Authentication in Smartphone using OTP

Tejaswini Kadu[1,] Preshita Kamdi[2]
Dept.of Information Technology
KDK College of engineeringNagpur-09,India
–kadutejaswini@gmail.com-,pkamdi514@gmail.com

*Abstract- **This paper explains about the how the authentication uses in Smartphone using OTP for online transaction. The mai n purpose of this method to provide security from hackers while performing transaction. The proposed system involves generating and delivering a One Time Password to mobile phone. Smartphone can be used as token for creating OTP or OTP can be send to mobile phone in form of SMS. The generated OTP is valid for only for short period of time and it is generated and verified using Secured Cryptographic Algorithm. This system helps to prevent unauthorized use of online transaction by providing additional password.***

Index Term- One Time Password(OTP),Authentication,Security,Transaction,Personal Identification Number(PIN).

I.INTRODUCTION

Now a days security is major problem in all areas like governmental applications, healthcare organisation, military organization, educational institutions,industries etc.Increase in popularity of the Internet the number of frauds and abuses is literally exploding. Most serious is the theft of identity which causes grave damages both for the victim and also his entourage such as employee, banks,hobby clubs, etc. The proposed method guarantees that authenticating to services, such as online banking or ATM machines, is done in a very secure manner. In this system system we using a mobile phone as a software token for One Time Password(OTP) generation. The generated On Time Password(OTP) is valid for only a short user- defined period of time i.e.for second or for minutes and is generated by factors that are unique to both, the user and the mobile device itself[1]. Here Strong authentication solutions require often two identification factors i.e., in addition to the first factor "something you know" represented by passwords it is introduced a second factor "something you have" materialized by a security token.

There are many solutions have been proposed in order to fix this concern. Some of them are hard to implement, others don't meet the security concerns of the companies while others are difficult to be used. Two-factor authentication using hardware devices, such as tokens or ATM cards has also been proposed to solve these problems and proved to be successful and difficult to be hacked. The use of mobile phone as a software token will make it easier for the customer to deal with multiple two-factor authentication systems and will also reduce the cost of manufacturing, distributing and maintaining millions of hardware tokens[2].

II.RELATED WORK

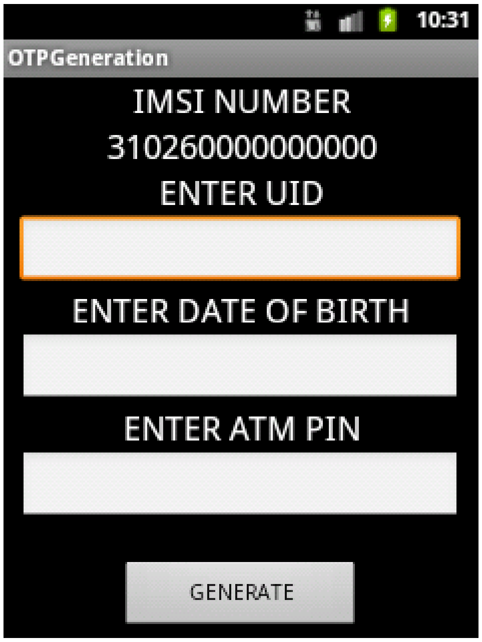
Online banking is a very prominent area and has many methods to make the transactions more secure. One time passwords, two factor authentication, digital certificate verification are considered to provide more security than general PIN number authentication. Authentication is the process of verifying the correctness of a claimed identity. It is a way of ensuring that users are who they claim to be when they access systems[2].This proposed work is more secure using two way authentication rather than one way authentication. There are three universally recognized factor this are:what you know(eg.password,PIN),what you have(debit card,credit card), what you are(eg.fingure print,face recognisation) therefore this two way authentication consider more secure and stronger than traditionally one way authentication system[3].

III.SYSTEM DESIGN ANDIMPLEMENTATION

A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as *something a person knows*.

OTP Algorithm:

For the security of system as well as smart phone, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it is very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micro payments, so we propose a Secured Cryptographic algorithm[1]. The unique OTP is generated by the mobile application offline, without having to connect to the server. The mobile phone will use some unique information in order to generate the password. The server will use the same unique information and validate the OTP.


OTPGeneration

IMSI NUMBER

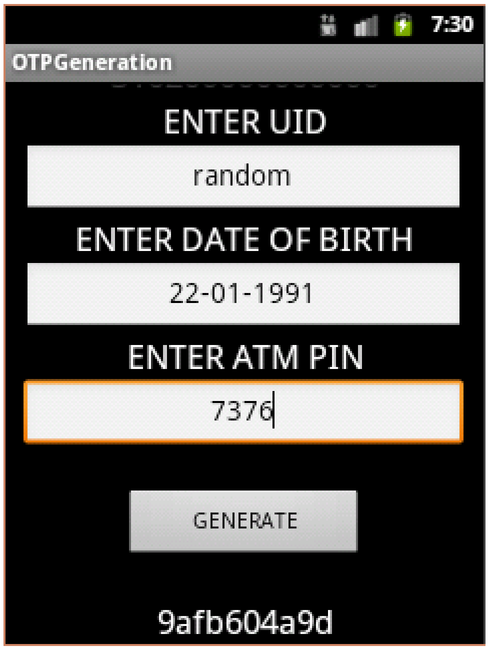
310260000000000

ENTER UID

ENTER DATE OF BIRTH

ENTER ATM PIN

Fig.1 shows menu to generate OTP (IMSI No. taken automatically)


OTPGeneration

ENTER UID

random

ENTER DATE OF BIRTH

22-01-1991

ENTER ATM PIN

7376

9afb604a9d

Fig.2 shows how OTP generated in Android mobile (Client Module)

- **IMSI**: *International Mobile* Subscriber *Identity*, unique to each mobile phone and allows each user to be identified by his device. This is accessible on the mobile phone and will be stored in the server's database for each user.

