IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 16-20
www.iosrjournals.org

An Approach towards Securing Data in Cloud Computing

Miss. V.T. Lanjewar[1], Prof. R.V.Dharaskar[2], Dr. V. M. Thakare[3]
[1](vrushali.lanjewar@gmail.com, *SGBAU, Amravati)*
[2]*(rvdharaskar@rediffmail.com, SGBAU, Amravati)*
[3](vilthakare@yahoo.co.in , *SGBAU, Amravati)*

Abstract: *Users store vast amounts of sensitive data on a cloud. Sharing sensitive data will help enterprises reduce the cost of providing users with personalized services and provide value-added data services. However, secure data sharing is problematic. Security is one of the most difficult task to implement in cloud computing. Different forms of attacks in the application side and in the hardware components. This paper proposes a framework for secure sensitive data sharing in cloud, including secure data delivery, storage, usage, and destruction on a semi-trusted in cloud environment. We present Kerberos protocol over the network and a user process protection method based on a virtual machine monitor, which provides support for the realization of system functions.*

Keywords: *Cloud environment, Kerberos, Sensitive data*

I. INTRODUCTION

Cloud computing is technology which enables the user to access resources using front end machines, there is no need to install any software. Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over loose coupling mechanism such as messaging queue. Cloud computing services are broadly divided into three categories as follows:

Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers" side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today, SaaS is offered by companies such as Google, Salesforce, Microsoft, etc.
Platform as a Service (PaaS): PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Such as Google App Engine, Yahoo Open Strategy, Microsoft Azure etc.

Infrastructure as a Service (IaaS): This is the base layer of the cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization. The application will be executed on a virtual computer (instance). There is choice of virtual computer, where a configuration of CPU, memory & storage can be selected that is optimal for our application. The whole cloud infrastructure viz. servers, routers, hardware based load-balancing, firewalls, storage & other network equipments are provided by the IaaS provider. Some common examples are Amazon, GoGrid, 3 Tera, etc.

- Deployment Models were classified as:
  - *Private cloud:* The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.
  - *Community cloud:* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, and policy).
  - *Public cloud:* The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group.
  - *Hybrid cloud:* The cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology.
- Management Models (trust and tenancy issues) are Self-managed, third party managed (e.g. public clouds and VPC)

SECURITY IN CLOUD COMPUTING

Cloud computing encompasses both a server and a client side. Maintaining physical and logical security over clients can be troublesome, especially with embedded mobile devices such as smart phones. Built-in security mechanisms often go unused or can be overcome or circumvented without difficulty by a knowledgeable party to gain control over the device. Several security schemes for data sharing on un-trusted servers have been proposed. In these approaches, data owners store the encrypted data files in un-trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.The lack of security of local devices can provide a way for malicious services on the cloud to attack local networks through these terminal devices; compromise the cloud and its resources for other users. The lack of security of local devices can disrupt the consumer and also provide a way for malicious services on the cloud to attack local networks through these terminal devices.

In today's ubiquitous computing environment, the local host machine may well be a desktop computer, a portable laptop or mobile device. While cloud consumers worry about the security on the cloud provider's site, they may easily forget to harden their own machines. The lack of security of a local host can compromise the cloud and its resources for other users. With mobile devices, the threat may be even stronger, as users misplace or have the device stolen from them.

Devices that access the cloud should have strong authentication mechanisms, should be tamper-resistant, and have cryptographic functionality when traffic confidentiality is required. Since this place a part of the security burden onto the consumer, the provider may need to stipulate in its policy or SLA. Users connect to the cloud from their local host machines. In particular, many secure cloud data storing technologies require users to generate master keys (used to encrypt data or session keys) and store them on the local machine. If a malicious service in the cloud can tamper with the local machine and access these keys, confidentiality of data stored in the cloud is at risk.

