Hybrid Data Encryption Algorithm using Id-based Encrypted Key at Cloud Storage

Ankita Gautam*, Prof. Garbita Gupta** and Dr. N. K.Tiwari***
*M.Tech Scholar, Department of CSE, BIST, Bhopal
**Professor, Department of CSE, BIST, Bhopal
***Bansal Institute of Science and Technology , Bhopal

Abstract: Now a day's cloud computing is being used in several areas like industry, medical, science and research, colleges etc for storage of huge amount of data. User can retrieve data files from cloud data center on request. While storing data files on cloud server several security issues may arise. Cloud computing has been flourishing in past years thanks to its ability to produce users with on-demand, flexible, reliable, and affordable services. With a concept of cloud applications being offered, information security becomes a vital issue to the cloud. To overcome from these security issues there are a number of techniques. Out of several security techniques Cryptography is more popular now a day's for data security. Use of a traditional cryptography algorithm is not effective or sufficient for high level security to data in cloud computing. So, as to create certain security of data at cloud data storage a design and implementation of an algorithm to enhance cloud security is proposed. In this paper we have introduced new security technique based on symmetric key cryptography algorithm and ID based cryptography algorithm. Proposed methodology or system is provides security to data files by using hybrid encryption/decryption technique. The hybrid algorithm is designed by using Vigenere algorithm and AES algorithm. Before encryption the cloud server generates encrypted key that is to be used to encrypt data files using hybrid algorithm. This encrypted key is generated by using concept of ID based encryption algorithm and hash value of secret password allotted to each registered user. This encrypted key is of variable size dependent on the data file's size. For authentication of user SHA-512 algorithm is used. As a result the proposed algorithm provides enhanced security as well as reduces time complexity during encryption and decryption process of data file.

Keywords: Cloud Computing; Security; Confidentiality; Authentication; Id-based Encryption.

Introduction

Cloud computing is based on such concept of abstraction and virtualization and deliver services to the client. Basically, the cloud computing has inherited these concept from Grid and Cluster Computing. All computing resources are aggregated into a packet and delivered as a service over the cloud. Cloud computing with an objective delivers computing resources and services as a utility over the network to the user and hence inherits such pay-as-you-go property from utility computing.

The concept of Cloud Computing came into existence since from 1950's with implementation of mainframe computers. Since then, cloud computing has been evolved from static clients to dynamic ones from software to services. By the end of the 90s and beginning of the 2000s were a great time for Internet which provided Cloud computing the right environment for growth, as multi-tenant architectures, high-speed bandwidth and universal software interoperability standards.

Cloud computing is a subscription based service where we can obtain networked storage space and computing resources. It makes possible for us to access our data from anywhere and anytime. It renders the cost of purchasing computational resources and storage as everything is available on cloud and delivered as per demand of user and we have to pay for that only for which we want to use [1]. Only requirement of cloud computing is that we need to have internet connection available to enjoy their computational services. Numerous companies and research organizations are applying cloud computing concepts to their business including GOOGLE, AMAZON and AZURE. NIST offers up several characteristics that are essential for a service to be considered as Cloud [2-3]. These essential characteristics of cloud are: On-demand self-service, broad network access, resource pooling, rapid elasticity and scalability and measured Services.

Trusted cloud computing is a computer security architecture that is refers to technologies or measures for resolving security problems and protecting cloud systems from attackers through hardware enhancement and software modifications. It will protect data which is being used by hypervisors and applications against unauthorized access by providing strong authentication method or by applying encryption methods[4].

In cloud computing environment, different entities such as users and resources from different sources aggregated together to form a Cloud. So, in such architecture authentication is important and complicated. Authentication in cloud computing is implemented by Trusted Cloud Platform (TCP). The TCP is based on the TPM. The TPM is an independent hardware which resists the attack from hardware and software. The TPM contain a private master key which can provide protect for other information store in cloud computing system. TPM provides the trust root for users because it is hard to attack.

Authenticating cloud computing with TCP : In TCP user's identity is proved by user's personal key and this mechanism is integrated in the hardware. So, it is very hard to the user to deceive from their information of identity. Each site in the cloud computing system will record the visitor's information. So, by using the TCP mechanism in cloud computing, the trace of participants can be known. Now, if the cloud user do some malicious behavior they can be easily traced. With trusted system in cloud computing we can know what the user can do and what the user have done. So it acts as a monitoring function in cloud environment to supervise the behavior of user.

