RESEARCH ARTICLE OPEN ACCESS

Enhancing Data Integrity in Multi Cloud Storage

Alisha Jindal*, Gagandeep**
*(Department of Computer Science, Punjabi University, Patiala)
** (Department of Computer Science, Punjabi University, Patiala)

ABSTRACT
Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. Cloud is surrounded by many security issues like securing data and examining the utilization of cloud by the cloud computing vendors. Security is one of the major issues which reduce the growth of cloud computing. A large number of clients or data owners store their data on servers in the cloud and it is provided back to them whenever needed. The data provided should not be jeopardized. Data integrity should be taken into account so that the data is correct, consistent and accessible. For ensuring the integrity in cloud computing environment, cloud storage providers should be trusted. Dealing with single cloud providers is predicted to become less secure with customers due to risks of service availability, failure and the possibility of malicious insiders in the single cloud. This paper deals with multi cloud environments to resolve these issues. The integrity of the data in multi cloud storage has been provided with the help of trusted third party using cryptographic algorithm.

Keywords **-** Cloud Computing, Data Integrity, Multi cloud, ECC algorithm

I. INTRODUCTION

Cloud computing is basically cost effective and on demand service offered to the clients. It is a model to access shared pool of configurable computing resources which include servers, storage, applications and also services to interaction provider. Cloud computing is computing on various resources over the network. Usage of cloud has changed the concept in the industry wherein organizations need not invest on resources; they rather rent the required resource on on-demand basis or take services from the cloud which has reduced the infrastructure costs.

According to NIST, Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models and four deployment models. Accenture defines cloud computing as the dynamic provisioning of IT capabilities (hardware, software, or services) from third parties over a network. McKinsey says that clouds are hardware-based services offering compute, network and storage capacity where: hardware management is highly abstracted from the buyer.

The cloud model differs from traditional outsourcing in that customers do not hand over their own IT resources to be managed. The latest example of cloud computing is Web 2.0; Google, Yahoo, Microsoft, and other service providers now offer browser-based enterprise service applications (such as webmail and remote data backup). In India, companies such as Ashok Leyland, Tata Elxi, Bharti, Infosys, Asian Paints and Maruti are using cloud computing. . The cloud is basically used in three service models namely, software as a service, platform as a service and infrastructure as a service. The clouds could be private clouds, public clouds as well as hybrid clouds.

Clouds have many advantages but it also brings certain challenges. Security mechanism for stored data is the major issue in clouds. The security problem concerns with the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation. As clients cannot physically access the data from cloud server directly and cloud provider can modify or delete data. Hence there is requirement of checking the data periodically for correction purpose. Checking of data is called data integrity so that data must be defined, exact and changed by allowable people only.

The idea on reducing the risk for data in a cloud is the simultaneous usage of multiple clouds. Multi cloud computing creates a large number of security issues and challenges. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. Different services are accessed from the multi-cloud user. The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. Various approaches for multi-cloud security differ in portioning and distribution patterns, technologies, cryptographic methods and security levels. The assessment of

different methods with regards to legal aspects and compliance implications is important.

II. LITERATURE SURVEY

There are security threats to which cloud computing is vulnerable. Security service level agreement's specification and objectives related to data locations, segregation and data recovery is summarized in [1]. They discussed about the services provided and the claims given if the services not met the agreement but have to mention many other issues like security policies, methods and their implementations and what legal actions are taken if the services are misused by the customer.

The security ecosystem [2] is modeled based on three participants of cloud system: service user, service instance and the cloud provider. The authors classified the attack into six categories (i.e. user to service, service to user, user to cloud, cloud to user, service to cloud and cloud to service). This was suggested to describe the threats and vulnerabilities presented in cloud computing and continue with the collection and classification of cloud based attacks and vulnerabilities in order to prove attack taxonomy's applicability.

The overall security perspective of cloud computing is discussed in [3] with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of cloud computing. It provides the management of security in cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise. With these guiding principles, a great deal of insecurities got easily expelled, saved business owners' valuable time and investment.

