Modeling and Verification of Contactless Mobile Banking System in E-Banking Using SPIN

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. During this prevailing generation of the digital world, mobile users are multiplying globally by leaps and bounds. A mobile banking system is an electronic channel for Electronic Banking (E-Banking) all over the world. The utility of mobile banking systems has become one of the innovations to transform financial institutions from the traditional to the digital world with all the banking services. However, financial institutions do not provide enhanced banking services and electronic cheques using the mobile banking system globally. This paper proposes a new contactless mobile banking system (C-MBS) that integrates enhanced banking services with novel functions like electronic cheques, registration of the user, and cancellation of the user account included in the model. This paper develops an extended finite state machine model with parameters, variables, and constraints for C-MBS. This paper also develops a verification model of C-MBS with system properties specified utilizing process meta language (PROMELA) and security properties applying linear temporal logic (LTL). A simple promela interpreter (SPIN) is employed to verify the verification model of C-MBS. SPIN verification results confirm that the proposed C-MBS model is free from deadlocks and errors. Hence, the financial institutions can implement this model as a secure enhanced mobile banking system in E-banking. Banking users can use the enhanced banking services remotely using C-MBS on mobile and will play a significant role towards a cashless society in the digital world.

Keywords: Mobile banking system · Security · Temporal logic · SPIN · Verification

1 Introduction

Electronic Banking (E-banking) provides banking services and products through electronic channels such as mobile banking systems, Internet banking systems, ATM, telephone banking systems, etc. E-banking has many advantages along with real-time and all-time access and has been expanding globally. There are many channels for using E-banking, and the mobile banking system is becoming the most-used channel for the utilization of E-banking. Banking users do log in into the online banking (Internet banking) using the internet to get the banking services. Similarly, banking users download bank applications on their mobile and log in into the mobile banking system using the app

O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12954, pp. 581–597, 2021.
https://doi.org/10.1007/978-3-030-86979-3_41

to get the banking services. During this prevailing generation of the digital world, mobile users are multiplying globally by leaps and bounds. The use of mobile banking systems has become one of the innovations to transform financial institutions from traditional to the digital world with required banking services. A global pandemic (COVID-19) has created a very difficult situation, and customers would like to access all of the banking services remotely. Banking customers use mobile banking systems just for balance inquiry, mobile recharge, utility payment (such as electricity bill payment, water bill payment, etc.), small amount fund transfer in many countries. The mobile banking system is still not utilized for providing enhanced banking services (such as fund transfer, third-party payment, lending, etc.) globally. Banking customers do not use the mobile banking system because of not having enhanced banking services and security problems.

Digital 2021 global overview report [30] shows that there are approximately 5.22 billion unique mobile phone users among 7.83 billion population globally, but mobile banking users in 2019 is 1.8 billion only (Juniper research report 2020). It is a well-known fact that the number of banking customers is large, and the number of mobile banking users is low in many countries. Therefore, there is a need for complete automation and a secure mobile banking system to increase mobile banking users in E-banking.

Some research in E-banking is modeling and verification of payment systems [1], retail banking system [2], and Internet payment system [3]. The authors of [1] presented modeling and verification of Automated Teller Machine (ATM) for the interbank payment system. The authors of [2] accomplished modeling and verification of a retail banking system. Zhang, Ma, Shi, and Zhu [3] employed the model checking method to verify the security and reliability of Internet payment systems. The authors of [4] focused on modeling and verification of a new mobile payment system. Shaikh, And, and Devane [5] focused on modeling and verification of payment protocol, and the authors of [6] emphasized modeling and verification of extensible authentication protocol. Ciurea [7] developed a model of mobile application in a collaborative banking system. Aithal [8] compared a mobile banking system with an ideal banking system. Bojjagani and Sastry [9] proposed a mobile banking model with an end-to-end SMS-based application system. Anwarul Islam and Salma [10] developed a model of mobile banking for banking facilities to rural people. However, the authors have not incorporated enhanced banking services in [7–10], and users have limited banking operations facilities in the proposed model of the mobile banking system. The authors of [11] performed a review of enhancements in the mobile payment system, Istrate [12] developed a cardless withdrawal system for the mobile banking system, and the authors of [13] developed a model for the mobile banking payment system. The authors of [14] developed a model for an Internet banking system, and Uddin and Akhi [15] developed a model for an electronic payment system. The developed mobile banking models [11–15] do not include all of the enhanced banking services for the end-users.

The authors presented security challenges for mobile banking systems [16], vulnerabilities in E-banking [17], enhanced security model for the mobile banking system in Tanzania [18], and a case study of Croatian banks using biometrics in the mobile banking system [19]. The authors of [20, 21] focused on practices, challenges, and security issues of the mobile banking system in India. The authors of [22–25] studied technology adoptions for the mobile banking system, and [26, 27] reviewed user satisfaction using the mobile banking system. The authors of [28] emphasized the blockchain based electronic cheque (e-cheque) clearance framework that allows the drawer to download the e-cheque as a valid e-cheque. The authors of [29] used a third party for the trust in e-cheque in the electronic payment system. However, the proposed e-cheque is not secure because the e-cheques are available in pdf form and the risk increases when the banking user downloads the pdf and uploads the pdf using the online banking system.