Access Control in cloud computing environment by TCP : In cloud, user login from the TCP based on Trusted Platform Module (TPM), and get the authentication certificates or accessing rights. When the user wants to communicate with remote entity and access resources, it has to give all authentication credentials such as ID, password or certificates. And the information between cloud and user is protected by the session key, which is generated by TCP.

TCP based cloud data security : As TPM provides the encryption key and session key which can be used by cloud computing to encrypt important data stored in cloud.

In cloud computing environment there is need of security technologies that are required for providing protection to the resources and virtual machines or virtual servers. To provide security and privacy one of the effective security solutions is Cryptography [5-11]. This is a technique to protect sensitive data, especially at the cloud storage. Cryptography is a method of achieving security by changing readable form of data into unreadable form. Using cryptography we can protect the sensitive data in network. In cryptography the sensitive data of the user are encrypted in cipher text which adds a security level over the data. Cryptography schemes are divided into two groups i.e. symmetric-key cryptography and asymmetric key cryptography. Mostly used cryptographic algorithms used in cloud computing are:

Modern Encryption algorithms, such as RC6, AES, DES, 3DES and Blow-Fish play a vital role in data security of cloud computing.

Homomorphic encryption is a form of encryption technique which performs some computation on ciphertext and result thus generated matches with the result of operation that is performed on plaintext, when decrypted. Generally, Homomorphic technique is to maintain integrity of data over the cloud.

Identity based encryption is a public key cryptography in which key is generated by using some unique information about the identity of user such as user Id, email address, etc [13, 14].

Related Work

Sahai and Waters proposed Fuzzy Identity-Based Encryption [9] projected the very initial idea of the attribute-based encryption scheme through public key cryptography. Fuzzy Identity Based Encryption has a set of explanatory attributes. Fuzzy IBE can be used for a purpose that is called as attribute based encryption. In this proposal in which each user is identified by a set of attributes, and some function of this attributes is used to determine decryption ability for each cipher text. Sahai and Waters, first introduced the public-key cryptography attribute based encryption (ABE) for cryptographically imposed accessing rights. In ABE mutually the secret key of the user and the ciphertext are coupled with a set of attributes. A user is able to decrypt the ciphertext if and only if in any case a threshold number of attributes that have common characteristics between the ciphertext and user secret key. Different from traditional publickey cryptography such as Identity-Based Encryption, ABE is intended for one-to-many encryption in which ciphertexts are not necessarily encrypted to one particular user. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. Threshold access control in Fuzzy-IBE is based on polynomial interpolation. Each user in the system picks a random k-1 degree polynomial to associate with the private key and embed the attributes into the polynomial. If a user's private key can match more than k attributes of the ciphertext, he/she can decrypt the ciphertext. Since each user in ABE systems is associated with a random polynomial, multiple users cannot combine their attributes in a useful way for a collusion attack.

N. Sengupta and J. Holmes [14], researcher had presented a hybrid cryptography system. In this Hybrid cryptography Vigenere and Caesar Cipher Encryption algorithm are implemented which will prevent the cloud infrastructure in three main places, in client location, in the network and in server. Motive of such type of concept to increase computation time for decryption of cipher text messages for the hackers will be more compared to any single cryptographic system. The Hybrid Vigenere Caesar Cipher Encryption (HVCCE) work in three phases. In the first phase, Caesar cipher is applied on the plain text. In the second phase, according to Vigenere Square value, Vigenere Cipher is applied along with the keyword on the encrypted text achieved from the first phase. In the third phase, according to Vigenere Square value, Vigenere Cipher is applied with the reverse word of the keyword considered in second phase.

Chao Yang et al. [15], author has proposed the data security in cloud data storage. For that a novel triple encryption scheme is presented, which combines DEA, RSA, IDEA. They implemented the triple encryption scheme in Hadoop-based cloud data storage. HDFS files are symmetrically encrypted by DES algorithm and then uses RSA algorithm to encrypt the Data key asymmetrically and IDEA is used to encrypt the private key of RSA which would be used at retrieval time of file.

