IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-10 E-ISSN: 2347-2693

Providing Confidentiality, Integrity and Atomicity for data stored in the cloud storage

Akanksha Bansal[1*], Arun Agrawal[2]

[1,2] *Dept. of Computer Science and Engineering, ITM Gwalior, India*

Available online at: www.ijcseonline.org

Received: 02/Sep/2016 Revised: 13/Sep/2016 Accepted: 17/Oct/2016 Published: 31/Oct/2016

***Abstract*— Cloud computing is a kinds of computing that depend on distribution computing resources before having local servers or own devices to knob applications. Cloud computing is equivalent to grid computing, In the cloud is a kind of computing where vacant handing out rounds of the entire computers in a network are harnesses to solved the concerns also focused for some stand-alone mechanism. Cloud computing security mentions to the group of processes, procedures and standards designed to deliver information security guarantee in a cloud environment. Cloud computing security comprises both logical and physical security concerns across all the diverse various models of software platform, infrastructure and software. It also defines how these services are delivered (public, private or hybrid delivery model).**

***Keywords*— Encryption, Decryption, ECC, RSA, SLA cloud storage etc.**

I. INTRODUCTION

Cloud computing enables its clients to store their data on remote database via internet and utilize various other service models provided by it such as Software as a Service, Platform as a Service and Infrastructure as a Service. And Clients are charged for the services, they are using based on some metering mechanism, adopted by the cloud facility provider. The main advantage of the cloud is that the clients do not require disbursing for the infrastructure, its deployment, the expertise to handle and maintain such infrastructure. As the client stores the most significant data externally on the cloud storing so it becomes the prime duty of service provider to assurance the defense of data from existence disclosed to some other persons and also guarantee integrity of stored data. [1] .

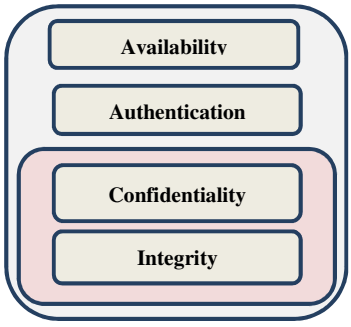

Figure1 : Layers of the data security

Data security is the core protection difficulties in cloud storage. Data security is anxious with data availability, integrity, authentication, confidentiality and so on. Data privacy means that only official persons can usage the data. Data integrity mentions to info that has not been changed or leftovers untouched. Authentication mentions to the method of verified whether the incoming user is authorized or not. Data availability mentions to the aptitude to guarantee to use data in time when needed and also mentions to the accessibility of the cloud facility provider on-demand [2].

Layers of the Data Security One and only of the main use of the cloud are data storage. Cloud provides enormous capacity of storage to the users. In the cloud computing data storage is the benefits of data storage are fetching progressively attractive to both individuals and businesses. In cloud data hubs by via resources "on demand" developers can considerably reduce deployment overheads and management. Infrastructure-as-a-Service (IaaS) solutions, for instance Rackspace Cloud, operate multiple, geographically-distributed data center locations with resources for computation, storage and communication [3].

To design and develop a system by which we delivered a safe saving of our private data in the cloud storage in an effectual way which needs low computational power and time and disallowing hacker from penetrating into our privacy data storage. Despite the major advantages that cloud computing has, there are motionless many other security obstacles such as confidentiality and data integrity. The development of cloud technology raised a lot of questions regarding data security or risks upon data exposure; hence, cloud storage provider should ensure data confidentiality, availability and integrity [4].

In this paper we are going propose a system, which decrease workload of the client and provide confidentiality, security and integrity in an effectual manner. Since the data is not

physically available to the user the cloud should deliver the user a way to check for integrity. We delivered a method which gives an evidence of the integrity for the data in the cloud which the client employs to check the accuracy of user data in the cloud. To secure the Cloud resources protected the behaviors and storage "databases hosted by the Cloud provider" Three Security goals of the data comprise points namely: Confidentiality, Integrity, and Availability (CIA). Data Privacy in the cloud is achieved by Decryption/encryption process [5].

