International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Survey on Privacy preserving public auditing scheme for shared data in cloud

Ms.Kirtee Chaudhari & Prof. Sonali Patil

Department of Computer Engineering JSPMS Bhivrabai Sawant Institute of Technology & Research,
Wagholi pune, Maharashtra, India
kirteechaudhari09@gmail.com
Department of Computer Engineering JSPMS Bhivrabai Sawant Institute of Technology & Research,
Wagholi pune, Maharashtra, India
psonali119@gmail.com

Abstract— *Cloud computing permits not only to get computing resources on-demand however additionally to store massive amounts of data (big data) with a high level of fault tolerance. Nevertheless, information confidentiality for users of hybrid and public clouds is cannot secured fully. Cloud suppliers have full access to user information that threatens to compromise the integrity of data. Existing ways of providing security think about ways to increase the speed and scale back the load throughout authorization and encryption. The paper proposes a way that describes the use of separate services outside the cloud for authentication, data management and data storage to eliminate the possibility of getting unauthorized access to information, and therefore the use of data to perform integrity management. The developed technique is getting used to form a stand supported OpenStack and two services on separate servers. The owner of the database limits the access to information that's hold on in an encrypted type and doesn't allow provider to move with database.*

Keywords—Signaturet; Distributed Matching Engine; 3D,2D

I. INTRODUCTION

Due to an opportunity to get computing resources on demand, Cloud computing allows not only finishing up resource intensive computations, however additionally storing massive amounts of information. Moreover, data keep in cloud computing is protected from faults of hardware. Nonetheless, when victimization cloud computing, and distributed cloud storage (DCS) especially, there arises a spread of topical problems related to confidentiality and integrity of data within the process of each storage and transmission. A cloud service provider has a vast access to the information stored, and this aspect becomes particularly necessary once public or hybrid clouds area unit used and also the solely issue users will suppose is decency of the provider. That's why confidentiality in cloud computing is a very important security interest each users and providers. The difficulty of trust to use of cloud resources, and to DCS especially, is directly associated with the problem of guaranteeing data security This issue has been taken under consideration in multiple reports, such as IDC Cloud survey 2015 [1], RightScale State of Cloud Report 2016 etc. data is accessed in associate unauthorized approach, once information isn't encrypted. Methods of ensuring confidentiality that area unit in use at the moment area unit ineffective for cloud computing. This matter has been lined in various surveys created by Dai [3–5]. Mao [6] contributed a concept of associate authentication medium while not a certificate however victimisation private key generators (PKG) instead. The major drawback with victimisation private key generator systems lies in access the owners need to key generators and a break to use them for decrypting of information inside cloud computing. An ID-base authentication for cloud computing [7] was proposed on the idea of works by Lim. The solutions proposed change acceleration and reduction of load within the method of authentication, however they are doing not improve confidentiality and, therefore, don't enhance security of the information stored.

- **Data Security:**

1) Confidentiality :

Data confidentiality is that the property that data contents are not created on the market or disclosed to hot users. Outsourced data is hold on throughout a cloud and out of the owners' direct management. Only approved users can access the sensitive data whereas others, along with CSPs, should not gain any information of the information. Meanwhile, data owners expect to altogether utilize cloud information services, e.g., data search, data computation, and data sharing, while not the leakage of the information contents to CSPs or different adversaries.

2) Integrity

Data integrity demands maintaining and reassuring the accuracy and completeness of information. A data owner continuously expects that his data during a cloud is hold on properly and trustworthily. It means the data shouldn't be illegally tampered, improperly changed, deliberately deleted, or maliciously made-up. If any undesirable operations corrupt or delete the info, the owner ought to be able to find the corruption or loss. Further, once a little of the outsourced data is corrupted or lost, it will still be retrieved by the information users.

II METHODS OF SAFE DATA HANDLING

Information security is geared toward ensuring three aspects of security, like confidentiality, integrity and accessibility. Ensuring information confidentiality implies a necessity to confirm controlled access to specific objects at intervals a system. It would be affordable to encipher databases before transmission them to cloud computing. In addition, it's needed to limit access of users to the information hold on by dividing users supported their rights of access. All operations with encrypted information allotted in cloud computing should be performed while not decryption. This will create it not possible to intercept encryption keys on the aspect of cloud computing. It is essential to store encryption keys on the far side cloud computing. So as to ensure integrity, a system of storage and generation of data supported checksums of data and time is introduced. The set of methods of encrypted information handling in DCS that we've got developed consists of procedures of saving, receiving and deleting data from DCS

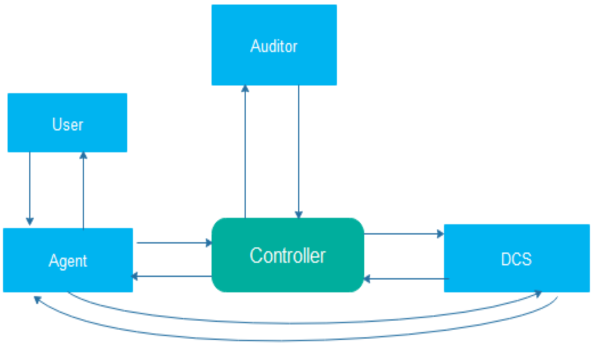

Fig: 1 Methods of encrypted data handling within a distributed cloud storage.

