A Fog-Centric Secure Cloud Storage Scheme

[1]Ms. Alice Nineta R.J, [2]Ms. Lini Raj L.A

[1]Assistant Professor, [2]PG Scholar
Department of Computer Science and Engineering,
Marthandam College of Engineering and Technology, Kuttakuzhi, India

***Abstract*: Cloud computing is now being utilized as a prospective alternative for storage service. Privacy breach, malicious modification and data loss are emerging cyber threats against cloud storage. Recently, a fog server based three-layer architecture has been presented for secure storage employing multiple clouds. Fog computing is a promising computing paradigm that extends cloud computing to the edge of networks. Similar to cloud computing but with distinct characteristics, fog computing faces new security and privacy challenges besides those inherited from cloud computing. The proposed system is a improved and efficient fog-centric secure cloud storage scheme to protect data against unauthorized access, modification, and destruction. To enhance the efficiency of fog based cloud storage service by implementing the secure data search. It performs data search on encrypted data, which provides provable secrecy for encryption, query isolation, controlled searching, and support of hidden query. The security is improved by a robust fog centric cloud computing infrastructure. The user data is outsourced and user's control over data is handed over to fog node, which introduces same security threats as it is in cloud computing. First, it is hard to ensure data integrity, since the outsourced data could be lost or incorrectly modified. Second, the uploaded data could be abused by unauthorized parties for other interests. To address these threats, auditable data storage service has been proposed in the context of cloud computing to protect the data. Techniques such as homomorphic encryption and searchable encryption are combined to provide integrity, confidentiality and verifiability for cloud storage system to allow a client to check its data stored on untrusted server.**

***Keywords*: Fog Computing, Homomorphic Encryption, Searchable Encryption**

1. INTRODUCTION

In traditional cloud computing scenario, once users outsource their data to the cloud, they can no longer protect it physically. Cloud Service Provider (CSP) can access, search or modify their data stored in the cloud storage. At the same time, the CSP may loss the data unintentionally due to some technical faults. Alternatingly, a hacker can violate the privacy of the user data. Using some cryptographic mechanisms (such as encryption, hash chain), confidentiality or integrity can be protected. However, cryptographic approach cannot prevent internal attacks, no matter how much the algorithm improves. To protect data confidentiality, integrity and availability (CIA), several research communities introduced the idea of Fog Computing placing fog devices in between the user and the cloud server. The proposed system a secure cloud storage scheme based on fog computing employing. To enhance the efficiency of fog based cloud storage service by implementing the secure data search.

To protect data privacy, sensitive data from end users have to be encrypted before outsourced to the fog node, making effective data utilization services challenging. One of the most important services is keyword search, i.e., keyword search among encrypted data files. The proposed scheme is the first ever scheme for searches on encrypted data, which provides provable secrecy for encryption, query isolation, controlled searching, and support of hidden query.

To improve the security of fog server for a robust fog centric cloud computing infrastructure and To enable cloud server to compute cryptic data without revealing any information from it. The user data is outsourced and user's control over data is handed over to fog node, which introduces same security threats as it is in cloud computing. First, it is hard to ensure data integrity, since the outsourced data could be lost or incorrectly modified. Second, the uploaded data could be abused by unauthorized parties for other interests. To address these threats, auditable data storage service has been proposed in the context of cloud computing to protect the data. Techniques such as homomorphic encryption and searchable encryption are combined to provide integrity, confidentiality and verifiability for cloud storage system to allow a client to check its data stored on untrusted server.

II. RELATED WORKS

M A Manazir Ahsan et al., proposed the scheme which employs a new technique Xor-Combination to conceal data. Moreover, Block-Management outsources the outcomes of Xor-Combination to prevent malicious retrieval and to ensure better recoverability in case of data loss. Simultaneously, we propose a technique based on hash algorithm in order to facilitate modification detection with higher probability.

Rachna Arora et al., states that Cloud Computing is the ability to access a pool of computing resources owned and maintained by a third party via the Internet. It is not a new technology but a way of delivering computing resources based on long existing technologies such as server virtualization.

Raghul et al., proposes the keyword search enabling technology for cloud computing is virtualization. Virtualization technique allows a physical computing device to be systematically separated into one or more "virtual" peripheral each of which can be easily used and managed to perform computing processes. Cloud computing adopting the description from Service oriented Architecture (SOA) that can help the user to break these problems into services that can be integrated to provide a solution.

