An Enhanced Cryptographic Scheme for Data Security in the Cloud

Mrs. R Geetha, Assistant Professor, EPCET,Bangalore,India,geetha2312@gmail.com

Abstract- One of the primary usage of cloud computing is data storage. Cloud provides huge capacity of storage for users. Benefits of cloud storage are easy access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. Because of these benefits each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. To store and retrieve their data at anytime or anywhere it should be reliable and flexible. In the present day, security is the major goal in all applications. For securing data in cloud computing there are lot of techniques available. In this research work, we try to present a fair comparison of different parameters between the existing cryptographic algorithms such as DES, blowfish, Rivest Cipher 4, etc, and analyze the time taken for encryption for different file sizes and then develop a symmetric cryptographic algorithm for encryption for data in the cloud that is reliable and eliminates many of the attacks that can occur. Comparison of the experimental results shall be carried out over different data types like plain text, document files, of text, audio and video data. In this research, the proposed work plan is to eliminate the concerns regarding data privacy using symmetric algorithms to enhance the security in cloud as per different perspective of cloud customers.

***Keywords* —Cloud Computing, Cryptographic algorithms, Encryption, Cloud**

I. INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available.

Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Because of these benefits each and every organizations are moving their data to the cloud. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

Cloud is basically the collection of computers on the internet that companies are using to offer their services. One cloud service that is being offered is a revolutionary storage method for your data. From music files to pictures to sensitive documents, the cloud invisibly backs up your files and folders and alleviates the potentially endless and costly search for extra storage space. An alternative to buying an external hard drive or deleting old files to make room for new ones, cloud storage is convenient and cost-effective.

It works by storing your files on a server out in the internet somewhere rather than on your local hard drive. This allows us to back up, sync and access our data across multiple devices as long as they have internet capability. However, if you wish to store information virtually, you must consider

 DOI : 10.18231/2454-9150.2019.0598

the added risk that your information may be accessible to others potentially people who you do not wish to have access. Below, we outline a few security risks to take into account and how to protect yourself and your data. Encryption algorithm plays an important role for information security. In Fig 1 Encryption is the process of transforming plain text data into the cipher text (secure data) in order to reveal its meaning. Decryption is the reverse of the Encryption process in which we retrieve the original plain text from the cipher text.

There are many Encryption algorithms which are developed and are used for information security. They are categorized into mainly two types depending upon the type of security keys. The two categories are symmetric and asymmetric encryptions. In symmetric or private encryption only one key is used to encrypt or decrypt the data. Strength of the symmetric encryption depends upon the size of the key. For the same algorithm, encryption using the longer key is tough to break than one using smaller key. In a symmetric or public encryption two keys are used, one is used to encrypt and other is used to decrypt the data.

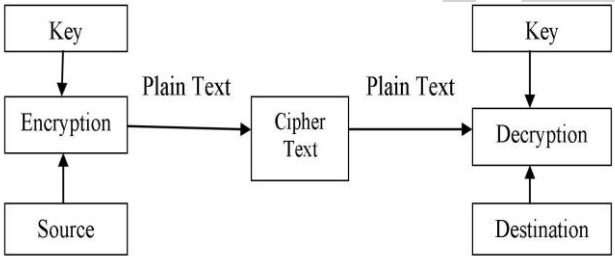

Fig. 1. Encryption and Decryption Process

II. PROBLEM STATEMENT

- A number of researchers have discussed the security challenges that are raised by cloud computing. It is clear that the security issue has played the most important role in hindering the acceptance of Cloud Computing.
- For securing data in cloud computing there are lot of techniques available. Various disadvantages in cloud are security, data protection, network security, privacy concerns and are also prone to a variety of attacks like Denial of Service, IP spoofing, etc.
- Without strong encryption and unique credentials, files can be vulnerable in the cloud, but there are also risks during data transmission.
- Keys should also be securely escrowed, and difficult to retrieve, so that no outside party can obtain that key to access your data.

For security purpose of cloud storage various encryption techniques are being analyzed by researchers. As discussed in survey there are many security techniques which are currently applied to cloud storage. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the cloud storage.

III. LITERATURE SURVEY

Cloud computing has been defined by US National Institute of Standards and Technology (NIST) [1] as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction .

Brian Hay et. al [2] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data.

Kevin Curran et.al [3] mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems by storing their data in Cloud Storage they will be faced with the task of seriously reassessing their current security strategy.

A. SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS

In the recent years, there has been a great need for much improved techniques of securely transmitting and storing information. The field of cryptography encompasses some of these requirements and has been focus of a growing research effort. The core of this field is the efficient realization of cryptography algorithms in software and/or hardware. The introduction of such algorithms started at the 70‟s. Some commonly used symmetric key encryption algorithms are described as:

- ***Data Encryption Standard (DES):*** DES was the result of a research project set up by International Business Machines (IBM) Corporation in the late 1960‟s which resulted in a cipher known as LUCIFER. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and R i which are then passed into 16 rounds (the subscript i in Li and Ri indicates the current round). Each of the rounds is identical and the effects of increasing their number are twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number

 DOI : 10.18231/2454-9150.2019.0598

chosen was 16, probably to guarantee the elimination of any correlation between the cipher text and either the plaintext or key. At the end of the 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text. [4][5].

