INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 4)
Available online at: www.ijariit.com

Enhanced adaptive security system for SMS – based One Time Password

R. Idayathulla
idayathulla86@gmail.com
Ponnaiyah Ramajayam Institute of Science and Technology (Deemed to be University), Puducherry

Chandrapriya C.
chandrapriya2992@gmail.com
Ponnaiyah Ramajayam Institute of Science and Technology (Deemed to be University), Thanjavur, Tamil Nadu

ABSTRACT

Wireless Network is used for all Portal Electronic Devices (PED). The main concept of using Authentication Network in PED for Online Banking. The user authenticates the transaction has a strong static ID and password. SMS based OTP provides an additional security layer for an authorized person. All Banks provide the same process for security purposes for they are beneficiaries. According to the recent thread, it is also vulnerable to various attacks. In this paper how it does can happen and what is the mechanism to prevent security-based OTP throughout using IMEI.

***Keywords** – PED, Authentication, OTP, IMEI.*

1. INTRODUCTION

Wireless Network is a center score of our daily life. In that 21st-century consciousness reformation in financial services such as bill payment, an international fund transaction, and money transfer. All channels are linked to one main channel called the Internet. Online banking accommodates for people access they are Individual account anywhere, anytime it is also termed as a security hazard. In banking user authentication is the significant processing for secure and confidential data. User authentication has a login ID and static password, beneficiaries modified they are password if it's mandatory, or if the user forgot the password. To quell vulnerable against the static password, one-time password launched.

OTP is also calling upon as One Time Pin or Dynamic password. Password veiled for only one's login session or transaction on PED. It's two-factor authentication. A Technological mechanism to reduce the risk of an unauthorized person obtaining to access the account. The most important advantage of OTP is in contrast to a static password. OTP, security technique shield for the various password-based attacks, specifically password sniffing and reply attack.

Short message services (SMS), Neil Papworth sent over text message, Vodafone GSM network to Richard Jarvis using Orbitel 901 handset, the United Kingdom on 3 December 1992. SMS based OTP to verified users to access a specific site, to enhance their security.

One Time Password (OTP) can contribute to the protection of the login - time. In the early 1980s, Leslie Lamport first proposes the idea of OTP. OTP generated and distribution. One time password is an excellent way of authenticating bank Transactions, the next step of transferring payment. OTP, ensure data safety user also receive the OTP through, Interactive voice response (IVR). Australia, North America, and Europe have the OTP mode using SMS or IVR to deliver the code. If OTP fails to deliver, it immediately has the option, auto-generated IVR call.

2. OTP PROCESS

One Time Password method usually delivered to the end-user. The process of OTP contains 1- Time Synchronization 2- Mathematical Algorithm 3- Method of Delivering the OTP.

2.1 Time Synchronization

The time synchronization method mainly present by Greenwich meantime(GMT) and the algorithm delivered the OTP in the concept of Time based One -Time Password (TOTP). TOTP algorithm based on Hash-based message authentication code (HMAC). TOTP is commonly used for the Two-factor Authentication (TF-A) method that uses the synchronous or Time -synchronized token for authentication. Time - synchronized OTP is a security token and is usually identified by a piece of hardware.Up to till SMS based OTP delivery by as a text message. The temporary OTP expired after 30, 60, 240 or 380 seconds.

2.2 Mathematical Algorithm

OTP generated in 6 or 4 digits. Every new OTP created from the old OTPs.Leslie lampost introduced the algorithm and the function call (x). This process starting the initial seeds x(y) is a hash function. And the hash function value presented as x(y),x(x(y),x(x(x(y))),…
(a) new seed feed from the call function and it determined- x(y).
(b) Initial seeds - (y).
A new seed fetches after when the (y) is exhausted. In the Mathematical Algorithm, The server provides the static key for the use as an encryption key for sending the One - Time Password. The s/key one-time password system and its

derivative OTP is based on Lamport's scheme. To get the next password, in the series from the previous password, we need to find a way of calculating the inverse function x^{-1}. If x is a cryptographic hash function, a one-time password may have access for one time or login time, but it becomes useless once that period expired. The method of delivering the OTP which are the token-based type of algorithm instead of Time -synchronization.

3. METHOD OF DELIVERING THE OTP

To deliver the General process of OTP, use short Message Service (SMS) or e-mail. In Fig 1 explain OTP request is given by the user to the Web server. HTTP accept the post request and sent into the OTP server for the configured bank. The bank server generated the OTP. SMS gateway accepts the OTP within the particular time session sent int to the SMS broadcast mobile network to the user.

