ENHANCING DATA PRIVACY IN CLOUD STORAGE: A THREE-LAYER FRAMEWORK WITH FOG COMPUTING

P. Kavitha
Assistant Professor, Department of Computer Applications,
Annamacharya Institute of Technology and Sciences (Autonomous), Rajampet
Ph No: 9703489363
Email-id: kavithapaleti@gmail.com

Abstract

In the recent years, there have been notable advancements in cloud computing technology, driven by the escalating volume of unstructured data. This has resulted in heightened attention and improved development of cloud storage technology. Despite these advancements, the current storage approach entails the complete storage of user data on cloud servers, relinquishing users' control and exposing them to privacy risks. Commonly, traditional privacy protection methods rely on encryption technology; however, these approaches often fall short in effectively resisting internal attacks within the cloud server. To address this challenge, I suggest a storage framework comprising three layers with a focus on fog computing. This inventive framework efficiently leverages cloud storage while ensuring the Data confidentiality. Furthermore, our algorithm 'HashSolomon code' is crafted to partition data into separate segments, facilitating the secure storage of a portion on local machines and fog servers for enhanced privacy protection. Furthermore, leveraging computational intelligence, this algorithm calculates the distribution ratio of data stored in the cloud, fog, and local machines, individually. The proposed scheme's feasibility has been confirmed through theoretical safety analysis and experimental evaluations, establishing it as a robust complement to existing cloud storage schemes.

Keywords:

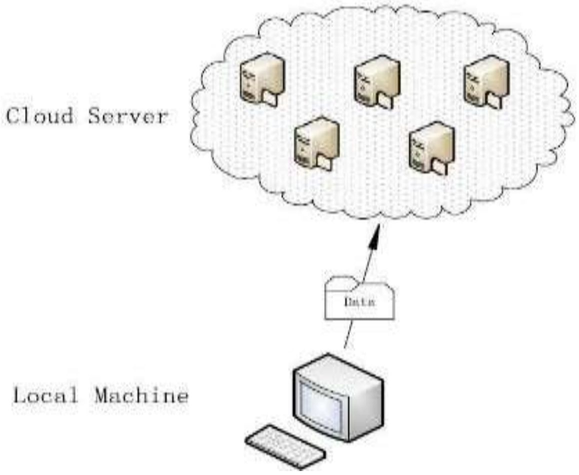
Cloud Technology, Unstructured Data, Cloud Storage Advancement, Privacy Protection Fog Computing, Computational Intelligence.

I INTRODUCTION

In the 21st century, computer technology has experienced rapid progress. Cloud computing, a nascent technology introduced during SES 2006 in San Jose and defined by NIST, enables the maintenance, management, and backup of data irrespective of its location. This innovative approach to computing has become a cornerstone in contemporary technology, offering versatile solutions for data handling and storage, marking a significant milestone in the evolution of computing paradigms.

With the exponential increase in user data due to the rapid development of network bandwidth, the capacity of local machines is no longer sufficient to meet user requirements. Consequently, people are seeking alternative methods to store their data. A growing user base is adopting cloud storage due to its expanded capacity, marking a rising trend towards storing data on public cloud servers in the foreseeable future.

As a component of cloud computing systems, cloud storage provides services for data storing as well as management. Utilizing applications, network technology, distributed file system technology as well as cloud storage enables various storage devices to work together cohesively. Numerous companies, including Google Drive, Drop box etc provide diverse cloud storage services with large storage capacities, attracting a significant number of subscribers and achieving success.



However, cloud storage services still face security challenges, with privacy concerns being particularly notable among these issues. Typically, users directly upload data to the cloud instance, allowing the Cloud Service Provider to take over data management. Users lack control over data storage, leading to a gap between ownership and management. The Cloud Service Provider has unrestricted access, raising the risk of loss and data leakage. Conventional secure solutions for cloud storage predominantly focus on imposing access restrictions to address these concerns. However, the existing solutions prove inadequate in effectively addressing internal attacks, regardless of algorithmic improvements. Consequently, I suggest a Three Layer Storage (TLS) plan rooted in a fog computing model, integrating a Hash-Solomon code with the application of Computational Intelligence.

Fog computing expands upon the cloud computing model and includes multiple fog nodes, each equipped with processing capabilities and storage capacity. In this approach, I have divided user data into three segments, housing them individually on the user's local machine, cloud server and fog server. Moreover, the Hash-Solomon code's attributes guarantee the impossibility of recovering the original data solely from partial data. Further-more, employing the Hash-Solomon code generates redundant data blocks used in the decoding process. While increasing redundant blocks enhances storage reliability, it also leads to additional data storage requirements. Through judicious data allocation, this scheme effectively safeguards user data privacy. The Hash-Solomon code involves complex calculations, which Computational Intelligence (CI) assists in. Compared to conventional methods, this scheme offers superior privacy protection against internal threats, particularly from Cloud Service Providers (CSPs).

II. PROCEDURE

1. **Storage Procedure:** When a user intends to store a file on the cloud server, the process unfolds as follows: Initially, the user's file undergoes encoding using Hash-Solomon code. Subsequently, the file is segmented into multiple blocks of data and the system concurrently provides encoded information. Approximately 1% of the data blocks and the encoding information are stored locally, with the remaining 99% of data blocks being uploaded to the fog server.

