

Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography

Niharika Gupta¹ and Rama Rani²

¹Research Scholar, Department of Computer Science & Engineering, DAV University, Jalandhar, Punjab, India

²Assistant Professor, Department of Computer Science & Engineering, DAV University, Jalandhar, Punjab, India

Abstract— *As a high-speed internet foundation is being developed and people are informationized, most of the tasks are engaged in internet field so there is a risk that any private data like personal information or applications for managing money can be wiretapped or eavesdropped. The consolidation of One Time Passwords (OTPs) and Hash encryption algorithms are used to evolve a more secured password-protected web sites and data storage systems. The new outlined scheme had higher security, small system overhead and is easy to implement.*

Keywords—*multifactor authentication; one time passwords; cryptography; hashing*

I. INTRODUCTION

Authentication based on cryptographic techniques is a great challenge research area in client-server system. Password authentication is one of the simplest and the most common authentication mechanism over an insecure channel. It provides the legal users to use the resources of the client-server systems. Many researchers proposed several password authentication schemes for secure registration and login process. However, the current Internet environment is vulnerable to various attacks such as replay attack, guessing attack, modification attack, and stolen-verifier attack. In 1981, Lamport proposed a onetime password authentication scheme using cryptographic hash functions [11]. The purpose of a OTP is to make it more difficult to gain unauthorized access to restricted resources. Traditionally the static passwords can be more easily accessed by an unauthorized intruder given sufficient attempts and time. This risk can be greatly reduced by constantly altering the password. Dynamic passwords or one-time passwords play an important role in authentication. As the existing one-time password schemes use only encryption algorithm and hash function in registration process, the password is still vulnerable. Therefore, the impersonators may pretend like the authorized users to get the services. This ticket-based onetime password authentication system is more secure than the existing authentication schemes by preventing from guessing attack and replay attack. It is essential property to get the mutual authentication in the registration phase. The ticket supports the server to authenticate the user and the signature response of server also supports the user to authenticate the server. In this proposed scheme, there is no password transmission in registration phase by the

use of ticket. The main responsibility of the trusted third party, RC is to generate Ticket to user. The user must use Ticket instead of password in registration process to get the strong confidentiality.

A. MULTIFACTOR AUTHENTICATION

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories[6] :

i. Knowledge factors ("things only the user knows"), such as passwords Knowledge factors ("something only the user knows") are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate.

- A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many multi-factor authentication techniques rely on password as one factor of authentication.
- A personal identification number (PIN) is a secret numeric password and is typically used in ATMs. Credit and ATM cards do not contain the PIN on the magnetic stripe. This aligns with the principle that the PIN is not part of "something the user has" for this use.

ii. possession factors ("things only the user has"), such as ATM cards Possession factors ("something only the user has") have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems.

- Mobile phones
- One-time pads

iii. inherence factors ("things only the user is"), such as biometrics Inherence factors are "something only the user is". Biometric authentication also satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault.

B. CRYPTOGRAPHY

Cryptography[5] or cryptology is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that block adversaries; various aspects in information security such as data confidentiality, data integrity, authentication, and nonrepudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted

persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

II. SECURITY ISSUES IN CLOUD COMPUTING

The security issues [1, 9] in cloud computing can be categorized into the following three classes:

- Conventional security issues
- Availability issues
- Third party data control-related issues

A. *Conventional Security Issues:* These security issues involve computer and network attacks or intrusions that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their safety measures and security processes are full-grown and tested than those of the usual company. Concerns in this category include VM-level attacks, Cloud service providers' vulnerabilities, Phishing cloud provider, expanded network attack surface, Authentication and authorization, Forensics in the cloud.

B. *Availability issues:* These concerns center on data and critical applications being available. Well-publicized incidents of cloud outages include Gmail's one-day outage in mid-October 2008 (Extended Gmail Outage), Amazon S3's over seven-hour downtime on July 20, 2008 (Amazon S3 Availability Event, 2008), and FlexiScale's 18-17 hour outage on October 31, 2008 (Flexiscale Outage). Maintaining the uptime, preventing denial of service attacks (especially at the single-points-of-failure) and ensuring robustness of computational integrity (i.e. the cloud provider is authentically running and giving applicable outcome) are some of the major issues in this category of threats.

