Improved Cloud Security Approach with Threshold Cryptography

Manish Mishra
M.Tech. Scholar, Computer Science & Engg.
JNCT, Bhopal, India
Redefine_manish@yahoo.com

Dr. Mukta Bhatele
Associate Professor Computer Science & Engg.
JNCT, Bhopal, India
mukta_bhatele@rediffmail.com

Abstract: **The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un trusted. Since cloud computing share disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading cause of hampering its development. Cloud computing security has become a hot topic in industry and academic research. This paper has made an extensive survey over existing approaches which secures the environment and also propounded a framework to be implemented to secure data outsourcing by deploying threshold based cryptography , and the same is being evaluated on the basis of different parameters.**

Keywords: Cloud computing; Security; Encryption; Decryption; Threshold Cryptography.

I INTRODUCTION

Cryptography has evolved from the earliest forms of secret writing to current era of computationally secure protocols, addressing range of security issues. In modern age, cryptography is not only about encryption, but it has larger objective of ensuring data protection from adversary's activities. Scope of modern cryptography also includes techniques and protocols to achieve authentication, non-repudiation, and integrity objectives. Complexity of cryptology methods and its applications have continuously increased and evolution of computers has given a completely new dimension to this. Now cryptography problems/algorithms are measured in terms of computational hardness. In this journey, cryptography has always received a threat of getting obsolete because of rapidly increasing computational capabilities. However, cryptography techniques still have great relevance and importance for modern ICT (Information and Communication Technology), and ICT enabled industry to keep them protected from dynamically changing threat scenarios [6].

It is a tool for providing simple, needed network access to shared resources of configurable computing environment (network, storage etc) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Today most of the companies have to process huge amounts of data in a cost- reducing manner. Classic users are operators of Internet search engines such as Google, Yahoo, or Microsoft. The vast amount of data they have to deal with every day has made database solutions more expensive.

Cryptography is the science of encrypting information. It provides the services of confidentiality, integrity and non-repudiation to support information protection. In general, these services are realized by two cryptographic primitives. The encryption primitives can be used to provide confidentiality and the authentication primitive can be used to provide data integrity and non-repudiation. Few most popular encryption schemes are AES, DES, SHA, IDEA, RC5, RSA, ECC etc.

II CLOUD COMPUTING

A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand [4].

2.1 RELATED CONCEPTS

2.1.1 DEPLOYMENT CLOUD MODELS

Public cloud: the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.

Private cloud: the cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS [7].

Community cloud: the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.

Hybrid cloud: the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

2.1.2. CLOUD CHARACTERISTICS

- On demand service.
- Ubiquitous network access.
- Easy use.
- Business model.
- Location independent resource pooling.

2.1.3. CLOUD SOLUTIONS

- Infrastructure as a service (IaaS)
- Software as a service (SaaS)

- Platform as a service(PaaS)

III CLOUD SECURITY CHALLENGES

The cloud services present many challenges to an organization. When an organization mitigates to consuming cloud services, and especially public cloud services, much of the computing system infrastructure will now under the control of cloud service provider. Many of these challenges should be addressed through management initiatives. These management initiatives will requires clearly delineating the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of customer. Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization. Here are security risks list [10].

Regulatory compliance: cloud computing providers who refuse to external audits and security certifications.

Privileged user access: sensitive data processed outside the organization brings with it an inherent level of risk.

Data location: when you use cloud, you probably won't know exactly where your data hosted.

Data segregation: data in the cloud is shared environment alongside data from other customers.

Recovery: even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.

Investigative support: investigating inappropriate or illegal activity may be impossible in cloud computing.

Long term viability: you must be sure your data will remain available even after such an event [9].

IV THRESHOLD CRYPTOGRAPHY

The basic working of the security achievement is based around sharing secret and retrieving the same collaboratively using Shamir's Approach (Shamir, A., 1979). The basic idea is to divide the secret into 'n' parts by following approach (Pareek P., 2013):

We choose at random (k-1) coefficients i.e. $a_1 \ldots a_{k-1}$

- We divide our secret S by picking a random degree polynomial

$$q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

where $a_0 = S$ (i.e the SECRET), and $a_1, a_2, a_3, \ldots, a_{k-1}$ are assumed positive integers.

Now if we wish to divide the secret into n parts, we will substitute 'n' different values of x in the polynomial q(x) and obtain n such sets of (x, y), here y is our polynomial q(x).

