravindh, Ambeth Kumar, Harish, and Siddarth [18] used the method of pass matrix which allows the user to select an image from a set of pre-defined images in combination with the password for authentication in banking systems. Sukanya and Saravanan [19] showed a safe graphical confirmation framework named pass grid to be used for a password by the user during authentication in the banking systems. Modibbo and Aliyu [20] emphasized multifactor biometric authentication systems to transform into a cashless society and to decrease the electronic payment system fraud in the Nigerian financial service industry. Tam, Chau, Mai, Phuong, Tran, and Hanh [21] pointed out various types of cybercrimes in the banking industry of Vietnam and made preventive recommendations for commercial banks, policymakers, stakeholders, and customers for the proper mitigation of cybercrimes in the banking system. Lakshmi Prasanna, and Ramesh [22] proposed a proficient and handy

client confirmation plot utilizing individual gadgets that use distinctive cryptographic natives such as encryption, computerized signature, and hashing for authentication in the Internet banking system.

Authors of [23–27] emphasized the multifactor authentication system in mobile banking systems. Aldwairi, Masri, Hassan, and ElBarachi [23] implemented a three-stage authentication system for mobile applications in which the first stage is the user-name with device serial number, the second stage is the selection of the correct square from a large grid of independent squares and the final stage is the selection of particular images in the same order as picked them during the registration. Srinivasa Rao, Deepashree, Pawaskar, Divya, and Drakshayini [24] used geolocation in addition to the existing two-factor authentication scheme using the user ID, password, and OTP for additional security in mobile banking transactions. Miiri, Kimwele, and Kennedy [25] utilized keystroke dynamics and location for authentication in the mobile banking system. Likewise, Song, Lee, Jang, Lee, and Kim [26] proposed a face recognition authentication scheme in which distance between the point of eyes, nose, and mouth from captured user's face is compared with the stored facial features and Macek, Adamovic, Milosavljevic, Jovanovic, Gnjatovic, and Trenkic [27] proposed a cryptographically secured iris biometrics for authentication in the mobile banking system.

Our paper proposes a new anti-phishing model for the mobile banking system that prevents phishing attacks in mobile banking systems at the authentication level. Banks and financial institutions can implement this model for the mitigation of enduring phishing attacks in Electronic banking (E-Banking) globally.

3 Proposed Anti-phishing Model for Mobile Banking System at Authentication Level

The proposed model is an **anti-phishing** model for **Mobile Banking System** at the **authentication level (AntiPhiMBS-Auth)**. AntiPhiMBS-Auth aims to mitigate phishing attacks in the mobile banking system at the authentication level for two categories of banking users. The first category is the banking users who download the phishing app misguidedly and start using the phishing app inadvertently in place of a genuine bank app. The second category is the banking users who may receive phishing emails or phishing SMS or social media platform messages and may click the link of the phishing login interface. Phishers design the phishing app and phishing login interface looking similar to that of the banks. Banking users do not understand the phishing mechanisms and may input login credentials in the phishing app or the phishing login interface. AntiPhiMBS-Auth safeguards banking users from the phisher's use of stolen login credentials for authentication in the mobile banking system as in Fig. 1.

