© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Providing Security to Data in Cloud by Using new Methodology Fragmentation and Replication

Radhika Chavan*, Prof. S. Y. Raut
Computer Engineering Department, Pravara Rural Engineering college, Loni, Maharashtra, India

ABSTRACT

As the use of the internet increases day by day, Cloud Computing becomes popular technology among users, customers, in scientific field and industries. 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 tremendous use of cloud computing, there are some barriers to adoption. 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. User only uses the services provided by the cloud. 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. Fragmentation avoids the single point failure situation and replication improves the availability as well as performance. T-coloring method is used to assign the fragments and their replicas to improve the security.
Keywords: Cloud Security, Fragmentation, Graphical Password Authentication, Replication, Performance

I. INTRODUCTION

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. 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.

1) 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 attack like dictionary attacks, guessing attacks, brute force attacks, social engineering attacks etc. So, graphical password authentication is a promising solution to the text-based authentication. In this method selectable images are used or more than single images selected and user has to select point from that image which creates a password.

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.

2) Fragmentation

Fragmentation 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 probability to find whole fragments is also very low. Thus, this system uses a fragmentation technique by using T-coloring method. Fragmentation is divided into horizontal, vertical and mixed fragmentation.

3) 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 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]

II. METHODS AND MATERIAL

1. Related Work

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

Need for Security

The essential services of cloud computing increases the risk level because data is controlled by third party. [3] 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.

As the popularity of cloud computing increases day by day, the security issue also arises.[2] 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.

Security Solution : Fragmentation Method

The key principles of the security are availability, integrity and confidentiality. [9]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.

Security Solution: Replication Method

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 canters 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.

I. PROPOSED SYSTEM OVERVIEW

This proposed system includes three main parts:

1. Graphical Password Authentication
2. Fragmentation
3. Replication

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.

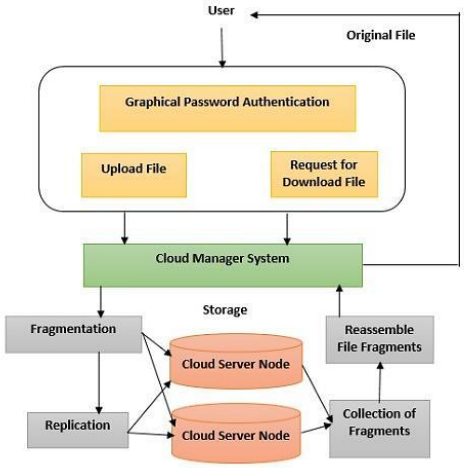

Figure 1: Proposed System Architecture.

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. The implementation includes following algorithms.

A. Graphical password algorithm

1. Start the authentication process.
2. User has to select the image and points in that image.
3. This process repeats more than one time.
4. The combination of multiple images and multiple points created the password.

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

B. Fragment Assignment

1. Take input.
2. Select the nodes for assignment of fragment which is very close to the cloud network for access by using centrality measure.

3. Then generate positive random number and create a set which starts from zero.
4. Assign initially all nodes as open color.
5. Now using T-coloring concept, check if the node has the open color and its size is greater than the size of the fragment.
6. Assign close color after the assignment of node.
7. Repeat the process until all fragments assign to the node.

C. 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.

II. RESULTS AND DISCUSSION

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. This graphical password used multiple images and selects the multiple points. This is used when user wants to login the system. In next figure the two points are selected which is used at the time of login. This reduces the shoulder surfing attack.

Figure 2 : Graphical Password Authentication

Then, user login and uploads the file. The time required to upload and download described in following table which may get different results by using 3G or 4G networks. The upload and download time basically depends on network type and bandwidth. The hardware configuration also changes in results. This system provides security by using fragmentation and replication. Secret key like a one-time password is generated while uploading the file which is then used to download the file safely. In the next figure the processing time is calculated when the file is uploaded. The time varies with increase in file size, threshold size and network speed and bandwidth.

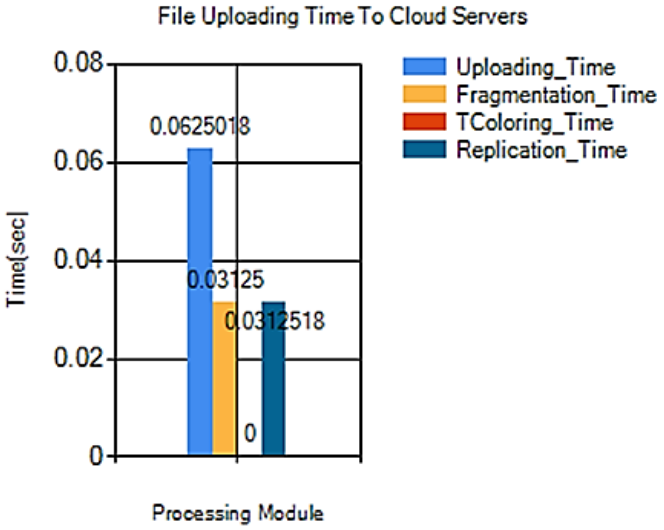

Figure 3: Processing time for file

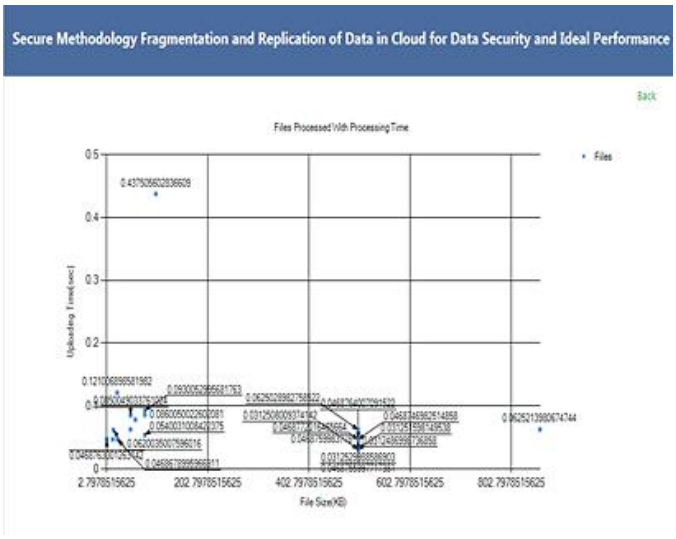

Figure 4 : Performance Graph

Performance graph in figure 4 changes with updates like uploads the number of file over cloud server.

This system also uses the parameters like size of nodes, storage capacity, size of fragments to check the performance and security. This table shows the increase the time with increase in file size.

TABLE I : The performance in terms of time.

File Size	Fragment No.	Total Upload Time	Network type 2G/3G/4G
500KB	2	0.046876	4G
500KB	3	0.031253	4G
500KB	4	0.0312487	4G
500KB	5	0.0312516	4G
500KB	6	0.0468747	4G
500KB	7	0.0312508	4G
500KB	8	0.0468764	4G
500KB	9	0.0625029	4G

The system access the file easily when there will be any run time error or network problem by using replicas.

III. 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 work on auditing the fragments, attacks and time.

IV. 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.

[2] Keiko Hashizume, David G Rosado, Eduardo Fernndez Medina, 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.

[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.