- ***Advanced Encryption Standard (AES):*** AES emerged as a powerful replacement of DES during a competition held by National Institute of Standard and Technology (NIST). The competition was organized to develop a substitute of existing DES. Rijndael: an algorithm designed by Daemen and Rijmen was judged the best and announced to be new AES. NIST choose Rijndael, due to its simplicity and high performance. It is fast, compact, and has a very simple mathematical structure [4] AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively.[4][5] Triple Data Encryption Standard (3DES): In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks. Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryptor, we simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three subkeys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key [4].
- ***Blowfish***: Blowfish is block cipher 64-bit block that can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all users. Blowfish has variants of 14 rounds or less.

Blowfish [6] is a symmetric block encryption algorithm designed in consideration with, • Fast: It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.

- Compact: It can run in less than 5K of memory.
- Simple: It uses addition, XOR, lookup table with 32-bit operands.
- Secure: The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length

As per given paper [7], the author focus on cloud security using blowfish algorithm. They provide data security and data protecting using various channels. Author confirmed that proposed approach performs better in decreasing the safety threat on cloud.

In this paper [8], the author works Hybrid algorithm that is combination of two algorithms one is public key cryptography and another is secret key cryptography. They provide security on data at the time of uploading and downloading data from cloud server. Digital signature will use in future for data will reached at destination correctly.

B. SUMMARY ON LITERATURE REVIEW

A number of researchers have discussed the security challenges that are raised by cloud computing. It is clear that the security issue has played the most important role in hindering the acceptance of Cloud Computing.

For security purpose of cloud storage various encryption techniques are being analyzed by researchers. As discussed in survey there are many security techniques which are currently applied to cloud storage. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the cloud storage.

IV. OBJECTIVE OF THE PROPOSED RESEARCH

- The main object of this paper is to analyze the time taken for encryption by various cryptographic algorithms for parameters like data type, data size, data density and key size on different file size of text, audio and video data in order to select the most suitable cryptographic algorithm for encryption for data in the cloud.
- To develop a cryptographic algorithm for encryption for data in the cloud that is reliable and eliminates many of the attacks that can occur.
- The objective of the paper is to provide a performance analysis between Blowfish algorithm and proposed symmetric algorithm. The analysis will be conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithms for encryption and decryption.

V. PROPOSED METHODOLOGY

The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following methodology which is helpful in increasing the security of data storage.

 DOI : 10.18231/2454-9150.2019.0598

The following are the methods to be followed in this research proposal:

- Upload Text files: The files can be selected based on size of data.
- For Encryption of text files: Upload Text file Implementing the symmetric encryption algorithm to generate encryption
- For Decryption of text files: Read Cipher Text from

  Database. Implementing the symmetric decryption algorithm to generate decryption.
- Display Plain Text to User
- Comparison of execution time and speedup for the different data sets for encryption and decryption.

The execution time should be studied for different number of file size used and file types results compared against blowfish algorithm.. In this way the efficiency of the proposed symmetric algorithms can be found.

VI. EXPECTED OUTCOME OF THE PROPOSED RESEARCH

The execution times for encryption and decryption using the proposed algorithm should be less than the blowfish algorithm. Also there should be a proportional increase in execution time only against the size of the size.

VII. CONCLUSION

This research proposes a new enhanced cloud security algorithm. The proposed model improves the security issues related to cloud models and protection of file.

REFERENCES

[1] Wayne Jansen ,Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP - 800-144 ,80 pp., 2011.

[2] Brian Hay, Kara Nance, Matt Bishop, “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing” Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.

[3] Kevin Curran, Sean Carlin and Mervyn Adams, “Security issues in cloud computing”, Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.

[4] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, PP. 58-309.

[5] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha “A Study of New Trends in Blowfish Algorithm”, International Journal of Engineering Research and Applications(IJERA)ISSN:2248-9622 ww.ijera.com Vol. 1, Issue 2, pp.321-326.

[6] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994.

[7] B.Thimma Reddy, K.BalaChowdappa, S.Raghunath Reddy ― Cloud Security using Blowfish and Key Management Encryption Algorithm ‖International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-2, Issue-6, June 2015

[8] JasleenKaur, Dr. SushilGarg, ―Security in Cloud Computing using Hybrid of Algorithms‖,International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015 ISSN 2091-2730.

[9] Viney Pal Bansal ,Sandeep Singh―A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs ―RAECS UIET Panjab University Chandigarh 22nd December 2015 , 978-1-4673-8253-3/15/$31.00 ©2015 IEEE

[10] M.Rama Raju,J Purna Prakash “Protecting Data in Cloud Storage Using Blowfish Encryption Algorithm and Image Based One Time Password”. dec 2016 IJIR.

[11] TingyuanNie and Teng Zhang ,”A study of DES and Blowfish encryption algorithm“, in Proc. IEEE ,Jan, 2009.

[12] DeyanChen,Hong Zhao,” Data Security and Privacy Protection Issues in Cloud Computing, ” 2012 IEEE International Conference on [Computer and Electronics engineering.Nadeem2005] Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005

[13] N. Jayapandian, Dr. A. M. J. Md. Zubair Rahman, R.B.Sangavee, R.Divya Improved Cloud Security Trust on Client Side Data Encryption using HASBE and Blowfish”, IC-GET 2016

[14] Aakash Gore, S.S.Meena, Preetesh Purohit.”Hybrid Cryptosystem using Modified Blowfish Algorithm and SHA Algorithm On Public Cloud”.Dec 2016 IJCA

 DOI : 10.18231/2454-9150.2019.0598