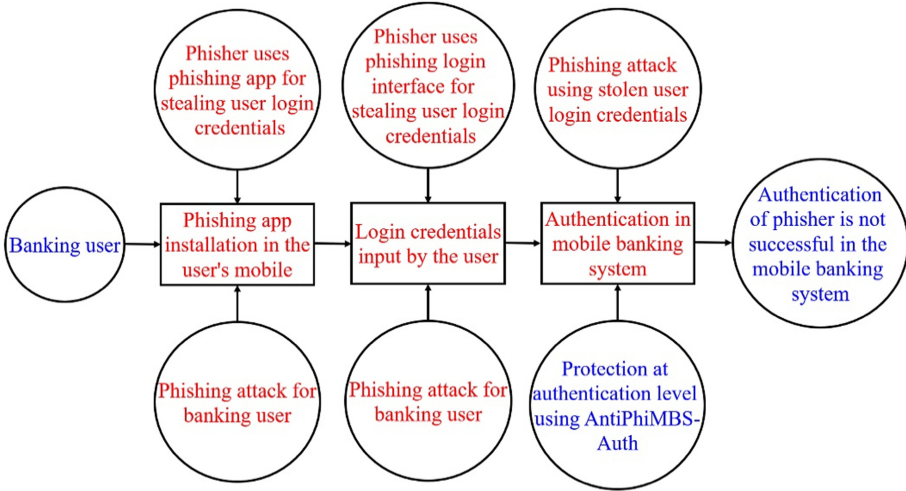


Fig. 1. Phishing attack protection in the mobile banking system at the authentication level

This paper proposes the architecture of the anti-phishing model AntiPhiMBS-Auth. It also verifies that AntiPhiMBS-Auth satisfies the system specification and security properties and is error-free to implement in financial institutions.

3.1 Architecture of Anti-phishing Model AntiPhiMBS-Auth

The architecture of the anti-phishing model AntiPhiMBS-Auth consists of the model for defending against phishing attacks in the mobile banking system at the authentication level. Participating entities in the model are mobile user, bank, bank application, mobile banking system, and phishing application. A mobile user opens an account in a bank and receives login parameters for authentication in the mobile banking system. The bank develops a bank application that communicates with the user and the mobile banking system server. The bank shares required parameters with the bank application and the

Table 1. Notations used in AntiPhiMBS-Auth

Notation	Description	Notation	Description
U	Mobile User	mobNo	Mobile Number
B	Bank	app	Application
MBS	Mobile Banking System	appId	Application Id
uId	User id	BA	Bank App
lgnPwd	Login Password	PA	Phishing App
uniqIdAuth	Unique Id for Authentication		

mobile banking system. The phisher might develop a phishing application for impersonating the attacks in the mobile banking system. Notations of entities and various parameters used by AntiPhiMBS-Auth are in Table 1.

Entities and Initial Conditions for Working of AntiPhiMBS-Auth

- A mobile user (U) opens an account in the Bank (B).
- Bank provides uId, lgnPwD, and unqIdAuth to the user for authentication in the Mobile Banking System (MBS).
- Bank shares uId, lgnPwD, unqIdAuth, appId, and mobNo of each user to MBS.
- Each of the banking applications is identified by an appId, and the bank administers the database of all appId.
- Only bank and MBS know the relationship between uId, and unqIdAuth.
- Only bank, bank app, and MBS know the relationship between appId and uId.
- Users do not reveal the information provided by the bank to others.

Model for Defending Against Phishing Attacks in the Mobile Banking System at the Authentication Level

This model proposes a unique id for authentication (unqIdAuth) and an application id (appId) system in addition to the traditional login credentials to strengthen the security for authentication in the mobile banking system. The participating entities (User, bank, bank app, and mobile banking system) of the model must follow the necessary steps for the successful operation of AntiPhiMBS-Auth to mitigate the phishing attacks in the

