ISSN:0975-9646

A Security Architecture of Cloud Computing for Business applications

Sreeja S , Chithra P,Jesna jose

Department Of Computer Science, Sree Buddha College of Engineering
Sree Buddha College of Engineering, Pattoor
Alappuzha(Dist), Kerala

Abstract: **Cloud computing is internet based computing in which it provides on demand access of resources and services at lower cost. It is very necessary to consider security, privacy and integrity when designing and using cloud services because both user data and programs are resides in the cloud service provider premises. Integrity checking becomes imperative to secure data in a cloud environment. It is important to ensure that the stored data is neither compromised nor corrupted. Many of existing protocols reveals client's sensitive data by sharing the encryption and decryption keys with the cloud server. The proposed work draws conceptual cloud architecture by adopting a hybrid encryption/decryption system algorithm to ensure the security and doesn't compromise any information with the cloud server. It involves a third party called privacy manager who encrypts the clients' information for ensuring the security. It then generate the hash value of the encrypted data, store and manage these details for verification purpose. This paper provides data integrity and user privacy through Privacy Manager.**

Keywords- Data Storage, Cloud Computing

I. INTRODUCTION

In recent years, cloud computing has become a hot topic in the global technology industry. The U.S. National Institute of Standards and Technology (NIST) [3] have put an effort in defining cloud computing. The NIST definition of cloud computing is (NIST 2009a): Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

In the context of cloud computing, the cloud service provider is known as cloud provider which is an organization that provides cloud computing service. On the other hand the organization that receives the cloud computing service is known as the cloud customer. It is an increasing concept because of several reasons including reduction in cost and energy consumption of the shared computing resources (servers, software, storage, and networking) [12]. It also enables effective IT resources usage and increases flexibility for expanding new infrastructures in instant time [12].

Like traditional computing environments, cloud computing brings risks and security concerns to the business that need to be considered appropriately. Such risks and security concerns include challenges in handling privileged user access, ensuring legal and regulatory compliance, ensuring data segregation, maintaining data recovery, difficulty in investigating illegal activities, and lack of assurance of long-term viability of the cloud provider [3].

This paper deeply describes the Cloud computing security mechanisms. The proposed system support scalable and efficient auditing in the Cloud Computing without any third party auditor. The proposed system consists of a privacy manager. The privacy manager acts as an interface between cloud storage server and client. Request handling and Integrity Checking is also done by this Privacy manager.

II. RELATED WORK

In cloud computing environment the data are outsourced. The biggest concerns about Cloud are security and privacy. Common methods for protecting user data are

- Authentication procedures prior to storage or retrieval
- Building secure channels
- Encryption prior to storage

In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, administrative access must now be conducted via the Internet, this increasing exposure and risk .So it is necessary to apply some security measures to protect the privacy of the organizations data. The traditional cryptographic technologies for data integrity and availability, based on hash functions and signature schemes, they cannot work on the outsourced data without a local copy of data.

Wang et al.[5] proposes a model that enable privacy-preserving third-party auditing protocol .In this model the clients can ask an external audit party to check the integrity of their outsourced data. But the audit demands retrieval of user's data; this is not privacy-preserving and the communication and computation complexity increases with the size of data .And here the cloud system is responsible for both tasks on storage and encryption/decryption of data. So it is very easy to obtain both the decryption key and cipher text and their by encrypting the data by an authorized person inside the service provider.

Sravan kumar et al. [11] modeled a method of proof for checking the correctness of user's sensitive data by adopting the use of Meta data. Meta data is created using randomly selected bits from original data file and is appended in an encrypted form to be stored on cloud. Whenever verifier wants to check integrity, he throws a challenge by specifying block number and its corresponding Meta data and finally decrypted for proof of correctness.

In 1991, Philip Zimmermann develops a Pretty Good Privacy (PGP) [8] computer program for ensuring cryptographic privacy and authentication. While in 1998, the Internet Engineering Task Force (IETF) created the open PGP Standard in which the Standards develop helps to run Internet. Open PGP is a computer program which developers a framework for combining different widely algorithms for ensuring security and privacy into a secure system. This open PGP Standard published by IETF is in form of Request of Comment (RFC). Open PGP combines symmetric and asymmetric algorithms together to formulate a security model.

III. PROPOSED SYSTEM

Nowadays not just large organizations, but even small and medium size businesses are looking forward to adopt an economical computing resource for their business application, i.e. by introducing a new concept of cloud computing in their environment. Cloud computing improves organizations performance by utilizing minimum resources and management support, with a shared network, valuable resources [3] bandwidth, software's and hardware's in a cost effective manner and limited service provider dealings.

Basically it's a new concept of providing virtualized resources to the consumers. Consumers can request a cloud for services, applications, solutions and can store large amount of data from different location. But due to constantly increase in the popularity of cloud computing there is an ever growing risk of security becoming a main and top issue.

This paper proposes a backup plan required for overcoming the security issues in cloud computing. In a cloud computing, the business operation can be leased from a single service provider. While the data related to the business operation can be stored on the equipment by the same service provider. But storing the company's data on the equipment the increases risk factor of leaking the information [7]. This raises the disclosure of the data internally.

