THE DESIGN OF SECURE CLOUD STORAGE SCHEME BY USING FOG CENTRIC

Mr.P.Bhaskar, M.Tech, Assistant Professor
Department of Computer Science and Engineering
Santhiram Engineering College, Nandyal, A.P, India.

***Abstract* – Cloud computing has a powerful storage capacity. Every internet users have his/her own cloud to store their data. Most of the users are interested to store their privacy data in the cloud. Local storage doesn't fulfil the requirements so the users switched to another medium to protect their data. Privacy breach, malicious modifications, are the cyber threats to the cloud computing. For this reason recently we introduced a fog based three layered server (1,2,3) to protect the data from unauthorized users by employing multiple clouds. To prevent the data from illegal access we proposed a new technique using XOR - BLOCK management to split the data into multiple blocks. We can protect and retrieve the data from multiple sources using this technique. Moreover i can use Reed Solomon Code and Hash digest centric customized algorithms.**

***Index Terms*-Cloud Server, Fog Server, XOR-combination, CRH privacy**

I. INTRODUCTION

The word cloud computing was introduced in Search Engine Strategies and defined formally by National Institute of Standards and Technology(NIST).Cloud computing has many functionalities and cloud storage techniques are becoming increasingly important due to rise in volume of user's data and it depends on network bandwidth. The data is ranging from GB's to TB's. As we know in earlier days local storages doesn't reach up to the level and they failed to satisfy the users. People have inherent need to access their data so they are interested to search for other mediums. Storing the data in a public cloud will become a trend in coming future getting inspired from the fact many organizations like Google Drive, Dropbox, cloud provides a different storage services to the users.The main advantage are combined with cyber threats in cloud computing. Privacy is one of the major issue in addition to the loss of data, server crash are some of the cyber threat examples. We have some important cyber incidents occurred in the history. For example yahoo three billion accounts exposure by hackers in 2013, Apple's Cloud leakage in 2014.

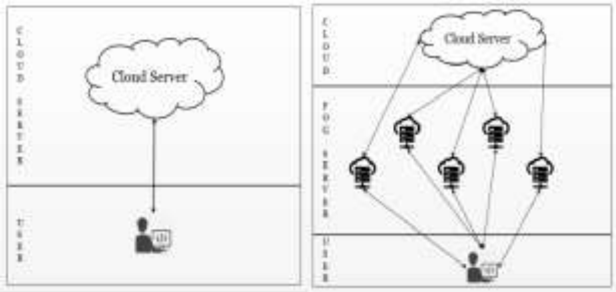
In the case of traditional computing once the user outsources his data to access they can't protect the data physically. Cloud Service Provider is used to search, access, and modify the data at the same time it losses a small portion of data due to some technical faults. This gives a chance for the hacker to violate the user's privacy data by using some cryptographic mechanisms (such as encryption, hash, chain).Though, how much we improve the algorithms it doesn't even matter because it cannot prevent the internal attacks..To protect the data from confidentiality, integrity, availability, we proposed a fog based devices in between users and cloud servers. By doing more recent works in this field Wang et.al utilized Reed Solomon code and Hash digest centric customized algorithms to preserve confidentiality and integrity of the data. We also use computational intelligence (CI) to determine the portion of data to be stored in the cloud. They maintained a rating system for the cloud servers so that users can rate the cloud servers and they tend to act responsively. We proposed a fog based cloud storage scheme. To provide confidentiality, and availability, we use XOR combination to split the data into multiple blocks. Block Management technique is used to protect the data and retrieve it from multiple resources to maintain privacy and to prevent the data loss.

II. LITERATURE SURVEY

After doing lots of research and surveys, Zissis et al evaluated cloud security by uniquely identifying the security requirements with the trusted third parties(TTP).They use public key cryptographic tools to ensure confidentiality, integrity and authenticity of data. Wang et.al focused on integrity protection on cloud computing and proposed public audit ability scheme. They set two goals like one was the efficient public auditing without requiring local copy of data and the other one was not to cause any vulnerability of the data. To preserve the public auditing of cloud data they utilized homomorphism authenticator.