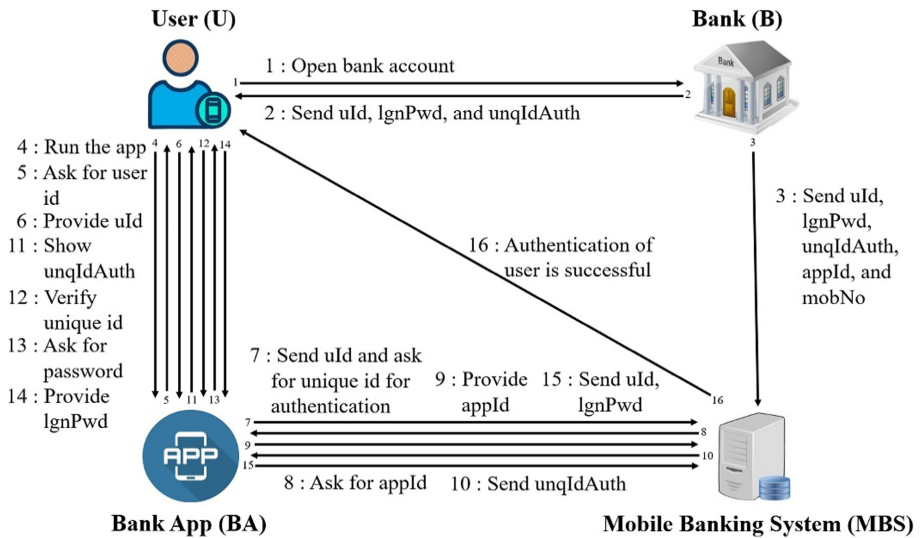


Fig. 2. Scenario of authentication in the mobile banking system using bank app

mobile banking system at the authentication level. The scenario of authentication in the mobile banking system using a bank app is in Fig. 2.

Scenario of Authentication in the Mobile Banking System Using Bank App

The following steps are necessary for authentication in MBS using a bank app.

- Step 1. A mobile user (U) opens a bank account in the Bank (B).
- Step 2. Bank sends user id (uId), login password (lgnPwd), and a unique id for authentication (unqIdAuth) to the user for authentication in the mobile banking system (MBS).
- Step 3. Bank sends user id (uId), login password (lgnPwd), unique id for authentication (unqIdAuth), application id (appId), and mobile number (mobNo) of each user to the mobile banking system (MBS).
- Step 4. A mobile user runs the installed mobile app.
- Step 5. Bank app (BA) asks for a user id from the user.
- Step 6. The user provides a uId to BA.
- Step 7. BA sends uId to MBS and requests for a unique id for authentication for uId.
- Step 8. MBS asks for an appId from BA.
- Step 9. BA provides an appId to MBS.
- Step 10. MBS searches the unique id for authentication based on the user id and sends a unique id for authentication to BA.
- Step 11. BA shows unqIdAuth to the user.
- Step 12. The user verifies the unqIdAuth.
- Step 13. BA asks for a login password from the user.
- Step 14. The user provides a lgnPwd to BA.
- Step 15. BA sends uId and lgnPwd to MBS for authentication.
- Step 16. MBS verifies the uId, lgnPwd, unqIdAuth, and authentication of the user is successful in MBS.

In the scenario of authentication in the mobile banking system using the bank app, in addition to the login credentials (user id and login password), the bank manages a unique id for authentication for each user. Furthermore, the bank also administers an application id for its bank application. Bank application knows its application id that is already known to the mobile banking system too. The mobile banking system knows the relationship among user id, login password, and a unique id for authentication for each user of the mobile banking system. The bank app asks the user to input the user id after the user runs the application. The bank app requests the mobile banking system for a unique id for authentication after getting the user id from the user. The mobile banking system wants to verify the bank app and asks to input the application id. The mobile banking system sends a unique id for authentication after confirming the correct application id from the bank app. The bank app shows the unique id for authentication to the user after getting it from the mobile banking system. The users have the choice for entering the password within the authentication process. The users have the choice of not entering the password if the bank app does not show the right unique id for authentication to the users. The user verifies the unique id and inputs the password as long as the unique id is correct. Then, the banking app requests the mobile banking system for authentication with login

credentials. The mobile banking system authenticates the user for the operation of the mobile banking system if the login credentials are correct.

Scenario of Authentication in the Mobile Banking system Using Phishing App

Even though banking users might be knowing the correct procedure for downloading the bank app, they might receive phishing emails or phishing SMS, or phishing social media platform messages from the phishers. Users might download and start the phishing app unintentionally. Sometimes, users might click phishing links and are redirected to the phishing login screen to steal the login credentials. Thus, phishers collect the login credentials from the users either by a phishing app or by a phishing login screen. The scenario of authentication in the mobile banking system using a phishing app is in Fig. 3.

