iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 Issue: VI Month of publication: June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6011

Securing Data in Clouds-A Review

Aayushi[1], Natasha Sanjay Ayare[2], Manish R[3], Shreyas G[4], Gowrishankar B S[2]
[1, 2, 3, 4]B.E. Students, Dept of Information Science and Engineering, Visvesvaraya Technological University, INDIA
[5]Assistant Professor, Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Karnataka, INDIA

Abstract: Cloud computing is a popular approach that is used to store any kind of data or information over the internet rather than storing it on our desktops. But there is one major issue that arises when we wish to adopt this method which is the security of the data of the user. When data is stored in the cloud it is not completely under the control of the user. So we need to make use of methods that will make sure that the data of the user stored in the cloud cannot be accessed by the cloud service provider and that only valid or authorised users can access the data. These methods will ensure security of the data and will increase the rate of adoption of cloud computing services.

Keywords: Cloud computing, security, cloud service provider, authorised users

I. INTRODUCTION

The use of cloud to store and access data is becoming common these days. Cloud computing makes use of a network of servers to store and manage data. It is also used to share resources. Applications of cloud computing do not have to be installed on the computer of the user. They can also be accessed from any location. It allows multiple users to use the data at the same time hence increasing productivity.

Cloud computing includes security risks like identity theft, malware infections, compliance violations, denial of service attacks, negligence of the employees in an organization , the loss of important data and inadequate backup of data, phishing and other attacks, or system vulnerabilities. In this paper we discuss the different ways to keep the data in clouds safe and secure. It includes using methodologies like decentralized access control in clouds, symmetric encryption, certificateless proxy re-encryption, privacy preserving authenticated access control, secret sharing algorithm and using multi clouds.

II. RELATED WORK

1) Paper [1] The authors V. Gowthami and Dr. M. Sreedevi have proposed a data centric access control solution that focuses on protecting the data of the user that is stored in cloud. The techniques used for protection are identity based and proxy re-encryption. This method makes sure that the service provider does not access the user data. It uses rule-based approach to make sure that the access rules are under the control of the user.

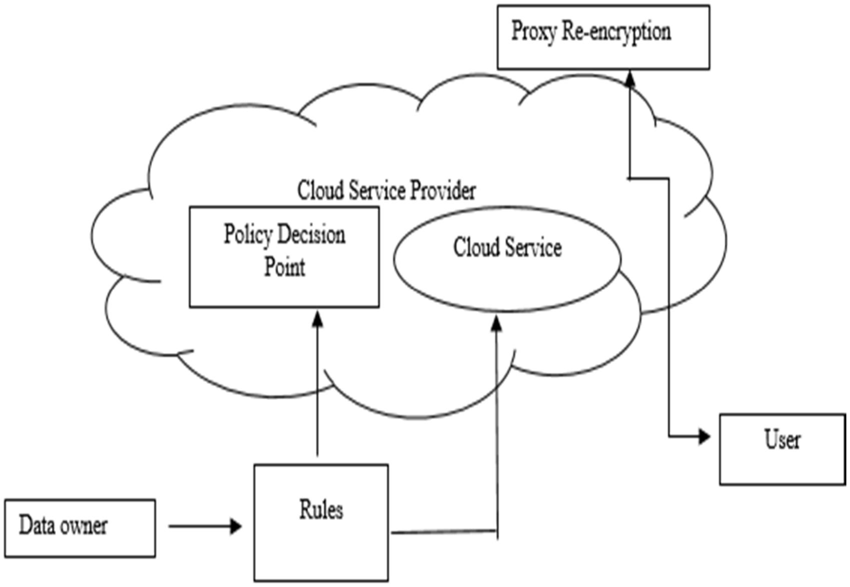

Figure 1 Data centric access control solution

2) Paper [2] The authors Mazhar Ali, Revathi Dhamotharan and Eraj Khan have proposed a method to encrypt a file to be stored in the cloud using a single encryption key. The SeDaSC methodology deals with the insider threats by generating two key shares, one key for the user and another key for a trusted third party called the cryptographic server. If a user has the key then he becomes a legitimate user of the data. The cryptographic server is used to authenticate the user and on authenticating him it can download the data from the cloud. Symmetric encryption is used here.

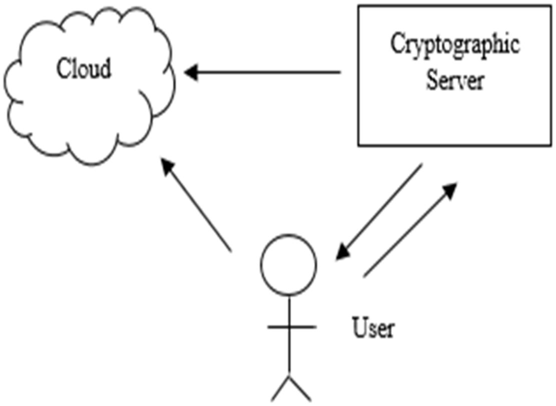

Figure 2 SeDaSC methodology

3) Paper [3] The authors Lei Xu, Xiaoxin Wu and Xinwen Zhang have proposed a Certificateless Proxy Re-encryption scheme to secure the sharing of data in cloud. First the data in the cloud will be encrypted by the owner of the data using an encryption key then that will be again encrypted by the cloud before this data is received by any recipient. The re-encryption keys are derived from the private key and public key of the data owner and recipient respectively. This eliminates the need to use a certificate and also the key escrow problem. Certificates are also not required to authenticate the public keys.

