ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Review on Password Storage in Cloud Environments

Kratika Ingle, Prof. Bharat Solanki, Prof. Nitin Shukla, Dr. Samar Upadhyay

Research Scholar, Dept. of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, India

Dept. of Master of Computer Application, Shri Ram Institute of Technology, Jabalpur, India

HOD, Dept. of Master of Computer Application, Shri Ram Institute of Technology, Jabalpur, India

HOD, Government Engineering College, Jabalpur, India

ABSTRACT: There various conventional technique are obtainable for authentication. But these technique have disadvantage. To overcome this disadvantages multi - factor authentication is used for authentication. In multi - factor authentication more than one authentication method is combined to perform authentication. One form of authentication that is mostly used with other forms of authentication for multifactor authentication is one time password (OTP). One time password is valid for one login session. But in cloud environment, the trusted third party is not always reliable for sharing and storing login information. Hashing algorithms are commonly used to convert passwords into hashes which theoretically cannot be deciphered. This paper analyses the security risks of the hashing algorithm MD5 in password storage and discusses different solutions, such as salts and iterative hash the login information. There are some approaches to using MD5 in password storage by using external information, a calculated salt and a random key to encrypt the password before the MD5 calculation.

KEYWORDS: component; MD5, Salt key, Cloud Computing, OTP

I. INTRODUCTION

In cloud computing, 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 [1]. 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.

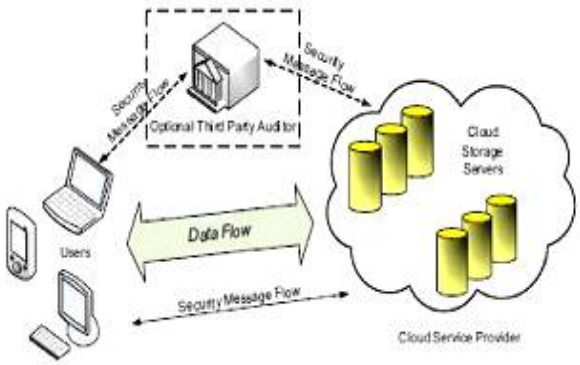

Figure 1. Cloud data storage architecture

With the advent of computer technology, it became more productive to store information in databases instead of storing in paper documents. Web applications, needing user authentication, typically validate the input passwords by comparing them to the real passwords, which are commonly stored in the company's private databases. If the database

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

and hence these passwords were to become compromised, the attackers would have unlimited access to these users' personal. Nowadays, databases use a hash algorithm to secure the stored passwords but there are still security breaches.

II. INFRASTRUCTURE SECURITY ISSUES

Cloud suppliers provide security-related services to a good vary of client types; the security equipped to the foremost demanding clients is additionally created on the market to those with the smallest amount stringent necessities. Whereas Infrastructure Security Solutions and product are often simply deployed, they need to a part of an entire and secure design to be effective.

Securing Data-Storage - In Cloud computing environment data protection as the most important security issue. In this issue, it concerns include the way in which data is accessed and stored, audit requirements, compliance notification requirements , issues involving the cost of data breaches, and damage to brand value. In the cloud storage infrastructure, regulated and sensitive data needs to be properly segregated. In the service provider's data centre, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact. Software encryption is less secure and slower because the encryption key can be copied off the machine without detection.

Network and Server - Server-Side Protection: Virtual servers and applications, very like their non-virtual counterparts, have to be compelled to be secured in IaaS clouds, each physically and logically. Example, virtual firewalls are often used to isolate teams of virtual machines from different hosted teams, like production systems from development systems or development systems from different cloud-resident systems. Rigorously managing virtual machine pictures is additionally vital to avoid accidentally deploying pictures underneath development or containing vulnerabilities. Preventing holes or leaks between the composed infrastructures could be a major concern with hybrid clouds, as a result of will increase in complexity and diffusion of responsibilities. The supply of the hybrid cloud, computed because the product of the supply levels for the part clouds, also can be a concern; if the % availability of anyone part drops, the availability suffers proportionately. In cloud environment, purchasers want to form certain that every one tenant domains are properly isolated that no probability exists for data or transactions to leak from one tenant domain into successive.

III. END USER SECURITY ISSUES

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found.

Browser Security - In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform in-dependent client software useful for all users throughout the world. This can be categorized into different types: Software as- a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication.

Authentication - In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF-MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. Other such risks which are marked as high risk in cloud

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

security are

Loss of Governance: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.

