ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Efficient and Reliable Data Storage Security against Malicious Data Modification in Cloud Computing

Sagar Rushi .D, Pragna Makawana

Student, Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, India
Assistant Professor, Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, India

ABSTRACT*:* Cloud Computing becomes the next generation architecture of IT Enterprise. In contrast to traditional solutions, Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges which have not been well understood. In cloud computing, both data and software are fully not contained on the user's computer; Data Security concerns arising because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers with different demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. This paper investigates the basic problem of cloud computing data security. We present the data security model of cloud computing based on the study of the cloud architecture. We improve data security model for cloud computing. In proposed system, we are going to make robust data storage security model in which group member's data accessing scheme is used, for dynamic groups in the cloud. We analyze the security of our scheme with data confidentiality and demonstrate the efficiency of our scheme in experiments against malicious data modification.

KEYWORDS: cloud computing, security, privacy, authentication, confidentiality, data integrity

I. INTRODUCTION

In the traditional system, data and software stored or resides on the user's computer while in cloud computing, user's computer do not contain data or software while they resides on cloud server.

Cloud computing is based on five characteristics like on demand service, broad network access, measured services, easy use, business model and location independent resource pooling. Further descriptions of characteristics are as follows:

- **On demand service:** Cloud is a large resource and service pool from where the service or resource can be utilized whenever needed by paying the amount for the service being used [1].
- **Broad network access:** When cloud computing is to be efficient and effective replacement for in house data centers, high bandwidth communication links must be available to connect to the cloud services. High-bandwidth network communication provides right to use a large pool of IT resources [1].
- **Measured Service:** The amount of cloud resources used by a consumer can be Monitored and billed automatically for usage of that particular session. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of concept suitable to the type of service like storage, processing, bandwidth etc [1].
- **Easy use:** The most cloud providers' offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services [2].
- **Business model:** Cloud is a business model because it is pay per use of service or resource [2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

- **Location independent resource pooling:** The providers computing resources are pooled to supply multiple clients using multitenant model with diverse physical and virtual resources vigorously assigned and reassigned according to order [2].

II. RELATED WORK

In [1] this paper they have presented the data security model of cloud computing considered on the learning of the cloud architecture. They have improved data security model and implemented software to increase work in a data security model and also apply this software in the Amazon EC2 micro instance. They have covered cloud computing overview its main attributes, service model, deployment models. Proposed model covers three layers of security with software, which compares eight modern encryption algorithms based on statistical test to get best secured algorithm. Now compare P-values with significance level α i.e. 0.01. **If** P-value >= αthen Accept the sequence **else** Reject the sequence. The higher P-value the better and vice versa with rejection rate, the lower the better. In [2] this paper he has presented the entire analysis of different symmetric key encryption algorithm like DES, CAST-128, 3DES, RC6, MARS, AES, IDEA, and Blowfish based on various parameters like Architecture, Scalability, Flexibility, Limitations , and Security. Performance of DES and CAST are equal, memory requisite by the AES and DES are the same but the performance of the AES is very high compare to DES. DES doesn't support future modification. After evaluation, it is analyzed that AES is more secure, faster, better and useful encryption algorithm among all other algorithms by means of less storage space, high encryption performance without any weak point and limitation. In [3] these research papers they have examine two broad categories of cryptography like encoding & symmetric key encryption. And they also study a range of algorithms and evaluate them on the basis of performance & security. Performance of algorithm is evaluated based on parameters like file size, encryption time and encoding time. They have examined MD5 & SHA-256 encoding techniques and AES, DES & 3DES symmetric encryption techniques. AES is more secure for symmetric key encryption. In encoding technique, MD5 is faster other SHA but SHA seems to be extra secure. In [4] this paper, they have mainly focus on the precaution aspects of data storage from point of threats and attacks. Our scheme achieves the integration of storage correctness insurance and data error localization. The paper including topics like major challenges and problems, cloud deployment models and their design goals, methods for increasing cloud data storage. This paper suggests a methodical application of "defense in depth" security techniques that can help reduce security risks in networked storage. In [5] this paper, they have evaluated security and privacy issues associated with cloud computing and describes some reason for why all IT company are not used cloud and give solution of some issues. Also discuss various attacks against cloud architecture. Security in cloud computing is very much needed as data in the cloud storage are not secure and require lots of attention of user. Some of the challenges like security issues and data issues are very much required for the users to use the services provided by the cloud. So for protecting data in cloud we have to develop new mechanism which provides strong security as well ensuring safety of data and consuming performance cost is less. In [6] this article, cloud computing technology architecture and the cloud computing data security features are the first to be studied and then the cloud computing data security model is raised. The model adopts a multi-dimension architecture of three layers defense. First layer is user authentication that manages user's permissions to ensure that information cannot be tampered. Second layer is of encrypting user's data and the file entered the system encrypts and privacy defense level at user. If intruder gets the key, then user data can't get valid information even it is obtained during function of privacy protection. The final layer is the quick file regeneration layer, user data can get highest regeneration even it is damaged through rapid renewal algorithm in this layer. Every layer accomplishes its own job and combines its result among others to ensure data security. This paper tells us about data safety model against unauthorized users and this problem can be solved by combined efforts of information security academia, the relevant government departments & industrial circles.

