ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

An Efficient Approach to Encrypted Cloud Database

Sakshi Sanjay Deshmukh, Dr.G.R.Bamnote

M.E. Student, Department of Computer Science & Engg., P.R.M.I.T.&R., Badnera. India.

Head, Department of Computer Science & Engg., P.R.M.I.T.&R., Badnera. India.

ABSTRACT: Cloud computing is one of the renowned and fascinating technology all over the world. It consists of various hardware and software resources made available on internet. Many times large number of sensitive data available on cloud. With the growth of the cloud users malicious activity in the cloud has been increased day by day. Millions of people are using services over cloud database, so it becomes more secured and integrity of data should be maintained. The proposed system consists of creation of multiple virtual clouds. Security of data over cloud would be maintained by using various encryption algorithms. Concurrent and secured sharing of data on cloud database would be maintained.

KEYWORDS: Cloud, Encryption, Decryption, Virtual clouds

I. INTRODUCTION

Cloud computing has been conceived as the next generation pioneer for IT Enterprise. In modern era of networking system, Cloud computing is one the most precious and developing concept for both the developers and the users. Cloud computing is a preferable platform for those people who are mostly interrelated with the networking environment. It offers dynamically scalable resources provisioned as a service over network. Cloud computing refers to manipulate, configure, and access various applications online [1]. From past few years the world of computation has changed from centralized system to distributed systems. Generally, in Cloud computing services, data maintenance provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored [4]. Logically, the client has no control over it. Internet is the communication media for Cloud computing. In the Cloud computing environment, various services and information are shared among all of the servers and clients. As a result files or data stored in the cloud many times publicly accessible. Therefore, there is possibility that all files or data become more prone to attack. So it is very easy for an intruder to disturb the original form of information [15]. Thus, it is important to protect the data or files in the midst of unsecured processing. From the security viewpoint, various risks and issues are discussed for data over cloud. There are various threats associated with the security but one of the major issues is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. Although Cloud computing has achieved a great success in various industries whether it is a software industry, a Government Organization or a Healthcare sector, but this transition to Cloud computing has various concerns on a critical issue for the success of information systems, communication and information security. There are various risks associated with the security but one of the major issues is the security of data being stored on the provider's cloud database and privacy while the data is being transmitted [19]. So to make Cloud computing technology more secure; for concurrent access to data on cloud database and for independent access of data on cloud database; a framework is proposed to encrypt the data over cloud database using various encryption algorithms.

II. RELATED WORK

Luca Ferretti, Michele Colajanni, and Mirco Marchetti proposed a novel architecture for describing possibility of executing concurrent operations on encrypted data and integrates cloud database services with data confidentiality [1].**Sushmita Raj, Milos Stojmenovi and Amiya Nayak** proposed a new decentralized access control scheme .In that cloud verifies the authenticity of unknown user before storing data [2]. **Julisch K. & Hall. M.** proposed importance of Virtualization, Web Service, Service Oriented Architecture and Application Programming Interfaces for cloud computing [13]**.Gellman** discussed standards for collection, maintenance and disclosure of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

personal information over cloud[20]. **Jarabek and Hyde** described possible attacks on cloud data [12][15].**Guo Yubin et** al, had done work on storage solution for No SQL database using homomorphic encryption algorithms. Data querying Protocol described in this work and algorithms for data manipulation are given also[5].**Ming Li** et al, proposed a novel framework of secure sharing of personal health records over clouds. Considering partially trustworthy cloud servers, patients will be able to maintain their own privacy through encrypting their PHR files to allow fine-grained access [6].**Omer K. Jasim** et al**,** discussed the various encryption symmetric key algorithms and asymmetric key algorithms. They also discussed the performance of encryption algorithms on a cloud environment for input blocks of different sizes and how the change in the size of the files after encryption is complete [7].**T. Sivasakthi and Dr. N. Prabakaran** proposed use of digital signature for authentication purpose in cloud computing. The propose work assured to secure the information in cloud server[3].**Sanjoli Singla, Jasmeet Singh** proposed a design that can help to encrypt and decrypt the file at the user side that provide security to data at rest as well as while moving. For this Rijndael encryption algorithm along with EAP-CHAP used [4].**Kuyoro S. O.**described key security considerations and challenges which are currently faced in the Cloud computing [8]. **J. Bethencourt** et al, discussed Attribute Based Scheme (ABE). For this, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs that are In key-policy and Cipher text-policy [17]. **ENISA**(European Network Information and Security Agency)investigated the different security risks related to adopting cloud computing along with the affected areas, various risks, impacts, and vulnerabilities in the cloud computing may lead to such risks[18]. **Balachandra** et al, discussed the security SLA's specification and objectives related to data locations, segregation and data recovery[16].**Kresimir** et al, discussed high level security concerns in the cloud computing model[14]. **Bernd** et al, discussed the how security weaknesses existing in the cloud platform and how they affect the client data. [20]. **Cloud Security Alliance (CSA)** had given TOP threats to cloud computing [19].**Service Level Agreements (SLA)** also defined many times for data on the cloud [20].