While doing research, of the researches have suggested that the data should be encrypted before storing on service provider equipment [10]. When the data is encrypted and stored in the equipment which helps in protection and firewalls are used in order to make surety that decryption keys associated with encrypted user are disclosed to outsiders.

This paper introduces a hybrid cryptographic approach which combines the advantages of both Symmetric and Asymmetric encryption techniques; this technique improves both security and privacy of the data. The integrity of data is the main concern, for that a hash function is generated for each block of data .It is a fast mechanism and not so complex communication to verify the integrity of data. This facility is provided by the Tag generator at the Privacy manager in order to show the client that his data is retrievable without any loss or corruption.

IV. SYSTEM DESIGN

The proposed system comprised of three entities, a trusted third party called a Privacy manager, clients and cloud storage service providers as shown in figure 4.1

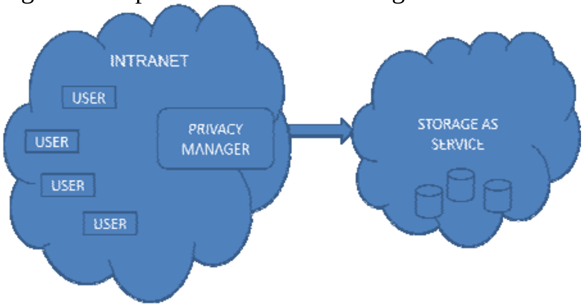

Figure 4.1 Proposed System Architecture

Clients of the cloud may be individual customers and any organization that have data to be stored in the cloud and rely on the cloud for data computation and its security maintenance. Mainly they store encrypted data in the remote server and to ensure security it queries the data through the privacy manager for integrity checking.

The *storage servers* provide significant resources and expertise in managing cloud storage servers. It stores client's sensitive data in encrypted form and is considered to be un-trusted entities.

The *Privacy manager* acts as an interface between cloud storage server and client. Request Handling and Integrity Checking is done at this side. It is considered to be a trusted entity to assess and expose risk of cloud storage services on behalf of the clients upon request. The Privacy manager entity comprised of an authenticator, encryptor, decryptor, Tag generator, and verifier .

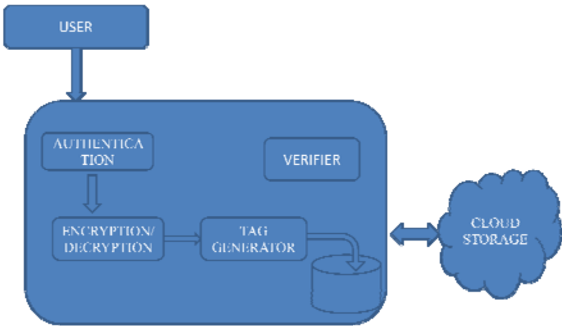

Figure 4.2 Privacy manager

PRIVACY MANAGER

The privacy manager for cloud computing reduces the risk to the cloud computing user by preventing by their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. Privacy manager does the main operation while the client transmitting the data to the cloud Server. It consists of functionality like,

- Authentication
- Encryptor/decryptor
- Tag generator
- Verifier

Authenticator

For all of the enterprises, the management of user's account and their corresponding authorized access privilege is very important and must be strictly defined. Through the implement of Identity and Access Management (lAM), every enterprise could easily establish a managing mechanism to achieve the goal of user identification, authentication, and authorization simultaneously. In this paper three Factor authentication [9] techniques is used to ensure authorized access of data. The three factors are

Something the client knows: password.

Something the client has: smart card.

Something the client is: biometric characteristics (e.g., fingerprint, voiceprint, and iris scan).

Three-factor authentication is introduced to incorporate the advantages of the authentication based on password, smart card, and biometrics. A well designed three-factor authentication protocol can greatly improve the information assurance in Cloud computing system

Encryptor/Decryptor

In this paper a hybrid cryptographic system like PGP is used. This hybrid cryptographic system combines symmetric and asymmetric algorithms together to formulate a security model. This helps in protecting the data and doesn't affect the performance of the system. In symmetric algorithms, while encrypt and decrypt the data the same key is used. Figure 4.3 shows the working of Encryption /Decryption system

