Design and Implementation of an Algorithm to Enhance Cloud Security

Aayushi Priya
Department of C.S.E
Radharaman Engineering College
Bhopal, (M.P.)

Y.K. Rana
Department of C.S.E
Radharaman Engineering College
Bhopal, (M.P.)

B.P. Patel
Department of C.S.E
Radharaman Engineering College
Bhopal, (M.P.)

ABSTRACT

Cloud computing concept has been envisioned as architecture of the next generation for Information Technology (IT) enterprise. The Cloud computing idea offers with dynamic scalable resources provisioned as examine on the Internet. It allows access to remote computing services and users only have to pay for what they want to use, when they want to use it. But the security of the information which is stored in the cloud is the major issue for a cloud user. Cloud computing has been flourishing in past years because of its ability to provide users with on-demand, flexible, reliable, and low-cost services. With more and more cloud applications being available, data security becomes an important issue to the cloud. In order to make sure security of the information at cloud data storage end, a design and implementation of an algorithm to enhance cloud security is proposed. With a concept, where the proposed algorithm (PA) combines features of two other existing algorithms named Ceaser cipher and Attribute based cryptography (ABC). In this research work, text information are encrypting using "Caesar Cipher" then produced cipher text again encrypted by using proposed algorithm (PA) with the help of private key of 128 bits. And in the last step of encryption process, based on ABC, attribute related to cipher text is stored along with cipher text generated after encryption which provide two-step authentication during decryption process. A security approach is designed and developed for data security concept regarding higher confidentiality and authenticity for the cloud data at cloud storage end with experiment analysis to authenticate its efficiency. From the result analysis it is clearly seen that the proposed technique has better Avalanche Effect and execution time than existing technique and hence can be incorporated in the process of encryption/decryption of any plain text or on any key value.

Keywords

Cloud Computing, Cryptography, Encryption, Decryption, Security issues, Confidentiality, Authentication.

1. INTRODUCTION

Cloud computing is a concept of evolving large number of computers connected, virtualized and organized in terms of portable workloads. Cloud computing is an application and service that run on a distributed network using virtualized resources and accessed by common Internet networking protocols and networking standards.

Cloud = abstraction + virtualization

It abstracts details of system implementation from users and developers i.e. applications runs on physical system is not specified data stored in location is unknown administration of system is outsourced to other. Example: AZURE Platform, AMAZON services, GOOGLE etc.

Virtualization is applied in cloud model to virtualizes system by pooling & sharing resources. Cloud computing is the computation of various resources which delivers the resources across the network (Internet). Instead of maintaining data on self or updating the application desires in our self can be done around the network (Internet) also [1,2]. At remote locations it allows the user (individuals) and organization to use the software and hardware, which is managed by the third parties. This type of network is called "cloud". Resources in cloud can be extended unlimitedly, got anytime and used on-demand. It with dynamism delivers the whole thing as a service on the internet based on demand of the user, such as operating system, network, hardware, software, resources and storage. The degree of acceptance for any computing paradigm is measured by its strengths and weaknesses [3]. Architecture of cloud comprised of characteristics, delivery model and deployment model. Various Characteristics of Cloud Computing [1,4] are on demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Delivery Methods of Cloud Computing [1,4] are:
Software-As-a-Service (SaaS) in which software is provided as a service to the user. Example: Gmail, Google Drive, DropBox etc. Platform-As-a-Service (PaaS) in which cloud provides a platform or environment to the user for their applications over Internet. Example: Google Gears, Microsoft Azure. Infrastructure-As-a-Service (IaaS) in which cloud service provider delivers computing, storage and networking capabilities to the user. A virtual version of infrastructure is given to user but actual physical infrastructure is handled by service providers at remote locations. Example: Amazon Web Services, Google's Compute Engine.

Deployment Models of Cloud Computing [1,4] are:
Private Cloud is owned and used for particular organization that controls the virtualized resources. Public Cloud is owned and delivered for general public use by a particular organization or company to offer access to computing resources at minimal cost. Community Cloud is shared through various organizations or company. Hybrid cloud mean more than two cloud form a single cloud.