A. Cloud Storage

As cloud computing is popular and in demand similarly cloud storing technology has greater demand. Cloud storage is a virtualized storage areas over a network basis .It provides services on the basis of QoS assured. Cloud storage consist of many resources but yet act as single system. It has greater fault tolerance by redundancy. As the data produced by IT sectors are dramatically growing we can't update our hardware frequently instead we can adopt for the cloud storage which is a better choice. Cloud storage can we just for different purpose just back-up our home desktop data into cloud storage or as an archive to retain data for regulatory. Cloud storage allows user to access extensive range of application and resources immediately, which are hosted by others [6].

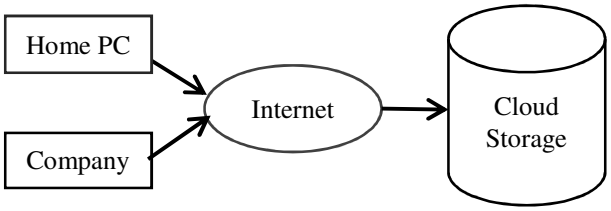

Figure 2: Sample Cloud Storage

B. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) was introduced in 1985 by Neil Koblitz and Victor Miller as a supernumerary technique that implements public-key cryptography.

• The equation of an elliptic curve is given as,
y2 = x3 + ax + b

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (It should be a prime number)

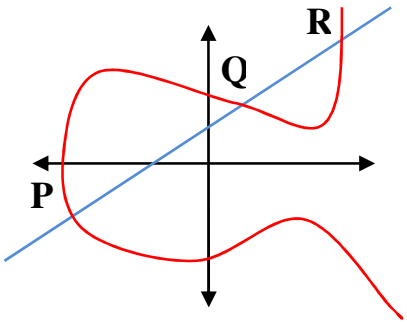

Fig.3. Simple Elliptic Curve

$$y^2 = x^3 + ax + b$$

Key Generation:
Key generation is an essential part where both public and private keys are generated. The message is encryption by sender by using recipient's public key on receiving the encrypted message by intended recipient it is decrypted by its private key. For generating key firstly select a arbitrary number say'd' in the range of 'n'. With the help of given below equation can generate key.

Q = d * P

Where:
d = the random number selected in the range of (1 to n-1).
P = the point on the curve.
'Q' is the public key and 'd' is the private key.
Encryption:
Suppose 'm' is the message to be send. Thus representing this message on the curve.
Consider 'm' has the point 'M' on the curve 'E'. Arbitrarily choose 'k' from [1 – (n-1)].Two cipher texts will be created let it be C1 and C2.

C1 = k*P
C2 = M + k*Q

C1 and C2 will be sending.
Decryption:
For decrypting the message m,
M = C2 – d * C1
M is the original message that was send.[7]

II. RELATED WORKS

A. Security Challenges in Cloud Storage

This paper provides a transitory explanation on cloud storage. Mainly, it describes the security challenges composed with the recent improvements for each challenges. This is ended by reviewing previous literature and laying it into context. We are also looking into emerging approaches and technologies that may be potentially continued and improved for future research in this paper will discuss some of the tests of make safe a cloud storage and laying it into context by studying relevant literature. The challenges related with the three main

security facets (availability, confidentiality and integrity) are discuss together with the susceptibilities allied to them. It is significant to look into these contests as the cloud storing is not only about technical development but involves security considerations [8].

B. Complete Privacy Preserving Auditing for Data Integrity in Cloud Computing

In this work, a cloud resident data integrity auditing protocol founded on a Rather Holomorphic Encryption (SHE) scheme is presented. Having the data encrypted with SHE, computations could be perform over encrypted the data. The reviewing protocol runs above the encryption of the data using encrypted holomorphic data authentication tags. The protocol offers block less and stateless verification with moderate communication complexity. Security of the SHE and the studying protocol future are thoroughly analyzed. In this paper we proposed a novel protocol for verified the integrity of data stored at the remote cloud server, founded on the applied version of the integers based holomorphic encryption. The offer is the first try in linking the confidentiality and data integrity in new ways to provide an impending solution [9].