III. BASIC CLOUD COMPUTING ARCHITECTURE

i. Cloud Computing Service Model

- This cloud computing technology provides **three main services** as given below in cloud service model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

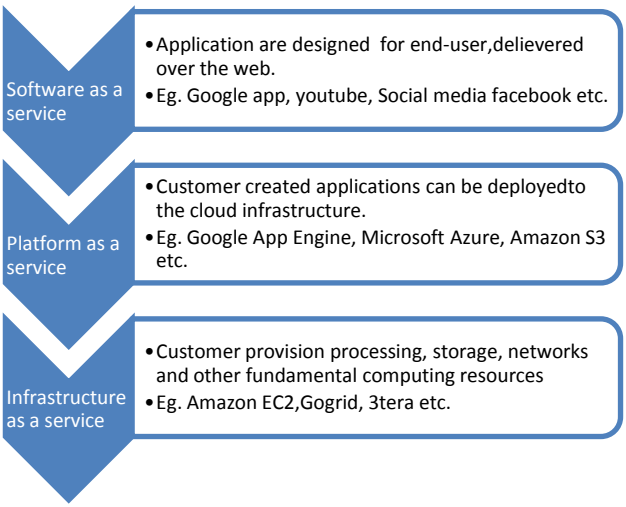

Figure 3.1: Cloud Service Model

ii. Cloud Computing Deployment Model

- There are three deployment models for cloud computing:
- **Public cloud:** The infrastructure of computing is owned and managed by CSP. Public cloud is used by anyone [3].

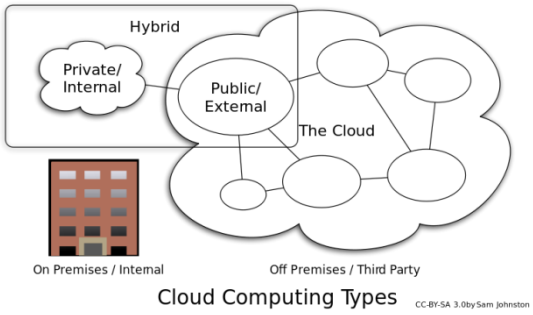

Figure 3.2: Cloud Deployment Model

- **Private cloud:** It is highly virtualized cloud data center located inside company's firewall. It may also be a private space dedicated to company within a cloud vendor data center designed to handle company's workload. Your business is part of an industry that must conform to strict security and data privacy issues. A private cloud will meet those requirements [3].
-
- **Hybrid cloud:** This model of cloud computing is a composition of two cloud (public or private). Company likes a SaaS application and wants to use it as a standard throughout the company; they concerned about security. To solve this problem, SaaS vendor creates a private cloud just for the company inside their firewall. They provide company with a virtual private network (VPN) for additional security. Now you have both public and private cloud ingredients [3].

iii. Cloud computing benefits

Lower computer costs, improved performance, reduced software costs, instant software updates, improved document format compatibility, unlimited storage capacity, device independence, and increased data reliability [4].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

iv. Cloud computing drawbacks

Requires a constant Internet connection, does not work well with low-speed connections, can be slow, features might be limited, stored data might not be secure, and stored data can be lost [4].