Various security challenges in the cloud and key areas for the improvement of cloud system security are illustrated [4]. As broad acceptance of cloud computing for deploying business and medical computations depends significantly on the foundation of future systems' security. Security issues in the cloud must be tackled with a firm foundation. The importance of general security issues from cloud specific security issues are pointed [5]. Also, cloud computing vulnerabilities from various aspects are also summarized and defines risk factors of cloud computing. Thus challenges are of special interest for cloud computing security research.

Different security risks [6] that pose a threat to the cloud are presented. This survey is more specific to the different security issues that have emanated due to the nature of the service delivery models of a cloud computing system. A detailed analysis of the cloud computing security considerations and key challenges focusing on the cloud computing types and the service delivery types are focused [7].

Multi cloud providers have been used to affect privacy and data integrity challenges. Multi-cloud model in [8] described the combination of various clouds where user data is distributed and executed in those clouds simultaneously. It is observed that multi–clouds improve performance provided by single cloud environment by dividing security, trust and reliability among different clouds. They have made a survey of various techniques available for multi cloud security like use of cryptography, secret sharing algorithm and redundant array of cloud storage. They have shown limitations and suggested for secure cloud database as their future work but they had not given their solution in details.

Then multi-cloud computing framework [9] uses proxy VM instance for sharing resources and dynamic collaboration among cloud based services. This framework manages security, mutual trust and policy issues without need of pre-collaboration agreement which is necessity in cloud mash-ups. Whenever cloud user wishes to use any services, he sends request to cloud where CSP has pre-installed proxy instance which may interact with multi-cloud services and provide results to user. It helps for collaboration among various cloud users.

The different architecture for multi-cloud computing paradigm for improving security and privacy of user and provider was developed [10]. First approach specifies replication of application which helps to verify integrity of data after execution in cloud is over. Second approach helps to protect data and logic by separating them from data. In third approach data and application are distributed by breaking application logic in parts and executing it over multiple clouds. Similar approach is given in last architecture where data is broken into parts and executed over various clouds which helps to protect from malicious cloud service provider. The architecture has their own pros and cons however combination of that architecture give better secure approach for multi-cloud systems.

In 3-tier architecture [11], there is a central server provider which keeps the data of the cloud users. There are servers which may reside in different physical locations. The CSP decides the servers to store the data depending upon available spaces. Load balancing algorithms have been used for making the decision, on which server we should actually store the data. The CSP also keeps track about the files stored on each server. The cloud servers only store the data, but they do not have any records about the user accounts. Symmetric key algorithms have been used for the purpose of encrypting and decrypting data while storage. Secret key encryption algorithm uses same secret key to encrypt and decrypt data. The protection of key access from unauthorized agents is an issue.

Multi-cloud platform [12] to mitigate the risks of malicious data manipulation, disclosure and process tempering have been used. The multi-cloud works on the encrypted inputs to compute the encrypted output. The intermediate or final results have to decrypt. For this, there is requirement of either the interaction with entity that holds the key or the key is shared among several clouds that then assist in decrypting values that are needed in clear with an encryption scheme. In this technique RSA cryptographic scheme is used. The multiparty computation between clouds is made so that cloud providers do not know about the inputs. RSA algorithm is used to securely transmit the keys. There can be more fields of cryptanalysis which can be used to maintain the security in the multi clouds.

III. PROPOSED ARCHITECTURE

This paper specifies a framework to ensure security in aspect of data storage in cloud. Cloud service providers provide data storage services and possess enough computation but there is no guarantee for security of data stored on the single cloud. As data owner cannot fully trust the cloud service provider. Therefore multi cloud service providers have been used to store and maintain client's data on the cloud. The clients are allowed to access their data for various applications. Clients store data in multiple clouds and must have permissions to access the data. The integrity of the outsourced data in multi cloud storage has been provided with the help of trusted third party. It checks the data integration and maintenance using cryptographic algorithm.

