International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

A Three Layer Privacy Preserving Secure Cloud Storage Based on Fog Computing

Ms. Sakina, Ms. Hummatul Sara, Ms. Syeda kaleem Fatima, Mr. Mir Mustafa Ali,
[1]Dept. of IT, Deccan College of Engineering and Technology, Hyderabad.
[2]Dept. of IT, Deccan College of Engineering and Technology, Hyderabad
[3]Dept. of IT, Deccan College of Engineering and Technology, Hyderabad
[4]Assistant Professor, Dept. of IT, Deccan College of Engineering and Technology, Hyderabad

Abstract: *Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud servers. In other words, users lose their right of control on data and face privacy leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. In order to solve this problem, we propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Besides, Hash-Solomon code algorithm is designed to divide data into different parts. Then, we can put a small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to existing cloud storage scheme.*

Keywords: Cloud computing, cloud storage, fog computing, privacy protection.

1. Introduction

The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. For example, Apples iCloud leakage event in 2014, numerous Hollywood actresses private photos stored in the clouds were stolen. This event caused an uproar, which was responsible for the users' anxiety directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user do not actually control the physical storage of their data, which results in the separation of ownership and management of data [6]. The CSP can freely access and search the data stored in the cloud. Meanwhile the attackers can also attack the CSP server to obtain the user's data. The above two cases both make users fell into the danger of information leakage and data loss. Traditional secure cloud storage solutions for the above problems are usually focusing on access restrictions or data encryption.

These methods can actually eliminate most part of these problems. However, all of these solutions cannot solve the internal attack well, no matter how the algorithm improves. Therefore, we propose a TLS scheme based on fog computing model and design a Hash-Solomon code based on Reed-Solomon code [7], [8]. Fog computing is an extended computing model based on cloud computing which is composed of a lot of fog nodes. These nodes have a certain storage capacity and processing capability.

In our scheme, we split user's data into three parts and separately save them in the cloud server, the fog server and the user's local machine. Besides, depending on the property of the Hash-Solomon code, the scheme can ensure the original data cannot be recovered by partial data. On another hand, using Hash-Solomon code will produce a portion of redundant data blocks which will be used in decoding procedure. Increasing the number of redundant blocks can increase the reliability of the storage, but it also results in additional data storage. By reasonable allocation of the data, our scheme can really protect the privacy of user' data.

The Hash-Solomon code needs complex calculation, which can be assisted with the Computational Intelligence (CI). Paradigms of CI have been successfully used in recent years to address various challenges, for example, the problems in Wireless sensor networks (WSNs) field. CI provides adaptive mechanisms that exhibit intelligent behavior in complex and dynamic environments likeWSNs [9]. Thus in our paper, we take advantage of CI to do some calculating works in the fog layer. Compared with traditional methods, our scheme can provide a higher privacy protection from interior, especially from the CSPs.

2. Literature Survey:

The NIST Definition of Cloud Computing

Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

A survey of mobile cloud computing: Architecture, applications, and approaches

This paper gives a survey of MCC, which helps general readers have an overview of the MCC including the definition, architecture, and applications. The issues, existing solutions, and approaches are presented. In addition, the future research directions of MCC are discussed.

Joint virtual machine and bandwidth allocation in software defined network (SDN) and cloud computing environments.

We propose a unified approach that integrates virtual machine and network bandwidth provisioning. We solve a stochastic integer programming problem to obtain an optimal provisioning of both virtual machines and network bandwidth, when demand is uncertain. Numerical results clearly show that our proposed solution minimizes users' costs and provides superior performance to alternative methods. We believe that this integrated approach is the way forward for cloud computing to support network intensive applications.

Secure and Privacy-Preserving Data Storage Service in Public Cloud

This paper focuses on the enabling and critical cloud computing security protection techniques and surveys on the recent researches in these areas. In addition, we further point out some unsolved but important challenging issues and hopefully provides insight into their possible solutions.

Survey on secure cloud storage

In this paper, we present a typical Cloud Storage system architecture, a referral Cloud Storage model and Multi-Tenancy Cloud Storage model, value the past and the state-ofthe- art of Cloud Storage, and examine the Edge and problems that must be addressed to implement Cloud Storage. Use cases in diverse Cloud Storage offerings were also abridged.

