Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Computing System Using Multilevel Dynamic Data Possession

R. Thenmozhi*
M.E-CSE&NPR College of Engineering and Technology, Tamilnadu, India

T. Rani Mangammal
Assistant Professor & NPR College of Engineering and Technology, Tamilnadu, India

Abstract- Outsourcing data to remote cloud service provider is increasing nowadays. The security is the important issue in outsourcing. This outsourcing process relieves the burden of data owner updation process. The data owner stores the data in cloud service provider after the encryption. For securing the data Elliptic curve cryptography and Blowfish algorithms are used which is more secured than the Advanced Encryption Standard algorithm. By using Secure Hash Algorithm-1 owner can check the integrity of the data. It uses 160 bits of key for generating Message Authentication Code. It is more effective than the Message Digestive-5 algorithm. The data owner update one of the copies from Cloud Service Provider and the remaining data must be updated by the Cloud Service Provider. By the way Message Authentication Code is also been updated and then the client can send the request and receive the data from the Cloud Service Provider. By using the Secure Hash Algorithm-1 the client can check the integrity of the data, whether it is updated or not. This mechanism will increase the security when compared to the existing process.

Keywords- Cloud Service Provider (CSP); Blow Fish; Elliptic Curve Cryptography; Message Authentication Code (MAC); Advanced Encryption Scheme (AES); Message Digest (MD5).

I. INTRODUCTION

Cloud computing provides shared processing environment for data storage and accessing also known as internet-based computing. It is a model which provides configurable computing resources such as networks, servers, storage, applications and services. Cloud computing has a high computation power, lowest cost of services, higher performance, scalability, accessibility and availability for that reason it is highly demanded.

II. RELATED WORK

A. Blowfish

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits and making it ideal for securing data. It is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption.

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or AES. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. It has been analysed considerably, and it is slowly gaining acceptance as a strong encryption algorithm much faster than DES and AES.

B. Secure Hash Algorithm 1

SHA1 was developed by the NSA for NIST as part of the Secure Hash Standard (SHS). SHA1 is similar in design to MD4. The original published algorithm, known as SHA, was modified by NSA to protect against an unspecified attack; the updated algorithm is named SHA1. It produces a 160-bit digest -- large enough to protect against "birthday" attacks, where two different messages are selected to produce the same signature, for the next decade.

SHA1 is implemented in Kremlin. It is suitable and efficient for hardware implementation. Besides, it is unpatented and no license is required. Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. Blowfish is also one of the fastest block ciphers in public use.

C. Elliptic Curve Cryptography

It is Elliptic Curve Cryptography. ECC was introduced by Victor Miller and Neal Koblitz in 1985.It uses Asymmetric Key Algorithm. It uses 224 bit key length. For DSA, RSA we need larger key length.ECC requires significantly smaller key size with same level of security as DSA & RSA. Although it has smaller Key length, it provides higher Security equivalent to RSA. Since it is asymmetric, it has greater efficiency. Having Smaller Key Size, it has faster computations and needs less storage space.

III. SYSTEM ARCHITECTURE

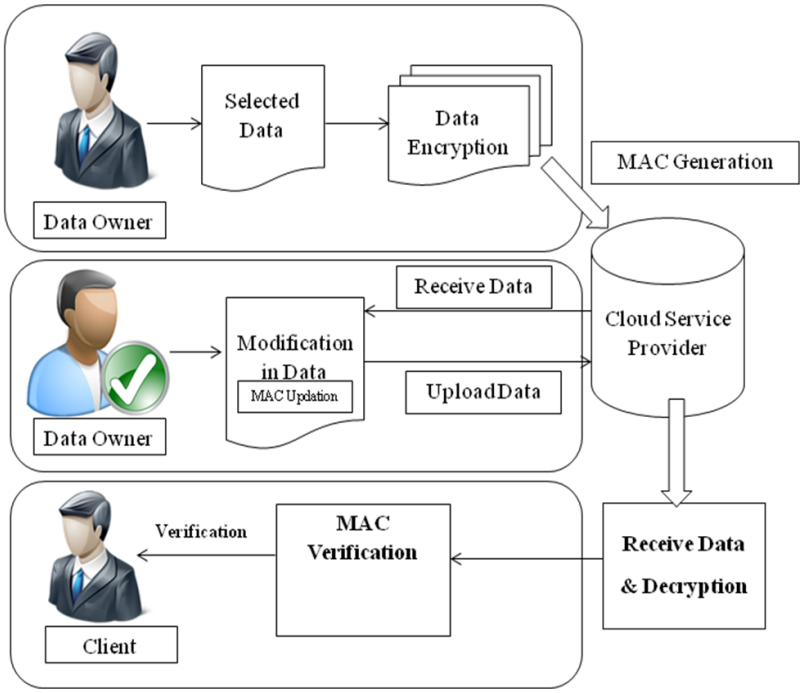

Fig1. System Architecture

IV. PROPOSED SYSTEM IMPLEMENTATION

A. Data Owner Registration

Data owner have to register the details. And then select the data. The data are splitted. A data owner that can be an organization should maintain the data stored in the clouds database. A Cloud Service Provider maintains the cloud servers and provides paid storage space to the user. A user is a set of owner and clients having the right to access the remote server and its data.