Fig. 1 Activities performed for Cloud Storage

3.1 Environmental Setup

The physical environment and tools for cloud storage are identified. Windows Azure has been used as cloud hosting storage platform. Windows azure is a cloud service operating system that serves as the development and service management environment. The storage requires a minimum processor speed of 1.6 GHz and should have minimum 1024 MB RAM. There should be atleast 5.5 GB available hard disk space. Internet Information Services (IIS) is a necessary software requirement for Windows azure. It includes a set of programs for building and administering websites and search engines.

3.2 Cloud Interactions

In this phase clouds are created according to the user requirement. Cloud providers should address privacy and security issues as matter of high and urgent priority. To reduce security risks that affect cloud computing user, this work aims to use multi cloud rather than single cloud. The multi-cloud tools help cloud providers construct a distributed cloud storage platform for managing clients' data. Multi-cloud formation is done with the help of Azure emulator. The database for each field created or inserted within the cloud is formed. It concerns with the concept of primary key and specifies all the columns in the database declared upon a defined domain. It is maintained with the help of SQL services. After the database is designed, the tables store the data in the database created.

3.3 Enforcing Integrity

The integrity within the clouds has been done using third-party auditor. It plays an important role for the storage auditing in cloud computing. It is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request.

3.3.1 Interaction using trusted third party:

The subsequent step is related with the interaction between two parties of multiple clouds using trusted third party (TTP). The main concern is to maintain data integrity while data is accessed from multiple clouds. TTP is formed so that the data exchanged from one cloud to the other must be secure and should not leak the information while moving the data.

3.3.2 Implementing cryptographic algorithm: The third party module has been linked up with the other clouds that have been created and thus perform the activity of maintaining security with the help of ECC cryptography algorithm [13][14]. This prevents unauthorized user access.

Encryption

Let 'm' be message to be sent. Consider 'm' has point M on the curve. P is a point on curve. Randomly select a value k from [1 - (n-1)]. Two cipher texts are generated let it be B1 and B2.

$$B1 = k * P$$
$$B2 = M + (k * P)$$

Decryption

Use the following equation to obtain original message that was sent i.e m.

$$M = B2 – d * B$$

M is original data that was sent and d is random number in the range of (1 to n-1).

3.4 Verification and Analysis

The initial steps of the project are carried out in a proper way and obtain various results. These results are observed on the basis of response time. Then speedup percentage between the response time of RSA and ECC algorithms can be measured using

$$\text{Speedup } (\%) = \frac{\text{RSA} - \text{ECC}}{\text{RSA}} * 100 \qquad (1)$$

The given formula evaluates the improvement in performance of response time of two cryptographic algorithms.

IV. IMPLEMENTATION

This paper deals with the storage of data in more than one cloud hence multi-clouds are used. In this section, multi clouds have been implemented so as to resolve the issues of integrity, availability and privacy of data in cloud computing. The main objective is to develop a cloud storage where user can store their data and can fetch that data whenever it is required. For this three clouds have been created which are named as Cloud1, Cloud2 and the third one is trusted party cloud. For accessing the cloud, users can sign up into the cloud and can upload their data. Any user can login into the cloud by using username and password.

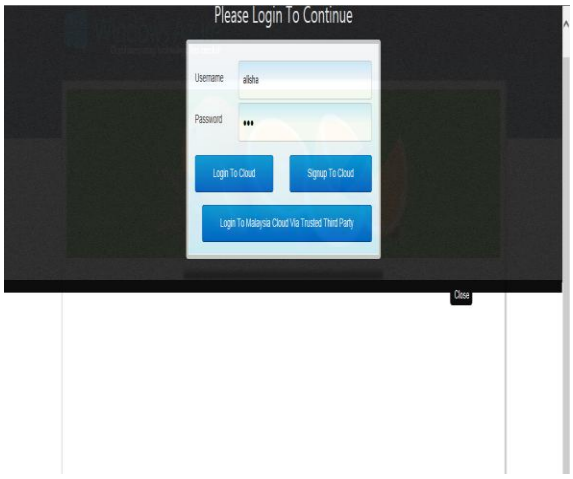

Fig. 2 Creating client to access a Cloud

After signing in to the cloud the contents within the cloud are displayed where users can upload their data. Any updates in the data are available on the database. The database used here is Microsoft SQL Server. The data and information regarding profile, blog, chat and hobbies are stored in the clouds.

