International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 04, April 2017
www.ijates.com
ijates
ISSN 2348 - 7550

HYBRID INFORMATION SECURITY MODEL for CLOUD STORAGE SYSTEMS

Harpreet Kaur*, Sheenam Katna**

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

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

ABSTRACT

In todays on demand, data driven word, the most important assets of an organization are their information. The information that the computer systems create, process, transfer and store have become absolutely necessary to the modern enterprise. Before storing user's data, the cloud verifies their authenticity. With the developments in society, the main 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 drastically. Cloud computing is an internet based technology that enables on demand access to computing and data storage resources at a very low cost. The applications that require transfer of data over the network require secure data storage on cloud environments. As the data belongs to the users its security is quite important. This technique of cloud computing provides storage and computation at a minimal cost. To reduce the risk of unauthorized access to their data, resources and systems organizations use various access control mechanisms. 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 other.

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

people believe that cloud is an unsafe place to store data and once the data is sent to the cloud, you do not have control over it. They are somewhat right, as data confidentiality gets violated by collusion attacks from malicious users and heavy computation.

In order to ensure these security requirements, many schemes have been proposed 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.

Fig. 1 Cloud Computing

1.1 Deployment models of cloud computing

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

Public Cloud: A public cloud can be accessed by any subscriber who is having internet connection and has access to the cloud space. Since there is an additional burden of ensuring that the data available on public cloud is not subject to malicious attacks, it seems to be less secure than other cloud models.

Hybrid Cloud: A hybrid cloud is 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.

Private cloud: A private cloud is the one that is set up within an enterprises data centre. It is established for a specific group or organization and can be accessed by only the particular group or organization. Utilization on private cloud can be more secure than private cloud.

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): This model involves outsourcing the equipment required to support operations, including storage, hardware, servers and networking components.

Platform as a Service (PaaS): It is a platform which allows cloud consumers to develop cloud services and application directly on the cloud. It hosts both completed and in-progress cloud applications.

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. It hosts only the completed Cloud applications

II LITERATURE REVIEW

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

The authors have proposed a technique that makes use of threshold cryptography. Here the data owner partitions clients into groups and provides a single key to each group for decoding oaf information. Every client in the gathering shares parts of the key. This plan provides data confidentiality and also lessens the quantity of keys. Additionally it provides user revocation and manages access control. The proposed system has utilized ability list to guarantee fine grained access control of outsourced information.

2016 Nancy Garg, Kamalinder Kaur [2]

Here the authors have used 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.

2016 Keerthana G, Dr. Prabu S, Dr. Swarnalatha P [3]

Cloud computing is a technology where virtual shared servers provide various facilities to clients on a pay-as-you-use basis. Here the important points of interest include unlimited storage, backup and recovery. 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.

2015 Prachi Shah [4]

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. In an organization Role-based access control (RBAC) method controls access to network resources based on the role given to an individual. 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 an organization.

2015 Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma and Sundaram Vats [5]

In this paper the authors have presented an approach which provides security for data outsourced at CSP. By employing the threshold cryptography at the user side, the outsourced data is protected from collusion attack. Since, DO stores its data at CSP in encrypted form and keys are known only to DO and respected users group, data confidentiality is ensured. To ensure fine-grained access control of outsourced data, capability list has been used. Public key cryptography and MD5 ensure the entity authentication and data integrity respectively. Public key cryptography and D-H exchange protected the data from outsiders in this approach. Number of keys has reduced in the proposed scheme.

2014 Ruj, Sushmita [6]

The authors have proposed a decentralized access control scheme for secure data storage. This technique supports anonymous authentication. Here the cloud verifies the authenticity of the user without knowing the user's identity before storing data. The feature of access control in this scheme allows only valid users to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading of data stored in the cloud.

III . PROBLEM FORMULATION

Cloud computing is a technique that provides storage and computing at a very low cost. However the most important task here is to ensure the confidentiality, integrity and access control of data. 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. Here the data owner divides users in groups and provides single key to each user group for decryption of data. 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 threshold cryptography 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 the encrypted message the user's main concern is to decrypt the data. The process of decryption requires a certain 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

In this research, we have proposed a cloud data security model for the cloud storage using third party auditors. This technique will be implemented by combining various techniques together to achieve the data security and data privacy goal. The techniques included in the combination would be Encryption of data, Compression, key exchange and divining the user groups. Encryption will store 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. This means, if a hacker will attack and download the data, he will have to work hard a lot to access the data caused by the mathematical computations to generate the key and decrypt the data. Then the data encryption will be used to create a completely unreadable and hashed data. The combined scheme will be called as PCP-MABE (Pipeline Cipher Policy- Multiple Attribute Based Encryption).