Zhihua Xia et al., introduces a scheme that supports CBIR over the encrypted images without revealing the sensitive information to the cloud server. Firstly, the feature vectors are extracted to represent the corresponding images. Then, the pre-filter tables are constructed with the locality-sensitive hashing to increase the search efficiency. Next, the feature vectors are protected by the secure k-nearest neighbor (kNN) algorithm.

Cheng Guo et al., present a multi-phrase ranked search over encrypted cloud data, which also supports dynamic update operations, such as adding or deleting files. We used an inverted index to record the locations of keywords and to judge whether the phrase appears. This index can search for keywords efficiently. In order to rank the results and protect the privacy of relevance score, the relevance score evaluation modelis used in searching process on client-side.

III. PROPOSED SYSTEM

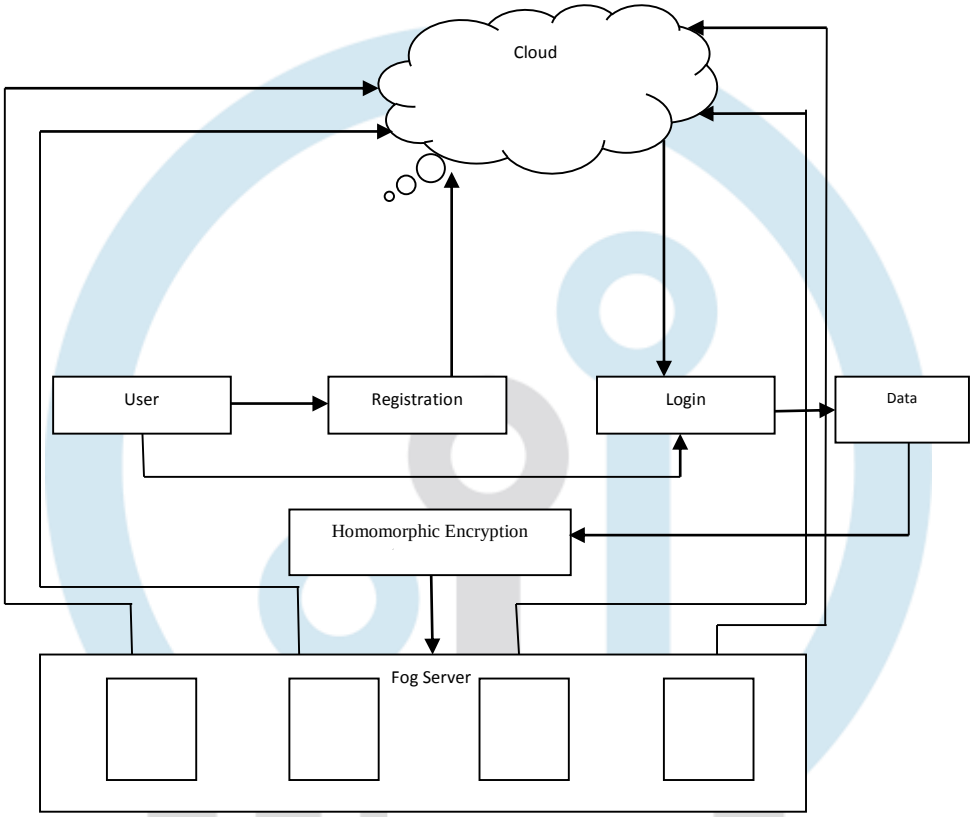

Fig 1 : Block Diagram

IV. METHODOLOGY

As user needs a trustworthy storage to save data, the proposed scheme considers an architecture where user has full control over fog devices. Users can rely on fog computing/storage devices for the management of their data. Fog computing devices further communicate with multiple clouds for advanced storage requirements. Besides, long-thick channel between cloud-fog and short-thin channel between fog-user contributes to resolve the communication issue (i.e. transmission delay). User uploads the data to the fog devices, fog device utilizes the techniques of proposed scheme to split the data into different blocks and send the different blocks to different cloud servers. Fog server can store several blocks of data to its own storage system. While retrieving data, user requests the fog server and the fog server brings corresponding blocks from cloud server, combines to form the requested data and send it back to the user. Here, proposed scheme employs different techniques for privacy preservation, data loss detection and disaster recoverability.

