

## **ISSUES AND SECURITY MEASURES OF MOBILE BANKING APPS**

**Dr. S. Paulmurugan**

Assistant Professor of Commerce, (Deputed From Annamalai University), Govt. Arts college,  
Tiruvannamalai-606603

**Nagashree R Pujari**

Assistant Professor (Ph.D. Scholar), Department of Commerce, Annamalai University  
Tamil Nadu

### **Abstract**

The invention of mobile phones makes the human life easier. The purpose of this study is to identify security risks in mobile banking and to provide an authentication method for mobile banking transaction by using bio-metric mechanism. Current mobile banking authentication is challenging and identified as a major security risk. Literature review shows that customer distrusts mobile banking due to security issues. The authors discuss security risks in current authentication methods in mobile banking. There are different methods and approaches to handle authentication in mobile banking. In this thesis, we propose a new approach of authentication in mobile banking. The strengths and weaknesses of existing approaches of authentication are identified with the help of Literature Review and interviews. The authors present basic transaction model and include security risks. By Literature Review it is found that finger print mechanism is a suitable method for authentication. Authors focus on authentication method and present a biometric scanning device which can identify the customer's finger print thus enabling the customer to access mobile banking facility. To promote mobile banking, it is necessary to improve customer trust in terms of security.

**Keywords:** Mobile banking, Security Authentication, SMS based Mobile banking Digital Signature.

### **INTRODUCTION**

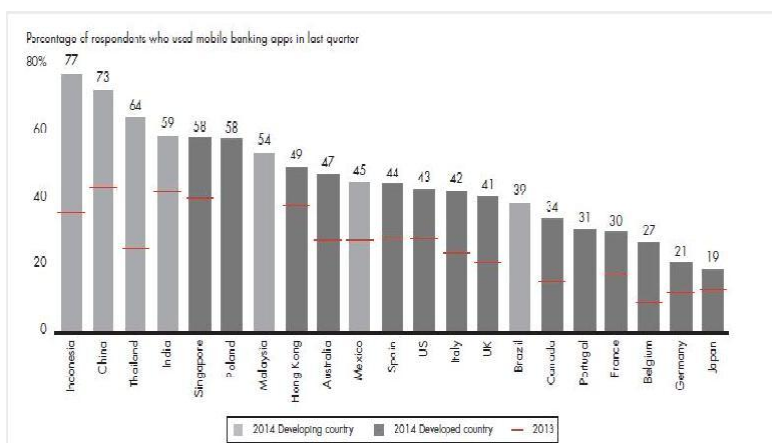
Financial services and transactions through mobile device are called Mobile banking. Mobile banking security will include data transmission which is important to secure the data of the users to prevent the hacker to attack and steal the data. Authentication is also important which is only allowed authorized users to have access to the data. Also avoiding complex authorization is crucial in order to make quickly for the data.

The protocol translation and compression of contents from mobile devices are working through online banking architecture. The architecture of online banking can be at variance by subject on outline by the panel of bank bodies; in-house services and third parties hosted services. These

online banking architectures were applied into mobile internet banking application since the bank has application servers that involve e-mail server, website server and others. Then the router will direct the transaction request by the user into those application servers. But the process for each architecture will be differ.

Recently, the communication of internet banking application in smartphone will be asynchronous through back-end system. To work on back-end system, Service Oriented Architecture (SOA) is needed for all application components provide services to other components by the use of a communications protocol, usually an Internet. It compromises bank bodies with option in involving old application with the current internet banking. It is due to the advanced technology and wireless technology users are more convenience to do their financial services through mobile. Mobile banking based on WAP (Wireless Application Protocol) and SMS (Short Message Service) is popular. However, there still many security problems when making transaction through SMS. The data are not secure while transmitting through SMS because sending and receiving SMS have no encryption technique. Using mobile devices to access to the internet through WAP (Wireless Application Protocol) is insecure as WAP is vulnerable to hacker's attacks due to its protocol translation and compression of contents which is insecure. Thus, Intrusion Detection System (IDS) is introduced into internet banking security system for safety on online transaction processing. Basically, IDS is used to review, analyse and record report of the system and network activities.

### **THE USAGE OF MOBILE BANKING APPS**



Source: Bain/Research Now NPS survey, 2018

The number of mobile banking apps users are increasing as shown in the statistics above from Bain / Research survey in 2018, which Indonesia is on the top followed by China and Thailand. As

we can see from the statistics more user in asia pacific use mobile banking apps. That shows us how people in this pacific are more conviniece with mobile banking apps although research has shown that hacking or malware has been the predominant method of Credit Card data breaches that occurred from 2005 to 2018.