T1: Erasure codes for storage applications

This tutorial will cover the fundamentals of erasure coding, the mechanics of many erasure codes that apply to today's storage systems, and the properties of various erasure codes designed for a variety of storage scenarios.

3. System Analysis:

Existing System:

- User uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user does not actually control the physical storage of their data, which results in the separation of ownership and management of data.

- In order to solve the privacy issue in cloud computing, previous researches proposed a privacy-preserving and copy-deterrence CBIR scheme using encryption and watermarking techniques. This scheme can protect the image content and image features well from the semi-honest cloud server, and deter the image user from illegally distributing the retrieved images.

- Previous works consider that in traditional situation, user’s data is stored through CSP; even if CSP is trustworthy, attackers can still get user’s data if they control the cloud storage management node. To avoid this problem, they propose an encrypted index structure based on an asymmetric challenge-response authentication mechanism. When user requests data from cloud server, the user sends a password to the server for identification. Taking it into consideration that the password may be intercepted, the structure uses asymmetric response mode.

Disadvantages:

- The CSP can freely access and search the data stored in the cloud. Meanwhile the attackers can also attack the CSP server to obtain the user's data. The above two cases both make users fell into the danger of information leakage and data loss. Traditional secure cloud storage solutions for the above problems are usually focusing on access restrictions or data encryption.

Proposed System:

- However, all of these solutions cannot solve the internal attack well, no matter how the algorithm improves. Therefore, we propose a TLS scheme based on fog computing model. Fog computing is an extended computing model based on cloud computing which is composed of a lot of fog nodes. These nodes have a certain storage capacity and processing capability. In our scheme, we split user's data into three parts and separately save them in the cloud server, the fog server and the user's local machine.

- We propose a new secure cloud storage scheme in this paper. By dividing file with specific code and combining with TLS framework based on fog computing model, we can achieve high degree privacy protection of data. It does not means that we abandon the encryption technology. In our scheme encryption also help us to protect fine-grained secure of the data.

Advantages:

- Compared with traditional methods, our scheme can provide a higher privacy protection from interior, especially from the CSPs.

- From a business perspective, company with high security degree will attract more users. Therefore improving security is an crucial goal no matter in academia or business. In this section, we will detailedly elaborate how the TLS framework protects the data privacy, the implementation details of work flow and the theoretical safety and efficiency analysis of the storage scheme.

Modules:

Data Owner:

File owner will register with application and login with valid user name and password if verification is successful client can upload files to cloud server through fog server by keeping 1 percent of encrypted data at owner side and send 99 percent data to fog server for further processing.

Data owner will have permission to give key to user who wants to access data along with

1 percent data. In this process data owner will get information of any kind of activity happening to his data which is stored in cloud server.

Fog Server:

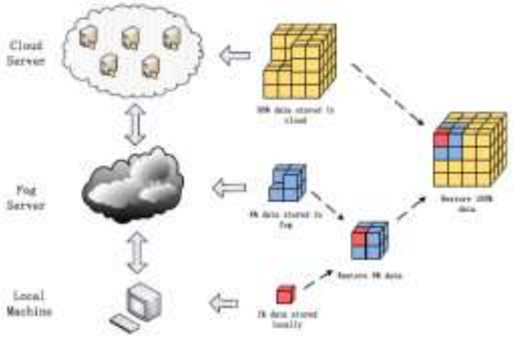
In this module fog server will act as small storage server and perform basic operations before sending data to cloud. In this second stage, after receiving the 99% data blocks from user's machine, these data blocks will be encoded again. These data blocks will be divided into smaller data blocks and generates new encoding information. Similarly, assuming that 4% data blocks and encoding information will be stored in the fog server. The remainder 95% data blocks will be uploaded to the cloud server.

When user request for downloading data fog server will verify and send 4 percent of data to user.

Cloud Server:

Cloud can login with valid user name and password the cloud storage server provides storage services to the registered clients for storing outsourced files. Storage server can view details of file uploaded by user which is received from fog server. In this process cloud server will only store 95 percent of data. When user requests for downloading data cloud server will store 95 percent of data.