The essential idea of threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes "k" points to define a polynomial of degree "k-1".

Select "k" sets, any k combination of the available n parts will generate the same result. The value in these sets are meaningless alone, it is only when "k" sets are brought in together and further worked upon that we get our secret back. These "k" instances of original polynomial are processed using Lagrange polynomials.

The Lagrange basis is:

$$l_1 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2}$$

$$l_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2}$$

$$l_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1}$$

Substitute the values of x from the selected "k" sets into the Lagrange basis and we obtain "k" fractional equations for the same. Finally on taking summation of the equations obtained from Lagrange basis and y form the selected "k" sets, we get back our original polynomial. The summation can be represented mathematically as:

$$f(x) = \sum_{j=0}^{2} y_j l_{j(x)}$$

And hence we can generate the aforesaid polynomial again and can recover the secret as a_0 in the generated polynomial.

Along with aforesaid approach, we will also implement proactive share updates to enhance the security. This will be done from the end of user by calculating shares periodically with different sets of prime numbers, every time to improve the security factors. Each time adversary tries to compromise next node, the only thing in his hands will be failure as with different sets (generated by different set of prime number) of shares, there is no way to recover the secret [13].

V EXISTING WORK

AlZain et al [1] made a survey and suggested research related to single and multi-cloud security and addresses possible solutions. He proposed and supported the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

Sharma B. [2] introduces the existing issues in cloud computing along with network security and proposed a security framework to achieve secure cloud platform using Elliptic Curve Cryptography.

Venkataramana, K.&Padmavathamma M. [3] proposed an another security architecture in which they have used threshold data sharing technique to be used in federation of clouds which allows data privacy and security in transit between them.

Buyya et al. in [4] suggests a cloud federation oriented, just-in-time, opportunistic and scalable application services provisioning environment called Inter Cloud. As a result Cloud application service (SaaS) providers will have difficulty in meeting QoS expectations for all their consumers. Hence, they would like to make use of services of multiple Cloud infrastructure service providers who can provide better support for their specific consumer needs. This kind of requirements often arises in enterprises with global operations and applications such as Internet service, media hosting, and Web 2.0 applications. This necessitates building mechanisms for federation of Cloud infrastructure service providers for seamless provisioning of services across different Cloud providers.

Even within the cloud provider's internal network, encryption and secure communication are essential, as the information passes between countless, disparate components through network domains with unknown security, and these network domains are shared with other organizations of unknown reputability[6].The confidentiality of sensitive data must be protected from mixing with network traffic with other cloud hosts. If the data is shared between multiple users or clouds, the CSP must ensure data integrity and consistency. The CSP must also protect all of its cloud service consumers from malicious activities or data modification [7].

Subashini and kavitha[5], has discussed various security issues at various service models like Data, Network security, Data locality & integrity, Data segregation, Data access, Authentication and authorization. In the case of federated clouds this becomes more serious issue that is to be addressed. For computation exchange of data between clouds in federation is necessary so both privacy and integrity of data should be considered.

Li et. Al [8] in their paper proposed an approach to secure Personal Health records over Cloud environment by using attribute based encryption and focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of the proposed scheme.

Sudha, M., & Monica, M. [13] investigated the existing security schemes to ensure data confidentiality, integrity and authentication. They have employed RSA and AES and SHA algorithms to expound a hybrid security structure for cloud computing environment and have verified the test cases of their modelin the a simple cloud setup.

Arockiam, L., &Monikandan, S. [12]discussed reliable and flexible approach to users to store and retrieve their data at anytime and anywhere. Cloud computing is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage. This paper proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is described in detail and the decryption process is reverse of the encryption. This algorithm is used in order to encrypt the data of the user in the cloud.

Kaur, G., &Mahajan, M. [14] analyzed the performance of security algorithms, namely, AES, DES, BLOWFISH, RSA and MD5 on single system and cloud network for different inputs. These algorithms are compared based on two parameters, namely, Mean time and Speed-up ratio.

Sanyal, S., &Iyer, P. [15] proposed an algorithm which uses AES technique of 128/192/256 bit cipher key in encryption and decryption of data. AES provides high security as compared to other encryption techniques along with RSA.
There are many other approaches existing and been tested to make data outsourcing in Cloud computing environment bit more secure.

