Cloud Security Solution: Fragmentation and Replication

Mrs. Radhika Chavan[1], Prof.S.Y.Raut[2]

[1] *PG Student, Computer Department, PREC, Maharashtra, India.*
[2] *Prof. S. Y. Raut, Computer Department, PREC, Maharashtra, India.*

ABSTRACT

Nowadays the world is known as digital world. As the use of the internet increases day by day, Cloud Computing becomes popular technology among users, customers. The customers are attracted towards the Cloud due to its offers like on-demand network access, reduced space, pay-per-use service, flexibility, scalability etc. Though the remarkable use of cloud computing, there are some hurdles to acceptance. Performance, security, availability, quality of service are the main challenges and issues cloud computing has to face. One of the most barriers is the security because users have to share their information among the cloud nodes. The location of information storage is not known to the user. In this paper, we proposed a new solution which presents the Graphical Authentication System with fragmentation and replication technique. The graphical password authentication provides a security and usability of the proposed system. Here in this system, when user upload any file that the file is fragmented and replicated to provide a better security and performance in terms of access time. When any network is not available to access then, the data will be accessed by using replicas in very short time. T-coloring method is used to assign the fragments and their replicas to improve the security. This system mainly focuses on the data and authentication system with good performance.

Keyword : - *Cloud security, fragmentation, graphical password authentication, replication, performance.*

.

1. INTRODUCTION

1.1 Cloud Computing

The term "cloud" has been used to mention to platforms for distributed computing. Cloud Computing is a kind of internet-based computing which provides dynamic resources, virtualization, flexibility, scalability to users.[3] The goal of cloud computing is to cut down the cost and allow users to take benefit from all the services provided by the cloud and helps them to focus on their core business. Cloud computing is closely related to Grid computing but different from it. Cloud computing associates the computing and storage resources controlled by different operating systems to make available services such as large-scaled data storage and high performance computing to users. Circulation of data is in a different way of cloud computing, comparing with the grid computing. Nowadays, organizations and companies are moving and spreading their business by accepting the cloud computing to lower their cost. In the cloud computing environment, customers of cloud services do not need anything means not going into detail about the implementation and they can get access to their data and complete their computing tasks only by using the Internet connection. Throughout the access to the data and computing, the clients do not even know where the data are put away or the location of the data. Thus, here the security issue stands up rapidly. Data security in the cloud computing is more complicated than data security in the traditional information systems. [2]

Therefore, it is necessary to work on the data security. This proposed system provides the security and improves the performance by using graphical password authentication system, fragmentation and replication.

The main objective for this system is as follows:

1. To design a system that will provide good authentication system which allows only authorized users to enter.

2. To provide security as well as improve the performance.

3. To provide controlled replication to increase the performance.

4. To provide a file to the client whenever there will be run time error in network.

1.2 Graphical password authentication

These days, user authentication is an essential area in the field of information security. To apply security of information, passwords were introduced. User authentication is the basic concept. Text based password is a very popular authentication method used, but it is hard to recall and easy to attacks. The first module is Authentication system to give security to the system. It uses multiple images and multipoint to avoid shoulder surfing attack. It is very secure as compared to the previous text-based system. It is very easy to remember and hard to guess. Images are different for each case and every time, so if hackers try to find or match the each combination to find the correct password will take millions of year. [4] Thus, it is more secure than previous one. This system used multiple image multi cued point technique.

1.3 Fragmentation

Splitting is used to minimize the total data transfer cost .To achieve reliability, performance, balanced storage capacity and security, fragmentation plays a vital role. Fragmentation is a process which cuts every sensitive file into several fragments in such a way that it is impossible to achieve total file in one try. The probabilities to find whole fragments are also very low. Thus, this system uses a fragmentation technique by using T-coloring method. Fragmentation is divided into horizontal, vertical and mixed fragmentation.

