Three Layer Privacy Preserving Using Fog Computing

Manasa.R,
Dept. of CSE, PEC, Chennai, India
Gayathri.T.K.
Dept. of CSE, PEC, Chennai, India
K.Shankar
Asst. Professor, Dept. of CSE, PEC, Chennai, India

ABSTRACT

Fog computing is an architecture that uses edge devices to carry out a substantial amount of computation, storage, communication locally and routed over the internet backbone. The development of cloud computing technology with the explosive growth of unstructured data, cloud storage technology gets more attention and better development.The cloud provider does not have suggestions regarding the information and the cloud data stored and maintained globally anywhere in the cloud. The privacy protection schemes are usually based on encryption technology. A three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Here we are using hash- solomon code algorithm is designed to divide data into different parts. In this framework we are using bucket concept based algorithms to secure the data information and using BCH code algorithm for error-correcting cyclic problem.Based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively.

Keywords - **Hash-solomon code, Fog computing, cloud computing, bucket framework**

I. INTRODUCTON

In Computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or transported. Every month, they pay for what they consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Cloud computing is usually Internet-based computing. The cloud is a metaphor for the Internet based on how the internet is described in computer network diagrams; which means it is an abstraction hiding the complex infrastructure of the internet. It is a style of computing in which related capabilities are provided “as a service”, allowing users to access technology-enabled services from the Internet ("in the cloud") without knowledge of, or control over the technologies behind these servers.

Fog computing can be perceived both in large cloud systems and big data structures, making reference to the growing difficulties in accessing information objectively. This results in a lack of quality of the obtained content. The effects of fog computing on cloud computing and big data systems may vary. However, a common aspect that can be extracted is a limitation in accurate content distribution, an issue that has been tackled with the creation of metrics that attempt to improve accuracy. Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives, dense geographical distribution and local resource pooling, latency reduction and backbone bandwidth savings to achieve better quality of service (QoS) and edge analytics/stream mining, resulting in superior user-experience and redundancy in case of failure.

II. EXISTING SYSTEM

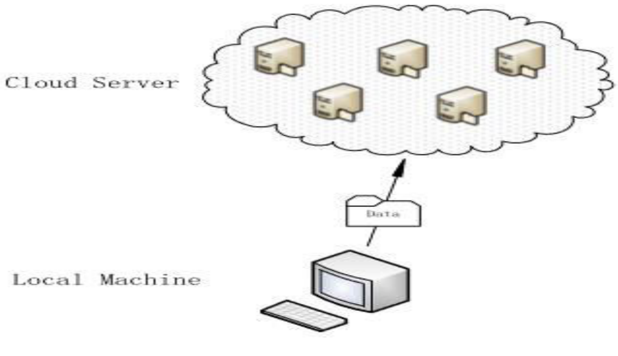

Fig1. Traditional cloud storage structure

In existing system, data has been partitioned and stored in three storage servers such as cloud server, fog server and local server by hash- Solomon code algorithm. One important thing is that the third party don’t have the knowledge about our data partitioning. The Cloud server contains 80% of unimportant information, the Fog server contains 15% of most important information and the Local server contains 5% of important information. If hacker hacks the data in any one these layers either he/she will modify the data or delete the data. Hence the user will loose that data. This is the major disadvantage.

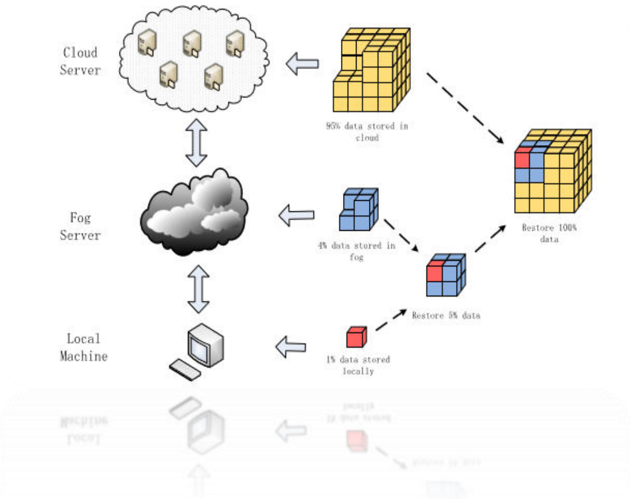

Fig2. Illustration of Existing System

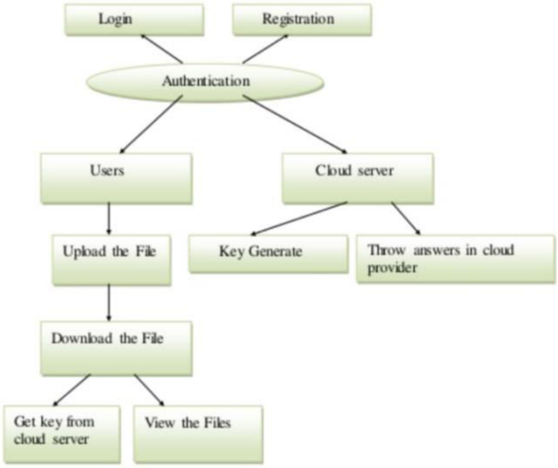

Fig5. ER Diagram

III. PROPOSED SYSTEM

We implement a framework called bucket to secure and restore the lost data.Bucket is like a mirror, whatever data has been implemented by the user the data will be automatically stored in the bucket framework. We proposed BCH code algorithm data comparison in three layers and matched data are stored in bucket.