Xia et al. proposed a content based image retrieval(CBIR) to protect the image outsourced to the cloud server using locality sensitive hashing and K-nearest neighbouring algorithms. It preserves privacy of sensitive images and ensures efficient retrieval but does not guarantee integrity or elimination of an image. All introduced a cloud infrastructure for urbanization and to share the data to the urban people from the cloud. Attribute Based Encryption is used to protect the privacy of shared data. As we discussed previously are commonly related to integrity preservation by various public/private auditing frameworks. On the other hand privacy is protected by encryption though it makes searching operation very difficult. After all these research et al. Proposed a new scheme of cloud storage resorting to a fog server to protect the data against different attacks. A three layered architecture kept the fog server in between the cloud server and the users. Considering fog server being trusted by the user, they presented a Nobel scheme preservation, modification detection, and data loss prevention. They encode the data utilizing Reed-Solomon code and deduce Computation Intelligence (CI) to determine the amount of data to be outsourced to cloud/fog servers so that no individual cloud server can reconstruct the data. On the other hand Malicious Modification detection is used to detect the malicious data which has no advantage over traditional hashing algorithms to detect malicious modification. We undertook the similar work with the same architecture by using fog based solutions for secure based cloud storage and importantly to protect against the cyber threats. The authors propose a secure cloud storage scheme on the basis of fog server considering Tian et al.'s scheme as the benchmark.

III. PROBLEM FORMULATION



a.Traditional cloud b.Fog based cloud

Fig. 1. Comparative computing architecture

1 *SYSTEM MODEL*

Fig. 1(a) Outsourcing data to the cloud may breach the privacy of the data. There are situations where large amount of data gets accumulated from a particular location and is processed in real time to generate some result Sending data to a centralized infrastructure may cause transmission delays. Fog computing can resolve the issue and it is a smaller version of cloud computing placed in between cloud servers and users. Fig 1(b) shows the fog based cloud storage device and it communicates with multiple clouds .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.

2. *THREAT MODEL*

Cyber threats can be classified into three categories: Privacy breaches, malicious modification and data loss. Once data is entered into the cloud server, user cannot protect it any more. Apart from saving data in cloud storage, cloud computation requires data as data is an essential part of computation. Thus, whenever cloud server gets data, the privacy of data can be jeopardized by internal employees of the cloud. Alternatively, an external attacker can attack cloud server to violate the privacy of the user data. In either case, privacy of data is susceptible to internal and/or external attackers. Inside/Outside attacker can modify the sensitive data intentionally it may appear false data to right. Cloud server can hide data intentionally which may result in permanent data loss of the user and it also crash causing the data loss from the server. The above mentioned threats overcome by using fog based techniques.

IV.IMPLEMENTATION

A. MODULES

1) User

User is the owner of data. Privacy, disaster recoverability, modification detection of user's data is ultimate goal .It has only certain permissions to act.

2) Fog Server

Fog server is trusted to user. User relies on fog server with his data. Close proximity of fog devices to the user, robust physical security, proper authentication, secure communication, intrusion detection ensures fog server's reliability to the user. It is a third party authorizer to give permissions to the cloud server.

3) 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. Cloud server may pretend to be good but acts as a potential adversary. In that case, cloud server may modify data in order to forge as original data. Similarly, cloud server may hide/loss the data resulting in permanent data loss of the user. Furthermore, hardware/software failure may result in data modification or permanent loss as well.

