International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-5, June 2017

Design Robust Data Integrity Scheme in Cloud Computing Based on Image Histogram and Crypto-Hash Function

Nadra J. Ali AL-Saad

Abstract: ***Cloud technologies are revolution in computing world which support on demand access to several virtualized customers and servers which are existed outside of data owner's center. In this computing model, the databases and applications of data owners are arise to the unified large data centers and may be lead to many security issues in the management of data and services. Preserving the secrecy and reliability of the message communicated between the main elements of Cloud considers one of the significant aims of Message Authentication Code (MAC). In this paper, we propose a robust scheme based on image histogram and Crypto-hash function to check the integrity of data message between sender and receiver. This scheme is selected the pixels that located in top peak of histogram to generate more efficient message capacity. As well as, our proposed scheme includes many security features such as resisting the well-known attacks, user's message anonymity, session key agreement, and data integrity for user's message. The security analysis proves that the proposed scheme can resist the public security malicious attacks such as Insider attacks, key recovery attack. Finally, our scheme is efficient in terms of performance.***

Keywords: ***Cloud Computing, MAC, Insider attack, MAC, Histogram.***

I. INTRODUCTION

Cloud computing considers as a network where the user can use many services based on *Cloud Service Provider* (CSP) by using pay per use bases service. Most of originalities are determined to reduce their computing cost via the funds of virtualization. This demand of reducing the cost of computing has referred to the innovation of Cloud Computing. As well as, this modern of computing is used to indicate a set of internet and information technology services that are support to many customers and users over a network on a rented basis and with offering ability to user for scaling up or down as per their service supplies. Regularly cloud computing services are provided by a third party provider who called CSP and owns the main infrastructure. Additionally, it has become one of the most spoken about modern technologies in recent years and has acquired lots of attention from mass media in addition to analysts because of the chances it is offering [1-3]. The security is a constitutive issue that hinders its widespread adoption.

Manuscript published on 30 June 2017.
***** Correspondence Author (s)
Nadra Jamil Ali, M.Phil, Department of Computer Science (Sussex Univ. UK) College of Education, Basra University, Basrah, 61004, Iraq. E-mail: nadraa55@gmail.com

In Cloud computing, data bases and software applications are moved to outsource storage that means the management of remote data is not fully trustworthy. Therefore, to keep security is very important to outsourcing data and applications which located in the third party service provider. Moving of data in cloud is suitable for customers as they do not have to deal with sophisticated data management and other hardware associated issues on their local/ regional data centers. But this appropriateness brings down the user to the mercy at their cloud service providers for correctness, accuracy, and trustworthiness of their outsourcing data. Since the applications and data are under control of the third party service provider, the users have to rely on the security mechanisms implemented by service provider for availability and integrity of their data. Additionally, the exchanging messages among parties are suffered from malicious attacks over communication channel. So, it is necessary to check the integrity and authenticity of each component's message [4,5]. Clearly, a legal user generates user's message and is provided by Message Authentication code (MAC) for ensuring from the integrity and authenticity of received message. MAC functions need possessing many security tools such as SHA-1, SHA-2. For building strong security, a MAC function should be armed in good features to resist celebrated attacks such as Key recovery and forgery attacks. Furthermore, even if an attacker can be reached an oracle which holds the secret key and creates MACs for messages of an attacker's selecting; he cannot guess MAC for other messages without execution infeasible amounts of computation. The main elements (sender and receiver) of MAC values are applied the same secret key. This means that the components of a message should be agreed on the same key in the initial phase, as is the case with symmetric encryption. Additionally, any legal user has ability to verify a MAC is also capable of generating MACs for other messages [4, 5]. Constantly, MACs represent very sensitive to any updating of the message. If one or more bits of user's message edit, MAC updates about 50 percent of their bits and cause to be the message unfeasible. Moreover, the successful verification of MACs requires equivalence of all of bits of the received sender's MAC with computed receiver's MAC. Such a inflexible condition for the effective verification of messages endangered by MACs is not appropriate for some applications. There are many schemes in this fields that suffered from several shortcomings such as forgery attacks, insider attacks, and guesting secret key between the trust parties [6].