III. SECURITY ISSUES TO CLOUD DATABASE

Following are the security issues to be fulfilled while working with cloud database:

a) **Privacy and Confidentiality**

Once data get dispatched on the cloud database, there will be limited access to that data. Privacy of sensitive data should always be maintained. Appropriate privacy policies and procedures should be there to assure the cloud users of the data safety [3].

b) **Data integrity**

Integrity of data should be maintained with security. Cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point [6].

c) **Data location and Relocation**

High degree of mobility can be offered by Cloud computing. There should be a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.

d) **Data Availability**

When data is available on different locations or clouds, integrity of data on cloud database would be maintain. Uninterruptable data should be provided.

IV. SYSTEM ANALYSIS

Existing System Issues:

Original data must be accessible only to the trusted parties that do not include cloud providers, intermediaries and internet [13]. In any trusted parties data must be encrypted. Satisfying these goals has different level of complexities depending on type of cloud. It was also a time consuming task to encrypt data on cloud database and access it [8].

Disadvantages of Existing System:

- ❖ Implementation of encryption becomes difficult due to computational complexity.
- ❖ Security was less.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

V. PROPOSE SYSTEM DESIGN

User has to go through following steps as shown in Figure 1; while dealing with proposed work.

- Authentication is checked; if it is successful then User is able to create a new cloud, having access to Public cloud and having access to Private cloud.
- If user selects 'Public Cloud Access' then he will be able to Upload plain/encrypted data file on public cloud and Download plain/encrypted data file from Public cloud.