C. *Third Party Data Control:* The legal implications of applications and data being held by a third party are complex and not well understood. There is also a potential lack of control and precision when a third party holds the data. Part of the publicity of cloud computing is that the cloud can be implementation-independent, but in reality, regulatory compliance requires transparency into the cloud. Various data privacy and security issues are prompting several companies to build clouds to avoid these issues and yet maintain some of the benefits of cloud computing. However, concerns like Due diligence, Auditability, Contractual obligations, Cloud provider espionage, Cloud provider espionage, Transitive nature of contracts need to be addressed properly.

III. RELATED WORK

A one-time password (OTP) [14] is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional or static password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows.

The original specification of the algorithm was published in 1993 as the Secure Hash Standard, FIPS PUB 180, by U.S. government standards agency NIST (National Institute of Standards and Technology). This version is now often referred to as SHA-0. It was withdrawn by NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly referred to as SHA-1. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function; this was done, according to NSA, to correct a flaw in the original algorithm which reduced its cryptographic security. However, NSA did not provide any further explanation or identify the flaw that was corrected. Weaknesses have subsequently been reported in both SHA-0 and SHA-1. SHA-1 appears to provide greater resistance to attacks[citation needed], supporting the NSA's assertion that the change increased the security.

Authentication is the key for information security for the reason that if the authentication mechanism is compromised, the rest of the security measures are by passed as well [4]. One-time password (OTP) schemes, where each password is used only once, offer available alternative or a supplement to traditional password schemes [4]. The approaches [3], [6] designed password authentication schemes to overcome guessing attack and achieve mutual authentication. Lamport [11] introduced the first one-time password authentication scheme. This initial work has been followed by a number of subsequent improvements [6-9]. The Lamport algorithm for generating and applying onetime passwords (OTPs) is a simple solution that provides great value in the right context. Not only can the Lamport OTP scheme provide effective security for distributed client/service interactions, but it's also simple to comprehend and implement.

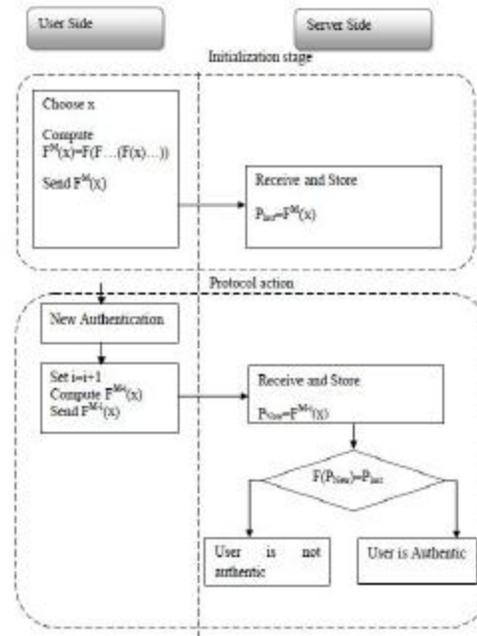


Figure 1 Lamport One Time Password scheme

The mechanism of Lamport's method consists of two phases: the registration phase and the authentication phase. The registration process is performed only once, and the authentication procedure is executed every time the user logs in to the system. These two phases are described below.

A. Registration Phase of Lamport's Algorithm

- a. The user inputs own password and calculates the verifier for the 1st authentication session.
- b. The user sends the registration data to the server for subsequent authentication.
- c. The server stores the verifier for subsequent authentication.

B. Authentication Phase of Lamport's Protocol

- a. The user inputs own password and calculates authentication data for the i th authentication session.
- b. The user sends the authentication data to be authenticated by the server.
- c. The server authenticates the user with the stored verifier and the transmission data.
- d. The server stores the verifier for the next authentication session.

In earlier mechanisms only one type of hashing is used to protect the password or there is no protection at all. The single hashing mechanism can be easily broken using reverse engineering methods and several instances have been found where cryptographic hash functions have been

attacked.

