

# Mobile Secured Transaction using Two-Factor Authentication in Cloud

Vijayarajan.V<sup>1</sup>, Siva Shanmugam.G<sup>2</sup>, Kannadasan.R<sup>3</sup>, Krishnamoorthy.A<sup>4</sup>, Sendhil kumar.K.S<sup>5</sup>

<sup>1</sup>Associate Professor, School of Computer Science & Engineering  
VIT University, Vellore, Tamil Nadu.

## ABSTRACT

In this paper security and authentication plays a major role. It can be mainly used in online banking or ATM machines. The mobile phone act as a security token for authentication. The user login's the ATM machine by scratching the card and entering the password. For providing more security separate token number is used for performing the banking operation like money withdrawal, checking the balance etc. This token no is generated using the SHA algorithm and XOR operation. The user mobile number, IMEI number, pin number and IMSI number were included to generate the token number. The token number is six digit random number that were obtained from the included number. The token number is sent to the user mobile. This token number is given for accessing or performing the banking operations. The token number is generated for every interval of time. For more than three times if the user gives any invalid pin number the ATM card is blocked.

## 1. INTRODUCTION

In the existing system, only the scratch card and the pin number were considered for accessing the ATM machine. But in case 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. Here the mobile phone is used for security and authentication. Here the token number is generated using the mobile number, IMEI number, pin number and IMSI number. The SHA algorithm and XOR operation were used for the generation of token number. The generated token number is sent to the user mobile and only by entering the token number the user can access the ATM machine.

The major drawback of authentication performed using something that the user possesses and one other factor is that the plastic token used (the USB stick, the bank card, the key or similar) must be carried around by the user at all times. And if this is stolen or lost, or if the user simply does not have it with him or her, access is impossible. There are also costs involved in procuring and subsequently replacing tokens of this kind. In addition, there are inherent conflicts and unavoidable trade-offs between usability and security. Mobile phone two-factor authentication was developed to provide an alternative method that would avoid such issues. This approach uses mobile devices such as mobile phones and smartphones to serve as "something that the user possesses". If users want to authenticate themselves, they can use their personal access license (i.e. something that only the individual user knows) plus a one-time-valid, dynamic passcode consisting of digits. The code can be sent to their mobile device by SMS or via a special app. The advantage of this method is that there is no need for an additional, dedicated token, as users tend to carry their mobile devices around at all times anyway. Some professional two-factor authentication solutions also ensure that there is always a valid passcode available for users. If the user has already used a sequence of digits (passcode), this is automatically deleted and the system sends a new code to the mobile device. And if the new code is not entered within a specified time limit, the system automatically replaces it. This ensures that no old, already used codes are left on mobile

devices. For added security, it is possible to specify how many incorrect entries are permitted before the system blocks access.

## 2. RELATED WORK

Enhancing the level of security by using personal mobile devices is attracting attention due to the increasing number of user adopting mobile technologies. The security researchers has started to devise approaches the may increase the level of security in accessing critical information by end users through the employment of mobile devices. We use a mobile phone as handled authentication and a security token. Authentication using mobile devices is one way to bring such devices into the realm of security. However, previous research efforts that use mobile devices for authentication purposes, have employed weak authentication (i.e., only a username and password pair) using input and output features of such devices. Weak authentication is known for its vulnerability to several attacks, including shoulder surfing, phishing, and key logging. Moreover, the compact size of the mobile devices imposes constraints on their efficient and consistent usability, it is unreasonable to expect a user to enter a potentially long password into a mobile device several times a day. Likewise, we cannot expect users to use small screens of mobile devices as a proper output device for their daily transaction.

[1] A. Josang and G. Sanderud, “**Security in Mobile communication: Challenges and Opportunities**,” in Proc. Of the Australasian information security workshop conference on ACSW frontiers, 43-48, 2003. In this paper deals about the terminals having poor user interface and limited processing capacity, as well as complex combination of network protocols, makes the design of security solutions particularly challenging[2]. It discuss some of the difficulties system architects are faced as well as some advantages mobile networks offer when designing security solutions for mobile communication.

