IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. V (May - June 2017), PP 23-27
www.iosrjournals.org

Data Integrity Verification in Cloud Computing

Gaurav Gupta[1*], Prof.(Dr.) Naveen Hemrajani[2], Ajay Kumar[3]

[1]*Gaurav Gupta, M.tech scholar, JECRC University, Jaipur, Rajasthan state, India.*
[2]*Prof.(Dr.)Naveen Heamrajani, HOD CSE, JECRC University Jaipur, Rajasthan State, India.*
[3] *Ajay Kumar, Asst. Prof., JECRC University Jaipur, Rajasthan State, India.*
Correspondence address: Department of CSE, JECRC University Jaipur, India.*

***Abstract**: Cloud computing is recognized as a hottest technology which has a significant impact on IT field in the nearby future. Cloud computing is an Internet based computing. It provides the services to the organizations like storage, applications and servers. Cloud computing is on demand and pay per use service. That means customers pay providers based on usage. Data Integrity is the major issue in cloud computing. To provide the integrity various methods have been proposed by the researchers. In this paper we will proposed a model which will provide the data integrity using Elgamal Algorithm and SHA-2 Algorithm. The Proposed model shows that the data which is uploaded on cloud is secured if the hash key matches with the local keys which are stored on the system.*

***Keywords:** cloud computing; data integrity; pay per use model*

I. Introduction

Cloud Computing is considered as most demanded technology by the customers because of its various advantages like scalable, pay per use model, on demand access to the resources.**[1]** Cloud Computing provides the interaction between user and cloud servers via the service layers which are mentioned in cloud computing architecture such as: 1) Software as a service (SaaS) which provides a application as a service but user is not allowed to make any changes in to this service. SaaS providers of cloud services are Google Apps, Salesforce.com and Sql Azure. 2) Platform as a service (PaaS) which provides a platform to so that customer can put their application on cloud platform. In this user can’t make any changes to the cloud platform but they can control their applications. 3) Infrastructure as a service (IaaS) Infrastructure have set of hardware, software, storage devices and CPU cycle and other components that allows consumers to use these services and components, here the user has full control over the infrastructure means they can modify it. **[2]**

Cloud computing offered three deployment models public or private or combination of both, 1) Public Cloud: This can be a common computing model the place the computing infrastructure may also be shared between businesses. Public cloud provider may be free or provided as pay-per usage, 2) Private Cloud: Computing architecture is committed to the client and isn't shared with other businesses and managed internally or via a third-social gathering and hosted internally or externally, 3) Hybrid Cloud: Hybrid cloud is a composition of two or more clouds (personal, community, or public) which can be collaborate collectively, offering the benefits of multiple deployment items.**[3]**

Cloud computing is gathering traction with businesses, and in order to take advantage fully from this new computing paradigm heightened security threats must be overcome. The cloud security Alliance is a non-profit consortium that seeks to promote the best practices for providing security assurance within the cloud computing environment. The Cloud Security Alliance identifies nine security issues found within the cloud. They are: Data Breaching, Data Loss, Service Traffic Hijacking, Insecure Interfaces and APIs, Denial of service, Malicious Insider, Cloud abuse, Insufficient due diligence and Shared technology vulnerabilities.

Security requirements will aide when analyzing or developing any solution, and also when describing the security offered. Moreover, it was emphasized that when describing the possible threats to data in the cloud two perspectives must be taken into account: a) the users; and b) the CSP. This emerged as data is either in the cloud or not in the cloud. Thus the security requirements will be the responsibility of: a) the user; b) the CSP; or c) of both the user and the CSP. This shall be addressed for each security requirement presented. **[3]**

1. Confidentiality: Confidentiality ensures that knowledge shouldn't be disclosed to unauthorized humans. Confidentiality loss occurs when data can be read or observed through any members who are not authorized to access it.

2. Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the basic idea that when a user tries to access something, it is available to be accessed.

3. Integrity: Integrity ensures that data held in a system is a proper depiction of the data intended and that it has not been modified by an authorized person. When any application is running on a server, to make it safe in the event of a data-loss incident a backup routine is configured.**[4]**

DOI: 10.9790/0661-1903052327

This paper describes the issue of data integrity verification of the data which is uploaded on to the cloud. When user retrieves the data from the cloud integrity has been checked. If there is any tampering with the data hash key would not matched with the local hash keys else the data is not tampered i.e. integrity has been achieved.