In Cloud computing environment, there are set issues [5] such as privacy, security, performance, load balancing and reliability. The most important of these issues is the data security [6,7]. Secure cloud architectures [8] are proposed to enhance the data security at cloud end. Most effective technique to protect our data is cryptography. Different encryption schemes [9] for protection of data have been in use for many decades.

The paper has the following structure, section 2: related work, section 3: proposed methodology, section 4: results and section 5: conclusion.

2. RELATED WORKS

In recent years, security issues related to cloud computing has been widely studied. In order to realize secure data storage at cloud end several mechanisms are proposed. Various existing studies on cloud security and approach used to overcome issues related to the security of data is illustrated in Table 1.

To facilitate our proposed work following algorithms used in cloud security is briefly introduced.

2.1 Modern Cryptography

Modern Encryption algorithms, such as RC6, AES, DES, 3DES and Blow-Fish still play a vital role in data security of cloud computing. The evaluation has been performed for those encryption algorithms according to randomness testing by using NIST statistical testing in cloud computing environment (Amazon EC2) [9].

2.2 Searchable Encryption

Searchable encryption is a form of encryption that deals with search or retrieve of data in encrypted data, without having to decrypt all the data. Cloud secure architecture [10, 11] by using encryption/searchable encryption technologies allows the search process in the form of encrypted data and the retrieval of data in a safe manner.

2.3 Homomorphic Encryption

Homomorphic encryption [12, 13] 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.

2.4 Attribute based Encryption

Attribute-based encryption (ABE) [14] is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. There are two kinds of ABE schemes: key-policy ABE and ciphertext-policy ABE.

2.5 Hybrid Encryption

Hybrid encryption [15,16] is a mode of encryption that merges two or more encryption systems to benefits from strengths of each form of encryption.

Table 1. Various existing cryptographic techniques in cloud

Author name	Problems	Approach Used	Conclusion
Preeti Garg et al.[17]	Confidentiality and Integrity of data	RSA with Hash function is used.	Maintains confidentiality and correctness of data at cloud.
Neha Tirthani et al.[18]	Confidentiality and authenticity	Elliptic curve cryptography for data encryption and Diffie-Hellman Key Exchange mechanism for connection establishment	Provides authenticity and confidentiality and computation cost is less.
Shuaishuai Zhu et al.[14]	Secure File sharing in cloud, confidentiality, authenticity	Attribute based encryption used for secure file sharing.	More authentic method for file sharing in cloud.
Sengupta N. et.al[16]	Confidentiality	Hybrid cryptography system using Caesar cipher and Vigenere encryption is used.	Enhances Confidentiality
Chao Yang et al.[15]	Confidentiality and secure key exchange	Hybrid triple encryption algorithm using DES, RSA and IDEA.	Enhances Confidentiality

3. PROPOSED METHODOLOGY

As more and more organizations and individuals tend to outsource their data to cloud storage, the security and user privacy protection attract more attention. Encryption and decryption of data files are primarily user-centric, that only legitimate users are allowed to upload and download files, and specify whether a file can be shared to other users. There are two ends while we talk about the security of the data in a cloud environment. In the first end, the security of the data may concern while data is moving into the network after taking data from the user site through the any web based application. And in the second end the security concern could be at Cloud end when data is already through network and about to store in cloud disk. The main motive of the proposed work is the second concern which is security concern of the data file at the Cloud End while data is getting stored in cloud disk. In order to keep securities at cloud storage researchers have given following skeleton of the proposed work which is hybrid in nature containing three stages.

