A STUDY ON DISTRIBUTED FILE SYSTEM SECURITY USING SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY

M.V.Bhuvaneswari[1], P.Sateesh[2], .B.Srinivas[3], P.R.S.Naidu[4]
[1]Student, CSE Dept, M.V.G.R College of engineering, Vizianagaram
[2,3,4]CSE Dept, M.V.G.R College of engineering, Vizianagaram

Abstract

The rapid growth of services provide by internet, mobile and web applications and the progress of cloud computing concepts lead to the availability of huge volumes of data online. Even the modern computers have no potential to manage, search, analyze and visualize such vast amount of data as information. So Distributed File System assists in processing of such extremely-large volumes of data. Cloud computing is providing enormous benefits these days and at the same time posing various challenges. Since sharing an infrastructure / applications among multiple users may raise a question of threat to sensitive data/losing data. Data integrity comes into consideration during data outsourcing i.e., protection of static and dynamic data from unauthorized access. The proposed work mainly concentrates on technical security issues and data integrity emerging with the use of cloud services.

Key words: Security, Authentication, Integrity.

I. INTRODUCTION

Regarding “cloud computing” many issues have been arising day by day in perception of security and data integrity. A cloud offers huge benefits like helps in creation, configuration and customizing the applications online but at the same time poses huge threats in terms of authentication and authorization. One more concern is that cloud providers may have access to client’s unencrypted data whether it is on disk, in memory or over the network.

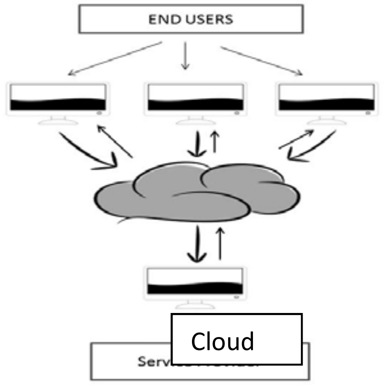


Figure1: Working of Cloud

A. Distributed file System:

A Distributed File System offers client/server based services allowing clients to access, process and share data stored on a server. Distributed file system makes it appropriate for sharing data and files among multiple clients over a network in a controlled and authorized manner there by allowing the user to think that data storage is done locally. Various technologies were developed to bring convenience for sharing resources and files over a network, among which DFS is one such process used regularly.

B. Security Issues:

Even though popularity of cloud has an extreme growth, complications arise with respect to data privacy and data protection that still plague the development of various organizations and business market. The security issues comes under two categories: security issues of cloud providers where different organizations provide software-platform or infrastructure via using cloud. The other issue is regarding customers hosting their applications and storing their data on the cloud. On both hands security and privacy of data and infrastructure has to be ensured. Below are the enclosed discussions concerning cloud security problems, being attentive to the management interface.

C. Emerging Research challenges:

1. Cloud Aggregation: Aggregating resources from various clouds requires adding additional layers of service management.
2. Cloud Management: In a scalable environment it's a big challenge for delivering resources to multiple tenants available.
3. Data Encryption: The data is decrypted and stored when entered into the cloud. Hence there is a choice for encrypting data before storing where the user has to worry about encryption in prior to uploading the data into cloud or directly choose the cloud computing service.
4. Access Controls: Authentication and identity management are most significant areas to take care of involving various techniques.
5. Multi-tenancy: Multiple clients accessing the same hardware, application server and databases may affect the response times.
6. Platform Management: The most important part of cloud platforms is to provide the developers either to publish their own applications in cloud or to use the existing applications offered by cloud.

