Volume 1, No. 4, Nov-Dec 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secured Authentication for Online Banking using Mobile Phones

Prof. S Sumathy*
Assistant Professor [SG]
VIT University
Vellore-632014, India
ssumathy@vit.ac.in

R Hemalatha
MS [Software Engineering]
VIT University
Vellore-632014, India
hema.ms74@gmail.com

V Jayashree
MS [Software Engineering]
VIT University
Vellore-632014, India
venugopal.jayashree@yahoo.com

Abstract: Online banking is essentially safe, but equally fraud is also on the rise and consumers need to be more aware. The widespread use of online banking means more convenience for consumers and offers better ways to monitor account activity. The client accesses the ATM using a private key which is the security token that is sent to client's mobile through an SMS by the bank's authentication server. The key is generated by implementing SHA256 and Base64 algorithms using the registered IMSI (International Mobile Subscriber Identity), IMEI (International Mobile Equipment Identity) numbers of the client's mobile. SMS based mechanism makes sure that the key is delivered to the registered client.

The client is given a PIN and a Master key when registered to the Online banking service. If in case a client's mobile is lost, authentication is done using Unique Master key, else the private key token is used thereby making transactions secured and simple without the need of carrying any USB Tokens. The additional functionality provides the client more security with their transactions. Phishing attacks by the hackers are avoided to an extent in the proposed methodology. The proposed method has been implemented and tested in Java (J2ME). Initial results show the success of the proposed methodology.

Keywords: Authentication, OTP, Online Transactions, Security, IMEI, IMSI, Mobile Phone.

I. INTRODUCTION

Credit unions and Banks across the country provide multiple forms of identification authentication, log-in procedures and encrypted communications to make sure cyber criminals can't access confidential banking information while consumers are using an Online Banking application.

Today security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions, etc. Member institutions of Online Banking Association rated Security as the most important issue of online banking. Recent survey finds that 31 percent of bank customers avoid online transactions because of security reasons.

The proposed methodology guarantees authenticated to online banking service in a secured manner. Online banking is not different to traditional banking process. It makes use of technology for time-saving, paper-based procedures of traditional banking in order to manage banking service efficiently and quickly. Clients perform transactions on a secure website operated by their bank.

Transactions in online banking differ from general internet shopping transactions. Attacks on online banking deceive the user to steal the login data. A weak password is easy to remember, but open to potential attacks. It is not secured in many cases and therefore risks are high.

While digital certificates are used against phishing and pharming, attacks lead to an increasing number of phishing websites which duplicates victim's passwords. The less the password security relies on human mediation, the more it is secure. Dynamic Key Token is used for performing the banking operation.

Security plays a significant role in Online Banking. A dynamic private key token is generated for the client's account for authentication. Authenticated clients can access the overall account information.

II. LITERATURE CITED

Online banking is a very prominent area and has many methods to make the transactions more secure. One time passwords, two factor authentication, digital certificate verification are considered to provide more security than general PIN number authentication [2]. Several methods regarding the Online banking security are discussed in the following literature tabulated.

Table I. Literature Cited

REF NO:	TITLE	AUTHOR'S DESCRIPTION
1	One Time Password System[1]	One-time password systems provide additional protection but their use has been limited by cost and inconvenience.
2	Two Factor Authentication Application[2]	The user is simply requested to possess a Bluetooth enabled handheld device to enforce authentication based

		on weak credentials.
3	Security Token For Unified Authentication[5]	Authentication scheme based on One-Time Password (OTP) MIDlet running on a mobile phone for unified authentication towards any type of service on the Internet.

REF NO:	TITLE	AUTHOR'S DESCRIPTION
4	Online Authentication Protocol[7]	Online authentication is to verify identities through cyber networks.
5	Noisy Password Scheme[3]	Every time a user is authenticated by totally different password with noisy parts.
6	Delegation based Security for Web Services[6]	It extends the basic security models and supports flexible delegation and evaluation-based access control.
7	A countable and time-bound password based user authentication scheme[1]	Countable feature is to limit the use to a certain number of times. The users are able to login to the system for a fixed number of times.

III. DESIGN METHODOLOGY

A. *SHA (Secure Hash Algorithm)*

Hashing, used in many encryption algorithms is the transformation of a string of characters into a shorter fixed-length value or key that represents the original string. The hashing algorithm is called the hash function. A cryptographic hash function is a procedure, which takes a block of data and gives a fixed-size bit string, the (cryptographic) hash value.

