

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Preserving Data Integrity and Data Dynamics by Using Third Party Auditor in Cloud Computing

Lavanya G¹

Mtech, dept. of CS&E
P.E.S College of Engineering
Mandya – India

Sanjay H M²

Assistant Professor, dept. CS&E
P.E.S College of Engineering
Mandya – India

Abstract: Cloud computing is acquiring a huge attention in IT industry which changes the way of doing business. Based on the user demand it delivers computing as a service by pay per use model and moves all the uploaded data to large data centres. The proposed design helps the cloud user to store his important data with high quality cloud applications and very low computational cost and light communication by providing effective services. Cloud service provider takes care of all the data that are moved to larger data centres which is not as trustworthy as there is a chance of misusing the stored data without the knowledge of user. To improve the data confidentiality and data integrity in cloud service provider side a new model is introduced which decreases the fear of data being misused. In this model a new third party security vendor has been added to reduce the burden of owner which takes care of stored data security that reside on the cloud service provider side. The third party auditor ensures the data integrity by verifying the correctness of data in cloud storage and fast error localization in identifying misbehaving servers. Cloud data is dynamic in nature supporting secure and efficient dynamic operations on data like insertion, delete and restore. This proposed scheme is highly efficient and resists against byzantine failure, malicious data modification attacks and even server colliding attacks.

Keywords: Cloud computing, Cloud service provider, Third party auditor, Data security model.

I. INTRODUCTION

Cloud computing has getting more and more attraction towards IT industry which changes the way of doing business by proving computing as a service to the user by pay per use model. It acts as an alternative to industries based on traditional client-server model. Cloud computing helps the user to move their data and application software to the network which is different from traditional solutions [1]. Cloud computing has the capacity to change the entire working of IT industry and often said as most promising technology. On considering the term computing refers to as application as a service, software as a service and platform as a services. Cloud computing renowned when amazon lend their server space to outside world at moderate cost. By this many startup companies and small companies make use of cloud computing which was not able to furnish separate hardware and software for their business. As the company pay based on what the resource has been used for their business it reduces the cost by large number. After this most of the companies started storage business which was a real big deal to earn profit providing storage as a service. It provided gain for both cloud service provider and as well as the cloud users. The term cloud in IT industry brings new promising technologies like SMAC by IBM and many others. By these centuries in the middle of the technology era which changes the way computing takes place with its features which has being used in all IT industries. Cloud computing is also considered as marketing hype which brings a new face to old technologies such as virtualization, grid computing and utility computing.

Cloud computing is used in order to reduce the cost on storage and applications which are mostly needed in IT industries. It is greatly used by all startup companies to buy storage space from cloud service provider based on their demand and only pay

for what the resource they has been used. Likewise cloud computing also provides most of choice to user such as what kind of software they wish to use and only pay for it and the user can also check for the suitable software. Based on the variety of services they provide cloud computing has become more comfortable. Cloud computing consists of loosely coupled components which are combined to work together and are interconnected with each other for communication between them [2].

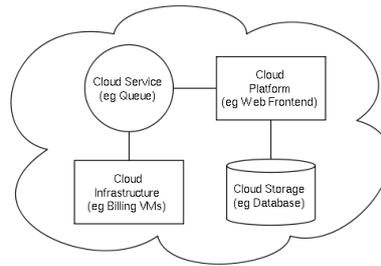


Fig. 1 Cloud architecture

Cloud computing are proprietary technology whereas grid computing are based on open source technologies. Cloud service provider knows how data requests, security arrangements and managed. Cloud computing consists of multilayer know as front end layer and back end layer. Front end helps the user to interact with the software whereas back end consists of hardware and software architecture which delivers data to frontend [3]. There are 3 cloud service delivery models that are application as a service, platform as a service and infrastructure as a service.

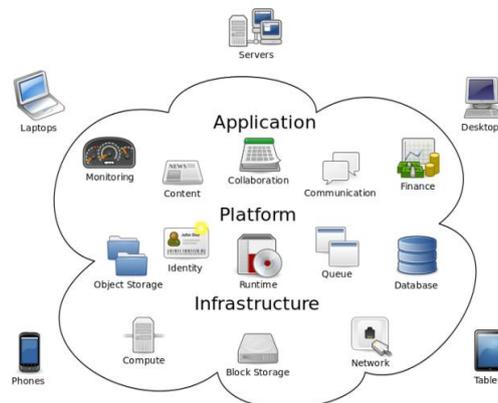


Fig.2 Cloud computing services

II. SECURITY IN CLOUD COMPUTING

Security plays a very important role in cloud computing to all enterprise cloud computing is a greatest advantage it made possible for some of the security issues to be rectified and provide solution to all security related problem. Cloud computing can't sustain in computing industry, if security issues are not solved. To overcome by this all the security issues in cloud computing has to be nullified. Cloud computing has to made sure that both cloud users and cloud service provider data are safe without any internal or external thread.

A. Different security issues in cloud computing

Cloud computing provide different security issues hat incline he use directly or indirectly [4], few of them are listed below .