II. Material and Methodology

whenever it comes to the security there are three major issues those issues are Data Integrity, confidentiality and availability. These three issues are applied to all kind of data either they are stored on cloud or locally. There are lot of methods have been proposed by the researcher to provide data integrity. One of the method is proposes cloud architecture which ensures secure data transmission from the client's organization to the servers of the Cloud Service provider (CSP). In this, combined approach of cryptography and steganography is used because it will provide a two-way security to the data being transmitted on the network. First, the data gets converted into a coded format through the use of encryption algorithm and then this coded format data is again converted into a rough image through the use of steganography. Steganography also hides the existence of the message, thereby ensuring that the chances of data being tampered are minimal.**[5]**

Another architecture based model that provides data integrity verification and privacy preserving in cloud computing. This model has presented an effective mechanism that provides data integrity verification without allowing third party to violate the privacy of data. AES and MD5 algorithms are used for data integrity and privacy are ensured against unauthorized parties.**[6]**

Proposes a new technique in order to ensure the confidentiality of data in network. The author has used two approaches encryption and Obfuscation. On the basis of data type, these 2 approaches are used i.e. on characters encryption is used and on numbers obfuscation is used. This will provide more protection against the un-authorized access.**[7]** Here the author reflects on security in cloud computing. As cloud computing provides Internet-based services. Since the growth of the Internet is increasing rapidly. Hence cloud computing leads to the vision of the Internet as a supercomputer. There are many techniques for protecting user data outside attackers. Currently there is no effective way to protect confidential data from users of the service providers of cloud computing. In this paper, the author presents a new approach to protect the confidentiality of data in the cloud computing. In this paper, the author considers the protection of the confidentiality of the attackers outside the cloud computing systems.**[8]**

Describes one new approach is defined named Trusted Cloud Computing Infrastructure (TCCI) which is based on Infrastructure security. TCCI approach describes that different nodes are required to run on secure environment so to keep hackers away. Moreover, if node runs in a secure environment than even administrator is incapable of access the user data. To make the infrastructure secure TCCI approach is proposed which handles the nodes by third party known as Trusted Coordinator (TC).**[9]**

In this paper to share the important data in public cloud securely mediated certificate less encryption scheme is used. This method is used to solve the problem of escrow in identity based and revocation in public key. In this paper they create public cloud environment and then implement above scheme for data in cloud. The key that are created saved to the cloud. For decryption user authenticate itself on cloud. Then cloud decrypts some part of encrypted data. After that it decrypts the all data through private key.**[10]**

They came up with the literature survey describing the evaluation of the context of research and the problems discussed in them. Based on these what process were used in them, but whether they are justified or not, if condition satisfies, can there be more furtherance in them. They proposed a new governance, risk management and compliance store for cloud computing i.e. cloud security alliance.**[11]**

Enhancing data dynamics and storage security for cloud computing using Merkle hash tree and AES algorithms" according to this paper auditing the data on cloud server is necessary to prevent data integrity and assure the client safety of data. Whatever data is stored on cloud is altered by the client only. Most of the cloud providers support data auditing only for the static data so the dynamic data auditing is another problem. As we know that it's not feasible to download entire data file from server and check the integrity of the data file as it's not the one time process.**[12]**

Proposed Model This model is designed to achieve data integrity verification. To improve the data integrity two encryption algorithms are applied to every transaction of data upload and download being carried out. These algorithms are Elgamal and SHA-2 algorithm. Elgamal algorithm is used to encrypt the clients data which is going to store on cloud and SHA-2 is used to encrypt the keys.

This model consists of four main component that interacts with each other to provide data integrity. These components are:

1. Client application machine: This component shows the fully trusted local machine. It represents the implementation of algorithms used for data integrity verification.

2. Key: A key is stored on local machine and when the data is downloaded we need to match the keys. If the local key matches with the generated key we can say that the data is secured.

3. Integrity checking: This is the main feature of this model as it allows the user to check the integrity of the data stored on the cloud.

