WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CLOUD STORAGE WITH CIPHER

Saima Samreen, Ibtesam Mehveen, Sakshi K Doijode.

Guru Nanak Dev Engineering College Bidar Students Dept. of CSE GNDECB, Bidar Karnataka 585401, India

A B S T R A C T

CIPHER is an overwhelmingly popular application for file transfer and Secure Computing, which has the ability to provide demanded services for information for companies, enterprises and even individuals. However, users may not have faith in the CSPs so henceforth in that case it is difficult to determine whether the CSPs meet their required credentials for information security. Therefore, it is important to develop effective requesting and authorizing techniques to strengthen data senders' and receivers' trust and confidence in cloud storage.

In this paper, a global public examining scheme is presented for safe and secure cloud storage based on CIPHER which uses public key cryptography and a new two-dimensional data structure located at a third-party auditor (TPA) to record the data property information for secure transmission of data and information. Unlike from the existing works, the proposed system grants permission for accessing the information from the proxy cloud to only authenticated end users while in the existing systems there are no barrier gates that would check for the users credentials and authentication.

Additionally, this technique extends our scheme to support privacy prevention by adding the holomorphic authentications based on the symmetric secret key with the random masking generated by the CIPHER. Therefore the proposed system results to be more efficient than the existing one in terms of user authentication, cost effective storage and maintain data integrity.

1. INTRODUCTION

In today's world sharing of data without internet web being involved has become almost inevitable. As more and more users connect to this World Wide Web and we all know that internet is an open-source platform the data being transferred can easily be accessed and tampered by mischievous threats. Data security and authenticated access ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data and secures the files being transferred from any form of eavesdropping. Henceforth adding authenticating gates at the access of cloud storage can be an effective method. For achieving this level of security, various algorithms and techniques have been developed. One of such techniques is cryptography which ciphers the given data that has to be transferred over a network using secret key and certain algorithms which makes the original text unintelligible to any sane human being unless deciphered.

2. LITERATURE SURVEY

A basic feature of these applications is that they need to access data sets which are very large but simple. Cloud computing provides computing requirements for these kinds of new generation of applications involving very large data sets which cannot possibly be handled efficiently using traditional computing infrastructure. In this paper, we describe storage services provided by three well-known cloud service providers and give a comparison of their features with a view to characterize storage requirements of very large data sets as examples and we hope that it would act as a catalyst for the design of storage services for very large data set requirements in future. We also give a brief overview of other kinds of storage that have come up in the recent past for cloud computing.

3. SYSTEM SPECIFICATION

3.1 Software Requirements

1. Operating system : Windows 7.
2. Coding Language : jkd1.7
3. Data Base : MySQL

3.2 Hardware Requirements

1. System : Intel Core i3 2.8 GHz.

2. Hard Disk : 250 GB.

3. Monitor : 15‖ VGA Colour.

4. Mouse : Logitech.

5. Ram : 1 GB.

4. 4. OBJECTIVES

- To ensure the privacy of a user's personal information from others.
- To achieve authentication of data sender and receiver in the network.
- To ensure transmitted data integrity.
- To minimize third party eavesdropping.

5. PROBLEM DEFINITION

Digital files and assets sharing have been the norm in organizations for a long time, but security is still a big concern. Cybersecurity firm Varonis found that organizations share files with an average of 800 domains. The wide-scale adoption of IM and collaboration tools, as well as cloud-based file-sharing systems, has made the process of sharing data easier but also less secure than ever. The majority of internally circulated files are shared without much attention to security. Organizations must prioritize secure file transfers, as company files often contain sensitive, proprietary and classified information. This project focuses on providing cloud-based file sharing with multi-gated authentication, secret keys and encrypted files.

6. PROPOSED SYSTEM

Cloud storage auditing has grabbed the attention increasing. Some of the older relative works is proof of retrievability which also gives the function output such as examining the integrity of the data and information saved on the proxy cloud server and ensured safe withdrawal of data. But, PoRs is moreover a private auditing solution, and does not allow any third party to perform any auditing. Later in the same year, Ateniese et al. [3] introduced a public examining scheme, provable data possession, which involves RSA based algorithms to check the integrity and truthfulness of the data to be withdrawal. Upon comparing both the schemes the public examining scheme turned out to be more effective in terms of providing better user data overall security and it is expected to be more practical and reliable. In addition to the cloud storage this this system provides many authentication barriers in order to prevent unauthorized access of data as well as encrypted file transfer to maintain data integrity.

7. Advantages

1. Cost Savings
2. High Speed
3. Back-Up and Restore Data
4. Unlimited Storage Capacity
5. Reliability

8. SYSTEM DESIGN

System design is the stage where overall design of the system is decided. Theoretically, according to the philosophy of object-oriented systems, is to think of a system as interactive objects. While designing the system, the basic focus lies on the objects comprising the system and not on the processes being carried out. This system basically consists of cloud storage as proxy, key generation centre both connected to the organization or individuals who can to securely transfer the data between themselves.

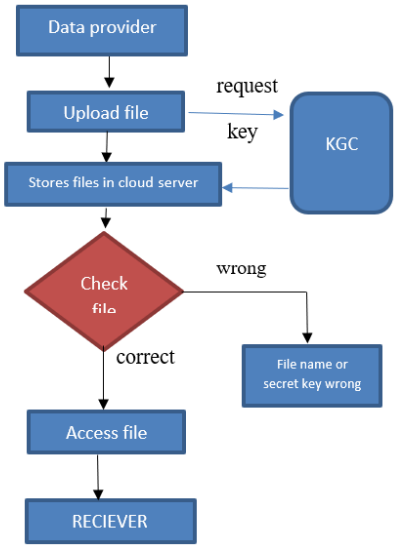

Figure 1: Data flow representation of the system.

9. CONCLUSION

Nowadays, cloud storage, which can offer on-demand access to outsourcing data for both organizations and individuals eventually, has attracted more and more attention now a days. However, if cloud storage could incorporate a mechanism that could also advocated for user authentication and ensure data integrity would gain even more popularity and become more efficient. This paper motivates to make cloud storage more effective by adding user authentication and data safety measures with the help of cryptographic techniques whose main essence is ciphering the given text being transferred over a network, hence protecting the data from being eavesdropped and eventually resulting in maintaining data integrity.

REFERENCES

[1] A. Juels and B.S. Kaliski Jr., “PoRs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Communications Se- curity (CCS ’07), pp. 584-597, 2007.

[2] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li. ‘‘Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,’’ IEEE Trans. on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[3] G. Ateniese, R.B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, ‘‘Provable Data Possession at Untrusted Stores,’’ Proc. 14th ACM Conf.

[4] C. Wang, K. Ren, W. Lou and J. Li. ″Toward Publicly Auditable Secure Cloud Data Storage Services″, IEEE network, vol. 24, no. 4, pp. 19-24, 2010.

[5] F. Sebé, J. Domingo-Ferrer, A. Martínez-Ballesté, Y. Deswarte and J.-J. Quisquater, “Efficient Remote Data Possession Check- ing in Critical Information Infrastructures,” IEEE Trans.