IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 81-84

Cloud Data Security with Mixed Algorithms

A.Mercy, M.Savithiri
M.Phil Research Scholar, Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore, Tamilnadu, India.
Assistant Professor, Department of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore, Tamilnadu, India.

Abstract: *Cloud Computing is one of the most preferable technologies in the current era. Many computing services are moved to Cloud because of that attractive cost saving method. However, they have little fear to move cloud because of some cloud issues. Here, Data Security is one of the main drawback or issue of the cloud technology. The security of data in cloud computing is the most of the essence difficulty in the recent times. A fundamental method of protecting data is encrypting it before outsourcing or third party. In the existing methods (or traditional methods) are only concentrate on the transaction and storage area (or state). In my proposed method also concentrate on processing state, with the use of crossbreed Algorithms. In this data security method is provides (a) key management (b) access control and, (c) computation on cipher text.*

Keywords: *Cloud Computing, Data Security, Hybrid Algorithms.*

I. Introduction

Data Security is a key challenge. The data security problems can cause a great loss, even devastating blow [1]. Therefore to make the enterprise and the organization accept cloud computing services, it is necessary to solve security problems. With the benefit of wireless ad-hoc networking in terms of flexibility and ease of deployment come many challenges in network security. Wireless ad-hoc networks are exposed to a variety of security threats in that adversaries may disrupt or halt network operation, compromise the continuous flow of valid information, and violate the privacy of network users and their data. In particular, due to the extensive use of the wireless medium in ad-hoc networks, message communications are vulnerable to passive attacks such as eavesdropping and active attacks such as message insertion or jamming.

Data Security in Cloud Computing

Data security is the practice of keeping data protected from corruption and unauthorized access [2]. It protecting personal data and helps to insuring privacy. In cloud computing the concerns of the data security are increasing due to the ongoing development of the internet and communication and also ease of data sharing. Data security is critical in all the aspects of our lives; banking information, personal files and businesses. Almost all of those are processed using the technologies and through network communication. One major reason security concerns are rising because the companies are Conducting core and noncore business functions through other companies.

A. Authentication

Authentication is verifying that the person who requested an access to the information is who he claims to be. It is a process of proving identity. Authentication is a major security measure for cloud computing service providers and users. It is important for service providers to insure that the technologies of authentication are accurate. The main techniques used in the authentication are: username and password, tokens, biometrics, certificates, and Kerberos. Username and password is the most common user technique which is most often used. A token is a security device which has a permission to access embedded in the token itself. This is about the authentication process [3].

B. Access Control

After the authentication and making sure that the user is who that claims to be, the next step is access control; which is restricting the user from access all information, and limiting his access to only material which the user has permission to access. Assigning rights to the groups is more efficient than assigning them to the specific users. Thus, the users should be assigned to groups and then getting the same privileges for all the group members. The models to determine the access control types are: Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Discretionary Access Control (DAC) [3].

C. Audit

Third and last part of the data security is Auditing. Information security configurations should be audited to ensure the access controls that are in place. Some of the auditing techniques are; logging and system scanning. Logging is keeping record of the activities performed by the users and the time at which it is occurred. The information recorded in the logging is useful when it is compared with the access control list (ACL) [3].

II. Literature Review

Cloud computing is a new technology which is a result of wrapping Virtualization, parallel computing and distributed computing into a single unit. The NIST definition of cloud computing "Cloud computing is a delivery model that enabling ubiquitous, convenient, efficient on -demand network access to a pool of shared configurable computing resources such as networks, storage, applications, server and services that can be rapidly provisioned and reduced". This cloud model is consists of five essential characteristics, three service models and four deployment models. The cloud computing is a web based model which is connected with more than one system. Cloud computing is the combination of fundamental technique which are utility computing and service oriented architecture.

It removes the necessity of setting high cost devices for infrastructure for any organization, with the help of cloud computing the organization takes care of its functions work rather than to develop a costly infrastructure. In cloud environment all the data are outsourced to external provider and they take concern of that data is now a responsibility of the cloud provider and we can access this data on virtual machines or any other device. Since the data center of cloud provider is spread to all over in the world and we can access our data from any corner of the world. Cloud Computing is the result of advancement in the presented technologies. At the current world of networking system, Cloud computing is one of the most important and developing idea for both the developers and the users. In the cloud environment, resources are shared among the servers, users and individuals.

These Cloud services can be further comes under the three categories.

- ***SaaS***- Application that is deployed over a network, typically the web, accessible via a browser or program interface; referred to as software on demand.
- ***PaaS***- A platform on which user can build their application using languages, libraries, tools and services supported by provider.
- ***IaaS***- Processing and storage capacity, networking and computing resources where the user has control over operating system and deployed application; sometimes referred to as utility computing.

Number of companies such as Google, Amazon, Microsoft etc. are developing clod infrastructure providing services to customer through network. Cloud computing enhanced the utilization of computing resources by sharing in number of users, which is so called utility computing.

