A Survey Paper on Algorithm for Securing Outsource Data in Cloud

[1]Honey Patel, [2]Jasmine Jha
[1]M.E. Information Technology, Assistant Professor
L.J. Institute Of Engineering & Technology , Ahmedabad, INDIA
[1]Patel1111honey@gmail.com , [2]jhajasmine@gmail.com

***Abstract*— Cloud computing is recommended as a promising technology, which delivers computational facilities as services to users over the Internet. As well as, the cloud computing brings significant risks for greater exposure to data security when users outsource sensitive data for sharing on cloud servers. To keep sensitive data confidentiality against untrusted cloud service provider. it employs double cryptographic methods to limit authorized users accessing updated cloud data with expired keys. Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites. Since Cloud Computing share distributed resources via network in the open environment thus it makes security problems.In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system.In this paper To store object over cloud with homomorphic encryption technique with Elgamal Algorithm that provide data confidentiality in cloud..Finally Apply this encryption method in Amazon S3.**

Keywords - Cloud computing, Data Security, Amazon S3, Homomorphic Encryption, Elgamal

I. INTRODUCTION

Cloud computing is a natural evolution of the widespread adoption of virtualization service, service- oriented architecture (SOA), autonomic, and also utility computing. Cloud computing is the broader concept of infrastructure convergence. This results in reduced cost of the services. Quality of services also gets better as the organization can spend the saved amount and time on improving it . In cloud computing environment, resources are shared among all of the servers, users and individuals . As a disarray invention with foreseen implication, cloud computing is mending way it uses business with IT . Security and Privacy issues are of more concern to cloud service providers who are actually hosting the services. Cloud computing models are of two types: Deployment model and Service model. Deployment model is further classified into four type's namely public cloud, hybrid cloud, private cloud and community cloud. Cloud computing service providers provide their services in a number of fundamental models. Cloud computing is a term which is often used with synonyms like grid computing; cluster computing, autonomic processors together with the software as a service and computing architecture are transforming data centre into pools of computing service on a huge scale[1].

Cloud computing is an emerging technology aimed at providing various computing and storage services over the Internet. It generally incorporates infrastructure, platform, and software as service. Cloud service providers rent data- center hardware and software to deliver storage and computing services through Internet. By using cloud computing, Internet users can receive services from a cloud as if they were employing a super computer. They can store their data in the cloud instead of on their own devices, making ubiquitous data access possible. They can run their applications on much more powerful cloud computing platforms with software deployed in the cloud, mitigating the users' burden of full software installation and continual upgrade on their local devices. However, the cloud computing provides more opportunities to develop more services as well as significant risks for greater exposure to data security when users outsource sensitive data for sharing on cloud servers, which are not trusted for data owners.

II. Basic Cloud computing architecture

A. Cloud computing service models[5]

- Cloud Software as a Service (SaaS): Application and Information clouds, Use provider's applications over a network, cloud provider examples Zoho,Salesforce.com, Google Apps.
- Cloud Platform as a Service (PaaS): Development clouds, Deploy customer-created applications to a cloud, cloud provider examples Windows Azure, Google App Engine, Aptana Cloud.
- Cloud Infrastructure as a Service (IaaS): Infrastructure clouds, Rent processing, storage, network capacity, and other fundamental computing resources, Dropbox, Amazon Web Services, Mozy, Akamai.

B. Cloud computing deployment models[5]

- Private cloud: Enterprise owned or leased
- Community cloud: Shared infrastructure for specific community

- Public cloud: Sold to the public, mega-scale infrastructure
- Hybrid cloud: Composition of two or more clouds

C. Cloud computing sub-services models[5]

- IaaS: DataBase-as-a-Service (DBaaS): DBaaS allows the access and use ofa database management system as a service.
- PaaS: Storage-as-a-Service (STaaS): STaaS involves the delivery of data storage as a service, including database-like services, often billed on a utility computing basis, e.g., per gigabyte per month.
- SaaS: Communications-as-a-Service (CaaS): CaaS is the delivery of an enterprise communications solution,such as Voice over IP, instant messaging, and video conferencing applications as a service.
- SaaS: SECurity-as-a-Service (SECaaS): SECaaS is the security of business networks and mobile networks through the Internet for events, database, application, transaction, and system incidents.
- SaaS: Monitoring-as-a-Service (MaaS): MaaS refers to the delivery of second-tier infrastructure components, such as log management and asset tracking, as a service.
- PaaS: Desktop-as-a-Service (DTaaS): DTaaS is the decoupling of a user's physical machine from the desktop and software he or she uses to work.
- IaaS: Compute Capacity-as-a-Service (CCaaS) CCaaS is the provision of "raw" computing resource, typically used in the execution of mathematically complex models from either a single "supercomputer" resource or a large number of distributed computing resources where the task performs well.