V. RESULT ANALYSIS

- **Security Analysis**

This section analyzes various attacks on cloud and our defense mechanisms.

System Bootstrap: During the system bootstrap in cloud nodes, the hackers can attempt to inject the malicious content or malware on the cloud nodes. The proposed solution is self adaptive. Hence, every node is made capable so that they can take care of their own security. The node authenticates the nodes only after they share a key table of certain measurement. The randomized key from secure key table is used for verifying the received data, which defends system from penetration attacks for malware injection.

Key Life-cycle Operations: Hackers can try to change the key tables saved on the nodes or to change the key generation policy by tweaking into the node software. The nodes will not change the table on any of the hacking attempt by sending the data to the cloud nodes. Data of only those nodes will be accepted which are replying with the reply keys. The key table is generated using high randomization based secure code generation technique. This technique does not hold any computational dependency on the base key. So the hackers can't gain access and can't change key information table.

Key Generation and Usage Control: The key generation policy used in the proposed model is based on the high randomization and mathematical array value shuffling operation, which creates highly randomized and undependable numeric keys. Any key in the key table can't be calculated mathematically in order to find the next key in the table. Unauthorized applications and hackers cannot bypass the cloud scheme running on the sensor nodes because, to gain the authority to send the data to the sensor nodes, one has to obtain the authorization by sending a reply or response key in return to the request or question key However, this administrative operation can be recorded in the sensor node audit log and held accountable.

- **Graphical Analysis of Implementation**

Entropy of the Key Generation Scheme in Cloud: Entropy is the quantitative measure of disorder or randomness in a system. High entropy means higher security.

The following figure shows the entropy comparison of implemented scheme with ECG/EEG scheme. The implemented scheme has higher entropy as compared to ECG/EEG scheme which means it has more randomness on average.

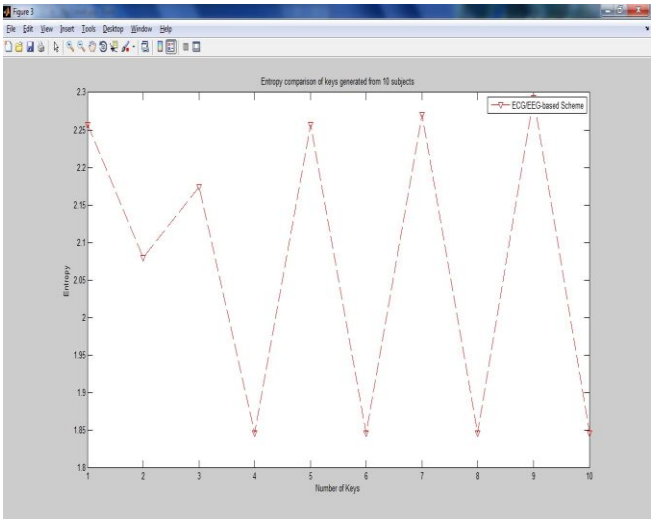

Figure 2: Entropy comparison of keys generated for 10 subjects.

Table I

Sr. No.	Entropy Value
1	**2.26**
2	**2.174686323**
3	**1.712706175**
4	**1.991399344**
5	**2.137048954**
6	**2.058408958**
7	**2.174686323**
8	**2.137048954**
9	**1.712706175**
10	**2.058408958**

- **Time comparisons for Implemented key management Scheme**

The time taken by various processes in the key management has recorded in the form of graphs and figures. The MATLAB simulator is used for plotting these procedures. Various procedures for which time is recorded are Key Generation Time, Key Transfer Time and Key Verification Time.

