International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 9 2957 – 2962

ABC based Double Layer-Triple Encryption Method for Data Security in Cloud

Priyanka Vishwakarma
Department of Computer Science & Engineering, NIIST
RGPV University
Bhopal, INDIA
priyanka1032@gmail.com

Sini Shibu
Professor, Department of Computer Science & Engineering,
NIIST, RGPV University
Bhopal, INDIA
sini.shibu09@gmail.com

***Abstract*—** CLOUD computing is a new computing paradigm that is constructed on virtualization, aligned and circulated computing, utility computing, and service oriented architecture. The advantages of cloud computing include decreased charges and capital expenditures, expanded operational efficiencies, scalability, flexibility, immediate time to market, and so on. Distinct service oriented cloud computing forms have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and programs as a Service (SaaS). In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is generally a financial enterprise, which will not be completely trusted. That is the main reason behind researchers' motivation of the work. The proposed method provides better the data storage security with lesser time.

***Keywords*—** *Cloud Storage, Access Control, Data Security, Data Authentication, Hadoop.*

*****

I. INTRODUCTION

Cloud computing is an extension of grid computing and distributed computing, which is a software concept indeed [1], it works through variety of technologies such as software technologies, integration, management, and the use of various hardware resources. Cloud computing is realized mainly through the virtual technology [2]. The virtual technology can be divided into single virtualization and multiple virtualization; the single virtualization uses the virtual technology on a machine to work as many machines working together, such as VMware, while multiple machine virtualization links the machines through the control center and makes them work like one machine.

Hadoop, as a distributed open-source framework, which not only can be used as a platform for massive data storage based on its distributed file system HDFS [3,4,5], but also integrate Google's Map Reduce distributed programming framework, are now being widely used in cloud computing platform. But using Hadoop as a platform for massive data storage, data confidentiality, integrity and access control are worthy of deep consideration. For example, Owen O'Malley et al. have ever pointed out that various services in Hadoop cannot provide complete access control and identity authentication, at the same time, Data Nodes in Hadoop also lack essential access control for each data block [6]. As a result, a user can at ease forge legal identity to access HDFS or Map Reduce clusters. In order to tackle the troublesome problems, some have done a certain kinds of research. Owen O'Malley et al. designed the Kerberos protocol based on SSL to launch user identity authentication [6]; Indrajit Roy et al. designed and implemented the Airavat platform, which could ensure the vital data secure and privacy protection in the Map Reduce calculation process[7]; What's more, a framework of SecureMR has been proposed by Wei Wei et al. to guarantee the data and service integrity [8]. In fact, the research works they have done were mostly aimed at providing the user identity authentication to ensure the security and privacy protection. But in our opinion the most useful way to ensure security is providing a mechanism to protect the data itself.

So in this paper, we dedicate to propose a novel model of cloud data secure storage model with data authentication, which ensures the data security and integrity based on HDFS. The innovation of this model is that we provide access control mechanism on data files stored in HDFS and integrate cryptography with symmetric encryption to provide the data with the privacy protection and integrity check.

The rest of this paper is structured as follows: Section II presents the related work in the area of secure storage and related information in the cloud. In section III we present our

scheme and algorithm for solving the secure problem of the distributed storage system based on Hadoop. In section IV we prove our scheme to be safe. In section V we present our implementation and experiments. Finally, in section VI we conclude our work.

II. SECURITY: DATA STORAGE

Out of so many concerns of cloud environment, data storage play very vital role, That's the reason, which motivates researchers to work in this area. In any cloud environment user can store the data on the cloud after getting logged in. This work can be done with the help of the any browser, and in the similar fashion user get back the data from the cloud storage by the help of the browser on his or her iPad, Laptop, Mobile or any other device. With the growing techniques cloud makes more convenient and effective ways to upload the data simpler, faster, and convenient way. But at the point of time, users are not willing to upload their confidential data for the reason of security. The issue of security restricts cloud further progress and development. There is lot of print documents, which told about security breaches and threats with so many challenges in the cloud-computing environment with their 3 main patterns (Saas, Paas, Iaas). [9, 10, 11, 12] Analyzed and summarized the threats being faced from different aspects. Weak security of the Cloud storage is mainly happened in the bellow aspects:

1) Transmission security: This category handles the security breaches when the data is in transmission state. Someone can capture the data and try to decode it, but this category would not be very much connected with the strong encryption based data storage protection system.