VI PROPOSED APPROACH

The main entities in the proposed algorithm are cloud users, cloud storage server, cloud manager, key splitter servers, share holder servers, security servers, log editor which are defined in detail as follows:
1. **User**: The user can create, update and delete his/her profile, store and retrieve the data.
2. **Cloud Storage Server**: It is a model of data storage on virtualized storage pools or servers located remotely. Cloud storage can be used by users to store their data. Users can buy storage capacity from the cloud hosting companies. The main responsibilities of cloud storage server are storing the encrypted document, storing the splitted encryption key values for the purpose of key management .
3. **Key Management Server**: Key splitter server splits the encryption keys into different shares and store the splitted keys in different share holder servers.
4. **Share Holder Server**: These servers stores the shares for the different keys for different users. Share holders can be of two types. Primary share holder directly receive the shares from the cloud manager. Secondary share holder at the leaf level and these share holders receive their shares through primary share holders.
5. **Log editor**: It checks the share holder servers timely to see if the shares are getting modified.
6. **Security server**: It has the encryption decryption algorithm.

6.1 Encryption process

Step 1- Split the letter of modified plaintext.
Step 2- Assign the position(i) of the letter.
Step 3- Generate the ASCII value of plaintext letter.
Step 4- E=(p+k+i)
p-plaintext, k-shared key, i-position
Step 5- Generate the ASCII character of the corresponding decimal value
in the result from the above given formula. This would be the cipher text.

6.2 Decryption process

Step 1- Generate the ASCII value of the cipher text character.
Step 2- Same encryption key is used.
Step 3- Assign the position i of the cipher text.
Step 4- D=((c-k-i)+256)
p-plaintext, k-shared key, i-position.

Step 5 Generate the ASCII character of the corresponding decimal value in the result from the above given formula. This would be the original plain text.

Log editor checks in period of 60 sec if any share gets updated. If no key updates are performed the primary share holders are used in decryption process. If a primary share holder gets updated other primary share holders are also checked. If more than half are unchanged the unchanged values are used. Table 3.1 shows the actions that should be performed for different values of primary and secondary share holders.

6.3 Cloud Manager

It consists of a voter module and a security server module. Security server has the encryption decryption algorithm and the voting module in cloud manager performs the voting to check whether the share key holder is authentic or not. System reliability is increased by using the voting technique. It is assumed that the communication channel between the client and cloud manager is secure. Figure 1 shows the different modules in the cloud manager.

The proposed technique is suggested for the cloud systems using symmetric encryption.

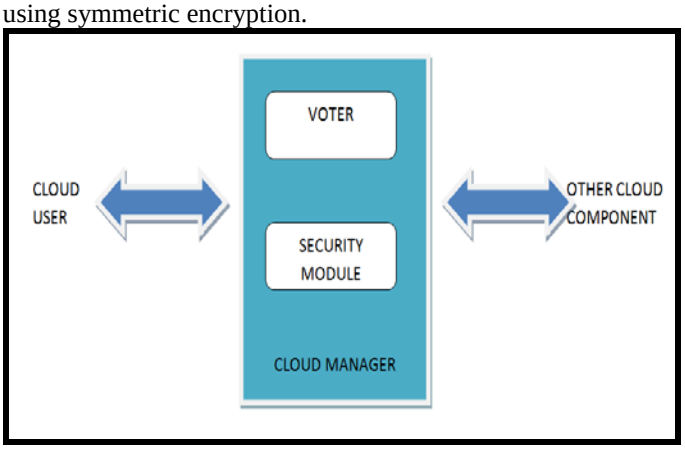

Figure1: Cloud Manager.

6.4 Share Renewal Phase

The keys are assumed to be stored in a hierarchical way. The secondary key manager distributes the shares to the primary key holders. Primary key holders in turn distribute the secret to the secondary key holders. The shared keys will have a crypto period. When this period is about to expire all the shares will be renewed. The values of shares that the share holders are having should also be monitored from time to time since there may be a possibility of some of the shares being modi_ed by the attackers. Figure 2 shows how the primary and secondary share holders are monitored by the log editor.

6.5 Overview of voting technique

Security and privacy of users data is preserved in the proposed technique by the replication of key share among several clouds, but the use of the secret sharing approach, and using a voting method to check the integrity of shares. Figure 3 shows how the voting is performed by the voter module in cloud manager.