C.Data Intergity Proofs in Cloud storage

In this paper we have operated to enable the customer in receiving a proof of the integrity of the data which he needs to store in the cloud storage servers with plain minimum costs and efforts. Our method was advanced to reducing the storage and computational above of the customer other than to decrease the computational above of the cloud storage server. We also decreased the sized of the evidence of the data integrity so as to reducing the network bandwidth consumption. In this paper we make available a method which offers a proof of the data integrity in the cloud computing which the client can employ to check the accuracy of his data in the cloud. This proof can be arranged upon by both the customer and cloud and can be unified in the Service level agreement (SLA)[10].

D. Data Confidentiality and Integrity Verification using User Authenticator

In this paper mainly we discussed cloud security about the issues, the research problems in the security level and User Authenticator system is propose that helps to checked the integrity of the data deprived of using TPA scheme. A protected cloud is unmanageable without sustaining the entire those research issues starting from protecting data from cloud facility provider till virtualization environment for the cause that the complex and altering nature of the cloud computing. So a new security solution should be providing to safe the data from different kinds of attack different people at different places. Our research is focusing on providing solutions to all these issues and develops a model to give secure cloud infrastructure that helps to adopt the cloud as and when required. In this paper is a survey of diverse security problems that affects the cloud environment and related work that are carried out in the area of integrity [11].

E. Changes and Security issues in cloud computing from two perspectives: Data Security and Privacy Protection

Cloud computing is demand to access a communal shared of computing resources. If the cloud technology is used in an appropriate manner, it would lead to reducing costs, reduce management responsibilities, and increase ability together with organization efficiency. Cloud storing is single of the most populated services offered by the cloud facility provider to store customer data on remote server. Despite the ads by cloud providers, founded on the fact that the storing data remains safe and sound, there are static attacks which resulted in the loss of data. In this paper security problems and challenges in the cloud are investigated from two perspectives begin data security and privacy [12].

F. Study of Data Security and Privacy Preserving Solutions in Cloud Computing

In this study, we observed that most of the Privacy Preserving and security solutions proposed by the authors have complex adaptable behavior in its working environment. Hence we need an effectual privacy preservative & security model (Encryption based) which could be easily adopted in current working environment of cloud. Our future work will focus on suggesting a fast encryption solution that should be adjusted in each share of the cloud and provide complete solution of data privacy & security as a Service. Therefore, data security must be provided in the cloud models. There are some solutions proposed, to resolution these issues, based on encryption techniques. The main contribution of this paper is to perform a study of different solutions to provide data safety and privacy in existing cloud computing scenario [13].

III. PROPOSED WORK

Cloud Storage is built with a simulated storage plan. Global data is encrypted both mid-flight and at rest. If users are allowing for moving formless data to the cloud, then strongly recommend evaluating the security method of each potential solution according to the following criteria. On general public cloud services, such as AWS, S3 or EBS (Elastic Block Store) the data from every company or version will be stored on servers sharing with other clients and potentially crossways various physical devices. There is no guarantee that this data will be encrypted by default.

From the shared viewpoint alone it is needed to encrypt the data at repose, so as to defend against network or guest misconfiguration that could expose data from the one client to another client.

- A user who storing and access his data on cloud storage.
- Every user contains a unique key by which account can be access.
- In cloud computing uses 56 bits, vacter size 64 bits, contain less than capacity, execution time is Equals to encryption and decryption identical key is used.

```
package nomad;
importjava.security.*;
importjava.security.spec.InvalidKeySpecException;
importjavax.crypto.*;
importsun.misc.*;
publicclassencryptencrp {
privatestaticfinalString ALGO = "Encryption";
Privatestaticfinal byte [] keyValue =
new byte[] { 'T', 'h', 'e', 'B', 'e', 's', 't', 'S', 'e', 'c', 'r','e', 't', 'K', 'e', 'y' };
```