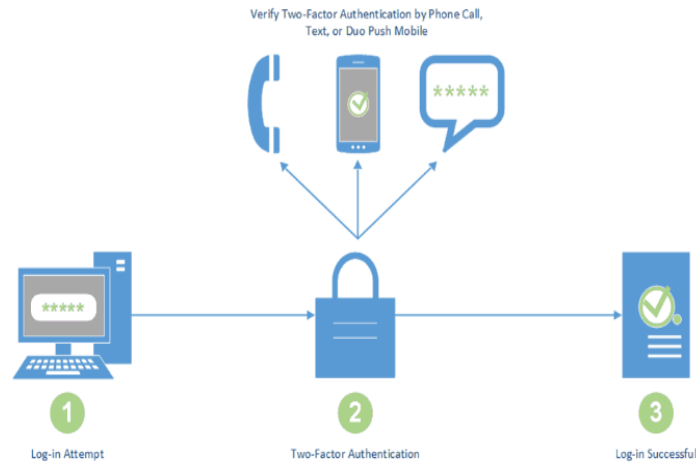
[2] B. Schneier, “**Two-Factor Authentication: Too Little, Too Late**,” in Inside Risks 178, Communications of the ACM, 48(4), April 2005. In this paper the two-factor authentication mitigates. If your password includes a number that changes every minute, or a unique reply to a random challenge, then its difficult for someone else to intercept. An intercepted password wont be usable the next time it’s needed. And a two-factor password is more difficult to guess. Sure someone can always give his password and token to his secretary, so no solution is foolproof.

[3] A. Herzberg, “**Payments and Banking with Mobile Personal Devices**,” Communications of the ACM, 46(5) 53-58, May 2003. In this paper explained about mobile devices enable secure, convenient authorization of e-banking, retail payment, brokerage, and other types of transactions.

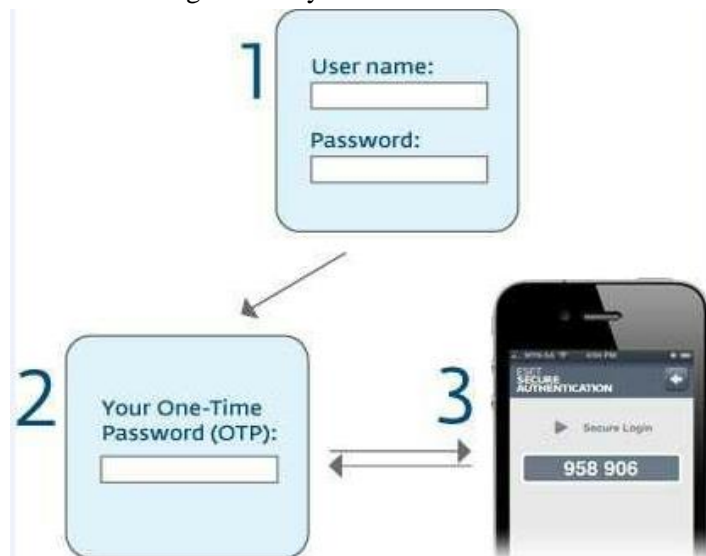
## 3. IMPLEMENTATION

We propose a mobile-based software token system that is supposed to replace existing hardware and computer-based software tokens. This system is secured and consists of three parts: software installed on the client’s mobile phone, server software, and a GSM modem connected to the server. The system will have two modes of operation:

1. **Connection-Less Authentication System:** A one-time password is generated without connecting the client to the server. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally.



2. **SMS-Based Authentication System:** In case first method fails, the password is rejected, or client or server is out of sync, the mobile can request the one time password directly from the server without the need to generate the one-time password locally on the mobile. But this concept won't support all the times [4][5] and also chances of misbehaving are also high. In order to prevent this we produced Two Factor authentication to provide secure transaction. After entire process initiated, finally adopted in cloud which gives more advantage to the system.