Some of the earlier researchers have developed models for ATM [1], retail banking system [2], and Internet payment system [3]. Some researchers have developed different models for mobile banking systems [7–15]. Some researchers have emphasized security issues [16–21] on the model of the mobile banking system. However, the adoptions for mobile banking system [22–25] and user's satisfaction using mobile banking system [26, 27] show that there is still a need for improvement in the model of the mobile banking system. Banking users download the e-cheque in pdf manually and upload the pdf [28, 29] using the online banking system. However, cybercriminals impersonate different attacks during the download and upload of the e-cheque in the online banking system. Unfortunately, earlier researchers have not incorporated the enhanced banking services and have not included automatic e-cheque in the proposed model of the mobile banking system. To overcome this gap, the paper proposes a new contactless mobile banking system (C-MBS) that consists of enhanced banking functionalities and a novel concept of a secure mobile banking based e-cheque system for banking operations.

C-MBS consists of the following modules for managing the users and providing banking services using the mobile banking system.

- Registration
- Fund transfer
- Third-party payment
- Digital lending
- e-cheque issuing
- e-cheque clearing
- Cancellation

This research aims to build an enhanced mobile banking system in which banking customers can request for registration in the mobile banking system and can use the enhanced banking services using C-MBS. C-MBS can cancel the users based on the passiveness of the users in the mobile banking system. The proposed system is developed to be considered by the banks. The system behaviors of the model are specified in a process meta language (PROMELA) and security properties are specified using linear temporal logic (LTL). This paper uses SPIN to formally verify the proposed C-MBS model of the mobile banking system. The rest of the paper is further structured as follows: Sect. 2 describes the related works. Section 3 describes the new model of a contactless mobile banking system, Sect. 4 presents the results and discussion, and Sect. 5 describes conclusions and future work.

2 Related Work

The utility of E-Banking has been expanding for digital payment in the financial world, and researchers have been working to provide better solutions for secured enhanced functionalities in E-Banking. Researchers have focused on the modeling and verification of ATM, retail banking system, Internet banking system, etc. in E-banking. Authors of [1–3] presented the modeling and verification of electronic channels in E-banking. Obaid, Kazmi, and Qasim [1] presented modeling and verification of 1-link Automated Teller Machine (ATM) for the interbank payment system. Transactional properties of 1-link ATM are specified and verified using SPIN, but security properties are not specified and verified in the system to minimize the attacks in the E-banking system. The paper recommended the mobile banking system for future research. Shi, Ma, Yang, and Zhang [2] accomplished model checking and verification of the retail banking system through an ATM using SPIN and recommended the mobile banking system as future research. Zhang, Ma, Shi, and Zhu [3] employed the model checking method to verify the security and reliability of Internet payment systems. Ahamad, Udgata, and Sastry [4] proposed formal verification of a novel payment instrument in the name of mobile traveler's check (MTC) for mobile commerce applications. Shaikh, And, and Devane [5] focused on formal verification of payment protocol using AVISPA (automated validation of internet security protocols and applications), and Hegde, H K, and Singh [6] emphasized on modeling and verification of extensible authentication protocol using PROMELA and SPIN. Ciurea [7] presented a classification of mobile applications with an accent on collaborative mobile applications. Aithal [8] compared a model of the mobile banking system with an ideal banking system that can have significant performance in specified conditions. Bojjagani and Sastry [9] proposed a model to address the security of SMS (Short Message Service) using elliptic curve cryptography and the proposed model provides end-to-end SMS communication for the banking users. Anwarul Islam and Salma [10] described mobile banking operations and banking facilities to rural people in Bangladesh.

Dahlberg, Guo, and Ondrus [11] reviewed enhancements in mobile payment research after a previous literature review (Dahlberg et al. 2008b) and pointed out that the researchers have continued to focus on the same topics for mobile payment systems. Istrate [12] developed a model of a cardless withdrawal system for mobile banking applications for payments and money transfer. Yang, Liu, and Chiu [13] developed a model for a mobile banking payment system in which customers use electronic money instead of cash. Alanazi, Alnaqeib, Hmood, Zaidan, and Nabhani [14] used unified modeling language (UML) diagrams and developed architectures for the Internet banking system. Uddin and Akhi [15] described a model of the E-wallet system as an electronic payment system to replace the existing physical wallet, with its notes, coins, plastic cards, ATM cards, and loyalty cards in Bangladesh.

Islam [16] reviewed the security challenges of mobile banking and payment system. Brar, Sharma, and Khurmi [17] studied various security aspects including vulnerabilities in E-banking. Nyamtiga, Sam, and Laizer [18] focused on an SMS-based enhanced security model with security features to enhance data protection across mobile networks for the mobile banking systems in Tanzania. Avdic [19] explained the use of biometrics in mobile banking security using a case study of Croatian banks. Gupta, Kumar, and

Bharadwaj [20] proposed a web-based application with all related information in a centralized database that provides a banking facility through which all payments can be done at a single place using a mobile banking system. Goyal, Pandey, and Batra [21] developed a classification framework for mobile banking research.

Alalwan, Dwivedi, and Rana [22] investigated the factors influencing behavioral intention and adoption of mobile banking by customers of Jordanian banks. The results showed that behavioral intention is significantly and positively influenced by performance expectancy, effort expectancy, hedonic motivation, price value, and trust. Al-Jabri and Sohail [23] investigated many factors that may help the bankers to design suitable mobile services that can be adoptable by banking customers in Saudi Arabia. Raja, Umer, and Shah [24] found the new determinants of ease of use for mobile banking adoption in Pakistan. Safeena, Date, Kammani, and Hundewale [25] determined the consumer's perspective on mobile banking adoption in India. Bharti [26] focused on the roadmap for the proper implementation and adoption of the mobile banking system for banking users. Asfour and Haddad [27] studied the mobile banking important dimensions such as reliability, flexibility, privacy, accessibility, ease of navigation, efficiency, safety, etc., and measured the impact of mobile banking on enhancing customer satisfaction in Jordan. Singh, Kumar, and Vardhan [28] proposed a blockchain based e-cheque clearance framework that allows the banking users to download the e-cheque and used it for upload as and when required or print the pdf version of the e-cheque. Yahid, Nobakht, and Shahbahrami [29] focused on the trust in e-cheque in electronic payments using a third party as a guarantor for the security of the e-cheque.

