International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Mobile Based Multi-Factor Authentication Algorithm for Secure Online Transaction

Ved Prakash Bhardwaj, Piyush Chauhan, Nitin

Abstract*: *In today's world, online payment system is one of the essential requirements of people. Security in online transactions is still a major challenge for the researchers. This work is emphasizing on providing highly secure environment for online transactions to user. One time password is one of the mechanisms to reduce online fraud, still many cases of fake transactions are happening frequently. It requires more attention to establish the faith in E-banking services. The present research article is proposing a multi-factor based secure algorithm which enhances the security for the online transaction services. To increase the authenticity, the proposed algorithm is working on two strategies: a) One Time Password Based Authentication and b) Dedicated Hardware Based Authentication.

***Keywords* : IMEI, Encryption, Decryption, OTP, Transaction**

I. INTRODUCTION

In recent years, the mobile phone users increase rapidly. Many of smart phone users prefer the online transaction. It is one of the finest and smart way, as it reduces the user's precious time, and their efforts. There are many modes available for performing online money based operations. It can be done using various payment apps like phone pay, google pay, paytm and through net banking. Security is one of important concern in this regard.

There are many factors responsible to breach the security of online transactions. Here, the current article is highlighting some of the factors which are given as:

A. Phishing Scams

Phishing is a cyber-attack in which the attacker accesses the sensitive information like user name, password, and many more things using various means of communication like phone call, email, social media etc. User may get any kind of communication from attacker through email like hyperlinks, attachments, and many fraud websites are also there which are created by attackers for accessing sensitive data of user.

B. Malicious Software

It is a kind of program which captures the user's data without permission.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Ved Prakash Bhardwaj*, School of Computer Science, University of Petroleum and Energy Studies. Dehradun, India,Email: ved.juit@gmail.com
Piyush Chauhan, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India, Email: shbichauhan@gmail.com
Nitin, Indian Institute of Management, Shillong, India, Email: nitin@iimshillong.ac.in

There are various types of malicious softwares; some of them are listed below:

- Spyware
- Virus
- Worm
- Logic Bomb
- Trapdoor
- Trojan
- Mobile Malicious Codes

C. DDoS Attacks

Both DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are very dangerous for the users. In case of DoS, the target URL is flooded by the attacker from one source. The server is overloaded with TCP and UDP packets. In case of DDoS, the same task has been performed by attackers with more than one source.

D. Other Factors

There are many other factors which cause online transaction fraud, like:

- Session Hijacking
- Eavesdropping
- Social Media

All the above mentioned factors anyhow get the sensitive data of the consumer and become the reason of cyber-attacks.

There are some common practices that a consumer can have to avoid such kind of attacks like:

- Don't use public WiFi for online banking and shopping.
- Update your softwares regularly, which enhance the security of the mobile device.
- Avoid installing unnecessary apps.

Further, the research article is organized as follows:
Section II is discussing about the preliminaries and related work in this direction. The proposed work has been discussed in section III. Section IV is covering the multi-level of authentication, and discussions. In section V, the conclusion and future scope of the work have been discussed. The references are given at the end of paper.

II. PRELIMINARIES AND BACKGROUND

Before moving towards the preliminaries, the following table will help the readers to understand the symbols which have been used throughout the paper:

Table- I: Symbol Table

S.No.	Symbol	Meaning
1.	IMEI	International Mobile Equipment Identity
2.	SIM_Install	Installation of Sim into the mobile device
3.	Install_IMEI	Installation of IMEI application
4.	Enter_Details	User name, and password or card details
5.	Trns_Fail	Transaction Fail
6.	Trns_Succ	Transaction Successful
7.	R_IMEI	Bank is Requesting to Consumer to activate IMEI Application
8.	Bio_Data	Biometric data like thumb or figure impression
9.	Invo_IMEI	IMEI Application is invocated
10.	IMEI_Data	Verification of IMEI and other user data at bank server
11.	Algo_OTP	One Time Password Generation Algorithm generates OTP and sends to Consumer
12.	Data_Ins	OTP insertion by the Consumer
13.	SIM	Subscriber Identification Module
14.	Cons_Pay_IMEI	Payment portal with IMEI number at consumer side
15	Algorithm_MFA	Muti-Factor Authentication Algorithm
16	IMEI_OTP	Combination of IMEI and OTP

A. Multifactor Authentication

In secure and successful online transaction user authentication is most vital component [1]. Here authentication helps us to verify originality [2] of entity in online transaction. Entity is either a person, also it can be user's device or anything constituting component of online transaction. Entities are authenticated with help of authentication factor [3].