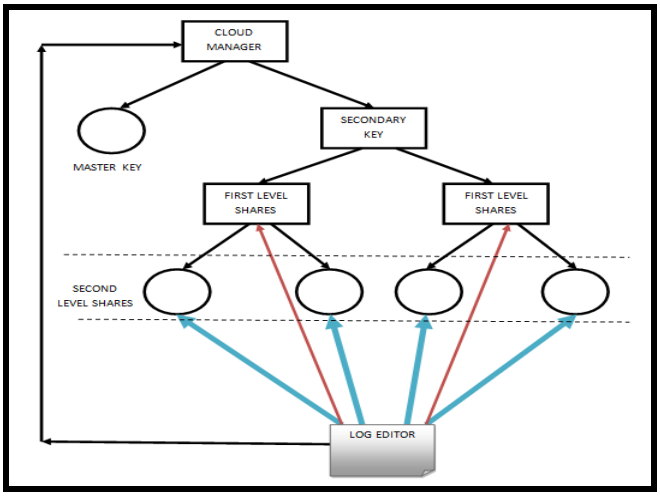

Figure 2: Proposed Key management scheme in cloud

6.7 Working of proposed system

6.7.1 File Upload

When the cloud user wants to submit a file to a cloud first the file is forwarded to the cloud manager. Security module in cloud manager generates the key and encrypts the file using the encryption algorithm as shown and then forwards the key to key management module. Encrypted file is forwarded to the cloud data storage center. Key management module divides the key into number of shares.

Sends a master key to the cloud user and distributes all the remaining keys to the Share Holder Servers. All the primary share holders and secondary share holders are monitored from time to time to ensure that their values are not modified by attacker.

The file upload consists of following communications:

1 User requests to upload a file in cloud system.

2(a) Encrypts the file. Forwards the shares to the secondary key manager.

2(b) Forwards the master key to the cloud user.

2(c) Forwards the encrypted file to the data storage server.

3 Key manager distributes the shares among the share key holders.

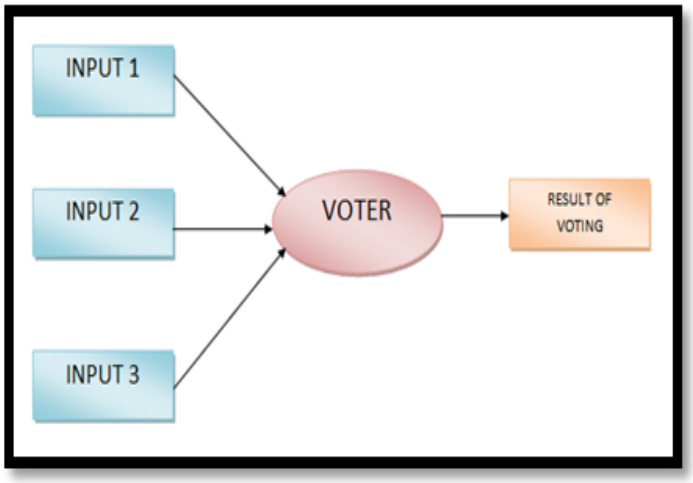

Figure 3: Voter in Cloud Manager Module.

6.7.2 File Download

When the cloud user wants to download a file that is stored in cloud file name and shared master key are entered by cloud user. Download request is forwarded to key management server. Key management server requests all the Share Holder Servers.

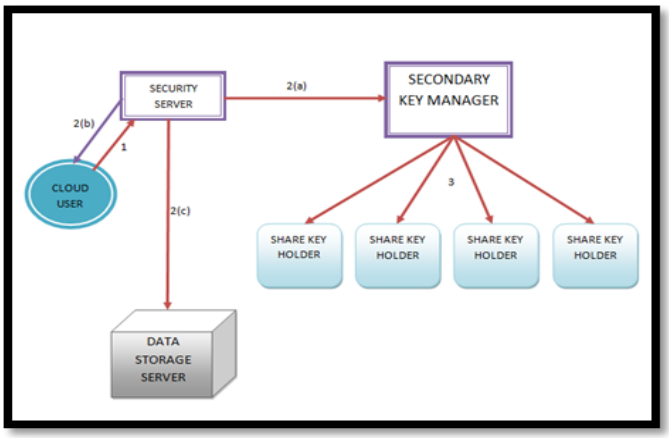

Figure 4: Communication in file upload.

to forward their part of keys that correspond to the file name required to it. Key management server combines all the shares to generate the 2nd level keys and forwards the key to the security server Security server combines the master key with other secondary key to generate the main key. The file is decrypted and is sent to the cloud user.