A. User

User is the owner of data. User uploads the data to the fog devices. This module performs the Homomorphic Encryption Homomorphic Encryption scheme is a quadruplet of polynomial algorithms (Gen,Enc ,dec,Eval) verifying:

- Gen (λ): Is an algorithm of key generation, takes as input a security parameter λ and outputs public and secret keys (pk,sk).
- Enc (m,pk): Is an encryption algorithm, takes as input a plaintext m and a public key pk and outputs a ciphertext c.
- Dec(c,sk): Is a decryption algorithm, takes as input a ciphertext c and a secret keysk and outputs a plaintext m.
- Eval (c,c1,….cn): Is an evaluation algorithm, takes as input a circuit c and ciphertexts c,c1,…cn and verifies Dec(Eval(c,c1,…cn)sk) = c(m1,…m).

B. Fogserever

Fog server is trusted to user. User relies on fog server with his data. It performs the Searchable Encryption. The cloud performs the searchable encryption and store the data on cloud.

- **AA.Setup** (λ, U)→(PP, MK, UK, GK): The setup algorithm takes a security parameter λ and an attribute universe description U as input. It outputs the public parameters PP, master private key MK, proxy update key UK and proxy grant key GK.
- **DO.Enc** (PP,M,T)→CT: The encryption algorithm takes public parameters PP, a message M, and an access structure T over the universe of attributes as input. It generates a ciphertext CT.
- **AA.KenGen** (Mk,U_{id} ,SU_{id}): The key generation algorithm takes master private key MK,a unique user identity U_{id} and the corresponding attribute set as input. It outputs U_{id}'s corresponding private key , user's search key , and user's search key in CS.
- **U.Dec** (CT, $SkU_{id)}$: The decryption algorithm take a ciphertext CT, and a private key as input. If the set of attributes related to satisfies the access structure related to CT, then it successfully decrypt and output the message M Once a user has the data (i.e. a document or a file) for safe keeping into the cloud storage and sends it to his reliable fog server device, then the fog device processes the steps as follows:

- Performs the searchable encryption on the dta.
- After that, $Block-Management$ decides which blocks are to be preserved in which clouds and sends the blocks to corresponding clouds. Different Meta data (i.e. data number, block tag, ID, cloud number) is preserved into Table 1.
- Simultaneously, fog server executes CRH operation on each of the data blocks which produces$DataDigest$. It computes hash digest of a particular data block, generates a random number R, computes hash digest of the data concatenated

C. File Processing

Storing procedure takes a file to be uploaded to cloud server securely. It has several steps and most crucial steps take place in fog server. When the user intends to upload a data file, he sends the file to the fog server through some secure channel. Then, fog server starts processing the file.

Splitting File

Fog server pads the file as per needs based on system policy. After that fog server splits the file into several fixed length blocks At the end of this step, it gets two sets of 2-block-combinations and 3-block-combinations together known as combined blocks.

Block Management

At this step, fog server determines which block to be stored to which cloud server using Block management technique, stores this metadata into fog database and sends the blocks to respective cloud servers. Cloud server receives and stores the blocks along with metadata into its storage.