1.4 Replication:

Data replication methodology is very important in today's popular systems for problems such as data reliability, availability and response time. Data replication means keeping a number of replicas on the same server or on dissimilar servers. In replication data is copied and distributed from one database to another. So, it reduces the workload from the original server and the data on the server where it is copied are always active which is not present in mirroring technique. Replication decreases the chance of data loss, increases the performance, availability, reliability. [5]

1.5 Motivation

Nowadays, everyone uses the internet. The usage of internet increases day by day. The cloud computing becomes popular among users due to its services and technology. The third-party administrative control introduces security issues. This is the main obstacle for cloud computing.

Based on the studies that were done on the security issues the number of attacks disturbed the services of the cloud like Social engineering attack, XML signature wrapping attack, malware injection, data manipulation, account hijacking, data discovery, VM rollback, VM escape etc. To protect the data, this system will concentrate on security and improve the performance of the overall system. By using graphical password, fragmentation and replication techniques the system will be able to provide the security and improves the performance in terms of access time.

The essential services of cloud computing increases the risk level because data is controlled by third party.[2] The technologies like virtualization, web 2.0 creates their security issues. Thus, for using cloud computing it is necessary to understand the difference between the vulnerabilities and threats. After understanding the difference we can find what vulnerabilities are converted into threats. The traditional security methods are not fully solved the problem of security.

2. RELATED WORK

As the frequency for using internet increases, threats, attacks also increases. Therefore, number of researchers works on security issues in cloud.

As the popularity of cloud computing increases day by day, the security issue also arises.[6] The most features of cloud computing which attracts the customers are flexibility, scalability, broad network access, reduced cost. Trust plays a vital role in cloud computing. Here the new security method , Trusted Third Party introduced which is based on the cryptography to ensure the confidentiality, security and authentication. Availability and quality of service is not fully maintained here.

The key principles of the security are availability, integrity and confidentiality. [7]This system based on cryptographic encryption and token generation. The division method is used to distribute the data which prevents the system from single point failure situation. This paper also discussed the previous existing systems. This system checks for authorized user and then user uploads the file. This file is divided and stored with encryption. Token is generated to check whether the file is correct or not. The security provided by this system but at a time performance is not increased.

The replication is required to increase the availability of resources. It creates a copy of any file. This system [8] presented the topic of data replication in geographically distributed cloud computing data centers and introduced a unique replication solution which differs from traditional method. It works on availability of network bandwidth, optimizes energy efficiency of the system. The optimization of communication delays in this system states the quality of user experience increased.

The new system, [1] presented the cloud security solution which is not a cryptographic technique. This nature of method avoids the time delay. Here the user uploads the file then, that file gets divided and then replicate over the cloud nodes for security purpose. T-coloring and centrality terms are used for security and performance in terms of retrieval time. The single point failure avoids and increases the availability with performance. This system does not work on the security of the authentication system.

The main computer security starts with authentication system which basically includes the user name and password. But by using text-based password system the probability to attack is high. It is also difficult to remember or recall during login process. Thus, to overcome these problems graphical password authentication is the new alternative solution developed. [4] It is natural that any person remembers the images as compared to the numbers or text. This system prohibits the attacks like shoulder surfing, dictionary attack etc. Here this proposed system collectively work on performance and security. By using graphical password system, security provided to the authentication system which is not provided in existing system.

3. PROPOSED SYSTEM OVERVIEW

This proposed system includes three main parts:

1. Graphical Password Authentication
2. Fragmentation
3. Replication

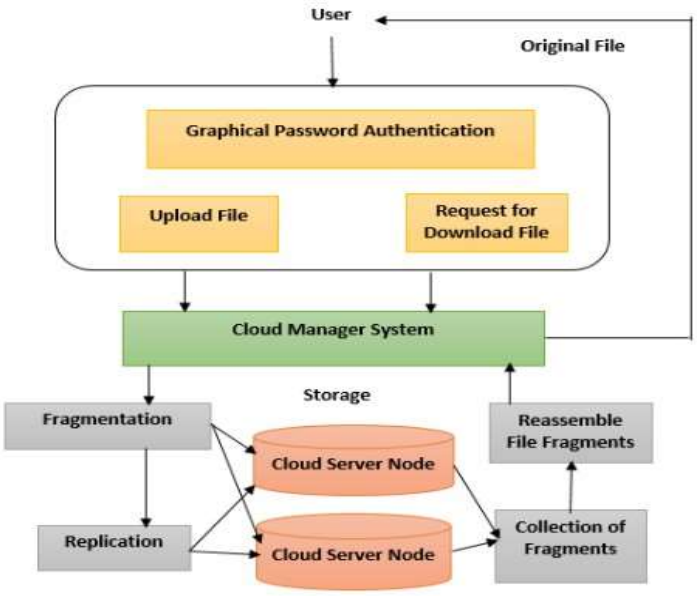

Fig. 1: Proposed System Architecture

Figure shows the architecture of the proposed system. As illustrated, in the design, first registration process completed by giving the information about the user. Then that authorized user login to the system. Here this system provides graphical password authentication methodology which provides a good security. This is an alternative solution to text-based authentication, which is very susceptible for attacks. After the authentication process user enters into the system. User uploads his file on the system and request for that file whenever he wants to access that file.

Then the cloud manager system parts begin. That uploaded file gets fragmented in such a way that fragments do not include the meaningful information. Fragmentation is done by using binary fragmentation. Here any type of file gets fragmented, which is not present in previous method. T-coloring is useful while placing that fragments on a cloud node. This helps to keep away the attacker from finding the location of next fragment.

After the fragmentation process that fragments get replicated on a cloud node in such a way that the access time will be low which increases the performance. Here this system provides the controlled replication which is necessary to manage the ideal performance. If at the time of network error or network is not accessible then the fragment is accessed from the replicas within very short period.

4. ALGORITHMS

The algorithmic steps are as follows:

4.1 Graphical password algorithm

1. Start the authentication process.
2. The Server-side calculation is done, which is based on username.
3. User has to select the image and select point on that.
4. This process repeats more than one time.
5. The combination of server and user created the password.

By using multiple image multi point cued technique attacks like shoulder surfing, brute force will be prohibited.

4.2 Fragment Assignment

1. Take inputs as file fragments.
2. Select the nodes for assignment of fragment in such a way that node is very close to the cloud network for access by using centrality measure.
3. Now using T-coloring concept, check if the node has the open color and its size is greater than the size of the fragment.
4. Then generate positive random number and create a set which starts from zero.
5. Assign initially all nodes as open color.
6. Assign close color after the assignment of node.
7. Repeat the process until all fragments assign to the node.

After authentication process user uploads the file and then the cloud manager's part begins. The fragmentation process is used for fragmenting the user files. All the fragments can upload to various node in different region. Once the file is fragmented, the initial node among the fragments should be determined. Based on that, the retrieval process can be done. The cloud manager should locate the initial node in secured manner, so that no-one can achieve the information about the storage node. The amount of compromised data can be reduced by making fragments of data file and storing them on separate nodes.

Therefore, the probability of finding fragments on all of the nodes is very low. In cloud systems with thousands of nodes, the probability for an attacker to obtain a considerable amount of data reduces significantly. To improve the data retrieval time, fragments can be replicated in a manner that reduces access time. [1]

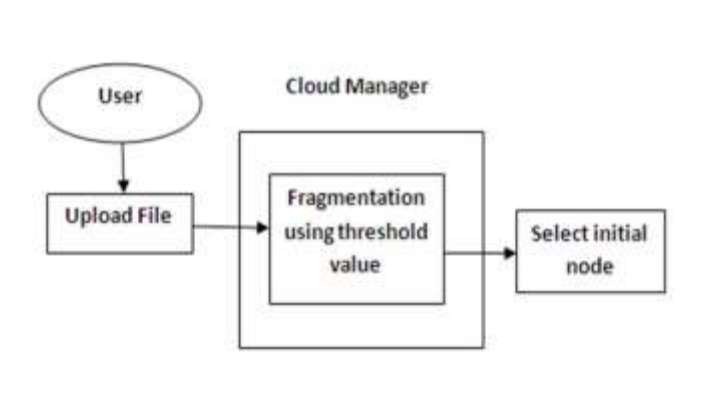

Fig. 2: Fragmentation Process

4.3 Fragment Replication Assignment

1. Take inputs as file fragment replicas.
2. Select the node if the node has the open color and its size is greater than the size of the fragment. Assign close color after assignment of replicas.
3. The remaining replicas are assigned randomly to the nodes which are not assigned yet.