❖ **Algorithm I for the encryption**

For the encryption:

```
PublicstaticString encrypt (String Data) throwsException {
Keykey = generateKey ();
Cipher c = Cipher.getInstance (ALGO);
c.init (Cipher.ENCRYPT_MODE, key);
byte [] encVal = c.doFinal (Data.getBytes ());
StringencryptedValue =
newBASE64Encoder().encode(encVal);
returnencryptedValue;
   }
```

Step 1: encrypt data of string
Step 2: Key generate
Step3: Algorithm Applied in cipher text
Step4: Encrypt mode is converted in cipher text
Step5: final value is encrypt value

❖ **Algorithm II for the decryption**

For the Decryption:

```
publicstaticStringdecrypt(StringencryptedData
throwsException {
) Keykey = generateKey ();
      Cipher c = Cipher.getInstance (ALGO);
c.init (Cipher.DECRYPT_MODE, key);
byte[]decordedValue=new
BASE64Decoder().decodeBuffer(encryptedData);
byte[] decValue = c.doFinal(decordedValue);
StringdecryptedValue = newString (decValue);
returndecryptedValue;
   }
privatestaticKeygenerateKey() throwsException {
Keykey = newSecretKeySpec(keyValue, ALGO);
return key;
}
}
```

Step 1: Decrypt data of string
Step2: Key generate
Step3: Algorithm applied in cipher text
Step4: Decrypt mode is converted in cipher text
Step5: Final value is decrypt value

- In the archive encryption file is saved.
- The to verify the integrity the user request the meta data
- The user compares Meta data and find whether the data is modified or correct.
- If the file has been modified. it is indicated to the user.

IV.THE OUTPUT OF THE RESULTS ARE CLOUD

Fig4.Home Form (welcome to secure cloud storage)

Fig5. Register form (Registered successfully)

Fig6.Login Form (User id to login)

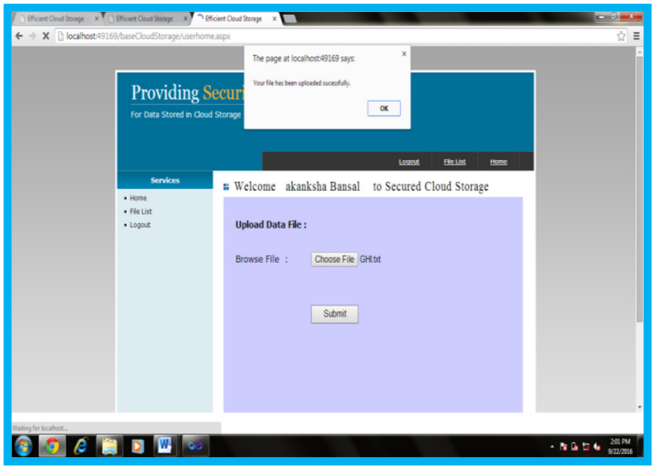

Fig7. Uploaded data file form (File has been uploaded successfully)

Fig.8 File list form (Uploaded files in file list)

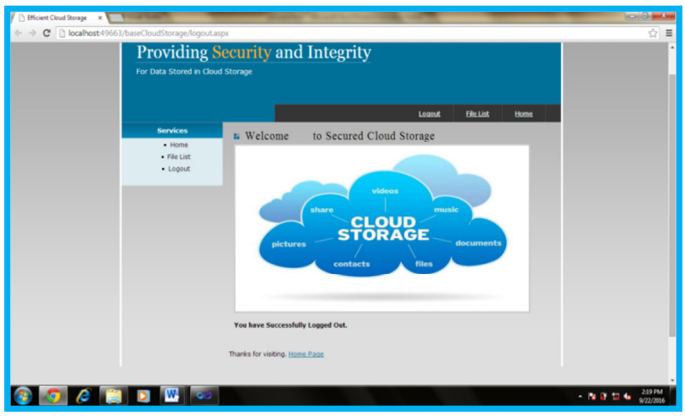

Fig.9 Logout form

V. CONCLUSION

Cloud computing is a model for providing IT facilities in which assets are regained from the internet over web-based applications and tools, sooner than a direct linking to a server. Software and data packages are storing in servers. Nevertheless, cloud computing structured allowed access to the information providing an electronic device has accessed to the network. This category of system permits employers to effort remotely. Cloud security methods should addressed the security controls the cloud supplier will integrate to maintain the customer's privacy, data protection and obedience with essential rules. The methods will also likely contain business continuity and the data backup strategy in the case of a cloud security breach in this paper.