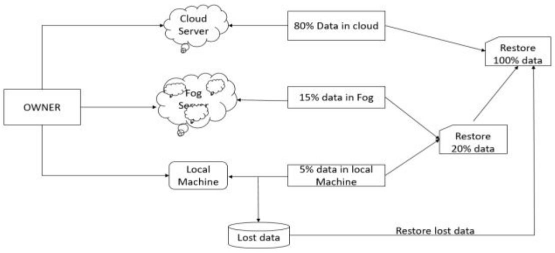

Fig3. Illustration of three layer privacy preserving using fog computing

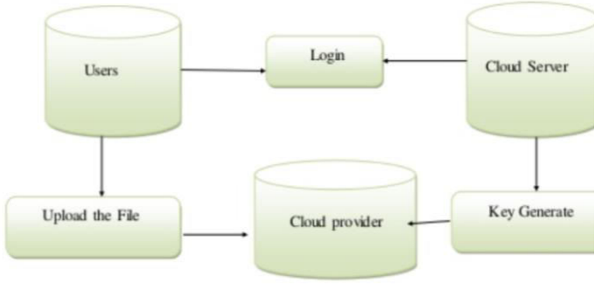

Fig4. DataFlow Diagram

IV. RELATED WORKS

In current storage schema, user’s data is totally stored in cloud servers. Users lose their right of control on data and face privacy leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but the sekind sofmethodscannoteffectivelyresistattackfromthe inside of cloud server. In order to solve this problem, we propose a three-layer storage framework based on fog computing.

The proposed frame work can both take full advantage of cloud storage and protect the privacy of data. Besides ,Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog ,and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.

V. METHODOLOGY

5.1 Hash- Solomon Code Algorithm

Hash- Solomon code algorithm is mainly designed for dividing the data into different parts. Here the data is divided and stored in three different parts. Data is divided based on their importance of information in it.

5.2 BCH Alogithm

In coding theory, the BCH codes or Bose–Chaudhuri–Hocquenghem codes form a class of cyclic error-correcting codes that are constructed using polynomials over a finite field(also called Galois field). BCH codes were invented in 1959 by French mathematician Alexis Hocquenghem, and independently in 1960 by Raj Bose and D. K. Ray-Chaudhuri. The name Bose–Chaudhuri–Hocquenghem (and the acronym BCH) arises from the initials of the inventors' surnames (mistakenly, in the case of Ray-Chaudhuri).

One of the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors. Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes, using small low-power electronic hardware.

BCH codes are used in applications such as satellite communications,compact disc players, DVDs, disk drives, solid-state drives and two-dimensional bar codes.

5.3 Bucket Framework

This framework is specially designed for the user to retrieve the data if the data has been lost or modified by third party.

Bucket acts as a mirror, whatever data has been entered by the user it will be automatically stored in it.

VI. MODULE DESCRIPTION

6.1 Registration Module

This module is used for the user to register their login id by providing the minimal information.User want enter their minimal information such as mail id, name, mobile number, password which is used for further logins.So that they can login to the website.

6.2 Login Module

In this module, user can login to the website by registered login id and a valid password. If it is not a valid user he/she cannot login to it.Only the authenticated users can login and use the website.

6.3 Storage Module

In this module, user can store their files into three different storage server. The storage servers are cloud server, fog server and local server. In cloud server we store 80% of data.In fog server we store sensitive 15% of data.In local server we store 5% of data.

6.4 Recovery Module

In this module, user can recover their files from three different storage server.By using BCH algorithm, if the data matched with these three layers of data then it will be stored in the bucket.If the data has been hacked in any one of the layers, the user can easily recover it from bucket framework.

6.5 Download Procedure

When user wants to download his file from the cloud server, the procedure is shown in Fig. 5. Firstly, cloud server receives user’s request and then integrates the data in different distributed servers. After integration, cloud server sends the 95% data to the fog server. Secondly, the fog server receives the data from the cloud server. Combining with the 4% data blocks of fog server and the encoding information, we can recover 99% data. Then the fog server returns the 99% data to the user. Thirdly, the user receives the data from fog server. User can get the complete data by repeating the above steps.

