International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 03, March 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

HYBRID INFORMATION SECURITY MODEL for CLOUD STORAGE SYSTEMS

Harpreet[1], Sheenam Katna[2]

[1]*Department of Computer Science and Technology, Doaba, Kharar, Chandigarh (India)*

[2]*Department of Computer Science and Technology (India)*

ABSTRACT

Computer systems and the information they create, process, transfer and store have become absolutely necessary to the modern enterprise. In todays on demand, data driven word, many organizations count their information systems as their most important assets. The cloud verifies the authenticity of the users before storing their data. With the recent developments in society, the most important focus has been on the value of knowledge and information. However the incidents of personal and corporate information being leaked frequently happen and also the damage is getting increased day by day. The secret information of individuals is leaked by personal mistakes or outside attacks, thus misused, and thereby considerable damage is occurring. Therefore there is a need to effectively manage personal and corporate information. This study tends to suggest a method that can protect the media information which requires security.

Keywords- Attribute Based Access Control(ABAC), Infrastructure as a Service(IaaS), Platform as a Service(PaaS), Software as a Service(SaaS), Data Owner(DO), Cloud service provider(CSP).

I. INTRODUCTION

In recent years the trend of cloud storage systems has increased dramatically. Cloud computing is a new and fast growing technology in the field of data computation and storage. It is an internet based technology that enables on demand access to computing and data storage resources. The applications where data are being transferred between servers or users require secure data storage on cloud environments. The security of data is quite important as it belongs to the users. It provides storage and computation at a minimal cost. Organizations use access control mechanisms to reduce the risk of unauthorized access to their data, resources and systems. There are various access control models. Their corresponding access control mechanisms make use of different techniques and components.

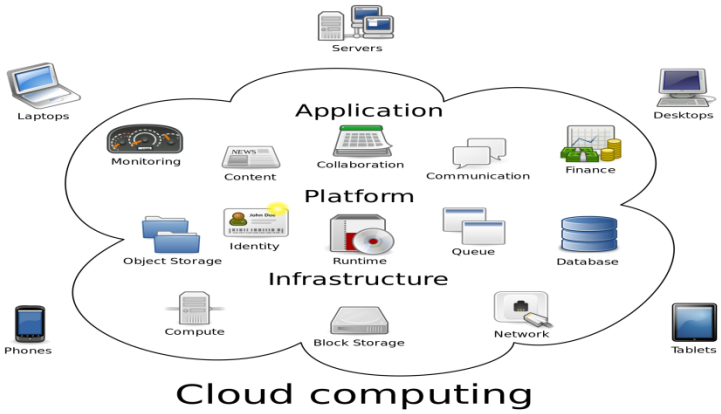
One of the access control models is the Attribute Based Access Control (ABAC). Here the access control decisions are made on the basis of a set of characteristics, attributes, environment and the resource itself. Each attribute is a distinct field that determines whether to allow access or to deny access. It is not necessary that the attributes need to be related to each `or some combination of the above.

The five characteristics of cloud computing are: on-demand service, location independent, self service, elasticity and measured scale service. Industries and institutions are exploiting these characteristics of cloud computing in order to increase their profit and revenue. However data security is a major obstacle in the path of

ISSN (O) 2454-9665
ISSN (P) 2454-0663

cloud computing. Some people still believe that cloud is an unsafe place to store data and once you send your data to cloud, you lose control over it. They are somewhat right, as data confidentiality gets violated by collusion attacks from malicious users and service providers.

Many schemes are given to ensure these security requirements but they are suffering from collusion attack of malicious users and heavy computation. In this scheme, there are three entities: Data Owner (DO), Cloud Service Provider (CSP), and Users. Users are divided in group on the basis of location, project, and department. We have proposed a hybrid security model which is implemented by combining various techniques together to achieve the goal of data security. The various techniques included in this model are Encryption, Compression, Key exchange and divining the user groups.



1.1 Deployment models of cloud computing

In cloud computing, the available deployment models are: Public cloud, Private cloud and Hybrid cloud.

Public Cloud: A public cloud model allows users access to cloud using interfaces via web browsers. It is less secure than other cloud models, because there is an additional burden of ensuring that the data available on public cloud is not subject to malicious attacks.

