IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fog Buckler

Amol Jamdhade
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India

Anam Khan
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India

Shital Ilag
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India

Rushikesh R.Nikam
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India

Abstract - Recently, a fog server architecture has been presented for secure storage. In today's era for storage services cloud computing is now being utilized but in its widespread adoption, the most challenging issue is related to the security of the cloud storage. Against cloud storage security threats there are many issues like Privacy issue, malicious modification, data alteration and data loss. Therefore, fog servers are used to protect the data against unauthorized access and provide the data security. In order to achieve milestone, the different techniques which are used is hash code and hash algorithm which may resulted in minimum amount of data loss to cloud servers and failed to provide better data recoverability and modification detection. Here a fog based secure cloud storage system is built to protect data against unauthorized modification, and destruction created by attackers even unauthorized access to data is prevented. To prevent illegitimate access, the proposed scheme employs a new technique Xor - Combination to conceal data. For updating and altering we offered a technique based on hash algorithm for feasible modification. To prevent malicious retrieval Block - Management is also used for better recoverability in case of data loss. Simultaneously, by analyzing security issues, we are providing robustness in the proposed system through encryption. Test cases validate performance supremacy of the proposed system.

1. INTRODUCTION

Cloud computing has many functionalities and cloud storage technique is becoming increasingly important for growing volume of data.

Volume of user's data is rising exponentially with the rise of network bandwidth [1]. Almost every internet user has his/her own cloud storage ranging from GB's to TB's. Local storage fails to fulfil this immense storage requirement alone. Most importantly, people have inherent need for ubiquitous access to their data.

Consequently, people are finding new mediums to store their data. Giving preference to powerful storage capacity, a growing number of users have switched to cloud storage; they even prefer to save their private data to the cloud. In near future commercial public cloud server will be a prevalent trend for storing data. There are so many organizations, which are proving a variety of storage and security services to their end users. For examples Dropbox, Google Drive, iCloud are providing a variety of storage services to their users. With all these advantages there a possibility of cyber treats and data loss [2-4]. Privacy issue is one of the major threats in addition to loss of data, malicious modification, server crash are some examples of cyber threats.

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. Hacker may violate the privacy of the user data due to some issue because it is possible that CSP may loss the data because of some kind of technical problem. Confidentiality or integrity of the data can be protected by using cryptographic mechanisms (such as encryption, hash chain) [5], However, internal attacks cannot be prevented by cryptographic approach. 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. Nonetheless, this scheme reveals that some portion of data (not the entire data) to the cloud and their customized hash algorithm, despite taking extra computation/storage overhead, adds no value over standard hash algorithm (i.e. MD5) in terms of collision resistance. In this paper, we propose a fog-based cloud storage scheme for data confidentiality, integrity and availability. For confidentiality and availability (even after malicious events), we propose a method referred to as Xor - Combination that splits the data into several blocks, combine multiple blocks using Xor operation and outsource the resulted blocks to different cloud/fog servers. In order to prevent any individual cloud server to retrieve a portion of original data, the proposed technique Block – Management selects the cloud server to store each particular data blocks. Xor - Combination along with Block – Management helps to protect data and to retrieve data from multiple sources even when some blocks are missing. Based on traditional hash algorithm (i.e., SHA256, MD5) we proposed hashing mechanism entitle as Collision Resolving Hashing (CRH) operation for security features [6]. The proposed scheme thrives to be a robust solution for efficient and secure cloud storage.

2. FOG COMPUTING

Cloud computing is a sophisticated technology used to cater computing, storage and communication service over the internet with flexibility and efficiency. Nonetheless, there are cases where massive amount of data spanning in a large geographical area needs to be stored, processed and analyzed efficiently. Furthermore, privacy guarantee of the collected/processed data is sometimes critically important. To fulfil the gap, the concept of fog computing emerged which is able to extend cloud computing in more proximity to the user that it serves. In contrast with cloud, fog computing can provide computing and storage facilities at the edge of the network, hence, it is alternatively called edge computing.

A fog node can be any network device with the ability to handle data over network, network connectivity (i.e., routers, switches, cameras, servers, etc.). Privacy and security issues in fog computing induce. The security and privacy issues can be mitigated by counter technologies mentioned such as proper authentication, access control, secure channel, intrusion detection, trust management. While all these techniques are in place, fog computing can be considered as a trusted device upon which the users can rely for processing, storing and managing data. This paper presents fog computing as a trusted device. On the basis of fog computing, the present research proposes a secure cloud storage scheme.