- Data confidentiality is lost when the user data has been accessed by other user.
- Data integrity is the data obtained from the cloud should be same as the data stored in the cloud no others should be able to access the data in the middle that belongs to particular user.
- Data authentication is the most important aspect as only the registered users are able to authenticate to server to access data.
- Data loss occurs when hacker attacking the data to the closest server as data is the most valuable assets of any user.

- Data location may be an issue if the user does not want his data to be stored somewhere in the world as the uploaded data can be stored anywhere.

B. Security model based on trusted third party

Trusted third party helps the user by reducing the burden by doing the work on behalf of the user. Trusted third party are used for many purpose, one of the main advantage is that for checking data integrity that is the data sent to the cloud service provider must be same as the data that is received by the cloud service provider. There are also other purpose using third party for encryption and decryption, authentication and other little task needed for security aspects [5].

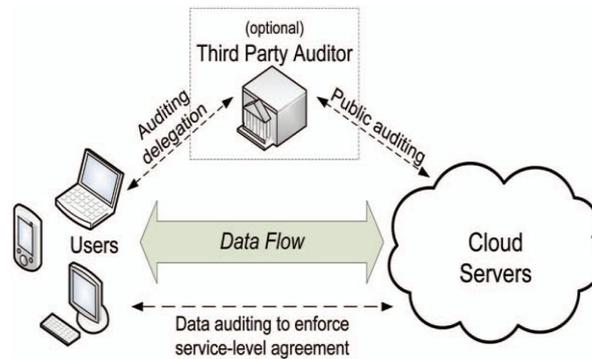


Fig.3 Cloud computing with trusted third party

C. Existing system problems

There are many problems in using existing method like trusted third party concentrates more on data inspection rather than data security in cloud computing. It has more burden on the client side as the load increases to do encryption and decryption of the data and does not involve in privacy protection of the data. It does not perform anything on the cloud service provider side like encryption and decryption of the data [5].

D. Related works to overcome the problems including trusted third party

Trusted third party ensures data integrity and dynamic data correctness for multiple users at a time simultaneously and efficiently with RC5 encryption algorithm [6]. By using RC5 encryption algorithm it reduces computational cost providing high efficiency handling multiple users. Another model use digital signature method for verifying correctness of data [7]. It is easy to implement and support all the features by providing more security to the user by using RSA and also propose a way to implement TPA which not only checks the data integrity and consistency using RSA algorithm on client side. Another model proposed by assuming TPA as a trusted one where user authentication can be done by using TTP [8]. Here the login is secured and authenticated which is simple and effective method by using salt and hash function for data integrity. Another specific method has been proposed to address the data integrity, data confidentiality and authentication which check the correctness of the data by using TTP [9]. It successfully checks the data integrity for the data stored in the system and also hashing has been done on trusted third party side using the algorithms like RSA, DES, and AES. Another more specific method with data integrity as the main objective is provided by using Merker Hash Tree algorithm is done seeking the help of TTP depending on the cloud user request. Here Merker Hash Tree algorithm has been used to ensure data integrity in cloud computing [10]. This method has an advantage that data integrity can be monitored easily and data inspection is more

III. PROPOSED SYSTEM

A. Motivation

The cloud computing user has mistrust on cloud service provider where it can used the data without the knowledge of the owner, to overcome this disadvantage we propose a new model with trusted third party which we assume it as a secured one. Trusted third party takes care of 3 major factors they are data confidentiality which is satisfied by performing data encryption

and decryption on trusted third party side on behalf of the user, data integrity are obtained using hash technique on the trusted third party side and data authentication is achieved with the help of one time password system to the user by trusted third party.

B. Architecture

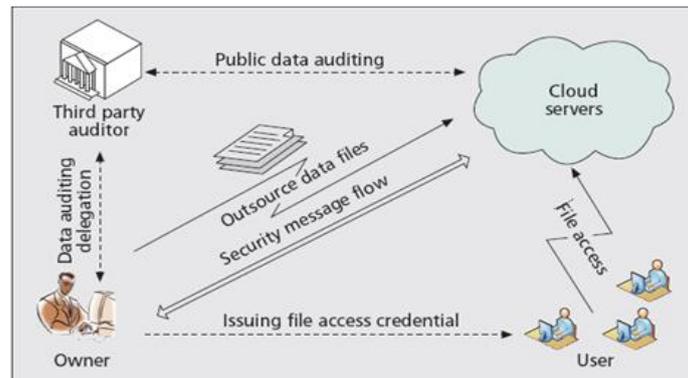


Fig.4 Proposed model with trusted third party

- Owner: Owner is an entity which is responsible for storing the data that user wish to upload to the cloud data storage.
- Cloud service provider (CSP): CSP is an entity which is totally responsible for storage of the data. There is a connection between the CSP and TTP which helps in encryption of data that are going to be stored on cloud storage.
- Trusted third party (TPA): TPA is an entity which consists of capabilities for encryption and decryption services. It helps the user by encrypting the data and storing it on the cloud and decrypts the data when any other registered users access the data.
- User: user is an entity who accesses the required data by requesting the owner to get the permission to access the data.