Methods of encrypted information handling include four key elements, like an agent, a controller, an auditor and a DCS. The agent is put in on client's hardware and contains all procedures of saving, reading, deleting, encrypting and decrypting of information, further as requests for authentication and authorization for accessing a DCS and algorithms of client's data encryption and causing information to nodes among the DCS.

The controller is chargeable for storing data regarding files during a info and contains procedures of receiving tokens and data distribution to nodes among the DCS, and authentication and authorization procedure using the auditor. In this case, there square measure 3 objects of interaction within the method of authorization (a user, cloud computing platform associated an auditor), whereas two of them share common data that's unknown to the third one. Within the process of verification, the user receives numerous identifiers (tokens) with a selected life span. And now, allow us to verify the procedure of saving data in a DCS

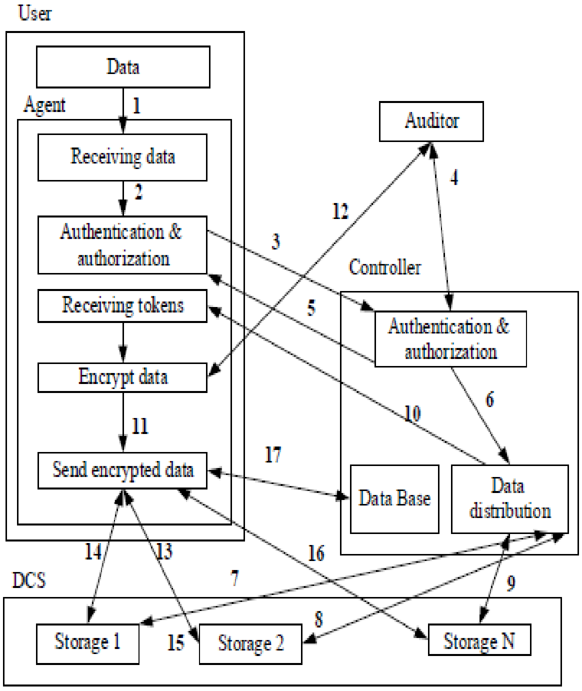

Fig: 2 Procedure of saving encrypted data in a distributed cloud storage

Fig. 2 represents a diagram of saving information during a DCS. The user provides unencrypted information to the agent (Step 1). The user enters his/her ID data (Step 2) that is distributed to the controller by the agent (Step 3). The controller verifies user's access rights with the auditor (Step 4). If the user has been authorized with success, the controller notifies the user (Step 5) and sends requests to nodes of the information repository.

In order to get direct access to nodes of the DCS, the agent can receive data containing tokens in an exceedingly specific node that may permit the agent to quickly access the DCS node so as to save lots of information. check and encrypted data control is meted out using information and, thus, integrity of the former is verified. The controller sends an invitation for temporary access to choose nodes so as to save lots of data and receives tokens for access from DCS nodes (Step 9). The controller sends the tokens to the agent (Step 10) that are then distributed between the nodes (Step 11). Further, segments of information are encrypted (Step 12) and transmitted to the algorithmic rule of sending data (Step 13) that dis-tributes the encrypted segments between the nodes (Steps 14–16). When the DCS nodes have received information, the agent receives information concerning location of the info} that's sent to the database (Step 17). The procedure of receiving information from a DCS is given below (Fig. 3).

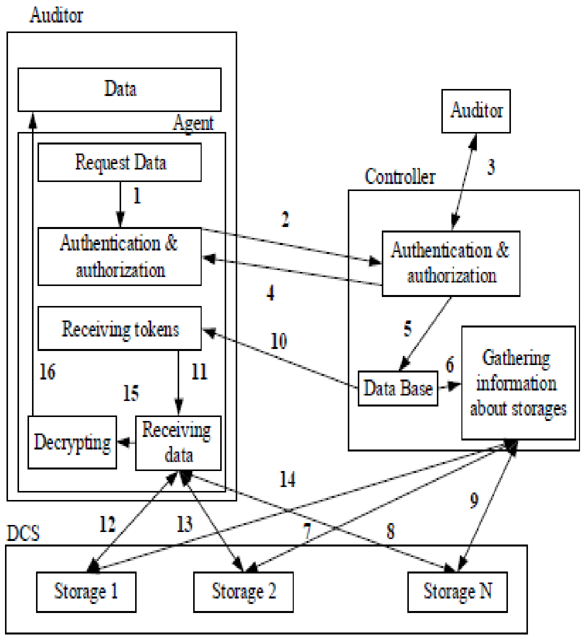

Fig. 3. Procedure of receiving data from a distributed cloud storage.