IV. DATA SECURITY ISSUES IN CLOUD COMPUTING

Data security threats can be classified into internal threats and external threats. Internal threats, mainly come from an insider attack because cloud service providers and users, are the main reason for these threats. External threats mainly come from outside attack because data can be accessed from third party. The attacker can steal the user's personal data [5].

4.1 Data Authentication

A user may gain access within a LAN by entering a cloud identification and password, which may be affirmed by a cloud authentication mechanism. If the authentication mechanism validates the certification, the user identification and password are stored locally for subsequent authentication requests. The authentication mechanism may be applied in both domain and Workgroup LAN and may function in parallel with other users who may have a LAN or client credentials which may not be authenticated from the cloud [5].

4.2 Data Privacy and Confidentiality

Once the clients outsource data to the cloud there should be assurance that data is accessible to only authorized users. The cloud computing service provider should make secure the customer personal data is well protected from other service provider's and user. Authentication is the best solution for data confidentiality because service provider must ensure who is accessing the data and who is maintaining the server; so that the customer's personal data is sheltered. The cloud customer must be guaranteed that data stored in the cloud will be confidential [5].

4.3 Data Integrity

Data Integrity means data is complete and consistent. The data stored in the cloud may experience damage during integration operations. The cloud provider must make the client aware of what particular data are outsourced to the cloud, the native and the integrity mechanisms put in place [5].

4.4 Data Location

The cloud users did not know where the data will be hosted and in fact, their users want to know the location exactly. It requires a contractual agreement between the users that data should stay in a particular location [5].

4.5 Data Availability

Data provided by the customer is normally stored in different servers often placing in different locations or in different clouds. Data availability becomes a major legitimate issue as the availability of corrupted and relatively difficult servers [5].

V. ANALYSIS OF EXISTING SYSTEM

The data security model in cloud computing contain three layers system structure in which first layer is responsible for the user authentication, second layer is responsible for user's data encryption and protect the privacy of users through one symmetric encryption algorithm, and third layer is responsible for fast recovery of data and that depends on decryption.

5.1 Disadvantage of Existing System

Data accessing in a group members while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. The data confidentiality and efficiency of the system is very less. For accessing any particular file from cloud it takes higher amount of time as numbers of users are increasing day by day.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

VI. PROPOSED SYSTEM

Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, data accessing in a group member manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. We are going to propose a secure group members data accessing scheme, for dynamic groups in the cloud. By using applying group key and dynamic broadcast

encryption techniques, any cloud user can anonymously share data with others members within group itself. Here we are going to add the functionality of updating the data file that we are going to store on cloud server.

6.1 Flow Chart of Proposed System

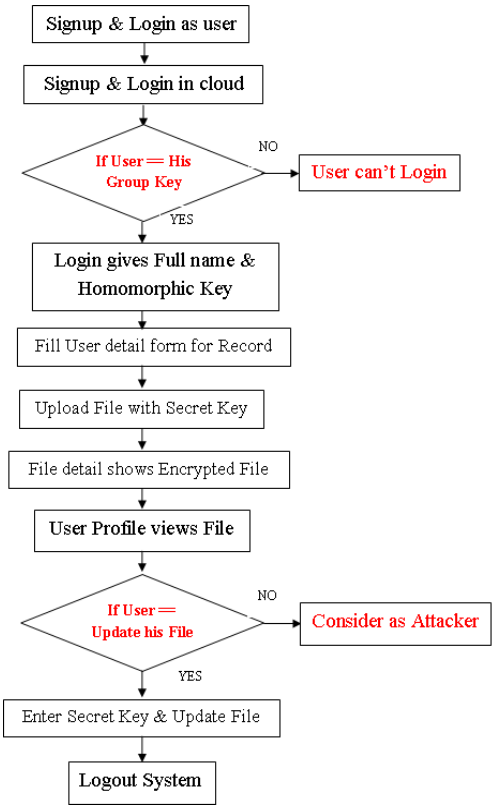

Figure 5.1: Flowchart of Proposed System

6.2 Advantage of Proposed System

By introducing Group member data accessing scheme, we are going to improve efficiency of system and also increase data confidentiality, so that system become robust and secure against malicious data modification attacks.