4. Virtual cloud environment: In this cloudsim is used to create the virtual cloud environment.

To solve the problem of security in cloud computing two way techniques are deployed for preventing security breaches on cloud computing. Data Hiding Architecture is used for securely transmitting the data over the cloud environment.

1. Data hiding Architecture: To keep the data secure from attackers on the network, data is encrypted using Elgamal algorithm before sending to cloud environment.

2. Maintaining the integrity of the data by using the hash codes. Matching of hash code at the user end and at the server end will help us to ensure the integrity of the data.

3.1. Proposed System: The actual functionality of the proposed solution and detailed execution of the solution is shown below in flow chart-

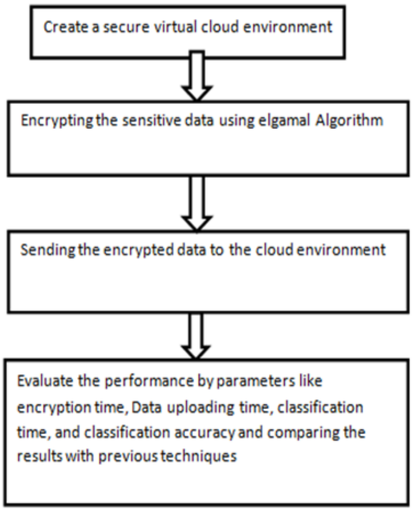
Create a secure virtual cloud environment
Encrypting the sensitive data using elgamal Algorithm
Sending the encrypted data to the cloud environment
Evaluate the performance by parameters like encryption time, Data uploading time, classification time, and classification accuracy and comparing the results with previous techniques

Fig. 1 Proposed System Design

Implementation: The virtual Cloud environment is created on local machine using cloudsim. Cloudsim is also used to store the data on virtual cloud. This virtual environment is created on clients local machine. Once the cloud environment is created the client decrypts the data and sends it on the cloud. The hash value is also calculated by the client before the data is sent for storage on virtual cloud. To check the integrity of the data one set of key is stored on the local machine. If the local key matches with the generated keys it means the integrity is maintained.

Performance Parameter: There are two performance parameters evaluated, encryption time parameter and decryption time parameter. In which we measure the time, that how much time data taking during uploading according to data and measure the time while decrypting.

Encryption time: Multiple files of different size have been used to calculate the encryption time. To perform this operation various file size have been uploaded on cloud.

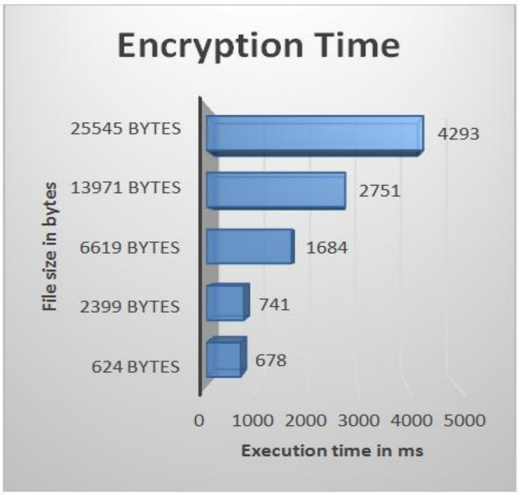

Fig. 2 File size V/s Encryption Time

File Uploading Time: Multiple files of different size have been used to calculate the encryption time.. To perform this operation various file size have been uploaded on cloud.

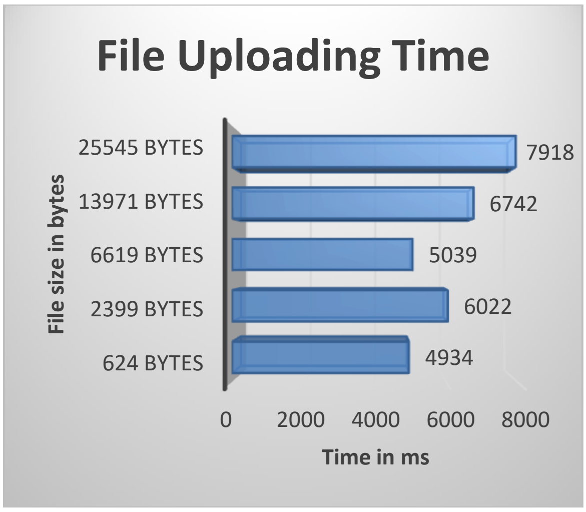

Fig. 3 File size V/s uploading time

Processing Cost: Multiple files have been used to calculate the cost of different file size. In general view if file size increases process cost will automatically increases as show in below graph-