As shown in Fig 1, in first stage Ceaser Ciphering technique [13] is used which provides initial level security and at the same time it provides more efficiency, undoubtedly. In the second level of proposed work deals with new designed encryption algorithm which is based on the symmetric cryptographic concept (block based). This work uses 128-bit block size for the encryption purpose and this 128-bits block size provides more security level and at the same time this 128-bits block size is encrypted with the help of the encrypted key which size is also 128-bits. Encrypted key is generated by applying XOR operation over private key of user and secret key of the cloud. 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. So, the third stage of the newly proposed work gives concentration on authentication of the cloud user by the means of the Attribute Based Cryptography (ABC) techniques. Through this technique, algorithm generates an attribute related to ciphertext and based on this attribute authentication of the user requisite is handled. If user satisfies this condition then newly proposed Cloud based Security checks for the key too.

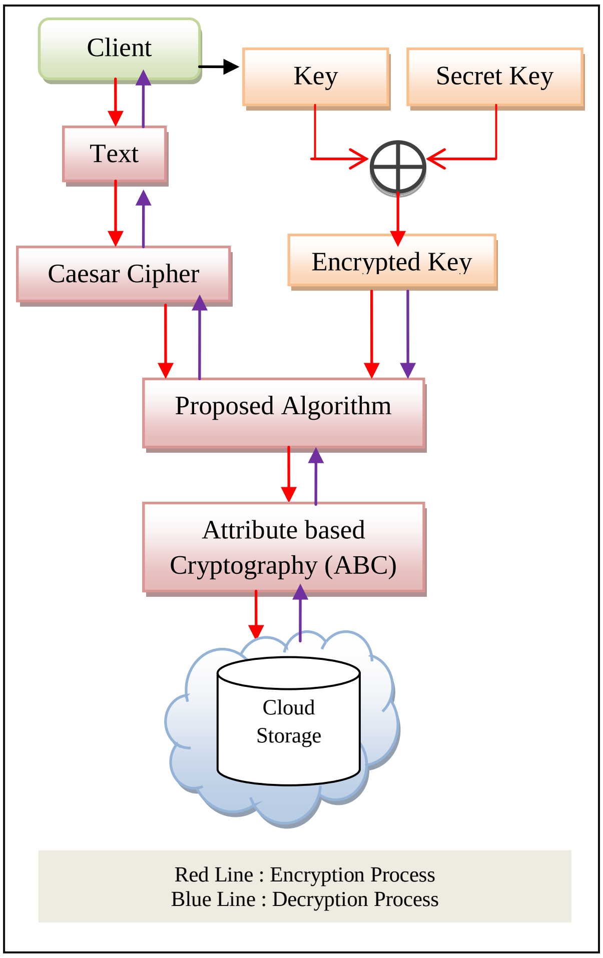

Client
Key
Secret Key
Text
Caesar Cipher
Encrypted Key
Proposed Algorithm
Attribute based Cryptography (ABC)
Cloud Storage
Red Line : Encryption Process
Blue Line : Decryption Process

Fig 1: Block diagram of proposed concept

3.1 Some Definitions

K < --- *Private key given by user.*

SK < --- Gen(s): *is a key generator that takes input key size 's' and generates output secret key 'SK' of size 's'.*

CT_1 := Cae(T, 5): *an algorithm that takes text 'T' as an input and encrypt with shift of 5 characters and generates ciphertext* CT_1.

EK := En (K, SK)*: an algorithm that encrypt K with SK and generates encrypted key EK.*

CT_2 := PAE(CT_1, EK): *an algorithm that takes input cipher text 'CT_1' and encrypt it with EK and generates output ciphertext 'CT_2'.*

α := ABC(CT_2, K): *an algorithm that takes CT_2 and K as an input and generates an attribute α.*

CT_1' := PAD(CT_2, EK): *an algorithm that takes input cipher text 'CT_2' and decrypt it with EK and generates output ciphertext CT_1' such that CT_1' == CT_1.*

T' := Cad(CT_1', 5): *an algorithm that takes text CT_1' as an input and encrypt with reverse shift of 5 characters and generates T' such that T' == T.*