They have many information security applications, including digital signatures, message authentication codes, and other forms of authentication.SHA (Secure Hash Algorithm) is one among a number of cryptographic hash functions.

It is a series of cryptographic hash functions:

- SHA-1, the 160-bit version.
- SHA-2, a newer revision with four variants: SHA-224, SHA-256, SHA-384 and SHA-512.
- SHA-3, an under development version.

Though SHA-2 has similarities to the SHA-1 algorithm, it includes a significant number of changes from SHA-1, and security flaws identified in SHA-1 are avoided.

SHA-256 and SHA-512 are new hash functions computed with 32 and 64-bit words respectively, use different shift amounts and additive constants, differing only in the number of rounds. SHA-224 and SHA-384 are truncated versions of the first two, computed with different initial values.

SHA-256 is used to authenticate Debian Linux software packages and in the DKIM message signing standard. SHA-512 is part of a system to authenticate archival video. UNIX and Linux vendors are moving to use 256 and 512-bit SHA-2 for secure password hashing.

B. *BASE 64*

Base64 is a way of interpreting bits of data to transmit over a text-only medium, such as the body of an e-mail. Base64 is a group of similar encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Base64 encoding schemes are used to encode binary data to deal with textual data, a number of applications including email via MIME, and storing complex data in XML. It ensures that the data remains unchanged. Base64 just represents data in a different form and is one of the data representation schemes that does not encrypt, compress the data. Basic authentication over the internet encrypts the username and password using base64.

It has many variants, of which first known standardized use of the encoding is now called MIME Base64. Selection of the character set for the 64 characters required for the base varies between its variants. The idea is to choose a set of 64 characters that is both part of a subset common to most encodings, and also printable.

Base64 can be used in many contexts including obfuscation of email passwords, transmit and store text, evade basic anti-spamming tools, encode character strings, embed binary data in an XML file, encode binary files (images within scripts) to avoid depending on external files.

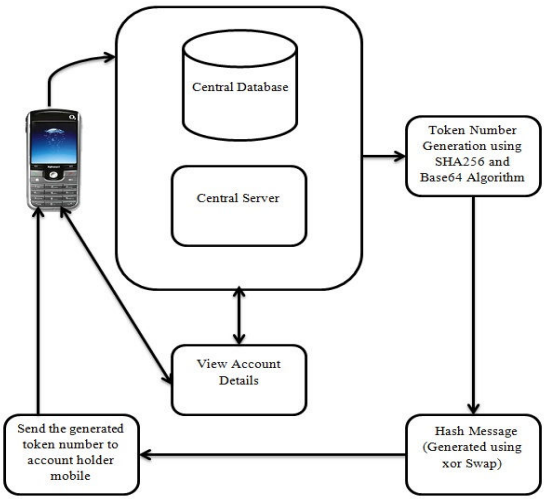

Figure 1. Architectural Design Block Diagram

C. *Client Design*

A J2ME program is developed and installed on the mobile phone. The program runs on any J2ME-enabled mobile phone. The key token program generates the dynamic key using the mobile credentials, such as IMEI, IMSI numbers and requests token from the server via SMS message. In order for the user to run the key token program, the user must enter the username and PIN and generate the security token.

D. *Database Design*

A database on the server side is used to store the client's identification information such as the first name, last name, username, pin, password, mobile IMEI number, IMSI number, unique symmetric key token, and the mobile number for each user. MySQL is used as a back-end.

E. Server Design

A server is implemented to generate the token on the organization's (Bank) side. *Database* is connected to a modem for SMS messages exchange. The server application is multithreaded. The first thread is responsible for initializing the database and SMS modem, and listen on the modem for client requests. The second thread is responsible for verifying the SMS information, generate and send the token. A third thread is used to compare the token. In order to setup in the database, the client must register at the organization. The client's mobile phone/SIM card identification factors, such as IMEI, IMSI numbers are retrieved and stored in the database, in addition to the username and PIN. The software is configured to connect to the server's GSM modem for the SMS option.

A unique symmetric key is also generated and installed on both the mobile phone and server.

IV. IMPLEMENTATION

A mobile-based software token system that is supposed to replace existing hardware and computer-based software tokens is proposed. The proposed system is secured and consists of three parts: (1) software installed on the client's mobile phone, (2) server software, and (3) a GSM modem connected to the server.

(1) The JAVA platform is recommended in which the program runs with J2ME application.

