ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(5), DOI: 10.17485/ijst/2016/v9i5/87154, February 2016* ISSN (Online) : 0974-5645

PB Verification and Authentication for Server using Multi Communication

D. Ganesh Kumar[1*], S. Rajasekaran[1] and R. Prabu[2]

[1]Department of Computer Science and Engineering, Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai - 600062, Tamilnadu, India; ganeshprivate@gmail.com, rajasekaran009@gmail.com|
[2]Department of Information Technology; Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai - 600062, Tamilnadu, India; dprpit@gmail.com

Abstract

Objective: To provide Password authentication by cloud through performing tri stages and also to improve the security. **Method:** First stage is registration phase; it involves issuing of cloud space to user. Cloud space is used for storing all self information of the client which is used for checking authenticity for later usage. Password of user is generated by user or by server based on password user can registered into cloud. If registration process is completed, then users are able to access the server log-in whenever they needed. Protocol based verification and authentication for two different mediums (Duos) uses user's cell phones or mobile devices is used as SMS to avoid hacking of password and backtrack attack using password. Using unique phone number Duos system possesses website and involves a telecommunication service provider in recovery and registration phase-in Duos based authentication system user want to remember only the Long-Term Password (LTP) for login in all websites. Efficient and affordable authentication is provided by Duos. For successful login of user's, they need valid smartcard and correct password. It involves two-factor password phase and cloud space. **Findings:** Users able to change their password freely in password changing phase and update his/her information to cloud space. **Applications/Improvements:** The secured web authentication done successfully by using two types of registration which are named as Registration on Website and on the Mobile device. The scalability of the device is achieved.

Keywords: Long Time Password (LTP), Mobile Device, QR Code, SOAP Protocol

1. Introduction

Cloud authentication system involves cloud, user, and a server. Cloud based password authentication consists of three phases. The first phase is registration phase wherein the user register personal information in system in cloud phase which is allocated by server. Cloud space contains all personal information about user that needed for authentication. Initial generated password during this phase is either chosen by server or user. After registration succeeded, user can access log-in phase of the server as many times as they needed. Protocol based verification and authentication for Duos medium (two different medium) such as user's mobile device and short message service prevents hacking of password and password reuse attacks. Duos system needs unique phone number for each websites and involves telecommunication service provider for registration and recovery phases. Duos system allows user to remember only Long Time Password for registration login for all websites. Duos are affordable and efficient authentication systems compared with other web authentication mechanisms. Successful login of user involves two-factor, password and cloud space authentication. This contains valid smartcard and correct password. After registration process into web application, users are able to freely change their Password and update the changed information into cloud space used for further authentication of users.

2. Problem Definition

Text based password is conveniently used for authentication

* *Author for correspondence*

system on websites due to its simplicity. It forms a threat due to password theft, compromised under different situations using algorithms and undergo vulnerabilities. Users select weak password or easily guessed passwords vulnerable for attackers to get password of users and access in user account. Attackers repeatedly reusing of same password causes domino effect; where adversary compromised users password and exploit to gain access of more websites. Second, when users type their password using untrusted computers then adversaries get password forms thief thread. Adversaries launch password stealing attacks such as phishing of password, malware and snatching passwords. Cloud based authentication is a security mechanism which recognize remote client, which should hold valid cloud space and password to verify successful authenticity with server. Disadvantage of Duos system is scanning of QR code. Scanning of QR code need smart phone and internet connection. Without internet connection QR code must not be scan and it also need to download the application before start of scanning QR code.

Decentralized access control allows anonymous authentication shows initialization of system[1]. Here private key is used for message signed and public key used for verification. Prime number we selected is q. for registration KDC-key distribution contains kbase used for signature. KDC setup: used for key distribution to user. It includes Token verification: used for verification of user's signature and retrieves kbase consistency. Cloud act as intermediate and send data as cipher text. Attribute verification: if attributes of stored value and entered value is satisfied then data is accessed by user. Access: person authenticates to access the data. Verify: contains creation of attributes, encryption of data by cloud and decryption of data by owner and attributes. Data accessing in cloud uses two algorithms it includes 1) APPROX-POLICY COVER1 algorithm: includes attribute based accessing. 2) POLICY DECOMPOSITION algorithm: used to generate two types of tokes. One set is kept by owner and another is distributed to cloud. These two sets are unique key called as ILE key, given for access control provider. They encrypt all data with key and execute keygen for generate public key and trusted key. Users at destination site receives data and decrypt data twice because public key generation of cloud at first and owner of data. Cloud service provider (CSP) forms mutual understanding between server and CSP[2]. It allows CSP to perform operation like insert, delete, etc., of sensitive data by CSP. It allows indirect mutual trust between owner and CSP. It contains 1) Data owner registration and load a data to CSP. 2) Data owner registration who wants the data. 3) TTP (trusted third party) Login: monitors the file send by data owners. Augmented Encrypted Key Exchange[3] Bellovin and Merritt about sharing of password for communication without exposing password by two parties. Hash function used for storing password. Hash function calculates password to find matching of stored password and given password. Augmented encrypted key exchange (A-EKE), contains information about host used for store the password. Both users share their password using EXE exchange. It defines user must to send additional messages like password by different one-way function together with session key, used for validate login function.

