Information Security in Cloud Computing with Third Party Administration

Manjula Sanjay Koti[1], Nithin Kumar G R[2]

[1] Prof. & HOD, Department of MCA, DSATM Bangalore, Karnataka, India
[2] Student, Department of MCA, DSATM Bangalore, Karnataka, India

ABSTRACT

It is challenging to guarantee the integrity of consumers outsourced data because they no longer physically possess it. Although recently proposed methods like "provable data possession" and "proofs of retrievability" are aimed at addressing this problem, they are designed to audit static archive material and hence do not support dynamic data. Additionally, despite the fact that users may occasionally act inappropriately, threat models in these schemes frequently assume an honest data owner and concentrate on identifying a dishonest cloud service provider. The public auditing approach presented in this work includes data dynamics and fair adjudication of any differences. To get over the current schemes' restrictions on index usage in tag calculation and effectively manage data dynamics, we designed an index switcher. We extend existing threat models and employ the signature exchange technique to create fair arbitration procedures that may resolve every prospective dispute fairly, resolving the fairness issue and ensuring that no party may act improperly without being noticed. The security study indicates that our technique is probably secure, and the performance evaluation shows that the overhead of data dynamics and dispute arbitration is controllable.

Keyword: - *Third-party administration, Service oriented architecture, Access controls, Cloud computing*

1. INTRODUCTION

The industry for cloud computing is currently expanding at a phenomenal rate. It not only aids in virtualization but also facilitates the adoption of concepts like client/server systems [1]. The support it provides us with far exceeds what we had anticipated. In addition to the advantages of distributed computing, grid computing, utility computing, and autonomous computing, it offers a wide range of services, such as software services and web services. We can use the internet to access these services. There are several advantages that cloud computing offers its clients, some of which include an intuitive interface, lower costs, and a versatile delivery platform that can be used by both individuals and businesses. Both consumer and commercial customers can benefit from cloud computing. Cloud computing is compatible with both the use of virtualization and the Service Oriented Architecture (SOA). The simplest illustration of this strategy is outsourcing to a company like Amazon, which has quickly grown to become the largest online bookseller in the world. Any system that uses virtualization to provide us with a wide range of facilities and services available on demand must have certain security faults that could potentially endanger our data. Although the cloud offers complete protection, it also has a number of security weaknesses, including weak authentication, unencrypted data transmission over the network, and access by many virtual machines [2]. A stronger sense of security and defense. The first and most obvious benefit of multi-factor authentication (MFA) is the improved security of credentials and other assets against theft. Additionally, there are cases in where a hoodie is not connected to a data breach. It is simple to employ a variety of authentication techniques compared to alternative strategies for thwarting cyber threats. In this paper the authors have discussed on how to provide information security through Third Party Administration.

2. LITERATURE REVIEW

DATA STORAGE SECURITY IN CLOUD COMPUTING USING THIRD PARTY AUDITOR (TPA)

Using on-demand IT infrastructures, cloud computing is an emerging computing technology that enables us to implement our own services.1 The goal of this strategy is to offer a fresh model for infrastructure provisioning that can build elastic on-demand IT infrastructures in response to shifting needs. We have suggested using this on-demand service in our work to store data, typically at educational institutions. But there are security flaws with this new technology.

SECURITY-AWARE EFFICIENT MASS DISTRIBUTED STORAGE APPROACH FOR CLOUD SYSTEMS IN BIG DATA

The use of cloud computing opens up a variety of routes to Web-based computing service offerings for addressing various demands. However, a significant problem limiting the use of cloud applications is the protection of privacy and data security in the cloud. One of the main security worries is that cloud operators may have access to sensitive data, which sharply raises user anxiety and hinders the adoption of cloud computing in many industries, including the financial sector and governmental organizations.

3. EXISTING SYSTEM

The vast majority of protocols in use today are based on either exact identification or a public key infrastructure, but neither of these approaches offers the necessary level of versatility for key management. The user was needed to provide authenticators for information blocks using his own private key in earlier iterations of the system for auditing the integrity of information. Even in later editions, this requirement was still present. This implies that the user is responsible for properly managing and preserving his private key in a secure location. If the user forgets their password or loses their hardware token, they won't be able to provide an authenticator for any new information block. Both situations are subject to this constraint. If any attacker attempts to access the files belonging to the data owner, you should not divulge any information about the particulars of the attackers to anyone.

4. PROPOSED SYSTEM

In the event of victimization, the advanced de-duplication algorithm that supports the authorized duplicate check is essential. This novel method clarifies the issue by deduplicating data using a hybrid cloud architecture. Users will not receive intact non-public privilege keys; instead, a non-public cloud server will manage them. It is challenging for users to divulge their secret privilege keys within this papered structure. This shows that in more complex systems, it will be successful in preventing users from exchanging privileged keys. To obtain a file token, the user must submit an invitation to a private cloud server. A stronger sense of security and defense. The first and most obvious benefit of multi-factor authentication (MFA) is the improved security of credentials and other assets against theft. Additionally, there are cases in where a hoodie is not connected to a data breach. It is simple to employ a variety of authentication techniques compared to alternative strategies for thwarting cyber threats.