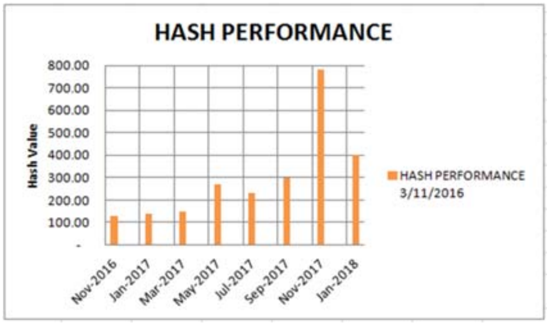
II. RELATED WORK

Security issues lead to various discussions. To achieve data integrity "cloud audit" [1] has been enabled which ensures the security of data and performance quickly and readily available to public. In such case, users turn to an external audit party or third party auditor to care of integrity of data. For performing auditing securely TPA has to efficiently audit the cloud data without causing burden on user of cloud and the TPA shouldn't introduce any new kind of vulnerabilities. Privacy-preserving public cloud data auditing system, a method was introduced which is homomorphic authentication [2] [9] with random masking and also using ElGamal Public Key Encryption Algorithm [3] with Homomorphic Random Authenticator wouldn't allow TPA to access the content of data available in cloud server. This also leads to noise because of Add Doubles and square root of products. Further it is enhanced to bilinear aggregate signature [4] allowing multiple auditing tasks by TPA. Batch auditing [5] is one more method that is preferrable for the TPA to batch multiple tasks together and audit them at a time. A secure cloud storage architecture which is Data Integrity as a Service (DIaaS) [6] which is based on the principle of Service-Oriented Architecture and web services. Hyper-Combined Public key [7] based cloud storage key management scheme is one which helps in solving the problem of large-scale key management and storage issues in cloud storage. The Cloud Computing idea offers dynamically ascendible resources provisioned as a service over the web. Economic benefits are the foremost driver for the Cloud, since it assures the reduction of cost (CapEx) and operational expenditure (OpEx). To make this successful, there are still more challenges to be solved. Among which privacy and data integrity are main issues. This paper [8] focused on technical security issues that came into picture with the use of Cloud services and particularly by the underlying technologies accustomed for building these cross-domain Internet-connected collaborations.

III. RESULTS

The structure involves two nodes (devices) required for the experimental analysis. This includes identifying of performance and efficiency of Syncthing. Results generated presents the outcomes of memory usage and hash performance of syncthing. The graphs below represent the average of metrics of the nodes participated per day.

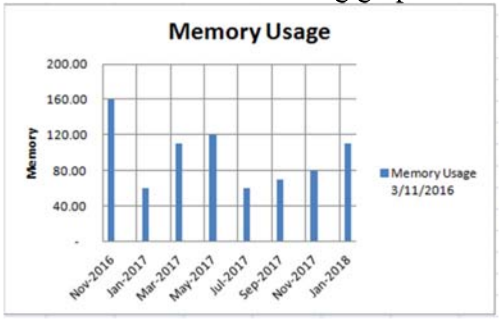
1. HASH PERFORMANCE: Each file is divided into number of blocks in syncthing there by calculating hash for each block. Hashing is done using SHA-256. The resulting hash is a 256 bit which is encoded using base32. The hash performance is calculated as follows.



Graph-1: Hash Performance

1. MEMORY USAGE:

Syncthing is preferable when you have less number of files. Size of the files depends on RAM size. It is suggestible to use disk space instead of saving data in RAM during the times when data goes to infinity for synchronizing. However syncthing supports syncing of files at a maximum rage of ~12GB. Memory space utilization is shown in following graph.



Graph-2: Memory Usage

IV. FUTURE ENHANCEMENT

Since the existing systems include Third party auditing techniques for securing data in cloud also raised several issues. There may be situations where TPA could have illegal access to the client's data or data present in cloud sever. In the proposed design, data integrity verification is done using hash service, encryption/decryption service and outlining the list of individuals which may access information firmly by a trusted third party that is variant from storage cloud supplier. This involves in using a distributed file system where the privacy, data integrity and security is incorporated by encrypting the data using symmetric and asymmetric cryptography while uploading the data into the cloud by the clients.

This is done by using AES and RSA algorithms thereby securing the session between the client and cloud server. For this to implement an open source cloud called "Syncthing" is used for incorporating the symmetric and asymmetric cryptographic techniques and thereby results will be obtained.

V. CASE STUDY

The cloud will be at risk any time for service and account hijacking. This hijacking or attacks may occur in any number of types. Since cloud is a network running on various servers there are chances where it is vulnerable to all such attacks. In 2010 one of the companies that vanguard-Amazon.com, Inc. was targeted by an attack where the hijackers performing Cross-site scripting (XSS) attack gained credentials and were successful. They pervaded the Amazon Relational Database Service (RDS) so that to have the backend into Amazon System even though if they lose their original access. This whole process was done by injecting Zeus Trojan horse (malware) on various machines, where the infected computer started reporting to Amazon EC2 for updates and instructions by gaining access.