REFERENCES

[1] Ranjit Kaur and Raminder Pal Singh "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques" International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE-2014

[2] Dr. L. Arockiam and S. Monikandan "Efficient Cloud Storage Confidentiality to Ensure Data Security" International Conference on Computer Communication and Informatics (ICCCI), IEEE-2014, DOI-Jan. 03 – 05, 2014, Coimbatore, INDIA

[3] R.K. Banyan, V.K. Jain and Pragya Jain "Data Management System to Improve Security and Availability in Cloud Storage" International Conference on Computational Intelligence & Networks, IEEE-2015, DOI 10.1109/CINE.2015.32.

[4] Mohammed faez AL-Jaberi, AnazidaZainal "data integrity and privacy model in cloud computing" International Symposium on Biometrics and Security Technologies (ISBAST), IEEE, 2014.

[5] Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi and L.D. Dhinesh babu "An enhanced data security and trust management enabled framework for cloud computing systems" 5th ICCCNT, IEEE-2014, DOI- July 11-13, 2014.

[6] Mr.Chandrashekhar S. Pawar ,Mr.Pankaj R. Patil "Providing Security and Integrity for Data Stored in Cloud Storage" ICICES2014 - S.A. Engineering College, Chennai, Tamil Nadu, India , IEEE 2014
[7] Rukaiya Sheikh, Disha Deotale Security and Authentication Process using ECC in VANET". International Journal of Advance Research in Computer Science and Management Studies
[8] F. Yahya, V. Chang, R.J. Walters and G.B. Wills "Security Challenges in Cloud Storage" 6th International Conference on Cloud Computing Technology and Science, IEEE-2014, DOI 10.1109/CloudCom.2014.171.
[9] Y Govinda Ramaiah and G Vijaya Kumari "Complete Privacy Preserving Auditing for Data Integrity in Cloud Computing" 12th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE-20 13,DOI 10.1109/TrustCom.2013.191.
[10] Sravan kumar R and Ashutosh Saxena "Data Integrity Proofs in Cloud Storage" IEEE-2011.
[11] V.Nirmala, R.K.Sivanandhan and Dr..R. Shanmuga Lakshmi "Data Confidentiality and Integrity Verification using User Authenticator" International Conference on Green High Performance Computing ,IEEE-2013, March 14-15, 2013.
[12] S.Mahdi Shariati, Abouzarjomehri and M Hossein Ahmadzadegan "Changes and Security issues in cloud computing from two perspectives: Data Security and Privacy Protection"2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), IEEE-2015.
[13] Siddharth Dutt Choubey and Mohit Kumar Namdeo "Study of Data Security and Privacy Preserving Solutions in Cloud Computing" International Conference on Green Computing and Internet of Things (ICGCloT), IEEE-2015.

AUTHORS PROFILE

Akanksha Bansal was born in 21th August 1992. She received the Bachelorof Engineering in Computer Science & Engineering from Shriram College of Engineering & Management (Banmour). Gwalior, India in 2014, and she is currently pursuing M.tech in Computer Science & Engineering from ITM Universe, Gwalior, India. Her main area of research interest as Data mining, cloud computing & cloud databases.

Dr. Arun Agrawal was born in 4th'July'1978. He received his M.Tech from AAIDU Allahabad in 2006. He is currently working as Assistant Professor in Computer Science & Engineering Department of Institute of Technology & Management, Gwalior. Currently, He is pursuing his Ph.D from Mewar University, Rajasthan on the topic of Study on Traffic Congestion detection in Vehicular Adhoc Networks using GPS. His research interests are Vehicular Adhoc Networks, Embedded System, Digital Image Processing,