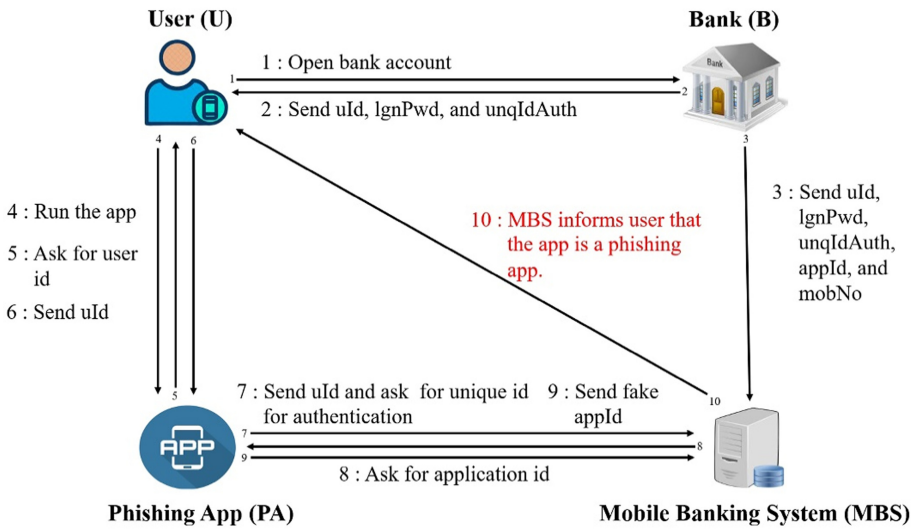


Fig. 3. Scenario of authentication in the mobile banking system using phishing app

The following steps may be executed in the scenario of authentication using a phishing app.

- Step 1. A mobile user (U) opens a bank account in the Bank (B).
- Step 2. Bank sends user id (uId), login password (lgnPwd), and a unique id for authentication (unqIdAuth) to the user for authentication in the mobile banking system (MBS).
- Step 3. Bank sends user id (uId), login password (lgnPwd), unique id for authentication (unqIdAuth), application id (appId), and mobile number (mobNo) of each user to the mobile banking system (MBS).
- Step 4. User may receive phishing emails or phishing SMS or phishing social networking messages with links to login into the phisher's phishing app. User may run the phishing app.
- Step 5. Phishing app asks for a user id from the user.

- Step 6. The user may provide uId to the phishing app.
- Step 7. Phishing app sends uId to the MBS and requests for a unique id for authentication for that user.
- Step 8. MBS asks for an app id to the phishing app.
- Step 9. Phishing app provides fake app id to the MBS.
- Step 10. MBS cannot find the phisher’s app id in the database and informs the user that the app is a phishing app.

Banking users might use phishing apps or phishing login interface unknowingly. Phishing apps ask for a user id to fool the user by imitating the procedure of the banking app. The user may provide a user id to the phishing app. Phishing apps send valid user id to the MBS and request a unique id for authentication for that user. MBS asks for the application id to the phishing app. Phishing apps provide a fake phishing app id to the MBS. MBS verifies the phishing app id and knows that the unique id requester is a phishing app. After that, MBS informs the user about the phishing app. On the other hand, the phishing app does not show a unique id for authentication to the user, and the user does not provide a password in the phishing app. Thus, AntiPhiMBS-Auth prevents the phishers from authenticating in the mobile banking system and forbids them from doing the transactions in the mobile banking system.