Figure 5 shows the process of file downloading. It consists of the following data communication:

1(a) Request to the security server for file downloading.

1(b) Request to cloud user to provide master key that was given in the encryption process.

1(c)Master Key provided by cloud user.

2(a) Request to data storage server to send the encrypted file as requested by user.

2(b) Data storage server sends encrypted ile to cloud storage server.

3(a)Security server enquires the secondary key from the key manager.

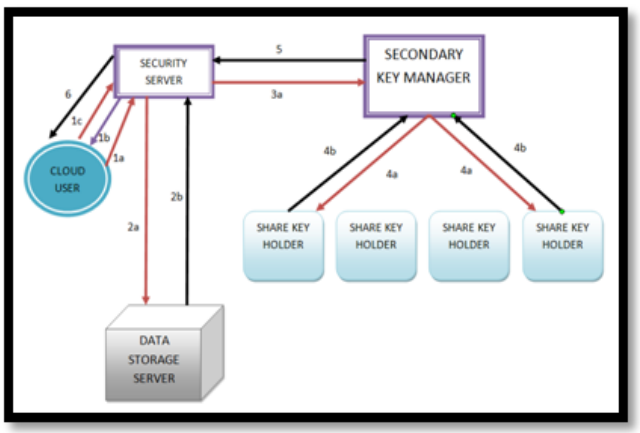

Figure 5: Communication involved in file download.

4(a) Key Manager request the share from the different share holders.

4(b) Share holder servers forward their shares corresponding to the user to the key manager.

5. Key manager combines all the shares and sends it to security server.

6. Security server combines the master key provided by the user and the secondary key provided by key management server and generates the actual key. Then, It decrypts the user file stored in cloud and send it to the user.

VII SIMULATION RESULTS

The implementation is done using the following tools and techniques:

- Cloud Sim
- J swings

Cloud Sim is a web app that runs in a virtual machine on the Amazon Web Services (AWS)cloud.

It allows users to launch, terminate and monitor virtual machines in the AWS cloud.

Different configurations can be launched, depending on the requirements, and available machines on the cloud.

Each Cloud Sim configuration map to a constellation, which are collections of multiple virtual machines running together.

The proposed technique is implemented with different file size ranges from 100KB to 50MB and we try to find out performance comparison between a existing technique and the proposed technique. The key provided from AWS is the token that allows Cloud Sim to access AWS on behalf of the AWS user. For our implementation 128 bit key is used and n=128.

Following snapshots illustrates the aforesaid experimental setup expounding Cloud manager module, user upload and download module etc.

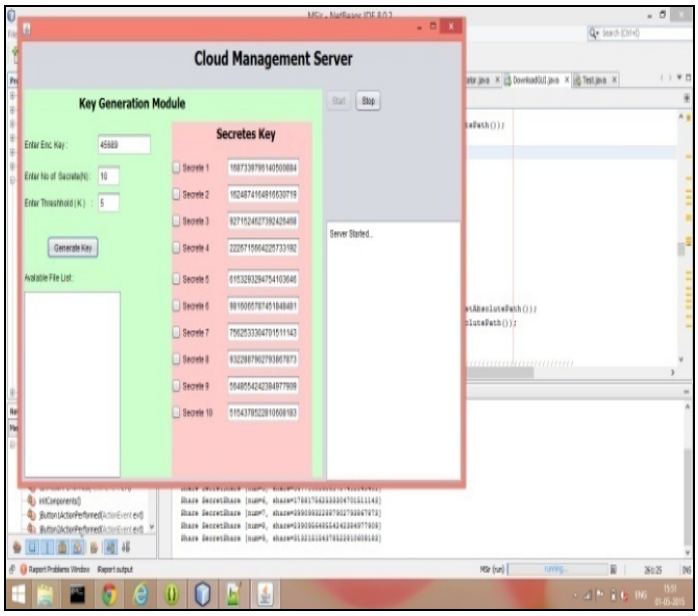

Figure 6: Cloud Manger server.

