International Journal of Advanced Science and Technology
Vol. 29, No.02, (2020), pp. 3088-3094

A Secure Message Integrity in Cloud Computing with Combined Cryptographic Approach

[1]Shivanna K, [2]Dr. Prabhudeva S
[1]Research Scholar, VTU, Belagavi
Asst. Professor, Department of CSE, GMIT
Davanagere-577006, Karnataka, India
[2]Professor, Department of ISE
JNN College of Engineering
Shivamogga-577201, Karnataka, India

***Abstract**: Message authentication ensures that there is no modification, deletion, insertion or replay of shared data. Today, millions of users sharing resources on internet through cloud computing. Providing integrity of shared data among data owner and data user is a major issue. Many research works is carried out related to message integrity, but still there is a lack of security interns of message authentication between data owner and cloud user. In this paper, we implement a technique, where data owner wants his message to be private so that the cloud user can access it. The proposed work comprises of different technique and procedures that ensure data protection. We commence with message integrity and confidentiality. The SHA1 and SHA2 are used for integrity check of data, Bluefish algorithm is for confidentiality. The owner wishes to do modification on stored data if necessary only by providing or regenerating message digest value on cloud platform.*

***Keywords:** Cloud security, Message integrity, Message digest, One Time Pad.*

I. INTRODUCTION

Today, cloud computing plays a vital role on information technology to store large amount of valuable data. Vast amount of data is processed across the network only through cloud computing paradigm. Towards high speed data transfer, various cloud terminologies are come into picture:

1. Cloud Service Provider(CSP):

Organization that provides on demand services in a pay and use manner. Services are deployed in a datacenter; we can access service by network connectivity.

2. Cloud user:

Cloud user is a person or organization that use cloud services and registered with CSP.

3. Data owner:

Data owner is a person or organizations who upload data on CSP. An administrative control over data may be granted to owner of data.

4. Datacenter:

Datacenter acts as communication server for remote storage. Its role is to process and distribution of vast amount of data across cloud environment.

5. Cloudlet:

Cloudlet is a small-scale cloud data center; it supplies resources to networked devices with low latency.

6. Broker:

Broker acts as an intermediary who creates virtual machine (VM), submission of cloudlets to VM and also disable activities of VM's.

Cryptography is a popular technique where in which the data resources are protected by encryption and decryption, which protects our data whether it is kept in a networked system or in transit. The key used to compute encryption and decryption is plays a major role in cryptography. Security of data stored and transmitted is based on key size. Today in all cryptographic techniques have 128 bits as a key size, but performance of the system is lower when key size is increases. In cloud computing, quantum of data is less in size but it is more valuable.

The paper is structured as follows: In section 2, existing work related to cloud security and what are the cryptographic techniques to solve security issues are highlighted. Section 3 provides a model which is designed for solving security issue of cloud computing. Section 4 summarizes experimental results. Section 5 provides security measures of proposed system. In section 6, we concluded this paper.

II. RELATED WORK

In [1], the researcher have proposed two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. They show that proposed authentication codes are more efficient compared with earlier techniques. Efficiency is increased by addition and modular multiplication, because of short messages have to be exchanged between mobile and pervasive devices.

In paper [2], remote health monitoring application (RHM) through cloud computing was implemented. The author highlights patient health data is super sensitive and privacy, security for cloud based shared storage. To reduce unauthorized access of patient health data captured by a set of bio-sensor is stored in the cloud, they use bio-metric based authentication and encryption. The methods, they implemented that protect from unauthorized access and self-protect the data in case of un-trusted access using bio-metrics. Still author needs to implement and integrate this technique within a cloud based application for healthcare monitoring.

Security of cloud data on a smart phone is addressed in paper [3]. Authentication ensures the secure communication between cloud and smart phone. An algorithm such as RSA and DES obtain relatively more authentication while considering the computing cost and battery power of a smart phone.

In cloud computing, data security is one of the biggest concerns [4]. Utilizing cloud data regularly, problems related to data missing is extremely high. The researcher have proposed a technique for providing secure data integrity on multi-server cloud infrastructure that ensures all information pertaining to cloud is in the secured condition in order to prove the trustworthiness of data. The experiment is done based on integration time on multi-server, security level and recovery efficiency level.

In paper [5] [6], researcher have proposed a secure cloud data processing and securing for Health data. Without privacy concerns the exchange of medical records with various institutes to provide a security model for cloud data. The execution time is measured by selecting a secret-sharing algorithm such as Shamir's secret-sharing scheme and Rabin's information dispersal for multi-cloud architecture.

A security, flexible data sharing scheme (SFDS) is proposed by Dongliang Lei at al [7]. It supports an identity-based system, which guarantees to provide strong security for cloud data when it is shared among multiple users.