4.4 Mathematical Model

S = { I, P, R, O }
Where,
I is set of Initial Input to the system.
I = {i1, i2, i3}
i1 = File given by the user.
i2 = Download request from User.
i3 = Download request from Client.

P is set of procedure or function or processes or methods.
P = {p1, p2, p3, p4, p5, p6, p7, p8}
p1 = Registration and Authentication.
p2 = Uploading a file on cloud server.
p3 = Fragmentation of file received from user.
p4 = Replication of that file.
p5 = Download Request from user.
p6 = Download Request from client.
p7 = Collection and reassemble of fragments.
p8 = Downloading the original file.
R is a set of rules or constraints.
R= { r1}

r1 = File accessed from Replication when network is busy.
O is a set of outputs.
O = {o1 }
o1 = Downloading the original file.

5. RESULTS

In this system the main focus is to give security to data and authentication system as well as performance in terms of retrieval or access time. The graphical password authentication system provides a better security than the text-based system.

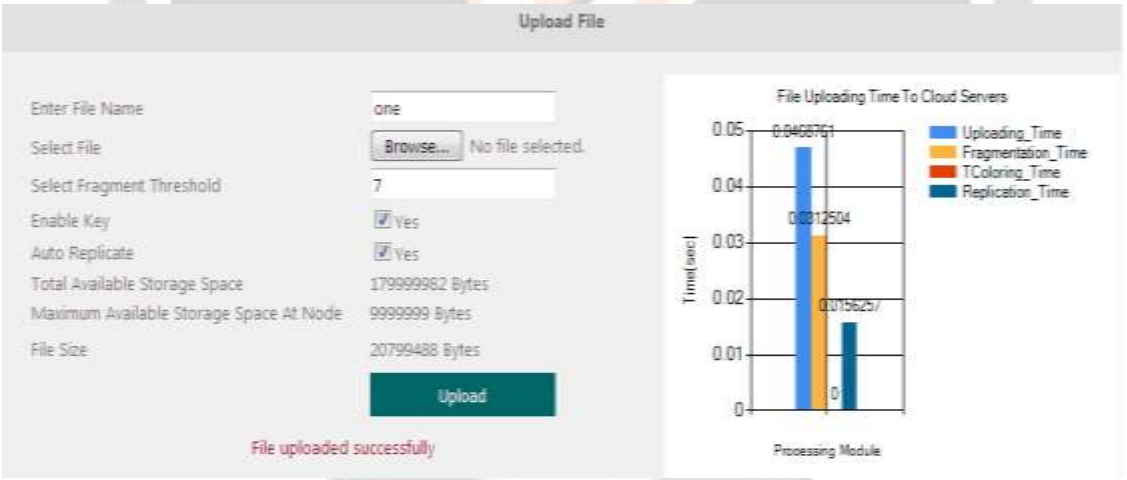

Fig. 2: Upload File Process

This above figure shows, the fragmentation value and file upload processing time.

The proposed system downloads the file within very short period whenever there will be any case like network busy, network run time error. It is due to the replication.

Table 1 : Comparison of two systems

Sr. No.	Existing System	Proposed System
1	Security to data only	Security to data and authentication system
2	User waits while network not available	The data collects from replicas within short period

The figure shows the gap analysis between existing i.e. DROPS (Division and Replication) and proposed system (Secure Methodology Fragmentation and Replication) i.e. SMFR. The existing system gives the file to the client whenever request comes. But when network is busy then existing system waits for network free. But in proposed system manager will take the fragment from replica and send the message to the user. The download time of existing system is greater than the proposed system.