4. System Design:



4.1 System Architecture

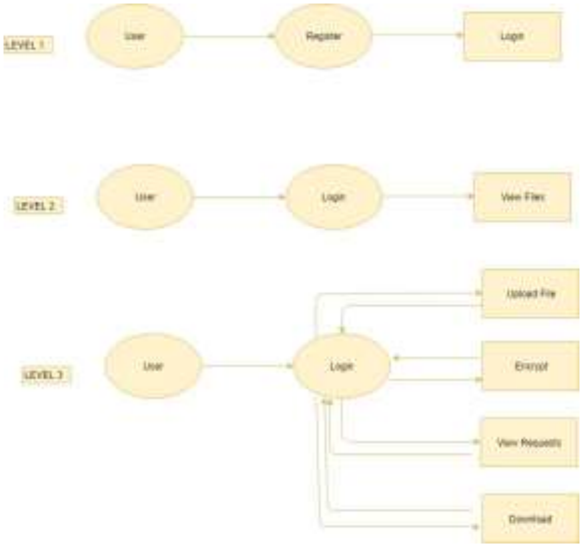


Image 4.2 Data Flow Diagram for User

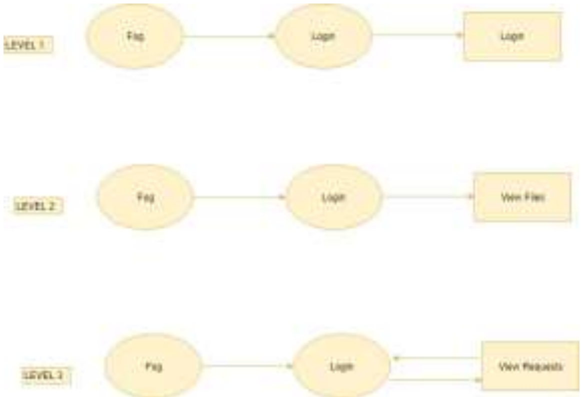


Image 4.3 Data Flow Diagram for Fog

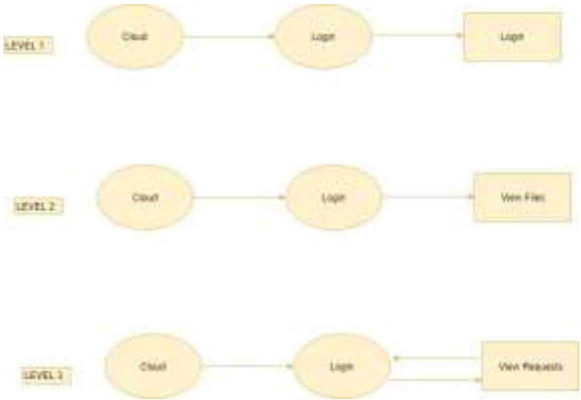


Image 4.4 Data Flow Diagram for Cloud

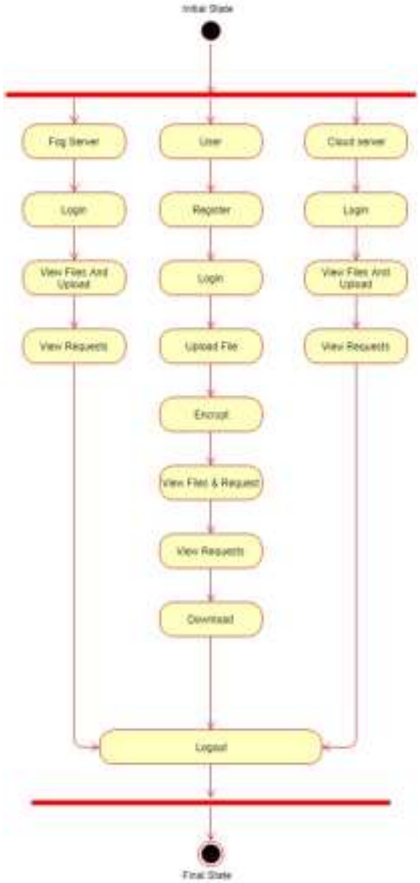


Image 4.5 Activity Diagram

5. Output Results:

Fig 5.1: Home page

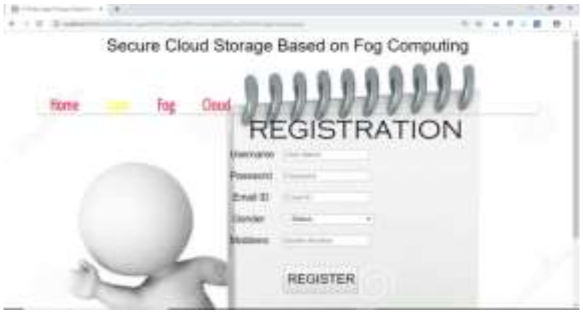


Fig 5.2: Registration

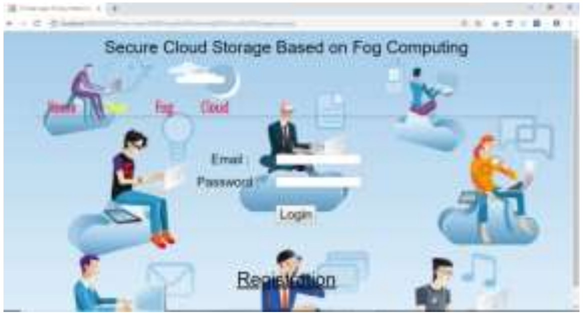


Fig 5.3: User login

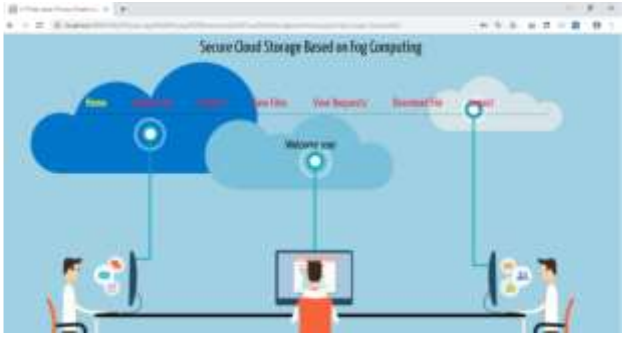


Fig 5.4: User home

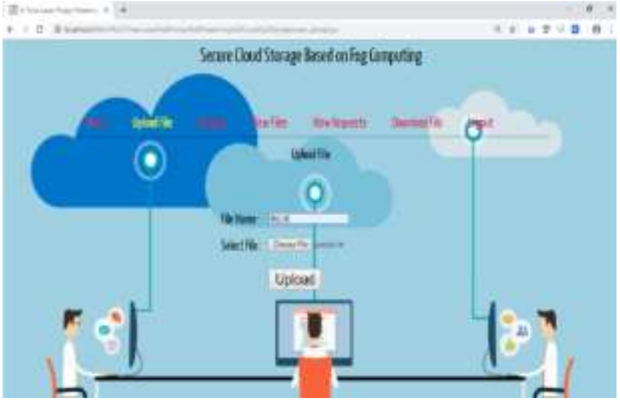


Fig 5.5: User uploads

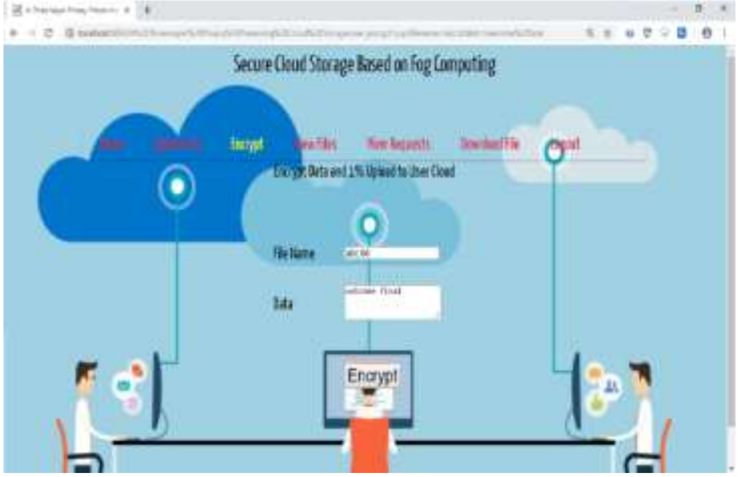


Fig 5.6: User encrypt

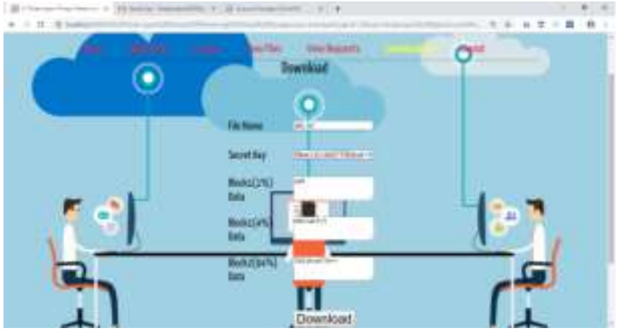


Fig 5.7: User downloads

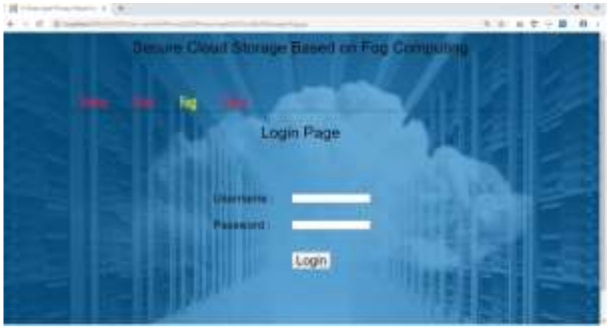


Fig 5.8: Fog login

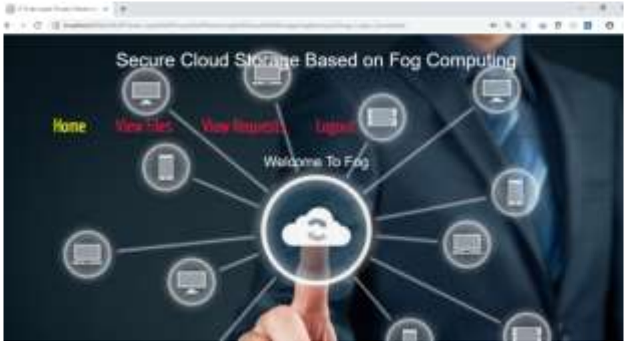


Fig 5.9: Fog home

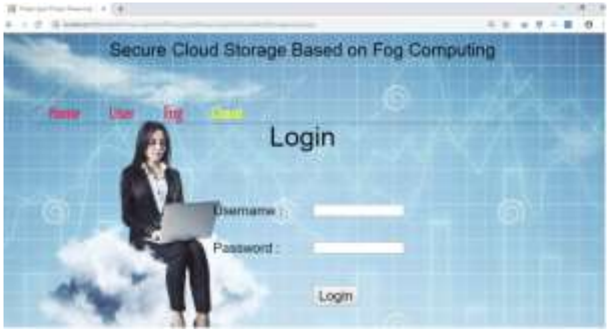