Authentication factor constitute of mainly three subcategories:

- Knowledge Factor,
- Possession Factor
- Inherence Factor

However various other subcategories like location based authentication exist. Further these authentication factors are mingled together to enhance authentication. This Hybrid form is known as Multi factor authentication [4].

B. SMS-OTP Based System

Multi factor authentication system is further strengthened with short message based onetime passwords. SMS-OTP system [5, 6, 7] works safely as long as only authenticated user has access to Mobile device used for online transaction. Though confidentiality of SMS message is difficult to maintain. SMS message can be accessed by unfair means because of following factors:

a) Attack on GSM and 4G network,

b)Dependencies on securities of cellular network,

c) Mobile phone Trojans and many more.

Hence security enhancement of SMS-OTP is need of a day for multifactor authentication system to work securely. SMS OTP system structure is similar throughout its vast applications. Fig.1. represent the SMS OTP system.

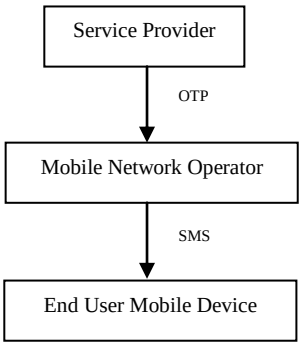

Fig.1. SMS-OTP Based System

After creating an OTP service provider requests mobile network operator to provide SMS-OTP to user's mobile device. User via mobile device enters the OTP on webpage of OTP service provider. However there are a lot of parties involved in SMS-OTP system structure.

This yields a security threat to confidentiality of SMS- OTP system. Attacker has several options to breach this SMS-OTP system via, physical access to mobile device, SIM Swap attack, Wireless interception, Trojans. Cellular Network insecurity and design issues in Mobile Phone Operating systems leads to SMS-OTP system Breach by attacker.

SMS-OTP system can be further protected with help of many maneuvers and counter measures. In [8] various countermeasures methods are proposed. In first method, authors revolve around idea of applying end to end encryption of SMS. This technique has dependency on mobile network operator. Further SMS will be visible to SMS-OTP Trojan, though customer specific key will not be accessible to Trojan. This methodology leads to another controversial additional step of key distribution. Hence authors proposed second technique of dedicated channel on operating system of mobile. Here also we need to modify Mobile operating system.

Final methodology neither requiring modification of Operating system, nor the support of service provider was proposed; as filter based channel message. Here we have a filter mechanism which acts independently inside mobile operating system's SMS fetching code.

Two type of filters were proposed in [8]. This filter will lead to additional computation cost at client side. Prior to above research article another work [9] only gives glimpse of mTAN (mobile Transaction Authorization Number) security risk analysis for both Andoid and iOS based handheld devices.

Recently in [10] researchers have utilized NDB (negative Databases) to further enhance password authentication scheme instead of OTP authentication founded on encryption algorithms. This scheme is extra safe because of bonus layer, grounded on the NDB is engaged to shield private data. However this research work requires further investigation to resist insider attack and server spoofing attack. In [11], new methods have been discussed for secure mobile payments.

III. PROPOSED WORK

The main concern here is the IMEI number, and based on IMEI, a dedicated application is required to be built on every mobile phone by the manufacturing company.

The idea is to have IMEI application on every mobile device and it must be mandatory to install IMEI application by the consumer for smooth functioning of device.
Therefore, before moving on the functionality of Multi-Factor Authentication Algorithm, here we are discussing about IMEI application and its core components.

A. Registration of IMEI Application

The idea is to process the online transaction request with dedicated hardware only. The device with IMEI number which has been registered with bank server will receive the OTP, in case when any online query is prompted by registered user.
It will happen with the help of IMEI application, which has been installed with user's mobile phone. The mobile manufacturing companies should provide the IMEI application as a mandatory installation whenever user inserts the SIM to activate the phone.
Before activating the proposed algorithm, following steps are required to follow by the consumer:
Step1: IMEI Application Installation
To activate a SIM in mobile device, a mandatory IMEI application has to be installed by the consumer in the mobile phone. This application will take following details from the consumer:

- Complete Name
- Aadhar Number
- Permanent address
- Occupation
- Biometric Authentication
- Mobile Number with alternate options
- Authentic Email Address
- Mobile Number
- SIM Number

The IMEI number is hard coded on the device means it is already provided by the mobile manufacturing companies and it must never be changed by the consumer.
Step2: Bank Registration
Here the consumer will provide all the details which are given in step 1, to the authorized bank.
Step3: Data Transmission through IMEI Application
After sharing the details with bank, consumer will send the request to bank server to authenticate the same.
Step4: Verification
Bank will verify the data and it will add the IMEI application request number in its record.