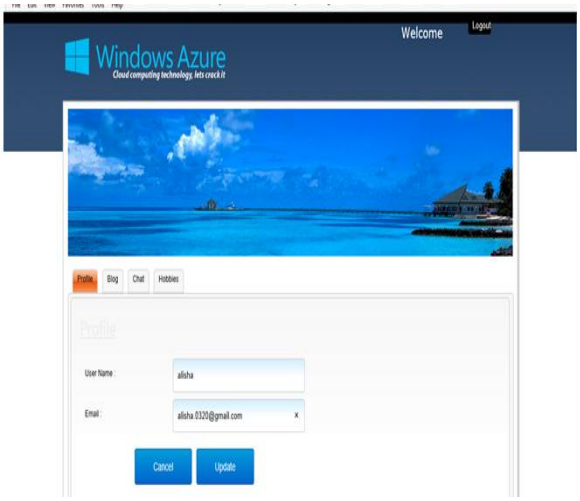

Fig. 3 Cloud storage in Cloud1

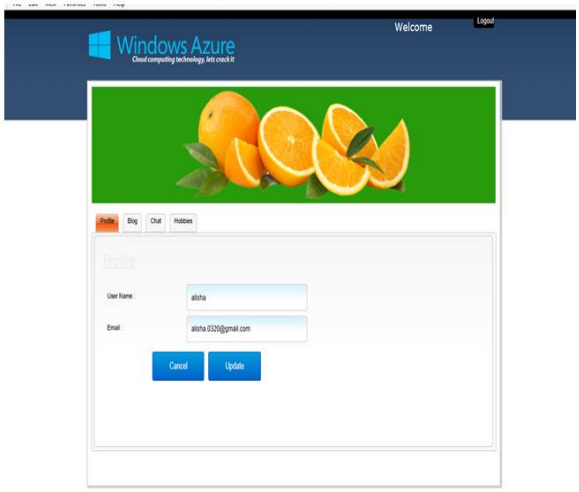

Fig. 4 Cloud storage in Cloud2

Clouds store the following the data and information. The data present by the same user in the two clouds can be same or can be different. User can update, delete or insert any fields into the table is also possible.

1) Profile: Client's basic information is stored such as username and email id. The users who logged in into the cloud are allocated with a userid.

2) Blog: In this field contents of the user are saved and entitled according to the will of user.

3) Chat: User can chat with several different users in the cloud by selecting the user from the dropdown list and sending the message to the selected user from the list. When the selected user gets logged in into the cloud, he gets the message. This message displays the date and time when it was send.

4) Hobbies: Here users are uploaded with their hobbies. User can upload more than one hobby. If user wants to make updates within these fields that can be done.

The data present on the two clouds by the same user are different and the user wants the data present on one cloud to be displayed on the other cloud then it is

possible via trusted third party. For accessing the data of another cloud, it is logged in to the cloud but this is done with the help of trusted third party. For accessing data from one cloud to another there should be trust between both clouds.