Faraz Fatemi Moghaddam et al. [16], authors proposed hybrid asymmetric-key encryption algorithm grounded on RSA Small-e and Efficient RSA allowing to the security concerns in cloud computing environments. In the proposed methodology, the number of exponents has been improved to three and a dual encryption technique has been useful to increase the safety level of the algorithm in evaluation of original RSA. Bestowing the simulation consequences, the total execution time of HE-RSA was improved up to almost 50 percent reduced than the original RSA and this increase may be reasonable and suitable as compared to the security level and the efficiency of HE-RSA.

V.S. Mahalle and A. K. Shahade [17], projected a hybrid algorithm grounded on AES and RSA. In hybrid algorithm 3 keys are used. For file upload on cloud compulsory keys are secret key of AES algorithm as well as public key of RSA. Private key of RSA and AES secret key are important to retrieve data from cloud. Every time use makes a strength to upload data on cloud leading that file stored onto directory for short time. During encryption procedure first AES algorithm is practical on file afterward that RSA algorithm is functional on encrypted data [18]. Reverse process is followed for file retrieval time i.e. decryption. Afterward applying keys that file is converted into encoded form and stored on cloud data center.

Keke Gai et al. [19], delibrates on security challenges and designed a novel data encryption method, termed as Dynamic Data Encryption Strategy (D2ES). Their approach of proposed methodology objects to selectively encrypt data file by applying privacy classification technology under timing limitations. This technique is intended to maximize the privacy shield scope by using a selective encryption strategy contained by the essential execution time requirements.

G.Prabu kanna and V.Vasudevan [21], proposed a new identity based hybrid encryption using RSA with ECC to improve the security of outsourced data file. In this methodology cloud user encrypts the sensitive data file with hybrid algorithm. Then the proxy re-encryption method is applied to encrypt the keyword and identity in normalize toward enhanced security of data.

Bhale Pradeepkumar Gajendra et al. [22], proposed an algorithm that is concerned to overwhelmed the security trade-off and increase the performance of data transmission and enhance the security level through Third Party Auditor and Identity Based Encryption.

With increasing cloud popularity, clients concern about data security, data integrity, and sharing of data is also raised which must be resolved for efficient deployment of cloud services. There exists multiple means of achieving this such as client encrypt the data on his/her machine and then store it to cloud storage server, computing and storing hash value of data on client machine, sharing of difficult or tricky key which may be used for encryption with specific group of clients or users. As a result, it had become heavy task for client to keep these information and share such information. If in an event, these sensitive information about data get lost or stolen poses a great threat to the total data. The aforementioned approaches burden the client with load of securing data before storing it to the cloud storage[20-25]. So, another approach in which cloud service provider provides the service for secured sharing, hashing, and encryption/decryption for the sensitive data of client along with computational overhead as well as time complexity are main overhead in designing secure model for data security in cloud computing.

Proposed Methodology

As a lot of and additional organizations and people tend to outsource their data to cloud storage, the protection and user privacy protection attract a lot of attention. Encryption and decryption of data files are primarily user-centric, that solely legitimate users are allowed to transfer and download files, and specify whether or not a file is shared to alternative users. There are two ends whereas we tend to mention the security of the data in a cloud environment. Within the 1st end, the protection of data might concern whereas data is moving into the network after taking data from the user web site through the any web based application. And in the second end the security concern could be at Cloud end once data is already through network and on the point of store in cloud disk. The main objective of the proposed work is the security concern associated with data files at the Cloud End. In order to keep securities at cloud storage following skeleton of the proposed work which is hybrid in nature containing three stages is given.

File Storage Process

The proposed work, in figure 1, consists of three stages. In first stage, authentication of user is checked. The hash value of password is generated using SHA-512 at both end (user end and cloud end) and matched at cloud end. If user is found authenticated then secure key generation process is performed in second stage. As a result of this key generation technique, an encrypted key of variable size depending on the size of file is generated which reduces the threat of key exposure to intruders, undoubtedly.

The ID- based encrypted key is generated by performing XOR operation between ID-based secret key generated by cloud and the hash value of secure password generated by cloud using SHA-512. In the third stage, proposed work deals with new designed encryption algorithm which is based on the Vigenere cipher and AES cryptographic concept. In this stage the Vigenere cipher encrypt the data using variable sized key that is dependent on the size of the data file. After ciphered data is generated then it is encrypted using AES algorithm which uses 256-bit block size for the encryption purpose and this 256-bits block size is encrypted with the help of the encrypted key which size is also 256-bits. So in this way through the new designed encryption algorithm provides the double level of data security. At last but not least, it is very obvious that while talking about the security of the data the cryptographic encryption technique plays an important role but at the same time it is important to check authentication rights of the user who tries to access these cloud-disk stored data. Authentication or verification of the user before granting the access to the cloud data plays a very vital role in measures of security.