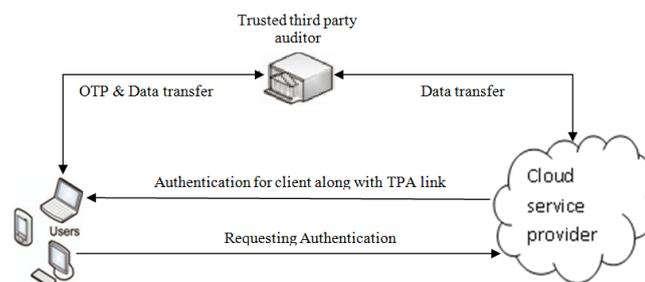


Fig.5 workflow of module with trusted third party

C. Algorithms

a) Data Confidentiality

Data encryption on the cloud storage can be done by using both symmetric key and asymmetric key [9]. Symmetric key algorithm has high performance and can do faster compared to asymmetric key algorithm. Symmetric key algorithm is used for cloud storage which contains a large set of database. Algorithms like RSA, DES, 3DES, AES, RC4, DH, blowfish are used for encryption and decryption purpose [11]. ASE is a simple symmetric technique and can be implemented faster than DES and finally blowfish. In RSA algorithm is faster than DH algorithm which uses asymmetric key technique.

b) Data Integrity with Hash Codes

Hash value is nothing but a numeric value of fixed length that identifies the data uniquely. It uses digital signature and represent a large amount of data with a small numeric value. Signing a hash value is more efficient than signing a large value. It is also used to check data integrity for the data passing through insecure channels. The hash value of sent data is compared with the hash value of received data by which we can identify the data which is modified.

c) *OTP (Authentication)*

OTP is abbreviated as one time password which is valid for only one time login session or transaction on computer system or any other digital device. OTP's avoid traditional method associated with number of shortcoming. OTP's are not vulnerable to replay to attacks as they contrast with static passwords to address important shortcoming [11]. The major advantage is that an attacker who manages to record the OTP that was already used to login to a service once will not be valid anymore. Users who use some password to multiple systems are discarded to all of them, if one the password has been hacked by the attacker.

IV. CONCLUSION

The proposed model is very useful for the user to trust the cloud computing so that the more potential customer can use cloud computer without fear of misuse of data. The TPA helps with the authentication, data confidentiality and data integrity thus achieving security for the user's data and also maintain storage correctness assurance if user delete or modify the data. It ensures the user that their data are stored appropriately and kept intact all the time in cloud. If there is any data modification it automatically replaces the data and informs the owner about the attacker if there are any with his location and user ID to take serious actions to stop the hacker.

ACKNOWLEDGEMENT

It's my immense pleasure to express my indebtedness to my guide Mr. Sanjay H.M, Assistant professor, department of Computer Science & Engineering, who guided me at various stages and I also thank the principal and management P.E.S. College of Engineering, Mandya.

References

1. Shuai Han, Jianchuan Xing, "Ensuring data security through a novel third party auditor scheme in cloud Computing", Proceedings of IEEE CCIS2011.
2. http://en.wikipedia.org/wiki/Cloud_computing
3. <http://www.cloud-lounge.org/how-do-clouds-work.html>
4. Cong wang, Qian wang, Kui ren, Ning cao and wenjing lou, "Towards secure and dependable storage services in cloud computing" IEEE transaction in cloud computing.
5. M. Thamizhselvan, R. Raghuraman, S. Gershon Manoj, and P. Victor Paul, "A novel security model for cloud using trusted third party auditor" IEEE sponsored 2nd International Conference on innovation in Information Embedded and Communication system.
6. R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
7. Nuppor M. Yawale, V. B. Gadichcha, "Third Party Auditing (TPA) for data storage security in cloud with RC5 algorithm", International Journal of Advanced Research in Computer Science and Software Engineering 2013.
8. Abhishek Mohta, Ravi Kant Sahu, Lalit Kumar Awasthi, "Robust Data Security for cloud while using Third party auditor", International Journal of Advanced Research in Computer Science and Software Engineering 2012.
9. Susmita J A Nair, Anitha K L, Rosita F Kamala, "Trusted Third party Authentication in cloud computing", International journal of Engineering Research and Technology 2013.
10. Patel Himani Atulkumar, Patel Srushti Hasmukhbhai, "Cloud Model -With TPA (Third Party Auditor)", International journal of Research in engineering and advanced technology 2013.
11. K. Meenakshi, Victo Sudha George, "Cloud Server Storage Security using TPA", International Journal of Advanced Research in Computer Science and Technology 2014.
12. P. Victor Paul, A. Ramalingam, R. Baskaran, P. Dhavachelvan, K. Vivekanandan, R. Subramanian and V. S. K. Venkatachalapathy, "Performance Analyses on Population Seeding Techniques for Genetic Algorithms", International Journal of Engineering and Technology (IJET), Vol 5, No 3, Jun-Jul 2013, pp. 2993-3000.
13. Figure Retrieved from http://en.wikipedia.org/wiki/Cloud_computing.