SOAP (simple object access protocol) is used for communication between two different running operating system (such as communication between Linux and windows 2000) using World Wide Web (WWW)'s Hypertext Transfer Language (HTTP) and Extensible Markup Language (XML) used as mechanism for information exchange between two different operating systems. Web protocols are installed which is used by all operating systems. SOAP protocol defines about encoding of HTTP header and XML file used for calling a remote program and passing of information. This describes the response of called program[4].

SOAP XML document consists of following elements:

- Optional header element consists of header information.
- Body element consists of response information
- Envelope element identifies XML document as a SOAP message.
- Fault element contains information about errors occurred during processing of message.

3. System Model

Shared authority based privacy-preserving authentication protocol (SAPA) used to addressing the privacy issues of cloud storage which is defined in existing work[5]. SAPA follows 3 steps for achieving privacy issues. 1) SAPA works based upon request matching mechanism such as data authentication, privacy, forward security and data anonymity; 2) attribute based access control is used for verification of user who are authenticate to access the data fields; 3) data sharing among multiple users is provided through proxy-re encryption[6]. Universal compensability

model having correct design which attractive for multi-user collaborative cloud application. Risk is arising due to scanning of code. Other authentication system is text based password login system, cryptography based login system such as digital signatures, Biometric based login system etc, that generates risk as, forget of password didn't allow user to access within the website. So users are denied from accessing the required data. Existing security system mainly focuses on only authentication to avoid illegal use of user's data. It does not consider about privacy issue during sharing of cloud server to request other user for sharing. Reusing of passwords cause domino effect, if adversary compromised one password they are able to access more websites. Hackers apply algorithm and random-key function/method for getting user passwords.

4. Proposed System

Two types of adversaries present is cloud space for access user's data, 1) stored pre computed data in cloud space, and 2) stored different data at different time slots in cloud space. Objective of Duos system is to free the users for remembering passwords for authentication given in conventional system. Unlike authentication[7] given by user in normal system Duos involves generation of Context Token using SOAP protocol used for communication between two different mediums using building communication channel, In SOAP protocol verification is take place based upon LTP and STP using mobile application. Through the mobile application LTP and STP is verified and induce communication among the Duos system. Authentication and verification is challenging job.

Advantages

- Protection of mobile phones Phishing protection
- Avoidance of domino effect
- Provide secure transaction of data Anti-malware
- Secure registration and recovery process

5. Architecture Description

If a person tries to access different platform, then user first registers in mobile application for authentication of that user. Mobile application generates long time password for user. It generates short time password for temporary creation of session. From that password generate from mobile application user can access web application using cloud or GPRS[8]. In web application user can register using long time password generate by mobile application for longer session. For temporary creation session can login to system using short time password. Figure 1 describes the system Architecture of the proposed solution. Figure 2 describes about control flow of system. It ensures login of users, after user details are provided then login success messages are passed to user. Registration performed in both mobile system and webpage[9]. In mobile device long term password should submit by user. SOAP protocol verifies user details, and then login process is provided in mobile. In web page LTP is entered and submitted. Ensures successful login for accessing application. In failure opened and submitted recovery process finds whether information stored in permanent database and user details are same. If details same recovery process is performed. Figure 3 describes the overall view of this work. It is the pictorial representation of the entire work which is to be carried out. This architecture consists of five modules. Each module is listed separately and described in detail in the later part. Initially a user needs to install OPass application in her/his mobile device. In Registration phase, user has to register their details in website as well as mobile. After registering in website, those details will be moved to temporary table in server's database. The server sends two different OTP to mobile through SMS (here we choose Way to SMS as a gateway). The next webpage which will ask these two OTPs (verification codes) to fill. Once giving these correct OTPs, our details will be moved to permanent database. Meanwhile, we have to complete the registration in mobile device also. In this similar way we need to finish Login to prove that you are an authenticated user. If a user forgets his password or miss his mobile, the recovery phase will be taken place. The architecture given below shows the detailed description and a pictorial representation of the work.