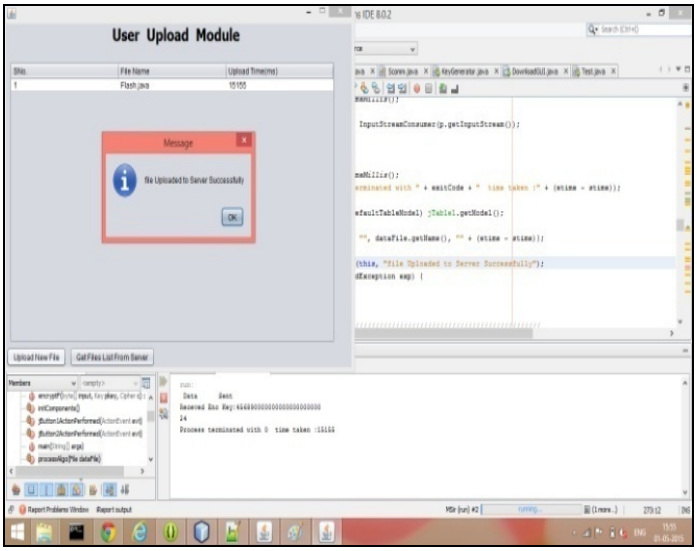

Figure 7: User upload module.

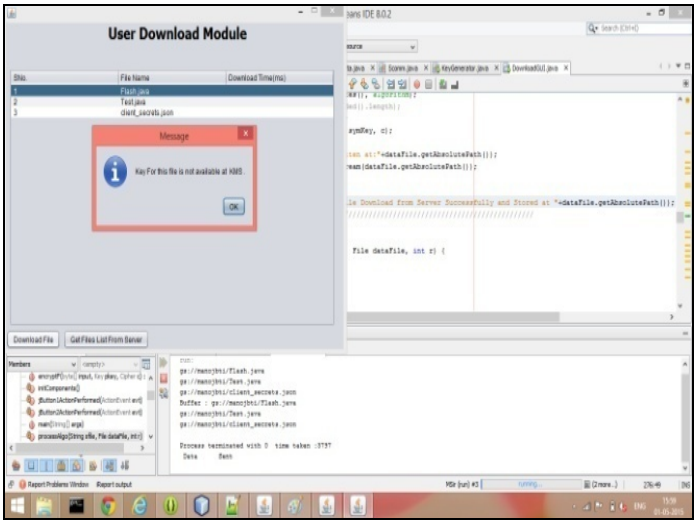

Figure 8: User download module.

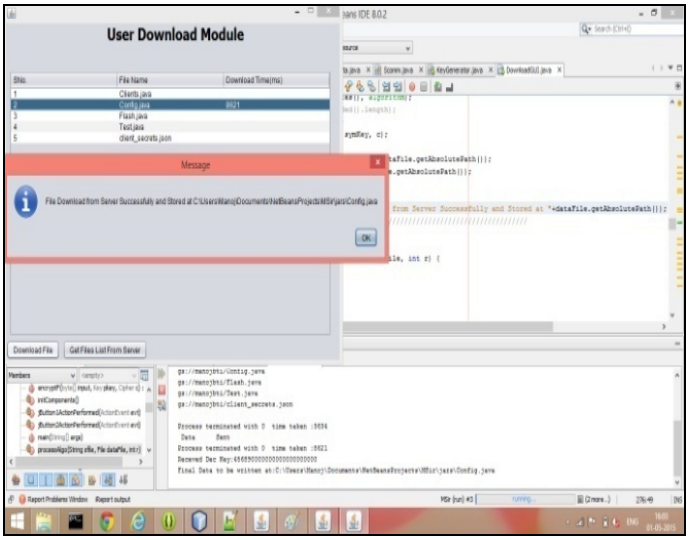

Figure 9: User download module illustrating downloaded file.