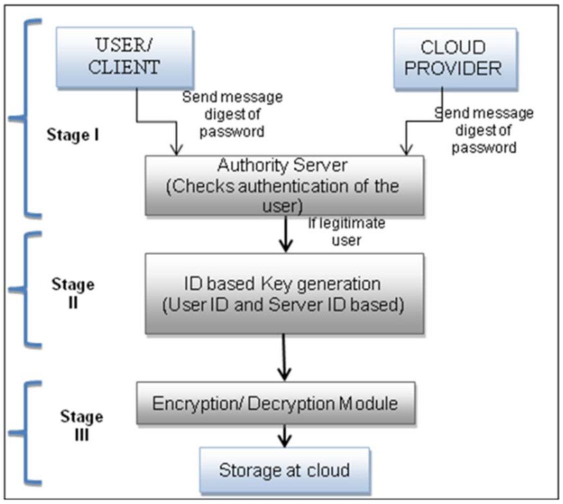
USER/ CLIENT
CLOUD PROVIDER
Send message digest of password
Send message digest of password
Stage I
Authority Server (Checks authentication of the user)
If legitimate user
Stage II
ID based Key generation (User ID and Server ID based)
Stage III
Encryption/ Decryption Module
Storage at cloud

Figure 1: Proposed methodology architecture

Stage I: User Authentication

This is the first step of proposed work where the cloud user authenticates itself on the cloud server.

Figure 2 depicts the functionality of the first stage of the proposed work, i.e. user authentication. Detailed steps of authentication process as described below:

- Start
- User sends its hash value of shared password that was created while registration of the user. The hash value is generated by using SHA-512 algorithm that generates 160-bit hash value. By applying such algorithm it is not necessary to send shared secret password over the untrusted channel or medium and user is authenticated as well.
- Server also sends hash value of the password.
- Authority server matches the hash value of password of send by user and cloud server.
- After authentication of user the authority server generates the secret key for hybrid encryption further in stage II.

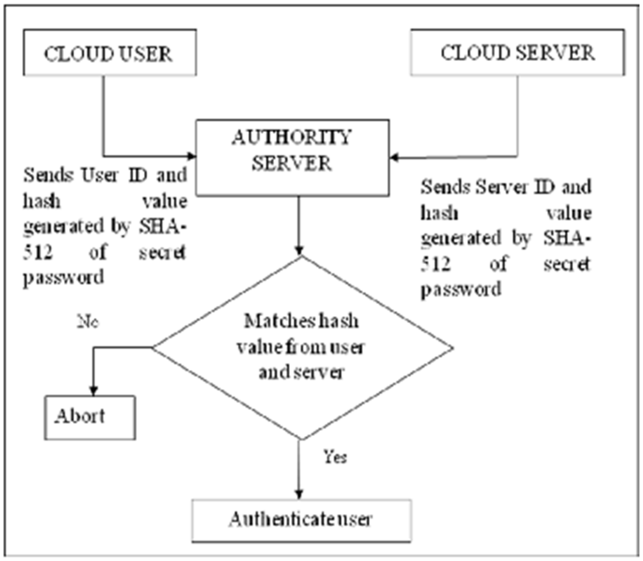
CLOUD USER
CLOUD SERVER
AUTHORITY SERVER
Sends User ID and hash value generated by SHA-512 of secret password
Sends Server ID and hash value generated by SHA-512 of secret password
Matches hash value from user and server
No
Abort
Yes
Authenticate user

Figure 2: User authentication process

Stage II: Key generation

After authentication of user by authority server, this stage proceeds towards generation of ID based secret key that is used for data/file encryption and decryption. This key is generated by XOR operation of hash value and User and Server ID. This process results encrypted key. So, the proposed algorithm encrypt data file and key that enhances the security level as well as reduces computational overhead. Figure 3 depicts the procedure of second stage of the encryption process.