3.2 Verification of Proposed Anti-phishing Model AntiPhiMBS-Auth

We specified the system properties and security properties and developed a verification model of AntiPhiMBS-Auth using PROMELA. We verified the PROMELA verification model employing the SPIN. This paper does not show the PROMELA codes (239 lines) because of space limitations but explains the overview of the PROMELA codes. The PROMELA verification model of AntiPhiMBS-Auth consists of the processes, message channels, and data types. The processes used in the verification model of AntiPhiMBS-Auth are in Table 2.

Table 2. Processes used in AntiPhiMBS-Auth

Process name	Description
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 it is responsible for the administration of the mobile banking system for all the banking users
mobileBankingSystem	The process represents the mobile banking system that offers banking services to the banking users using mobile
bankApp	The process represents the bank’s genuine application which communicates with the user and the mobile banking system
phishingApp	The process represents the phisher’s app which imitates the bank application and tries to fool the users to collect login credentials for performing the phishing attacks

The processes in the PROMELA model communicate using message channels. Message channels are used to model the exchange of data between the processes. The message channels used for communication in the AntiPhiMBS-Auth model are in Table 3.

Table 3. Channels used in AntiPhiMBS-Auth

Channel name	Description
mobileUser_bank	It is used to send messages from mobileUser to bank
bank_mobileUser	It is used to send messages from bank to mobileUser
bank_mobileBankingSystem	It is used to send messages from bank to mobileBankingSystem
mobileUser_bankApp	It is used to send messages from mobileUser to bankApp
bankApp_mobileUser	It is used to send messages from bankApp to mobileUser
bankApp_mobileBankingSystem	It is used to send messages from bankApp to mobileBankingSystem
mobileBankingSystem_bankApp	It is used to send messages from mobileBankingSystem to bankApp
mobileBankingSystem_mobileUser	It is used to send messages from mobileBankingSystem to mobileUser
mobileUser_phishingApp	It is used to send messages from mobileUser to phishingApp
phishingApp_mobileUser	It is used to send messages from phishingApp to mobileUser
phishingApp_mobileBankingSystem	It is used to send messages from phishingApp to mobileBankingSystem
mobileBankingSystem_phishingApp	It is used to send messages from mobileBankingSystem to phishingApp

We defined the processes and message channels in the PROMELA code of AntiPhiMBS-Auth. All the processes of AntiPhiMBS-Auth communicate with each other using the above-defined message channels for the operation of AntiPhiMBS-Auth.

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

$\square(((usrId==bankUsrId)\&\&(lgnPwd==bankLgnPwd)\&\&(usrUnqIdAuth==bankUnqIdAuth))\rightarrow \langle \rangle (authenticationSuccess==true))$.

Authentication of the user in the mobile banking system is successful only 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, and (iii) the unique id for authentication provided by the user and received by MBS from the bank is equal.

4 Results and Discussion

This paper verifies the safety properties and LTL properties of the proposed model AntiPhiMBS-Auth. 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 set advanced parameters in the SPIN environment for optimal results during the verification. We set physical memory available as 4096 (in Mbytes), maximum search depths (steps) as 1000000, estimated state space size as 1000, search mode as depth-first search (partial order reduction), and storage mode as bitstate/ supertrace for the verification. Besides, extra compile-time directives were set to DVECTORSZ as 9216 to avoid the memory error during the experiments. After that, we ran SPIN to verify the safety properties of AntiPhiMBS-Auth for up to 100 users. SPIN checked the state space for invalid end states and assertion violations during the verification of safety properties. The SPIN verification results for safety properties are in Table 4.

