International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Data Security in Cloud using Hybrid Cryptography Algorithms

Abhishek H M[1], Ashwij A[2], Harisha[3], Amol[4]
[1, 2, 3, 4]*Department of Computer Science Engineering, Dayananda Sagar College of Engineering, Karnataka, India*

Abstract: ***Cloud Computing is used in many areas to store large amount of data securely. Some of the areas such as military, industries etc use cloud to store their confidential data. But whichever the area is, security of data would be the prominent entity. Cryptography is the best technique to store and retrieve data efficiently and securely. Using single algorithm will not contribute highly for greater level security of data in cloud. In this paper we have introduced a better security mechanism using symmetric key cryptography algorithms. In this proposed system AES and blowfish algorithms are implemented to provide block wise security to data. Key size of both the algorithms is 128 bit. File will be split into four parts. Each and every part is encrypted using AES and blowfish algorithms alternatively. All parts are encrypted simultaneously due to multithreading. The same technique is applied in reverse for file decryption. Integrity of data in the file will not be lost after the decryption process.***
Keywords: Cloud Computing, Cryptography, Encryption, Decryption, Integrity.

I. INTRODUCTION

Cloud Computing is storing and accessing data, programs over the internet. Cryptography is a technique which transforms original data into non-readable form. This technique has been divided into public and symmetric key cryptography. Only authorized person can access the data stored in the cloud server.

Lots of trends are opening up in the field of Cloud Computing. Storing the data in cloud will keep the user away from the overheads of maintaining the data. Cloud storage is not just a third party data warehouse. The stored data in cloud is frequently updated by users from time to time. The users have provisions for insert, delete, modify and append the data which is stored in cloud.

Some symmetric key cryptography algorithms are AES, IDEA, DES, 3DES, blowfish and BRA. Main objective is to deliver the key to the respected receiver, so that he can access the data stored in cloud server. Public and private keys are manipulated to public key cryptography algorithms. These algorithms provide high level data security, but increase time delay during data encoding and decoding. The existed data is not visible to all, only valid receiver can view the data. To improve security of file in cloud computing, the source file is broken down into different parts. Each and every part of the file is encrypted and stored. If the hacker try to get the source file, then he would end up with only single part of the file. The complication with key management is removed during access management and identity. File gets converted into non-readable form using AES and Blowfish algorithms. These encrypted files are stored securely and efficiently in cloud.

In the existed system, only single algorithm is used for encryption and decryption. But use of single algorithm is not effective for high level storage and security of data. If we implement single symmetric key cryptography algorithm, then there comes the problem of security because these algorithms use single key for data encryption and decryption. So problem arises during key transmission into multiuser environment.

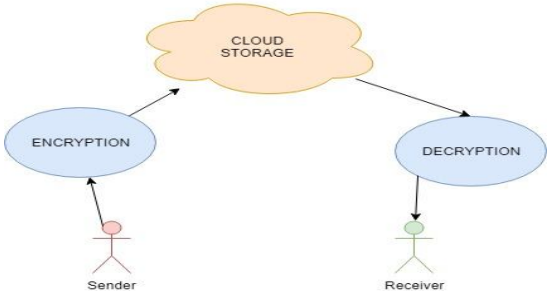

Fig. 1 System Architecture

Cloud owner and cloud user are included in system architecture as sender and receiver respectively. Sender uploads data on cloud server. File is split into four pieces. Each part is encrypted simultaneously using multithreading technique. Encrypted file is stored in cloud. These files while downloaded by a receiver, gets decrypted using same algorithms and the split files joins accordingly.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. RELATED WORK

In the paper having the title as "Ensuring Data Storage Security in Cloud Computing" the authors Cong Wang, Qian Wang, and Kui Ren has given importance to data security in cloud which is an important QoS. To provide security of data they have proposed a scheme which provides both data security and provision for data manipulation.

In the paper "Research on Cloud Computing Security Threats using Data Transmission", proposed by the author Raj Kumar, gave complete importance to cloud computing security. This security has been explained based on encryption and decryption techniques.

In the paper "Toward a Big Data Architecture for Security Events Analytic" proposed by the authors Laila Fetjah, Karim Benzidane, Hassan El Alloussi, Othman El Warrak, Said Jai Andaloussi and Abderrahim Sekkaki focused on scalable module. This was based on big data techniques and the tools which provide solution to process and analysis of events like packet flow and to generate informative decisions.

In the paper "Survey of Big Data Information Security" proposed by the authors Natalia Miloslavskaya and Aida Makhmudova has focused on big data security features. They have used big data mining algorithm which are formulated based on IS properties.

In the paper entitled "A Space-and-Time Efficient Technique for Big Data Security Analytics"propsed by the authors Suliman A. Alsuhibany imply focus on space and time efficient probabilistic technique. This technique is known as Bloom Filter (BF) which contributes to network security.

"Research on the Model of Big Data Serve Security in Cloud Environment" proposed by the author Hai-ting Cuiin gave importance on sharing the re liable data security services. This security is considered on the aspects of network transmission, cloud storage and data storage.

III. PROPOSED WORK

Data Security plays a vital role in providing quality of service (QoS). There are two challenges in which any cloud system inevitably poses.

A. There are different kinds of data which needs to be stored in the provided cloud server, which also has to ensure data correctness.

B. Clients will not use cloud only for storing the data. They frequently access the data and manipulate based on their requirements.