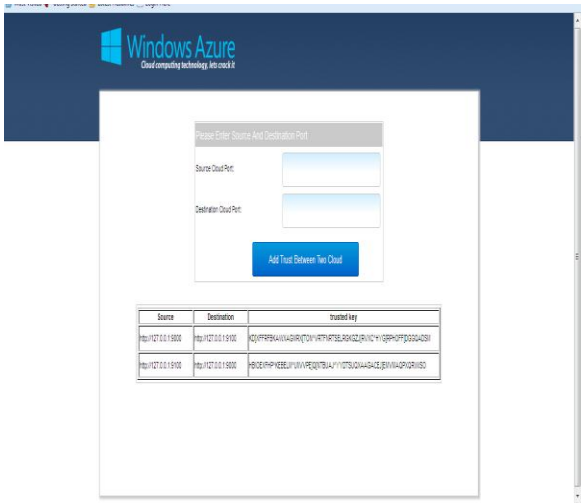

Fig. 5 Verification via Trusted Third Party

V. RESULT EVALUATION

It has been analyzed that the security of the stored data in multiple clouds is affected and maintains integrity of the data. The values of response time are calculated in accordance to the varying sizes. These results are compared with the earlier scheme which used RSA cryptographic algorithm.

TABLE I
RESPONSE TIME OF VARYING FILE SIZES

Size of file (KB)	Response Time (sec)		Improvement in Speedup (%)
	RSA	ECC	
69	9.4	7.3	22.3
105	10.5	7.9	24.5
158	11.8	8.1	31.3
194	13.1	8.8	32.8
263	16.2	10.4	35.8

The improvement in the speedup percentage of response time of these two algorithms is calculated using Equation (1). From the above Table I, it has been concluded that with the use of ECC cryptographic algorithm the response time decreases. The data has been compared between these algorithms.

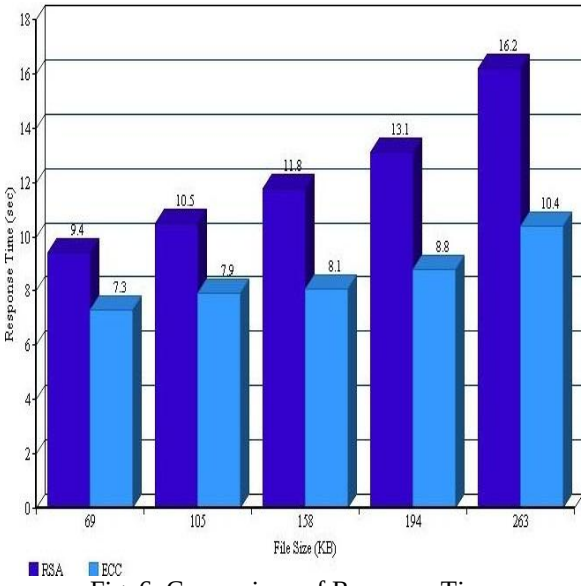

Fig. 6: Comparison of Response Time

Fig. 6 shows the comparison of response time for RSA and ECC algorithms. Also it has been noticed that with the increase in size of file, there is improvement in speedup percentage between the response time of RSA and ECC algorithms. It can be seen in Fig. 7.

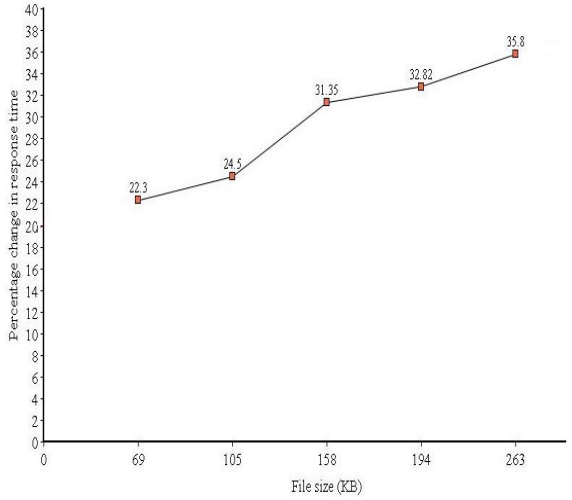

Fig.7 Improvement in response time w.r.t. file size

After executing these steps response time it can be concluded that as the file size increases, there is improvement in the performance of the algorithm. Also, security of the stored data is affected using multiple clouds and integrity of data is maintained with the help of ECC asymmetric algorithm.

