IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-5, Issue-6 E-ISSN: 2347-2693

A Review on Secured One Time Password Based Authentication and Validation System

Rachita Dubey[1*], Jijo S.Nair[2]

[1*]Dept. Of Computer Science, Oriental Institute of Science and Technology, Bhopal, India
[2]Dept. Of Computer Science, Oriental Institute of Science and Technology, Bhopal, India

[*]*Corresponding Author: rachitadubey1991@gmail.com*

Available online at: www.ijcseonline.org

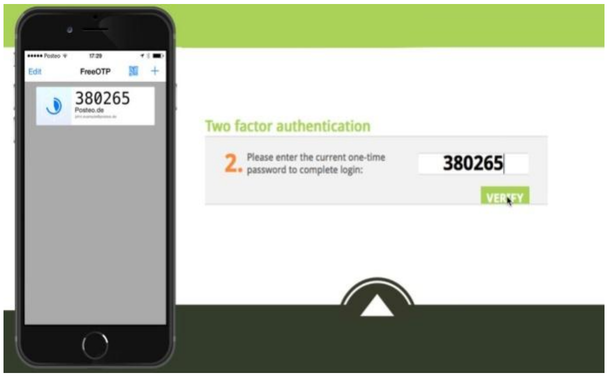
Received: 15/May/2017, Revised: 28/May/2017, Accepted: 17/Jun/2017, Published: 30/Jun/2017

***Abstract*—** In this digital world, authentication of legitimate user is highly important for secure banking transactions and activities, One Time Password (OTP) security is one of them. Online banking requires some kind of authentication to verify whether it is performed by legitimate user or not. By the help of One Time Password it can be performed securely. When someone perform any online transaction, he/she would be asked to input One Time Password which has been sent to his/her registered mobile number, if it is legitimate user then transaction would be successfully performed otherwise no one can do any fraudulent activity without having One Time Password. But what happens when someone has stolen your mobile phone and by having your username and password along with your mobile phone, he/she would be able to perform successful transactions. For this case we require much more tenable process to secure our banking account from any kind of fraudulent activities. This paper has been proposed for review of existing systems which provide security in the field of authentication.

***Keywords*—**Component OTP, Authentication, Legitimate, MATLAB, Mobile

I. Introduction

Each and every country is getting digital and peoples are getting involved in digital process. Digital payments, online banking, Identification system, attendance and many more get digitalized and all these areas require good security system to beware from fraudulent activities. There are so many security features available for better secure transaction. Consider an example of online banking where online transactions occur, this system get secured using the combination of username and password, after this username and password turned more complicated to guess for unauthorized users by making username and password strong. To enhance the security, One Time Password (OTP) has been introduced which provides the best security till now because OTP will be sent to your mobile phone while performing online transactions, you will have to input the correct One Time Password then only you can access your data or perform successful transactions otherwise no one can access it. But the problem occurs when you lost your mobile phone and third party knew about your username and password and by having your mobile phone he would be able to perform successful transactions. But this case is exception that is why it is considered as best security provider. But authentication is also concerned and it should not be ignored.



2. Please enter the current one-time password to complete login: 380265

Fig. 1 One Time Password – An Example

II. Related Work

Implementing One Time Password Based Security Mechanism for Securing Personal Health Records in Cloud proposed by Ramesh K and Ramesh S in IEEE. 2014 [1]

This paper proposed a system that claimed to secure personal health records in insecure cloud using one time password i.e. OTP. OTP would be asked while uploading data in cloud. Here OTP is used for authentication module along with

Advanced Encryption Standard i.e. AES. But what happened if you lost your mobile phone or when you are connected to the insecure network connection. Here we required more secured OTP authentication system for better security concerns.

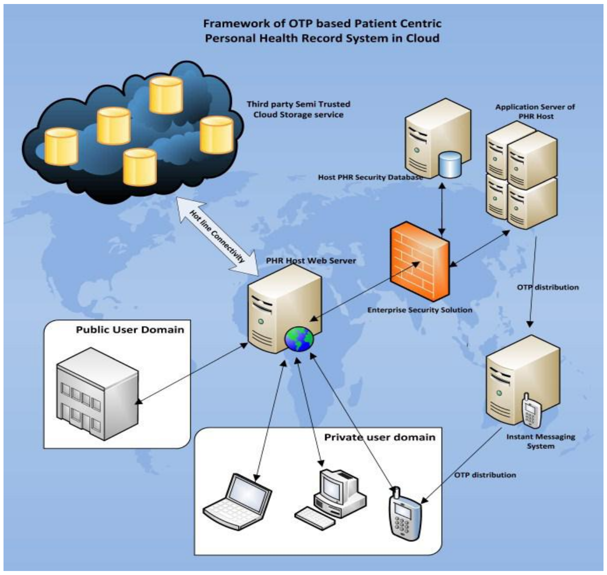

Framework of OTP based Patient Centric Personal Health Record System in Cloud
Third party Semi Trusted Cloud Storage service
Application Server of PHR Host
Host PHR Security Database
Hot line Connectivity
PHR Host Web Server
Enterprise Security Solution
OTP distribution
Public User Domain
Private user domain
Instant Messaging System
OTP distribution