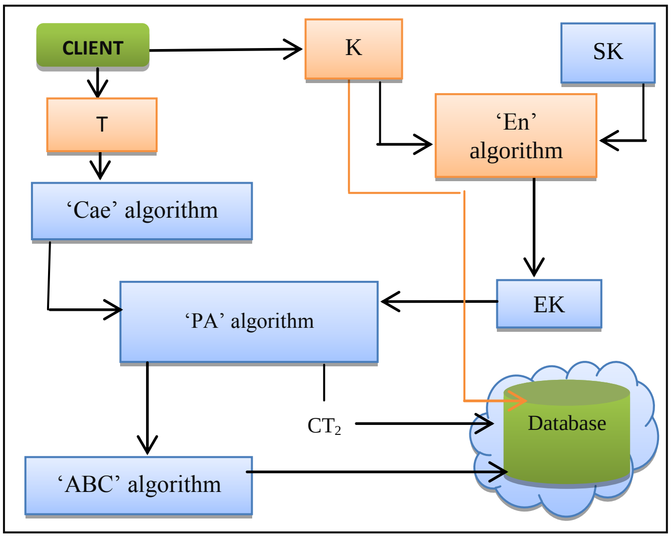


Fig 2: Encryption while storing data

3.2 Storing Process (Fig 2)

Storing or encryption process of text data is performed as shown in Fig. 2 where, CT2 = T(Cae, PAE, ABC), ciphertext is generated by applying algorithms Cae, PAE, ABC over text and stored at cloud storage. Detailed steps of encryption process is described below:

Step 1: Start

Step 2: Insert text data (T) and private key (128-bits) (K) by Cloud User.

Step 3: User text data (T) and key (K) reach at Cloud Server End.

Step 4: Read User text data and key (128-bits) at Cloud End.

Step 5: Apply algorithm 'Cae' to T.

Step 6: Produce Initial level cipher text CT_1.

Step 7: Prepare Encrypted key (EK)

Step 7.1 : Generate SK using algorithm 'Gen'.

Step 7.2: Apply algorithm 'En' to generate EK.

Step 8: Pass CT_1 and EK to next level algorithm.

Step 9: Produce Second Level of cipher text CT_2 by applying algorithm 'PAE'.

Step 10: Pass CT_2 to algorithm 'ABC' to generate an attribute 'α'.

Step 10: Stop

3.2.1 Proposed Encryption Algorithm Step (Fig 3):

Note: CT_1 = Cipher Text generated after level 1 encryption, EK = Encrypted Key, L = Left part of CT_1, R = Right part of CT_1, ${}^1K_{64}$ & ${}^2K_{64}$ = Sub-Keys of EK , CT2 = Cipher Text generated after level 2 encryption.

Step 1: Input CT_1 & EK

Step 2: Divide CT_1 = L & R

Step 3: Divide EK = ${}^1K_{64}$ & ${}^2K_{64}$

Step 4: L>>r -----> L (2-bit Right Circular shift)

Step 5: L $\oplus$ R -----> L (XOR operation)

Step 6: R>>r -----> R (2-bit Right Circular shift)

Step 7: Swap L & R

Step 8: L $\oplus$ $^1K_{64}$ -----> L

Step 9: L << l -----> L (2-bit Left Circular shift)

Step 10: L $\oplus$ R -----> R

Step 11: R << l -----> R (2-bit Right Circular shift)