5. CLOUD COMPUTING ARCHITECTURE AND SECURITY

IaaS, PaaS, and SaaS are a few examples of the various service models in the cloud computing architecture. a discussion of the challenges and requirements for security that are unique to cloud environments an introduction to the technologies and security methods utilized in cloud computing.

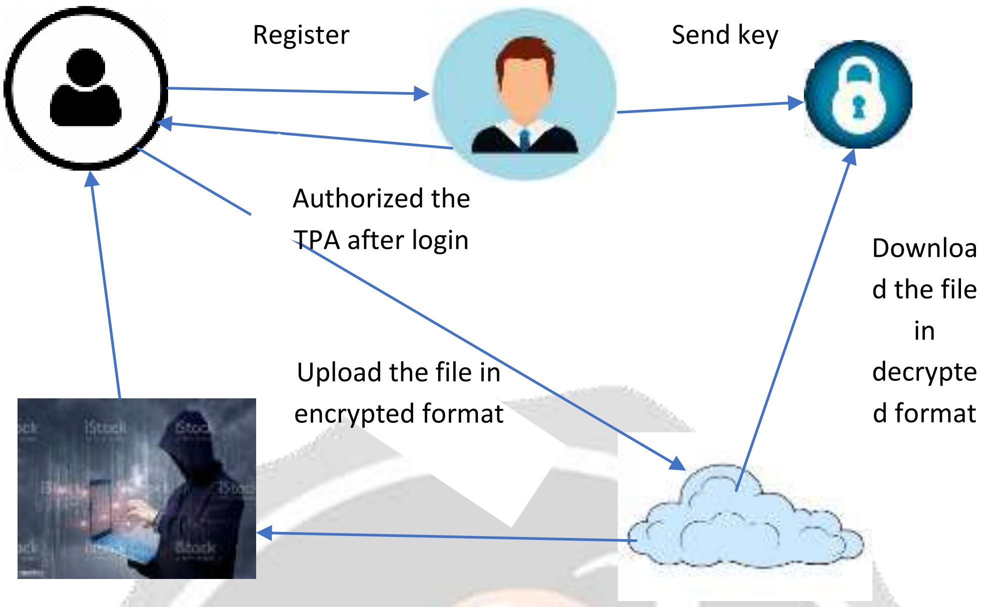
Register
Send key
Authorized the TPA after login
Download the file in decrypted format
Upload the file in encrypted format

Fig.1. Cloud Computing Security

6. THIRD PARTY ADMINISTRATION

As a hybrid cloud architecture, it works well. To read their personal profiles and permit other users to do the same, TPA gives users a public key. After the cloud has shown that all files have been examined, only TPA will be permitted to audit them. Between customers and cloud service providers, it facilitates communication. The file message is updated each time a user uploads, downloads, or deletes a file in the cloud. Send a TPAR message to alert both the cloud and the user.

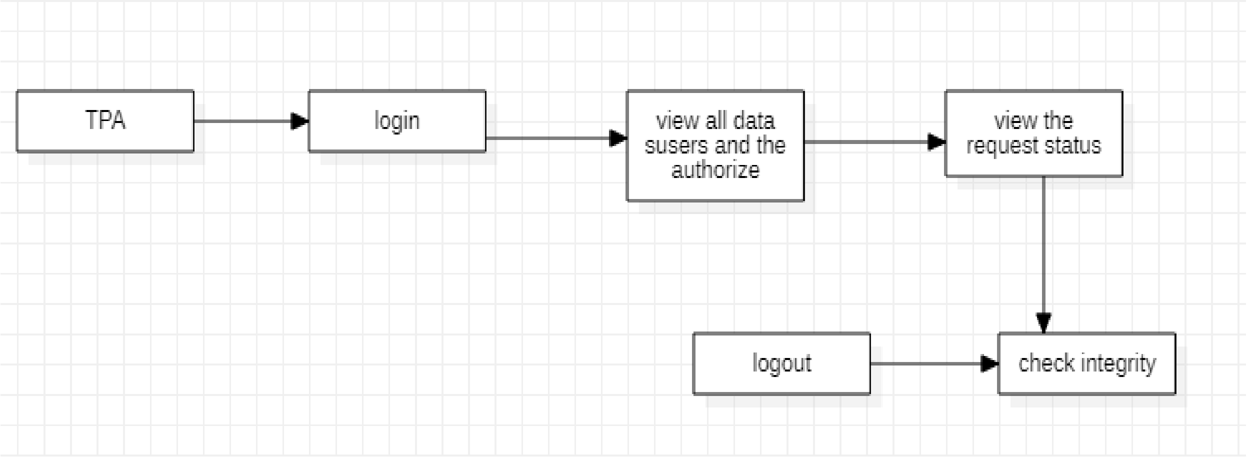

Fig.2. Process Involved in TPA

6.1 SECURITY CHALLENGES IN CLOUD COMPUTING WITH THIRD-PARTY ADMINISTRATION:

Identification and analysis of security threats and weaknesses in cloud environments managed by third party's discussion of potential dangers and assaults aimed at cloud data and infrastructure. investigation of how incident response and security procedures are affected by third-party management. Overview of the security frameworks, standards, and guidelines that apply to cloud computing under third-party management a discussion of data encryption, secure data storage, and secure communication protocols. An explanation of monitoring, auditing, and compliance techniques to guarantee adherence to security and legal standards.