VI. CONCLUSION

The major concern in adapting the cloud is its security as there are number of data breaches that affect the growth of cloud. Integrity of the data is an emerging field in cloud computing for security purpose. Extensive research has been done on the techniques of data integrity. Here multi clouds have

been for the storage of data. The leakage of data by an authorized user is prevented using ECC algorithm and creating a cloud as trusted third party.

VII. FUTURE WORK

Cloud is still a budding technology and needs various improvements and standardizations. Multi cloud concepts have to be adopted to increase the performance of cloud servers. The work can be further extended to use ECC by applying digital signatures or key exchange factors.

ACKNOWLEDGEMENTS

We would like to thank Dr. R.K Bawa for providing the necessary facilities for the successful completion of this study. I further thank my family and friends for their encouragement and support.

REFERENCES

[1] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit, Cloud Security Issues, *Proc. IEEE International Conf. on Services Computing*, Bangalore, 2009, 517-520.

[2] N. Gruschka and M. Jensen, Attack Surfaces: A Taxonomy for Attacks on Cloud Services, *Proc. 3rd IEEE Conf. on Cloud Computing*, Miami, FL, 2010, 276-279.

[3] S. Ramgovind, M. M. Eloff and E. Smith, The Management of Security in Cloud Computing, *Proc. IEEE Conf. on Cloud Computing*, Johannesburg, 2010, 1-7.

[4] T. Jaeger and J. Schiffman, Outlook: Cloudy with a Chance of Security Challenges and Improvements, *IEEE Security and Privacy, vol. 8, issue 1*, 2010, 77-80.

[5] B. Grobauer, T. Walloschek and E. Stocker, Understanding Cloud Computing Vulnerabilities, *IEEE Security and Privacy, vol. 9, issue 2*, 2011, 50-57.

[6] S. Subashini and V. Kavitha, A Survey on Security Issues in Service Delivery Models of Cloud Computing, *Elsevier Network and Computer Applications, vol. 34, issue 1*, 2011, 1-11.

[7] S. O. Kuyoro, F. Ibikunle and O. Awodele, Cloud Computing Security Issues and Challenges, *International Journal of Computer Networks (IJCN), vol. 3, issue 5*, 2011, 247-255.

[8] M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, Cloud Computing Security: From Single to Multi Clouds, *Proc. 45th IEEE Conf. on System Science*, Maui, Hawaii, 2012, 5490-5499.

[9] M. Singhal, S. Chandrasekhar, G. Tingjian, R. Sandhu, R. Krishnan, A. Gail-Joon and E. Bertino, Collaboration in Multicloud Computing Environments: Framework and Security Issues, *IEEE Computer Society, vol. 46, issue 2*, 2013, 76-84.

[10] J. Bohli., N. Gruschka, M. Jensen, L. L. Iacono and N. Marnau, Security and Privacy Enhancing Multi-Cloud Architectures, *IEEE Dependable and Secure Computing, vol. 10, issue 4*, 2013, 212-224.

[11] K. M. Borse, A. G. Deshpande, A. A. Deshpande and J. S. Hardas, Security in Multi Cloud Data Storage with SIC Architecture, *IJRET, vol. 3, issue 2*, 2014, 81-84.

[12] C. Priyadharsshini, S. SathishKumar and P. Ranjidha, A Securing and Sharing Data Less Cost Effective using Multicloud Storage, *IJARCST, vol. 2, issue 1, ver. 2*, 2014, 132-136.

[13] V. Miller, Use of Elliptic Curves in Cryptography, in H. C. Williams, *Advances in Cryptology CRYPTO 85*, V (Berlin: Springer Heidelberg, 1986) 417-426.

[14] N. Koblitz, Elliptic Curve Cryptosystems, *AMS Mathematics of Computation, vol. 8, no. 177*, 1987, 203-209.