The proposed methodology involves four stages:

1) *Splitting:* The file which has been uploaded through a java application has been divided into four parts. This data file can be of formats such as text, image, audio and video. Whatever the file size would be, the whole gets split into four parts.

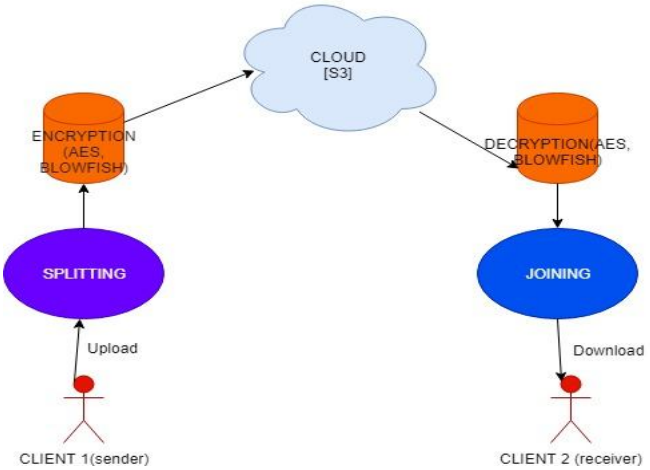

Fig. 2 Proposed Model Architecture

2) *Encryption:* In this phase, the split parts of the file will be encrypted. Each and every part will be encrypted by cryptography techniques. AES and Blowfish algorithms encode the pieces of file alternatively. That is, if the first part is encrypted by AES, then the next part is from blowfish and vice versa. After this, these encrypted parts will be stored in the cloud server of any private CSP. In the proposed model Amazon's S3 (Simple Storage Service) have been used.

3) *Decryption:* This is nothing but the reverse form of encryption. The encrypted files have been decrypted using the same algorithms. This begins only when the client starts downloading the files from the cloud to his local system. The non-readable form of the file has been converted into readable form.
4) *Joining:* This is the last phase in the process. The part of file which has been converted from non-readable to readable form has to get joined to retrieve the original form of the file uploaded. Once the joining is completed, the original file without any data loss gets downloaded in the client's local machine.

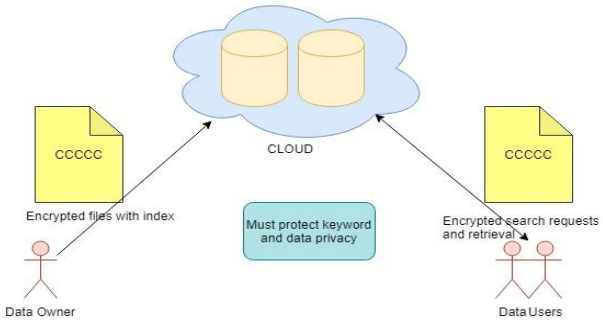

Fig. 3 Data accessing process

IV. RESULTS

The format of data can be image, text, audio and video. The data would not be lost for any size of file. However, it consumes more time for audio and video formats to encode and decode.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this current proposed model data security in cloud has been investigated and accurate results are obtained. For ensuring the correctness of user data stored in cloud the proposed method encode data and stores it in cloud server and user has a provision to modify the data.
Following conclusions are made from the results and analysis:

A. Cloud provides supercomputing power. This is beyond a single company and enterprises.
B. The user can not only store the data in cloud, he can even manipulate the stored data.
C. Cloud security is vast area for research and providing solutions for security challenges in cloud will be in a greater demand.

VI. ACKNOWLEDGMENT

Primarily, we would like to thank almighty for giving us all the courage and patience to accomplish this work. We express our heartful thanks to our guide Dr. Mohammed Tajuddin for all the guidance and support.

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren," Ensuring Data Storage Security in Cloud Computing", US National Science Foundation, 2015, pp 1-4.
[2] Raj Kumar, "Research on Cloud Computing Security Threats using Data Transmission" International Journal of Advanced Research in Computer Science and Software Engineering, India Volume 5, Issue 1, January 2015, pp. 399-402.
[3] Youssef Gahi, Mouhcine Guennoun, Hussein T. Mouftah,"Big Data Analytics: Security and Privacy Challenges", IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, June 2016, pp 15-17.
[4] S. Hesham and Klaus Hofmann , "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE,International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170,April 2014.
[5] Natalia Miloslavskaya and Aida Makhmudova, "Survey of Big Data Information Security", 4th International Conference on Future Internet of Things and Cloud Workshops, Vienna, Austria, Aug 2016,pp 4-9.
[6] Subhash, Shirole Bajirao. "Data Confidentiality in Cloud Computing with Blowfish Algorithm."International Journal of Emerging Trends in Science and Technology 1.01 (2014).
[7] Singla, Jasmeet Singh. "Cloud data security using authentication and encryption technique." Global Journal of Computer Science and Technology 13.3 (2013).
[8] S. Roy and M. Manasmita, "A Novel Approach to Format Based Text Steganography," in International Conference on Communication, Computing & Security (ICCCS '11), 2011.
[9] Saakshi Narula," Cloud computing security:amazon web service", Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, India,Feb 2015,pp 699-703 [10] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, USA, 2008, pp102-113.
[10] S. Shi, Y. Qi and Y. Huang, "An Approach to TextSteganography Based on Search in Internet," in International Computer Symposium, 2016.