- **PIN**: Needed for verifying the authenticity of the client. If the phone is stolen, a valid OTP can't be generated without knowing the user's PIN. The PIN isn't stored in the phone's memory. It is only being used only to generate the OTP and destroyed immediately after that. In order for the PIN to be hard to guess and resistant to brute-force attacks, a minimum of 8 characters long PIN is required, with a mixture of upper and lower-case characters, digits and symbols.

- **Timestamp:** Used to generate unique OTP, valid for a short amount of time. The timestamp on the phone must be synchronized with the one from the server.

- **DOB:** Date of birth of user whose going to use the application.

- **Username:** Username of customer provided by bank[4].

How OTP Generated?

The Username, password, date of birth of user is taken from the user and then concatenated with the current date, time and the time stamp for which the one time password is valid. This concatenated string is then given as input to Secured Hash Algorithm (SHA1) algorithim. SHA- 1 algorithm returns its message digest which is 20 bytes value. These 20 bytes are reduced to 5 bytes by XORing a group of 4 bytes , i.e byte no. 1, 4, 8, 12 are XORed ; 2, 5, 9, 13; 3, 6, 10, 14; 4, 7, 11, 15; 5, 8, 12, 16; 17, 18, 19, 20 are Xored. Then from this 5 byte value, every byte is right shifted with 4 digits and then is converted to hexadecimal. Finally by converting the ASCII values to a character string, it is displayed as a onetime password to the user[3].

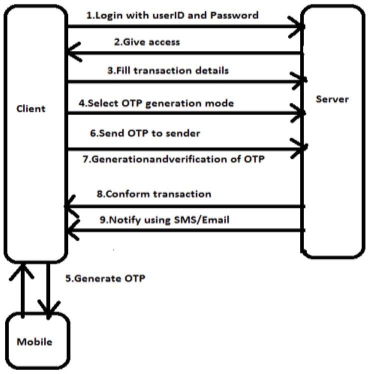

1.Login with userID and Password
2.Give access
3.Fill transaction details
4.Select OTP generation mode
6.Send OTP to sender
7.Generationandverification of OTP
8.Conform transaction
9.Notify using SMS/Email
Client
Server
5.Generate OTP
Mobile

Fig3:Proposed System flow

Working:

1.User visit bank website,login with userID and password.

2.If userID and password correct then bank give access to client and client use his/her account.

3.Client fill all details regarding to transaction.

4.Client choose mode of operation i.e.connectionless to generate own OTP and connection oriented to ask server to send OTP to his/her mobile phone.

5.After selecting connectionless mode user generate OTP on android based mobile phone using unique parameters.

6.Client use this OTP to complete the transaction.

7.As soon as OTP reach to the server,server start generating OTP using same parameter available at server.If both OTP gets match then transaction will be complited otherwise it will be denied.

IV. CONCLUSION

This paper focuses on the implementation of two-factor authentication on any smart-phone.Using smartphones we can easily perform transaction with help of OTP generation. Many time, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is difficult for both the client and organization. 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. The proposed work focuses on the implementation of two-factor authentication methods using mobile phones. It provides 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. Both methods have been successfully implemented and tested, and shown to be robust and secure. The system has several factors that make it difficult to hack. So this system provide more security than one way authentication and its difficult to hack or crack the OTP.

V. FUTURE WORK

This system provide authentication using OTP but we can implement this same system by using image based authentication i.e. using GUI.Initialy user create his/her account with ID and password and also select few category of things they can remember. TFA using Images creates a one-time authentication code and encrypts it within a randomly-generated grid of images. An application on the user's smartphone displays the grid of images The user identifies the pictures that match their secret categories by touching/tapping the appropriate pictures[5].By identifying the correct pictures, the user is essentially using their knowledge of their secret categories to decrypt the authentication code. Upon successful authentication, the web page automatically proceeds with the transaction or process.

VI. ACKNOWLEDGEMENT

We would like to thanks our institution as well as the faculty member.They gives us chance to present this paper and we also thanks to all friends for their suggestions and feedback for improving the ideas.

VII.REFERANCES

1.Sagar Acharya, Apoorva Polawar, P.Y.Pawar "Two Factor Authentication Using Smartphone Generated One Time Password" e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 85-90.

2. Professor T.Venkat Narayana Rao, Vedavathi K "Authentication Using Mobile Phone as a Security token" IJCSET |October 2011 | Vol 1, Issue 9, 569-574.

3. Costin Andrei SOARE " Internet Banking Two-Factor Authentication using Smartphones″ Journal of Mobile, Embedded and Distributed Systems, vol. IV, no. 1, 2012 ISSN 2067 – 4074.

4. Fadi Aloul, Syed Zahidi, Wassim El-Hajj "Two Factor Authentication Using Mobile Phones".

5.Rahul Kale,Neha Gore,Kavita,Nilesh Jadhav,Mr.Swapnil Joshi"Review paper on Two Factor Authentication using mobile phones(Android)"May 2013-vol2Issue5.

6. Himika Parmar1, Nancy Nainan2 and Sumaiya Thaseen "GENERATION OF SECURE ONE-TIME PASSWORD BASED ON IMAGE AUTHENTICATION" Sundarapandian et al. (Eds): CoNeCo,WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07,pp. 195–206, 2012. © CS & IT-CSCP 2012.