Fig. 2.1 System Overview

Mobile Attendance using Near Field Communication and One-Time Password proposed by John Jacob, Kavya Jha, Paarth Kotak and Shubha Puthran in 2015 on IEEE. [2]

This paper introduced NFC – Near Field Communication for M- attendance system for university students. NFC offers fastest way communication between two devices within a second. So by the help of NFC along with OTP i.e. one time password so that no one can make proxy attendance because OTP provides only one login session or transaction on a device that makes system more secure and proxy attendance of a student will not get possible to occur. But having device is not only a proof that it is you or an authorized user.

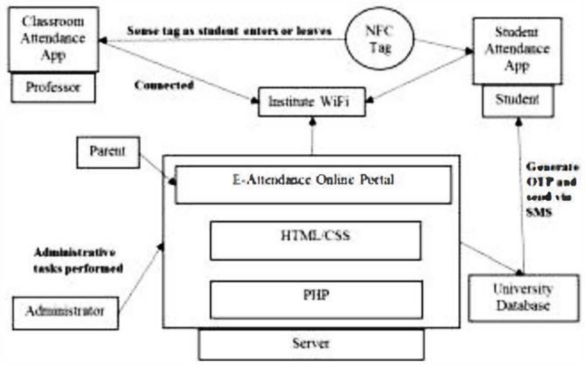


Fig. 2.2 Block Diagram

Towards Designing and Implementing a Secure One Time Password (OTP) Authentication System proposed by Swapnoneel Roy,Matt Rutherford and Charlene H. Crawshaw in 2016 on IEEE. [3]

This paper proposed a system that provides more secure OTP by having an analysis with respect to its recommended requirements for strong OTP, such as length, case sensitive, inclusion of numerical character, inclusion of special character, no words of significance (like it can't be found in a dictionary, do not relate to the habits of individual, meaningful combinations {like license number, telephone number etc.}, abbreviations). But this system only generates the OTP and by just generating a secure OTP is not a secure method to identify a legitimate user.

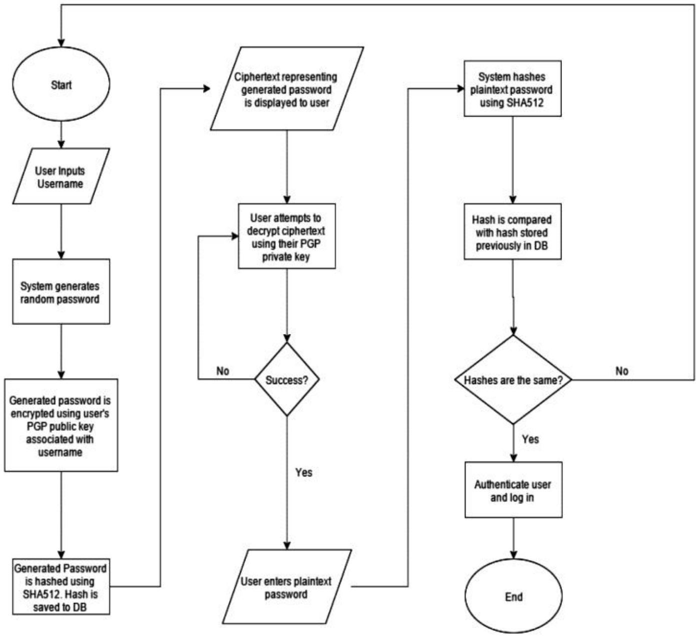

Start
User Inputs Username
System generates random password
Generated password is encrypted using user's PGP public key associated with username
Generated Password is hashed using SHA512. Hash is saved to DB
Ciphertext representing generated password is displayed to user
User attempts to decrypt ciphertext using their PGP private key
Success?
No
Yes
User enters plaintext password
System hashes plaintext password using SHA512
Hash is compared with hash stored previously in DB
Hashes are the same?
No
Yes
Authenticate user and log in
End

Fig. 2.3 Flow Chart

On The Generation of Alphanumeric One Time Passwords proposed by Shubham Srivastava and Sivasankar M in 2016 IEEE. [4]

In this paper a system is proposed in which a way of generating alphanumeric OTP using automation theory with linear functions is given but by using alphanumeric characters in an OTP will only assure the authenticity of the password not of the user who is getting that one time system generated alphanumeric password to access the data.