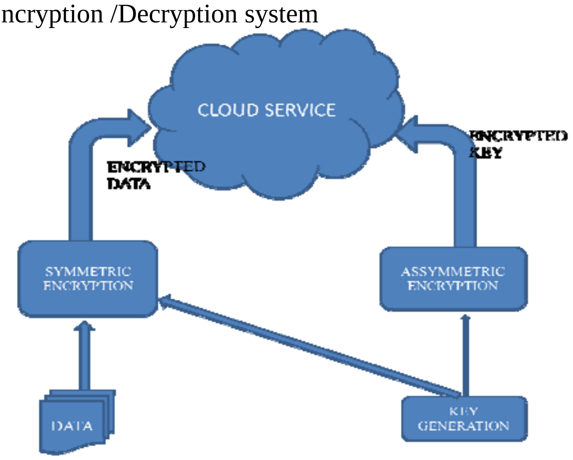

Figure 4.3 Encryption/Decryption system

Here both symmetric encryptions like AES for encrypting data and asymmetric encryption like RSA (Rivest-Shamir_Adleman) to encrypting the keys for encrypted data used by AES. Asymmetric Encryption is better than symmetric encryption for performing encrypt the data and simplifies key management. But comparatively it is slower than symmetric encryption. So this combination of Symmetric and asymmetric hybrid approach i.e. fast process of encrypt data symmetric algorithm and comparatively slow process of asymmetric encryption algorithm only for encrypt keys helps to attain high level of granularity and to encrypt data efficiently. Data in the cloud can be protected separately with symmetric key and those keys will be managed through asymmetric key. The user keeps the asymmetric keys in a key ring which one is the single point of access control to the whole system.

The user Id is very important while encrypting or decrypting the data as this cloud service provider mainly serve multiple users. So that unique user Id is stored with the keys on the same place. So this user Id is later used as an identifier to get the decrypted data key. This key is also stored on the same cloud which will later help while decrypting data whenever user required. After this the Encryption or decryption cloud service provider will sent the encrypted data to the Tag generator.

Tag Generator

The client before storing its data file the Privacy manager should process it and create suitable Meta data which is used in the later stage of verification. When checking for data integrity the client queries the cloud storage for suitable replies based on which it concludes the integrity of its data stored in the client .The encrypted data are then given to the tag generator to generate the hash key for those segments.

Hash value of the encrypted segment is generates with SHA algorithm as follows.

Hash value=SHA (encrypted segment)

The details like the identity of client's file, hash key generated for those encrypted segments are stored in the database, which is managed by the database manager. These details are required for the integrity checking of the clients' information which is managed by the privacy manager.

Verifier

Data integrity is one of the important aspect of cloud computing. Maintaining data integrity in the cloud is a major challenge that is faced by today's cloud users. Data integrity refers to the assurance by the user that the data is not modified or corrupted by the service provider or other users. When the clients want to retrieve the file from the cloud storage provider, it will send the retrieval request to the request handler in the privacy manager site. The request handler will send this retrieval request to the verifier module.

Verifier in turn with the identity of the client's file, retrieve the corresponding details from the database and send the retrieval request to the respective cloud storage server. It will generate the hash key of that encrypted segments which is retrieved from storage server once again and compare it with already stored hash value. If all segments match, the verifier concludes that the file is intact.

V. Conclusion

The usage of cloud computing as a computing environment for information systems and data can place data outside the data owner's control. The amount of protection needed to secure data is directly proportional to the value of the data. When the value of data increases, the number and extensiveness of needed security controls also increase. It could be a problem if these security controls are not supported by the cloud provider. The uncertainty of how security can be guaranteed in external computing environments raises several security questions concerning the availability, integrity, and confidentiality of data in these cloud computing environments. The proposed system provides a better integrity checking with the help of the trusted third party, a cloud Privacy manager at the client side with the Hybrid encryption mechanism. Storage security is highly enhanced since only the encrypted data is stored at cloud sites and the client even doesn't get the whole file without the knowledge of the Privacy manager.

REFERENCES

[1] K. Jeffery, and B. Neidecker-Lutz, The Future of Cloud Computing Opportunities for European Cloud Computing Beyond 2010, European Commission Information Society and Media.

[2] A Platform Computing Whitepaper, 'Enterprise Cloud Computing: Transforming IT', Platform Computing, pp6, viewed 13 March 2010.

[3] M. Peter, and G. Tim. "The NIST Definition of Cloud Computing," 19 June, 2010.

[4] Peeyush Mathur, Nikhil Nishchal, "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[5] Cong Wang, Qian Wang and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Department of ECE, Illinois Institute of Technology.

[6] Qi Zhang · Lu Cheng · Raouf Boutaba ,. " Cloud computing: state-of-the-art and research challenges" Journal of Internationet Services and Applications 2010 Vol. ,pg. 7–18. Springer,

[7] N. Hawthorn, "Finding security in the cloud," Computer Fraud & Security, vol. 2009, issue 10, pp. 19-20, October 2009.

[8] http://en.wikipedia.org/wiki/Pretty_Good_Privacy

[9] Xinyi Huang, Yang Xiang, Ashley Chonka,Jianying Zhou, and Robert H. Deng" A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems"

[10] A. Parakh and S. Kak, "Online data storage using implicit security", Information Sciences, vol. 179, issue 19, pp. 3323-3333 ,September 2009

[11] Sravan Kumar and Ashutosh Saxena, "*Data Integrity Proofs in Cloud Storage",* 978-1-4244-8953-4/11/$26.00©,2011 IEEE.

[12] R. Barga, J. Bernabeu-Auban, D. Gannon et al., "Cloud computing architecture and application programming," SIGACT News, vol. 40, no. 2, pp. 94-5, 2009.

[13] William Stallings," Cryptography and network security".