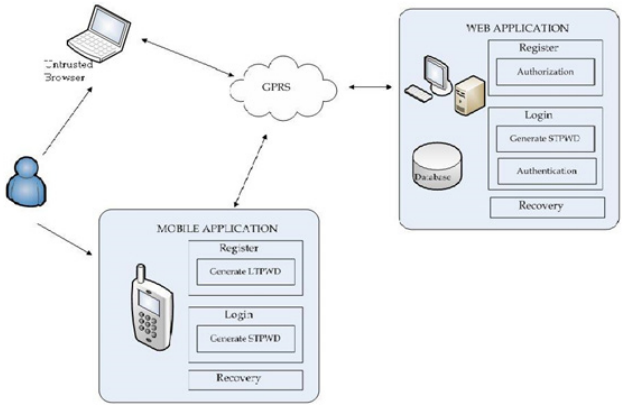

Figure 1. Architecture.

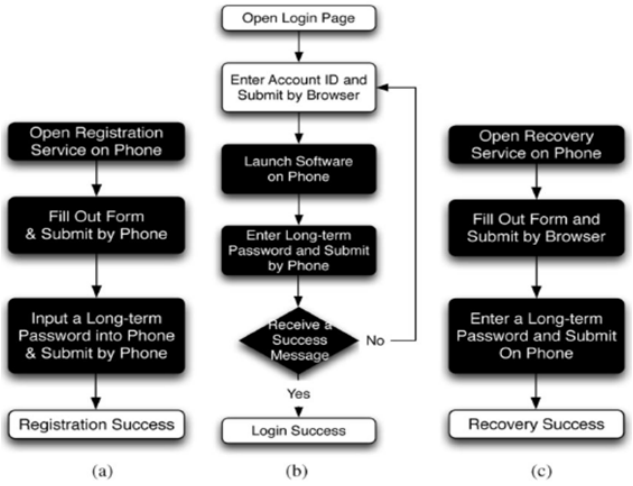

Figure 2. Dataflow diagram.

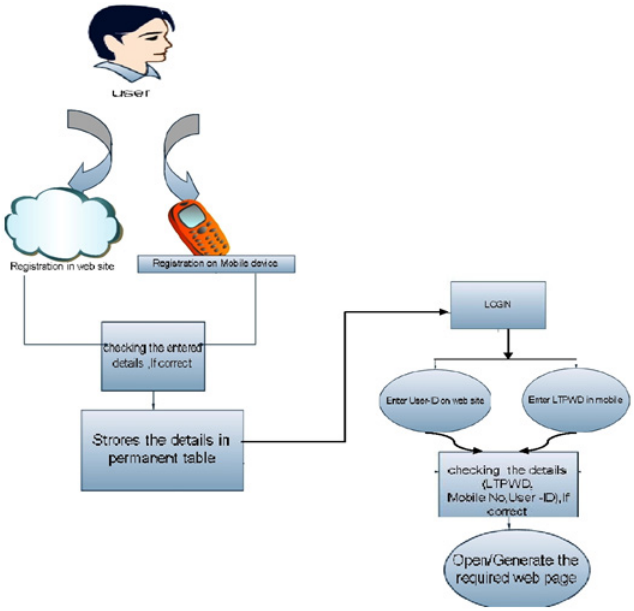

Figure 3. Overall Proposed System.

6. Implementation

Modules Description

- Registration On Website
- Registration on Mobile Phone
- Login
- Recovery
- Application maintenance

6.1 Registration on Website

6.1.1 User Authentication

Online customers access data based on online payment. In proposed system, user interactions performed by login process, registration, communication, online payments and transaction process. User details are stored in back end database and cloud systems. Computer login process is controlled by individual access of authenticate data given right to access data for authenticate person by identifying and verification of users based upon their credentials. When user A access data can logoff or logout from system is connection is no longer needed. One can logout then for another session is established based on LTP and STP process. It involves following steps,

Steps:

- Open the website that we wanted for web services.
- New user can login to system by entering their personal information.
- Open registration from for new user accessing authenticate data fill their details and submit it.
- For temporary user's data about the users are stored in temporary database.
- It will be stored on the Temporary table in server's database.

Registration process is performed using unique key generation algorithm.

All variables are unsigned 32 bit and wrap modulo 2^32 when calculating variant [64] s, K

//s specifies the per-round shift amounts

s [0..15] := { 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22 }

s [16..31] := { 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20 }

6.1.2 Mobile Email Validation and Verification

- The server will generate Mobile and E-mail verification codes (OTP-One Time Passwords).
- These verification codes (OTPs) will be sent to the corresponding Mobile (through SMS) and Mail-ID.
- After getting these verification codes (OTPs), we should enter these codes in another webpage when registration which is called as OTP verification.
- Waiting for Accessing page will be in processing mode.