VII. EXPERIMENTAL RESULTS

7.1 Experiment 1

Aim: This Experiment was carried out to find the probability of attacks of the system using both traditional cloud and modern cloud with group member scheme and compare the results of both the system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Explanation: The simulation was carried out with initial efficiency of traditional cloud in which we have seen that when number of users increases then possibilities of attack also increases. But due to introducing group member scheme numbers of users are divided into different group then the efficiency of system increases and possibilities of attack decreases. Following is the graph that compares both traditional cloud and modern cloud with group member scheme. It shows that efficiency of existing system is less compared to proposed system.

No. of File accessed simultaneously	No. of User/Group	No. of Groups	Total Number of Users	Proposed Scenario (Probability of attacks)	Existing Scenario (Probability of attacks)
3	10	3	30	0.1	1
6	5	6	30	0.2	1
10	3	10	30	0.333333333	1

Table 7.1 Comparison on probability of attacks of both systems

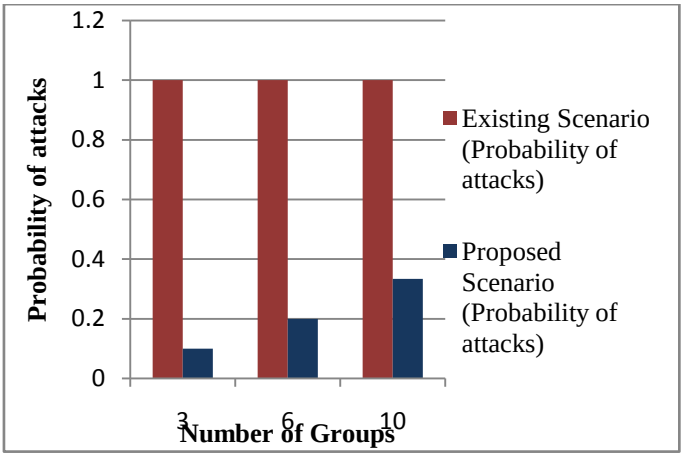

Figure 7.1: Result of Experiment -1

Conclusion: The above graph shows that modern cloud with group member data accessing scheme is more efficient compared to traditional cloud technique.

7.2 Experiment 2

Aim: This Experiment was carried out to find the file accessing time of the system using both traditional cloud and modern cloud with group member scheme and compare the results of both the system.

Explanation: The simulation was carried out with initial file accessing of traditional cloud in which we have seen that when number of users increase's then accessing time of the file also increases. But due to introducing group member scheme numbers of users are divided into different group then the efficiency of system increases and accessing time of the file decreases. Following is the graph that compares both traditional cloud and modern cloud with group member scheme. It shows that file accessing time of existing system is more compared to proposed system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

No. of File accessed simultaneously	No. of User/Group	No. of Groups	Total Number of Users	Proposed Scenario (File Accessing Time)	Existing Scenario (File Accessing Time)
3	10	3	30	0.333333333	1
6	5	6	30	0.166666667	1
10	3	10	30	0.1	1

Table 7.2 Comparison on file accessing time of both systems

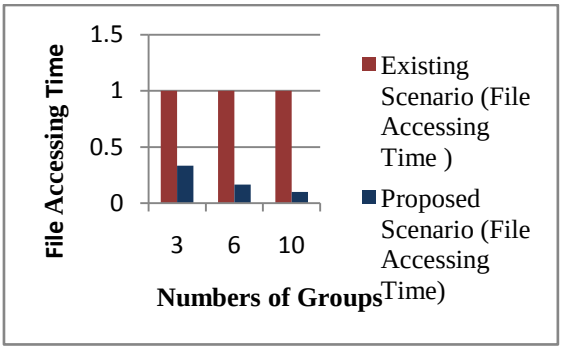

Figure 7.2: Result of Experiment -2

Conclusion: The above graph shows that modern cloud with group member data accessing scheme is more efficient compared to traditional cloud technique.