Our paper proposes a new contactless mobile banking system (C-MBS) with enhanced banking functionalities and a novel concept of a secure e-cheque for banking customers. Banks and financial institutions can implement this model for providing enhanced banking services and a secure e-cheque facility to the banking users using mobile for E-Banking globally.

3 Formal Modeling of C-MBS

The formal modeling methods provide a mechanism for eliminating problems in the early phases of the software development life cycle. There are different phases in the software development life cycle, and the software must be tested before the implementation in the real world. Software testing using test cases detects errors in the late phases of software development and costs more for fixing the errors. Model-checking and formal verification detects the bugs during the design phase of software development and helps in designing the bug-free system. The proposed model includes enhanced banking services along with e-cheque issuing and e-check clearing using the mobile banking system. Formal modeling of C-MBS consists of an extended finite state machine (EFSM) model and PROMELA model of C-MBS. Notations used in formal modeling of C-MBS are in Table 1.

Table 1. Notations used in formal modeling of C-MBS

Notation	Description	Notation	Description
reg	Registration	pmtAmt	Payment amount
par	Parameter	acBal	Account balance
usrOTP	One time password from user	crRat	Credit rating
mbsOTP	One time password from mobile banking system	minRat	Minimum rating
auth	Authentication	loanAmt	Loan amount
authoriz	Authorization	appLoanAmt	Approved loan amount
usrDOB	Date of birth from user	mbsDOB	Date of birth registered in mobile banking system
MBS	Mobile Banking System	CBS	Core Banking System

3.1 EFSM Model of C-MBS

In a conventional finite state machine (FSM), a transition is associated with a set of input boolean conditions and a set of output boolean functions. EFSM performs a state transition when a given set of conditions are satisfied. EFSM model provides a powerful model for the derivation of functional tests for software systems and protocols. EFSM model of C-MBS presents the complete life cycle of the mobile banking system including registration and cancellation of the banking users in C-MBS as in Fig. 1.

A banking user installs mobile banking applications on their mobile devices and requests for registration in C-MBS. C-MBS verifies the registration parameters such as mobile number, account number, date of birth (dob) etc. and sends OTP to the banking user. MBS verifies the OTP and registers the user in the C-MBS. The banking user requests authentication and access rights for authorization in the mobile banking system. After approval from the C-MBS, the banking user can log in into the C-MBS and perform the required banking operations using the C-MBS. Generally, banking users use the mobile banking system for statements, fund transfers, and third-party payments such as utility payment, merchant payment, QR (quick response) code payment, etc. in developing countries. The EFSM model introduces enhanced banking services such as digital lending, e-cheque issuing, and e-cheque clearing in the C-MBS that are not in practice in many countries. Banking users can request a loan using the C-MBS, and banks can approve the loan and credit in the customer account. Banking users do not have to visit the bank physically multiple times to get a loan from the bank.

There are limitations in the physical cheque, and therefore, it is necessary to switch from the physical cheque to an e-cheque in this era of digital banking. Banks manage digital certificates for the banking users for the security of the e-cheque. Banking users provide the cheque details such as payer name, account number, payee name, amount, date of payment, discount rate, etc. They sign the e-cheque digitally using a private key and request to issue the e-cheque using C-MBS as in Fig. 2. MBS sends the digitally signed e-cheque to the CBS for verification of the cheque. CBS verifies the digital

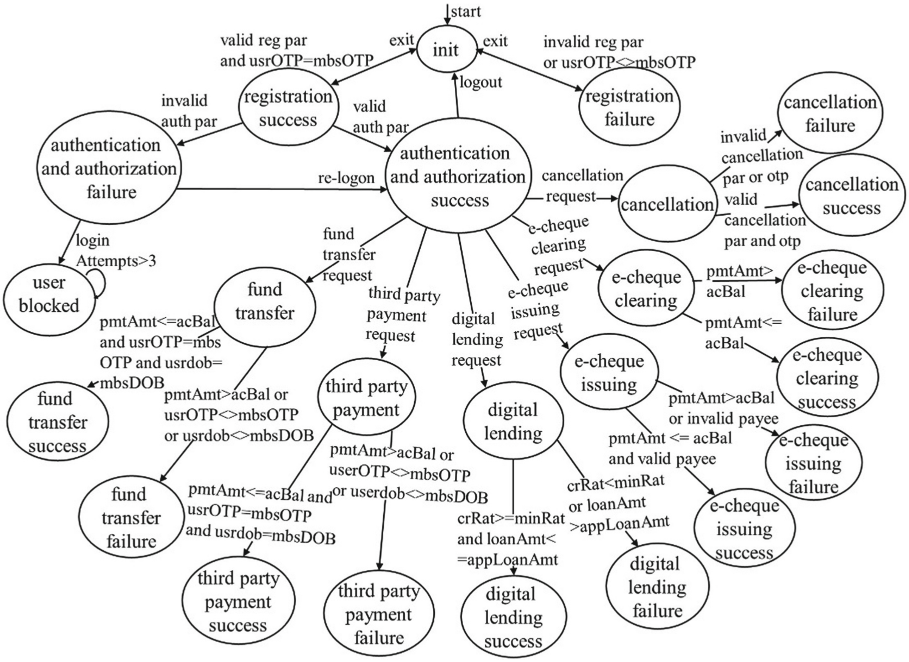

Fig. 1. EFSM model of C-MBS.

certificates and informs the MBS about the validity of the e-cheque. MBS notifies the payer about the issue of the e-check and sends it to the payee using the mobile banking system.