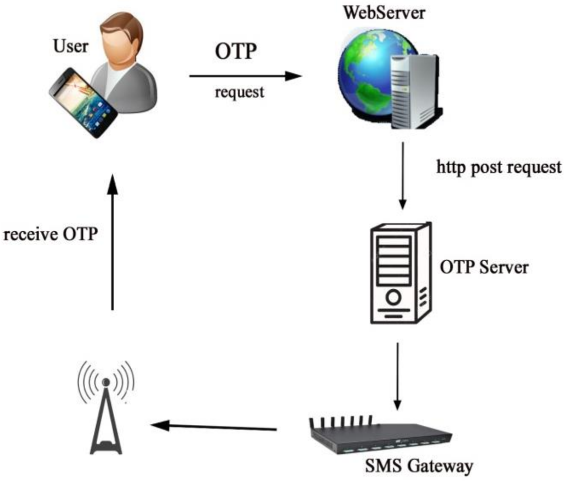


Fig. 1: Method of Receiving OTP

3. VULNERABILITIES IN SMS OTP

The major aim of the attackers to require the OTP. Let's discuss briefly below.

3.1 Wireless Spoofing

Wireless interception is achieved by placing an unauthorized device on the wireless network, bypassing the security process. Man-in-the-middle (MITM) attack, which the attackers intercept the communication between two parties. Easily they received every communication of your mobile.

IMSI catcher back cellular tower, which imitates the mobile phone towers to intercept calls and text messages. This device can grab information such as the phone's signals and, in some cases,, intercept the contents of the call and text.

Unsecured Wi-Fi, according to V3, three British politicians who agree to be part of a free wireless security experiment was easily hacked by technology export for an e.g.: free Wi-Fi network is usually unsecured. Where the hackers set up back access point's in high -traffic public locations, like a library, Airport, Railway Station and some point at the people crowd. Cybercriminals give an access point in the common name, free airport Wi-Fi. Encourage users to connect using their free services, allowing hackers to compromise their account, email and other sources of information.

3.2 Mobile Malware

Malicious software that targets mobile phone or wireless-enabled (PDA). The first virus Timofonica find out in June 2002. Timofonica sent SMS messages to GSM capable mobile phones the read, information for you Spyeye and Zeus probably the most prevalent ate at the bank password and other financial data. The first version of Zeus-in -the -Mobile (ZitMo), Malware which targets mTANs, discovered at the end of 2010.

An unauthorized, it's the latest method to adopt the OTP message. When cloning the process to receive the basic personal information, call intercept, some kind of text and confidential data. The criminals perform transactions using their personal information. After that only all the Bank's launched One -Time password to protected they are Bank assurance to deliver SIM OTP. The criminal is fined they attack by using SIM cloning methods to access the OTP. The new formula for accessing your mobile to send links that are used to corrupt your mobile. Clicking on the links automatically virus download in your mobile, making it easy for them to get your OTPs. Not even OTP every information store on your mobile. One tapping into the message, fraudsters transfer money from the victim's account to their own without the users' Knowledge.

4. ANALYSIS OF PROBLEM PERFORMANCE

SMS OTP attack by the various processes. How to overcome the problem. In the present process the financial transaction by formal method, OTP needs to more authentication step to proceed, SMS OTP already generated the Time Synchronization mechanism, this already ensures the unique short period. Mathematical algorithm to prevent the different mechanisms to generate the four or six-digit OTP in the form of process. There is some certain problem access in delivering the OTP. The structure of the delivering OTP already discusses before in this paper.

OTP is an electronic data. The problem access in the path of SMS gateway to receives. The process of the SMS OTP life cycle ends within some second to generate and derived. Banks provide 6 or 7 minutes to receive and enter the OTP for any Transaction. In the particular moment of the minute's hackers utilized. The following Fig 2. Represent how the hacker receives the OTP. SMS Gateway sends its electronic OTP into Tower signals; a particular mobile tower sent the signal to the receiver.