IV. OUR APPROACH

This research uses multiple hashing encryption so that password is not decrypted using Reverse Engineering. Also it uses Multiple Encryption and the sequence is changed every time.

A. PASSWORD PROTECTION USING MULTIPLE ENCRYPTION

Table 1 Representation of various hashing algorithms

Algorithm	Sequence No
SHA1	1
MD5	2
SHA512	3

Now to encrypt our Password We Will Use the Following Mechanism which will change on time to time basis:

Sequence 123

Input Password>> SHA1 >> Hashed Output >> MD5 >>
Hashed Output >>SHA512>> Hashed Output

Sequence 213

Input Password>>MD5 >> Hashed Output >> SHA1>>
Hashed Output >>SHA512>> Hashed Output

Sequence 312

Input Password>>SHA512>> Hashed Output >> SHA1>>
Hashed Output >>SHA1 >> Hashed Output

Using the above mechanism the Password will be hashed in a different way and will be less prone to reverse engineering. A different key is used every time for each user so that it adds more to the security.

B. DOS ATTACK AND BRUTE FORCE ATTACK PREVENTION:

Denial of service (DoS) attacks have become a major threat to current computer networks. A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. It consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. With respect to availability, hackers continue to focus on preventing access to online services and systems by crashing a service through exploitation or by flooding services to the point that the resource is no longer accessible. These types of denial-ofservice or DoS attacks can come directly from one IP address or from a multitude of computers located in disparate locations, known as distributed denial-of-service (DDoS) attacks.

In this paper prevention of DOS Attack is also done. Based on the Dynamic IP Restrictions System which provides Website Administrator a configurable module that helps mitigate or block Denial of Service Attacks or cracking of passwords through Brute-force by temporarily blocking Internet Protocol (IP) addresses of HTTP clients who follow a pattern that could be conducive to one of such attacks. This module can be configured such that the analysis and blocking could be done at the Web Server or the Web Site level.

Reduce the chances of a Denial of Service attack by dynamically blocking requests from malicious IP addresses Dynamic IP Restrictions for IIS allows you to reduce the probabilities of your Web Server being subject to a Denial of Service attack by inspecting the source IP of the requests and identifying patterns that could signal an attack. When an attack pattern is detected, the module will place the offending IP in a temporary deny list and will avoid responding to the requests for a predetermined amount of time.

Dynamically blocking of requests from IP address based on either of the following criteria:

- The number of concurrent requests.
- The number of requests over a period of time.
- Type of Browser Agent Being Used
- Country/Area based Request.

C. PREVENT PHISHING ATTACKS USING IMAGE VERIFICATION:

Image Seal is an Image that has been uploaded by user from his computer at the time of registration. Then at the time of login the same image along with two more images is shown to the user from them he has to select the image uploaded by him. This serves two purposes one is adding an alternative authentication mechanism second is that it prevents phishing attacks.

Phishing has been major threat to individual's account security. But to prevent phishing from happening we intend to show user a set of images out of which one image is uploaded from users Computer at the time of user Registration. If the user is unable to view the image which he had uploaded, that gives an impression of phishing site and user will get alert.

D. SQL INJECTION PREVENTION:

The module scans the user input for any possible SQL injections and thwarts any attempt by cleansing the user input.

E. IMPLEMENTING SMS BASED OTP APPROACH:

One Time Password is a Random 6 Digit Number that changes every time, when ever user logs on to the system and performs some transaction. The Concept has been implemented in a such a way that it adds high level of security to our Application. The user when he logs on the Online Website from his Mobile or Computer gets a screen that just prompts him to enter his username, once he enters the username the user is redirected to another screen where along with his Password is prompted to enter the One Time Password.

The OTP meanwhile has been delivered on to the users registered mobile number that user had provided at the time of opening the account with the bank. The OTP is valid only time every next time user logs in he needs to provide an new OTP that the user would have received at that particular moment of time. Thus this OTP becomes the most secure way to implement security in Net and Mobile banking applications as even if the password of a customer is compromised but using this OTP he is secure in the sense that the other password that he/she need to log in or perform a transaction will only be sent on to his mobile phone.