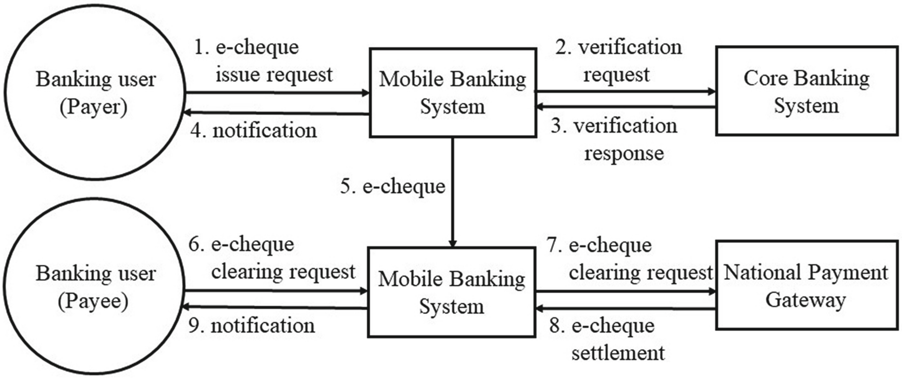

Fig. 2. e-cheque process using C-MBS

The payee does not need to download the e-cheque, and therefore, such an e-cheque mechanism is safer than the earlier pdf downloadable e-cheque. The payee request for clearing of the e-cheque using the mobile banking system. MBS requests a national payment gateway for clearing the e-cheque, and the national payment gateway makes settlement of the e-cheque as per the details of the e-cheques. MBS notify the payee about the settlement of the e-cheque using C-MBS.

The paper proposes cancellation of the users' account in C-MBS. Generally, banking users are registered in the mobile banking system and are not canceled either by themselves or by the bank. Banking users can request account cancelation using the C-MBS, and the bank can approve the cancellation of the users' account. In addition, the bank cancels the users' account automatically after a certain period of passiveness in the mobile banking system. The cancellation function in C-MBS will help in maintaining the data privacy of the banking users' account in the banks.

3.2 PROMELA Model of C-MBS

This paper develops the PROMELA model as the verification model to verify the proposed model C-MBS. The model consists of three basic types of objects. The objects are processes, message channels, and data types.

The following processes are used in the PROMELA model of C-MBS.

- mobileUser
  The process represents the banking user in C-MBS who employs the mobile banking system in mobile for banking services.
- mobileBankingSystem
  The process represents the mobile banking software which communicates with the banking users and the bank and offers banking services on their mobile.
- coreBankingSystem
  The process represents the banking application software with the bank.
- nationalPaymentGateway
  The process represents the private or government-owned centralized payment settlement system in the nation.

The processes in the PROMELA model communicate using message channels. This paper uses the channels as in Table 2.

The simple message flow of the processes in C-MBS is presented using a sequence diagram in Fig. 3. A sequence diagram depicts the interaction between processes in sequential order. It shows the flow of events among the agents (mobileUser, mobileBankingSystem, coreBankingSystem and nationalPaymentGateway) of C-MBS. A mobile user requests for registration in the mobile banking system (MBS) using C-MBS. MBS verifies the registration parameters of the user and verifies the user by sending a one-time password (OTP). After successful registration of the user, C-MBS provides interfaces to the user for the setting of authentication and authorization parameters. User requests for authentication in the system with received login credentials. MBS authenticates the users in the system after validating the authentication and authorization policies enforced for the user. MBS does not permit users to log in if they enter the wrong passwords more than three times.

Upon successful login in the MBS, the user can request for fund transfer with the required parameters. MBS forwards the request for fund transfer to the core banking

Table 2. Channel descriptions for C-MBS PROMELA model

Channel Name	Channel objective
mobileUser_mobileBankingSystem	Messages from mobileUser to mobileBankingSystem
mobileBankingSystem_mobileUser	Messages from mobileBankingSystem to mobileUser
mobileBankingSystem_ coreBankingSystem	Messages from mobileBankingSystem to coreBankingSystem
coreBankingSystem_mobileBankingSystem	Messages from coreBankingSystem to mobileBankingSystem
mobileBankingSystem_nationalPaymentGateway	Messages from mobileBankingSystem to nationalPaymentGateway
nationalPaymentGateway_mobileBankingSystem	Messages from nationalPaymentGateway to mobileBankingSystem

system (CBS). CBS approves the transaction if the transfer amount is less than or equal to the account balance and security parameters are verified. When the user requests third-party payment, MBS forwards the request to CBS and the national payment gateway. They check the constraints for the transaction and approves or disapproves of the transaction based on the parameters of the transaction. When the user requests MBS for digital lending, MBS forwards the request to CBS and grants the loan according to the credit rating of the customer. When user requests for an e-cheque issue to MBS, MBS forwards the request to CBS. CBS checks all the parameters required for e-cheque, issues e-cheque, and sends to the payee using a mobile banking system. Users do not need to download the e-cheque and just request for clearing of e-cheque using C-MBS. The settlement of the e-cheque payment is finalized by the national payment gateway.

4 Results and Discussion

This paper verifies the safety properties and temporal properties of C-MBS using SPIN for proper implementation of the model in the real world. We specified the following security properties using linear temporal logic (LTL) in the verification model of C-MBS.

LTL definition1 (LTL1)

[]((usrDob==mbsDob)&&(userMobileNo==mbsMobileNo)&&(userOTP==mbsOTP))
Authentication parameters such as dob, mobileNo and OTP received from mobile users must be the same as registered in the database of C-MBS during the system lifetime.