B. Multi-Factor Authentication Algorithm

As per the given algorithm, consumer selects the payment option like net banking or card payment and enters the details accordingly. The given details are verified by bank server, if it is okay, then bank server requests the consumer to activate the IMEI application. To activate the same, user provides the biometric data like thumb impression or face scanning. If it is okay then the IMEI application sends all the details including IMEI number to bank server for verification.

Algorithm_MFA

1. Begin
2. Consumer selects Payment Option .
3. if (Enter_Details == 0)
4. Trns_Fails
5. else
6. goto step 7
7. Activate IMEI Application.
8. if (Bio_data==0)
9. Trns_Fails
10. else
11. goto step 12
12. IMEI application is activated.
13. if (IMEI_data==0)
14. Trns_Fails
15. else
16. Algo_OTP( ).
17. Cons_Pay_IMEI
18. Consumer gets OTP and enters the same in given text box.
19. Bank server verifies the combination of IMEI number and OTP, entered by Consumer.
20. If (IMEI_OTP==0)
21. Trns_Fails
22. else
23. Trns_Succ.
24. End.

Further, bank server verifies all the information, especially the IMEI number. If all the data provided by IMEI application is okay, then bank sends the OTP to consumer on the registered mobile device. The OTP is created by the OTP generation algorithm. At the consumer side the payment portal is available; there the consumer will enters the OTP. The payment page will be having the IMEI number to maintain the uniqueness and security like this:

XXX-XXX-XXX-XXX-XXX	YY-YY-YY

Fig.2. 15-Digits IMEI and 6-Digits OTP

Here, on the payment portal the IMEI number will be provided by IMEI application, which is shown by the word X, and consumer will enter the OTP, which has been shown here by the word Y.
Therefore, it will be a 15+6, total 21 digit code for the payment and IMEI application again sends this combination to bank server for verification. If it is okay then transaction will be successfully completed or fails. Further, every consumer has a unique IMEI number and in case if the OTP is known to any hacker still the payment system will not work and transaction fails. It means the OTP will work only on the authenticate consumer's device. Therefore, it does not matter if anyone knows the OTP.

C. OTP Generation Algorithm

Basically, OTP generation is very sensitive issue. This research is supporting 6 or 8 digits OTP to complete any online transaction. The OTP can be created by various cryptographic algorithms. It is also a subject of research, which we will discuss in the future. Here, the algorithm is basically supporting the existing algorithms of OTP generation, which are used in current scenarios.

D. Reason of Choosing IMEI Application

Through this research, the author wants to suggest to all mobile manufacturing companies to create their own IMEI application. Therefore, it can be installed mandatorily when the consumer wants to activate his mobile device.

This app will store all the details of consumer and send it to bank server. The intention of this research is that, the OTP must reach on the only mobile device whose IMEI number with all details is stored on the bank server. IMEI number plays a vital role in this regard, as it is unique. All the other parameters like mobile number, address, and account number may change but it will not change. In case if IMEI number does not match, the bank server will not send any OTP and the transaction will fail.

