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

Enhance the Security for Outsourced Database in Cloud Computing by Using ECC Algorithm

V. Suganya
M.E-CSE & NPR College of
Engineering and Technology, Tamilnadu, India

J. Viswanath
Assistant professor & NPR College
of Engineering and Technology, Tamilnadu, India

Abstract: ***To enlightening the security by usingElliptic Curve Cryptography (ECC) Algorithm.Detect the duplicated data and avoid with a Secure Hash Algorithm (SHA).In many case when the fraudulent Cloud Service Provider (CSP) deliberately recompense(returns) an empty set for the query asked by the user so we avoid this fraudulent result by usingBloom filter tree whichis used to check the accuracy and completeness of the query result.Elliptic Curve Cryptography is used to improve security and throughput rate. Another use of ECC algorithm is used to improve the integrity level in Cloud while the data travellingfrom DataOwner to Authenticated personover the Network. In Deduplicated method is used to avoid duplicated Copies of data from other DataOwner and save our storage space in Cloud.***

Keywords: Elliptic Curve Cryptography (ECC), Deduplication, Secure Hash Algorithm (SHA), Cloud Service Provider (CSP).

I. INTODUCTION

Cloud which is used to deliver the resource over an internet without handling any hardware and software Cloud Computing is the distribution ofmany services like software (SAAS), platform (PAAS), infrastructure (IAAS) through the Internet. The infrastructure as a services provides both hardware and software as a service by using the virtualization technology to the cloud users. Virtualization is a process of creating a virtual version of operating system, server, hardware, software. Virtual Machine (VM) is like computer running within a computer and also known as "guest" machine. VMI formats are supported by hypervisor like Xen, Kvm, VMware, Virtual box etc. Elliptic Curve Cryptography (ECC) algorithm recently gained a lot of responsiveness in industry. The principal of ECC compared to RSA is that it offers equal security for a smaller bit size compared with RSA ECC algorithm has reduce computation overhead. ECC is ideal for constrained environment such as pager, PDAs, cellular phones and smart cards. ECC is more secured algorithm in Cloud Computing. Now a days the Cloud Computing Technology is the emerging Technology in the storage area.

II. RELATED WORK

A. Verifiable Auditing for Outsourced Database in Cloud Computing:

The Verifiable Auditing is used to verify the users there is no subsiding system can perfectly find out the correct properties for correctness and completeness of both query request. The Cloud Service Provider sometimes provide the empty set for the query request.to avoid this they used new Verifiable Auditing scheme for Outsourced Database which is concurrently achieve both correctness and completeness of the query request even an Cloud Service Provider can intestinally returns an empty set Further, the proposed system can be used to support the dynamic database setting by joining the concept of verifiable database with updates.in the checking process we used Tuple Merkle Hash tree which is used to provide the signature for each individual attribute(column) to check the correctness and completeness of the data. Bloom Filter is used to check whether the data is present or not Evdokimov's scheme is used here to encrypt the data. The benefit is that the user can efficiently performing the verifiable auditing for the result returned by the CSP in this paper there is many difficulties are there is less security, uploading downloading time is high, there is no chance to check the duplicated copies so the Cloud Service Provider consumes more space in Cloud.

B. Provable data Possession at untrusted stores:

The provable data possession(PDP) method which introduced that the client has used to store the data at untrusted storage server to verify all times that the data is original data it can verify the data without retrieving the data the client has to maintain the metadata to verify the proof. The response provably secure by using provable data possession schemes. Thebenefit of PDP is used to disguised blocks (called sentinels) hidden among regular file blocks in order to detect data modification by the server thedifficulty is security of the scheme is not proven because it contains the algorithms are less secured and not proved.

C. Network applications of bloom filters: A survey

A bloom filter is a resourceful randomized data structure for representing a set in order to support the accurate membership queries. The bloom filter is mainly used for space efficiency. The space efficiency is achieved at the cost of

© 2016, IJARCSSE All Rights Reserved

false positive. The bloom filter is used to check whether the data is present in the set in the database. The bloom filter is used in large scale network applications such as shared web caches, query routing, and replica location.A Bloom filter is a space-efficient representation of a set or a list that handles membership queries in Cloud. There are various example they used bloom filters in the network. Especially when space is an issue, a Bloom filter may be asuperb alternative one to keeping an explicit list. It represents a set for membership queries, with false positives. Probability of false positive can be controlled by design parameters.