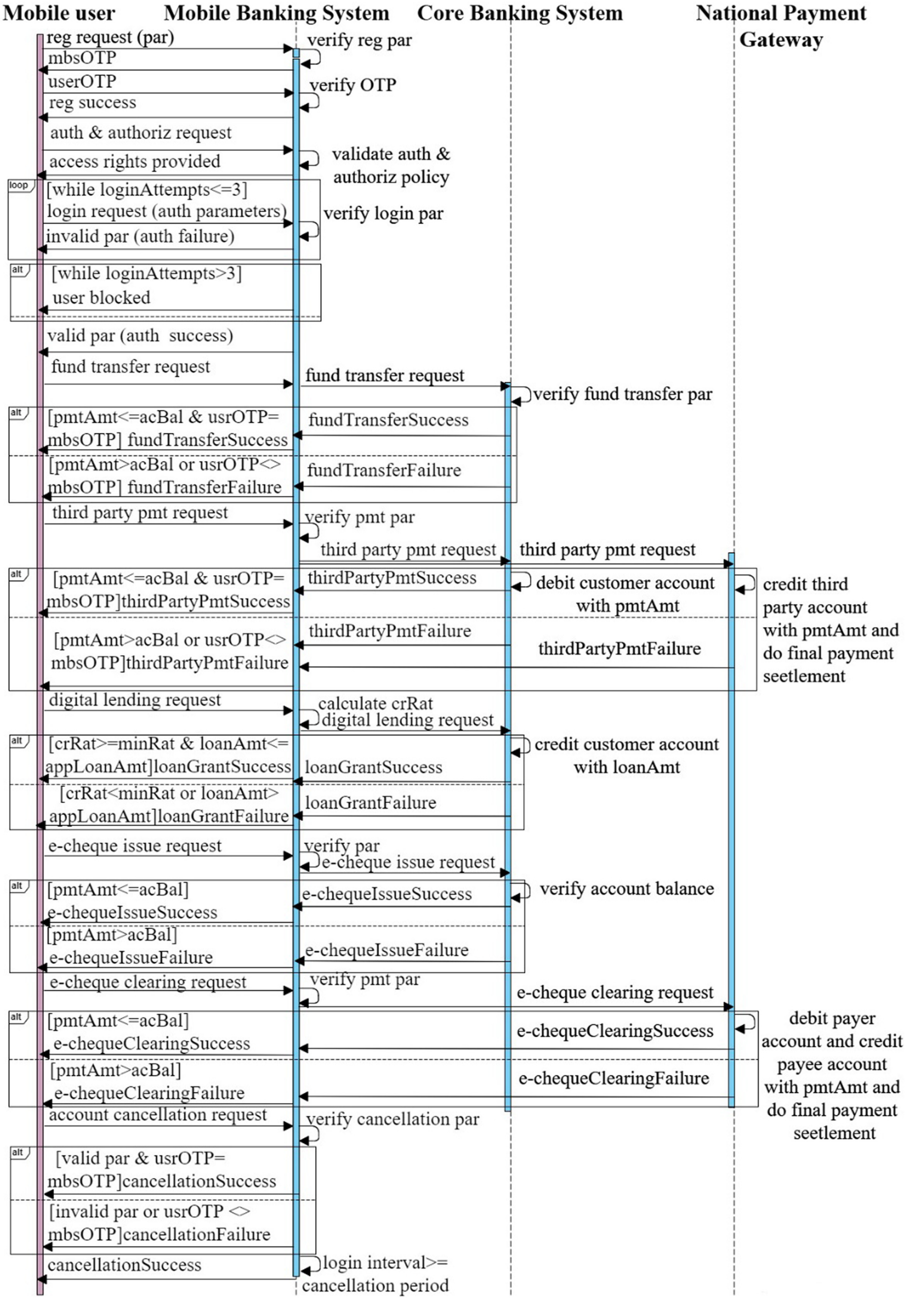
Mobile user
Mobile Banking System
Core Banking System
National Payment Gateway
reg request (par)
verify reg par
mbsOTP
userOTP
verify OTP
reg success
auth & authoriz request
validate auth & authoriz policy
access rights provided
loop
[while loginAttempts<=3]
login request (auth parameters)
verify login par
invalid par (auth failure)
alt
[while loginAttempts>3]
user blocked
valid par (auth success)
fund transfer request
fund transfer request
verify fund transfer par
alt
[pmtAmt<=acBal & usrOTP= mbsOTP] fundTransferSuccess
fundTransferSuccess
[pmtAmt>acBal or usrOTP<> mbsOTP] fundTransferFailure
fundTransferFailure
third party pmt request
verify pmt par
third party pmt request
third party pmt request
alt
[pmtAmt<=acBal & usrOTP= mbsOTP]thirdPartyPmtSuccess
thirdPartyPmtSuccess
debit customer account with pmtAmt
credit third party account with pmtAmt and do final payment seetlement
[pmtAmt>acBal or usrOTP<> mbsOTP]thirdPartyPmtFailure
thirdPartyPmtFailure
thirdPartyPmtFailure
digital lending request
calculate crRat
digital lending request
alt
[crRat>=minRat & loanAmt<= appLoanAmt]loanGrantSuccess
loanGrantSuccess
credit customer account with loanAmt
[crRat<minRat or loanAmt> appLoanAmt]loanGrantFailure
loanGrantFailure
e-cheque issue request
verify par
e-cheque issue request
alt
[pmtAmt<=acBal] e-chequeIssueSuccess
e-chequeIssueSuccess
verify account balance
[pmtAmt>acBal] e-chequeIssueFailure
e-chequeIssueFailure
e-cheque clearing request
verify pmt par
e-cheque clearing request
alt
[pmtAmt<=acBal] e-chequeClearingSuccess
e-chequeClearingSuccess
debit payer account and credit payee account with pmtAmt and do final payment seetlement
[pmtAmt>acBal] e-chequeClearingFailure
e-chequeClearingFailure
account cancellation request
verify cancellation par
alt
[valid par & usrOTP= mbsOTP]cancellationSuccess
[invalid par or usrOTP <> mbsOTP]cancellationFailure
cancellationSuccess
login interval>= cancellation period

Fig. 3. Sequence diagram of C-MBS

LTL definition2 (LTL2)
[]((registrationSuccess==true)->(mobileUserDataVerification==true))
Registration of mobile users in C-MBS can be successful only when banking user data are valid.