Now this experimental setup is used to evaluate the performance of implemented approach on the basis of few parameters such as:

- File size versus time of file downloading
- File size versus time of file uploading
- Key recovery time from shares
- Key dispersal for a 192 bit key

Following graphs illustrates performance of the approach implemented:

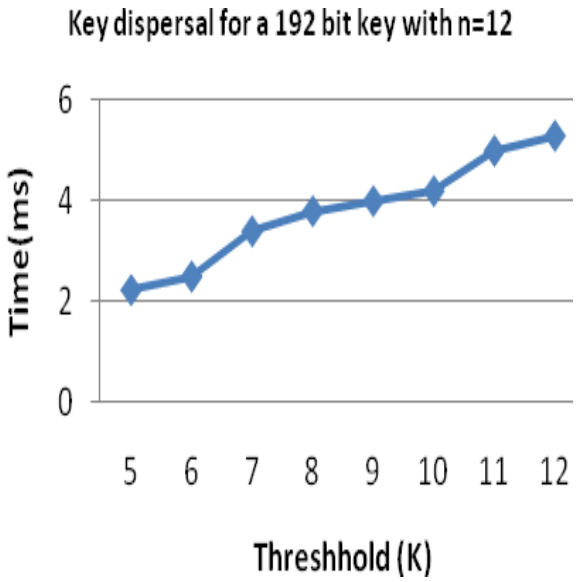

Figure 10: Key dispersal for a 192 bit key.

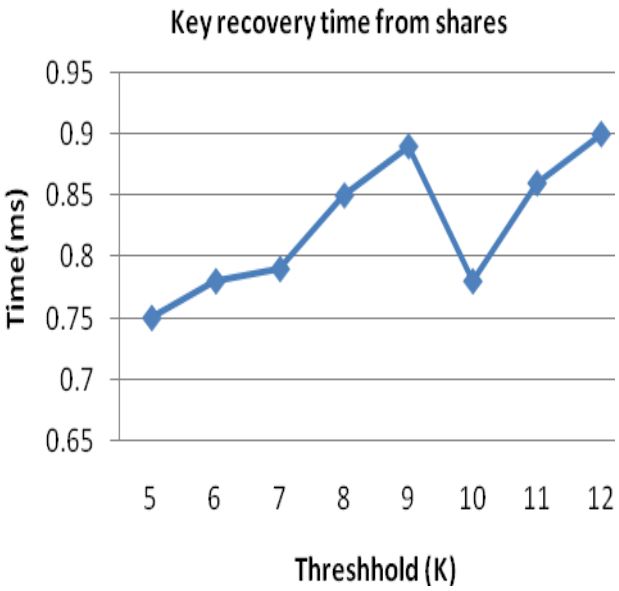

Figure 11: Key Recovery time from shares.

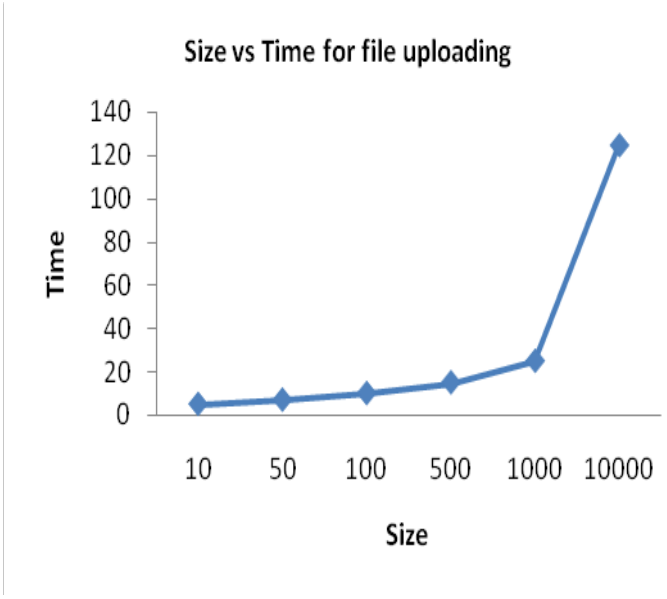

Figure 12: File Size v/s uploading time.

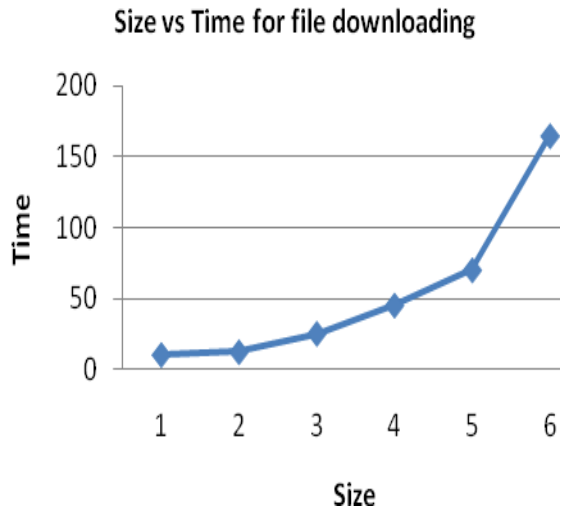

Figure 13: File Size v/s downloading time.