Table 4. Verification results for safety properties

No. of users	Time (Seconds)	Memory (Mbytes)	Transitions	States stored	Depth	Safety properties verification status
10	0.05	39.026	29786	1429	812	Verified
20	0.16	39.026	56906	2709	1472	Verified
30	0.34	39.026	84026	3989	2132	Verified
40	0.58	39.026	111146	5269	2792	Verified
50	0.88	39.026	138266	6549	3452	Verified
60	1.25	39.026	165386	7829	4112	Verified
70	1.69	39.026	192506	9109	4772	Verified
80	2.23	39.026	219626	10389	5432	Verified
90	2.72	39.026	246746	11669	6092	Verified
100	3.33	39.026	273866	12949	6752	Verified

Table 4 shows the results obtained from SPIN depicting the elapsed time, total memory usage, number of states transitioned, states stored, depth reached, and verification status for safety properties for various users. The SPIN verification results indicate that there is an unceasing rise in the verification time with the increase in the number of users, and the required memory remained constant for all the users during the verification of AntiPhiMBS-Auth. Moreover, an increasing trend is seen for the states stored, depth reached, and transitions for various users during the experiment. Also, the SPIN verification did not detect any deadlock or any errors during the runs of the AntiPhiMBS-Auth model.

After that, we executed SPIN in the same computing environment to verify the LTL properties for up to 100 users. SPIN checked the statespace for never claim and assertion violations in the run of LTL properties. The SPIN verification result for LTL properties is in Table 5.

Table 5. Verification results for LTL properties

No. of users	Time (Seconds)	Memory (Mbytes)	Transitions	States stored	Depth	LTL properties verification status
10	0.05	39.026	29786	1429	1487	Verified
20	0.16	39.026	56906	2709	2687	Verified
30	0.34	39.026	84026	3989	3887	Verified
40	0.58	39.026	111146	5269	5087	Verified
50	0.88	39.026	138266	6549	6287	Verified
60	1.26	39.026	165386	7829	7487	Verified
70	1.68	39.026	192506	9109	8687	Verified
80	2.18	39.026	219626	10389	9887	Verified
90	2.75	39.026	246746	11669	11087	Verified
100	3.32	39.026	273866	12949	12287	Verified

Table 5 depicts the results obtained from SPIN showing the elapsed time, total memory usage, states transitioned, states stored, and verification status for LTL properties for various users. The memory required for the verification of LTL properties for all the users is the same. The SPIN verification results show that there is a perpetual rise in the verification time with the increase in the number of users during the verification of LTL properties. Furthermore, there is also a continuous rise in the number of transitions, states stored, elapsed time, and depth with the increase in the number of users in the experiment. The SPIN verified the LTL properties of the AntiPhiMBS-Auth model successfully.

Table 4 shows the results after SPIN checked for the existence of deadlocks and assertion violations by generating the execution paths during the verification of the AntiPhiMBS-Auth model. Similarly, Table 5 shows the results after SPIN checked for temporal properties we expect the system behavior of the AntiPhiMBS-Auth model to conform during the system lifetime. The results of these experiments show that there is no error in the design of AntiPhiMBS-Auth. No counterexample was generated by SPIN during the experiments. Hence, the verified AntiPhiMBS-Auth is applicable for the development and implementation of the anti-phishing system within the banks and financial institutions globally to mitigate the continued phishing attacks in the mobile banking industry.

5 Conclusion and Future Work

The most conventional sort of phishing attack within the mobile banking industry is in the appearance of an authentication attack. Phishers employ a phishing app or phishing login interface to compile login credentials from the users and exploit the stolen credentials for authentication within the mobile banking industry. Even though credential thefts are soaring day by day, any anti-phishing model for the mitigation of such attacks has not been developed so far for the mobile banking industry. Therefore, this paper developed a new anti-phishing model for Mobile Banking System at the authentication level (AntiPhiMBS-Auth) to mitigate the phishing attacks in the mobile banking industry. A phisher might send phishing emails/SMS/social media messages to the banking users and redirect them to download the phishing app or input login credentials in the phishing login interface. Banking users might install, run, and input user id in the phishing app or the phishing login interface inadvertently. However, AntiPhiMBS-Auth applies a unique id for the authentication system, and users have the choice to not input the password without verifying the unique id for authentication. Besides, AntiPhiMBS-Auth employs an application id for the bank app so that the mobile banking system can differentiate the genuine bank app from the phishing app. Hence, AntiPhiMBS-Auth prevents phishing attacks in the mobile banking system as the phisher cannot disclose the unique id to the users, and the phishing app cannot evince its identity by rendering a genuine application id to the mobile banking system.