In 2006, Ashwin Swaminathan et al. have developed scheme for producing an image hash, using Fourier-Mellin transform characteristics which are constant to two-dimensional affine transformations. The aims of this scheme to build a secure and strong image hash and has a good performance [7]. In 2008, Rabadi and Mahmud [8] proposed a good and robust concept of message anonymity. Their scheme focused on using MAC which transferred from vehicle to vehicle and has authentication, anonymity, and message integrity. In 2010, Jamil and Aziz [9] proposed scheme to use permutation key to transformed image between sender and receiver to reduce the issues of security over communication. In this paper, we propose a robust message authentication scheme for cloud computing environment that involves of two stages—setup and verification. As well as, our work motivates to use authentication and integrity protection of messages exchanged over a secure communication channel between components that based on secret key and image histogram. Where, both of sender and receiver have been agreed to the secret key at initial stage. The generating of our proposed scheme actives a sender message to encode any message based on one time shared key generated from histogram of secret image which supported to all entities in initial phase. In the other side, the receiver has ability to detect the validity of sender's MAC that he uses the same secret keys to complete the integrity of message at verification phase. Our proposed scheme has central merits as follows: (1) the cloud service provider and a legal user can access authenticated session's keys; (2) Our proposed scheme can resist several attacks such as reflection attack, insider attacks, and forgery attacks; (3) we propose an efficient scheme for choosing a best parameter value to reduce computational cost of cloud audit services. Table 1 shows the comparison in security properties of our proposed scheme with other schemes.The rest of this paper is organized as follows. The essential primitives and requirements of our proposed scheme exist in Section 2. Our proposed scheme is presented in Section 3. We detail the security analysis and implementation results in Section 4, and Section 5 concludes the paper.

Table 1. Comparison with related works

Feature	Proposed scheme	[7]	[8]	[9]
C1	Yes	No	No	No
C2	Yes	No	No	No
C3	Yes	No	No	Yes
C4	Yes	Yes	Yes	Yes
C5	Yes	No	Yes	Yes
C1: one time key; C2: one time MAC; C3: Message Anonymity; C4: Key management; C5: Resisting Insider & Forgery attacks				

II. PRIMITIVES AND TOOLS

For more distinctness, we show concisely some of the tools that are used during our construction.

A. Crypto-hash function

- ✓ A hash function considers a flexible function mapping binary strings of arbitrary length to binary strings of fixed length (e.g. 128 bits), called the hash-value or digest. Conversely, for cryptography, a hash function should be one-way function as follows:-
- ✓ Specified only a digest, it should be computationally infeasible to detect a piece of data that generates the digest (pre-image resistant). The collision is a state indicated that we have two different messages M and M' such that H(M) = H(M').
- ✓ A hash function has ability to be collision free.
- ✓ A hash function is weakly collision-free or second pre-image resistant if given M it is computationally infeasible to find a different M' such that H(M) = H(M').
- ✓ A hash function is strongly collision-free if it is computationally infeasible to find different messages M and M' such that H(M) = H(M').

The *secure hash function* (SHA) family is a set of related with cryptographic hash functions and offered by the *National Institute of Standards and Technology* (NIST). SHA-0 considers the first member of SHA, was issued in 1993. SHA-1 represents as a advanced version of SHA-0, was issued in 1995. Four irregular models have been published by NIST with enhanced output ranges and a slightly different design as follow: SHA-22, SHA-256, SHA-384, and SHA-512 [10]. In this paper, we use SHA-512 enjoyed in high efficiency and flexibly.

B. Image histogram

An image histogram is a kind of histogram which performances as a graphical representation of the total distribution in an image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. The left side of the horizontal axis represents the black and dark areas, the middle represents medium grey and the right hand side represents light and pure white areas. The vertical axis represents the size of the area that is captured in each one of these zones. Thus, the histogram for a very dark image will have the majority of its data points on the left side and center of the graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph [11].