3. FOG BASED SECURE CLOUD STORAGE

Security is one of the essential features of cloud computing. Furthermore, security of data is the prime need for cloud storage and it comprises of data privacy, integrity and availability. To enhance the credibility of cloud, data security has always been the focus of research of relevant research community. At the same time, users are more concerned with the security of the outsourced data to the cloud. Hence, cloud with more security degree will attract more clients. Therefore, both research and business communities are testing the boundaries of cloud security. At the center of cloud data security, there are three aspects: confidentiality, integrity and availability. We address these issues of cloud storage using fog-based scheme referring the three issues as privacy protection, modification detection and recoverability respectively. In this section, we will elaborate how the proposed scheme works to preserve privacy, detect malicious modification and to ensure recoverability.

4. EXISTING SYSTEM

Zissis et al. After checking security requirement and solution by trusted third party we assess cloud security. As underlying cryptographic tool, they used public key cryptography to ensure confidentiality, integrity and authenticity of data and communication while addressing specific vulnerabilities [7]. Wang et al. focused on integrity protection on cloud computing and proposed public auditability scheme as a counter measure [8]. They set two goals of their work, 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. They utilized homomorphic authenticator with random masking for privacy preserving public auditing of cloud data.

Xia et al. proposed a mechanism titled Content Based Image Retrieval (CBIR) to protect image outsourced to cloud server relying on locality sensitive hashing (LSH) and secure k-nearest-neighbors (KNN) algorithms [9]. It is equally applicable to other data types (i.e., text) as well. It preserves privacy of sensitive images and ensures efficient retrieval but does not guarantee integrity or elimination of an image (or other type of data). Arora et al. enlisted and compared some cryptographic primitives for preservation of privacy and integrity of cloud storage [10]. This comparison is also befitting for other computing architecture. One recent work reported by Shen et al. used cloud infrastructure for urbanization. Their proposal illustrated cloud to share data between urban people and/or applications. To protect privacy of shared data they used attributed based encryption (ABT).

Disadvantages:

In the existing work, there is no Data Recoverability.

The system's security is very less due to lack of strong cryptography techniques.

5. PROPOSED SYSTEM

The proposed a secure cloud storage scheme based on fog computing employing Xor - Combination, Block-Management and CRH operation. Xor - Combination together with Block - Management contributes to maintain privacy and to prevent data loss. CRH Operation ensures detection of data modification.

Analysis proves the guarantee of privacy, data recoverability, and alteration of the proposed scheme.

The system implemented a prototype version of the scheme and conducted experiments to verify its performance in comparison with the contemporary scheme. Results prove its efficiency in terms of time and memory usage.

Advantages:

The data owner is totally trusted and will never be corrupted by any adversaries.

The system is more secured due to Sensitive data outsourced to the cloud is susceptible to the inside or outside attacker. Hence, information leakage takes place. Encryption can protect such leakage.

Use Case Diagram:

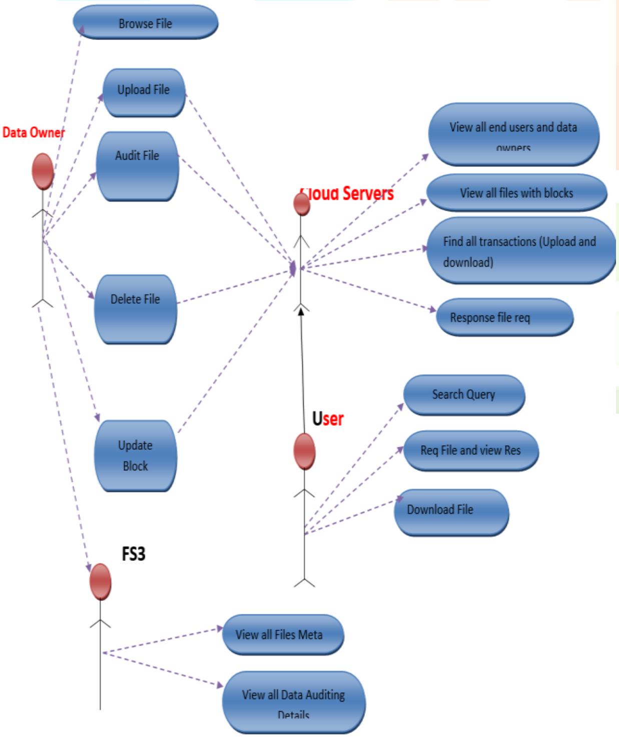

Fig 2. Use case

Above figure shows the Use Case Diagram which is a depiction of the interactions among the elements of the System.