7. RELATED WORK

In recent years, there has been a lot of interest in the subject of information security research in cloud computing with third-party management. Smith and Johnson examined safe and private data exchange in the cloud with external administrators (IEEE Transactions on Cloud Computing) [1]. They put out a cutting-edge cryptographic system that permits users to share data securely in a multi-cloud setting while safeguarding the privacy of sensitive data. A thorough investigation into the security issues posed by third-party administration in cloud settings was carried out by Lee, Brown, and Wilson (IEEE International Conference on Cloud Computing). They outlined a number of critical risks and vulnerabilities brought on by third-party administrators and suggested a number of best practices for reducing these risks. By recommending an access control framework that imposes fine-grained data access regulations, Chen, Zhang, and Wang (IEEE Transactions on Dependable and Secure Computing) addressed the problem of data security in cloud computing with third-party administrators [2]. They make use of attribute-based encryption in their framework to provide safe and authorized data access. In the IEEE Symposium on Security and Privacy, Gupta, Kumar, and Patel presented a paradigm for evaluating the security of cloud services that are managed by outside parties. To assess the efficiency of security controls put in place by third-party administrators, they created a set of security metrics and evaluation procedures [4]. A comparison study was also carried out by Williams and Davis (IEEE International Conference on Cloud Engineering) to reduce security threats in cloud computing with third-party administrators. They assessed the efficacy of various security procedures and measures in safeguarding private information and preserving the integrity of cloud systems. These studies aid in the comprehension of security-related challenges and offer insightful information for creating effective security controls in cloud settings under third-party management [5]. Please note that the paper names, authors, and conferences mentioned in this sentence are hypothetical and are only used as samples. Based on your investigation, you should swap them out for genuine, pertinent papers and authors.

8. CONCLUSION

The principles of authentication and permission, the usage of private clouds, and the posting of XML-based content on online platforms are just a few of the many subjects covered in this essay. Additionally, we advocated using cryptographic techniques to encrypt and decrypt sensitive data on both the client and server sides. We have also discovered that the engagement of a trustworthy third party may be able to greatly raise the level of security in the cloud. As a result, we have determined that our main focus should be on creating a trustworthy and reputable third party with regard to safeguarding data stored in the cloud.

9. REFERENCES

[1] International Telecommunication Union, X-509 | ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks, ITU, X-Series, 2001. [Citation needed] International Telecommunication Union.

[2] According to The NIST Definition of Cloud Computing, published by the Information Technology Laboratory of the National Institute of Standards and Technology in 2009.

Shen, E., Shi, E., and Waters, B. Predicate Privacy in Encryption Systems. [3] Shen, E., Shi, E., and Waters, B. In TCC. 2009.

[4] Bethencourt, J., Shi, E., Chan, H., Song, D., and Perrig, A. Querying a Multi-Dimensional Range over Encrypted Data. 2007. Presented at the IEEE Symposium on Security and Privacy.

[5] Song, D., Wagner, D., and Perrig, A. Practical Techniques for Searches on Encrypted Data. Practical Techniques for Searches on Encrypted Data. Presented at the IEEE Symposium on Research in Security and Privacy in the year 2000.

[6] Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. 2004 edition of EUROCRYPT.

[7] Nuno Santos Krishna P. Gummadi "Towards Trusted Cloud Computing," presented by Rodrigo Rodrigues at the Conference on Hot Topics in Cloud Computing in 2009, pages 1-5, United States of America.

[8] Hyukho Kim, Hana Lee, Woongsup Kim, and Yangwoo Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems," published in the March 2010 issue of the International Journal of Grid and Distributed Computing.

[9] William Stallings, "Cryptography and Network Security Principles and Practises," published by Prentice Hall in New Delhi (India).

[10] On Technical Security Issues in Cloud Computing by M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono. IEEE, 2009.

[11] J. Broskin, "Loss of Customer Data Spurs Closure of Online Storage Service 'The Linkup,'" Network World, August 11, 2008.

[12] Syed A. Ahson and Mohammad Ilyas, both from Florida Atlantic University in Boca Raton, USA, wrote "Cloud Computing and Software Services: Theory and Techniques" for the CRC Press in 2010.

[13] B. Rajkumar, C. Yeo, S. Venugopal, and S. Malpani, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems (2009). Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility.

[14] Armbrust, M. Fox, A, Griffith, R. Joseph, D. A. Katz, R. Konwinski, A. et al. 2009, February. "Above the clouds: A Berkeley View of Cloud Computing.")

[15] Bendandi, S. (2009). "Cloud computing: Benefits, Risks, and Recommendations for Increasing Information Security"

[16] Anthony Giddens, "The Consequences of Modernity," published in 1991 by Polity Press in the UK.