F. CLOUD STORAGE:

This enables users to store their files and folders in a secured mechanism on the cloud.

V. CONCLUSION

Multi-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as an application and the other of which is typically something memorized, such as a security code or password. In this context, the two factors involved are sometimes spoken of as something you have and something you know. The need for encrypting Passwords comes from fact that we need to protect passwords of users . The users then will be prevented from attacks like brute force attack, phishing, Distributed Denial of Service (DDOS) through password encryption and multifactor authentication(via One Time Password and image security at registration).

ACKNOWLEDGMENT

I would like to place on record my deep sense of gratitude to Er. Rama Rani, Dept. of CSE, DAV UNIVERSITY, Jalandhar, India for her generous guidance, help and useful suggestions. I express my sincere gratitude to my thesis guide for her stimulating guidance, continuous encouragement and supervision throughout the course of present work. Also, I am extremely thankful to Mr. Naresh Sahejpal, Dean Academics, DAV University, Jalandhar, for providing me infrastructural facilities to work in, without which this work would not have been possible.

REFERENCES

- [1] Anne Boehm and Ged Mead, Murach's ADO.NET 4 Database Programming with VB 2010,2011.
- [2] Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Sugata Sanyal and Svein Knapskog: A Multifactor Security Protocol For Wireless Payment- Secure Web Authentication using Mobile Devices, IADIS International Conference, Applied Computing 2007, Salamanca, Spain, pp. 160-167, February 2007.
- [3] Christoffer Haglund, "Two-factor Authentication With a Mobile Phone", Fox Technologies, Uppsala Department of Information Technology, Lund University, 7th November 2007.
- [4] Christoffer Haglund, "Two-factor Authentication With a Mobile Phone", Fox Technologies, Uppsala Department of Information Technology, Lund University, 7th November 2007.
- [5] Cryptography, <http://en.wikipedia.org/wiki/cryptography>
- [6] D. de Borde, "Two-Factor Authentication," Siemens Enterprise Communications UK-Security Solutions, whitepaper, 2008.

- [7] Deepa Panse, P. Haritha, "Multi-factor Authentication in Cloud Computing for Data Storage Security", International Journal of Advanced Research in Computer Science and Software Engineering, 2014
- [8] Dr.D.S.Rao, Gurleen Kour, "One Time Password Security through Cryptography For Mobile Banking", IJCTA, Vol 2 (5), 2011.
- [9] Fadi Aloul, Syed Zahidi, "Two Factor Authentication Using MobilePhones," in Proceedings Proceedings of the IEEE International Conference on Computer Systems and Applications, pg. 641-644, 2009.
- [10] Jesse Liberty, Dan Maharry and Dan Hurwitz, Programming ASP.NET 3.5,O'Reilly Media, November 3, 2008.
- [11] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, pp. 770-772, 1981.
- [12] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan, OTP-Based Two-Factor Authentication Using Mobile Phones, Eighth International Conference on Information Technology, IEEE, 2011.
- [13] Mohammad Mannan, P. C. Van Oorschot, "Security and Usability: The Gap in Real-World Online Banking", NSPW'07, North Conway, NH, USA, Sep. 18-21, 2007.
- [14] One Time Password, http://en.wikipedia.org/wiki/One-time_password.
- [15] Sagar Acharya, Apoorva Polawar, P.Y.Pawar, "Two Factor Authentication Using Smartphone Generated One Time Password", IOSR Journal of Computer Engineering (IOSR-JCE), 2013.
- [16] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009.
- [17] Sugata Sanyal, Ayu Tiwari and Sudip Sanyal, A Multifactor Secure Authentication System For Wireless Payment, 2012.
- [18] Web and Desktop Applications in ADO.NET and ASP.NET, Prentice Hall, September 13, 2003.
- [19] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011.
- [20] Young Sil Lee, Hyotaek Lim, "Online banking authentication system using mobile-OTP with QR-code", Computer Sciences and Convergence Information Technology (ICCIT), IEEE 5th International Conference, 2010.