Cloud computing is developed in four deployment model namely:

Private Cloud**:** It is also called internal cloud. It is operated for individual organization. Such infrastructure is accessed only by the member of the organization. Private cloud is managed by the organization or a third party such as Amazon Elastic Cloud Computing (EC2), Simple Storage Service (S3).

Public Cloud**:** It is owned and maintained by a single organization, but its services and application are available for general public use. In this all services are available and any user can get those services by paying appropriate amount.

Community Cloud**:** It is owned and maintained by an organization for a specific community. This cloud could be shared by many organizations for any particular reason; possibly it managed by internally or externally.

Hybrid Cloud**:** This type of cloud is a combination of two or more clouds (for example combining public and community clouds).

III. Related Work

K. Nasrin, et. al. [4] address that cloud storage frameworks are one of the key research area for cloud computing. Security is one of the major important concerns for research work. They derived a mechanism which is the combination of asymmetric and symmetric key method using RSA and AES algorithm. AES is good for key sharing and low overhead cryptographic mechanism further, RSA is good to create complex phenomena for attackers. The focus of the attackers was on proving secure file communication from vulnerable network.

Cindhamani.J et. al. [7] proposed an improved design for data security. It proposed a concept to achieve integrity, confidentiality and authentication in single architecture. They uses 128 bit key for RSA and Third party auditor for authentication purpose. Here, proposed solution consist two main parts one is storing data into storage and another is retrieve data from storage. This paper ensures the security goals during storage operations and guaranty about valid authentication and access.

Existing Algorithms

In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources, encryption algorithm [5] plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data.

In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption [6].

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in research work are as follows;

A. Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) [8] is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64- bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds [9]. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm.

B. RSA Algorithm:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Proposed Work

Nowadays Cyber Criminals can easily access data storage. In Personal Cloud Storage important data, files and records are entrusted to a third party, which enables Data Security to become the main security issue in Cloud Computing. In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

A. Proposed System Design:

The proposed system is designed to maintain security of text files only. This proposed system uses AES & RSA algorithm to generate encryption when user uploaded the text files in Cloud Storage and inverse AES & RSA algorithm to generate decryption when user download file from Cloud Storage. In between the processing state uses the Homomorphic Encryption (HE) Algorithm, for increasing security. This HE allows user to operate encrypted data directly without decryption. The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

1) For Encryption of text files:

- Upload Text file.
- Implementing the AES & Homomorphic algorithm of Encryption to generate first level encryption.
- Implementing the RSA algorithm of Encryption to generate second level encryption.
- Store Cipher Text into Database.

2) For Decryption of text files:

- Read Cipher Text from Database.
- Implementing the RSA algorithm of Decryption to generate first level decryption.
- Implementing the AES algorithm of Decryption to generate Plain text.
- Display Plain Text to User.

B. Proposed Algorithm:

We have proposed a combination of three different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: AES , RSA and

Homomorphic. AES (Advanced Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. Whereas, Homomorphic performed directly in cipher text. A user can upload Text file in Personal Cloud Storage. When uploading file AES and RSA Encoding schemes are used to encrypt data.

IV. Conclusion

In this paper, the problem of data security in cloud data storage was investigated, which is essentially a distributed storage system. Cryptography technique often used to secure the data transmission and storing between user and cloud storage services. The focus of this paper was on providing secure files Storage, processing, and transmission in the cloud environment.

A combination of asymmetric and symmetric encryption techniques (*i.e.* RSA and AES encryption methods) with HE was proposed in this approach to achieve the assurances of cloud data security. The focus was on RSA encryption to provide difficulty for attackers as well as reducing the time of information transmission by using AES encryption method and Homomorphic performed directly in cipher text. The process of sending the files to the cloud and retrieving the files from the cloud was accomplished by symmetric and asymmetric encryption respectively.

References

[1]. K. W. Miller, J. Voas, and G. F. Hurlburt (2012), “BYOD: Security and Privacy Considerations,” IT Professional, vol. 14, no. 5, pp. 53– 55, Sep. 2012.

[2]. Pearson, S., Benameur, A., “Privacy and Security Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010.

[3]. Gens, Frank. "IT Cloud Services User Survey, Pt.2: Top Benefits & Challenges." IDC EXchange. 02 Oct. 2008. Web. 14 Dec. 2010.

[4]. Nasrin Khanezaei, Zurina Mohd Hanapi “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services” IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia.

[5]. AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms” International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033-3037, May-Jun 2012

[6]. Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, “Homomorphic Encryption Applied to the Cloud Computing Security”, World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[7]. Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu “An enhanced data security and trust management enabled framework for cloud computing systems” IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China.

[8]. Neha Jain and Gurpreet Kaur ‘Implementing DES Algorithm in Cloud for Data Security” VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[9]. G. Devi , M. Pramod Kumar, “Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm” International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.