6.2 Registration in Mobile Device

In this phase we need to install Opass application in our Android mobile. When we go for registration it will generate a signup page.

Steps:

- User has to fill up the registration form by giving user's details.

- AES algorithm is used for encryption and decryption process[10].

Encrypt (byte in [16], byte out [16], key_arrayround_key [Nr+1])
begin
byte state[16];
state = in;
AddRoundKey (state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes (state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRoundKey (state, round_key[Nr]);
End

6.2.1 Generation of Long Term Password

- Now, the mobile device will generate a Long Term PWD for further successful logins[11].
- This Long Term PWD is used for secured mobile web authentication.
- This will be stored in an encrypted form in our database.

6.2.2 OTP Encryption

The main security for our system is one-time password authentication. Triple DES algorithm is used for one-time password encryption.

6.2.3 OTP Decryption

The One-time password decryption process done in android application using same Treble DES algorithm and same key of encryption.

6.3 Login

In this phase, user has to give the user-ID in Login webpage and user has to give LongTermPWD in their mobile device also. Meanwhile, another webpage called Loading will be opened. From these two logins on website and mobile device it will verify the details such as User-ID, LongTermPWD and mobile number. After this verification, the corresponding required webpage will be opened for access.

6.4 Recovery

This phase is taken places when two cases are occurred. First, if the user misses the mobile, which means that, if that particular mobile number cannot be used for the mean while, he cannot access through the old mobile number. Second, if the user forgets the LongTermPWD, he cannot access the mobile device. Different web pages will be opened, for both the above cases. By selecting and giving the necessary information that we currently have, in the particular WebPages, we can get our details related to our account back successfully. This is done successively by using LongTermPWD which is stored in the encrypted form in server's database.

6.5 Application Implementation

Final module of our project as application maintenance. That is, to maintain our application with more and more security. Such as PIN code evaluation and OPASS verification. In this application we use Mail Services. In this mail services we perform two operations. Such a read a mail from server and compose mail.

7. Conclusion

The secured web authentication has been done successfully by using two types of registration which are named as Registration on Website and on the Mobile device. The scalability and efficiency for secured web authentication using a personal device has been found out to be very essential. The Long Term PWD has been generated for secured web authentication which means that secured and successful Logins. The OTPs will be generated to eliminate the problems of PWD Reuse and Weak PWDs. The Long Term PWD will be stored in encrypted form for security purpose. Login and Application Maintenance should be implemented in the next phase which distributes the work among many sub modules by using web and the mobile device.

8. References

1. Ruj S, Stojmenovic M, Nayak A. Decentralized access control with anonymous authentication for securing data in clouds. IEEE Transactions on Parallel and Distributed System. 2014; 25(2):384–94.
2. Barsoum A, Hasan A. Enabling dynamic data and indirect mutual trust for cloud computing storage systems. IEEE

Transactions on Parallel and Distributed Systems. 2013; 24(12):2375–85.
3. Bellovin SM, Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In Proceedings IEEE Computer Society Symposium on Research in Security and Privacy. Oakland: CA; 1992. p. 72–84.
4. Rangarajan A, Rajasekaran S, Kumaran P. Incorporation of security features in agonistic protocol in the web search. Middle-East Journal of Scientific Research (MEJSR). 2015; 23(9):2051–9.
5. Nabeel M, Shang N, Bertino E. Privacy preserving + policy based content sharing in public clouds. IEEE Transaction on Knowledge and Data Engineering. 2013; 25(11):2602–14.
6. Wang H. Proxy provable data possession in public clouds. IEEE Transactions On Services Computing. 2012; 6(4):551–59.
7. Wang RC, Juang WS, Lei CL. User authentication scheme with privacy-preservation for multi-server environment. IEEE Communications Letters. 2009; 13(2):157–9.
8. Park J-K, Lee H-S, Kim S-J, Park J-P. A study on secure authentication system using integrated user authentication service. Indian Journal of Science and Technology. 2015 Sep; 8(23):1–6. DOI: 10.17485/ijst/2015/v8i23/79284
9. Kumar DG, Pasupathi K. Security in cloud for multi-owner using anonymous ID. International Journal of Engineering and Technical Research. 2013; 1(1):383–7
10. National Institute of Standards and Technology (NIST), U.S Department of Commerce. FIPS PUB 197, Advanced Encryption Standard. Available from: http://csrc.nist.gov/publications/fips/fips197/ fips-197.pdf.
11. Kumaran P, Rajasekaran S. Mobile based user authentication for guaranteed password security with key generation. International Journal of Computational Linguistics and Natural Language Processing. 2013 Apr; II(I):309–14.