In [8], data shared by the owner of the data and the user that intensively direct privacy preserving mechanism. Cloud technique proposed by an author that monitors sensitive data. Popular application known as LogCloud that carried out various test like load test, baseline test to monitor sensitive data is through storage of data access logs. This protects the identity, privacy against access of other people, detects person's identity who releases data to be accessed.

In paper [9] [10], researcher have addresses security issues and challenges about cloud computing. They discuss security issues, requirements and challenges with respect to technical and business community. Security issues like data leakage, insecure interface, sharing of resources, data availability and inside attacks are intensively considered by service providers as a best practice.

Sandeep k. sood et al. [11] described an approach to ensure data security in cloud computing using combination of cryptographic techniques. It presents three cryptographic parameters, i.e. confidentiality by searchable encryption, availability by dividing data into three sections to provide simple access to the data and integrity is checked by MAC (Message Authentication Code). However, this model was not proving complete protection of owner data in cloud computing, since we can't

have trustworthiness about cloud provider and majorly hackers. Computation time is also high because encryption technique the author presented in this paper has a key size of 128 bit.

III. DESIGN CONSIDERATION

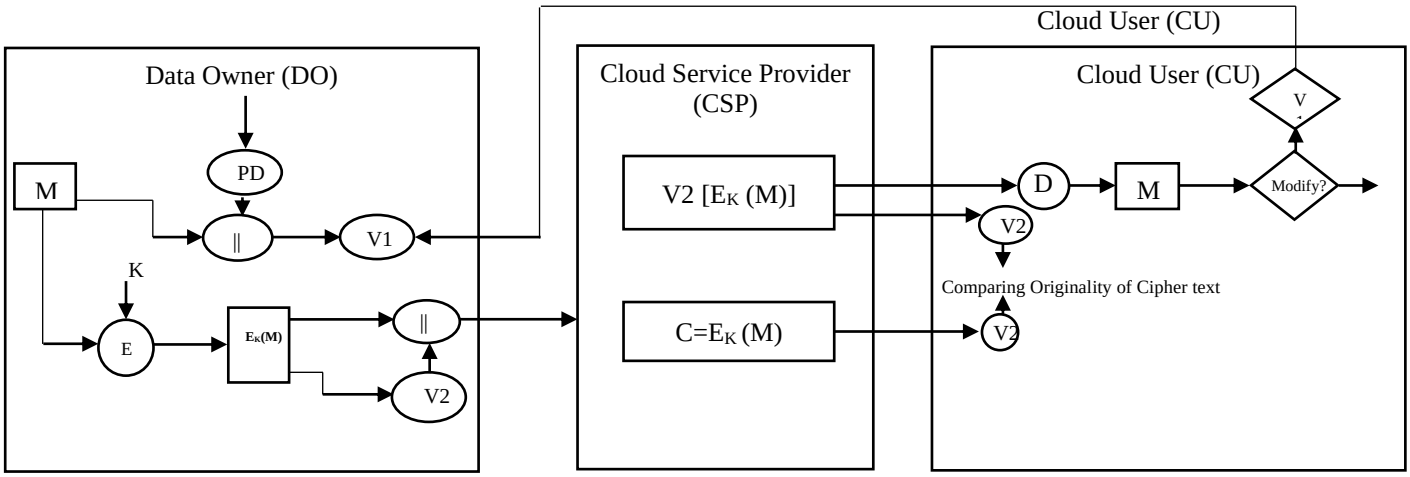
Proposed system has been designed to provide security to cloud data stored. If any alteration or modification required for cloud data that should be carried out by data owner by providing hash value or message digest on secure cloud platform. Thus, we can protect critical information from unauthorized parties or even cloud service provider. The system is divided into three sub models. First model deals with to generate first hash value of original data. Second model is to construct second hash value of cipher text. Third model is designed to compare originality of cipher text, also checking integrity of data uploaded. Thus, authorized entity can alter original data only by providing first hash value, since it is kept in an owner site. The design consideration of the proposed scheme includes notations and descriptions illustrated in Table 1.

Table 1: Notations and meanings

Notations	Descriptions
M	Message bytes
PD	Password of data owner
V_1	Integrity check value$_1$
V_2	Integrity check value$_2$
E	Encryption
D	Decryption
‖	Concatenation

A. Syatem Model

Figure 1 describes the system architecture, in which data files are securely stored and integrity has been checked. A proposed model allows data owners themselves can check the integrity of their cloud data by entering hash tag V1. The integrity check value is recorded on data owner site and it is not disclosed to others even cloud service provider.