Step 12: Swap L & R

Step 13: L $\oplus$ $^2K_{64}$-----> L

Step 14: Repeat step 4 to 13 up to 10 rounds

Step 15: CL + CR = CT2

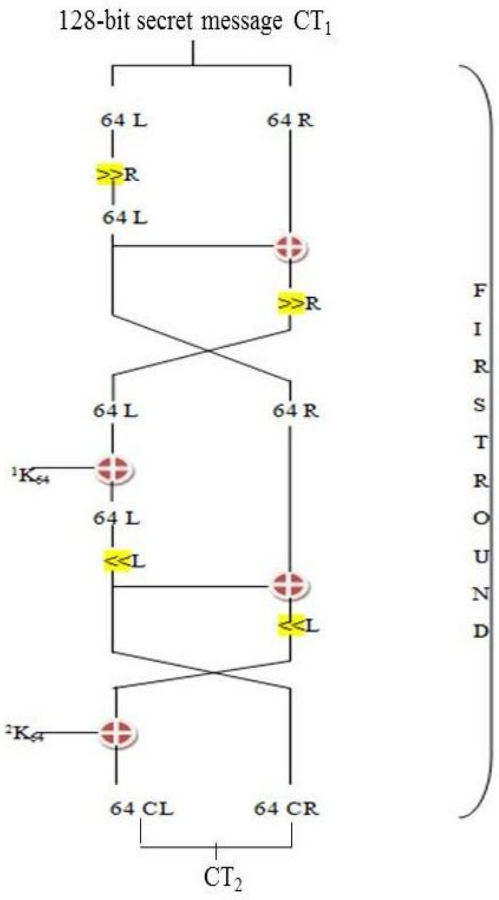


Fig 3: Architecture of Proposed Encryption

3.3 Retrieving Process(Fig 4):

Retrieving and decryption process of text data is performed as shown in Fig.4 where, T = CT_2 (ABC, PAD, Cad), text is generated by applying algorithms ABC, PAD, Cad over ciphertext retrieved cloud storage. Detailed steps of decryption process is described below:

Step 1: Start

Step 2: Enter 'K' and 'α'. (for the authentication of the user) by Cloud User.

Step3 : User key 'K' and 'α' reach at Cloud Server End.

Step 4: Check Authentication

Step 4.1: By matching 'K' and 'α' at the cloud storage.

Step 4.2: If user gets authenticated at step 4.1, then cloud security system goes next step.

Otherwise

Cloud Security system disallows the user to get accessing rights to the file.

Step 5: Prepare EK by applying algorithm 'En'.

Step 6: Pass EK and CT2 to algorithm 'PAD'.

Step 7: Generate initial level cipher text, CT_1' such that,

CT_1' == CT_1.

Step 8: Pass CT_1' to 'Cad' algorithm.

Step 9: Generate user Text data, T' such that T' == T.

Step 10: Send User text back to user at the user end (at another end of cloud environment).

Step 11: Stop

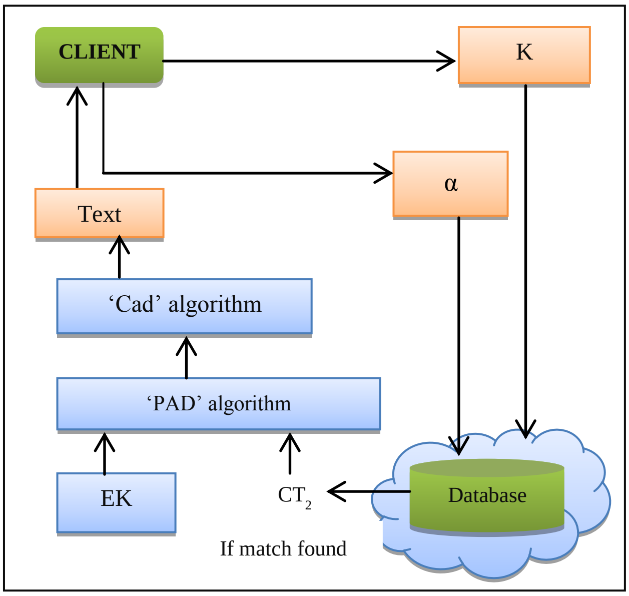


Fig 4: Decryption process while retrieving data

3.3.1 Proposed Decryption Algorithm Step (Fig 5):

Note: CT_2 = Cipher Text retrieved from database, EK = Encrypted Key, CL = Left part of CT_2, CR = Right part of CT_2, $^1K_{64}$ & $^2K_{64}$ = Sub-Keys of EK , CT_1' = Cipher Text generated after completion of decryption process of PAD algorithm.