LTL definition3 (LTL3)
[] ((userBlocked==true)->(loginSuccess==false))
Banking user login cannot be succeeded when the users are blocked in the system.

LTL definition4 (LTL4)
[] ((passwordExpired==true)->(loginSuccess==false))
If banking users' password become expired after certain allocated period of time, then user login cannot be succeeded in the system.

LTL definition5 (LTL5)
[]((IdExpired==true)->(loginSuccess==false))
Banking user login cannot be succeeded when the user's id is expired in the system.

LTL definition6 (LTL6)
[]((authenticationSuccess==true)->(registrationSuccess==true))
Authentication can be successful only if registration is also successful.

LTL definition7 (LTL7)
[]((authenticationSuccess==true)->(authorizationSuccess==true))
Authentication can be successful only if authorization is also successful.

LTL definition8 (LTL8)
[]((fundTransferSuccess==true)->(authenticationSuccess==true))
Fund transfer can be successful only if authentication of the user is also successful.

LTL definition9 (LTL9)
[]((fundTransferSuccess==true)-
>((loginSuccess==true)&&(authorizationSuccess==true)))
Fund transfer can be successful only if login is successful and authorization for the transaction is successful.

LTL definition10 (LTL10)
[](((transferAmount>accountBalance)||(transferAmount>dailyLimit))-
>(fundTransferSuccess==false))
Fund transfer cannot be successful if either transfer amount is greater than the available account balance or transfer amount is greater than the daily limit set for the transaction.

LTLdefinition11 (LTL11)

[](((transferAmount>accountBalance)||(transferAmount>dailyLimit))->(thirdPartyPaymentSuccess==false))

Third party payment cannot be successful if either transfer amount is greater than the available account balance or transfer amount is greater than the daily limit set for the transaction.

LTLdefinition12 (LTL12)

[]((transferAmount>=0)&&(paymentAmount>=0)&&(accountBalance>=0))

Transfer amount, payment amount and account balance should always be greater than or equal to 0.

LTL definition13 (LTL13)

[](((creditRating>=minimumRating)&&(loanAmount<=approvedLoanAmount))->(digitalLendingSuccess==true))

Digital lending can be successful only if credit rating of the banking customer is equal to or above the minimum rating and loan amount is less than or equal to the approved loan amount.

LTL definition14 (LTL14)

[](((registrationSuccess==true)||(fundTransferSuccess==true))->(mbsOTP==userOTP))

Registration or fund transfer can be successful only if OTP sent from C-MBS to the user and received from the user to C-MBS remains the same.

LTL definition15 (LTL15)

[]((thirdPartyPaymentSuccess==true)->(nationalPaymentGatewayOnline==true))

Third party payment can be successful only if the national payment gateway is online.

LTL definition16 (LTL16)

[]((loginInterval>=userCancellationPeriod)->(cancellationSuccess==true))

Banking user's account cancellation from C-MBS can be successful if the login interval period is greater than or equal to the user account cancellation period set in the system.

LTL definition17 (LTL17)

[]((eChequePaymentSuccess==true)->(nationalPaymentGatewayOnline==true))

e-cheque payment can be successful only if the national payment gateway is online.

LTL definition18 (LTL18)

[]((fundTransferSuccess==true)->((authorizationSuccess==true)&&(mbsOTP==userOTP)))

Fund transfer can be successful only if authorization is successful and OTP sent from C-MBS to the user and received from the user to C-MBS remains the same.

LTL definition19 (LTL19)
[]((transferAmount<=accountBalance)&&(transferAmount<=dailyLimit))
The transfer amount must be always less than or equal to the account balance and less than or equal to the daily limit set for the transaction.

LTL definition20 (LTL20)
[](~(transferAmount<0)&&(~(accountBalance<0))&&(~(loanAmount <0))&&(~(approvedLoanAmount<0))&&(~(paymentAmount <0))&&(~(fromAccountBalance<0)))
Transfer amount, account balance, loan amount, approved loan amount, payment amount and account balance cannot be less than 0 during the system lifetime.

This paper verifies the safety properties and LTL properties of the proposed model C-MBS. 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 1024 (in Mbytes), maximum search depths (steps) as 100000, estimated state space size as 1000, search mode as depth-first search (partial order reduction), and storage mode as bitstate/ supertrace for the verification.

Table 3. Verification results for safety properties

No. of users	Time (Seconds)	Memory (Mbytes)	Transitions	States stored	Depth	Verification status
1	4.99	6.772	12758522	612456	11659	Verified
3	7.51	7.846	12873553	616772	11469	Verified
5	10.2	11.264	13227429	620255	14375	Verified
10	57.7	16.315	13459389	619507	14106	Verified
20	108	24.136	13976019	620819	13048	Verified

After setting the parameters, we ran SPIN to verify the safety properties of C-MBS for up to 20 users. SPIN checked the state space for deadlocks and assertion violations during the verification of safety properties in C-MBS. The SPIN verification results for safety properties are in Table 3.