### **Security Issues in Mobile Banking**

Mobile banking refers to the use of a smart phone or other cellular device to perform online banking tasks while away from your home computer, such as monitoring account balances, transferring funds between accounts, bill payment and locating an ATM.

Mobile banking has two zones, one is the handset held by the user and the other is the bank zone. Literature shows that possibility of security threat exists for transaction of payment using mobile device.

### **Virus Attacks in mobile banking apps**

There are different types of computer viruses, internet malicious program and TrojanZeus Trojan targeted mobile bank users. Virus Zitmo has been commonly used by attackers to defect SMS banking. As well as virus Zeus is commonly used by the hackers to access to mobile transaction authentication number or password.

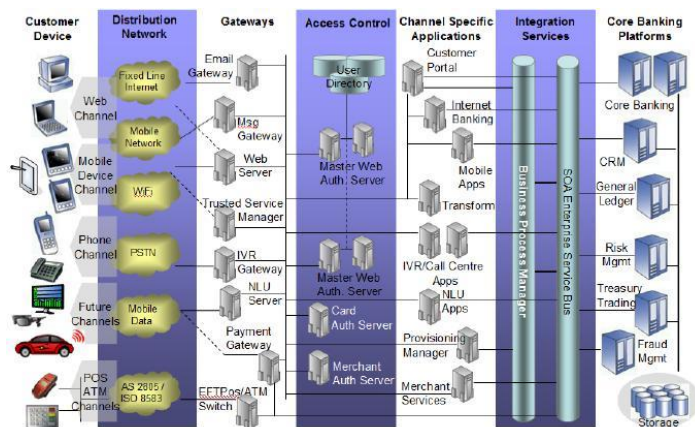


Figure 1: Various architectures on Multi-Channel Banking.

### **Mobile banking and Security issues with WAP (Wireless Application Protocol)**

WAP is used for communication between devices like digital mobile phones, internet, PDA etc. Through WAP customer can realize more functionality of internet banking. Encryption process is currently used for secure data transmission between bank and users

but the problem is that this encryption process is not good enough for the protection of sensitive data between bank and customer. The reason is that security methods require more powerful computing and high storage capacity. If we take internet banking it is realized that there are powerful computer systems and well defined complex encryption process to ensure the security. Mobile device have low computational capacity and hence we are unable to apply complex cryptographic system.

Due to advancement in technology, it is now necessary to provide end-to-end security. It means that if user uses his/her mobile device for mobile banking then the data transacted are secure at the bank end and not at the user end, thus leaving the data vulnerable to attacks. It was noted that it is difficult to provide end to end security through WAP. The reason is that the data is not encrypted at gateway during the switching of protocol process, which leads to security concern for mobile banking in WAP.

### **Authentication Risks and Issues**

One of the authentication method used in mobile banking is the login method. However PINS authentication method is an old method and many security issues such as password and id theft were discovered in this method. In such cases, the secret may be revealed and this results in customer's distrust on the security service company. Bank follows some security mechanisms in mobile banking. While the customers and the banks are bound to each other. This security mechanism is done by identifying the customer's phone number, SIM card number, pin number etc. Customer likes to use the mobile banking technology because of its mobility as they can access the bank anywhere and in any situation. They can transfer their money from one account to another account faster in a user-friendly environment. And also they can check the current status of their account. But all customers of the bank are not ready to use this service because of some security issues. They are not ready to adopt the mobile banking systems as it brings inconvenience to the users assuming that it cannot prevent direct or indirect attacks.

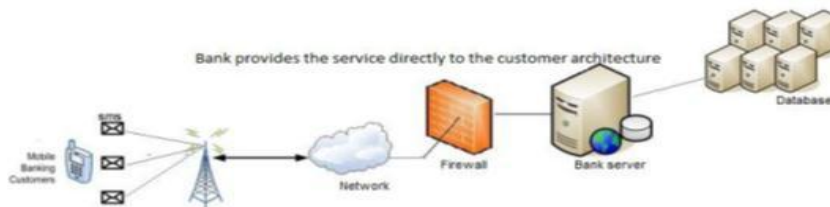
The security mechanism adopted by the banks face many security issues like being attacked by unauthorized users which is of highest priority in terms of security. If the device gets stolen then the hackers or unauthorized persons may find the password from the log files or saved draft files. Many customers save their password in their mobile or they may keep the password under auto fill settings of the form, this loophole can be easily used by the unauthorized person. Uneducated people are less aware of these issues and thus leading to loss of trust by customers.