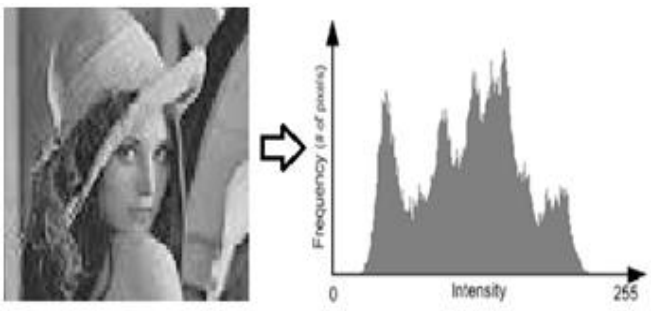

Figure 1 Shows Image Histogram

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

III. PROPOSED SCHEME

Our proposed scheme depends on three components, Cloud Provider (CP), User as a Sender (S), and User as a Receiver (R). Our work involves of two stages— Setup and Verification. Setup stage is implemented only once while the verification stage is performed whenever a sender and receiver want to exchange their messages with gather.

In the setup stage, the sender and receiver should be registered their identities into CP who supports key image (Img) to both the sender and receiver in the secure channel. Key image is used to extract secret key SK to secure message between entities in the next stage. The importance of SK will explain in more details in verification stage.

The main elements (CP, S, R) also uses a cryptographic hash functionh(.). After setup stage, the sender/receiver can extract his secret key (SK) from his key image (Img) to complete verification stage.

Verification stage is experienced as follows.

[1] $S \rightarrow R: M, Ms, Spoint, Epoint$. S does the following steps:

- The sender's message represents by M.
- Generate two random numbers $Spoint, Epoint \in Z_{Frq}$; where Frq is maximum frequencies of image histogram of key image (Img). So, $Frq = Max(imghist(Img))$; $imghist$ is function to compute histogram of key image (See Fig. 2).
- Compute secret key SK which is started from $Spoint$ to $Epoint$ of $imghist(Img)$. Fig. 2 shows the mechanism of extract secret key from image histogram of key image that supported of each user by CP in setup stage. SK generates once time for each exchanging message between receiver and sender.
- Compute anonymous message code $Ms = h(M||SK)$, this step protects user's message; If the sender resends the same message M to the receiver or vice versa, an attacker cannot detect message M' because the secret key SK generates once for each communication chanal between entites that leads to generate anonymous.
- Send $M, Ms, Spoint, Epoint$ to R.

[2] R checks the integrity of receiver's message as follows:

- Compute SK' based on compute image histogram of his image key $imghist(Img)$ and extract SK' by using $Spoint, Epoint$ that he has obtained it from sender. Then, R computes $Mr = h(M||SK')$. Finally, if the Mr matches with Ms, R ensures from integrity of sender's message authority of sender. Otherwise, R dismisses verification stages.

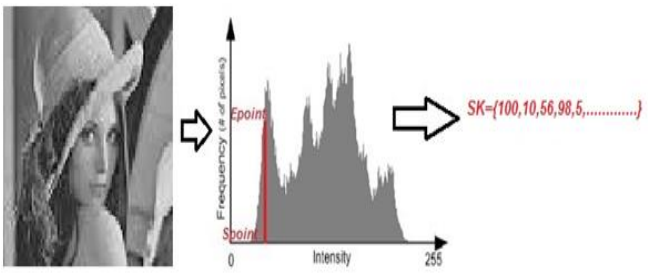

Figure 2. Viewing the mechanism to compute secret key *SK*

IV. DISCUSSION RESULTS

In this section, we support the security analysis of our work and experimental results as follows:

Formula 1. The proposed scheme can support Known-key security and session key agreement and resisting key recovery attack.

Proof. In our proposed scheme, when the sender submits his messages to the receiver or vice versa, he uses secret SK to compute $Mr = h(M||SK')$ based on $Spoint$ and $Epoint$. An attacker cannot access to the session keys (SK, Img), he is still unable to get fresh values of SK which generates once for each exchanging message between entities. As well as, an attacker does not has any advantages even he got importunes parameters $(SK, Spoint, Epoint)$ because these keys are generated once for each verification stage. We notice the secret key has generated once and difference size for each verification stage among components. Table 2 demonstrates the technique of generating key from histogram in figure 1. We focus on the first seventh time to exchange message between entities. Therefore, our proposed scheme provides session key agreement and resists key recovery attack.