Stage III: Encryption/Decryption module

In this stage of proposed methodology, after generation of encrypted key using ID based cryptography, the data file is encrypted using hybrid algorithm i.e. Vigenere cipher and AES algorithm. This proposed algorithm is combination of traditional as well as modern cryptography that overcomes their demerits.

Figure 4 depicts the flow diagram of proposed encryption/ decryption algorithm.

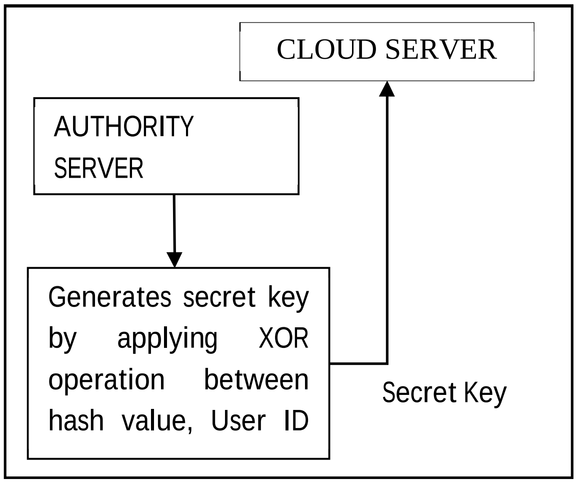
CLOUD SERVER
AUTHORITY SERVER
Generates secret key by applying XOR operation between hash value, User ID
Secret Key

Figure 3: Encrypted Key generation process

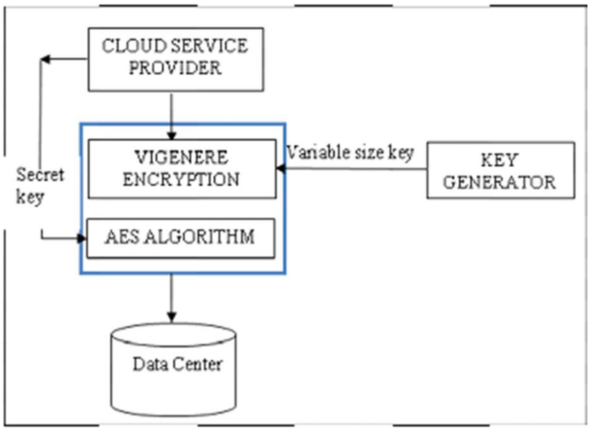

Figure 4: Encryption/ decryption module

The encryption process is illustrated in following steps:

- Start
- Encrypt the data file using Vigenere encryption algorithm. The key for encrypting data file is of variable length depending on the size of data file. This increase the key retrieval complexity for intruders as for every file there is different sized key. This key is generated by key generator of data file sized.
- The encrypted data file is again encrypted using secret key generated in above stage i.e. stage II by AES-256 algorithm. Decryption process is just reversal of this stage.

File Retrieval Process

File retrieval process is also termed as decryption of data file from cloud data center. When a user wants to access his data file that is saved at data center, then first of all he has to authenticate himself at authority server.

For this he has to send hash value of password, user ID and Server ID. Authority server also asks server to send hash value of password User ID and server ID.

After authentication of user the server generates the encrypted key that is again used for decrypting the data file. Then Vigenere encryption and AES algorithm is used to decrypt the data file from the data center. In this way whole process of file retrieval is proceeded.

Experimental Parameters And Result Analysis

The experiments are done are done under following system parameters such as Intel core i5, 240GHz, 4GB RAM, Java and Simulation using cloudsim.

For evaluation of performance of proposed algorithm the parameters or criteria is to be determined to analyze or test its efficiency. Since, the features or matrices related to security to determine their strength against cryptographic attacks is discussed. Here the key size and execution time are the preferred factors to analyze the performance of the proposed algorithm to encrypt/decrypt data blocks of various sizes.

The proposed algorithm is to be evaluated in terms of the execution time required to encrypt and decrypt the data files. All the implementations are simulated to make sure that the results are fair, accurate and efficient.

Evaluation of Execution Time

The total time taken by a process to encrypt data files i.e. convert plain text into cipher text is called encryption time or cipher text to plain text is called decryption time.