So, as it is obvious in above illustrated graph key dispersal rate (Figure 10) with increasing number of thresholds leads to increase in time which is an obvious factor.

Another factor of evaluation is key recovery time shown in Figure 11, which behaves proportionally with respect to time, but when the number of threshold increases to 10 approximately, it shows a sudden decline in time which is a favorable sign to our setup. Then we examined the file uploading/downloading time with respect to file size and found that the approach is practical and feasible if we try to upload files with certain limit of file size, as size beyond that limit leads to a drastic increase in time required for uploading. Similar is the case with downloading file.

VIII CONCLUSION

This paper highlighted how important it is to ensure that the information within the Cloud environment is to be secure. We have discussed the need of securing Cloud storage systems, challenges and basic security requirements of a Cloud computing, some of the possible threats to the Cloud Storage systems and countermeasures to deal with the same. In this paper a survey of existing approaches to secure cloud computing environment and services has been expounded and discussed and found that every approach has its own pros and cons. Alongside, an approach using threshold cryptography to secure cloud transaction has been implemented over simulation bed and evaluated on the basis of few parameters and found quite helpful in implementing cloud security. In the future scope of this work, we will implement an approach to secure the aforesaid environment by Identity based encryption by using other well known cryptographic algorithms, and the same will be evaluated and analyzed with its counterparts on the appropriate simulation bed.

REFERENCES

[1] AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). Cloud Computing Security: From Single to Multi-Clouds. 45th Hawaii International Conference on System Sciences.

[2] Sharma, B. (2013). Security Architecture of Cloud Computing Based On Elliptic Curve Cryptography (ECC). Proceedings of 2nd International Conference on Emerging Trends in Engineering and Management, Vol.3 (3).

[3] Venkataramana, K. &Padmavathamma M. (2012). A Threshold Secure Data Sharing Scheme for Federated Clouds. International Journal of Research in Computer Science, 2 (5): pp. 21-28.

[4] RajkumarBuyya, Rajiv Ranjan, and Rodrigo N. Calheiros,"InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", ICA3PP,2010,Part I, LNCS 6081, Springer, 2010, pp. 13–31.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2011), pp. 1-11

[6] Xiao Zhang; Hong-tao Du; Jian-quan Chen; Yi Lin; Lei-jieZeng,"Ensure Data Security in Cloud Storage", Network Computing and Information Security (NCIS), International Conference (IEEE),vol.1,14-15 May,2011, Pp 284- 287.

[7] Ming Li, Shucheng Yu, Yao Zheng, Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attributr based Encryption" IEEE transactions on parallel and distributed systems, Vol 24, No. 1, January 2013.

[8] Jun, F., Ryo, F., Takuya, M., Kengo, M., Toshiyuki, I., &Toshinori, A. (2013). A Privacy-Protection Data Processing

Solution Based on Cloud Computing. NEC Technical Journal, Vol.8 No.1.

[9] Kader, H. M. A., Hadhoud, M. M., El-Sayed, S. M. &AbdElminaam, D. S. (2014). Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing. International Journal of Technology Enhancements And Emerging Engineering Research, VOL 2, ISSUE 4.

[10] Kaur, G., &Mahajan, M. (2013). Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms. Int. Journal of Engineering Research and Applications, Vol. 3, Issue 5, pp.782-786.

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

[12] Sudha, M., &Monica, M. (2012).Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography. Advances in Computer Science and its Applications, Vol. 1, No. 1.

[13] Kaur, G., &Mahajan, M. (2013). Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms. Int. Journal of Engineering Research and Applications, Vol. 3, Issue 5, pp.782-786.

[14] Sanyal, S., &Iyer, P. P. (2013). Cloud Computing -An Approach with Modern Cryptography. Tata Consultancy Services, Mumbai, INDIA.

[15] Reddy, V. K., &Rao, J. E. (2014). A Survey on Security in Cloud using Homographic and Disk Encryption Methods. International Journal of Computer Sciences and Engineering, Volume-2, Issue-4.