V.PROPOSED A FOG BASED SECURE COUD STORAGE SCHEME

To enhance the credibility of cloud in the proposed scheme, fog server, furnished with some computing, storage and communication capabilities, is assumed to be reliable for the user. Reliable fog computing can be implemented by employing proper authentication, access control and intrusion detection mechanism. Close proximity of fog device to the user enhances its credibility as a secure computing infrastructure. Apart from the fog computing, proposed scheme utilizes its own techniques $Xor - Combination$, $Block$ – $Management$ and $Collision\ Resisting\ Hashing$ (CRH) to preserve privacy, ensure recoverability and to detect data modification for the data deployed in the cloud storage. By utilizing the cryptographic techniques cloud storage can combat external attacks and data becomes more vulnerable to the inside attackers when the cloud server turns itself into malicious adversary. Fog device outsourcing a smaller part of data to different cloud servers making it in a plain text format may lead to susceptible leakage of data. Conversely, we split data into smaller blocks using *Xor-Combination* before outsourcing to multiple clouds.$Xor - Combination$ conceals original content and ensures full data recovery even in case of malignant (or non- malignant) data loss from some cloud servers. we propose a noble technique of CRH that intends to minimize collision of a hash function. A proposed scheme aims to protect privacy, ensure recoverability and to detect malicious modification. For this purpose, fog centric architecture resorts to three techniques: $Xor - Combination$,$Block - Management$ and CRH. Particularly, $Xor - Combination$ plays an important role to preserve privacy and to reconstruct data if many portions of it is missing. On the other hand, CRH contributes to detect any malicious modification of data even if the underlying hash function fails to resist collision.

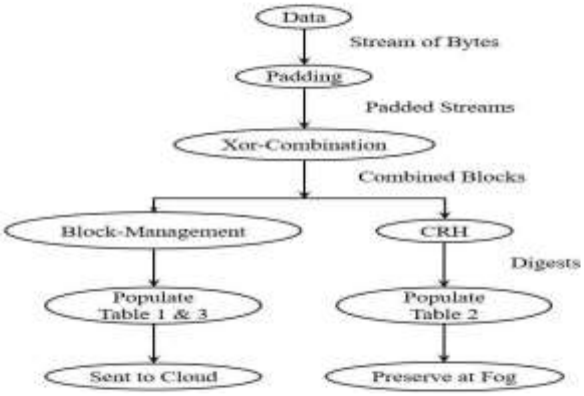


Fig. 2. Data processing flow

Fig. 2 illustrates the steps of data processing before outsourcing data to the cloud's storage. 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.

It pads the data if the data is not (exact) multiple of fixed length (L) block. Afterwards it executes *Xor-Combination* on the padded data which results in number of 2-block-combinations and n number of 3-block-combinations.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 .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 with the random number R.

A) Storing Procedure

Storing procedure takes a file to be uploaded to cloud server securely. 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.

B)Splitting File

Fog server pads the files. After that fog server splits the file into several fixed length blocks and combines them using $Xor-Combination$ algorithm. At the end of this step, we get two sets of 2-block-combinations and 3-block- combinations together known as $combined\ blocks$.

C) Integrity Processing

For each $combined\ block$, fog server generates random number, hash digest and random hash digest using CRH processing algorithm and stores this information into fog database for future purpose of checking.

D) Block Management

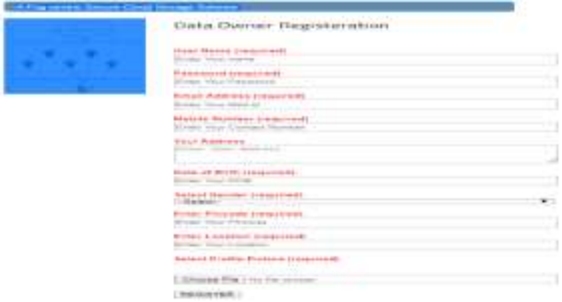
Fog server determines which block to be stored to which cloud server using $Block - Management$ technique, stores this metadata into fog database and sends the blocks to respective cloud servers.

E) Cloud Storage and Retrieval

Cloud server receives and stores the blocks along with metadata into its storage. It 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.

