IJIRMET ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Multiple Securities for Cloud Computing Using RIPEMD-160

[1] K.Sriprasadh, [2] S.Mageshkumar, [3] Dr.S.Sivasubramanian
[1] [2] Research scholar,Department of Computer Science and Engineering Bharath University Chennai.
[2] Principal, MSAJC of Engineering Chennai.

Abstract: ***Cloud facing many new security threats day by day the threats are vulnerable and reduces the confidentiality of the cloud secure cloud from these various attacks ,here a multiple security aspect is proposed to make the cloud more secure .There are dozens of security has been reported till now, in that in this paper it is tried to secure the cloud from the maximum number of security threats. In this paper three way of approach is been implemented to make the cloud secure, those implementations encryption security with the cryptographic algorithm to provide initial security to the data, message digest algorithm to provide security for cloud data which makes over security to avoid data breach one of the threat for the cloud data and overall security in form of authentication, which will enable a complete security format for the cloud datum.***

Keywords: Cloud threats, RIPEMD-160, data leakages , weak authentication.

I. INTRODUCTION

At present there around half a dozen of challenges for cloud computing in this paper it is listed out and solution is been sorted out in better manner with the limited and effective methodology challenges to the cloud are data leakage, weak authentication, cloud hijacking, complete data loss, DoS attack , service based issues . These challenges can be resolved with effective technique, before getting into solution the challenges are briefed [1].

Data leakage

When a data leakage occurs, organizations may incur fines, or they may face legal issues or criminal cases. Breach investigations and customer notifications can rack up significant costs. Indirect effects, such as brand damage and loss of business, can impact organizations for years. It is loss of important information about the concern; it may be loss organization success formula. This issue may be sorted out by the proper authentication techniques [1].

Weak authentication

Weak authentication leads to data leakage, organizations often struggle with identity management as they try to allocate work appropriate to the user's job role. More important, they sometimes forget to eradicate user access when a job function altered or a user resigns from the organization [2].

This challenge can be resolved by proper authentication from proper key distribution setup. Algorithm for authentication based on time stamp can be implemented to solve this issue in the cloud computing.

Cloud Hacking

The breaking into or taking over of the cloud account of an individual, business or other organization by an unauthorized user. Cloud hijacking can be accomplished by stealing a user's login credentials or by hacking. Cloud systems are an attractive target for cybercriminals since they contain so much information in a single location. This information can be used to steal money, commit identity theft and expose company trade secrets. It can also be used to spread malicious software or diverting the user to the unwanted sites where the user doesn't want to look at or the take the services in which the user doesn't require [3].

This issue can resolved by the secure cloud admin and security can be provided by proper authentication setup .A key distribution center can be established with strong algorithm which will challenge the user with the various types of authentication with multiple authentication setup hacking can be resolved by that attack such as hacking can be broke and cloud also can be saved.

Complete data Loss

Data loss in the cloud is a event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application. It occurs when one or more data elements can no longer be utilized by the data owner or requesting application. This normally occurs in the cloud when large number of data is transacted, data dumping is happened, in that case a part of old data can be overwritten by the new data. This can be avoided by proper space allocating technique, which can resolve the issue [4].

DoS attack

Denial-of-service (DoS) attacks typically flood cloud servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them. While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flooding attacks can be more difficult to recover from.

DoS attacks issue takes huge value of processing power, a bill the users may ultimately have to pay. While high-volume DoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities. The key is to have a plan to mitigate the attack before it occurs, so administrators have access to those resources when they need them. A proper authentication set up should be established to stop this attack[2].

Other service based issues.

Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone. If an integral component gets compromised - say a hypervisor, a shared platform component, or an application -- it exposes the entire environment to potential compromise and breach. This will make to collapse of the entire cloud in the worst conditions this too can be resolved by providing proper infrastructure based security.

Effective Solutions for the Issues

The cloud data leakage can be done through proper message digest form message digest is a technique which provides enough security to the data with proper coverage A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message. They are a type of cryptography utilizing hash values that can warn the copyright owner of any modifications applied to their work.

Message digest hash numbers represent specific files containing the protected works. One message digest is assigned to particular data content. It can reference a change made deliberately or accidentally, but it prompts the owner to identify the modification as well as the individual(s) making the change. Message digests are algorithmic numbers. There are n number of message digest formats, in the proposed system RIPEMD is been implemented for message digest for the cloud data security to avoid data leakage

RIPEMD

RIPEMD-160 is an improved, 160-bit version of the original RIPEMD, and the most common version in the family. RIPEMD-160 was designed in the open academic community, in contrast to the NSA-designed SHA-1 and SHA-2algorithms. On the other hand, RIPEMD-160 appears to be used somewhat less frequently than SHA-1, which may have caused it to be less scrutinized than SHA. RIPEMD-160 is not known to be constrained by any patents.

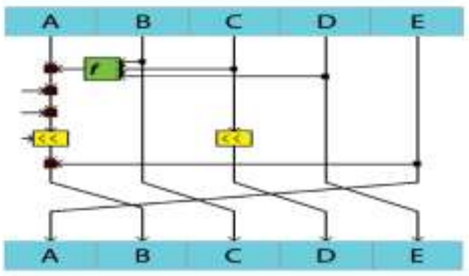


Fig-1 RIPEMD -160

As well as 160-bit, there also exist 128-, 256- and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. The 128-bit version was intended only as a drop-in replacement for the original RIPEMD, as the security aspect is good in RIPEMD -160 is considered message digestion. RIPEMD-128 is a 128-bit hash function that uses the Merkle-Damg˚ard construction as domain extension algorithm: the hash function is built by iterating a 160-bit compression function h that takes as input a 512-bit message block mi and a 128-bit chaining variable

cvi : cvi+1 = h(cvi , mi)

Where the message m to hash is padded beforehand to a multiple of 512 bits3 and the first chaining variable is set to a predetermined initial value cv0 = IV[5].