II. BACKGROUND

Regarding encryption technology, the Attribute-Based Encryption (ABE) algorithm includes Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CPABE). ABE decryption rules are contained in the encryption algorithm, avoiding the costs of frequent key distribution in ciphertext access control. However, when the access control strategy changes dynamically, a data owner is required to re-encrypt the data[1]. A security destruction scheme is proposed for electronic data. A new scheme, Self Vanish, is proposed. This scheme prevents hopping attacks by extending the lengths of key shares and significantly increasing the cost of mounting an attack. To solve the problem of how to prevent sensitive information from leaking, when an emergency occurs, proposed a real-time sensitive safe data destruction system. The proposed framework well protects the security of users' sensitive data. [2]

The scheme is of CCA2 security proves under the decisional q-Bilinear Diffie-Hellman Exponent assumption. In addition, the scheme implements and analyse its performance. The hierarchical authorization structure of the scheme reduces the burden and risk of a single authority scenario. [3]. The article provides a ciphertext policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. [4]

The paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. This paper explains the overview, rationale and components in the CCAF to protect data security.[5]

This paper introduced an approach towards achieving secure data in cloud computing i.e. **Section I** gives **Introduction**. **Section II** discusses **Background** of security in cloud. **Section III** discusses **previous work done**. **Section IV** gives brief description of **Existing methodology**. **Section V** presents **Analysis and Discussion Section VI** finally, **proposed methodology** and possible **Result**. **Section VII** describes **Conclusion** of paper.

III. PREVIOUS WORK DONE

Peng Li, et al (2014) [1] focused on ORAM algorithm that is applied to achieve privacy-preserving access to big data in clouds. A load unbalance phenomenon observed after deploying ORAM-based storage to multiple servers, which motivates us to investigate a data placement problem to achieve load balance. This problem is proved to be NP-hard. A low-complexity algorithm proposed to solve this problem with respect to large data volumes. *X. Dong, et al* (2015)[2] proposed a systematic framework of secure sharing of sensitive data on big data platform, which ensures secure submission and storage of sensitive data based on the heterogeneous proxy re-encryption algorithm, and guarantees secure use of clear text in the cloud platform by the private space of user process based on the VMM. At the same time the data owners have the complete

control of their own data, which is a feasible solution to balance the benefits of involved parties under the semi-trusted conditions.

Teng, et al (2015)[3] proposes a hierarchical attribute-based access control scheme with constant-size ciphertext. The scheme is efficient because the length of ciphertext and the number of bilinear pairing evaluations to a constant are fixed. Its computation cost in encryption and decryption algorithms is low. *J. Li, et al* (2016)[4] provided a formal definition and security model for CP-ABE with user revocation. When any user leaves, the group manager will update user's private keys except for those who have been revoked. A concrete CP-ABE scheme also construct which is CPA secure based on DCDH assumption. *Chang et, al* (2016)[5] proposed a Cloud Computing Adoption Framework (CCAF) and CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. The paper has demonstrated the CCAF multi-layered security for the data security in the Data Center under the proposal and recommendation of CCAF guidelines.

IV. EXISTING METHODOLOGY

ORAM Algorithm, Systematic framework with proxy re-encryption algorithm, CP-ABE access control scheme, CCA2 security scheme, Cloud Computing Adoption Framework (CCAF) were existing techniques.

ORAM algorithm: The ORAM algorithm is applied to enable privacy-preserving access to big data that are deployed in distributed file systems built upon hundreds or thousands of servers in a single or multiple geo-distributed cloud sites. Since the ORAM algorithm would lead to serious access load unbalance among storage servers, also studied a data placement problem to achieve a load balanced storage system with improved availability and responsiveness [1].

Proxy re-encryption algorithm: A framework for secure sensitive data sharing on a big data platform proposed including secure data delivery, storage, usage, and destruction on a semi-trusted big data sharing platform and present a proxy re-encryption algorithm based on heterogeneous cipher text transformation and a user process protection method based on a virtual machine monitor, which provides support for the realization of system functions. The framework protects the security of user's sensitive data effectively and shares these data safely [2].