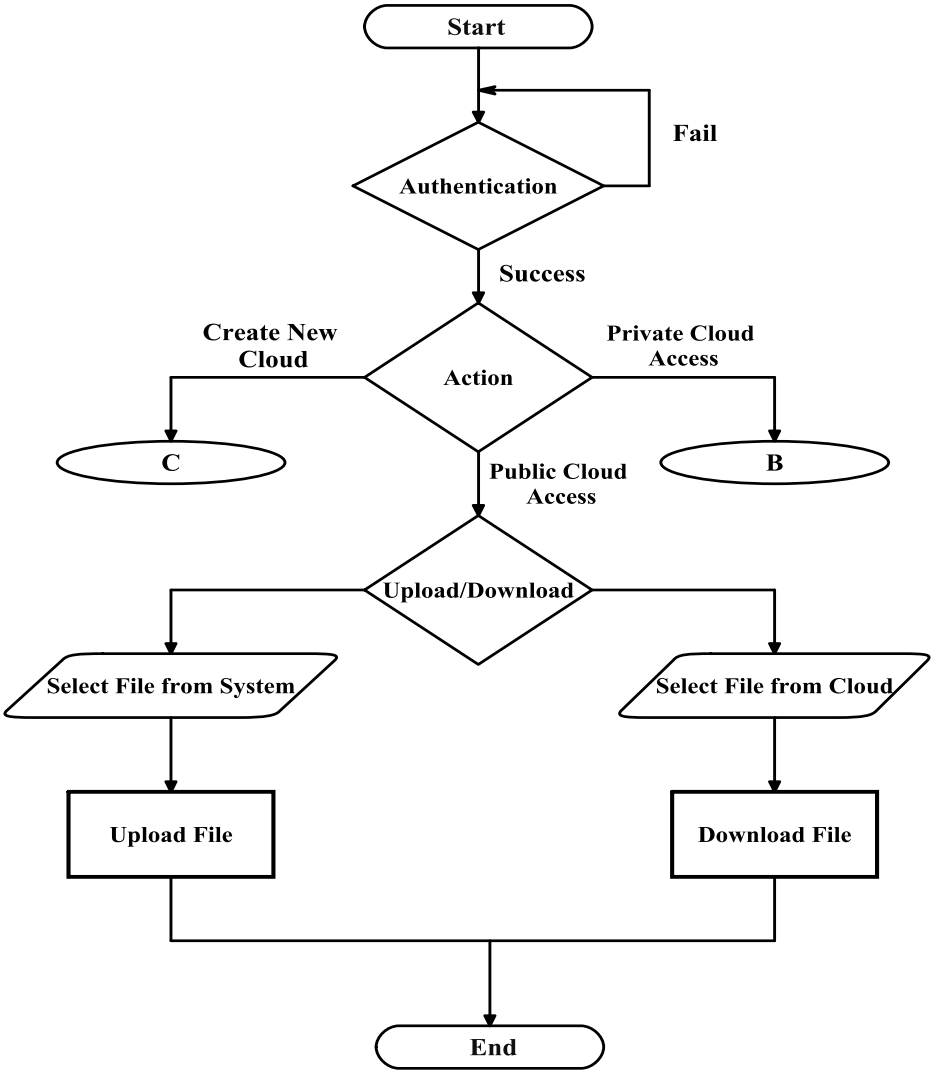


Figure 1: Working of propose system

If User/Client will choose 'Private Cloud Access' then following steps takes place and as shown in Figure 2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

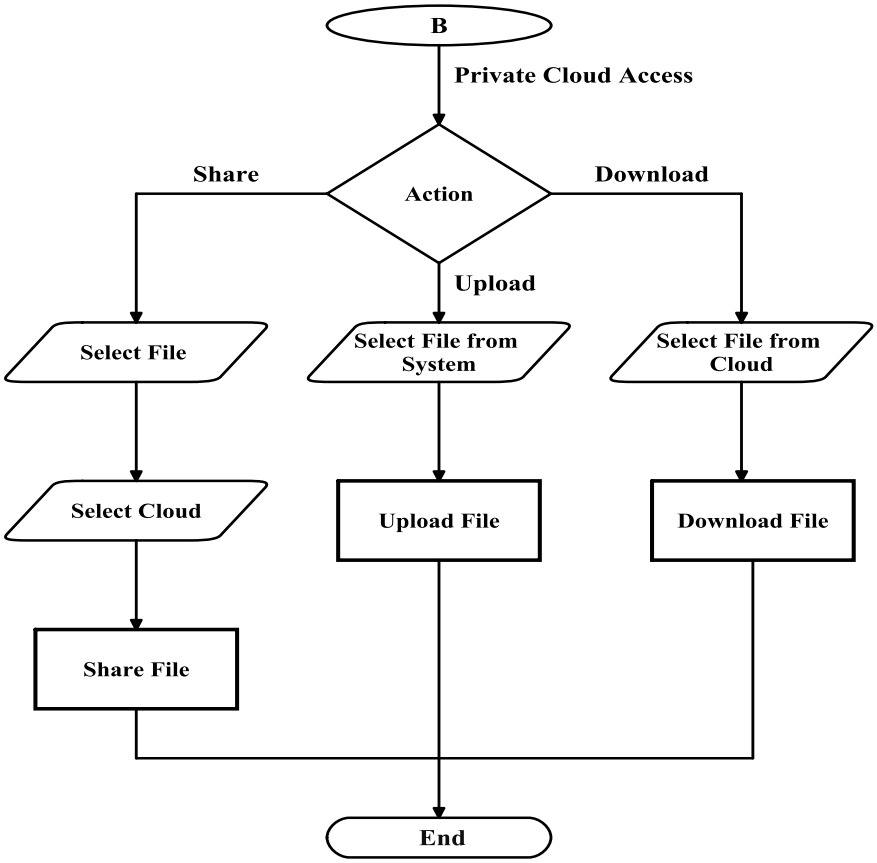


Figure 2: Accessing and sharing data on Private cloud

If User/Client has to Create a New Cloud then he has to follow steps shown in Figure 3.