VI.RESULTS

A Fog centric Secure Cloud Storage Scheme
Upgrading to a Cloud Server
Menu


Data Owner Registration

User Name (required)
Password (required)
Email Address (required)
Mobile Number (required)
Your Address
Date of Birth (required)
Select Gender (required)
Enter Pincode (required)
Enter Location (required)
Select Profile Picture (required)
Choose File
REGISTER

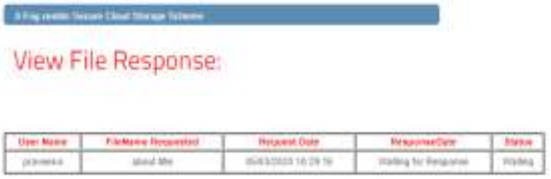
Data Owner Login

Submit

End User Login

Name (required)
vahaje
Password (required)
Submit

Hi Mr.praveena ur request sent to Cloud Server

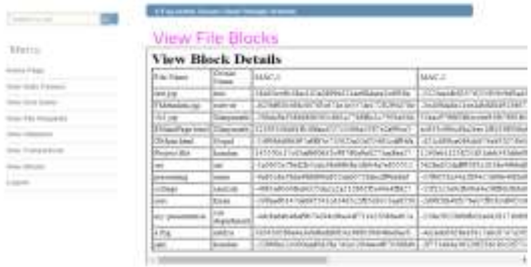

View File Response:

User Name	FileName Requested	Request Date	ResponseDate	Status
praveena	[illegible]	[illegible]	Waiting for Response	Waiting

Fog Server1 Login

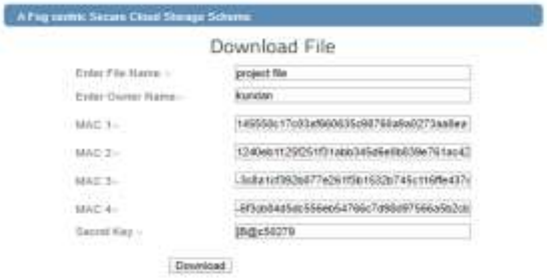
Name (required)
fogserver1
Password (required)
Submit

File Name	Owner Name	[illegible]	Status
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]



View Block Details

File Name	Owner Name	MAC 1	MAC 2
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	kundan	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]



Enter File Name :- project file

Enter Owner Name:- kundan

MAC 1:- 145658c17c03af660635c98768a6a0273aa8ea

MAC 2:- 1240eb1129f251f31abb345d6e8b639e761ac42

MAC 3:- -3cfa1cf992b677e261f5b1632b745c116ffe437c

MAC 4:- -6f3db84d5dc556eb54766c7d98d97566a5b2cb

Secret Key :- [B@c50279

VII.CONCLUSION

Fog based three-layer architecture befits to a secure solution for robust cloud storage against cyber threats. A trusted fog server puts the actual data in twisted format to multiple cloud servers. It presents $Xor - Combination$, CRH and $Block -Management$ approaches. $Xor - Combination$ prepares a dataset for outsourcing by split and combining into fixed length blocks. At the same time, $Xor - Combination$, along with $Block -Management$, contributes to reconstruction of any data block in case of malicious modification or data loss. Finally, CRH supports the detection of any modification.

VIII.FUTURE ENHANCEMENT

- It enhances the efficiency of fog based secure storage devices regarding to time and memory usage.
- It improves the fog based server security robustly by using strong cryptic techniques and to enable the cloud server to cryptic data without revealing information.

REFERENCES

[1] 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.

[2] 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.

[3] T. Wang et al., "Fog-based storage technology to fight with cyber threat," Future Generation Computer Systems, 2018.

[4] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, and Y. Liu, "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing," IEEE Transactions on Emerging Topics in Computational Intelligence, 2018.

[5] T. Wang et al., "Data collection from WSNs to the cloud based on mobile Fog elements," Future Generation Computer Systems, 2017.