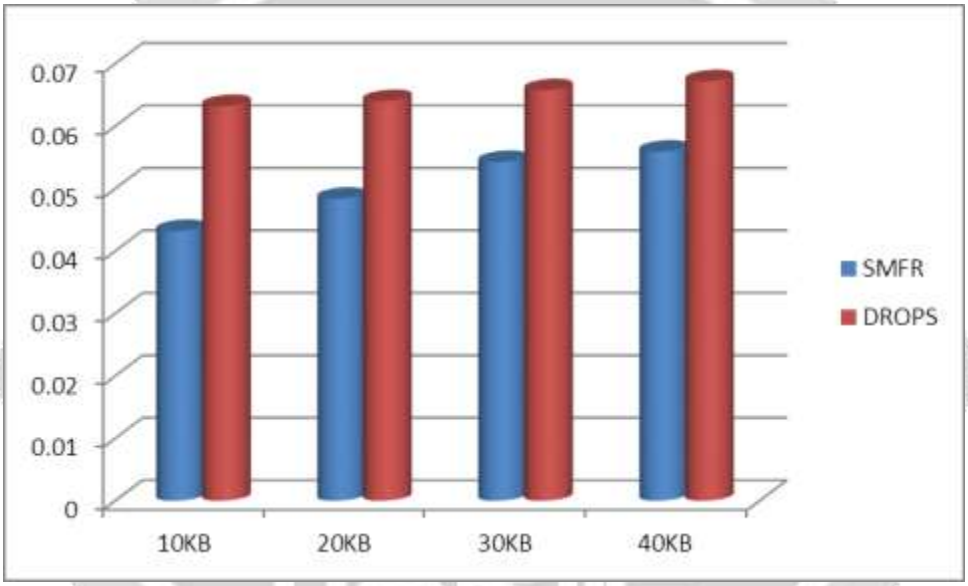

Fig. 3: Gap Analysis between two systems

The hardware configuration may change the results because the speed of processor, network bandwidth , node size, fragment size also gives results different.

6. CONCLUSION

Cloud computing growth raises the security concern due to its core technology. So, this system provides a better solution to achieve the security as well as performance by using three techniques, Graphical Password Authentication, Fragmentation and Replication. Nowadays, the use of the Graphical Password Authentication increases because it is very easy to remember and secure as compared to alphanumeric method. Fragmentation used to protect data from single point disaster. Replication can be useful for maintaining availability, reliability and performance in failure situations. But the extra replication can also result in high storage cost or drops in systems overall performance due to extreme use of bandwidth. So, here controlled replication is used. The future work will saves the time and work on some attacks.

7. ACKNOWLEDGMENT

I would like to thank my project guide Prof. S. Y. Raut, for her personal involvement and constructive suggestion throughout the work. We would like to thank to our Principal Dr. R.S. Jahagirdar for providing me an opportunity to work on this topic and his valuable support for my work.

8. REFERENCES

[1]. Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya ,DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security, IEEE Transactions On Cloud Computing,2015,in press.

[2]. Keiko Hashizume, David G Rosado, Eduardo FernndezMedina, Eduardo B Fernandez,An analysis of security issues for cloud computing,Journal of Internet Services and Applications,2013.

[3]. L. M. Kaufman, Data security in the world of cloud computing, IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[4]. Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare , Graphical Password Authentication Cloud securing scheme , 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014 IEEE .

[5] Manisha Kalkal, Sona Malhotra, Replication for Improving Availability and Balancing Load in Cloud Data Centres, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[6] Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman, Secure Overlay Cloud Storage with Access Control and Assured Deletion, IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 6, November/December 2012.

[7] A. Mei, L. V. Mancini, and S. Jajodia,Secure dynamic fragment and replica allocation in large-scale distributed file systems, IEEE transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003.

[8] D.Boru, D.Kliazovich, F.Granelli, P.Bouvry,and A.Y.Zoma ya, Energy-efficient data replication in cloud computing datacenters, In IEEE Globecom Workshops, 2013,

[9] Bharti Dhote,A.M.Kanthe,Secure Approach for Data in Cloud Computing, International Journal of Computer Applications (0975 8887) Volume 64 No.22, February 2013.

[10] S. U. Khan, and I. Ahmad, "Comparison and analysis of ten static heuristics-based Internet data replication techniques," Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008.

[11] J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, "Selecting the right data distribution scheme for a survivable storage system," Carnegie Mellon University, Technical Report CMU-CS-01-120, May 2001.