Data Protection: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g. between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g.,SAS70 certification. Data flowing from the Internet is filled with mal ware and packets intended to lure users into unknowing participation in criminal activities.

IV. SECURE WEB ACCESS

Secure web access provides the following services to the users:
i. Authentication service: The web server is configured to present a notarized credential called "certificates" to address identity concerns.
ii. Encryption service: The web server and web client negotiate a session key for encrypting the packet data exchanged among them, ensuring the confidentiality of the information.
iii. Option: mutual authentication service: The web server is configured to ask browsers to prompt the user to select a personal certificate, and then check on the authenticity of the signed personal certificate and against an access control ("password") list.

The mutual authentication service enables the web server to verify users without them presenting the login/password. Secure access to a web server can be enhanced by requiring a client to present its digital certificate. Certificate is signed by a CA: The CA takes all the fields of the certificate except the last field and generates the message digest (hash) typically using MD5 and SHA. CA then encrypts (also called signs) the message digest (256 bits if MD5 is used) using CA's private key. The resulting encrypted/signed message digest is called signature. The signature was filled in the last field of the certificate.

V. HASH FUNCTION

A hash function is a one-way encryption function that takes a variable-size input plaintext m and generates a fixed-size hash output. It is computationally hard to decipher the hash and any attempt to crack it is practically infeasible. A “secure” hash function should be able to resist pre-image attacks and collision attacks. Due to the pigeonhole principle and birthday paradox, there will be some inputs that will produce the same hash result. The output length is of fixed size 128 bits, making a total of 2128 possible output hash values. This value, as big as it may seem, is not infinite, hence resulting in collisions.

A. MD5 algorithm

MD5 (Message Digest Algorithm 5) was designed by Ron Rivest in 1991. MD5 processes a variable-length message into a fixed-length output of 128 bits. MD5 is a popular hash function. It works on blocks of 512-bits, and processes each block through 4 rounds, where each round in turn processes 16 sub-blocks (each 32-bits). The 512-bit message is divided into 16 sub-blocks before processing. If a message block is not up to 512-bits, it is padded as shown in Fig. 1. A detailed explanation of the algorithm can be found at [1].

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

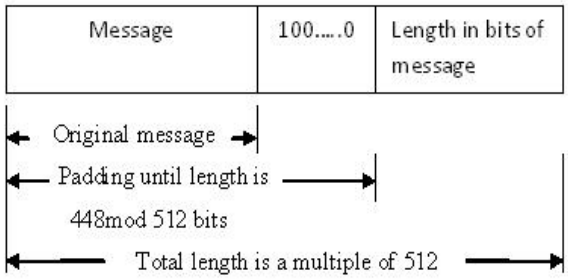

Figure 2. Length of message after padding (in bits)

VI. APPLICATION OF MD5 ALGORITHM IN PASSWORD

STORAGE SECURITY

It is highly insecure to store passwords in plaintext in the database. In order to increase the security of passwords, MD5 algorithms can be used to hash the original passwords and the hash values, instead of the plaintext are stored in the database. During authentication, the input password is also hashed by MD5 in a similar way, and the result hash value is compared with the hash value in the database for that particular user. MD5 algorithm is prone to two main types of attack: dictionary attacks and rainbow tables.

VI. COUNTERMEASURES RESEARCH

A. Information Entropy

Password strength is usually measured in terms of information entropy. In simple terms, the higher the information entropy, the stronger the password and hence the more difficult it is to crack it. A password of 6 characters would require only 2^6 attempts to exhaust all possibilities in a brute-force attack, while a password with 42 characters would need 2^{42} attempts. As can be seen, the longer the password and the larger the character set from which it is derived, the stronger the password. As best practice and preliminary requirement, the application should insist that the user uses a strong password during the registration process. Strong passwords run less risk of existing in dictionaries. Common simple passwords like “123456” have already been banned by Microsoft Hotmail.