Private cloud: A private cloud is set up within an enterprises data centre. Here all cloud resources and applications are managed by the organization itself. Utilization on private cloud can be more secure than public cloud.

Hybrid Cloud: A hybrid cloud is a private cloud linked to one or more external cloud services. It is a mix of both public and private clouds. Hybrid clouds allow more secure control of data and applications, allowing various parties to access the internet.

1.2 Service models

Cloud computing provides services according to three fundamental service models:

1) Infrastructure as a service(IaaS)
2) Platform as a service(PaaS)
3) Software as a service (SaaS)

Infrastructure as a Service (IaaS): Involves outsourcing the equipment required to support operations, including storage, hardware, servers and networking components.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Platform as a Service (PaaS): It is a platform which allows cloud consumers to develop cloud services and application directly on the cloud.

Software as a Service (SaaS): It is a software distribution model in which applications are provided by a service provider and made available to customers over a network.

II. LITERATURE REVIEW

2016 Nikeetaa P. Choudharri, Ms. Kanchan M. Varpe, [1]

Have proposed an approach that makes use of threshold cryptography. Here the data owner partitions clients in gatherings and provides a single key to each bunch for decoding of information. Every client in the gathering shares parts of the key. This plan not only provides data confidentiality but also lessens the quantity of keys. Additionally it provides user revocation and manages access control. To guarantee fine grained access control of outsourced information, the proposed system has utilized ability list. Open key cryptography and MD5 guarantee information integrity.

2016 Nancy Garg, Kamalinder Kaur [2]

Have used the hybrid approach for secure data storage on cloud. It is necessary to secure the data stored by users on cloud and maintain their confidentiality. Here the loaded image is encrypted and is hidden by the cover image. Thus the original content is not visible. Spatial domain technique least significant Bit (LSB) substitution is commonly used. Here the secret message bits replace the least significant bit of each pixel.

2013 Dr. L. Arockiam , S. Monikandan[3]

Security and Privacy of data stored in cloud computing is an area full of challenges. Symmetric Encryption is computationally efficient in handling large volumes of data in cloud storage. This paper proposed a symmetric encryption algorithm for secure data storage. This algorithm is used in order to encrypt the data of the user in the cloud. The encryption key acts as the primary authenticator as the user has no control over the data once their session is logged out. By applying this algorithm, user ensures that the data is secure and it cannot be accessed by malicious user's and intruders.

2014 Priya jaiswal , Randeep kaur , Ashok Verma[4]

In present scenario cloud network is a boon in network technology. It provides a number of services which are difficult to summarize. Microsoft 2012, window Azure, IBM is a few companies that provide these services at a nominal rate. This paper presents a secure cloud storage technology which encrypts the data using hybrid security algorithm using symmetric key. The proposed security technique provides a highly secure cloud network.

2016 Keerthana G, Dr. Prabu S, Dr. Swarnalatha P[5]

Cloud computing is Internet based technology where virtual shared servers provide software's and different facilities to clients on a pay-as-you-use basis. Here the important points of interest include unlimited storage, backup and recovery. Demerits of cloud computing include cost and absence of backup. In any case, fundamental drawback is security. In this paper, firstly the record is taken from client and then partitioned. After partitioning, all recorded parts are encrypted and sent to various cloud servers. At the point when client needs that information, it is taken back from cloud servers and decrypted. After decryption the information is merged and offered to the client.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

2015 Prachi Shah[6]

Today is the need of low-maintenance system which automates administration daily. There is a need of access control over network so that data security is ensured. Role-based access control (RBAC) method controls access to network resources based on the role given to an individual within an organization. Here the roles are defined according to job skill, authority, and responsibility within an organization. In RBAC, roles can be easily created, changed, or discontinued according to the requirements of the organization.

