Secure Server Login by Using Third Party and Chaotic System

**Firas A Abdulatif**, **Maan zuhiar**

1Department of Computer Sciences, College of Education for pure science, Baghdad University, Baghdad, Iraq.
2Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate, Iraq

**Abstract.** Server is popular among all companies and it used by most of them but due to the security threat on the server make this companies are concerned when using it so that in this paper we will design a secure system based on one time password and third parity authentication (smart phone). The proposed system make security to the login process of server by using one time password to authenticate person how have permission to login and third parity device (smart phone) as other level of security.

**Keywords.** Server security; one time password; third parity.

1. Introduction

Medium-to-large companies are using the server where computing requirements are high. It is depends on the client server model There are several services provided by the server and the most important one is storage [1].

Many online based application used password to authenticate a particular person from the login system. A password is a string of characters used during authentication process to verify user identity. Passwords can have letters, numbers and special characters and can vary in length. There are two type of password static password and one time password, most companies still use one single static passwords due it is easy to remember. But, when there are more than one systems have different passwords it may be hard to remember. Static passwords have many defects such as easy to decipher and are usually only letters and are often short and are based on topics close to user birthdays and child names. To overcome these defects a new method is discovered known one time password (OTP) [2]. So far OTP is the most effective way to provide secure login to the system. In one time password the password will be generated on the server side and after that will send to the client. This type of password, will be valid for only one login session and even if an attacker succeeds in acquiring an one time password, he may not be able to predict the next one time password [3].
2. Security challenges of server
Server has many disadvantage one of this loss of physical control such that users and tenants cannot access their data.
1- Malicious Insiders: granting powers to the current or former employee or partner to access user data and misuse this access in a way that negatively affects the confidentiality, integrity of data [4].
2- Data Leakage: data leakage is the accidental or unintentional distribution of private or sensitive data to an unauthorized entity. Data leakage poses a serious issue for companies as the number of incidents and the cost to those experiencing them continue to increase
3- SQL injection: this type of attack works on inserting SQL orders that destroy that database [5].
4- Brute force attack: this type of attack try to get user information such as username and password by using automated program to generate a large number of consecutive guesses [6].
5- Denial of service: The denial-of-service attack block legal users from accessing their data. The denial-of-service attack can alter the encryption key or slow the system to block users from using the service by trying to use the wrong password more than once. Therefore cloud service providers should develop a mechanism so that the attackers cannot impact on the services provide by the cloud [6, 7].
6- Account or Service Hijacking: Is a ways of fraud, phishing and vulnerability exploration moreover password credentials used in distributed methods give breadth to this problem. The anxiety with abduction of accounts was the goal of many cloud service providers already consolidated in the market, such as Amazon.
7- Cross-site scripting (XSS) attack: this type of attack commonly found in web applications. It is makes it possible for attackers to inject malicious code into victim’s web browser and steal the victim’s credentials [8].
8- Insecure Interfaces and Application Programing Interface (API): There are group of APIs or software interfaces provided for users to control and interact with services provided by the server. To protect against accidental and malicious attempts to circumvent, the interfaces must be designed in a safe manner. Organizations and third parties often build upon these interfaces to offer value-added services to their customers [9].

3. Proposed system
The proposed system provide security of data stored on server by using third party authentication and one time password. Using smart phones as a third party because they are used by the owner only and stay with him wherever he are. Using one time password for authentication. This one time password will be usable for one time to prevent unauthorized people from access and manipulate user’s data that stored on the server and expiry after half hour until if not used. This one-time passwords will be send to the third party to make sure it only reaches to the authorized person. ‘Figure 1’ explain the general structure of the propose system.
The proposed system is implemented on a remote server and uses Firebase Cloud Messaging (FCM) API to send the one-time password from the server to the user. To use the services provided by the server, the first user must register on the server by entering the username and static password and then register their smartphone as a third party to complete the registration process; an Android mobile application design to confirm the account of the user on the server and send/receive notifications from the server. To complete the smartphone registration process, the user will enter the same username and static password previously registered in the server. A phone application designed for this purpose will be used to search for the server database. When the user name and password are found, the server will send a request to the Firebase Cloud Messaging API (application programming interface) to ask for registration, and then the FCM will respond with a message of a unique string (token) generated for a particular user's smartphone. This token will be stored in the server database according to the user name and password to use it when sending or receiving notifications on the mobile. After the token is stored in the server database, the user completes the process of registration and can log in to the server at any time and from anywhere by using their information. 'Figure 2' explains the steps of the registration process.
After complete the process of registering his account on the server and the corresponding third party device, now can he login to server. He must enter the previously registered user name and if valid system will generate the one time password using chaotic system. This chaotic system is non liner equation called sin map chaotic equation that used to generate random number that cannot be predicted. The one-time password will be expired after half an hour or one use. The sin map is one of the important equations that used in security. It shown 'as in equation (1)'.

$$X_{n+1} = r \sin (\pi X_n)$$  \hspace{1cm} (1)
This is sin map chaotic equation. The one time password that generated from the chaotic system will be send to the user on mobile as shown in ‘figure 3’ then the user can used this received password on mobile application with the static password that used in the registration as a password. User input the received password in mobile and after that go to the server and input the static password to login the server and using server storage to store his data, browses his file that stored on the server storage and downloading any file, ‘figure 4’ explain the login operation.

![One time password that user received on mobile.](image)

**Figure 3.** One time password that user received on mobile.
Figure 4. Login process to server storage

When the user login to the server, he can use all the facilities provided by the system such as browse any file that are pre-stored in the server and can download any file and read it and can upload any file to server. The mobile application designed to receive the one-time password that send from server. It is programed by using Java programing languish.
4. Conclusion

Servers offer valuable services but due to security challenges makes both organizations and people are concerned so that a system has been proposed to address these security threat. The proposed system provides a secure way to use the server services by using one-time password, third party authentication (smart phone). This one time password will be valid only for one time and will be expire after half an hour and the using the third party device (smart phone) to receive the one time password. The proposed system overcomes the brute force attack and denial of service attack by following the method in case if the user entered the password wrong for more than four times the proposal will offer the user groups of image to select from each group the image have number equal to the password that received on the mobile in the login step. The propose system handle many type of attack such as SQL injection attack and many other type of attack.

Reference

[1] F Abidi and V Singh 2013 Cloud Servers vs. Dedicated Servers – A Survey Conf. MOOC. IEEE pp 1–5
[2] M E K, M C A, M Phil, J M Sc, M Phil and D Ph 2013 Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology Int. J. Eng. Sci. 2 10 pp 14–17
[3] S Srivastava On The Generation of Alphanumeric One Time Passwords i pp 1–3
[4] Cloud Security Alliance Top Threats to Cloud Computing Security 2010 pp 1–14
[5] C M R Da Silva, J L C Da Silva, R B Rodrigues, G M M Campos, L M Do Nascimento and V C Garcia 2013 Security threats in cloud computing models: Domains and proposals. IEEE Int. Conf. Cloud Comput CLOUD pp 383–389
[6] F A Abdulatif 2017 Cloud Security Issues and Challenges : Important Points to Move towards Cloud Storage International 6 8 pp 2105–2112
[7] A Hendre and K P Joshi 2015 A Semantic Approach to Cloud Security and Compliance Proc. IEEE 8th Int. Conf. Cloud Comput. CLOUD pp 1081–1084
[8] A Kie, P J Guo and M D Ernst Automatic Creation of SQL Injection and Cross-Site Scripting Attacks
[9] F A A Latef 2012 Web Ranking and Rating Server Using Web Service pp 411–424