Subsequently, after obtaining the 99% data blocks from the user's machine, these blocks undergo a secondary Hash-Solomon encoding process. These segments undergo further division into tiny data blocks, creating new encoded information. Analogously around 4% of the data blocks and corresponding encoding details are kept within the fog server, while the remaining 95% of data blocks are sent to the cloud server. Finally, when the cloud server receives the data blocks from the fog side, a cloud management system allocates these blocks accordingly. The storage procedure concludes when all relevant information is recorded in different servers.

2. **Download Process:** When a user wishes to retrieve their file from the cloud server, the process unfolds in the following manner:
   - The user's request is received by the cloud server, which then compiles data from diverse distributed servers. Following integration, 95% of the data is transmitted to the fog server.
   - The fog server receives the data sent by the cloud server. By utilizing both the 4% data blocks sourced from the fog server and the corresponding encoding information, it becomes feasible to reconstruct 99% of the data. The fog server then returns the 9% reconstructed data to the user.
   - The fog server send the data to user and by iteratively following the above steps, the user can successfully retrieve the complete dataset.

III RELATED WORK

The significance of cloud storage security has generated substantial interest in academic and industrial domains. Recent years have witnessed numerous studies exploring secure cloud storage architectures. Shen et al. advocate for a semi-trusted cloud and propose an urban data sharing framework using attribute-based cryptography, deemed secure against potential attacks. Hou, Wu, Zhen, and Yang stress security and privacy as the core of cloud storage, proposing a secure virtual protection scheme based on SSL. However, encryption methods like SSL pose challenges for cloud search, leading to a surge in interest in searchable encryption. Various approaches in this area prioritize accuracy, security, and efficiency. Shen Wei et al. highlight a gap in previous works, noting a focus on storage security over computation security in cloud security research. Atan R et al. contribute a two-layer secure framework with distinct agents, representing advancements in privacy protection through diverse encryption policies, auditing, and secure framework development. However, a common flaw exists in these studies: their vulnerability when the Cloud Service Provider (CSP) is untrusted. To overcome this constraint, I introduce an innovative secure cloud storage solution. By employing specific codes to divide files and integrating them with a TLS framework based on a fog computing model, this scheme ensures a high degree of data privacy. It is essential to note that this approach does not discard encryption technology; rather, encryption plays a crucial role in safeguarding the fine-grained security of the data in this scheme.

IV SECURE CLOUD STORAGE BASED ON FOG COMPUTING

The security level serves as a vital indicator for evaluating the effectiveness of a cloud storage system. Additionally, data security constitutes a pivotal component of cloud storage security, encompassing three crucial aspects: data privacy, data integrity, and data availability.

Ensuring the privacy and integrity of data has consistently been a focal point in relevant research. From the user's perspective, data privacy holds particular significance, and, from a business standpoint, a company boasting a high security level is likely to attract a larger user base. Consequently, enhancing security is a pivotal objective in both academic and business domains.

A. Fog Computing the suggested approach is based on the fog computing model, an extension of cloud computing introduced by Cisco's Bonomi in 2011. Unlike the concentrated nature of cloud computing, fog computing is positioned closer to the edge network, offering benefits such as broader geographical distribution, enhanced real-time capabilities, and reduced latency. Considering these characteristics, fog computing is especially well-suited for applications that require minimal delays. Additionally, fog computing nodes possess storage capacity and data processing capabilities, distinguishing them from sensor nodes and enabling simple data processing, especially for geographically-based applications. Consequently,Computational Intelligence (CI) can be implemented on the fog server for computational tasks.

Fog computing commonly adheres to a three-tiered architecture. At the pinnacle is the cloud computing layer, endowed with robust storage capacity and computational prowess. Subsequently, the fog computing layer assumes an intermediary role, bridging the gap between the cloud computing layer and the sensor network layer. Within the fog computing layer, fog nodes possess specific storage capacity and computing capabilities.

The bottom layer comprises the user's local machine, primarily responsible for collecting and uploading data to the cloud server. Additionally, the rate of data transfer between the fog computing layer and the remaining layers surpasses the direct rate between the cloud layer and the lowermost layer. The incorporation of fog computing mitigates the burden on the cloud computing layer, consequently improving overall efficiency. In this approach, I make use of the fog computing model, implementing a three-tier structure.

B. Privacy-Preserving Cloud Storage Scheme with Three-Layer Structure Grounded in Fog Computing Model

To safeguard user privacy, I propose a Three Layer Storage framework based on the fog computing model. This framework empowers users with a degree of data management control and effectively protects user privacy. To tackle the issue of internal attacks, this approach utilizes encoding technology to partition user data into three parts of varying sizes. Each segment lacks a portion of essential information necessary for sensitivity. Leveraging the fog computing model, these three data segments are individually stored on the cloud server firstly, then in fog server, and finally on the user's local machine, following a size-based order. This approach ensures that even if an attacker gains access to all the data from a specific server, they cannot reconstruct the user's original data. Additionally, for the Cloud Service Provider (CSP), obtaining useful information is impossible without data from both the local machine and fog server as they are under the user's control.