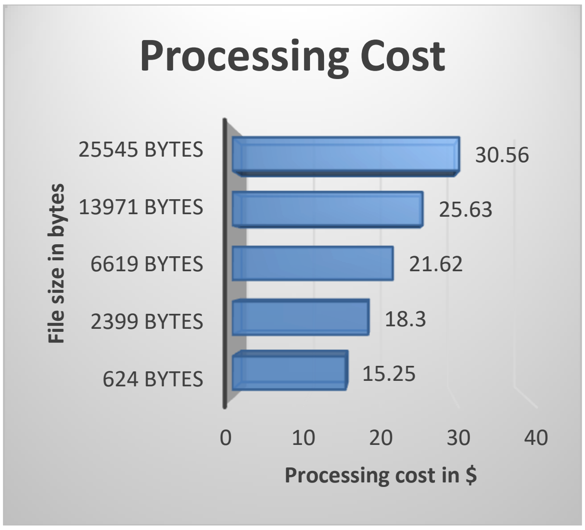

Fig. 4 File size V/s processing cost

III. Conclusion and Future Work

Thus the security of sensitive data on cloud environment is achieved using SHA2 and elgamal algorithm. Elgamal algorithm is used to encrypt the message before sending it on cloud. This scheme also solves the problem of the key escrow and revocation problem. To create virtual cloud environment the cloudsim simulator is used. Before storing or uploading the important data to the cloud environment that data is encrypted. The Private Key that generated on cloud also encrypted using SHA algorithm before storing the data. After encryption process the encrypted keys and the data saved on the cloud.

In future, security can be extended to have multiple files on cloud environment and cryptographic techniques can be combined with some steganography techniques.

Acknowledgment:

The authors would like to acknowledge the support rendered by JECRC University, Jaipur. we would also thankful for all those who have supported us for this research.

References

[1] Sarvan Kumar, R. and A. saxena.2011 Data integrity proofs in cloud storage in communication system and network, third international conference.

[2] Subhashini S. and V. Kavitha. 2011. A survey on security issue in service delivery models of cloud computing, journal of network and computer application.

[3] Nepal S.2011. data integrity as a service in cloud computing, IEEE.

[4] S. Mahdi Shariati, Abouzarjomehri, M. Hossein Ahmadzadegan.2015.Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection. 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 1078 - 1082.

[5] A. Dhamija and V. Dhaka. 2015. A novel cryptographic and steganographic approach for secure cloud data migration. International Conference Green Computing and Internet of Things (ICGCIoT), pp. 346–351.

[6] M. F. Al-jaberi and A. Zainal. 2014. Data Integrity and Privacy Model in Cloud Computing. International Symposium on Biometrics and Security Technologies (ISBAST), pp. 280–284.

[7] L. Arockiam and S. Monikandan.2014.Efficient cloud storage confidentiality to ensure data security. International Conference on Computer Communication and Informatics (ICCCI -2014), pp. 1–5.

[8] S. K. Abd, S. A. R. Al-Haddad, F. Hashim, and A. Abdullah.2014. A review of cloud security based on cryptographic mechanisms. International Symposium on Biometrics and Security Technologies (ISBAST), pp. 106–111.

[9] H. Banirostam and a Hedayati. 2013. A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure. UKSim 15th International Conference on Computer Modelling and Simulation, pp. 717–721.

[10] Seo, S.H.; Nabeel, M.; Ding, X.; Bertino, E. 2013. An efficient certificateless encryption for secure data sharing in public clouds. IEEE Knowledge and Data Engineering, pp. 2107-2119.

[11] F. B. F. Shaikh and S. Haider, “Security threats in cloud computing. 2011. International Conference for Internet Technology and Secured Transactions (ICITST), pp. 214–219.

[12] Poonam M. Pardeshi and Deepali R. Borade. 2014. Enhancing data dynamics and storage security for cloud computing using Merkle Hash tree and AES algorithms. International Journal of Computer Application, vol. 97, July.