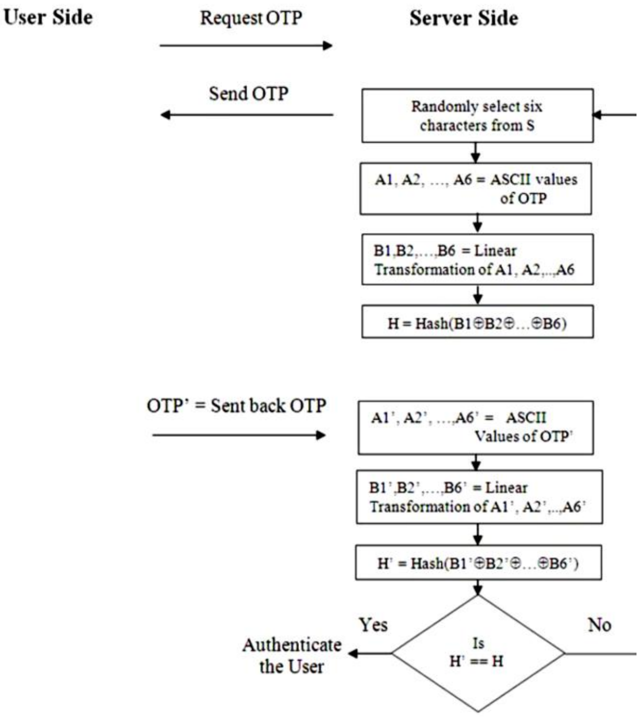

User Side
Request OTP
Server Side
Send OTP
Randomly select six characters from S
A1, A2, …, A6 = ASCII values of OTP
B1,B2,…,B6 = Linear Transformation of A1, A2,..,A6
H = Hash(B1⊕B2⊕…⊕B6)
OTP' = Sent back OTP
A1', A2', …,A6' = ASCII Values of OTP'
B1',B2',…,B6' = Linear Transformation of A1', A2',..,A6'
H' = Hash(B1'⊕B2'⊕…⊕B6')
Yes
No
Authenticate the User
Is H' == H

Fig. 2.4 OTP Sending & Verification Phase

SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account proposed by Eddy Prasetyo Nugroho, Rizky Rachman Judhie Putra, Iman Muhamad Ramadhan in 2016 2nd International Conference on Science in Information Technology (ICSITech) of IEEE. [5]

A system is proposed in this paper in which Advanced Encryption Standard Algorithm of cryptography is used to generate the SMS authentication code i.e. OTP. This system uses 256 Bit encryption scheme of AES as it contains more key combinations. The algorithm used in this paper have been modified with S-Box and Shift Rows which has passed testing avalanche effect and randomness tests can be implemented to generate the authentication code. But this algorithm takes more time to execute than the standard AES-256 algorithm. This paper enhances the security of generation of activation code to reduce the creation of fake accounts but the authorization of the user to completely secure the system is not the part of this project as it emphasizes on the security of OTP only which will not secure the system completely.

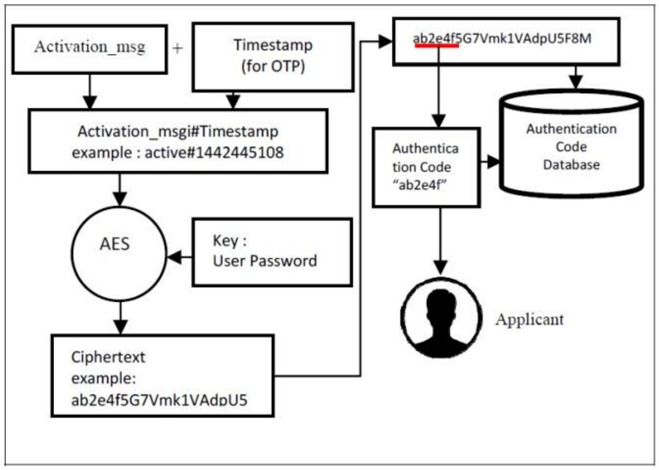


Fig. 2.5 Generating Authentication Code

Considerations of Emerging Cloud Computing in Financial Industry and One-Time Password with Valet Key Solution proposed by TE-YUAN LIN and CHIOU-SHANN FUH in 2016 IEEE International Conference on Computer and Information Technology of IEEE. [6]

This paper proposed a design called "Hybrid Cloud Architecture with OTP Valet Key Protection" based on the mixed deployment model to get a balance in between of the security concerns and the merits brought by the cloud computing. Basically in this project, an extra valet key token is generated with the OTP and send it to the user's registered credentials to enable any data access operations. This token is time limited but if the user who is getting this OTP is not the registered one, the possibility of the processing of data against any unauthorized access or theft may increase.