TLS framework maximizes the utilization of the data processing capabilities and fog server's storage. Each server retains a specific portion of data, with the storage allocation determined by the strategy of user. Initially, the user's data undergoes encoding on the user's local machine, for instance, with 1% of the encoded data stored locally and the remaining 99% uploaded to the fog server. Subsequently, similar operations are conducted on the fog server for the data received from the user's machine, resulting in approximately 4% of the data stored on the fog server, with the remainder uploaded to the cloud server.

C. Theoretical Security Analysis

This segment aims to furnish a theoretical security analysis of the framework put forth in this study and substantiate that the secure storage structure genuinely enhances privacy protection. The contention stands that it is infeasible to reconstruct the original data using the data from any individual server. Consequently, the TLS framework significantly mitigates the risk of user privacy leakage.

In contrast, the hash code divides the sentence into distinct fragments using a randomized sequence. Consequently, Hash-Solomon code enhances privacy protection as well as deters attackers from obtaining fragmented.

MODULES

This Paper consists of the following modules:

- ❖ Owner
- ❖ Fog server
- ❖ Cloud
- ❖ User

Module Descriptions:

1. **Owner Module**: The initial module encompasses the capabilities for the owner. Within this module, the owner has the capability to upload a new file. Additionally, they can inspect the file, which is split into blocks and stored in three locations with MAC codes.
2. **Fog Server Module:** In the Fog Module, the owner can review details of file and the download history of related files. Similar to cloud storage, the fog server retains a portion of the data for the overall security of the complete dataset. Accessing the entire file requires both the owner's part data and the fog server-stored data. Consequently, the Fog module also maintains a record of history related to file download.
3. **Cloud Module:** This module is dedicated to the security and storage of data. Once a file is uploaded to the cloud by the owner, file details become accessible in the cloud. The

cloud module is also equipped to view file download history and user request details.

4. **User Module:** The user functionalities are designed within this module. Users can peruse the available files and submit requests for file access. Upon receiving the key from the data owner, users can then proceed to download the complete file.

V. CONCLUSION

Cloud computing progress brings convenience, especially in storage expansion through cloud storage. Yet, it introduces security challenges as users cede control over data storage. To address privacy concerns, I propound a Three Layer Storage (TLS) framework built upon fog computing, incorporating a Hash-Solomon algorithm. The feasibility of the scheme is substantiated through theoretical safety analysis. By judiciously allocating the ratio of data blocks stored in different servers, I can ensure the privacy of data on each server. Theoretically, the encoding matrix is impervious to cracking, and hash transformation serves to safeguard fragmentary information. Experimental testing reveals that this scheme adeptly executes encoding and decoding processes without compromising the efficiency of cloud storage.

Moreover, I have devised a comprehensive efficiency index, aiming for optimal efficiency. Additionally, I extend the efforts by implementing a prototype that supports the tangible realization of fog-based Internet of Things applications.

VI.REFERENCES

[1] Z.Xia,X.Wang,L.Zhang,Z. Qin,X.Sun,and K. Ren, “A privacy preserving and copy-deterrencecontent-basedimageretrievalschemeinclouddcomputing,”*IEEETrans.Inf.ForensicsSecurity*,vol.11,no. 11,pp.2594–2608, Nov.2016.

[2] J. Chase, R. Kaewpuang, W. Yonggang, and D.Niyato,“Jointvirtualmachineandbandwidthallocationinsoftwaredefinednetwork(sdn)andcloudcomputingenvironments,”in*Proc.IEEEInt.Conf. Commun.*, 2014,pp.2969–2974.

[3] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving data-storage service in public cloud,” *J. Comput. Res. Develop.*, vol. 51, no. 7, pp.1397–1409,2014.

[4] R.Kulkarni,A.Forster,andG.Venayagamoorthy,“Computationalintelligenceinwirelesssensornetworks:A survey,”*IEEECommun. Surv. Tuts.*, vol. 13, no. 1, pp. 68–96, FirstQuarter2011

[5] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “Asurveyofmobilecloudcomputing:Architecture,applications,andapproaches,”*WirelessCommun.MobileComput.*,vol.13,no.18,pp.1587–1611,2013.

[6] J.S.Plank,“T1:Erasurecodesforstorageapplications,”in*Proc.4th USENIXConf.FileStorage Technol.*, 2005,pp.1–74.

[7] L. Xiao, Q. Li, and J. Liu, “Survey on secure cloud storage,” *J. Data Acquis. Process.*, vol. 31, no.3, pp.464–472,2016.

[8] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen,“Efficientdatacollectioninsensor-cloudsystemwithmultiplemobilesinks,”in*Proc.Adv.Serv.Comput., 10th Asia-Pac. Serv. Comput. Conf.*, 2016,pp. 130–143.

[9] R. J. McEliece and D. V. Sarwate, “On sharing secret sand reed-solomon codes,”*Commun. ACM*,vol.24, no. 9,pp.583–584, 1981.