Table 3 shows the results obtained from SPIN demonstrating 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 show that there is an increase in the memory requirement and verification time with the increase in the number of users during the verification of the C-MBS model. The verification results show that there is no deadlocks or error in the design of the C-MBS model.

After that, we ran SPIN in the same computing environment to verify the LTL properties for 20 users. SPIN checked the statespace for never claim and assertion violations

Table 4. Verification results for LTL properties

LTL properties	Time (Seconds)	Memory (Mbytes)	Transitions	States stored	Depth	Verification status
LTL1	5.30	6.869	12780646	612189	20637	Verified
LTL2	5.35	6.869	12776991	612348	20504	Verified
LTL3	5.36	7.846	12728746	612790	27710	Verified
LTL4	5.28	7.553	12577602	612141	25968	Verified
LTL5	5.21	7.358	12412751	612309	24462	Verified
LTL6	5.23	8.139	12395190	612778	30396	Verified
LTL7	5.37	6.967	12780583	612409	21723	Verified
LTL8	5.39	8.334	12388721	612754	31557	Verified
LTL9	5.50	6.967	12725493	612239	21657	Verified
LTL10	5.12	9.409	12113245	611408	40379	Verified
LTL11	5.35	7.358	12792229	612491	24084	Verified
LTL12	5.34	7.455	12788075	612163	25109	Verified
LTL13	5.36	7.065	12673574	613144	21893	Verified
LTL14	5.27	8.041	12508195	611731	29198	Verified
LTL15	5.33	6.967	12680220	612835	21771	Verified
LTL16	5.36	6.967	12778965	612643	20976	Verified
LTL17	5.31	7.162	12679934	612184	22718	Verified
LTL18	5.21	9.116	12257835	612894	37689	Verified
LTL19	5.18	8.041	12238896	612744	29563	Verified
LTL20	5.29	6.577	12727399	611718	18187	Verified

in each run of LTL properties. The SPIN verification result for LTL properties is in Table 4. Table 4 depicts the results obtained from SPIN showing the elapsed time, total memory usage, states transitioned, states stored, and verification status for LTL properties in the C-MBS model. The SPIN verification results show that the memory requirement and verification time have not been increased significantly with the increase in the number of users during the verification of LTL properties in the C-MBS.

Table 3 shows the results after SPIN checked for the existence of deadlocks and assertion violations by generating the execution paths during the verification of the C-MBS model. Similarly, Table 4 shows the results after SPIN checked for temporal properties of the C-MBS model to conform during the system lifetime. The results of these experiments show that there is no error in the design of the C-MBS. SPIN did not generate any counterexample during the verification of the C-MBS. Hence, banks and financial institutions can implement this verified model for providing enhanced banking services to the banking users using mobile. The C-MBS model will increase the banking users to use the enhanced banking services remotely and will play a significant role in the transformation towards a cashless society in the digital world.

5 Conclusion and Future Work

In this prevailing generation of the digital world, digital products are driving our daily lives, and one of the beautiful digital products for everybody is the mobile device. Mobile users are redoubling by leaps and bounds universally. Mobile banking is an electronic channel for Electronic Banking (E-Banking) all over the world. Mobile banking users have not been increased yet significantly in proportional to the increase in the number of mobile users. Banking customers do not employ the mobile banking system because of not full automation and security problems. Therefore, this paper developed a new contactless mobile banking system (C-MBS) that includes enhanced banking services with novel functions like e-cheque, registration of the user, and cancellation of the users' account included in the model. This paper incorporated enhanced banking services such as registration of the user, fund transfer, third party payment, digital lending, e-cheque issuing, e-cheque clearing, and cancellation of the user account by using the EFSM model and PROMELA model of C-MBS. Security properties are specified using LTL, and system properties are specified using the PROMELA model of C-MBS. We used SPIN to verify the safety and LTL properties in the PROMELA model of C-MBS. SPIN verified the safety properties and the LTL properties within the C-MBS model. We observed from our experimental SPIN results that C-MBS does not have any deadlocks or errors within the model. Hence, banks and financial institutions can implement this verified C-MBS model for a secure enhanced mobile banking system that can play a significant role in making the cashless payment society in the world of E-Banking.

In future research, we will design a new mobile banking model that mitigates different attacks like man in the middle (MITM) attack, SQL injection attack, man in the browser (MITB) attack, replay attack, and other probable attacks in the banking systems. Likewise, we will extend our research in modeling and verification of digital banking and omnichannel banking in E-Banking.

References

1. Obaid, I., Kazmi, S., Qasim, A.: Modeling and verification of payment system in E-banking. Int. J. Adv. Comput. Sci. Appl. **8**(8), 195–201 (2017). https://doi.org/10.14569/IJACSA.2017.080825
2. Shi, H., Ma, W., Yang, M., Zhang, X.: A case study of model checking retail banking system with SPIN. J. Comput. **7**(10), 2503–2510 (2012). https://doi.org/10.4304/jcp.7.10.2503-2510
3. Zhang, W., Ma, W., Shi, H., Zhu, F.: Model checking and verification of the Internet payment system with spin. J. Softw. **7**(9),1941–1949 (2012). https://doi.org/10.4304/jsw.7.9.1941-1949
4. Ahamad, S.S., Udgata, S.K., Sastry, V.N.: A new mobile payment system with formal verification. Int. J. Internet Technol. Secur. Trans. **4**(1), 71–103 (2012). https://doi.org/10.1504/IJITST.2012.045153
5. Shaikh, R., And, A., Devane, S.: Formal verification of payment protocol using AVISPA. Int. J. Inf. **3**(3), 326–337 (2010). https://doi.org/10.20533/iji.1742.4712.2010.0035