2) Access control: The category of access control authority deals with the authority concerns of the data stored in a cloud environment. The user may lose right to monitor his or her data safety.

3) Data storage: This category handles about the data, which is stored by the cloud user. The data in store in a distributed manner in cloud environment, where user is not aware of specific and exact location or position store data.

4) Data verification: Data verification deals the situations where it deals with lack of concerns of cloud in no verification uploaded data. Cloud would not give any kind of guarantee to uploaded data is order to the originality of the data which comes from user

III. DATA AUTHENTICATION: ATTRIBUTE-BASED ENCRYPTION

In the basic service of cloud safety, storage service should store data in the form of cipher text; the realization of the corresponding cloud access control service should be different with the traditional access control service model (as the access control based on role, the access control service model based on property, forcible/independent access control model, and so on).

ABE(Attribute-Based Encryption) is a kind of encryption based on property, it indicates that all the nodes do not use single identity as the mark, but use a series of properties to mark. It is assumed that the set of properties that marks the nth node is set Dn, the node preserves the private keys corresponding to these properties. The encipherer first provides the properties set C, which should be used in the decryption of the super secret information, and the cipher text M composed of the public keys of these properties. While it is to be decrypted, only if the properties set owned by the node and the properties set needed for the decryption intersect with each other, the number of the same properties achieves some threshold value (set by the encipherer), e.d. $Dn \cap C \geq d$(the threshold value), should the ciphertext be decrypted

IV RELATED WORK

In 1949, Shannon published a paper entitled "Communication theory of secrecy systems". After that the theory of modem cryptosystem is gradually established. According to the key characteristics, modem cryptosystem is can be classified into symmetric cryptosystems and asymmetric cryptosystems. For a symmetric cryptosystem, the sender and receiver share an encryption key and a decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystems are DES (Data Encryption Standard) and AES (Advanced Encryption Standard). For an asymmetric cryptosystem, the receiver possesses a public key and a private key. The public key can be published, but the private key should be kept secret. The representatives of asymmetric cryptosystems are RSA (Rivest, Shamir Adleman) and

ECC (Elliptic Curve Cryptosystem). Considering the difference of encryption speed, the symmetric cryptosystem always encrypt a large quantity of text data, and the asymmetric cryptosystem always encrypt the short massages, such as keys. The principle of massive data encryption based on modem cryptosystem is converting the data into binary stream, and then encrypting this binary stream with modem use of modem cryptosystems.

First, convert the plain text into small data blocks; second, encrypt these data blocks with the selected modem cryptosystem; finally, convert the encrypted data blocks into cipher text

(1) DES

National institute of standards and technology (NIST) recruited cryptosystems all over the world on May 15, 1973. DES was proposed in this activity [13]. NIST approved DES as the data encryption standard of USA government in 1981. DES is a block cipher algorithm, whose block length is 64 bits and the key length is 56 bits

(1) AES

Because of the short key, DES cannot satisfY the security requirements in practice [14]. Therefore, NIST recruited the advanced encryption standard all over the world on Apnl 5, 1997. NIST declares Rijndael algorithm as AES in October 2000, which is instead of DES on November 26,2001. AES is a block cipher algorithm, whose block length can be 128, 192 or 256 bits

(2) RSA

In 1978, Rivest, Shamir and Adleman proposed RSA cryptosystem [15]. Its advantages are simple encryption principle and easy realization. However, with the improvement of the integer factorization algorithm and computmg capability of computers, we should continuously extend the key length of RSA to ensure the security of interactive information. Hermante Riele et ai, successfully broke down 512 bits-RSA with the method of number field sieve on August 22, 1999. Therefore, experts suggest using 1024 bits-RSA to ensure the 1O-years, security, and 2048 bits-RSA to ensure the 20-year security in practice.