We observed from our experimental SPIN results of the AntiPhiMBS-Auth Promela program that the AntiPhiMBS-Auth does not encompass any deadlocks or errors within the model. Moreover, SPIN verified all the safety properties and LTL properties within the PROMELA model of AntiPhiMBS-Auth. Hence, financial institutions can implement this verified AntiPhiMBS-Auth model to mitigate the unending phishing attacks within the mobile banking industry and increase the mobile banking transactions to transform into a cashless society in this era of digital banking.

In future research, we will propose a new anti-phishing model to mitigate fraudulent transactions in the mobile banking system at the transaction level. Moreover, we will further extend the AntiPhiMBS-Auth model in mitigating phishing attacks in other digital systems utilizing login credentials for authentication.

References

1. Tchakounte, F., Molengar, D., Ngossaha, J.M.: A description logic ontology for email phishing. *Int. J. Inf. Secur. Sci.* **9**(1), 44–63 (2020)
2. Subasi, A., Kremic, E.: Comparison of adaboost with multiboosting for phishing website detection. *Procedia Comput. Sci.* **168**, 272–278 (2020). <https://doi.org/10.1016/j.procs.2020.02.251>
3. Ozker, U., Sahingoz, O.K.: Content based phishing detection with machine learning. In: 2020 International Conference on Electrical Engineering (ICEE), Istanbul, Turkey, pp. 1–6. IEEE (2020). <https://doi.org/10.1109/ICEE49691.2020.9249892>
4. Priya, S., Selvakumar, S., Velusamy, R.L.: Detection of phishing attacks using radial basis function network trained for categorical attributes. In: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1–6. IEEE (2020). <https://doi.org/10.1109/ICCCNT49239.2020.9225549>