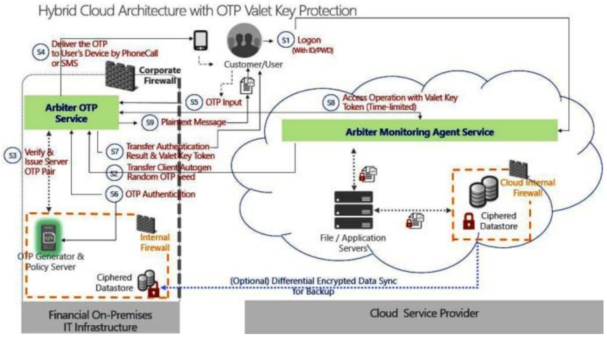

Hybrid Cloud Architecture with OTP Valet Key Protection
S4 Deliver the OTP to User's Device by PhoneCall or SMS
Customer/User
S1 Logon (With ID/PWD)
Corporate Firewall
Arbiter OTP Service
S5 OTP Input
S9 Plaintext Message
S8 Access Operation with Valet Key Token (Time-limited)
Arbiter Monitoring Agent Service
S3 Verify & Issue Server OTP Pair
S7 Transfer Authentication Result & Valet Key Token
S2 Transfer Client Autogen Random OTP Seed
S6 OTP Authentication
Cloud Internal Firewall
Ciphered Datastore
Internal Firewall
OTP Generator & Policy Server
File / Application Servers
Ciphered Datastore
(Optional) Differential Encrypted Data Sync for Backup
Financial On-Premises IT Infrastructure
Cloud Service Provider

Fig. 2.6 Hybrid Cloud Architecture with OTP Valet Key Protection Overview

Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP proposed by Joyce Soares and A.N.Gaikwad in 2016

International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) of IEEE. [7]

Based on the OTP (One Time Password), a security authentication model that is called OTP_SAM is mainly proposed in this paper. The model combines with the current system time to compute the one-time key, and then use the key to generate the message authentication code by hash algorithm. Finally, the model achieves the objective of the security authentication through the verification of the authentication code in Option180. In this paper, the project examines the security vulnerabilities to DHCP protocol, and discusses some existing techniques to secure DHCP protocol and their shortcomings. On the basis of them, the implementation of the DHCP security authentication Model OTP_SAM, which can be implemented together with the traditional DHCP protocol and that user can choose whether start authentication module. This paper is again emphasizes on the security of system generated OTP which secures the authentication message generated by the system but not the user who will receive that OTP.

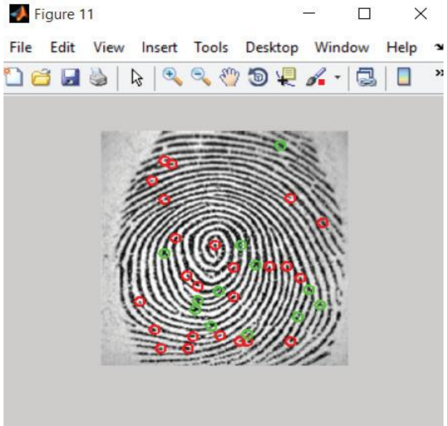


Fig. 2.7 Fingerprint Authentication

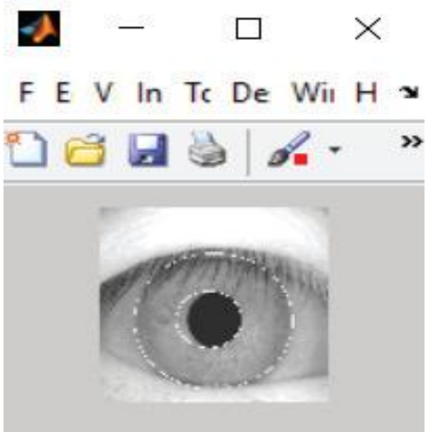


Fig. 2.8 Iris Authentication

OTP_SAM: DHCP security authentication model based on OTP proposed by Fuqiang Zhang and Lin Chen in 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design. [8]