A consumer sends a request for information (Step 1), within the same manner as it is completed within the procedure of causing information to a DCS. The user is documented and licensed (Steps 2-4). The controller matches the requested information with their location within the DSC (Step 5).

Accessibility of encrypted segments of the information is verified (Step 6) and access tokens are transmitted. Then requests are sent to nodes of the DCS (Steps 7–9) and also the controller sends the tokens to the agent (Step 10), that are responsible for starting the method of loading fragments (Steps 11–14). When the fragments are received (Step 15), the agent decrypts and saves the info (Step 16).

Deleting information from a DCS is distributed during method analogous to the opposite procedures. A user is allowed. In turn, the controller inquires for an opportunity to hold out the operation and accessibility of information for this user from the auditor. Upon verification the info keep within the DCS is deleted on the idea of the data available.

The process of encrypting separate segments of information running at the same time with automatic creation of containers for encrypted data turns the service model of cloud computing known as “Encryption as a Service (EaaS)” into an efficient solution. We’ve chosen to use block encryption looking on previous blocks. The running process of this kind of encryption has been established by the international standard IOS/IEC 10116 [8] and the nist 800- 38A guidelines [9]. It’s potential to reinforce quality of this cipher exploitation message authentication codes [10], authenticated encryption [11], and pseudorandom permutations [12]. And currently we add a refutable encryption algorithm to the block encryption algorithm we've chosen. The principal distinction lies within the range of keys every of which carries out resultant operations with data.

A consumer who desires to stay information in a DCS will produce fictive information additionally to actual data, that it'll be 274 possible to produce using the primary key, if a social engineering attack takes place. A consumer can even modify the primary key thus on provide at random generated information which will not be enough to protect the latter against social engineering attacks however still, it will add quality to successful use of different cryptologic methods.

The preceding set of ways of safe encrypted information handling that ensures a chance to hold out operations with encrypted data while not decrypting has been implemented based on OpenStack platform. So as to encrypt information, an EaaS-service supporting “deniable encryption” has been deployed. Authentication and control ar carried out by associate auditor and a controller severally in an allocated phase of the network. We’ve got tested the system for gaining unauthorized access and violation of integrity of encrypted information. Furthermore, we have distributed a series of tests attempting to crack encrypted information.

III Conclusion

The set of strategies proposed during this article allows delimiting access to users and providers of cloud computing by their roles. Access is restricted by the owner of a information him/herself, whereas information is hold on in an encrypted kind that does not enable the cloud computing supplier using the data without a particular encryption key. At a similar time, the auditor doesn't have data regarding authentication to receive encrypted information from the cloud computing platform. Complexity of the encryption algorithm and use of strategies of data handling in cloud computing can alter improvement of data security and hacking resistance. Moreover,it will be almost not possible to compromise information as a result of verification of checksums stored by the auditor.

References

[1] Boneh D., Gentry C., Hamburg M. Space Efficient Identity Based Encryption without Pairings. Proceedings of FOCS 2007, Providence,20-23 Oct, 2007 y. Providence, 2007, P. 647–657.

[2] Boneh D Generalized Identity Based and Broadcast Encryption Schemes. ASIACRYPT 2008. LNC Springer. 2008. V. 5350. P. 455–470.

[3] Hongwei Li. Identity-Based Authentication for Cloud Computing. CloudCom 2009, LNCS 5931. Springer-Verlag Berlin Heidelberg. 2009.P. 157–166.

[4] S. E. Arasu, B. Gowri, and S.Ananthi, "Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 2, no. 1, March 2013.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," in *Proceedings of the 14th European conference Research in Computer Security (ESORICS'09)*, Saint Malo, France, 2009, pp. 355-370.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in*Proceedings of the 29th Conference on ComputerCommunications (INFOCOM'10),* San Diego, USA, IEEE, 2010, pp. 1-9.

[7] T. S. Khatriand G. B. Jethava, "Survey on data Integrity Approaches used in the Cloud Computing," *International Journal of Engineering Research & Technology* (*IJERT*), vol.1, no. 9, November, 2012.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proceedings of the 17th International Workshop on Quality of Service (IWQoS'09)*, Charleston, South Carolena, IEEE, 2009, pp.1-9.

[9] Godhankar P B, Gupta D. Review of Cloud Storage Security and CloudComputing Challenges[J]. International Journal of Computer Science & Information Technolo, 2014, 5 (1):528-533.

[10] Tiwari D, Gangadharan G R. A novel secure cloud storage architecture combining proof of retrievability and revocation[C]. Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015.

[11] Spoorthy V, Mamatha M, Kumar B S. A Survey on Data Storage and Security in Cloud Computing [J]. International Journal of Computer Science & Mobile Computing, 2014, 3(6).

[12] Vrable M D. Migrating Enterprise Storage Applications to the Cloud[J]. Dissertations & Theses - Gradworks, 2011, 12(5):507-584.