7.3 Experiment 3

Aim: This Experiment was carried out to find the overhead generation of the system using both traditional cloud and modern cloud with group member scheme and compare the results of both the system.

Explanation: The simulation was carried out with initial overhead generation of traditional cloud in which we have seen that when number of user's increases then overhead generation decreases as group member scheme is not there. But due to introducing group member scheme numbers of users are divided into different group then overhead generated here got increase. As the number of groups increase with number of users than overhead also increases. Following is the graph that compares both traditional cloud and modern cloud with group member scheme. It shows that overhead generated of existing system is less compared to proposed system.

No. of File accessed simultaneously	No. of Groups	No. of Users/ Group	Total No. of Users	Overhead generated in Bits Per Group	Per User	Proposed Scenario (Overhead Generation)	Existing Scenario (Overhead Generation)
3	3	10	30	4	1	13	10
6	6	5	30	4	1	25	5
10	10	3	30	4	1	41	3

Table 7.3 Comparison on overhead generation of both systems

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

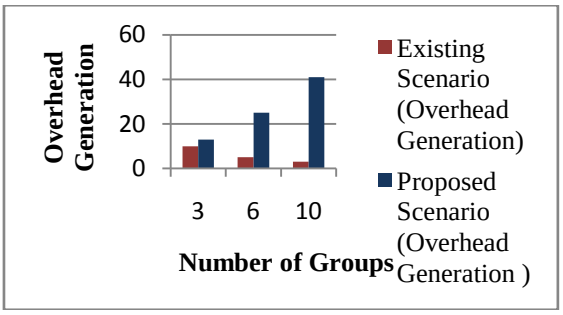

Figure 7.3: Result of Experiment -3

Conclusion: The above graph shows that modern cloud with group member data accessing scheme is not efficient compared to traditional cloud technique because it generates more overhead as group mechanism requires extra 4 bits per group.

VIII. CONCLUSION & FUTURE EXTENSION

Hereby it is concluded that our proposed system supports modern cloud computing in which we have perform cloud operation in which we encrypt the file and then upload it in cloud server and download it whenever it required. Also, we have implemented proposed system and improved efficiency of existing system by introducing group member's data accessing scheme plus going to add updating functionality to own file and also provide higher data confidentiality against malicious data modification attacks. At last we are going to compare efficiency of the system of both systems in terms of probability of attacks; probability of file accessing time and last is overhead generation.

Also, as future extensions there are many clouds security issues still to be solved. And one on the noticeable issues or disadvantage of proposed system is that as numbers of groups increased than overhead generated by group member's scheme also increases. So in future we can balance out right numbers of groups with correct numbers of users per groups. And second issue or disadvantage of proposed system is when attacker attacks on group manger and in such cases we have create additional group manager which can work as backup, when main group manager fails.

REFERENCES

[1] Nupur Gautam "Using Kerberos with Digital Signature and AES encryption to provide data security in cloud computing", proceedings of national conference on recent advancements in futuristic technologies, Volume 1-No. 1, 2013.
[2] Aparjita Sidhu and Rajiv Mahajan "Enhancing Security in Cloud Computing Structure by Hybrid Encryption", International Journal of Recent Scientific Research, Volume 5 – No. 1, 2014.
[3] Sahil Zatakiya and Pranav Tank "A Review of Data Security Issues in Cloud Environment", International Journal of Computer Applications, Volume 82 – No. 17, 2013.
[4] Eman M. Mohamed, Hetam S. Abdelkader and Sherif El-Etriby "Enhanced Data Security Model for Cloud Computing", the 8th International Conference on Informatics and Systems, IEEE CONFERENCE, 2012.
[5] N. Hemalatha, A. Jenis, A. Cecil Donald, L. Arockiam "A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing", International Journal of Computer Applications, Volume 96 – No. 16, 2014.