The paper proposes a system in which a security authentication model, termed as OTP_SAM is primarily projected. Combination of the existing system's time is used in this model to figure the one-time key, and then generate the key is used to create the message confirmation code by using the hash algorithm. At the end, the whole system reaches the objective of the security validation through the verification of the verification cipher in Option180. The projects inspect the safety susceptibilities to DHCP protocol, and discuss some existing techniques to secure DHCP protocol and their weaknesses. On the basis of them, the implementation of the DHCP security authentication Model OTP_SAM, which can be implemented together with the traditional DHCP protocol and that user can choose whether start authentication module. This paper again highlights the security of system generated OTP which secures the authentication message generated by the system but not the user who will receive that OTP.

III. PROBLEM STATEMENT

Existing systems are not intelligent enough to identify the legitimate users. Most of the papers which have been mentioned over here focused on transformation of simple OTP to complicated or strong OTP for better security concerns. But making OTP complicated or strong is not only the solution for the detection of unauthorized access. We require a system that can be able to identify the authorized users and allow them to access their data and deny the unauthorized users.

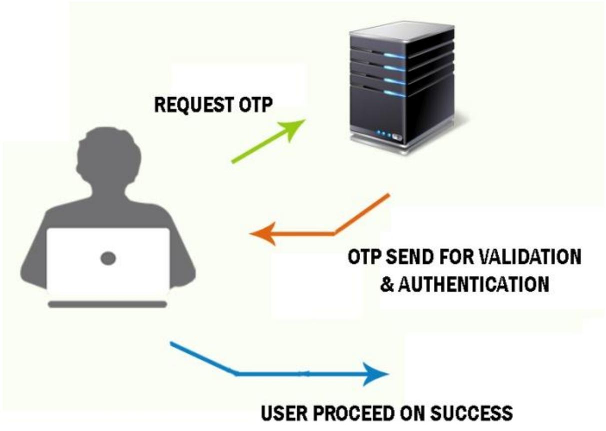


Fig. 3.1 OTP Validation & Authentication

IV. CONCLUSION

Thus the survey of all these systems concluded at a point of enhancement of One Time Password either by making it strong (i.e. using of special characters, use of capital letters, not uses of dictionary words and many more) or by fingerprint/iris authentication. Making OTP strong is not a confirmation of legitimate user and fingerprint/iris authentication is not convenient at all. Thus the system requires alternate solutions for better secure authentication.

V. FUTURE SCOPE

The current proposed concept of One Time Password get enhanced in future by making voice authentication based OTP which would be able to identify legitimate user by their voice which may provide best security features in the field of digital world.

REFERENCES

[1] Ramesh K and Ramesh S, "*Implementing One Time Password Based Security Mechanism for Securing Personal Health Records in Cloud*", IEEE Transaction, 2014.

[2] John Jacob, Kavya Jha, Paarth Kotak and Shubha Puthran, "*Mobile Attendance using Near Field Communication and One-Time Password*", IEEE Transaction, 2015.

[3] Swapnoneel Roy,Matt Rutherford and Charlene H. Crawshaw, "*Towards Designing and Implementing a Secure One Time Password (OTP) Authentication System*", IEEE Transaction, 2016.

[4] Shubham Srivastava and Sivasankar M, "*On The Generation of Alphanumeric One Time Passwords*", IEEE Transaction, 2016.

[5] Eddy Prasetyo Nugroho, Rizky Rachman Judhie Putra, Iman Muhamad Ramadhan, "*SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account*", IEEE Transaction, 2016.

[6] TE-YUAN LIN and CHIOU-SHANN FUH, "*Considerations of Emerging Cloud Computing in Financial Industry and One-Time Password with Valet Key Solution*", IEEE Transaction, 2016.

[7] Joyce Soares and A.N.Gaikwad, "*Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP*", IEEE Transaction, 2016.

[8] Fuqiang Zhang and Lin Chen, "*OTP_SAM: DHCP security authentication model based on OTP*", IEEE Transaction, 2016.

Authors Profile

Rachita Dubey pursuing Master of Technology in Computer Science and Engineering. Computational Sciences, Department of Electronic and Communication, University of Taiwan, Taiwan since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013, ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.

Mr Jijo S.Nair is working as a professor in Oriental Institute of Science and Technology, Bhopal in Madhra Pradesh. Bachelor of Science and Master of Science from University of New York, USA in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Telecommunication, University of New York, USA since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013 and ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.