B. Data Uploading

MAC generated for the splitted data then the data are encrypted and uploaded into the cloud service provider's storage space. The data owner has a file consisting of multi blocks and the CSP offers to store the multi copies of the owner file on various servers. The critical data should be replicated on multiple servers. On the other hand, non-critical, reproducible data are stored at reduced levels of redundancy. For data confidentiality, the owner encrypts his data before outsourcing to CSP.

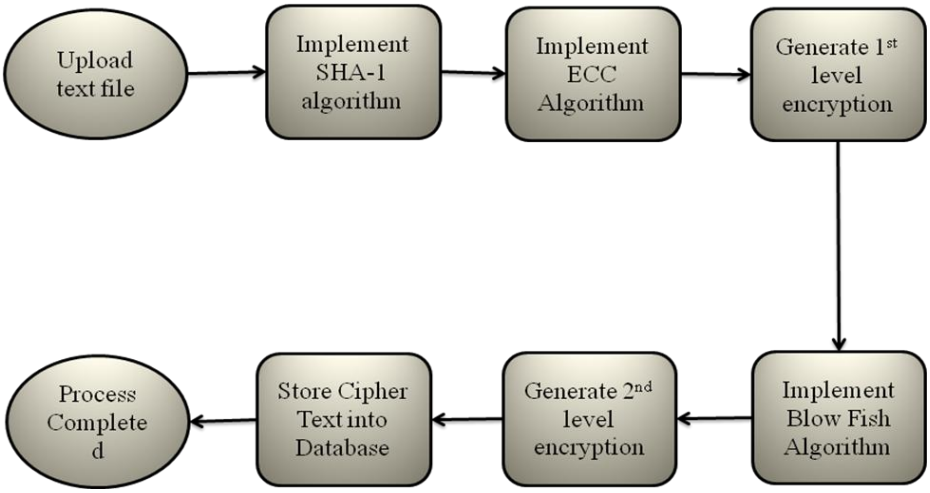

Fig2. Multilevel Encryption

C. Users Request

Users send the request to the cloud service provider. Cloud service providers send the related data to the user. An authorized user sends a data-access request to the CSP and receives a file copy in an encrypted form. Decryption is done by using a secret key shared with the owner. The work of the servers should be organized using the load balancing mechanism. The data-access request is directed to the server with the lowest congestion

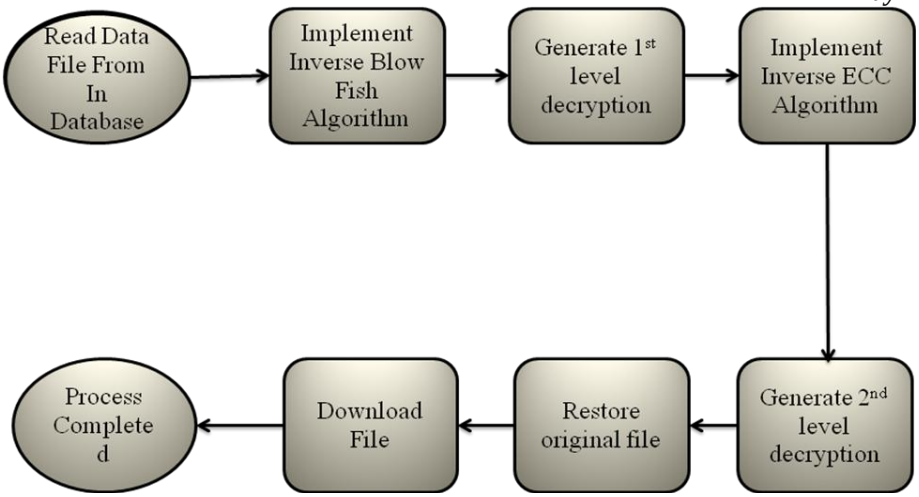

Fig3. Multilevel Decryption

D. Users Accessing Data

User get the key from the data owner and get the encrypted data from the cloud service provider then decrypts the data. The authorized users have the rights to access the owner file stored on the CSP. A new PDP scheme supports outsourcing of multi-copy dynamic data. Data owner having the capability to updating, scaling and access the data copies stored in the remote servers.

V. CONCLUSION

The existing system have TB-PMDDP scheme. It is used for dynamic single copy system. The TB-PMDDP needs high storage. So it leads to storage overhead. The remote system needs high computation for complete the task. The MB-PMDDP scheme reduces the computation time. The data owner stores the data in the cloud service provider. Multi copies are generated for the data stored in the cloud service provider.

REFERENCES

[1] Ayad F. Barsoum and M. Anwar Hasan, "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems,"2015.

[2] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," 2010.

[3] A. F. Barsoum and M. A. Hasan. "On verifying dynamic multiple data copies over cloud servers," 2011.

[4] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," 2007.

[5] Kochumol Abraham, Win Mathew John, "Proving Possession and Retrievability within a Cloud Environment: A Comparative Survey", 2014.

[6] A. F. Barsoum and M. A. Hasan. "Provable possession and replication of data over cloud servers," 2010.

[7] M.Yugandhar, D. Subhramanya Sharma. "Security of Data Dynamics in Cloud Computing" 2012.

[8] Yihua Zhang and Marina Blanton," Efficient Dynamic Provable Possession of Remote Data via Balanced Update Trees",2013.