This study gives the brief description of security issues occurring in cloud systems leading to huge loss of sensitive data and hindrance of various organizations nevertheless small or large scale and business market.

VI. CONCLUSION

Cloud computing is extremely beneficial for storing and processing of huge volumes of data, where such large volumes of data are organized by several distributed files systems. In the perspective of authentication and security many issues arise while storing data in the cloud. The proposed procedure brings forth the implementation of technique for securing data by using both symmetric and asymmetric cryptography while uploading the data into the cloud. The advantage of this method is it can be incorporated in free open source cloud systems like syncthing, seafile, etc where the users couldn't afford for cloud systems like Amazon Ec2, IBM etc that require payment access without any participation of TPA. This indeed helps various small scale organizations to secure their data by uploading them in open source cloud systems with the help of cryptographic techniques.

REFERENCES

1. Ranjith, G., et al. "Intelligence based Authentication-Authorization and Auditing for secured data storage." *International Journal of Advances in Engineering & Technology* 8.4 (2015): 628.

2. Jachak, K. B., et al. "Homomorphic authentication with random masking technique ensuring privacy & security in cloud computing." *Bioinfo Security Informatics* 2.2 (2012): 49-52.

3. Badhe, Mayuri V., and Prabhakar L. Ramteke. "A Survey on Privacy-Preserving Public Auditing for Secure Cloud Storage Using Third Party Auditor." *International Journal of Computer Science and Mobile Computing* 4.1 (2015): 168-174.

4. Wang, Qian, et al. "Enabling public auditability and data dynamics for storage security in cloud computing." *IEEE transactions on parallel and distributed systems* 22.5 (2011): 847-859.

5.Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." *IEEE transactions on computers* 62.2 (2013): 362-375.

6. Nepal, Surya, et al. "DIaaS: Data integrity as a service in the cloud." *Cloud Computing (CLOUD), 2011 IEEE International Conference on*. IEEE, 2011.

7. Song, Ningning, and Yueyun Chen. "Novel hyper-combined public key based cloud storage key management scheme." *China Communications* 11.14 (2014): 185-194.

8. Jensen, Meiko, et al. "On technical security issues in cloud computing." *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*. IEEE, 2009.

9. Rupa, Remidicherla. "Auditing outsourced data on cloud using HLA with random masking technique." *Journal of Engineering Development and Research* 3.3 (2015).

10. Govinda, K., and E. Sathiyamoorthy. "Data Auditing in Cloud Environment using Message Authentication Code." *International Conference on Emerging Trends on Advanced Engineering Research (ICETT)*. Vol. 11. 2012

11. Lin, Hsiao-Ying, et al. "Toward data confidentiality via integrating hybrid encryption schemes and Hadoop distributed file system." *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on*. IEEE, 2012.

12. https://syncthing.net/

13. Quinn, Conor, et al. "Forensic analysis and remote evidence recovery from syncthing: An open source decentralised file synchronisation utility." *International Conference on Digital Forensics and Cyber Crime*. Springer, Cham, 2015.

14. Paul, Partha Sarathi, et al. "On design and implementation of a scalable and reliable Sync system for delay tolerant challenged networks." *Communication Systems and Networks (COMSNETS), 2016 8th International Conference on*. IEEE, 2016.

15. Štědronský, Filip. "A decentralized file synchronization tool." (2017).

16. Endo, Patrícia Takako, et al. "A survey on open-source cloud computing solutions." *Brazilian Symposium on Computer Networks and Distributed Systems*. Vol. 71. 2010.

17. Rimal, Bhaskar Prasad, Eunmi Choi, and Ian Lumb. "A taxonomy and survey of cloud computing systems." *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*. Ieee, 2009.

18. Blaze, Matt. "A cryptographic file system for UNIX." *Proceedings of the 1st ACM conference on Computer and communications security*. ACM, 1993.

19. Harrington, Anthony, and Christian Jensen. "Cryptographic access control in a distributed file system." *Proceedings of the eighth ACM symposium on Access control models and technologies*. ACM, 2003.

20.http://www.pcquest.com/?s=syncthing+file+synchronization

21. http://www.pcquest.com/8-self-hosted-cloud-storage-solutions-2/