Fig 5.10: Cloud login

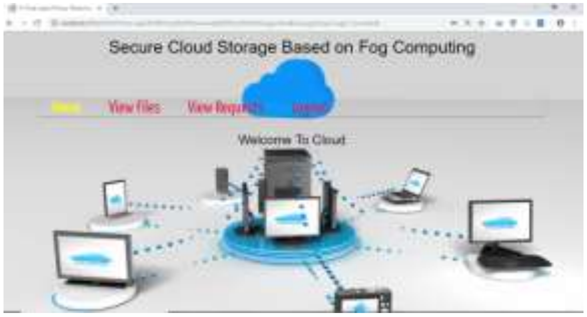


Fig 5.11: Cloud home

6. Conclusion

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible.

By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. Furthermore, we design a reasonable comprehensive efficiency index, in order to achieve the maximum efficiency, and we also find that the Cauchy matrix is more efficient in coding process.

.

References

[1]. P. Mell and T. Grance, “The NIST definition of cloud computing,” *Nat.Inst.*

Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[2]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, 2013.

[3]. 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 *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 2969–2974.

[4]. 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.

[5]. Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in *Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf.*, 2016, pp. 130–143.

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

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

[8]. J. S. Plank, "T1: Erasure codes for storage applications," in *Proc. 4th USENIX Conf. File Storage Technol.*, 2005, pp. 1–74.

[9]. R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme in

[11]. cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[12]. J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive Mobile*

[13]. *Comput.*, vol. 41, pp. 219–230, 2017.

[14]. Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

[15]. J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," *J. Hebei Acad. Sci.*, vol. 30, no. 2, pp. 45–48, 2013.

[16]. Q. Hou, Y. Wu, W. Zheng, and G. Yang, "A method on protection of user data privacy in cloud storage platform," *J. Comput. Res. Develop.*, vol. 48, no. 7, pp. 1146–1154, 2011.

[17]. P. Barham*et al.*, "Xen and the art of virtualization," *ACM SIGOPS Oper. Syst. Rev.*, vol. 37, no. 5, pp. 164–177, 2003.