III. PROBLEM FORMULATION

Cloud computing is a technique that provides storage and computing at a very low cost. However ensuring the confidentiality, integrity and access control of data is an important task here. Various approaches are given to ensure these security requirements but they lacked in some ways such as collusion attacks and heavy computation. In the existing base paper, authors have proposed a scheme that uses threshold cryptography. In this scheme, the data owner divides users in groups and provides single key to each user group for data decryption. Each user in the group shares a part of the key. The authors have used capability access to control data access. The capability list specifies the authorized data and operations for a user. In this scheme, no member of any group knows about the whole key. Data can be decrypted when at least threshold number of users will be present. Although this scheme improves the performance by reducing the number of keys, it is not too efficient. After getting encrypted message the users main concern is to decrypt the data as he can't decrypt on its own. The process of decryption requires a threshold number of users need to be present. Each user in the group needs to update the PKS vector and decrypts a part of the message with their key component. Although this technique provides security, the process of decryption of data seems to be time consuming. Hence it can affect the performance of the system.

IV. PROPOSED MODEL

The proposed scheme emphasizes on a hybrid data security model which is implemented by combining various techniques together. The techniques included in the combination include: Encryption of data, Compression, Key exchange and divining user groups. The process of encryption stores the data in cipher form, compression scheme reduces the size of the data to be stored, with key exchange user can decrypt the data and divining the user into groups means each group has access to relevant data. Encryption creates a completely unreadable and hashed data making it impossible for a hacker to decrypt it. The owner of the data encrypts the data in such a way that only those users can decrypt the data that possess appropriate access permission according to their role. Role grants permission to access data according to their role. The process of compression improves the performance of the system by reducing the data transmission time.

V. SECURITY AND PERFORMANCE ANALYSIS

Security Analysis

Here we analyze the approach in terms of strength and scalability.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

1) Data Confidentiality: In the proposed scheme, DO store its data at CSP in encrypted form. As the data is encrypted by the symmetric keys which are known only to DO and respective user groups CSP can't see the data. Here the members can access the data only to which they are authorized. Hence collusion attack of CSP and users is not possible.

2) Entity Authentication: In the proposed scheme user is authenticate at DO when he sends his personal details to DO during registration by encrypting its own private key. DO is authenticated at CSP when it sends capability list and data by encrypting its own private key. User is authenticated at CSP when users ID and password match with the ID and password stored at the CSP database.

3) Data Access Control: The proposed scheme uses capability list to ensure data access control. Capability list basically consists of UID, FID and AR. Only DO has the right to perform any operations on it. CSP sends only that data to users which are in their access rights.

Performance Analysis

In the proposed scheme, DO transfer most of its load and computation to CSP and does only necessary things by itself. As we have also used the technique of compression, the data transmission time required is less and the storage space required is also less.

VI. CONCLUSION

In this paper, we presented an approach that provides security for data outsourced at CSP. Various approaches have been given to secure the outsourced data, but they have been suffering from having collusion attacks and large number of keys. By implementing the technique of encryption and data compression, we protect outsourced data from collusion attack. Moreover there is an improvement in the performance of system as the data transmission time is low and the space required for data storage is also quite low. The scheme has used capability list to ensure fine-grained access control of outsourced data. User can access data from cloud based upon authorization and access permission policies

REFERENCES

[1] Nikeetaa P. Choudharri, and Ms. Kanchan M. Varpe, A stable Data Security in Cloud Computing Using Threshold Cryptography and User Revocation, International Journal on Recent and Innovation Trends in Computing and Communication , 2016.

[2] Nancy Garg and Kamalinder Kaur, Hybrid information security model for cloud storage systems using hybrid data security scheme, in International Research Journal of Engineering and Technology (IRJET), Volume 03 Issue 04 **,** 2016.

[3] Dr. L. Arockiam and S. Monikandan, Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Voume. 2, Issue 8, 2013.

[4] Priya jaiswal, Randeep kaur, Ashok Verma, Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique, in International Journal of Emerging Technology and Advanced Engineering (IJETAE), Volume 4, Issue 1, 2014.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

[5] Keerthana G, Dr. Prabu S and Dr. Swarnalatha P., An Efficient Data Security in Cloud Computing using Cryptography, in International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 5, 2016 .

[6] Prachi Shah, Data Security for Cloud Storage System Using Role Based Access Control, in International Journal of Science and Research (IJSR), Volume 4 Issue 1, 2015.