Table 1. Encryption Time Analysis

File Size	Existing Algorithm	Proposed Algorithm
100 KB	1.3 sec	0.39 sec
200 KB	2.8 sec	0.421 sec
400 KB	5.1 sec	0.577 sec
800 KB	7.9 sec	0.936 sec
1 MB	5 sec	1.217 sec
2MB	12 sec	2.98 sec
4MB	23 sec	10.436 sec
8MB	46 sec	33.494 sec

The table I shows the execution time observation of encryption process of existing and proposed algorithm. Execution process is evaluated using different file size such as 100 KB, 200KB, 400 KB, 800 KB, 1MB, 2MB, 4MB and 8MB.

After analyzing all data files on both existing and proposed algorithm, it is concluded that as data file size increases, execution time for encryption process increases. But it is also observed that as file size increases, the execution time for encryption process in existing technique increases approx. twice than proposed algorithm.

Figure 5 is showing the analysis of encryption time of proposed algorithm as compared with existing algorithm.

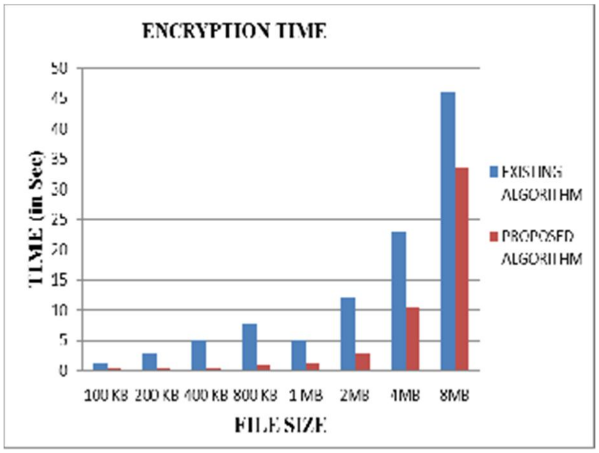

Figure 5: Analysis of Encryption Time

Table 2 is showing the analysis of decryption time of proposed algorithm as compared with existing algorithms.

Table 2. Decryption Time Analysis

File Size	**Existing Algorithm**	**Proposed Algorithm**
100 KB	1.2 sec	0.062 sec
200 KB	2.7 sec	0.109 sec
400 KB	5 sec	0.249 sec
800 KB	7.8 sec	0.624 sec
1 MB	7.5 sec	0.921 sec
2MB	16.5 sec	2.714 sec
4MB	33.5 sec	10.499 sec
8MB	40 sec	33.883 sec

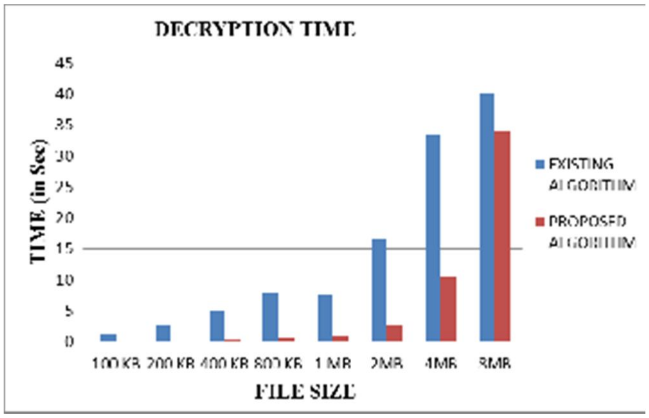

Figure 6: Analysis of Decryption Time

Decryption process is evaluated using different file size such as 100 KB, 200KB, 400 KB, 800 KB, 1MB, 2MB, 4MB and 8MB, in figure 6.

After analyzing all data files on both existing and proposed algorithm, it is concluded that as data file size increases, execution time for decryption process increases. But it is also observed that as file size increases, the execution time for decryption process in existing technique increases approx. twice than proposed algorithm.

Conclusion

Presented research work focused on the cloud data protection or security at cloud end. To make sure data protection or security of cloud data storage at cloud end, security architecture is designed that secures the data using encryption/decryption algorithm where the proposed algorithm is a hybrid encryption algorithm that uses the concept of ID based cryptography, Vigenere algorithm and AES algorithm along with SHA-512 for authentication purpose. Presented experiment results show that the proposed concept is reasonable, it enhancing efficiency about 65% in terms of execution time i.e. encryption as well as decryption time and security and providing confidentiality of cloud data at could end. This paper also uses the concept of authentication of the user by the concept of SHA-512. The proposed method provides a secure framework for confidentiality of text information at cloud storage data that can be useful in a number of applications at cloud end. Benefits to the proposed technique include the simplicity and confidentiality. A future improvement to the method could be a mechanism to process secure data sharing among different cloud users.