## The Java Technology

Java technology is both a programming language and a platform. Java programming language is a high-level language that can be characterized by all of the following buzzwords:

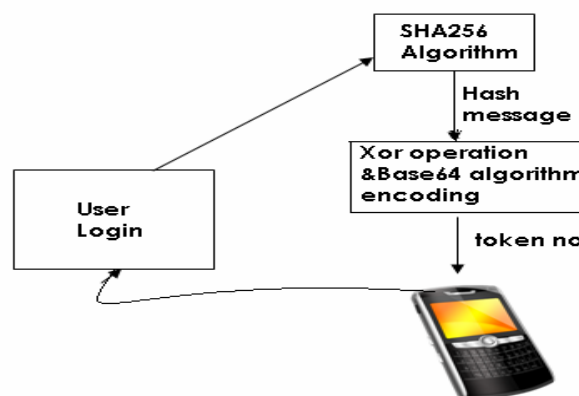
- Simple
- Object Oriented
- Distributed
- Multithreaded
- Dynamic
- Portable
- Secure

## The Java Platform

A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Microsoft Windows, Linux, Solaris OS, Mac OS. Most platforms can be described as a combination of the operating system and underlying hardware. The platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

The Java platform has two components:

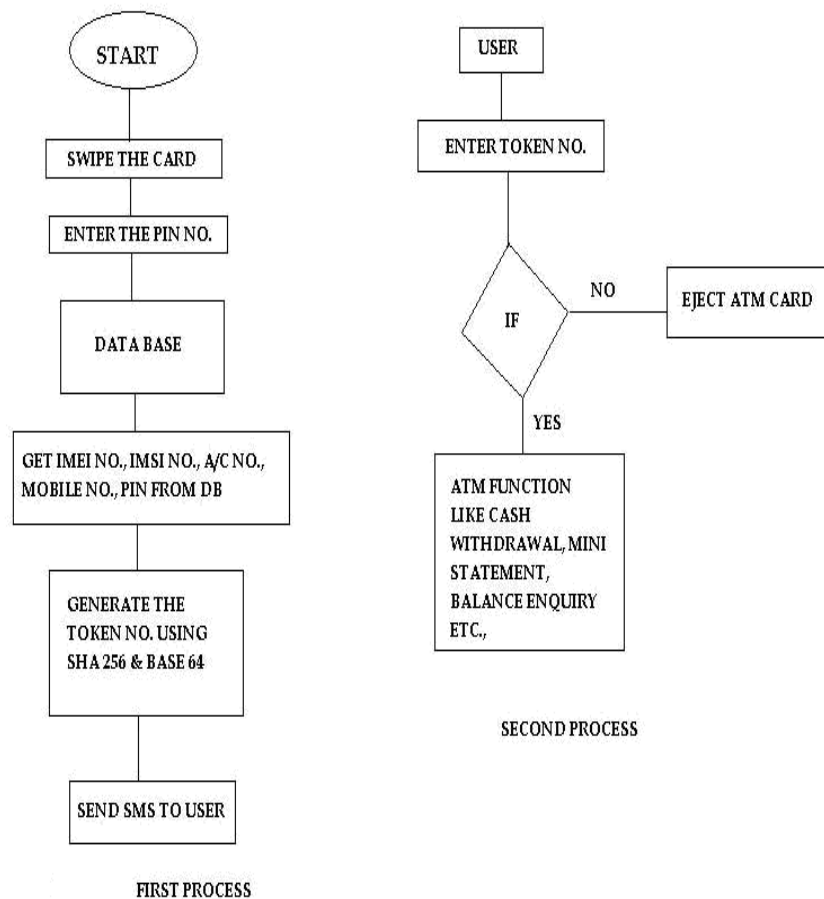
- The Java Virtual Machine
- The Java Application Programming Interface(API)



Architecture Diagram

User information such as his name, address, age, Year/Month/Date, mobile information and so on is registered in a Bank while creating the account. Mobile information include IMEI number, IMSI number. International Mobile Equipment Identity which is unique to each mobile phone allowing each user to be identified by his device. This will be stored in the server's database for each client. International Mobile Subscriber Identity which is unique number associated with all GSM. It is stored in the Subscriber Identity Module(SIM) card in the mobile phone. This number will also be stored in the server's database for each client. The above factors are concatenated and the result is hashed using SHA-256 which returns message[2]. The message is then XOR-ed with the PIN replicated to characters. The result is then Base64 which yields a character message. From the encoded message a random six digit output is taken as token number.