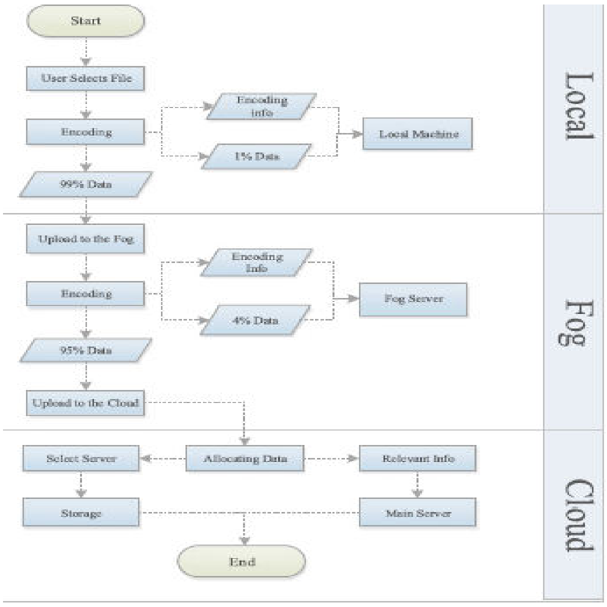

Fig 6.Diagram of stored procedure

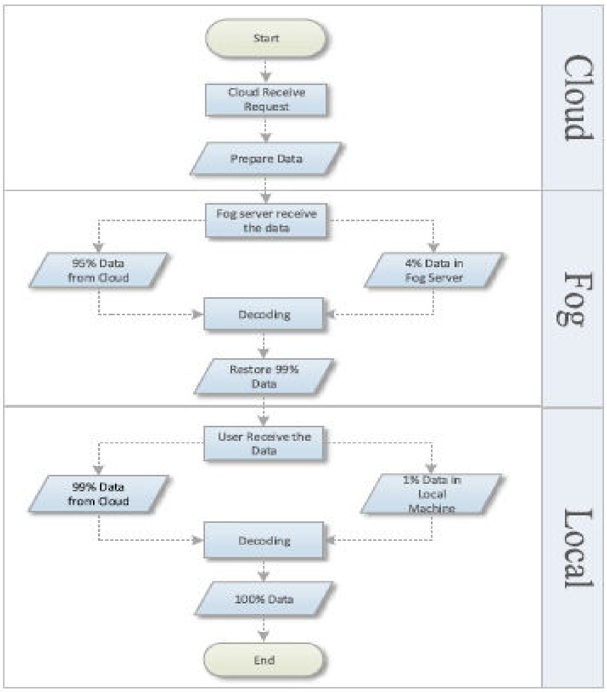

Fig 7. Diagram of download procedure

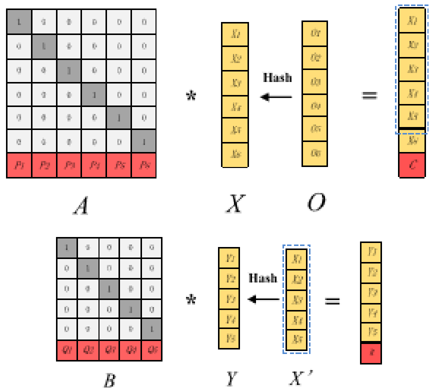

Fig 8. Diagram of download procedure

VII. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a bucket framework based on fog computing model and design a BCH Code algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible.

VIII. FUTURE ENHANCEMENT

As the cloud storage scheme based on fog computing is done by the mentioned algorithms, it can further developed by using some other algorithms to reduce the lines of code and to reduce the time complexity.

REFERENCES

[1] P. Mell and T. Grance, "*The NIST definition of cloud computing," Nat. Inst. Stand. Technol*., vol. 53, no. 6, pp. 50–50, 2009.

[2] Secure and Privacy-Preserving Data Storage Service *in Public Cloud Li Hui1, Sun Wenhai1, Li Fenghua2, And Wang Boyang1*Vol. 51, no. 7, pp. 1397–1409, 2014.

[3] L. Xiao, Q. Li, and J. Liu, *"Survey on secure cloud storage," J. DataAcquis. Process.,* vol. 31, no. 3, pp. 464–472, 2016.

[4] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "*A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11,pp. 2594–2608, Nov. 2016.

[5] Fog computing and its role in the internet of things F. Bonomi, R. Milito, J.Zhu, s.Addepalli vol. 11, no. 12, pp. 2706–2716, Dec. 2016.

[6] A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities Jian shena. b,c, dengzhiliuc, junshenc, qi liua,c, xingmingsuna,c vol. 41 , pp. 219–230, 2017.

[7] Privacy-Preserving public auditing for secure cloud storage congwang, student member, sherman s.-m. Chow, qianwang, student member, kuiren, member, and wenjinglou, membervol. 41, pp. 219–230, 2017

[8] A Survey on Secure Storage Services in Cloud Computing
Ms. B.Tejaswi, dr. L.V.Reddy& ms. M.Leelavathi vol. 24,NO. 9, 2017