(2) JSMS software will be installed on the mobile phone for SMS service. MYSQL with JDBC connectivity is connected to the front end application.

(3) Using Hyper terminal software, a GSM modem is connected to the server. It also checks the modem connection.

A. Executing a Java Program

A program called JVM (java virtual machine) executes java programs. The JVM contains run time environment and the class loader. When we compile a .java file, a .class file is created. To compile a file then javac utility is used. To execute a .class file, the java utility is used.

B. SMS Service

Messages may be sent and received by using any GSM Device capable of sending SMS messages and also by using the most common SMSC communication protocols.

With all these features, a dynamic private key token is created. The system has two modes of operation:

1) Connection-Less Authentication System

A private key security token is generated by connecting the client to the server without any physical connection. Server requests the Client for receiving an SMS token, and the Client will respond to it.

2) SMS-Based Authentication System

If the client and server are out of synchronisation, the client can request the security token directly from the server. The server checks the SMS content and if correct, returns a randomly generated token to the mobile phone.

The user will then have a given amount of time to use the token before it expires.

V. SYSTEM DESIGN

This section discusses about the modules included in the secured authentication system. System has four main modules as follows:

A. Registration and Login Module

- User's basic information such as his name, address, age (Year/Month/Date), mobile information are registered in the Bank while creating the account.
- Mobile information includes IMEI number, IMSI number.
- IMEI number: International Mobile Equipment Identity is unique to each mobile phone and allows a particular user to be identified by the device. This is accessible on the mobile phone and is stored in the server's database for each client.
- IMSI number: International Mobile Subscriber Identity is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the Subscriber Identity Module (SIM) card in the mobile phone. This number is stored in the server's database for each client.
- With the above information, PIN number and Master Key are generated which are unique to each user. Along with registration details, PIN number and Master Key are stored in bank's database.
- The user is logged in by swiping the card and entering the PIN number.

Figure 2. Registration Module

B. Token Generation Module

- The above factors are concatenated and the result is hashed using SHA-256, which returns a message.

- The message is then XOR-ed with the PIN replicated to characters. The result is then Base64 encoded which yields a character message.
- From the encoded message, a random six digit output is taken as token number.

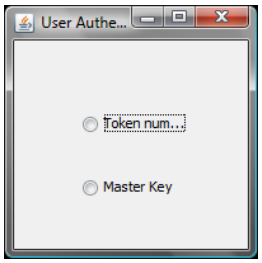

Figure 3. Token Generation Module

C. *SMS Module*

- The token generated is sent to the client's mobile number through a SMS.

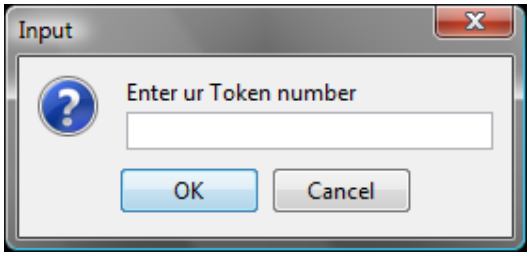

Figure 4. Client enters Token number got through SMS

D. *ATM Process Module*

- Client when enters this token number, the server decrypts the message, extracts the identification factors, and compares the factors with the ones stored in the database.
- The client then uses several services like withdrawal, checking account balance etc., if successfully authenticated.

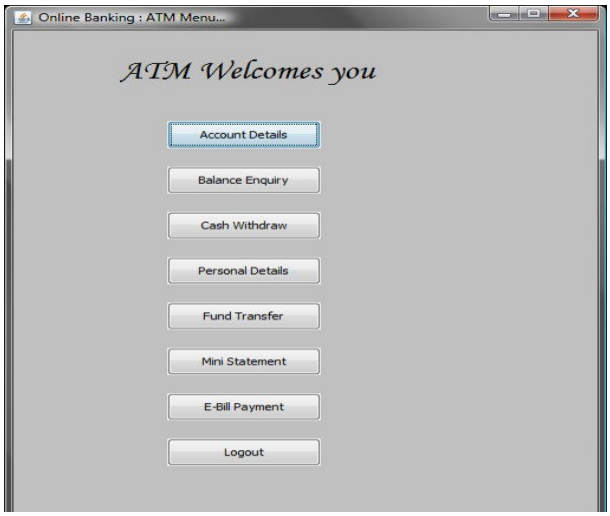

Figure 5. ATM Process Module

VI. SYSTEM STUDY

A. *Existing System*

Only swiping the card and the pin number are considered for accessing the ATM machine. In case of lost or theft of scratch card, the account can be easily accessed by the unauthorized user. This is not secure and not reliable for account maintenance.