6. PERFORMANCE EVALUATION

The proposed system provides user flexibility to store and access the data from the cloud and the security is provided to that data. The performance check of implemented models is done as follows

A. Performance

Expected: There must be a proper output given by server to the end users and the security to the data should be provided by the system.

Observation: There is proper output given by server to the end users and also the security to the data is provided by the system.

B. Test Case

Table 1. Test Case

Module Name	Expected Output	Actual Output
Data Owner	Proper Encryption of data should be done.	Encryption takes place properly.
End User	While searching the particular file, user should know whether the file is available or not by particular owner.	User can search a file using keyword. Also know whether the file available or not by owner.
Cloud Server	To check whether the file is divided into four blocks or not with secret key generation.	Files are divided into four blocks with proper secret key.
Fogserver1	Whether it is suitable to permit a particular file request.	File request with no risk of attack will be permitted.
Fogserver2	View all registry details related to cloud server and fogserver1.	All files can be viewed.
Fogserver3	Information about all the data should be given.	Metadata related to data is given.

7. CONCLUSION AND FUTURE SCOPE

The emergence of cloud computing has brought numerous advantages to the computing arena. The storage service is excellent unless users outsource their sensitive data to cloud storage server. Cloud server gets full access and control over user's data once data is outsourced to the cloud. It can read or search through the user's data. On the other hand, data can be permanently damaged by many cyber-attacks and cloud hardware or software malfunction. Three-layer architecture based on Fog gives secure solution to this problem to the robust cloud storage against malfunctioning and threats. We offered a system that undertakes preventive measures to a trusted fog server and puts the actual data in contorted format to different cloud servers. As preventive measures s, this paper presents Xor - Combination, CRH and Block - Management approaches. Xor - Combination prepares a dataset for outsourcing by splitting and combining into fixed length blocks. As encryption is vulnerable to cracking and causes computational overhead, the proposed scheme does not rely on encryption technology. 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. At the same time, or - 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. Unlike the prior scheme, the proposed scheme twists the data before outsourcing it to cloud using Xor - Combination so that no cloud server gets a smaller piece of data in plain text format. Similarly, Xor - Combination enables better data recoverability and CRH facilitates integrity checks almost with certainty. Security analysis proves that it is computationally hard to extract plain text from a combined block which is outcome of Xor - Combination. Similarly, CRH overcomes the collision of a hash function (if any) with high probability and detects almost any malicious detection. Extensive comparative experiments indicate that its performance is effective as compared to the prior schemes. Future work in this domain can be summarized as follows:

1. To enhance the efficiency of fog-based cloud storage service.
2. To improve the security of fog server for a robust fog centric cloud computing infrastructure.
3. To enable cloud server to compute cryptic data without revealing any information from it.

8. Acknowledgment

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of research project.

I am also thankful to principal Dr. Prashant Deshmukh and management of NHITM for their support and encouragement. I am highly indebted to my Head of Department Dr. Sanjay Sharma and guide Mr. Rushikesh R. Nikam for providing us their helping hand and positive feedback during complete preparation of this project with constant supervision and support.

I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project.

I am thankful to the review committee for their valuable suggestion and feedback. I also thank laboratory staff for their valuable support. Last but not the least, I sincerely thank to those from teaching and non-teaching staff from NHITM who were somehow attached with my endeavor.

9. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

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

[7] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation computer systems, vol. 28, no. 3, pp. 583-592, 2012.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Infocom, 2010 proceedings ieee, 2010, pp. 1-9: Ieee.

[9] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," Information Sciences, vol. 387, pp. 195-204, 2017.

[10] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," International journal of engineering research and applications, vol. 3, no. 4, pp. 1922-1926, 2013.