ABE access control scheme: A hierarchical CP-ABE access control scheme was proposed with constant-size ciphertext and discussed the algorithms in detail for our scheme. This scheme can fix the size of ciphertext and the computation of encryption and decryption at a constant value in addition to improving the efficiency of the system. This scheme can maintain the size of ciphertext and the computation of encryption and decryption at a constant value. Therefore, the scheme can improve the efficiency of the system. An application model is demonstrated in a Hadoop distributed cloud environment. This shows our scheme has good adaptability and scalability in cloud computing [3].

Ciphertext policy attribute based encryption (CP-ABE): A hierarchical attribute-based access control scheme with constant-size ciphertext is proposed. The proposed scheme adopts CP-ABE with constant ciphertext size and maintains the size of ciphertext and the computation of bilinear pairing at a constant value, which improves the efficiency of the system and reduces the extra overhead of space storage. This system supports inheritance of authorization that reduces the burden and risk in the case of single authority. Finally, the scheme has proved indistinguishable security under an adaptive chosen ciphertext attack and we analyze the performance of our scheme. A simulation model is apply the scheme in a cloud environment [4].

Cloud Computing Adoption Framework (CCAF): The CCAF approach provides an integrated solution to cloud security based on a clear framework, business process modelling to study the impact on the performance of a user accessed service which is often learned on the fly which is costly and a CCAF three layered model. [5]

V. ANALYSIS AND DISCUSSION

In this section, we analyse some algorithms and techniques used in five papers and also discusses our proposed framework are as follows.

ORAM algorithm is applied to enable privacy-preserving access to big data in cloud. To deal with the challenge of accommodating huge volume of data that continuously grows in high velocity, big data are stored in distributed file systems built upon hundreds or thousands of servers in a single or multiple geo-distributed cloud sites [1]. A systematic framework of secure sharing of sensitive data on big data platform, which ensures secure submission and storage of sensitive data based on the heterogeneous proxy re-encryption algorithm, and guarantees secure use of clear text in the cloud platform by the private space of user process based on the VMM [2]. The scheme uses CCA2 security under the decisional q-Bilinear Diffie-Hellman Exponent assumption. The scheme can maintain the size of cipher text and the computation of encryption and decryption at a constant value. Therefore, the scheme can improve the efficiency of the system [3]. A concrete CP-ABE scheme is constructed CPA secure based on DCDH assumption. To resist collusion attack, embedded a certificate into the

user's private key [4]. The CCAF approach provides an integrated solution to cloud security based on a clear framework, business process modeling to study the impact on the performance of a user accessed service which is often learned on the fly which is costly and a CCAF three layered model [5].
The comparison between methods gives brief idea and shown in table below:

Method / Algorithm Used	Advantages	Disadvantages
ORAM algorithm	The performance of ORAM algorithm is close to optimal solution, and it outperforms a random data placement algorithm.	ORAM tree would contain a large number of buckets to accommodate big data, resulting in too many variables and constraints in the formulation.
Proxy re-encryption algorithm	Heterogeneous proxy re-encryption algorithm guarantees secure use of clear text in the cloud platform by the private space of user process based on the VMM.	Further, need to improve the efficiency of encryption. In addition, reducing the overhead of the interaction among involved parties.
Attribute-Based Encryption (ABE)	This scheme is efficient, scalable, and fine-grained in dealing with access control for outsourced data in cloud computing.	ABE algorithm should be simpler and more efficient along with making it even more suitable for access control in a cloud environment.
Ciphertext policy attribute based encryption (CP-ABE)	1. CP-ABE scheme which is CPA secure based on DCDH assumption. 2. The results of experiment show that our scheme is efficient for resource constrained devices.	1. CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure.
Cloud Computing Adoption Framework (CCAF)	CCAF multi-layered security has an average of 20% better performance than the single-layered approach which could only block 7,438 viruses and trojans.	The number of viruses and trojans detected but unable to be blocked and sent to quarantine.

Table 1: Advantages and Disadvantages

The main goal is to extend Kerberos to be an open authentication system, but modifying Kerberos for each new authentication type is burdensome. Traditionally, new authentication types go through an approval process by the standardizing committee. The fig below shows the Comparison of Kerberos and SSL. The two are really suited for different purposes. It is a worthwhile exercise, however, to compare the two.