Algorithm 1 Integrity check value_1
Input: M_j, PD
Output: $V1$

Algorithm 1 is designed integrity check value V_1 considering input as a password of data owner value V_1 is extracted by using the SHA_2 hashing technique. The resultant output has stored at the data owner site.

1: *compute* $\{M_j \,||\, PD\}$
2: *compute* $\{M_j \,||\, PD\} \leftarrow V_1$
3: *record the secret key* V_1
4: *record* V_1 *at data owner site*

in such a way that an has been computed by message blocks M and PD. The integrity check concatenating M with PD

Algorithm 2 has been designed for obtaining integrity check value V_2 by considering input as a ciphertext C using SHA_1 hashing technique. The ciphertext has been produced by encrypting the message bytes using OTP algorithm. The encrypted message has been uploaded on cloud service provider (CSP).

Algorithm 2 Integrity check value_2
Input: M_j, PD
Output: $V1$
1: **for** $i=1$ *to* n
2: *compute* $V_2 \leftarrow SHA_1(V_2[i])$
3: **end for**
4: *record* V_2 *at data owner site*
5: *record* V_2 *at cloud service provider*
6: *compute* $E_{OTP}(M)$
7: *compute* $\{C \,||\, V_2\}$

Algorithm 3 is designed for comparing originality of ciphertext data whenever decryption of the message is carried out. The integrity check value V_2 of decrypted message has compared to original V_2 is stored in CSP.

Algorithm 3 Comparing originality of cipher text
Input: *Proof*
Output: *True or False*
1: *compute* $V_2 \leftarrow SHA_1(C)$
2: *retrieve original* V_2 *from cloud service provider*
3: **if** *original* V_2 == *computed* V_2 , **then**
4: *return true*
5: **else** *return false*
6: **end if**

Algorithm 4 is designed for providing authority to modify the content of the cloud data which is uploaded by the data owner. Soon after the cloud user has to decrypt the message data, he/she trying to modify the original content by generating integrity check value V_1 from the original message. But, the modication is not possible because the data owner has computed V_1 from M||PD. In the SDIC scheme, V_1 is kept at the data owner site, so that the data integrity will successfully achieve in any situation. The integrity checking is always failed when the other person trying to modify the original data.

Algorithm 4 Integrity check
Input: M_j
Output: *True or False*
1: **while** *true* **do**

find the corresponding message M
if *data modification found* **then**
*success //**integrity check fails***
else *not found*
reject the request
end if
compute $V_1 \leftarrow SHA_2(M)$
if *V1 of user == V1 of data owner* **then**
*success //**integrity check fails***
else *integrity check true*
end if

B. Implementation

The proposed scheme is implemented and tested on Java based Cloud Simulator 3.0.3 [12] as a freely down-loadable CloudSim toolkit. The parameters such as cloud terminology, cloud applications, number of users and network terminologies are considered for implementation.

IV. Experimental Results

The performance of the proposed scheme is compared with existing methodologies using dell i3 processor of 4GB RAM. The proposed methodology is implemented and tested on cloud simulator by considering cloud example-1 and cloud example-2. The processing time or computation time of the methodology is compared with two existing techniques proposed by the authors namely Priyanka Ora et al. [13] and Swapnali Morea et al. [14]. The processing time for encryption and computing integrity check tags such as V_1 and V_2 on data owner site depicted in Table 2.

Table 2: Time of encryption (ms) along with V1 and V2

Size of plain text (bytes)	**434**	**559**	**678**	**810**	**923**
Priyanka Ora and Dr.P R Pal (2015) [1]	3068	4792	5192	39045	49520
Swapnali More and Sangita Chaudhari (2016) [2]	1558	1563	1576	1581	1634
Proposed Scheme	1057	1070	1078	1086	1103

The processing time for decryption of data and computing integrity check tags such as V_1 and V_2 on cloud user site depicted in Table 3. The integrity check tag V_1 used to check the originality of ciphertext and the integrity check tag V_2 used at the time of data modification in the cloud service provider site.