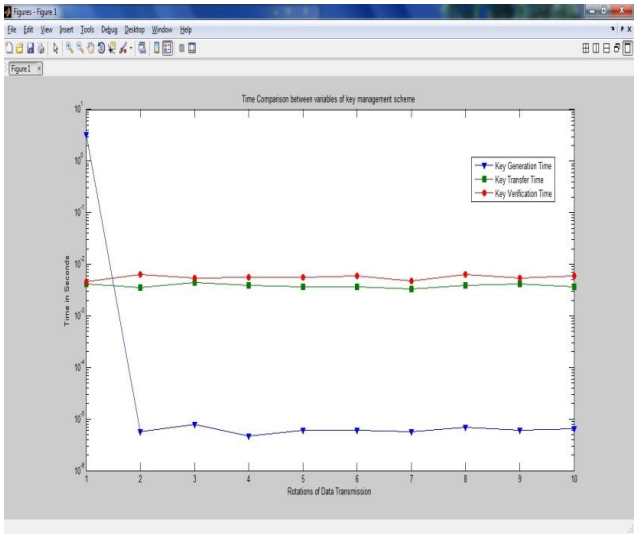

Figure 3: Time Comparison between variables of key management scheme.

The figure shows that only at first time the key generation time is high as compared to others. As key generation is done at starting so further there is no time devoted to key generation.

As there is a large difference between key generation and other variable so the following figure compare only key transfer and key verification. As it is shown in figure the key transfer and key verification time is very less ranges from 3 to 7 milliseconds.

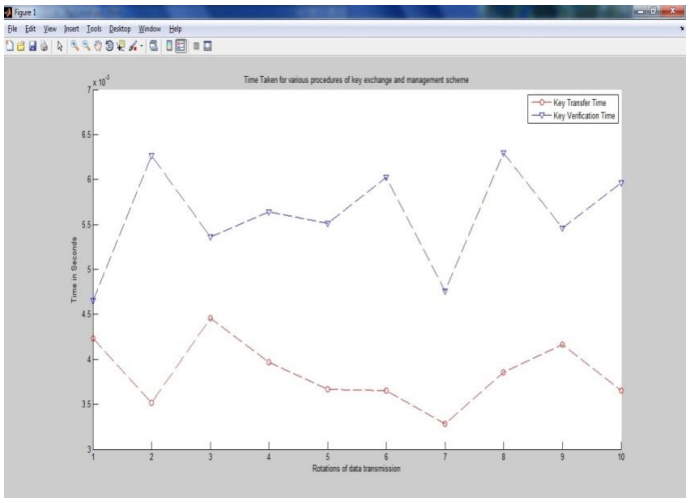

Figure 4: Time comparison between key transfer and verification time.

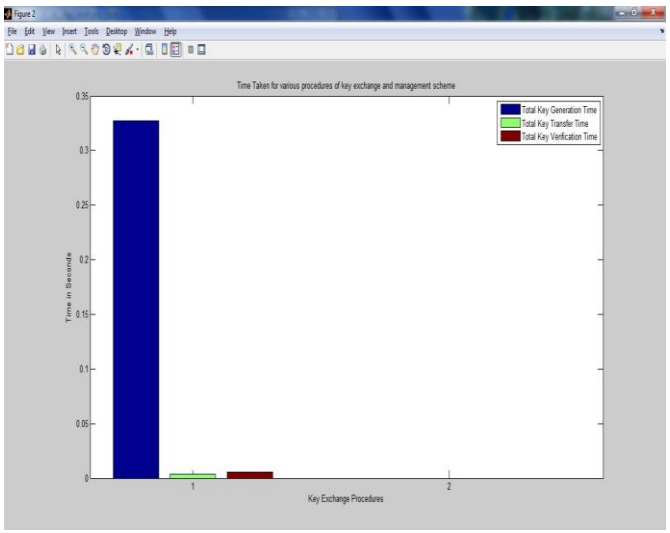

Figure 5: Total time comparison between variables of key management scheme.

The following figure shows Bar Graph presentation of key generation, key transfer and verification schemes. Others were compared for each key this is for total times taken.

V. CONCLUSION

In this research, we have proposed a cloud data security model for the cloud storage using third party auditors. 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] 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.

[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] 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.

[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.

[5] 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.

[6] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma and Sundaram Vats, Threshold Cryptography Based Data Security in Cloud Computing, in IEEE International Conference on Computational Intelligence & Communication Technology, 2015.