Step 1: Input CT_2 & EK

Step 2: Divide CT_2 = CL & CR

Step 3: Divide EK = $^1K_{64}$ & $^2K_{64}$

Step 4: CL $\oplus$ $^2K_{64}$ -----> CL (XOR operation)

Step 5: Swap CL & CR

Step 6: CR >> R -----> CR (2-bit Right circular shift)

Step 7: CL $\oplus$ CR -----> CR

Step 8: CL >> R -----> CL (2-bit Right circular shift)

Step 9: CL $\oplus$ $^{1}K_{64}$ -----> CL

Step 10: Swap CL & CR

Step 11: CR <<L -----> CR (2-bit Left circular shift)

Step 12: CL $\oplus$ CR -----> CR

Step 13: CL << L -----> CL (2-bit Left circular shift)

Step 14: Repeat step 4 to 13 up to 10 rounds

Step 15: CL + CR -----> CT_1’

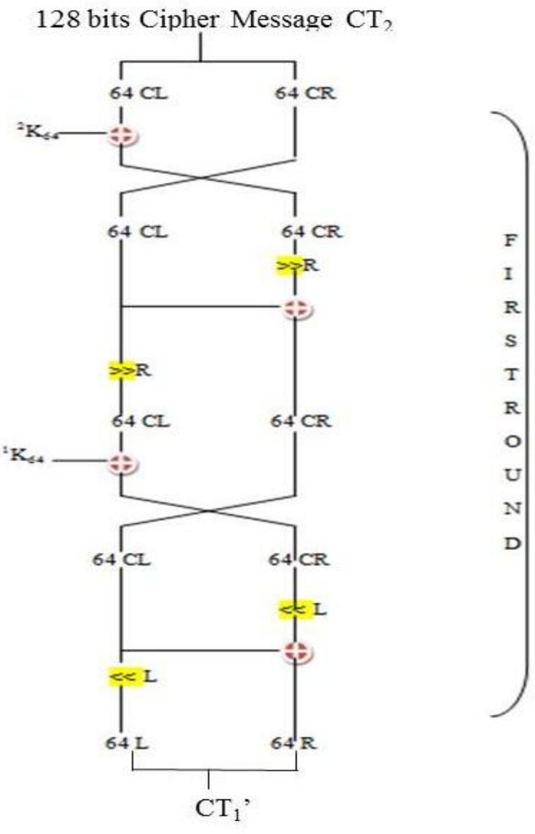


Fig 5: Architecture of Proposed Decryption

3.4 Main Features of Proposed Work

- Three Level Security Concept
- Key Generator Concept
- Block Ciphering with Encrypted Key Concept
- Confidentiality of text data with Authentication of the user
- Easy to understand.
- Robustness.
- Low Execution Time

4. RESULTS

4.1 Performance Evaluation Methodology

This section comprises with an analytical and numerical description of proposed triad security algorithm for cloud computing environment by simulations to obtain the performance of the algorithm. In addition to that, this section discusses parameters related to the methodology such as system parameters, experiment factors, and simulation constraints.

4.1.1 System Parameters

The experiments are done in Intel core i5, 240 GHz, 4GB RAM and simulated using cloudsim. Further consistency guarantee of proposed system, a number of retakes experimentally performed repeatedly to observe and assure its importance.

4.1.2 Experiment Factors

For evaluation of performance of proposed triad 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 discoursed. The factors preferred here is to conclude the performance of the proposed algorithm is execution time and key size to encrypt/decrypt data blocks of various sizes.