B. Salting

One of the most common reasons to successful password cracking attacks like the one against LinkedIn was because they were using unsalted hashes. This makes it much easier for hackers to crack the system by using rainbow tables, especially given the fact that many users use very common, simple passwords and these similar passwords result in similar hashes. A salt is a secondary piece of information made of a string of characters which are appended to the plaintext and then hashed. Salting makes passwords more resistant to rainbow tables as the salted hashed password will have higher information entropy and hence much less likely to exist in pre-computed rainbow tables. Typically, a salt should be at least 48 bits. Salting can be implemented using the following ways:

1) Single salt for all passwords: Given that the salt is sufficiently long and complex, a standard rainbow table, cannot be used to decipher the salted hashes. However, two same passwords will still produce the same hash.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

2) Different random salt for each password and storing the salt within the database itself: If we use different salts for each password, two same passwords will have different hashes. The attacker has to generate different rainbow tables for each individual user, making it computationally harder for an attacker to crack the hashes. These salts can be stored in plaintext in the database. The purpose of the salt is not to be secret, but to be random enough to defeat the use of rainbow tables.

3) Use an existing column value: An existing column value like username can be used as salt. This solution is similar to the second solution discussed above. It defeats the use of a standard rainbow table, but a hacker might generate a rainbow table for a specific username, for example, "root" or "admin".

4) Use a variably located calculated salt: The salt location can be prefix (salt appended in front of password), infix (salt appended within the password) or postfix (salt appended at the end of the password). If the salt's location is made random, then cracking the passwords is made harder. For example, we can set the salt location to be equal to the password's length modulo 3. The salt can be calculated by using a random character sequence (stored in the database) and using other characters (embedded within the code). For example, the salt can be made to be a combination of the first two letters of username, random sequence of characters and the last 2 letters of username.

5) Use a variably located calculated salt including information outside the database and the application code: The hacker now has to break into the database and the server containing the application code. He also needs to obtain the additional information needed to crack the password.

C. Improvement on MD5 processing

The following methods can be used to improve the MD5 processing:

1) Improved hash function: The hash computation function is altered, for example using one of the following functions as shown in (1), (2) and (3):

hash = Hash (password + salt) (1)

hash = Hash (Hash (password) + salt) (2)

hash = Hash (password + salt + key) (3)

2) Iterative hashing: The password is hashed a number of times. MD5 is a fast hashing function, that is, it is computationally fast to calculate. Iterative hashing makes the calculation slower, hence computationally slower and more difficult to crack. The number of iterations can typically be made to be equal to 1000.

3) Key stretching: This makes a password more resistant to pre-computation attacks by making the attack workload bigger. Iterative hashing is used, where a weak key is fed into the hash algorithm and the output results in a stronger key. There are 3 key stretching methods depending on the input used for the iterative hashing:

a) Simple Key stretching: Only the key is hashed iteratively, as in (4). No salt is involved.

key = Hash (key) (4)

b) Password Key stretching: The password along with the key are both used in the loop.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

c) Salted Key Stretching: The key, password and salt are used in the loop. This method is the best of the three key stretching methods.

4) Transform the password before hashing: Before calculating the MD5 hash for the password, the latter is transformed using a simple cipher method.

5) Chaining method and XOR(Exclusive OR) cipher: If iterative hashing is used, the hash output from the current iteration is used in the input for the next iteration. We use a simple XOR cipher to compute the final hash by "XORing" the hash output value from all iterations. A simple XOR cipher is typically of the form shown in (5). If the key is made random enough, the ciphertext will be almost impossible to crack.

plaintext XOR key = ciphertext (5)

which is a random string of 128 bits. Each user has a different initialization vector value.

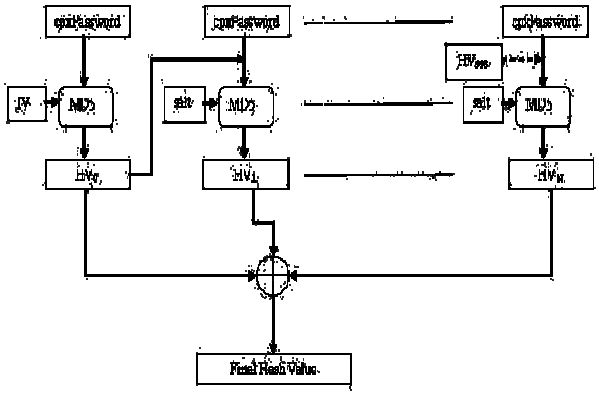

Figure 3. Improved MD5 processing

VII. CONCLUSION

In cloud computing environment user authentication is a major security concern. Another major security issue is the storage and transmission of user authentication or login details. In cloud environment, password storage security is one important aspect of data security as most systems nowadays require an authentication method using passwords. By increasing demand of stronger authentication mechanisms, on line services adopted sms based one-time passwords (OTP). Hashing algorithms such as MD5 are commonly used for encrypting plaintext passwords into strings that theoretically cannot be deciphered by hackers due to their one-way encryption feature. However, with time, attacks became possible through the use of dictionary tables and rainbow tables. In this paper, we discussed different methods to thwart these attacks: (1) the use of a strong password to reduce the probability of it existing in a dictionary, (2) using salts, (3) key stretching and iteration hashing to make the MD5 computation slower. By the survey of the encryption scheme, MD5 can be made safer when it is included by salt key. The grouping of these two methods will generate secure token for authentication and storage of login details in cloud computing environment.