### 3. PROPOSED WORK



### Flow Diagram

In earlier system, only the scratch card and the pin number were considered for accessing ATM machine. But in case lost of theft, the account can be easily accessed by the unauthorized user. This is not secure and reliable so the mobile phone is used for security and authentication. Here a token number is generated using

the user mobile number, IMEI number, pin number and IMSI number. The SHA algorithm and XOR operation were used for the generation of token number. The generated token number is sent to the user mobile and only by entering the token number the user can access the ATM machine.

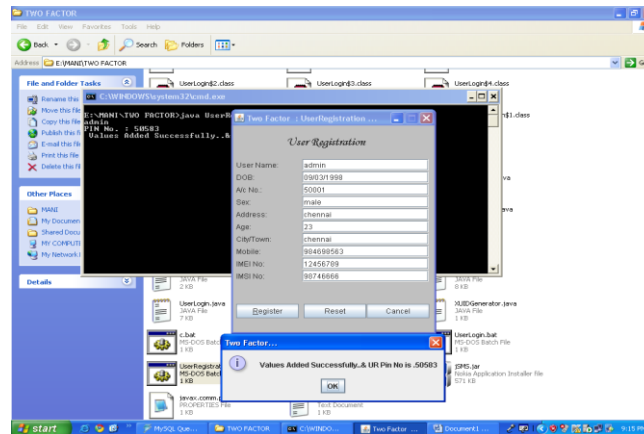
1. New user account is created.
2. Existing user is logged in by scratching the card and entering the pin number, now token is generated.
3. The IMEI number, IMSI number, username and pin number were considered for token number generation.
4. The SHA256 algorithm is used to generating the hash message.
5. The hash message is taken and XOR operation is made.
6. Then the XOR-ed message was encoding with Base64 algorithm.
7. From the encoded message a random six digit output is taken as token number.
8. The generated token number is sent to the account holder mobile number.
9. With the help of token number the user performs various operations like withdrawal, checking balance etc.

#### 4. RESULTS



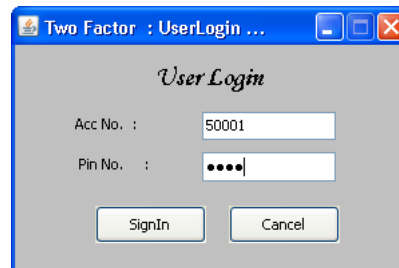
#### User Registration

Enter the user details and register to get the PIN number.



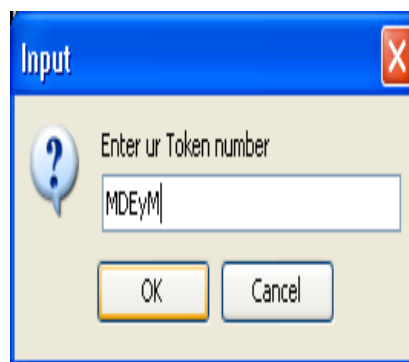
**Figure 4: Receiving Generated PIN number**

Now the account is created for the user and got the PIN number to login.



**Figure 5: User Login**

User login with created account with username and PIN number.



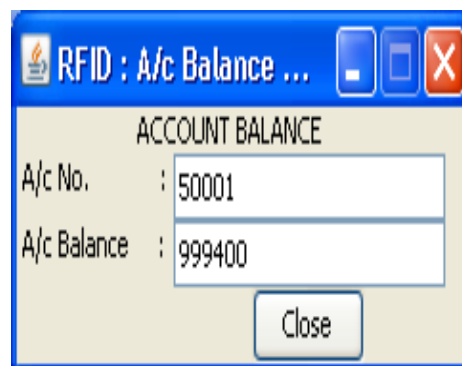
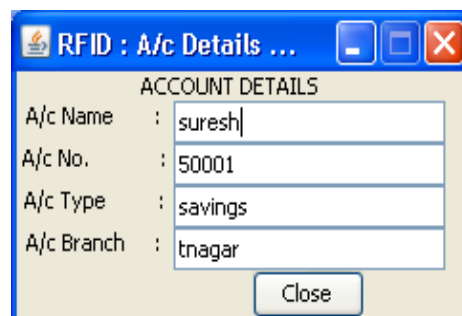
### Token Generation

The generated token number is sent to the account holder mobile number, we need to give the token number to various operations.



