Journal of Engineering Sciences
Vol 13, Issue 06, June/2022
ISSN NO:0377-9254

A FOG-CENTRIC SECURE CLOUD STORAGE SCHEME

[1]Prathyusha Muthukur,[2]Shaik Misbah Nurein
[3]Leena Goyal Dudekula,[4]Y. Prashanthi
[5]Kadire Meghana
[6]M Janardhan
[1,2,3,4,5,]STUDENT [6] ASSISTANT PROFESSOR
G PULLAIAH COLLEGE OF ENGINEERIONG AND TECHNOLOGY -KURNOOOL

ABSTRACT

Cloud computing is now being utilized as a prospective alternative for catering storage service. Security issues of cloud storage are a potential deterrent in its widespread adoption. 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. The underlying techniques used are Hash-Solomon code and customized hash algorithm in order to attain the goal. However, it resulted in loss of smaller portion of data to cloud servers and failed to provide better modification detection and data recoverability. This paper proposes a novel fog-centric secure cloud storage scheme to protect data against unauthorized access, modification, and destruction. To prevent illegitimate access, the proposed scheme 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. We demonstrate robustness of the proposed scheme through security analysis. Experimental results validate performance supremacy of the proposed scheme compared to contemporary solutions in terms of data processing time.

I. INTRODUCTION

CLOUD computing, a prominent computing paradigm was introduced in SES 2006 (Search Engine Strategies 2006) and was formally defined by NIST (National Institute of Standards and Technology) [1] in 2009. Since then, this technique has resulted in attracting increased market share with its powerful computing, storage and communication facilities [2, 3]. Its infrastructure resources are not only scalable on demand but also available at an economical price following convenient payment policy, pay as you go. Along with individual and enterprise customers, cloud computing also draws attention of many research communities who exert massive efforts towards its gradual maturity. Hence, 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

[4]. 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. Storing data on a commercial public cloud server will be a prevalent trend in the near future. Getting inspired by the fact, many organizations, such as Dropbox, Google Drive, iCloud and Baidu cloud are providing a variety of storage services to their users. However, advantages of cloud storage are accompanied with a set of cyber threats [5-8]. Privacy issue is one of the major threats in addition to loss of data, malicious modification, server crash are some examples of cyber threats. There are some prominent cyber incidents in the history, for example, Yahoo's three billion accounts exposure by hackers in 2013, Apple's iCloud leakage in 2014, Dropbox data privacy breach in 2016, particularly iCloud's leakage event, where numerous Hollywood actresses' private photos were exposed and caused massive outcry. Such incidents affect company's reputation fervently [9-11].

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 [12]. However, cryptographic approach cannot prevent internal attacks, no matter how much the algorithm improves [13]. 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. One of the prominent and recent works in this field is proposed by Wang et al. They utilized $ReedSolomoncode$ and hash digest centric customized algorithms to preserve confidentiality and integrity of the data respectively [12]. They also formulated the computational intelligence (CI) to determine the portion of data to be stored in cloud, fog and user's local machine. They maintained a rating system for cloud server so that user can rate the cloud servers and the cloud servers tend to act responsively. 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. At the same time, we propose a noble hashing mechanism titled as $CollisionResolvingHashing$ (CRH) operation based on traditional hash algorithm (i.e., SHA256, MD5) that withstands collision in hashing [14] and security features. The proposed scheme thrives to be a robust solution for efficient and secure cloud storage.

II.EXISTINGSYSTEM

Zissis et al. evaluated cloud security by identifying unique security requirements and presented a conceptual solution using trusted third party (TTP). As underlying cryptographic tool they used public key cryptography to ensure confidentiality, integrity and authenticity of data and communication while addressing specific vulnerabilities [21]. Wang et al. focused on integrity protection on cloud computing and proposed public auditability scheme as a counter measure [22]. 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 [24]. 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 [25]. 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 [26]. 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.

III.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. CRHOperation ensures detection of data modification.

Theoretical security analysis proves the privacy guarantee, data recoverability, and modification detection 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 corruptedby any adversaries.

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

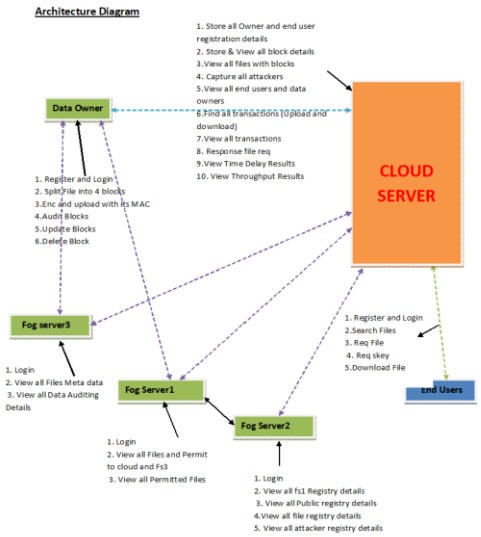
IV.SYSTEMREQUIREMENTS

➢H/W SystemConfiguration:-

➢Processor	- Pentium–IV
➢RAM	- 4 GB(min)
➢Hard Disk	- 20 GB
➢KeyBoard	- Standard Windows Keyboard
➢Mouse	- Two or ThreeButton Mouse
➢Monitor	- SVGA

Software Requirements:

- ➢ Operating System - Windows XP
- ➢ Coding Language - Java/J2EE(JSP,Servlet)
- ➢ Front End - J2EE
- ➢ Back End - MySQL



V.IMPLEMENTATION

User: User is the owner of data. Privacy, disaster recoverability, modification detection of user's data is ultimate goal of this paper.

FogServer: 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.

CloudServer: Cloud server is considered as $honestbutcurious$. This means that cloud server follows the Service Level Agreement (SLA) properly, but has an intention to analyze user's data. Conversely, 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.

VI.CONCLUSION

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. Moreover, data is susceptible to many cyber-attacks and cloud hardware or software malfunction may damage the data permanently. Fog based three-layer architecture befits to a secure solution for robust cloud storage against cyber threats. This article proposed 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 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 $combinedblock$ 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.

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.