REFERENCES

[1] C. Wang, S. Chow, Q. Wang, K. Ren, W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, No. 2, February 2013.
[2] Zhang Shaolan, Xing Guobo, Yang Yixian, Improvement and Security Analysis on MD5 [J]. Computer Application, 2009, vol. 29(4):947-949.
[3] Xiaoling Zheng, JiDong Jin, Research for the Application and Safety of MD5 Algorithm in Password Authentication, 9th International Conference on Fuzzy Systems and Knowledge Discovery, 2012.
[4] H. Mirvaziri, Kasmiran Jumari, Mahamod Ismail, Z. Mohd Hanapi, A new Hash Function Based on Combination of Existing Digest Algorithms ,

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

The 5th Student Conference on Research and Development – SCOReD 2007, 11-12 December 2007, Malaysia.
[5].Md. Didarul Alam Chawdhury, and A.H.M. Ashfak Habib, Security Enhancement of MD5 Hashed Passwords by using the Unused Bits of TCP Header, Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008) 25-27 December, 2008, Khulna, Bangladesh.
[6] H. Lv and Y. Hu,"Analysis and Research about Cloud computing security protect policy", in Proc. IEEE Int. Conference on Intelligence Science and Information Engineering. pp. 214-216, 2011.
[7] A. Bakshi and B.Yogesh,"Securing Cloudfrom DDOS Attacks using Intrusion Detection System in VM," in Proc. IEEE Second Int. Conference on Communication Software and
Networks., pp. 260-264,2010.
[8] M.Misbahuddin,"Secure Image Based Multi-Factor Authentication (SIMFA): A Novel approach for Web Based Services, Ph.D Thesis, Jawaharlal Nehru Technological University, [Online], http://shodhganga.inflibnet.ac.in/handle/10603/3473, 2010
[9] B.Meena and K.A. Challa , "Cloud Computing Security Issues with possible solutions," Int, Journal of Computerr Science and Technology, vol.2, Issue: 1, Jan–March, 2012
[10]Kazi Zunnurhain and Susan V. Vrbsky,,"Security Attacks and Solutions in Clouds, [Online] http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf, 2010 [11] N.S Chauhan and A.Saxena,"Energy Analysis of Security for
CloudApplication," in Proc. Annual IEEE India Conference, pp. 1-6, 2011.
[12] W.Liu, "Research on Cloud Computing Security Problem and Strategy," inProc. IEEE 2nd Int. Conference on Consumer Electronics, Communications and Networks, pp. 1216-1219, 2012.
[13] X. Yu and Q. Wen, "A view about Cloud data security from data life cycle, (2010)," in Proc. IEEE Intl. Conference on Computational Intelligence and Software Engineering, pp. 1-4, 2010.
[14] Kazi Zunnurhain and Susan V. Vrbsky,,"Security Attacks and Solutions in Clouds, [Online] http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf, 2010
[15] Danish Jamil & Hassan zaki, " Security Measures in Cloud computing and Counter measures", International Journal of Engineering Science and Technology(IJEST), Vol.3 No.4 ,2011

BIOGRAPHY

Kratika Ingle, Research Scholar, Dept. of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, India

Prof. Nitin Shukla Presently working as H.O.D , Deptt. of Master of Computer Application at Shri Ram Institute of Techology Jabalpur, India

Prof. Bharat Solanki Presently working at Shri Ram Institute of Technology,Jabalpur (as Asst. Prof.) since 2001. Published more than 10 research papers in International /National Journals/conferences. Attend more than 12 conferences/seminar/short term training program at various organisation.

Dr. Samar Upadhyay Presently serving at Government Engineering College, Jabalpur, (as Head of the Department) since 1994. Published more than 15 research papers in International and National Journals organised more than 15 national conferences/seminars/short term training programs at Govt. Engineering College, Jabalpur (M.P.).