### ATM Menu

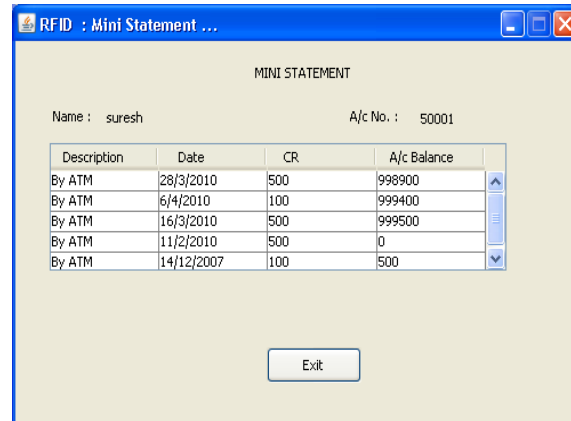
With the help of the token number the user performs various operations like withdrawal, checking account balance etc.



### Account Details

User can view their Account details and balance.





Name : suresh		A/c No. : 50001	
Description	Date	CR	A/c Balance
By ATM	28/3/2010	500	998900
By ATM	6/4/2010	100	999400
By ATM	16/3/2010	500	999500
By ATM	11/2/2010	500	0
By ATM	14/12/2007	100	500

Exit

### Mini Statement

After performing various operations like amount withdrawal, the account holder can take mini statement.

### CONCLUSION

Thus these are focuses on the implementation of two-factor authentication methods using mobile phones. It provides the reader with an overview of the various parts of the system and the capabilities of the system. The proposed system has two option of running, either using a free and fast connection-less method or a slightly more expensive SMS based method. But method have been successfully implemented and tested, and shown to be robust and secure. The system has several factors that makes it difficult to hack.

In future, the development include a more user friendly GUI and extending the algorithm to work on Blackberry, Palm, and Windows-based mobile phones. In addition to use of Bluetooth and WLAN features on mobile phones for better security and cheaper OTP generation.

### REFERENCE

- [1] A. Jøsang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities," in Proc. of the Australasian information security workshop conference on ACSW frontiers, 43-48, 2003.
- [2] Aladdin Secure SafeWord 2008. Available at <http://www.securecomputing.com/index.cfm?skey=1713>
- [3] A. Medrano, "Online Banking Security – Layers of Protection," Available at <http://ezinearticles.com/?Online-Banking-Security---Layers-of-Protection&id=1353184>

- [4] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," in Inside Risks 178, Communications of the ACM, 48(4), April 2005.
- [5] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005. Available at <http://www.silicon.com/financialservices/0,3800010322,39153981,00.htm>
- [6] D. de Borde, "Two-Factor Authentication," Siemens Enterprise Communications UK- Security Solutions, 2008. Available at [http://www.insight.co.uk/files/whitepapers/Twofactor%20authentication%20\(White%20paper\).pdf](http://www.insight.co.uk/files/whitepapers/Twofactor%20authentication%20(White%20paper).pdf)
- [7] A. Herzberg, "Payments and Banking with Mobile Personal Devices," Communications of the ACM, 46(5), 53-58, May 2003.
- [8] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth- Factor Authentication: Somebody You Know," ACM CCS, 168-78. 2006.
- [9] NBD Online Token. Available at [http://www.nbd.com/NBD/NBD\\_CDA/CDA\\_Web\\_pages/Internet\\_Banking/nbdonline\\_topbanner](http://www.nbd.com/NBD/NBD_CDA/CDA_Web_pages/Internet_Banking/nbdonline_topbanner).
- [10] Zhenning, Y., Kai, W., Liuyang, Z., Shanmugam, G.S., Caytiles, R.D. and Iyengar, N.C.S., 2017. Library Cloud: Concept and Design with Security Features.
- [11] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services," Communications of the ACM, 47(8), 42-46, May 2004.
- [12]. Shanmugam, G.S. and Iyengar, N.C.S., 2016. Effort of Load Balancer to Achieve Green Cloud Computing: A Review. International Journal of Multimedia and Ubiquitous Engineering, 11(3), pp.317-332.