- If User will select 'Create New cloud' then he will be able to create new virtual cloud as per requirement.
- If User will choose a 'Private cloud' option then it is created and file uploaded on his personal cloud and accessible to him only.
- If User choose a 'Public cloud' option in which global cloud will be created directly and shared cloud get created after members (users) of that cloud selected by owner.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

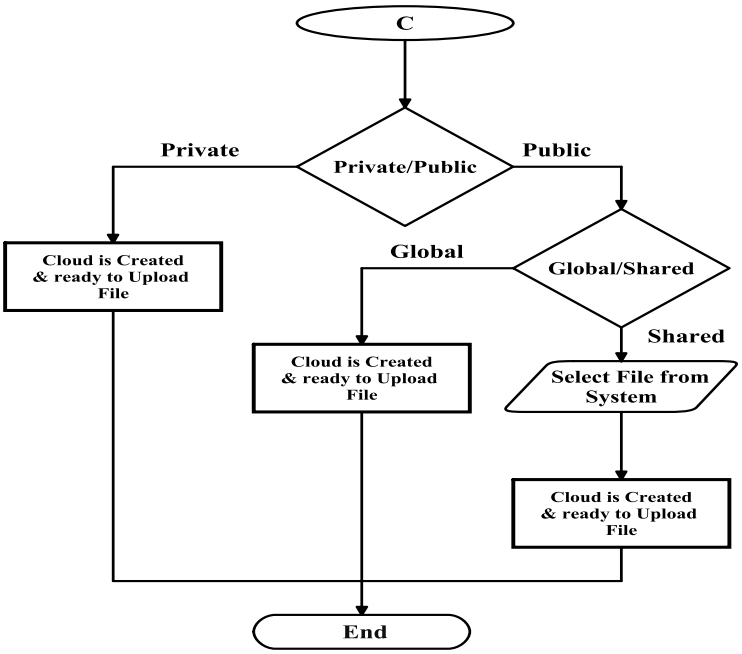


Figure 3: New Cloud Creation

VI. PROPOSE SYSTEM IMPLEMENTATION

- **User Registration:**

Many numbers of users will be able to do registration and create their virtual Private clouds by default when registrations get completed.
Input: Information of user will be taken for generation of User-id and Password.
Output: User gets registered and Virtual Private cloud will be created for registered user.

- **Virtual Cloud Creation:**

After registration, users have to Log-in and options will be provided for creation of shared (Public) or Private cloud.
Input: User-id, password, select option for Shared or Private cloud.
Output: Shared or Public cloud created for specific user.

- **Upload Data over cloud:**

Input: Select cloud name for keeping user's data file.
Output: User's data will be kept on particular cloud for future purpose.

- **Download Data from cloud:**

Input: Select cloud name from which client has to get data which is present over cloud.
Output: Client will be provided with required data from selected cloud.

- **Encryption of Plain Data File:**

Input: Generated key and Plain Data File from System.
Output: Encrypted file in Human Unreadable format.

- **Decryption of Encrypted Data File:**

Input: Same key used for Encryption and Encrypted Data File.
Output: Decrypted Data File in Human Readable format.

VII. EXPERIMENTAL RESULTS AND DISCUSSIONS

Comparisons of symmetric key algorithms are as shown in Figure 4 and the following results can be concluded:

i. The running time is faster on the cloud network.