6. Hegde, M.S., Jnanamurthy, H.K., J., Singh, S.: Modeling and verification of extensible authentication protocol using SPIN model checker. Int. J. Netw. Secur. Appl. **4**(6), 81–98 (2012). https://doi.org/10.5121/ijnsa.2012.4606
7. Ciurea, C.: The development of a mobile application in a collaborative banking system. Inf. Econ. **14**(3), 86–97 (2010)
8. Aithal, P.S.: A comparison of ideal banking model with mobile banking system. Int. J. Curr. Res. Mod. Educ. **1**(2), 206–224 (2016). https://doi.org/10.5281/zenodo.198708
9. Bojjagani, S., Sastry, V.N.: A secure end-to-end SMS-based mobile banking protocol. Int. J. Commun. Syst. **30**(15), 1–19 (2017). https://doi.org/10.1002/dac.3302
10. Anwarul Islam, K.M., Salma, U.: Mobile banking operations and banking facilities to rural people in Bangladesh. Int. J. Finan. Bank. Res. **2**(4), 147–162 (2016). https://doi.org/10.11648/j.ijfbr.20160204.14
11. Dahlberg, T., Guo, J., Ondrus, J.: A critical review of mobile payment research. Elsevier Electron. Commerce Res. Appl. **14**(5), 265–284 (2015). https://doi.org/10.1016/j.elerap.2015.07.006
12. Istrate, C.M.: Cardless withdrawal system for mobile banking applications. J. Mobile, Embed. Distrib. Syst. **6**(1), 11–16 (2014)
13. Yang, F., Liu, Z., Chiu, S.: Mobile banking payment system. J. Wireless Mobile Netw. Ubiquitous Comput. Depend. Appl. **2**(3), 85–95 (2011)
14. Alanazi, H.O., Alnaqeib, R., Hmood, A.K., Zaidan, M.A., Al-Nabhani, Y.: On the module of the Internet banking system. J. Comput. **2**(5), 133–143 (2010)
15. Uddin, M.S., Akhi, A.: E-wallet system for Bangladesh an electronic payment system. Int. J. Model. Optim. **4**(3), 216–219 (2014). https://doi.org/10.7763/ijmo.2014.V4.376
16. Islam, M.S.: Systematic literature review: security challenges of mobile banking and payment system. Int. J. u- and e- Serv. Sci. Technol. **7**(6), 107–116 (2014). https://doi.org/10.14257/ijunesst.2014.7.6.10
17. Brar, T., Sharma, D., Khurmi, S.: Vulnerabilities in e-banking: a study of various security aspects in e-banking. International Journal of Computing & Business Research, Proceedings of 'I-Society. pp. 2229–6166 (2012).
18. Nyamtiga, B.W., Sam, A., Laizer, L.S.: Enhanced security model for mobile banking systems in Tanzania. Int. J. Technol. Enhance. Emerg. Eng. Res. **1**(4), 4–20 (2013)
19. Avdic, A.: Use of biometrics in mobile banking security: case study of Croatian banks. Int. J. Comput. Sci. Netw. Secur. **19**(10), 83–89 (2019)
20. Gupta, R., Kumar, R.P., Bharadwaj, A.: Mobile banking system in India: practices, challenges and security issues. Int. J. Comput. Trends Technol. **43**(1), 24–48 (2017). https://doi.org/10.14445/22312803/ijctt-v43P106
21. Goyal, V., Pandey, U.S., Batra, S.: Mobile Banking in India: practices, challenges and security issues. Int. J. Adv. Trends Comput. Sci. Eng. **1**(2), 56–66 (2012)
22. Alalwan, A.A., Dwivedi, Y.K., Rana, N.P.: Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. Elsevier Int. J. Inf. Manage. **37**(3), 99–110 (2017). https://doi.org/10.1016/j.ijinfomgt.2017.01.002
23. Al-Jabri, I.M., Sohail, M.S.: Mobile banking adoption: application of diffusion of innovation theory. J. Electron. Commer. Res. **13**(4), 379–391 (2012)
24. Raja, S.A., Umer, A., Shah, N.: New determinants of ease of use and perceived usefulness for mobile banking adoption. Int. J. Electron. Cust. Relationship Manage. **11**(1), 44–65 (2017). https://doi.org/10.1504/ijecrm.2017.086751
25. Safeena, R., Date, H., Kammani, A., Hundewale, N.: Technology adoption and Indian consumers: study on Mobile Banking. Int. J. Comput. Theory Eng. **4**(6), 1020–1024 (2012). https://doi.org/10.7763/ijcte.2012.v4.630
26. Bharti. M.: Impact of dimensions of mobile banking on user satisfaction. J. Internet Bank. Comm. **21**(1), 1–22 (2016)

27. Asfour, H.K., Haddad, S.I.: The impact of mobile banking on enhancing customers' e-satisfaction: an empirical study on commercial banks in Jordan. Int. Bus. Res. **7**(10), 145–169 (2014). https://doi.org/10.5539/ibr.v7n10p145
28. Singh, N., Kumar, T., Vardhan, M.: Blockchain based e-cheque clearing framework. Scalable Comput.: Pract. Exper. **20**(3), 511–525 (2019). https://doi.org/10.12694/scpe.v20i3.1506
29. Yahid, B., Nobakht, M., Shahbahrami, A.: Trust in e-cheque in electronic payments. New Mark. Res. J. **4**, 19–28 (2014)
30. Digital 2021 global overview report. https://datareportal.com/reports/digital-2021-global-overview-report. Accessed on 15 June 2021