D. Cloud computing providers

Amazon Web Services (AWS) -include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others. Salesforce.com - Delivers businesses over the internet using the software as a service model. Google Apps - Software-as-a-service for business email, information sharing and security. And others providers such as Microsoft Azure Services Platform, Proof-point, Sun Open Cloud Platform, Workday and etc ....

III .Homomorphic Encryption

Input File come to the store over cloud. This file 1st encrypted with the help of homomorphic technique. For that Elgamal Algorithm will use. Then the encrypted object will store over cloud.

When the data transferred to the Cloud we use standard encryption methods to secure the operations and the storage of the data. Our basic concept was to encrypt the data before send it to the Cloud provider. But the last one needs to decrypt data at every operation. The client will need to provide the private key to the server (Cloud provider) to decrypt data before execute the calculations required, which might affect the confidentiality and privacy of data stored in the Cloud. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data[9].

Homomorphic encryption is a form of encryption. It allows users to perform specific algebraic operations on ciphertext and still get ciphertext as the result, which is as if the same operations are carried out on the corresponding cleartext and then the result is encrypted, since the two results would be the same.

The definition of Homomorphic encryption can be described as: Let E denotes the encryption operation, m be the plaintext, and e be the corresponding ciphertext, i.e. $e = E(m)$,then $m = E^{-1}(e)$. Given there is an operation f for plaintext, if we can construct a corresponding function F for E such that $F(e) = E(f(m))$, then E is a homomorphic encryption algorithm over f. An encryption algorithm may have the following attributes:

Additive homomorphism: it exists if $E(x+y)$ can be obtained by adding $E(x)$ and $E(y)$ without knowing the values of x and y.

Multiplicative homomorphism: it exists if $E(x \times y)$ can be obtained by multiplying $E(x)$ and y without knowing the value of x.

Full homomorphism: it exists if for an encryption algorithm the corresponding operations for both addition and multiplication can be found, that is both $E(x+y)$ and $E(x \times y)$ can be obtained by operating on $E(x)$ and $E(y)$ without knowing the values of x and y.

In this work, we use additive homomorphism [9]. Let M be plaintext, C be ciphertext, P and Q be two big random primes, $N=P \times Q$, and $\mathbf{R}$ be a random number, then the encryption formula is $C = (M+R \times P) \bmod N$, and the decryption formula is $M = C \bmod P$. The proof of the additive homomorphism is given below.

Assuming there are two plaintexts $M1$ and $M2$, we encrypt them using the above encryption formula to obtain[8]:

$$C1 = E(M1) = (M1 + P \times R1) \bmod N$$
$$C2 = E(M2) = (M2 + P \times R2) \bmod N$$

Then, for the ciphertexts $C1$ *and* $C2$, , we can obtain:

$$C3 = C1 + C2 = (M1 + M2 + P \times (R1 + R2)) \bmod N$$

Next, decrypt $C3$ using the above decryption formula:

$$M3 = C3 \bmod P = ((M1 + M2 + P \times (R1+R2)) \bmod N) \bmod P = M1 + M2$$

Therefore, we have proved that ***C3*** = ***E (M1 + M2)***, which can be obtained by adding ***E (M1)*** and ***E (M2)*** without knowing the values of ***M1*** and ***M2.***

Elgamal Algorithm[12]:

1. Get the File f to be stored on cloud.
2. Call elgmal_encryption( )
   a. Generate Keys.
   b. If (flength< p)then
      E(f) ← encrypt the file Elgmal(f)
   else
      fpart[x] ←create_file_partion( )
      E(fpart[x] ←encrypt each fpart[x]

   Concate each part to single fileE(f) ← E(fpart[0])+E(fpart[1])+…….+E(fpart[n])
3. Upload E (f)to cloud.

IV.Literature Survey

Cloud computing security challenges and issues discussed various researchers. The Cloud Computing Use Cases group discusses the different use case scenarios and related requirements that may exist in the cloud computing model. They consider use cases from different perspectives including customers, developers and security engineers.The cloud computing via a win-win solution by delivering **multi-tenancy** and **elasticity**[2]. Both have serious implications on the Cloud model security.

The virtualization security research area was a concern even before the cloud computing era. Research in this area can be categorized into: Traditional Security Solutions in the Cloud, Virtualization-Aware Security Solutions, Micro Hypervisors; and Hypervisor-Level Protection. The cloud virtual infrastructure is very complex and dynamic. In addition, the huge amount of traffic and workload flowing inside each physical server increases the complexity of the protected environment. The virtual architecture of the cloud erases many of the physical boundaries that are traditionally used in defining, managing and protecting organizations' IT assets, leading to a very complex virtual architecture. Adapting security solutions in the cloud environment to protect cloud virtual infrastructure is a real challenge and requires key characteristics to be addressed in order to deliver the accurate and pre-emptive protection. Our research is focusing on developing a new virtualization-aware security solution that can meet our research challenges and have the ability to defend the cloud virtual infrastructure different layers (including VMs, vSwitch and Hypervisor) against zero-day threats[3].