III. IMPLEMENTATION

Data Owner completes registration and encrypt their data using Elliptic Curve Cryptographyalgorithm and provide hash key to check duplication. Then upload their data to CSP and download afile from Arbitration Center.The CSP provides a secret Key to Data Owner after registration to upload and download the data the secret key is used to check the Authorized users to download the data which is checked by CSP and AC. The CSP provides encrypted data to users and AC decrypted the data to authorized user. The Arbitration Center gets hash key from Data Owner and checks if any file already exists. If so the Data will be avoid and give message to the Data Owner by using SHA algorithm.The main purpose of arbitration Center is used to check the private key mail id and password which is given by users the Arbitration Center Matches the key and with the corresponding person's mail id.by using SHA algorithm the checking process is easy to get the original content. The Deduplication process is used to avoid the wastage of memory space in cloud. The Data Owner Encrypts Their Data using Elliptic Curve Cryptographyand store it to Arbitration Center. The Arbitration Center get private key encrypted data then checks user's key which is provided by the CSP and gives data to users. The Arbitration Center while getting a private key it checks whether the private key is correct or not. If private key matched the corresponding Data Owner then it get the encrypted data and decrypt the data then provide it to the corresponding Data Owner. Here the misbehavior of cloud server will be avoid. The Arbitration Center is also known as Auditor because all checking process is achieved by Arbitration Center.