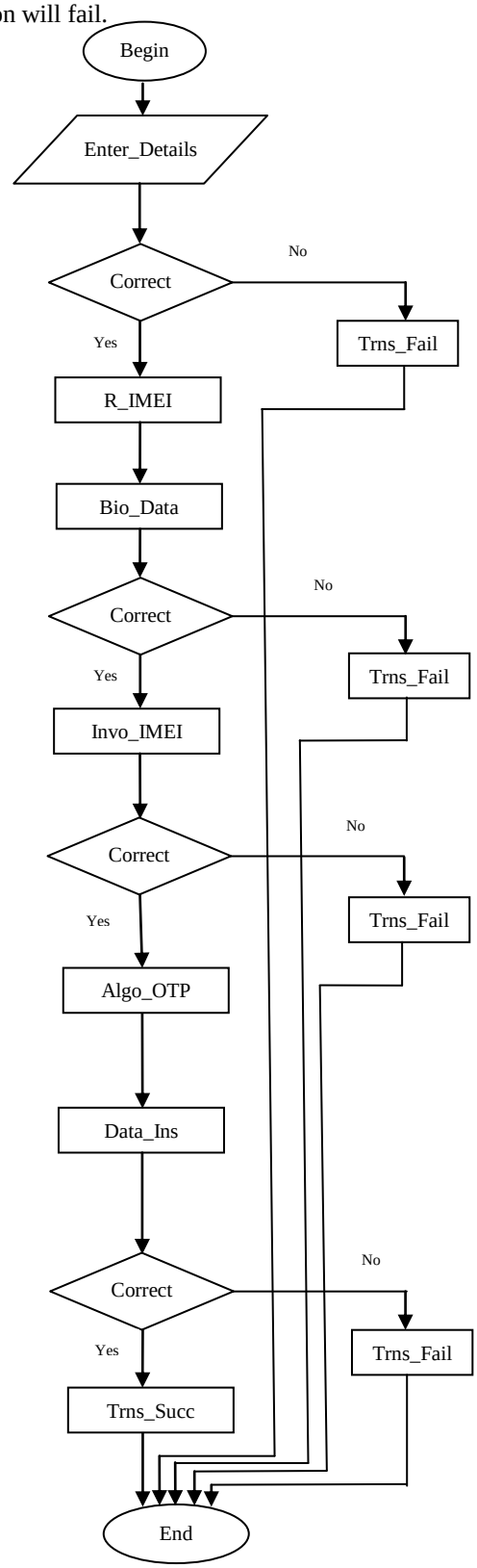

Fig.3. Flowchart of Proposed Algorithm

Fig.3. shows the basic flow of the online transaction procedure. In next section, the same has been explained in a detailed way.

IV. DISCUSSION ON MULTI-LEVEL AUTHENTICATION

Here the authors are discussing the number of authentication levels which are supporting their algorithm for a secure transaction. This process is shown in a more detailed way by step wise manner:

Step1.

When any consumer starts the online transaction process, then as per the algorithm the required details like user name and password are entered. If the consumer has the debit or credit card then card details will be entered.

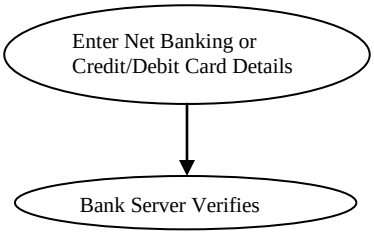

Fig.4. First Level of Authentication

It is the first step of authentication. Any wrong information will decline the transaction.

Step2.

Next, a request from bank server is sent to consumer to activate the IMEI application. Consumer needs to provide its biometric data.

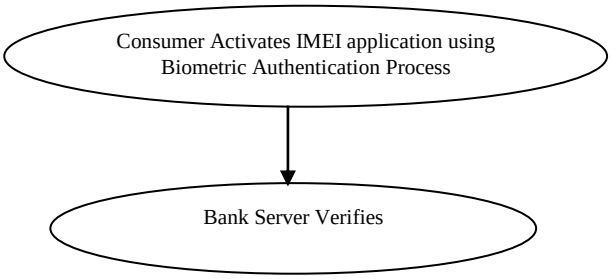

Fig.5. Second Level of Authentication

It is the second step of authentication. If the wrong biometric information has been entered, the transaction will be declined.

Step3.

When user put the correct biometric information, then in the transaction process consumer will redirect to IMEI application page and activate the same. After activation, all details of consumer including IMEI number will be communicated to bank server. Bank server verifies and responds accordingly.

It is the third step of authentication.

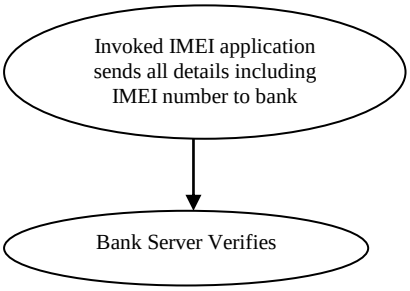

Fig.6. Third Level of Authentication

Step4.