Formula 2. Our scheme can resist the forgery attack and insider attack.

Proof. If any attacker tries to impersonate sender/receiver, he should be accessed a valid session message $(M, Ms, Spoint, Epoint)$ by using secret parameters (SK, Img). An attacker fails to access image key (Img) to compute $(SK, Spoint, Epoint)$. Thus, our proposed scheme prevents the forgery attack and insider attack.

Additionally, we performed many experiments for evaluating the efficiency and the effectiveness of our proposed scheme. Figure 3 views performance of verification stage. Conversely, we notice that the average time for the verification stage is equal to 0.0924 seconds for each entity who validates the authority and integrity of another entity's information. We have listed during our experiments 500 users.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 2. Explain the mechanism of generating key for each verification stage

Verification Stage Time	Spoint	Epoint	SK	Length
First Time	100	1150	{198,280,300,251,33……..}	1140
Second Time	5	10	{10,46,187,99,100}	5
Third Time	40	900	{55,109,78,……..}	860
Fourth Time	100	200	{40,981,781,33,……..}	100
Fifth Time	40	250	{67,98,541,32,123,231,……}	210
Sixth Time	200	245	{78,89,1011, 201, 31,…….}	45
Seventh Time	100	215	{451,200,321,35, 819,76,……}	115

V. CONCLUSION

In this paper, a robust scheme of using image histogram to generate once key and anonymous message authentication code is proposed. In our work, we employ the histogram of image to succeed to data integrity and user's authority. Additionally, we compared our proposed scheme with related work in this reverence for cloud data management.

Our proposed scheme aims to provide more elasticity and to resist well-known attacks. These main features include (1) our work support a strong MAC between the sender and receiver in cloud environment; (2) it presents one-time message anonymity; (3) Using image histogram for key management that making an attacker fails to get main keys. As a result, our proposed scheme achieves good balance between a good security and performance.