5. Odeh, A., Alarbi, A., Keshta, I., Abdelfattah, E.: Efficient prediction of phishing websites using multilayer perceptron (MLP). *J. Theoret. Appl. Inf. Technol.* **98**(16), 3353–3363 (2020)
6. Hossain, S., Sarma, D., Chakma, R.J.: Machine learning-based phishing attack detection. *Int. J. Adv. Comput. Sci. Appl.* **11**(9), 378–388 (2020)
7. Su, Y.: Research on website phishing detection based on LSTM RNN. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, pp. 284–288. IEEE (2020). <https://doi.org/10.1109/ITNEC48623.2020.9084799>
8. Abiodun, O., Sodiya, A.S., Kareem, S.O.: Linkcalculator – an efficient link-based phishing detection tool. *Acta Informatica Malaysia* **4**(2), 37–44 (2020). <https://doi.org/10.26480/aim.02.2020.37.44>
9. Sharathkumar, T., Shetty, P.R., Prakyath, D., Supriya, A.V.: Phishing site detection using machine learning. *Int. J. Res. Eng. Sci. Manag.* **3**(6), 240–243 (2020)
10. Drury, V., Meyer, U.: No phishing with the wrong bait: reducing the phishing risk by address separation. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, pp. 646–652. IEEE (2020). <https://doi.org/10.1109/EuroSPW51379.2020.00093>
11. Awan, M.A.: Phishing attacks in network security. *LC Int. J. STEM (Sci. Technol. Eng. Math)* **1**(1), 29–33 (2020)
12. Alabdan, R.: Phishing attacks survey: types, vectors, and technical approaches. *Future Internet* **12**(10), 1–39 (2020). <https://doi.org/10.3390/fi12100168>
13. Miller, B., Miller, K., Zhang, X., Terwilliger, M.G.: Prevention of phishing attacks: a three-pillared approach. *Issues Inf. Syst.* **21**(2), 1–8 (2020)
14. Ustundag Soykan, E., Bagriyanik, M.: The effect of smishing attack on security of demand response programs. *Energies* **13**(17), 1–7 (2020). <https://doi.org/10.3390/en13174542>
15. Natadimadja, M.R., Abdurrohman, M., Nuha, H.H.: A survey on phishing website detection using hadoop. *Jurnal Informatika Universitas Pamulang* **5**(3), 237–246 (2020). <https://doi.org/10.32493/informatika.v5i3.6672>
16. Chaudhry, J.A., Chaudhry, S.A., Rittenhouse, R.G.: Phishing attacks and defenses. *Int. J. Secur. Its Appl.* **10**(1), 247–256 (2016). <https://doi.org/10.14257/ijssia.2016.10.1.23>
17. Shaik, C.: Counter challenge authentication method: a defeating solution to phishing attacks. *Int. J. Comput. Sci. Eng. Appl.* **10**(1), 1–8 (2020). <https://doi.org/10.5121/ijcsea.2020.10101>
18. Aravindh, B., Ambeth Kumar, V.D., Harish, G., Siddarth, V.: A novel graphical authentication system for secure banking systems. In: 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, India, pp. 177–183. IEEE (2017). <https://doi.org/10.1109/ICSTM.2017.8089147>
19. Sukanya, S., Saravanan, M.: Image based password authentication system for banks. In: 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, pp. 1–8. IEEE (2017). <https://doi.org/10.1109/ICICES.2017.8070764>
20. Modibbo, A., Aliyu, Y.: Cashless society, financial inclusion and information security in Nigeria: the case for adoption of multifactor biometric authentication. *Int. J. Innov. Sci. Res. Technol.* **4**(11), 872–880 (2019)
21. Tam, L.T., Chau, N.M., Mai, P.N., Phuong, N.H., Tran, V.K.H., Hanh, P.H.: Cybercrimes in the banking sector: case study of Vietnam. *Int. J. Soc. Sci. Econ. Invention* **6**(5), 272–277 (2020). <https://doi.org/10.23958/ijsssei/vol06-i05/207>
22. Lakshmi Prasanna, A.V., Ramesh, A.: Secure Internet banking authentication. *J. Eng. Serv.* **11**(2), 152–161 (2020)
23. Aldwairi, M., Masri, R., Hassan, H., ElBarachi, M.: A novel multi-stage authentication system for mobile applications. *Int. J. Comput. Sci. Inf. Secur.* **14**(7), 389–396 (2016)

24. Srinivasa Rao, A.H., Deepashree, C.S., Pawaskar, D., Divya, K., Drakshayini, L.: GeoMob - a geo location based browser for secured mobile banking. *Int. J. Res. Eng. Sci. Manag.* **2**(5), 515–519 (2019)
25. Miiri, E.M., Kimwele, M., Kennedy, O.: Using keystroke dynamics and location verification method for mobile banking authentication. *J. Inf. Eng. Appl.* **8**(6), 26–36 (2018)
26. Song, J., Lee, Y.S., Jang, W., Lee, H., Kim, T.: Face recognition authentication scheme for mobile banking system. *Int. J. Internet Broadcast. Commun.* **8**(2), 38–42 (2016). <https://doi.org/10.7236/IJIBC.2016.8.2.38>
27. Macek, N., Adamovic, S., Milosavljevic, M., Jovanovic, M., Gnjatovic, M., Trenkic, B.: Mobile banking authentication based on cryptographically secured iris biometrics. *Acta Polytechnica Hungarica* **16**(1), 45–62 (2019)
28. Credential spill report. https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape_Credential_Spill_Report_2018.pdf. Accessed 20 Nov 2020
29. 2019 Phishing trends and intelligence report. <https://info.phishlabs.com/2019-pti-report-evolving-threat>. Accessed 20 Nov 2020
30. 2020 phishing and fraud report. https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf. Accessed 20 Nov 2020