RIPEMD 160 algorithm.

RIPEMD-160 Logic
Step 1: append padding bits .The message is padded so that its length is congruent to 448 mod 512 (length ≡ 448 mod 512). Padding is always added (1 to 512 bits).The padding pattern is 100…0

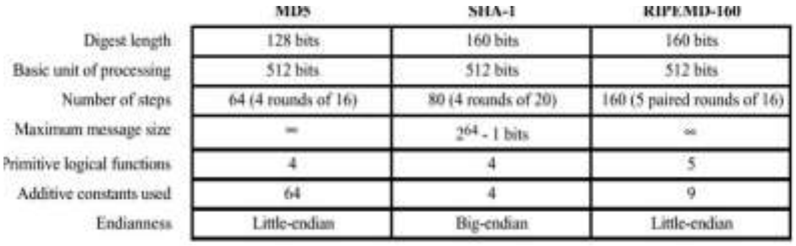
Step 2: append length A 64-bit length in bits of the original message is appended. If the original length is greater than 264, the length is modulo 264

Step 3: initialize MD buffer A 160-bit buffer is used to hold intermediate and final results of the hash function. The buffer is represented as 5 32-bit registers (A, B, C, D, E) initialized to the following integers (hexadecimal values): A = 67452301 B = EFCDAB89 C = 98BADCFE D = 10325476 E = C3D2E1F0 The values are stored in little-ending order, i.e., the least significant byte of a word in the low-address byte position: word A = 01 23 45 67 word B = 89 AB CD EF word C = FE DC BA 98 word D = 76 54 32 10 word E = F0 E1 D2 C3

Step 4: process message in 512-bit (16-word) blocks A module with 10 rounds of processing of 16 steps each The 10 rounds are arranged in 2 parallel lines of 5 rounds each Input – 512-bit block Yq, 160-bit buffer value CVq (ABCDE or A'B'C'D'E') Output – 160-bit chaining variable CVq+1 (updated ABCDE) Makes use of additive constant Kj. The output of the last round is added to the input of the first round (CVq) to produce CVq+1 in the following fashion:

CVq+1(0) = CVq(1) + C + D'
CVq+1(1) = CVq(2) + D + E'
CVq+1(2) = CVq(3) + E + A'
CVq+1(3) = CVq(4) + A + B'
CVq+1(4) = CVq(0) + B + C'

Step 5: output the output from the L-th stage is the 160-bit message digest



	MD5	SHA-1	RIPEMD-160
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
Number of steps	64 (4 rounds of 16)	80 (4 rounds of 20)	160 (5 paired rounds of 16)
Maximum message size	∞	2^{64} - 1 bits	∞
Primitive logical functions	4	4	5
Additive constants used	64	4	9
Endianness	Little-endian	Big-endian	Little-endian

Fig-2 Comparing performance RIPEMD -160 with message digest algorithm

Based on this cloud data can message digest can be forwarded to the concern client to avoid data leaks .In case it is leaks also it will be in unreadable format. This will provide security cloud in better manner [16].

II. CONCLUSION:

For multiple security based challenges RIPEMD-160 will provide security over threats like data leakage, weak authentication and complete loss, in future further more techniques can be included to provide complete security for cloud.

References

[1]https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

[2] https://www.incapsula.com/blog/top-10-cloud-security-concerns.html

[3]http://users.techtarget.com/registration/searchcloudcomputing/LoginRegister?auth=YpOy5Aw6Wkw%3D

[4] http://www.investopedia.com/terms/c/cloud-hijacking.asp

[5] Cryptanalysis of Full RIPEMD-128 Franck Landelle1 and Thomas Peyrin2,? 1 DGA MI, France 2 Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore landelle

[6]M. Preetha, M. Nithya," A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM", IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

[7] AMIT GOYAL and SARA DADIZADEH," A Survey on Cloud Computing"

[8] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, "Dual RSA and Its Security Analysis", IEEE Transactions on Information Theory, Vol. 53, No. 8, pp. 2922-2933, 2007.

[9] P.Saveetha & S.Arumugam," Study On Improvement In RSA Algorithm And Its Implementation"

[10] B.Persis urbana ivy,Mukesh kumar,Purshotam mandiwa" A modified RSA Cryptosystem based on n prime numbers",IJECS.

[11] CRS BHARDWAJ Modibada, Jabalpur (Mp), India," Modification Of Des Algorithm", IJIRD, Vol 1 Issue 9, November, 2012, , pg.495 – 505.

[12] Shah Kruti R.& Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[13] Mary Cindy Ah Kioon, ZhaoShun Wang and Shubra Deb Das," Security Analysis of MD5 algorithm in Password Storage", Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13).

[14] Priyanka Walia & Vivek Thapar," Implementation of New Modified MD5-512 bit Algorithm for Cryptography", international Journal of Innovative Research in Advanced

[15] Bert den Boer and Antoon Bosselaers. Collisions for the Compressin Function of MD5. In Tor Helleseth, editor, EUROCRYPT, volume 765 of LNCS, pages 293–304. Springer, 1993.

[16] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. RIPEMD-160: A Strengthened Version of RIPEMD. In Dieter Gollmann, editor, FSE, volume 1039 of LNCS, pages 71–82. Springer, 1996

[17] . Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding Collisions in the Full SHA-1. In Shoup [23], pages 17–36.