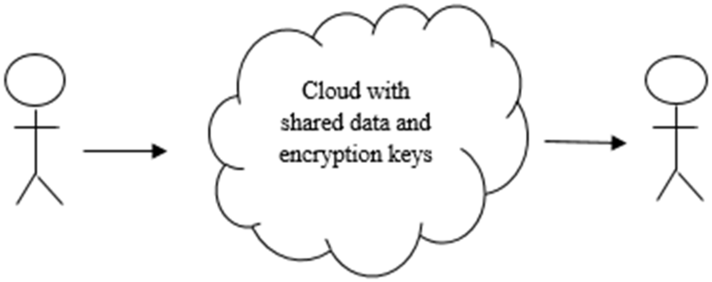

Figure 3 Certificateless Proxy Re-encryption scheme

4) Paper [4] The authors Ranjita Mishra and Sanjit Kumar Dash have proposed a method to secure the data in clouds by the use of a privacy preserving repository. The privacy preserving repository will control the access and usage of the shared data. It allows the owner of the data to entrust all the computation related tasks to cloud servers without revealing the actual contents. It is robust, cost-effective and secure according to standard security model.

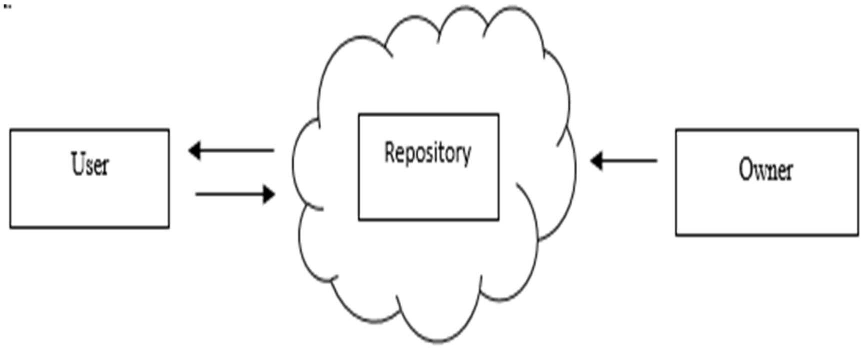

Figure 4 Privacy preserving repository

5) Paper [5] The authors Qingni Shen, Lizhe Zhang and Xin Yang have proposed a method to make sure that data is migrated securely between cloud storage systems. This paper describes the threat while doing the data migration and proposes a mechanism to deal with this security issue. A prototype is designed for this mechanism that is based on HDFS (Hadoop Distributed File System). The cloud's Central Node is embedded with the MDM (Master Data Management) to secure data migration. The secure migration of data between clouds uses SSL negotiation, migration ticket design and block encryption in distributed file systems. By SSL protocol we can share parameters safely.

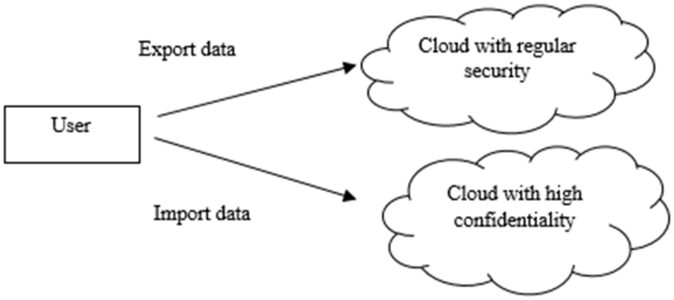

Figure 5 Secure migration of data between cloud storage systems

6) Paper [6] The authors A.Vijayalakshmi and R.Arunapriya have proposed the secure storage of data for decentralized access. It uses decentralized architecture and uses multiple KDC's for the key management. The stored information can be decrypted only by valid users. The cloud is not aware of the user's identity and only verifies his credentials. It is robust and prevents reply attack.

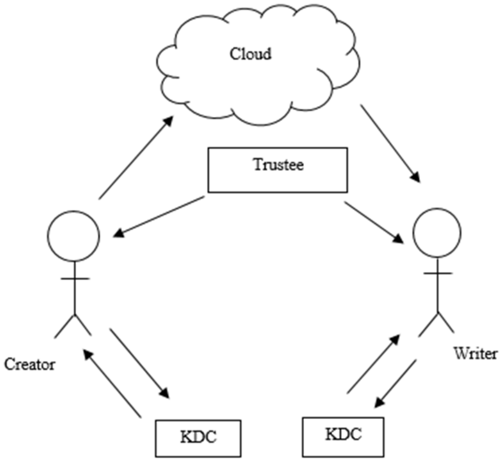

Figure 6 Decentralized architecture using multiple KDC's

7) Paper [7] The authors S Divya Bharathy and T Ramesh have proposed a method to secure data in clouds which makes use of decentralized key management for the keys and anonymous authentication of the user. The cloud makes use of a strategy involving attributes hiding and access control for security. It is robust and prevents reply attacks. The strategies used avoid issues relating to cloud services.