V. PROPOSED WORK: ENCRYPTION AND DECRYPTION OF DATA FILES

There is an advantages and disadvantages of each and every security methods. This concept motivates researchers to do work in the extension of the existing works. Researcher's proposed work can be divided into various stages. For the simplicity researchers can say the it is made up on following main ingredients:

1. Vigenere Cipher
2. Encryption key is generated with the help of Idea algorithm
3. A dedicated Proposed Encryption Algorithm
4. Apply Attribute based Encryption (ABE)

The detail of the algorithm is as follows which is shown in figure 1 and figure 2.According to figure 1user has enter two values (i) plain text and (ii) user key. How these are moving is expressed in both the figures. One more important thing, which needs to get in notice at this point of time is that, figure 2 is shown one iterations but in complete algorithm researchers have called it for ten iterations to provide better security level as compare to single iteration level. This idea is as same as DES concept.

Main Features of Proposed Work:

1. Block Ciphering with Encrypted Key
2. ABC (Attributed Based Cryptography)

Note: Blue color shows Cloud functionality and Red color show Encryption Method in figure 1.

At the same time figure 2 shows the Block ciphering based Encryption process. Which is made up of some logical operations like circular shifts and xor operations to provide the mode distance of the cipher text from the plain text to provide more security:

ISSN: 2321-8169
2957 – 2962

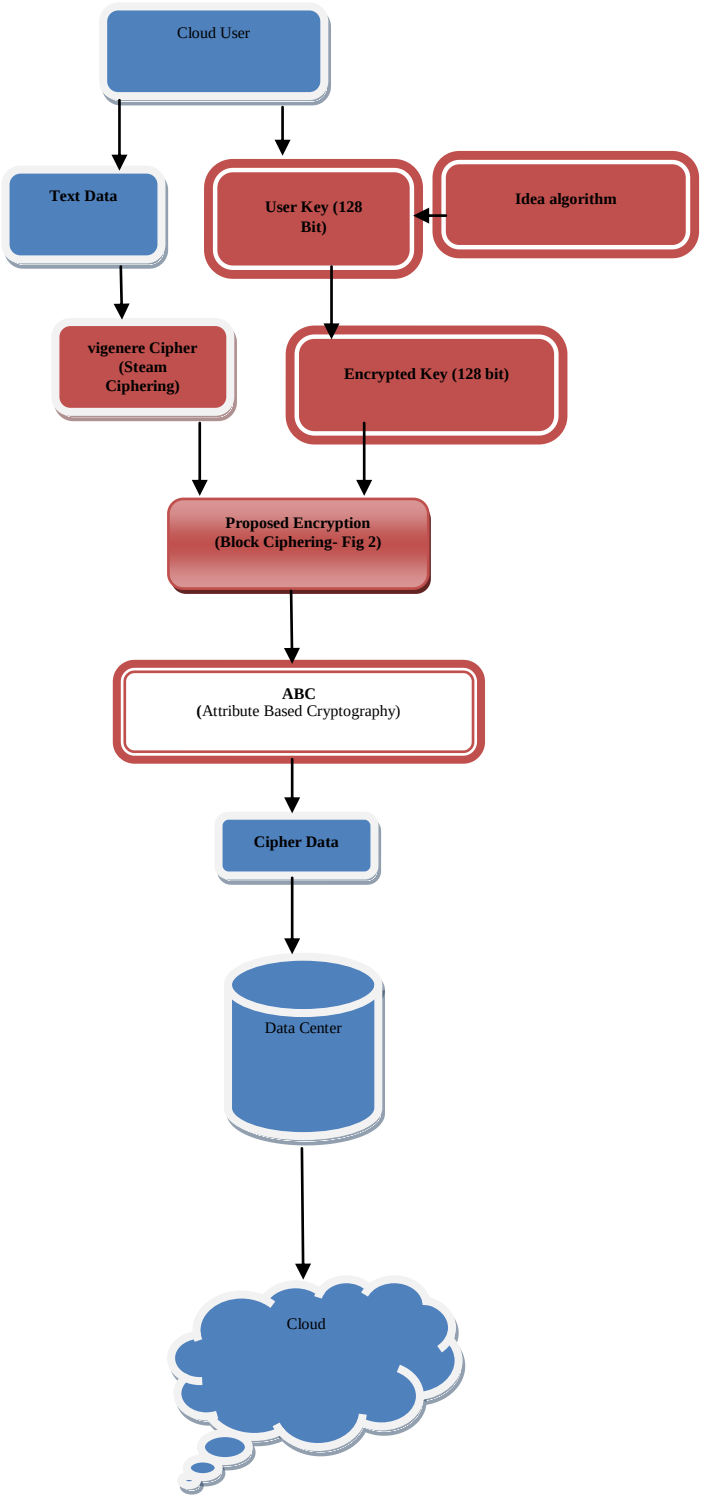


Figure 1: Proposed worked: ABC based Double Layer-Triple Encryption Method for data security in Cloud Environment

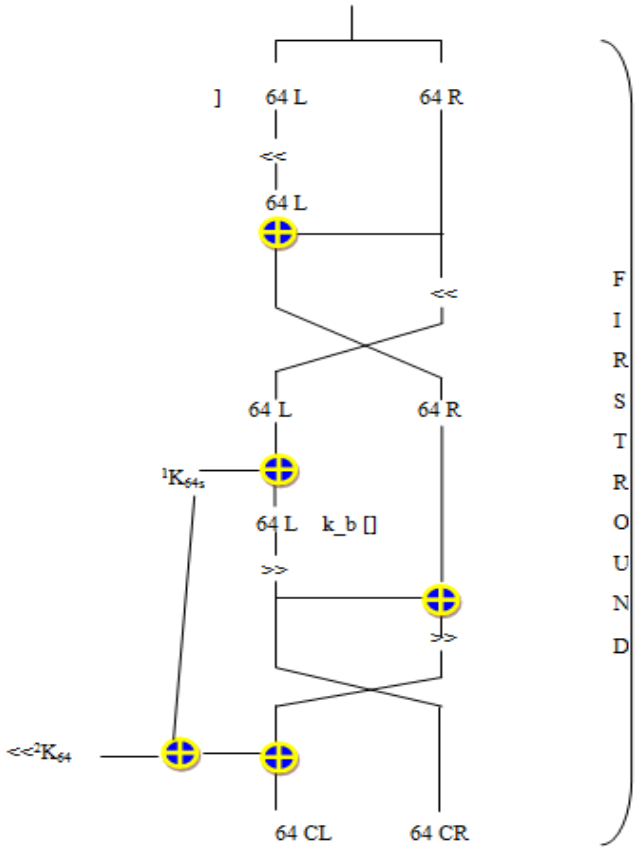


Figure 2: Encryption Architecture of the Encryption algorithm

VI RESULT AND ANALYSIS

Researchers have performed the encryption of the various data of different length. The system on which these iterations have be performed is having following configuration as shown in table 3.

TABLE 3: Shown the System configuration on which experiments have done.

Model	Pentium P-IV CPU
RAM	1GB
32 Bit Operating System	
Windows XP	

There is more than one text as well on which researchers have performed their experiments, which is shown in figure 4.