References

[1] P. Mell and T. Grance, “The nist definition of cloud computing”, US Department of Commerce, Gaithersburg, MD, 2011.

[2] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, “NIST Cloud Computing Reference Architecture” US Department of Commerce, Gaithersburg, MD, 2011.

[3] Rajkumar Buyya, Karthik Sukumar, “Platforms for Building and Deploying Applications for Cloud Computing”, CSI Communications, 2011.

[4] Mohammad Sajid, Zahid Raza, “Cloud Computing: Issues & Challenges”, International Conference on Cloud, Big Data and Trust, 2013.

[5] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, Springer, 2013.

[6] William stalling, “Cryptography and Network Security”, Pearson, Fourth Edition, 2006.

[7] From Wikipedia http://en.wikipedia.org/wiki/Cryptography.

[8] Shivani Gambhir, Ajay Rawat, Rama Sushil, “Cloud Auditing: Privacy Preserving using Fully Homomorphic Encryption in TPA”, International Journal of Computer Applications, 2013.

[9] A. Sahai and B. Waters, Fuzzy identity based encryption, in Proc. Advances in Cryptology-Eurocrypt, 2005, pp. 457–473.

[10] A. Shamir, Identity-based cryptosystems and signature schemes, in Advances in Cryptology, G. R. Blakley and D. Chaum, eds. Springer Berlin Heidelberg, 1985.

[11] Bhaskar Prashad Rimal, Eunmi Choi, Ian Lumb, “A Taxonomy And Survey Of Cloud Computing System”, IEEE 2009.

[12] Sherif El-etriby, Eman M. Mohamed, “Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing”, ICCIT 2012.

[13] Shuaishuai Zhu , Xiaoyuan Yang, Xuguang Wu “Secure Cloud File System with Attribute Based Encryption” IEEE International Conference on Intelligent Networking and Collaborative Systems, 2013.

[14] Sengupta N., Holmes J. “Designing of Cryptography Based Security System for Cloud Computing” International conferences on Cloud & Ubiquitous Computing & Emerging Technologies, IEEE, 2013.

[15] Chao Yang , Weiwei Lin, Mingqi Liu “A Novel Triple Encryption Scheme for Hadoop-Based Cloud Data Security” IEEE International Conference on Emerging Intelligent Data and Web Technologies, 2013.

[16] Faraz Fatemi Moghaddam, Maen T. Alrashdan, and Omidreza Karimi ”A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments” Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013.

[17] V.S. Mahalle , A. K. Shahade, “Enhancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm”, IEEE , 2014, pp.46-149.

[18] Preeti Garg, Dr. Vineet Shanna, “An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function”, IEEE 2014.

[19] Keke Gai, Meikang Qiu, Hui Zhao, Jian Xiong, “Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing”, International Conference on Cyber Security and Cloud Computing, IEEE, 2016. pp. 273-278.

[20] Nazatul Haque Sultan & Ferdous Ahmed Barbhuiya, “A Secure Re-Encryption Scheme for Data Sharing in Unreliable Cloud Environment”, IEEE 2016, PP. 75-80.

[21] G.Prabu kanna and V.Vasudevan, “Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud”, IEEE 2016, pp.3688-3693.

[22] Bhale Pradeepkumar Gajendra, Vinay Kumar Singh, More Sujeet , “Achieving Cloud Security using Third Party Auditor, MD5 and Identity-Based Encryption”, International Conference on Computing, Communication and Automation, IEEE 2016, pp.1304-1309.

[23] Punam V. Maitri, Aruna Verma, “Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm”, IEEE, 2016, pp. 1635-1638.

[24] Bhathiya Wickremasinghe, Rodrigo N. Calheiros, and Rajkumar Buyya, “CloudAnalyst: A CloudSim-based Visual Modeller for Analysing Cloud Computing Environments and Applications”.

[25] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, C´esar A. F. De Rose and Rajkumar Buyya, “CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms”, Wiley Online Library, 2010.