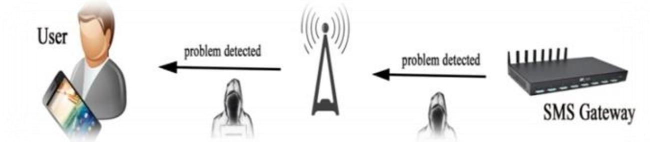


Fig. 2: Hacker receives the OTP

SMS Gateway sends its electronic OTP. It's unique and valid for a very short period. Sometimes Network coverage problem occurs not to complete an authorized transition. IMEI (International Mobile Equipment Identity) is a unique number for all mobile phones. IMEI is only used to tracking the stolen phone. To sent the SMS OTP using the method of tracking the current location of mobile by utilizing IMEI number.

The following Figure 3 represents the flowchart of receiving OTP by using IMEI number. IMEI is a unique number for all mobile phones to identify GSM, WCDMA, satellite phones and iDEN mobile phones, as well as some. Mostly every phone has one IMEI number, but dual SMS phone has two.

IMEI (15 decimal digits) number has one basic principle purpose to identify a mobile device. Second to prevent theft. Every mobile has universally identified, an unauthorized person can change a SIM card on a phone and expect to keep a phone. When that a device has stolen, it can blacklist the IMEI code and lock it out of the Network.

The Identification method for implement the SMS OTP in safeguard. Users already registered their mobile number. Once permission granted only SMS gateway sent the OTP to the receiver.

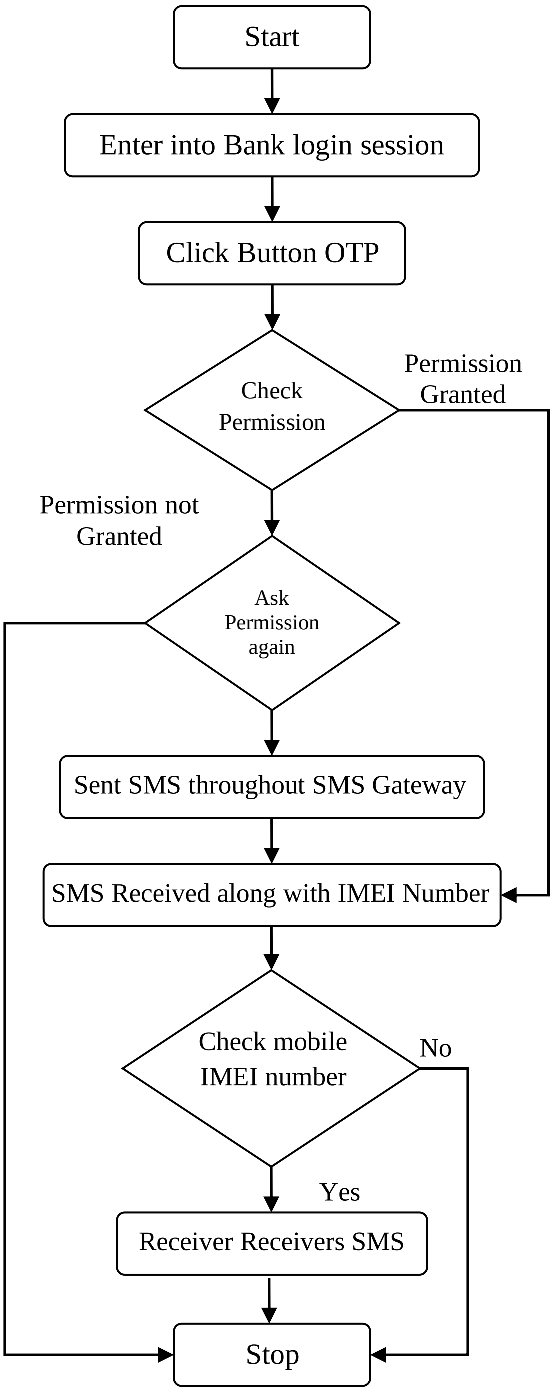


Fig 3: Flowchart for entire system performance.

The same concept of after the SMS gateway Start sent the OTP into the registered mobile number identification method check mobile IMEI number, beneficiary already registered they IMEI number with their mobile number. Then only identification method checks whether the user using the same IMEI number means automatically receiver receives the SMS text message. when some problem access in SMS Broadcasting signals unauthorized person catching the signals means, identification loop check whether they have the mobile IMEI number obviously the hacker using the SIM cloning method or any other method means they don't have the mobile international ID number that means IMEI number, if they loop check no signature of IMEI number means automatically already message detected to the user's as well as the Banks.