Table II. Existing and Proposed System

S. No	Existing System	Proposed System
1	Transaction dealt with swiping the user account card	Transactions are accessed by handling security token
2	Possible of shoulder attack	Secure transactions are maintained
3	Account cannot be accessed from anywhere(must search for an ATM)	Access the account using mobile phone from anywhere
4	No storage of customer details for Future Reference(except Customer's copy)	Stores customers digital certificates in the database

B. *Proposed System*

A solution for 'Authentication of Online banking services using Mobile Phone' to perform transactions, is proposed and developed. Mobile phones are more suitable for online banking authentication than the USB Flash drives. For providing more security, separate token numbers are used for performing the banking operations like money with- drawl, checking account balance and fund transfer.

The token number is generated using the user's mobile number, IMEI, IMSI and the PIN numbers. The SHA256 and Base64 algorithms are used for the generation of token number. The generated token number is sent to the user's mobile. On entering the token number received through mobile, the user can access the ATM machine. For each and every transaction, a dynamic password token is generated which avoids theft, phishing and hacking attacks.

VII. CONCLUSION

Most parts of the world have evolved into an electronic era. The Information Technology (IT) and the Internet plays a significant role among people's daily life. E-business, E-learning is reaching people almost everywhere wherever computers and the Internet connections are available. Single factor authentication methods, such as passwords, are no longer considered secure in the internet and banking world. Easy-to-guess passwords, such as names and age are easily found by the automated password collecting programs.

In most cases, a hardware token is given to each user for each account. The increase in number of carried tokens and cost of manufacturing and maintaining them is difficult for both the client and organization. Mobile devices and certainly

mobile phones are currently widely spread. Many clients carry a mobile phone now at all times. An alternative is to install all the software tokens on the mobile phone, which helps reduce the manufacturing costs and the number of devices carried by the client. It focuses on the implementation of two-factor authentication method using mobile phones.

The proposed system has two ways of implementing, either using a free and fast connection-less method or a slightly more expensive SMS based method. With the generation of Dynamic private key token, banking transactions are accessed in safe and secured manner. The token is unique and by this methodology, the thefts, hacking and phishing attacks is avoided. Both these methods have been successfully implemented and tested, and are shown to be robust and secure.

The system has several factors that make it difficult to hack, such as

(1) At least 10 factors related to the mobile phone, SIM card, user, date and time are used to generate a difficult-to-guess, unique one-time pass-word (OTP).

(2) The system can easily run on any J2ME-enabled phone.

(3) The system has a user-friendly GUI.

(4) The OTP is only generated on the registered mobile phone and SIM card for stronger authentication.

(5) Even if the mobile phone is stolen, 8-characters PIN must be input to the phone to generate the correct token which is hard to brute force or guess by the hacker.

Future developments include a more user friendly GUI, and extending the proposed work to be implemented on various mobile phone platforms. Bluetooth and WLAN features on mobile phones can be used for cheaper token generation.

VIII. REFERENCES

[1] Iuon-Chang Lin, Chin-Chen Chang. "A countable and time-bound password-based user authentication scheme for the applications of electronic commerce".

[2] J. Archer Harris, Department of Computer Science, James Madison University. "OPA: A One-time Password System".

[3] Khaled Alghathbar, Hanan A. Mahmoud. "Noisy Password Scheme: A New One Time Password System".

[4] Roberto Di Pietro1, Gianluigi Me, Maurizio A. Strangio."A Two-Factor Mobile Authentication Scheme for Secure Financial Transactions".

[5] Steffen Hallsteinsen, Ivar Jørstad, Do Van Thanh. "Using the mobile phone as a security token for unified authentication".

[6] Wei She Thuraisingham, B. I-Ling Yen. "Delegation-Based Security Model for Web Services".

[7] Xing Fang Zhan, J. "Online Banking Authentication Using MobilePhones".

[8] B. Schneier, “Two-Factor Authentication: Too Little, Too Late,” inInside Risks 178, Communications of the ACM, 48(4), April 2005.

[9] Do van Thanh, Tore Jonvik “ Strong authentication with mobile phone as security token”

[10] N. Mallat, M. Rossi, and V. Tuunainen, “Mobile Banking Services,”Communications of the ACM, 47(8), 42-46, May 2004.