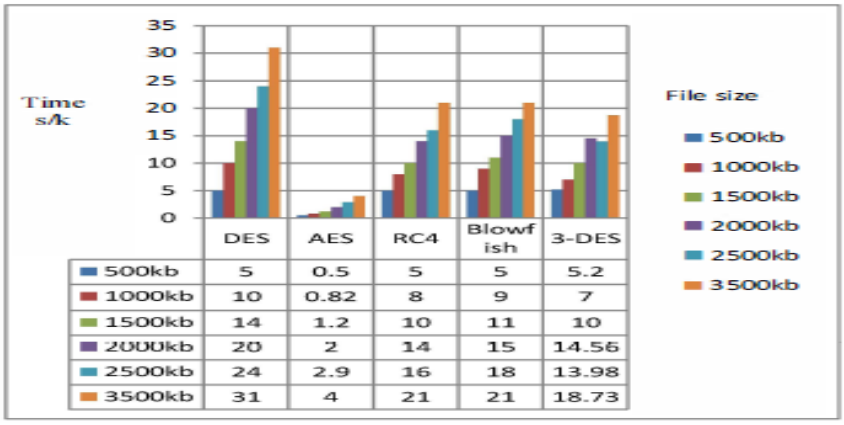
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

ii. Running time is proportional to the input file size as shown in Figure 4; more the file size more the time.
iii. It has been observed that AES encryption technique is the fastest symmetric encryption method and it can be analyzed from Figure 4.Here it is shown that it requires less time for processing and encrypting data on cloud database.



	DES	AES	RC4	Blowfish	3-DES
500kb	5	0.5	5	5	5.2
1000kb	10	0.82	8	9	7
1500kb	14	1.2	10	11	10
2000kb	20	2	14	15	14.56
2500kb	24	2.9	16	18	13.98
3500kb	31	4	21	21	18.73

Figure 4: Comparison of Symmetric Key Algorithms available for Cloud Security

VIII. CONCLUSION AND FUTURE WORK

Cloud computing offers real various alternatives to IT departments for improved flexibility and lower cost. Many services are readily accessible on a pay-per-use basis and offer great alternatives to businesses that need the flexibility to rent infrastructure on a temporary basis or to reduce capital costs. Proposed a framework which encrypts data before it is uploaded on to the cloud and it also create secured, concurrent and independent encrypted data over cloud. Use of AES algorithm provides secure transfer of Data File within few seconds. Thus, if used securely, cloud computing provides a user with amazing benefits and overcomes its only disadvantage of security thread. In future, Mechanism to be implemented to Compress large size files automatically so that it will take less space on cloud database . The work will have to be done to detect duplicate copies of same data on cloud database. System will have to be deployed on server nodes globally, so that it can be access from anywhere.

REFERENCES

1. Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud databases", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 25, no. 2, pp.437-445, FEBRUARY 2014.
2. Sushmita Raj, Milos Stojmenovic, Amiya Nayak," Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 25,no. 2, pp.332-345,February 2014.
3. T. Sivasakthi and Dr. N. Prabakaran, "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" , *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 2,pp.12-18, February 2014.
4. Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", *International Journal of Advanced Research in Computer Engineering & Technology* ,vol. 2, no. 7,pp.2232-2235, July 2013
5. Guo Yubina, Zhang Liankuanb, Lin Fengrena, Li Ximinga,"A Solution for Privacy-Preserving Data Manipulation and Query on NoSQLDatabase", JOURNAL OF COMPUTERS, VOL. 8, NO. 6, 1427-1432, JUNE 2013.
6. Ming Li, Member, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 24, no. 1, 131-143, JANUARY 2013.
7. Omer K. Jasim, Safia Abbas, Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", *International Journal of Emerging Trends & Technology in Computer Science*,vol.2,no.6,pp.270-274,December 2013.
8. Kuyoro S. O., Ibikunle F., AwodeleO. ,"Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol. 3, no.5, 247-255, 2011.
9. Gartner," From Secure Virtualization to Secure Private Clouds", *http://www.vmware.com/files/pdf/analysts/Gartner*
10. "Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud", *https://www.cloudsecurityalliance.org,December,2009.*
11. Jericho Forum," Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration", April, 2009.
12. C. Jarabek,"*A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management"*, Department of Computer Science, University of Calgary, 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

13. Julisch, K., & Hall, M., "Security and control in the cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.
14. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349,2010.
15. D.Hyde,"A Survey on the Security of Virtual Machines", *http://www1.cse.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf*, April 2009.
16. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, pp. 517-520, 2009.
17. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
18. *http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing- risk-assessment*
19. *https://cloudsecurityalliance.org/topthreats/csathreats.v1. 0.pdf.*
20. *http://en.wikipedia.org/wiki/Cloud_computing.*