OTP generation algorithm provides OTP to bank server, and bank server sends the same to consumer. Here, on the payment portal the IMEI application will throw the IMEI number and with this the consumer enters the OTP. Bank server checks the same.

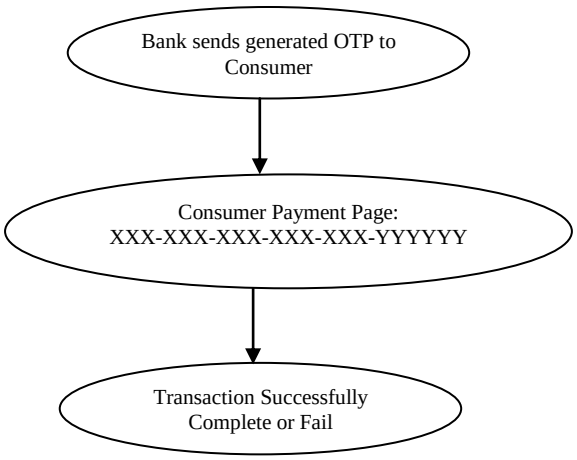

Fig.7. Forth Level of Authentication

It is the forth step of authentication. The IMEI number along with OTP will have a combination of 21 digits. Here we are considering the 6 digit OTP. This combination will be unique definitely. Any hacker can steal the OTP but will be unable to run the same on his mobile device. This is the power of IMEI application. Further, any wrong information will stop the payment process and transaction will fail.

V. CONCLUSION AND FUTURE SCOPE OF WORK

Emphasis of this research work is to provide highly secure environment for online transaction activities. To handle this issue, authors have suggested considering IMEI number as a main source of authentication. The OTP must reach on the authenticated hardware device, identified by its unique IMEI number or transaction gets fail.

The proposed IMEI application should be hard coded in the mobile device itself and must not be change in any circumstance. In future, securing the generated OTP from man in the middle attack or any other kinds of attack are still challenges for the researchers.

Additional security layer or some strong encryption techniques can be applied for securing the communication between consumer and bank server.

ACKNOWLEDGMENT

This research work is dedicated to my family members, almighty God, my guide, and University of Petroleum and Energy Studies. Further, commercialization of proposed algorithm is allowed only, after the approval of authors of the paper.

REFERENCES

1. W.Jansen, Authenticating Users on Handheld Devices, in Proceedings of the Canadian Information Technology Security Symposium, 2003, pp. 1–12.
2. R. Madhusudhan, R.C. Mittal, Dynamic ID-based Remote User Password Authentication Schemes using Smart Cards: A Review, In Journal of Networks and Computer Applications,Volume 35, Issue 4, 2012, pp.1235-1248.
3. H. Al-Assam, H. Sellahewa, S. Jassim, On Security of Multi-Factor Biometric Authentication, Internet Technology and SecuredTransactions, in International Conference of Internet Technology, 2010, pp. 1-6.
4. X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H. Deng, A Generic Framework for Three Factor Authentication: Preserving Security and Privacy in Distributed Systems, in IEEE Transactions on Parallel and Distributed Systems,Volume 22, Issue 8, 2011, pp. 1390-1397.
5. 3rd Generation Partnership Project. 3GPP TS 23.040 - Technical realization of the Short Message Service (SMS). http://www.3gpp.org/ftp/Specs/html-info/23040.htm, September 2004.
6. Google Inc. SMS Verification for App Creation. https://developers.google.com/appengine/kb/sms.
7. Google Inc. Verifying your account via SMS or Voice Call. http://support.google.com/mail/bin/answer.py?hl=en&answer=114129.
8. Mulliner C., Borgaonkar R., Stewin P., Seifert JP, SMS-Based One-Time Passwords: Attacks and Defense. In: Rieck K., Stewin P., Seifert JP. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2013. Lecture Notes in Computer Science, Volume 7967. Springer, Berlin, Heidelberg.
9. L. Koot. Security of mobile TAN an smartphones. Master's thesis, Radboud University Nijmegen, Feb. 2012.
10. D. Zhao, W. Luo., One-Time Password Authentication Scheme Based on the Negative Database. In Engineering Applications of Artificial Intelligence Volume 62, 2017, pp. 396-404.
11. T. K. Chang, A Secure Operational Model for Mobile Payments, in The Scientific World Journal, Volume 2014, Hindwai Publishing Corporation, 2014, pp. 1-14.