4.1.3 Simulation Constraints

By applying test data the proposed algorithms is evaluated in terms of the execution time required to store or retrieve the data blocks at cloud storage. All the implementations were exact to make sure that the results will be efficient relatively. The Simulation program accepts inputs: Algorithm and data block. After a successful execution i.e. encryption and decryption produce an efficient result. A analytical table is made after the successful encryption/decryption process to make sure that all the data are processed in the right way. Practically, based on three parameters we can say that our proposed work is better and these parameters are:

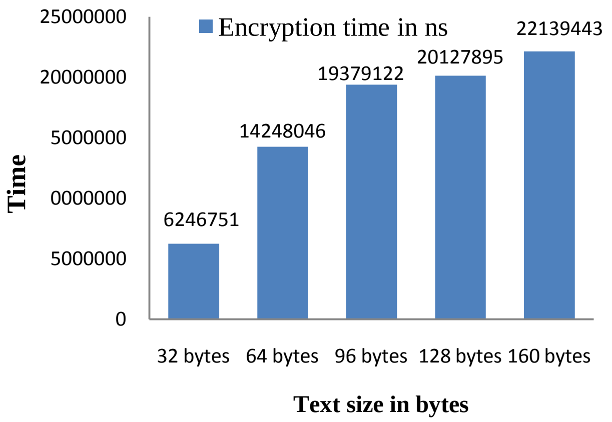
- Execution time
  - Encryption Time
  - Decryption Time
- Key Analysis
- Avalanche effect

4.2 Execution Time

The total time taken by a process to convert plain text into cipher text is called encryption time or cipher text to plain text is called decryption time. Table 2 and Graph 1 is showing the analysis of encryption time of proposed work and Table 3 and Graph 2 is showing the analysis of decryption time of proposed work.

Table 2. Encryption time analysis

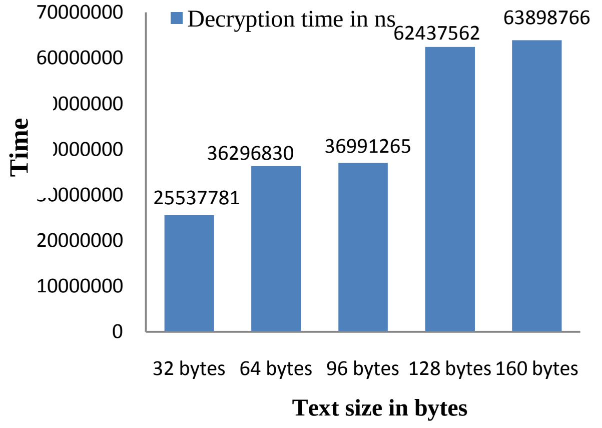
Size	Proposed Work
32 Bytes(16 Char)	6246751
64 Bytes(32 Char)	14248046
96 Bytes(48 Char)	19379122
128 Bytes(64 Char)	20127895
160 Bytes(80 Char)	22139443



Graph1. Encryption time analysis

Table 3. Decryption time analysis

Size	Proposed Work
32 Bytes(16 Char)	25537781
64 Bytes(32 Char)	36296830
96 Bytes(48 Char)	36991265
128 Bytes(64 Char)	62437562
160 Bytes(80 Char)	63898766



Graph 2. Decryption time analysis

4.3 Key Analysis

Proposed algorithm uses 128 bits key (EK) generated two other keys (i.e. K and CSK) which are used to encrypt and decrypt of secret data. According to brute force attack combination required to break the key it needs 2^{128} combination. It is near to impossible to calculate this value even from supercomputer. Hence it can be say that it is highly secure against brute force attack.

4.4 Avalanche Effect

In cryptography, the avalanche effect [19] is a most impressive property for block ciphering and hash function algorithms. The avalanche effect circumstance is fulfilled in following conditions:

- If the output changes considerably (e.g., half the output bits flip) causes a minor change in input (e.g., flipping a single bit).
- In block ciphers, such a small change in either the key or the plaintext should grounds to a strong change in the cipher text.

The above conditions of avalanche effect allow small changes to propagate rapidly through iterations of the algorithm, in such a way that every bit of the output should depend on every bit of the input before the algorithm terminates.