There is a huge number of publications on cloud security issues .In this section we concentrate on some attack on cloud computing.[4] describe the flooding attack in a cloud system. In this how adversary has achieved the authorization to make a request to the cloud, and create bogus data and pose this request to the cloud server. Result engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system. proposed approach is to organize the entire server in the cloud system as a group of fleet of servers. Hypervisor can be utilized for the Scheduling among fleets. PID can be appended in the messaging, which will justify the identity of the legitimate customers. Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment.We will focus on specific problems for various kinds of attack in the cloud: Denial of service (DOS) attack, fingerprinting attack, unauthorized user attack. We describe each of these security issues in cloud system and find out their basic causes. The propose method to mitigate such attacks to ensure the integrity and security of cloud systems.

In contrast to traditional solutions[5],Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges which have not been well understood. In cloud computing, both data and software are fully not contained on the user's computer; Data Security concerns arising because both user data and program are residing in Provider Premises. Clouds typically have a single security architecture but have many customers with different demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. This paper investigates the basic problem of cloud computing data security. We present the data security model of cloud computing based on the study of the cloud architecture. We improve data security model for cloud computing. We implement software to enhance work in a data security model for cloud computing. Finally apply this software in the Amazon EC2 Micro instance. We see that Amazon EC2 provider must use AES to ensure the most security in user data.

Effective Privacy Protection Scheme (EPPS)[6] is proposed to provide the appropriate privacy protection which is satisfying the userdemand privacy requirement and maintaining system performance simultaneously. At first, we analyse the privacy level users require and quantify security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data. Finally, the simulation results show that the EPPS not only fulfills the user-demand privacy but also maintains the cloud system performance in different cloud environments. The execution result of EPPS outperforms other security schemes by 35% to 50%. A feasible solution for data protection is data encryption. Encryption algorithm offers the benefit of minimum reliance on cloud provider. Thus, users' data can migrate from one provider to another provider without limiting to the specific provider. Furthermore, encryption algorithm protects data no matter where is

its physical location.Unfortunately,when performing the encryption algorithm, it often consumes a lot of system resources, such as CPU utilization, and stronger algorithm that generates more significant impact to the system performance. The tradeoff between security and system performance become an important issue when applying an encryption algorithm in cloud environment.

The cloud computing brings significant risks for greater exposure to data security when users outsource sensitive data for sharing on cloud servers. To keep sensitive data confidentiality against untrusted cloud service provider, Discusses this challenging open issue using re-encryption scheme in outsourced cloud data. On the one hand, it allows the data owner to delegate most of the computation tasks to untrusted cloud servers providers without the need to have knowledge of the underlying plaintexts[7]. On the other hand, it employs double cryptographic methods to limit authorized users accessing updated cloud data with expired keys.Also obtains the restrictions of choosing appropriate encryption algorithm to establish secure re-encryption scheme in cloud data services.

V .Conclusion

Security analysis of cloud data service mostly put emphasis on the security analysis of the encryption algorithm and key management, but not on the re-encryption scheme. Data privacy is a very important target of security assessment in the field of cloud service, which has direct relation to trustworthy degree of CSP. The Security of Cloud Computing based on Homomorphic Encryption is a new concept of security which is enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data.

VI.References

[1] Boopathy D,M.Sundaresan,"Data encryption model with watermark security for data storage in public cloud model" 2014 Fourth International Conference on Communication Systems and Network Technologies

[2] Mohamed Al Morsy, John Grundy and Ingo Müller," An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010

[3] Amani S. Ibrahim, James Hamlyn-Harris and John Grundy," Emerging Security Challenges of Cloud Virtual Infrastructure ", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010

[4] Rajkumar R chalse,Arun katara,Ashwin Selok,Roshni Talmale"Inter Cloud Data Transfer Security", 2014 Fourth International Conference on Communication Systems and Network Technologies

[5] Eman M.Mohamed,Hatem S. Abdelkader," Enhanced Data Security Model for Cloud Computing", The 8th International Conference on INFOrmatics and Systems (INFOS2012)-14-16 May Cloud and Mobile Computing Track

[6] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo," An Effective Privacy Protection Scheme for Cloud Computing", ISBN 978-89-5519-155-4 Feb. 13~16, 2011 ICACT2011

[7] Lizhi Xiong, Zhengquan Xu,"Re-encryption security model over outsourced cloud data" ,2013 International Conference on Communication Systems and Network Technologies

[8] Yingming Zhao, Yue Pan, Sanchao Wang, and Junxing Zhang," An Anonymous Voting System Based on Homomorphic Encryption " Inner Mongolia University, School of Computer Science, Huhhot, China

[9] Maha TEBAA, Said EL HAJII,"Secure Cloud Computing through Homomorphic Encryption"

[10] http://www.tutorialspoint.com/cloud_computing/cloud_computing_architecture.htm

[11] http://www.ieee.org

[12] https://cmsc414.wordpress.com/2009/09/23/el-gamal-examples/