IV. ARCHITECTURE

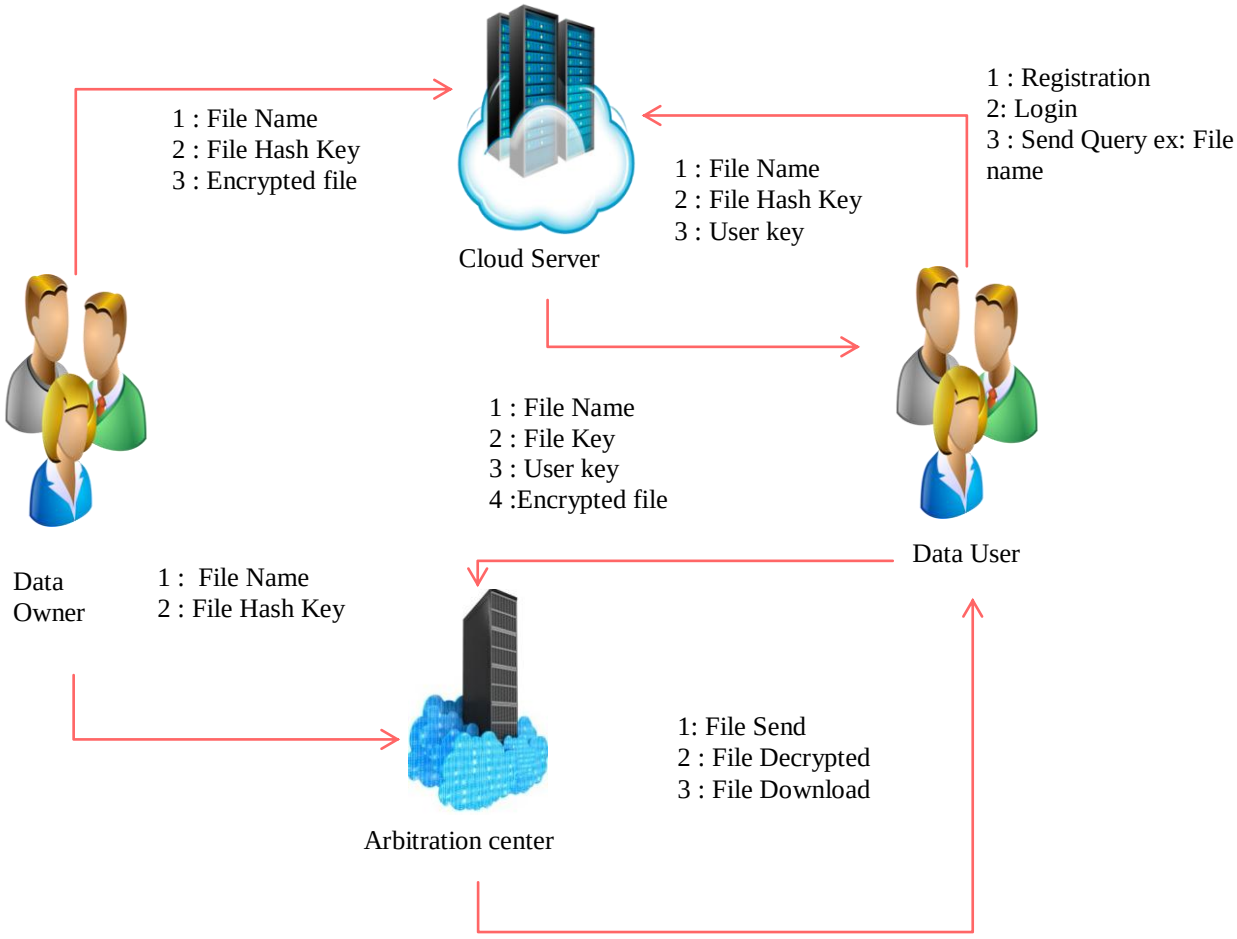

Fig. 1. Architecture of proposed system.

V. MODULES

- Creation of Data Owner Modules
- Creation of Cloud Service Provider Module
- Detection of Deduplication by using SHA Algorithm
- Creation of Arbitration Center(AC) Modules

© 2016, IJARCSSE All Rights Reserved

MODULE 1: Creation of Data Owner Modules

The Data Owner completes registration and encrypt their data using ECC algorithm and provide hash key by using SHA algorithm to check duplication. Then upload their data to CSP and download a file from Arbitration Center.

MODULE 2: Creation of Cloud Service Provider Module

The CSP provides a secret Key to Data Owner after registration to upload and download the data by using secret keys.the secret key is used to check the authorized users to download the data from Data Owners which is checked by CSP and Arbitration Center. The CSP provide encrypted data to users and Arbitration Center decrypts the data to authenticated users.

MODULE 3: Detection of Deduplication by using SHA Algorithm.

The Arbitration Center gets hash key from Data Owner and checks if any file already exists. If so the Data will be avoid and give message to the Data Owner by using SHA algorithm. The main purpose of AC is used to check the private key which is given by users the AC Matches the private key with the corresponding person's mail id and password the checking process is easy to get the original content by SHA algorithm. TheDeduplication process is used to avoid the wastage of memory space in cloud.

MODULE 4: Creation of Arbitration Center (AC) Modules.

The Data Owner encrypts Their Data using ECC and store it to AC. The AC get private key encrypted data then checks user's key which is provided by the CSP and gives data to users. The Arbitration Center while getting a private key it checks whether the private key is correct or not. If private key matched the corresponding Data Owner then get encrypted data and decrypts the data to users then provide to the corresponding Data Owner.

VI. CONCLUSION

The goal of the system is to improve the security by using Elliptic Curve Cryptography which contains two types of keys private and public key and integrity of data will not be changed. Sometimes the Cloud Service Provider (CSP) deliberately recompense (returns) an empty set for the query asked by the user to avoid this Misbehavior of CSP we are using Bloom filter tree which is used to check the correctness and completeness of the query result. The Deduplication is achieved by SHA using algorithm.

REFERENCES

[1] Jianfeng Wang, Xiao Feng Chen, Xinyi Huang, Ilsun You, and Yang Xiang,"*Verifiable Auditing for Outsourced Database in Cloud Computing*,"IEEE Transactions on Computers, Citation information: DOI 10.1109/TC.2015.2401036.

[2] G.Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "*Provable data possession at untrusted stores*," in Proc. 14th ACM conference on Computer and communications security, pp. 598-609, 2007.

[3] B. Andrei and M. Michael, "*Network applications of bloom filters*: A survey," Internet Mathematics, vol. 1, no.4, pp. 485- 509, 2004.

[4] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, "*Secure outsourcing of scientific computations*," Advances in Computers, vol. 54, pp. 215-272, Jan. 2002.

[5] E. Bertino, B. Carminati, E. Ferrari, B. M. Thuraisingham, and A. Gupta, "*Selective and authentic third-party distribution of XML documents*," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 10, pp. 1263-1278, Oct. 2004.

[6] S. Benabbas, R. Gennaro, and Y. Vahlis, "*Verifiable delegation of computation over large datasets*," in Proc. 31st Annual Cryptology Conference-CRYPTO 2011, LNCS 6841, Springer, pp. 111-131, 2011.

© 2016, IJARCSSE All Rights Reserved