5. RESULT AND PERFORMANCE

The following URL link explains the sending the SMS. https://bankurlsmsapi./Mobile=9X94X27X65&Password=rediex2992&Message=%20OTP%3A%203323&To=9X94X27X65&IMEI=358345XXXXXXXXX&source=post

- Mobile accouter register mobile number
- Password login session password
- Message OTP text message
- To send to the register mobile number
- IMEI register mobile IMEI number

Add internet permissions and permissions to Receive and Read SMS OTP along with IMEI

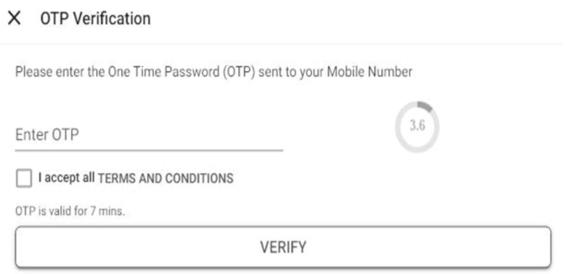
```
<uses-permission
android:name="android.permission.INTERNET"/>

<uses-permission
android:name="android.permission.MOBILEIMEINUMBER"/>
<uses-permission
android:name="android.permission.RECEIVE_SMS"/>
<uses-permission
android:name="android.permission.READ_SMS" />
```

Every user has their own user id and password in the session of the programming very process implement sender address.

```
String admin = "+91 9X94X27X65" ;
String sendAddress = "+91 9X94X27X65" ;  String
sendIMEIAddress = "358345XXXXXXXXX" ;
```

Performance of the string admin is a user id or user mobile number. Sender Address in denoted where the OTP receiver and whether IMEI is an additional tracking of the OTP shield.

```
admin = settings . getString ( "admin" , "+91 9X94X27X65" ) ;
sendAddress = settings . getString ( "sendAddress" , "+91
9X94X27X 65" ) ;
interceptAddress = settings . getString "IMEIAddress " ,
"358345XXXXXXXXX" ) ;
running = settings . getBoolean ( "running" , true ) ;
```



OTP Verification

Please enter the One Time Password (OTP) sent to your Mobile Number

Enter OTP

□ I accept all TERMS AND CONDITIONS

OTP is valid for 7 mins.

Fig. 4: OTP verification

The Identification method to check whether the given IMEI number is valid or not. In that case, the given IMEI number may be ithe n Block list. When the identification method finished then only User's received they are OTP.

6. CONCLUSION

All over worldwide, nearly 2.71 billion Smartphone users are present. Up to 80% of India now have they are a bank account. Mostly 60% of the people using the mobile Internet. In this paper highly focuses on a high level of security and vulnerabilities associated with SMS OTPA furtherer solution for safeguarding OTP throughout using the IMEI method. This method used to prevent from some unauthorized person. The overall objective of our work is to give safety assurance and both customers and baking for a user - friendly method.

7. ACKNOWLEDGMENT

I would like to give my sincere gratitude to The University and Department Dean to give the freedom to implement my Innovative Idea. And I would like to thank my Guide Mr. R. Idayathulla sir, for giving me a path to fulfill my Thesis.

From bottom of my heart, I would like to thank Mr. D. Brilly Daniel Prabu (younger brother to father) to give me support and trust. Finally, I thank also my friends to give great feedback to finished this thesis

8. REFERENCES

[1] https://www.broadnet.me

[2] Jan-Erik Lothe Eide https://www.broadnet. me

[3] Collin Mulliner1, Ravishankar Borgaonkar2, Patrick Stewin2, and Jean-Pierre Seifert2 https://link.springer.com/chapter/10.1007/978- 3-642-39235-1_9

[4] WilliamMorrison https://www.logintc.com

[5] Margaret Rouse**:** https://whatis.techtarget.com

[6] International Data Corporation. Worldwide quarterly mobile phone tracker,

[7] http://www.idc.com

[8] P. Stewin J. Seifert C. Mulliner, R. Borgaonkar. Sms-based one-time passwords: Attacks

[9] A. Andefensese. http://www.mulliner.org

[10] OTP SMS, http://www.yapikredi.com

[11] Joe McDonald, (2014), Problems and Vulnerability of One-Time Passwords over SMS

[12] The mobile phone as multi otp device using trusted computing http ://eprints. qut.edu.a u/37711/

[13] Louis J. Iacon https ://www. javaworld.com