TABLE 4: Various lengths of input data

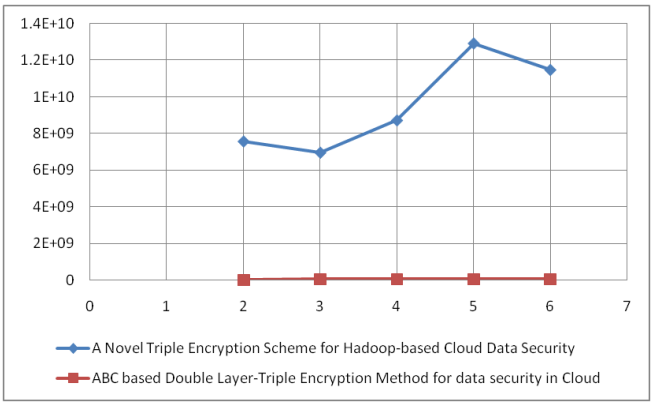
S. No.	Size
1	32 Bytes (16 Char)
2	64 Bytes (32 Char)
3	96 Bytes (48 Char)
4	128 Bytes (64 Char)
5	160 Bytes (80 Char)

As researchers have perform the proposed work on various of data on the cited system ten-ten time and put an average CPU execution time as shown in table 5.

TABLE 5:CPU Execution time in microseconds

S. No.	Base Paper	Proposed Paper
1	7579744534	2963403
2	6969728129	27096553
3	8724916837	34287246
4	12918579892	40135680
5	11475221175	45131062

Graph 1 clearly shows that researchers proposed algorithm works better in time as compare to base[16] work. The performance comparison of proposed method "ABC based Double Layer-Triple Encryption Method for data security in Cloud" with base paper [16].



Graph 1: "ABC based Double Layer-Triple Encryption Method for data security in Cloud" with base paper [16].

VII. CONCLUSION AND FUTURE WORK

In this paper, researchers have implemented a security architecture using encryption techniques to secure the management of data in cloud environment with lesser time re. Aiming at the existing popular cloud data storage security weakness including time requirement, researchers put forward a security encryption schemes based on cloud which satisfy the less timing and storage security

In the future versions of system, researchers plan to implement a more sophisticated technique for encryption and authentication.

REFERENCES

[1] HongBo Zhou. Cloud computing: technology, application, standar, Electronic Industry Press.2011

[2] http://en.wikipedia.org/wiki/Virtualization

[3] Hadoop. http://hadoop.apache.org, Nov. 2012.

[4] HDFS. http://hadoop.apache.org/hdfs, Nov. 2010.

[5] X.S Duo, J. Zhang and Q. Gao. A Mass Data Management System based on the Hadoop. Journal of Microcomputer Information, 2010, 26(5): 202-204.

[6] O. O'Malley, K. Zhang, S. Radia, et al. Hadoop Security Design. https://issues.apache.org/jira/secure/attachment/12428537/securitydesign.pdf, Oct. 2009.

[7] Airavat. http://www.cs.utexas.edu/~indrajit/ airavat.html, Nov. 2010.

[8] W. Wei, J. Du, T. Yu, X.H Gu. SecureMR: A Service Integrity Assurance Framework for MapReduce. Computer Security Applications Conference, 2009. ACSAC '09 Annual, PP. 73 – 82.

[9] MUNIER M.Self-Protecting Documents for Cloud Storage Security[C].Trust, Security and Privacy in Computing and Commu. Liverpool, 2012: 1231-1238

[10] SHAIKH F B. Security threats in cloud computing[C]. Internet Technology and Secured Transactions (ICIT . Abu Dhabi, 2011: 214-219.

[11] Security of Cloud Computing Providers Study, " Ponemon Institute, 2011.

[12] V. Winkler, "Securing the Cloud Computer: Security Techniques and Tactics, " Elsevier Inc., ISBN: 978-1-59749-592-9, 2011.

[13] S. M. Yoo, D. Kotturi, D. W. Pan and 1. Blizzard, "An AES crypto chip using a high-speed parallel pipelined architecture", Microprocess Microsy, vol. 29, no. 7, pp.3 17-326, 2005.

[14] Linguang Xie, "Analysis on AES algorithm", China Science and Technology Information, 2007, vol. 19, no. 20, pp.95-97.

[15] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

[16] Chao YANG, Weiwei LIN and Mingqi LIU "A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security, " IEEE 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.