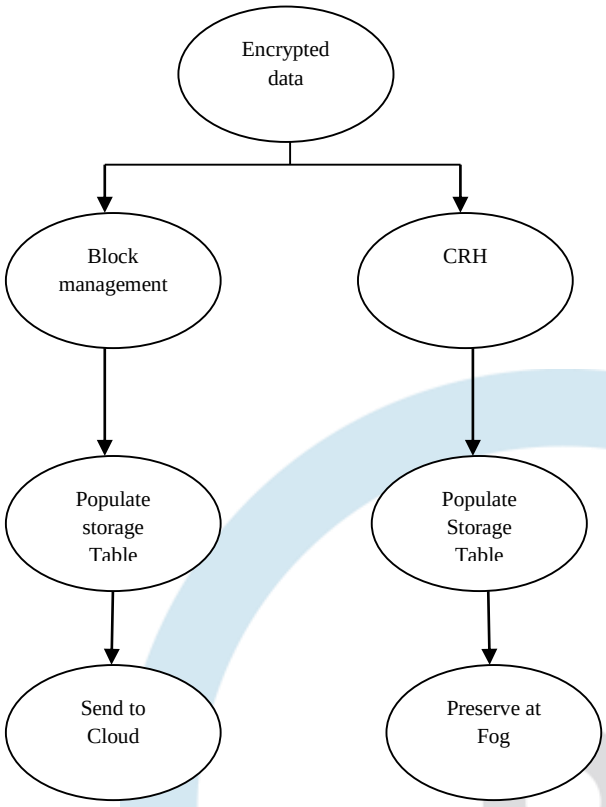

Fig 2 : Block Management

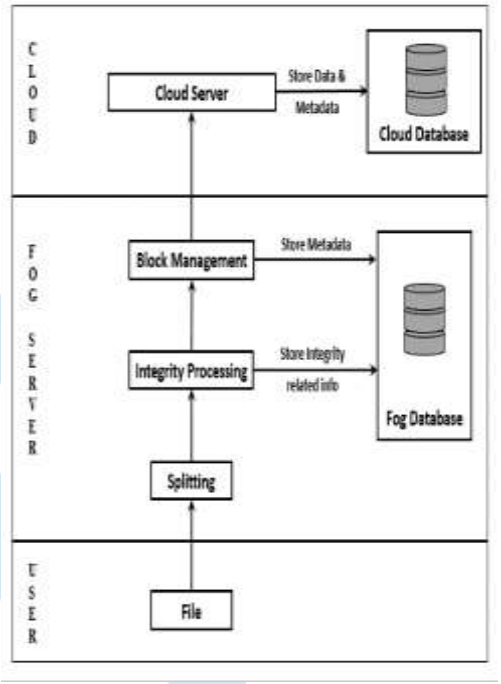

Fig 3 : File Processing

Retrieval Procedure

Retrieval procedure takes a request of a file, collects necessary *combined blocks* from various cloud servers, and checks their integrity. If integrity check fails then it requests faulty blocks from other cloud servers. When all the necessary combined blocks pass integrity check, the fog server reconstructs the entire file and sends it back to the user.

Once a user requests for a file to the fog server, the fog server looks up the relevant *combined blocks* to construct the file into its metadata database. Afterwards it sends request to corresponding cloud servers holding the *combined blocks*.

D. Cloud server

Cloud server is considered as *honest but curious*. This means that cloud server follows the Service Level Agreement (SLA) properly, but has an intention to analyze user's data.

CONCLUSION

Fog based three-layer architecture benefits to a secure solution for robust cloud storage against cyber threats. This proposed system is a scheme that undertakes preventive activities to a trusted fog server and puts the actual data in twisted format to multiple cloud servers. As preventive measures, the proposed system presents homomorphic encryption, searchable encryption, CRH and Block Management approaches. Homomorphic encryption combination prepares a dataset for secure outsourcing by splitting and combining into fixed length blocks. Block Management decides which combined blocks to be outsourced to which cloud server so that no individual cloud can retrieve the original data or a piece of data. Finally, CRH supports the detection of any modification. Unlike the prior scheme, the proposed scheme encrypt and twists the data before outsourcing no cloud server gets a smaller piece of data in plain text format. Security analysis proves that it is computationally hard to extract plain text from a combined block. Similarly, it overcomes the collision of a hash function (if any) with high probability and detects almost any malicious detection.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Communications of the ACM, vol. 53, no. 6, p. 50, 2010.

[2] X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, "Knowledge-aware proactive nodes selection approach for energy management in Internet of Things," Future generation computer systems, 2017.

[3] Y. Liu, A. Liu, S. Guo, Z. Li, Y.-J. Choi, and H. Sekiya, "Context-aware collect data with energy efficient in Cyber–physical cloud systems," Future Generation Computer Systems, 2017.

[4] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (SDN) and cloud computing environments," in Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 2969-2974: IEEE.

[5] B. Martini and K.-K. R. Choo, "Distributed filesystem forensics: XtreemFS as a case study," Digital Investigation, vol. 11, no. 4, pp. 295-313, 2014.

[6] N. D. W. Cahyani, B. Martini, K. K. R. Choo, and A. Al-Azhar, "Forensic data acquisition from cloud of things devices: windows Smartphones as a case study," Concurrency and Computation: Practice and Experience, vol. 29, no. 14, 2017.

[7] J. Fu, Y. Liu, H.-C. Chao, B. Bhargava, and Z. J. I. T. o. I. I. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," 2018.

[8] C. F. Tassone, B. Martini, and K. K. R. Choo, "Visualizing digital forensic datasets: a proof of concept," Journal of forensic sciences, vol. 62, no. 5, pp. 1197-1204, 2017.

[9] C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," Computer Law & Security Review, vol. 29, no. 2, pp. 152-163, 2013.

[10] D. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix," Future Generation Computer Systems, vol. 78, pp. 558-567, 2018.

[11] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study," Computers & Electrical Engineering, vol. 58, pp. 350-363, 2017.