## **Authentication Model**

There are two types of services provided to the customer which are as follows:

1. The bank provides the service directly to the customer
2. Banks share their facility to 3rd party service provider

Bank provides the service directly to the customer architecture.



**Figure: Provides the Service Directly to Customer Architecture**

This is a setup which shows the Internet web server, database, application server and firewall at the bank's side. The above architecture is an example of mobile banking service handled directly by the bank. In this application, server plays an important role to provide services to the customer. The database will be accessed by transactions both from the bank and from mobile device.

If a mobile bank customer wishes to process the transaction, for example, transaction of money from one account to another account he/she must first authenticate themselves to the bank server through firewall. And the security application at the server has to verify the user through password or pin number and the server allows the customer to do transactions. In this method, there are some security issues such as server failure, system crash, and malevolent intrusion. These are serious problems and will not make the server come back in normal form. So many banks do not prefer this method.

## **Banks Share their Facility to 3rd Party Service Provider**



**Figure: Banks share their facility to 3rd party service provider**

In this scenario, the user sends PIN number to the bank's server and then the server is ready for accepting the requests. This approach is not fully secure because the data is transmitted and the network operator has full access to the data.

SMS banking is useful for small consumer and for small merchant. SMS banking is also useful for travelers because customer can buy ticket for buses and trains easily and in urgent situations without going to the respective stations.

### **SMS Encryption**

1. As default data format for SMS is plaintext. Currently end to end encryption is not available.
2. The only encryption involved at base transceiver station and SMS bank server during transmission.
3. The encryption algorithm used is A5 which is proven to be defenseless.

### **SMS Spoofing Attack**

The most dangerous attack in SMS banking is spoofing attack where attacker can send messages on network by manipulating sender's number. Due to spoofing attack, most of the organizations are not adopting mobile banking through SMS.

### **Virus Attacks in Mobile Banking**

There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans. Software like Trojan horses can easily take up password on the web browser or any cached information on operating system. Malicious codes are written for remote communication. Zeus Trojan targeted mobile bank users. Zitmo has been used by attackers to defect SMS banking. Zeus is commonly used to steal mobile transaction authentication number or password.

### **Risk with Digital Signature**

To reduce hardware cost, designer may prefer digital signature. Digital signature is efficient that's why most companies are interested in digital signature for authentication. It is founded that digital signature is computational intensive. With unsigned values for example date, amount, they differed from transaction to transaction. So a signed template can be used with several unsigned values like date, amount etc.

## **Conclusion**

In first step, it was observed that there is lagging of security and there is no formal authentication between the customer and the bank. Hackers can easily cyberpunk and there is no assurance the bank authenticates the authorized person. For this reason bio metric authentication method was introduced to improve the security.

In second step the method based on designing was defined by using both strengths and weaknesses of current authentication mechanism. Much of the design process was based on suggestion from professionals and bank experts.

In third step the design method was validated by conducting workshop. The authors introduced biometric finger print design for authentication and the identified minimum requirements are selected for conducting workshop as time was a constraint.

This thesis fulfills the gap of authentication between the customer and the bank. The result shows that the biometric design increases the security level between the user and bank. The security will also increase the bank revenue. Fraud can be minimized by bio metric mechanisms; especially finger print is suitable and secure method for the authentication of customer. The author designed the mobile handset and proposed a future device through which customer can scan finger print. Due to uniqueness of finger print it assured that authorized customer is making use of mobile banking. As data is sensitive at server level of bank system we propose System Architecture process. In this way data will be secure for the customer doing mobile banking services from end to end.

## **References**

- Mohammed-issa R Jaradat, Naseem M Twaissi, (2010). "Assessing the Introduction of Mobile Banking in Jordan Using Technology Acceptance Model," vol4, IJIM
- Deli Yang, Hongxin Wang, Yawei Ren., & JianJun Wang, (2010). Mobile Payment Pattern Based on Multiple Trusted Platforms - China Case, Mobile Business and Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference on, 2010, pp. 353-362.
- Pousttchi. K., & Schurig, M. (2004). Assessment of today's mobile banking applications from the view of customer requirements, System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, p.10
- Gordon. M., & Sankaranarayanan, S. (2010). Biometric security mechanism in Mobile payments, Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On, pp. 1-6.
- Narendiran, C, Rabara, S., & Rajendran, N. (2008). Performance evaluation on end-to-end security architecture for mobile banking system, Wireless Days, 2008. WD '08. 1st IFIP, pp. 1-5.