Avalanche Effect Formula is given below:

$$\text{Avalanche Effect} = \frac{\text{Number of change bits in cipher text}}{\text{Number of bits in cipher text}}$$

Table 4. Avalanche effect analysis various input text

S.No.	Avalanche Effect	
	Input Text	**Proposed (No. of bits changed)**
1	testing of security	96
2	testing of security is	93
3	testing of security is basic	90
4	Basic of testing of security	120
5	How testing of security	98
for key=showtime/showtima		

From the above results analysis it can clearly see that the proposed technique has better Avalanche Effect (discussed in Table 4) and encryption/decryption time than existing technique and hence can be incorporated in the process of encryption/decryption of any plain text or on any key value. Also, however it is also clear from above discussion that, by applying proposed technique to the text of different sizes high bit difference is obtained as compare to different other existing. Similarly terms of execution time (Encryption Time as well as Decryption Time) of the proposed technique have very low as compared to existing technique.

5. 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 or to enhance cloud security a design of an algorithm is proposed and implemented with a concept where proposed algorithm is combined with two other encryption schemes named caser cipher and ABC attribute. Presented experiment results show that the proposed concept is reasonable, it enhancing efficiency in terms of execution time and security and providing confidentiality of cloud data at could end. In this research work the concept of proposed technique including the various encryption schemes of system based on the various type of key and proposed encryption algorithms. The proposed technique provides a framework for confidentiality of text information in cloud storage data at cloud environment that can be useful in various applications which is required for storage of data at cloud end. Benefits to the proposed technique include the simplicity and confidentiality. The security analysis shows that the produced avalanche effect strengthen the proposed technique which is based on the "proposed algorithm". Future work can present an enhancement of proposed algorithm which should focus on the random-generation capability of key with the key exchange process and also enhance the file sharing features of proposed algorithm based on attributes.

6. REFERENCES

[1] 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.

[2] P. Mell and T. Grance, "The nist definition of cloud computing", special publication 800-145," US Department of Commerce, Gaithersburg, MD, 2011.

[3] Bhaskar Prashad Rimal, Eunmi choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing System", International Joint Conference on INC, IMS and IDC, IEEE, 2009.

[4] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya, "Service-Oriented Cloud Computing Architecture", Seventh International Conference on Information Technology, IEEE 2010.

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

[6] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", IEEE, 2010.

[7] 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.

[8] Sanjay Dahal, "Security Architecture For Cloud Computing Platform", 2012.

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

[10] Hamdan M. Al-Sabri, Saleh M. Al-Saleem "Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security" IJCSI International Journal of Computer Science Issues, Volume 10, Issue 2, 2013.

[11] Mao-Pang Pang Lin, Trend Micro, Taiwan, Wei-Chih Hong, Chih-Hung Chen, Chen-Mou Cheng "Design and Implementation of Multi-user Secure Indices for Encrypted Cloud Storage" International Conference on Privacy, Security and Trust, IEEE, 2013.

[12] Shivani Gambhir, Ajay Rawat, Rama Sushil, "Cloud Auditing: Privacy Preserving using Fully Homomorphic Encryption in TPA", International Journal of Computer Applications, Volume 80, Number 14, 2013.

[13] Cong Wang, S.-M. Chow, Qian Wang, Kui Ren , Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Cloud Computing, Volume 62, Issue 2, 2013.

[14] Shuaishuai Zhu ; Xiaoyuan Yang ; Xuguang Wu "Secure Cloud File System with Attribute Based Encryption" IEEE International Conference on Intelligent Networking and Collaborative Systems, 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] Sengupta, N., Holmes J. "Designing of Cryptography Based Security System for Cloud Computing" IEEE International conferences on Cloud & Ubiquitous Computing & Emerging Technologies, 2013.

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

[18] Neha Tirthani, Ganesan R "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography".

[19] Ganesh Patidar, Nitin Agrawal, Sitendra Tarmakar, "A block based Encryption Model to improve Avalanche Effect for data Security", International Journal of Scientific and Research Publications, Volume 3, Issue 1, 2013.