Table 3: Time of decryption (ms) along with V1 and V2

Size of plain text (bytes)	**434**	**559**	**678**	**810**	**923**
Priyanka Ora and Dr.P.R Pal (2015) [1]	2834	4595	6431	9975	19101
Swapnali More and Sangita Chaudhari (2016) [2]	3	4	9	5	5
Proposed Scheme	3	4	4	5	6

The proposed method also designed to increase efficiency of the cloud computing environment in terms of throughput evaluation using equation (1). Whenever the throughput is increases that can able to reduce the power utilization to run applications on cloud system. The throughput of proposed technique is practically increased in comparison with existing solutions is shown in Table 4.

$$Throughput = \frac{\text{SizeofPlaintext}}{\text{EncryptionTime}} \quad \ldots\ldots (1)$$

Table 4: Throughput

Size of plain text (bytes)	434	559	678	810	923
Priyanka Ora and Dr.P.R Pal (2015) [1]	0.141	0.116	0.130	0.020	0.018
Swapnali More and Sangita Chaudhari (2016) [2]	0.283	0.357	0.428	0.512	0.564
Proposed Scheme 2	0.410	0.522	0.628	0.745	0.836

V. SECURITY MEASURES

The proposed scheme is proposed for the integrity and confidentiality of outsourced cloud data on cloud environment. The experimental results are very much related to tackle following issues:

A. Active attack

As data information is hosted on network, there is possibility that an attacker can easily encounter alteration of contents that leads to compromise confidentiality. To overcome this threat, SHA_2 message digest value is attached with confidential data. The proposed system is designed in such a way that message digest value is required when an attacker wants to alter confidential data but this is impossible because message digest value is only regenerated by data owner.

B. Collision resistance

Two different messages have been generated identical hash values that lead to collision resistance. Our approach may be a best possible solution to highjack such vulnerability. In this work, SHA_2 hashing technique is adopted to generate unique hash codes. Thus, we can restrict hacker has to get access the original data by generating hash codes.

C. Data leakage

There are plenty of ways to compromise the system by alteration or deletion of valuable records. In this technique, we strongly refuse such alteration on sensitive data. So that, reputation of cloud service provider may be increases and user can interact with cloud data in a secure manner.

VI. CONCLUSION AND FUTURE WORK

The proposed scheme provides a possible solution to the active attack in such a way that data integrity is able to increase. Data owner authentication, confidentiality of data is achieved in a better way. It is flexible for data owners to alter the cloud data by re-generating hash code. The computational evaluation shows that the proposed scheme requires less processing time and it will relatively reduce processing overhead to run this system on cloud platforms. Currently, the proposed scheme is experimented using a ClouSim toolkit (freeware) as a simulator and the practical implementation in a real cloud environment such as Amazon Web Service is considered as a future work.

References

[1] B. Alomair and R. Poovendran, "Effi-cient authentication for mobile and pervasive computing," in International Conference on Information and Communications Security. Springer, 2010, pp. 186-202.

[2] S. Sharma and V. Balasubramanian, "A biometric based authentication and encryption framework for sensor health data in cloud," in Proceedings of the 6th International Conference on Information Technology and Multimedia. IEEE, 2014, pp. 49-54.

[3] M. Al-Hasan, K. Deb, and M. O. Rahman, "User authentication approach for data security between smartphone and cloud," in Ifost, vol. 2. IEEE, 2013, pp. 2-6.

[4] S. M. Srinivsan and C. Chaillah, "Information interpretation code for providing secure data integrity on multi-server cloud infrastructure," International Journal of Modern Education and Computer Science, vol. 6, no. 12, p. 26, 2014.

[5] A. A. Hossain, S. M. S. Ferdous, S. Islam, and N. Maalouf, "Rapid cloud data processing with healthcare information protection," in 2014 IEEE World Congress on Services. IEEE, 2014, pp. 454-455.

[6] T. Ermakova and B. Fabian, "Secret sharing for health data in multi-provider clouds," in 2013 IEEE 15th Conference on Business Informatics. IEEE, 2013, pp. 93-100.

[7] D. Lei, K. Zhou, H. Jin, J. Liu, and R. Wei, "Sfds: A security and exible data sharing scheme in cloud environment," in 2014 International Conference on Cloud Computing and Big Data. IEEE, 2014, pp. 101-108.

[8] R. T. de Souza and S. D. Zorzo, "Privacy-preserving mechanism for monitoring sensitive data," in 2015 12th International Conference on Information Technology-New Generations. IEEE, 2015, pp. 191-196.

[9] K. Popovi¢ and š . Hocenski, "Cloud computing security issues and challenges," in The 33rd International Convention MIPRO. IEEE, 2010, pp. 344-349.

[10] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 1, no. 2, pp. 136-146, 2011.

[11] S. K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831-1838, 2012.

[12] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. Buyya, "Cloudsim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," Software: Practice and experience, vol. 41, no. 1, pp. 23-50, 2011.

[13] P. Ora and P. Pal, "Data security and integrity in cloud computing based on rsa partial homomorphic and md5 cryptography," in 2015 International Conference on Computer, Communication and Control (IC4). IEEE, 2015, pp. 1-6.

[14] S. More and S. Chaudhari, "Third party public auditing scheme for cloud storage," Procedia Computer Science, vol. 79, pp. 69-76, 2016.