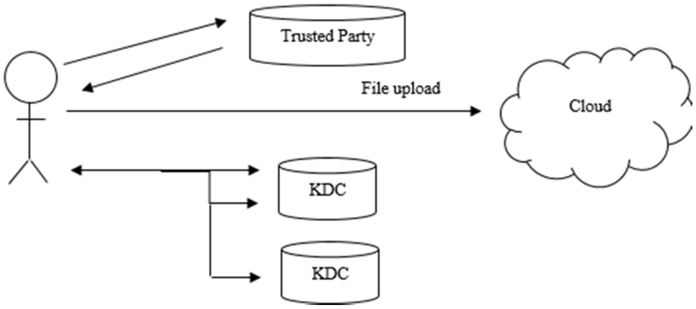

Figure 7 Decentralized key management

8) Paper [8] The authors M.Muhila, U.Hemanth Krishnaa, R.Kishore Kumara and E. A. Mary Anita have proposed a method to secure multi clouds. Single clouds suffer from security issues so users prefer using multi clouds which is also known as "cloud of clouds" or "inter clouds". The algorithm used is Secret Sharing Algorithm. Shamir proposed a secret sharing method that helps in storing of data in multiple clouds and encrypt it in the cloud before being transferred and saved.

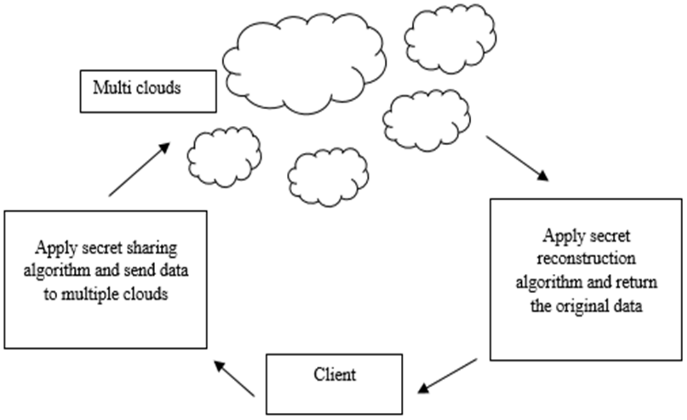
Multi clouds
Apply secret sharing algorithm and send data to multiple clouds
Apply secret reconstruction algorithm and return the original data
Client

Figure 8 Shamir's secret sharing for multiple clouds

III. CONCLUSION

Considering the security concerns relating to storing data in clouds, using a security solution is a requirement. We need methods that will be reliable, robust and efficient. The methods that prove to be that are identity based access control, proxy re-encryption and decentralized access. Through access control the cloud service providers will not be able to access the data of the user. It provides a comprehensive and feasible solution.

REFERENCES

[1] V.Gowthami, Dr. M. Sreedevi, "SecRBAC: Secure Data in the Clouds", International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885, Vol.07, Issue.04, April-2018, Pages: 0754-0757.

[2] Mazhar Ali, Student Member, IEEE, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Senior Member, IEEE, Athanasios V. Vasilakos, Senior Member, IEEE, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, Fellow, IEEE, "SeDaSC: Secure Data Sharing in Clouds", IEEE Systems Journal, 1932-8184, 2015 IEEE.

[3] Lei Xu, Xiaoxin Wu, Xinwen Zhang, "CL-PRE: a Certificateless Proxy Re-encryption Scheme for Secure Data Sharing with public cloud", 2012 ACM 975-1-4503-1303-2/12/05.

[4] Ranjita Mishra, Sanjit Kumar Dash, Debi Prasad Mishra, Animesh Tripathy, "A Privacy Preserving Repository for Securing Data across the Cloud", 978-1-4244-8679-3/11, 2011 IEEE.

[5] Qingni Shen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "SecDM-Securing Data Migration Between Cloud Storage Systems", 978-0-7695-4612-4/11, 2011 IEEE.

[6] A.Vijayalakshmi, R.Arunapriya, "Authentication of Data Storage using decentralized access control in clouds", Journal of global research in Computer Science, ISSN-2229-371X, Volume 5, No.9, September 2014.

[7] S Divya Bharathy, T Ramesh, "Securing Data Stored in clouds using privacy preserving Authenticated access control", International Journal of Computer Science and Mobile Computing, ISSN 2320-088X, Vol. 3 Issue 4, April-2014, pg. 1069-1074.

[8] M.Muhila, U.Hemanth Krishnaa, R.Kishore Kumara, E. A. Mary Anita, "Securing Multi-Cloud using Secret Sharing Algorithm", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), 1877-0509, 2015