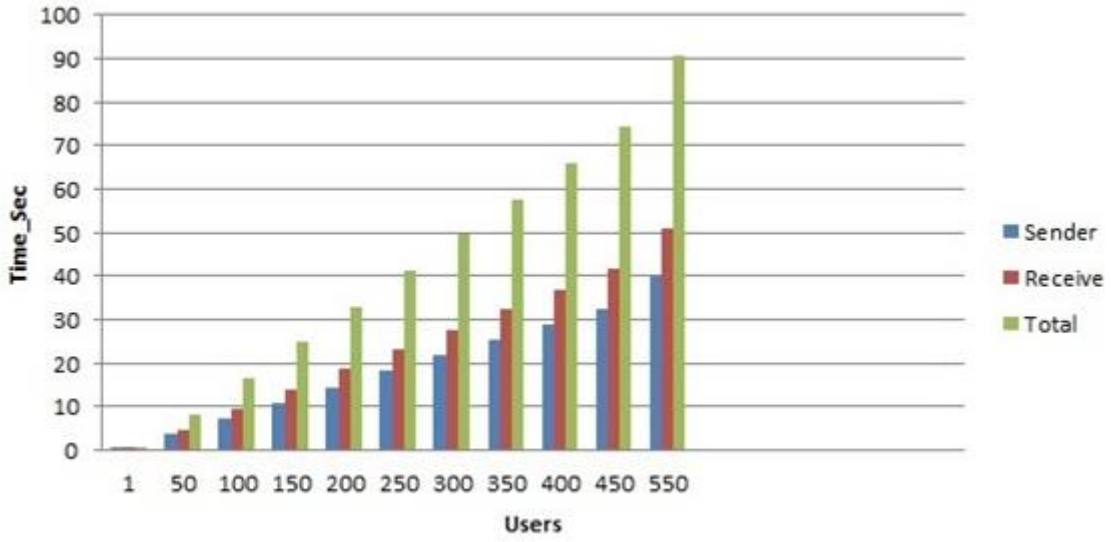

Figure 3 Demonstrates Performance of Proposed Scheme

REFERENCES

1. S. Singha, Y-S Jeongb, J. Park, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications, Volume 75, 2016, pp. 200–222.
2. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Vol. 34, no.1, pp. 1-11, 2011.
3. Ali. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, D. Zou, "A Practical privacy preserving Password authentication Scheme for Cloud Computing", Proc. of the IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW'12), May 2012, Shanghai, China, pp.1204-1211.
4. Ali A.Yassin, H. Jin, A. Ibrahim, D. Zou, Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing, Proc. Of the IEEE Second International Conference on Cloud and Green Computing (CGC'12), Nov. 2012, Chain, pp. 282-289.
5. R.L. Rivest. The MD message digest algorithm, In S. Vanstone, editor, Advances in Cryptology - CRYPTO' 10, LNCS 5 , pp. 0 - 11, 2011.
6. Zaid A. Abduljabbar, H. Jin; Ali A. Yassin; Zaid A. Hussien; Mohammed A. Hussain; Salah H. Abbdal; D. Zou, Robust scheme to protect authentication code of message/image documents in cloud computing
7. International Conference on Computing, Networking and Communications (ICNC'16), Feb. 2016, USA, pp. 1-5.
8. A. Swaminathan, Y. and M. Wu, ―Robust and secure image hashing,‖ IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 215-229, 2006.
9. N. Rabadi and S. Mahmud, ―Drivers' anonymity with a short message length for vehicle-to-vehicle communications network,‖ Proceedings of the Fifth IEEE Consumer Communications and Networking Conference (CCNC'08), Las Vegas, NV, USA, IEEE, pp. 132-133, Jan. 2008.
10. N. Jamil and A. Aziz, ―A Unified Approach to Secure and Robust Hashing Scheme for Image and Video Authentication, Proceedings of Third IEEE International Congress on Image and Signal Processing (CISP), Yantai, China, pp. 274-278, 2010.
11. R. Sobti1 , G. Geetha, Cryptographic Hash Functions: A Review, IJCSI, vol.9, No. 2, pp. 461-479, 2012.
12. R. Singh, M. Dixit, Histogram Equalization: A Strong Technique for Image Enhancement, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.8 (2015), pp.345-352.

Nadra Jamil Ali, Computer Science Department, College of Education, Basra University, Basrah, 61004, Iraq.Email: nadraa55@gmail.com

Academic Qualifications

1. B. Sc., Basrah University 1977.
2. Diploma Microcomputer and microprocessor Applications, Essex university/UK 1982.
3. MPhil. Sussex University / UK 1986, Mathematical Library in pascal.

1. Infrared spectroscopy and microcomputer, Al Henday Journal No. 38,pp43(1998),
Mohammed Barakat, Nadra Jamil Ali AL Saad
2. Quantum information between dream and reality, " the arab conference on information technology" ACIT2001 Amman Mohammed Barakat, Nadra Jamil Ali AL Saad
3. Evaluation of programming language's libraries investment, Journal of college of education of pure science, Thakkar university, Vol. 2 Issue 4 2012

Nadra Jamil Ali AL Saad

4. Object recognition in Image using Hybrid (DRA-CSO) Architecture, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS020114, Vol. 4 Issue 02, February-2015 Hamid Ali Abed AL-Asadi,.1 Hussein Ali Al_Iedane, Nadra J. Ali AL Saad
5. Texture Features Based Bag of Visual Words for a Spine MRI Images, Proc of the Fourth Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2016, Copyright © Institute of Research Engineers and Doctors, USA. All rights reserved. ISBN: 978-1-63248-092-7 doi: 10.15224/ 978-1-63248-092-7-46 Khawlah H. Ali, 2Entesar B. Talal, 3Nadra J. Al saad
6. Texture Features Analysis using Gray level Co-occurrence Matrix for a Spine MRI Images, International Journal of Computer Science and Information Security, IJCSIS September 2016 Volume 14 No. 9. Khawlah H. Ali, 2Entesar B. Talal, 3Nadra J. Al saad.
7. Security Issues in Wireless Sensor Network. Will be published in the Volume. 3, Issue. 5, May – 2017 of JMESS. H. Ali, 2Entesar B. Talal, 3Nadra J. Al saad