VI. PROPOSED METHODOLOGY

Good load balancing makes more efficient and improve user fulfilment in cloud computing. Thus, one future work is how to speed-up the decryption operation at low-end devices**.** However, the decryption may be still slow for low-end devices because a modular exponentiation operation is required. The load balancing in cloud has imported collision on the performance. So, proposed a framework that will use RSA encryption algorithm to encrypt the data. To secure sensitive data kerberos is used for a user process protection method based on a virtual machine monitor. The basic set up of Kerberos protocol is as shown.

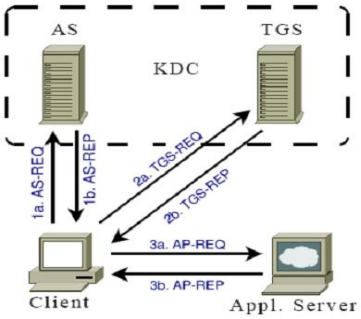

Fig. Kerberos protocol

The Kerberos server consists of an Authentication Server (AS) and a Ticket Granting Server (TGS). The AS and TGS are responsible for creating and issuing tickets to the clients upon request. The AS and TGS usually run on the same computer, and are collectively known as the Key Distribution Center (KDC). The Kerberos authentication process works in three phases as shown in Figure 1.
Kerberos is a distributed, identity-based authentication system that provides a method for a user to gain access to an application server.

Authentication is critical for the security Computer systems. Without knowledge of a principal requesting an operation, it is difficult to decide whether the operation should be allowed. Traditional authentication methods are not suitable for use in computer networks where attackers monitor network traffic to intercept passwords. The use of strong authentication methods that do not disclose passwords is imperative. So, the proposed Kerberos authentication system is well suited for authentication of users in such environments.

EXPECTED RESULTS

The goal of this paper was to ensure the security of data in cloud in cloud computing. Then an extensive systematic selection process was carried out to identify results of proposed framework using Kerberos protocol for authentication along with encryption algorithm in cloud computing. The results presented here thus will give a better picture of the existing securing sensitive data techniques used in cloud environment where security is the key issue these days.

VII. CONCLUSION

The expected results indicated that the proposed data sharing on cloud scheme is efficient for securely and flexibly managing media content in large, loosely-coupled, distributed systems. The protocol used in the framework is responsible for protecting data while transferring from sever to server in cloud. The framework protects the security of user's sensitive data effectively and shares these data safely. With the assistance of the cloud server, the decryption operation is accelerated significantly at the consumer side.

FUTURE SCOPE

In the future, further research work will optimize the primary purpose of the Kerberos authentication system to improve the performance on cloud. So that, the framework should be more efficient for securely and flexibly managing media on the client is to issue requests.

REFERENCES

[1]. Peng Li; Song Guo "Load Balancing for Privacy-Preserving Access to Big Data in Cloud", *2014IEEE INFOCOM Workshop on Security and Privacy in Big data* Computer Communications Workshops (INFOCOM WKSHPS), vol.21, no.4, 524 – 528, May 2014.

[2]. Xinhua Dong; Ruixuan Li; Heng He; Wanwan Zhou; Zhengyuan Xue; Hao Wu, "Secure Sensitive Data Sharing On a Big Data Platform", *Tsinghua Science and Technology published in IEEE*, Vol.20, No.1, pp.72-80, Feb. 2015; doi: 10.1109/TST.2015.7040516

[3]. W. Teng; G. Yang; Y. Xiang; T. Zhang; D. Wang, "Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing," in *IEEE Transactions on Cloud Computing* , vol.PP, no.99, pp.1-1, 02 June 2015,doi: 10.1109/TCC.2015.2440247

[4]. J. Li; W. Yao; Y. Zhang; H. Qian; J. Han, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing," in *IEEE Transactions on Services Computing* , vol. PP, no.99, pp.1-1, 22 January 2016, doi: 10.1109/TSC.2016.2520932

[5]. V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in *IEEE Transactions on Services Computing*, vol.9, no.1, pp.138-151, Jan.-Feb.1 2016,doi: 10.1109/TSC.2015.2491281