International Conference on Modern Trends in Engineering Science and Technology
© 2019 IJSRSET | Volume 5 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Review on Privacy Preservation over Data Leakage in Cloud

Sanjay Kumar Sharma[1], Dr. Sarvottam Dixit[2], Dr. Manish Manoria[3]
[1]PhD Scholar, Computer Science and Engineering, Mewar University, Chittorgarh, Rajasthan, India
[2] Professor, Computer Science and Engineering, Mewar University, Chittorgarh, Rajasthan, India
[3]Professor SIRT Bhopal Affiliated to RGPV Bhopal, Madhya Pradesh, India
**Corresponding Author: sanjaysharmaemail@gmail.com*

ABSTRACT

Cloud centered computing is the conclusion of acceptance and development of present-day technologies and prototypes. There are various researches take place to achieve external and internal reviews of cloud security. The information should be conserved and protectively accessible. The dissimilar safety disputes in cloud are heterogeneity, scalability, Data Truthfulness, Data Intrusion, Non- Disclaimer, Concealment, access control, authentication and authorization. Confidentiality of information data is additional safety issue connected with cloud computing environment. The motive of this paper is to review various techniques which have been proposed till now in the reference of cloud data security along with comparing their techniques. This paper also imputes the advantages and disadvantages of data accessibility through cloud and issues related to the databases.

Keywords : Cloud Computing, Cloud Security, Data Concealment, Data Encryption, SQL, Data Protection.

I. INTRODUCTION

At its modest form, cloud based computing [1] is the self-motivated distribution of information knowledge capabilities and resources as a facility over the Internet. The cloud computing can be well-defined as innovative computational proficiencies that motivation on both academia and industry. Cloud computing resources are storage, network, applications, servers and services. The cloud computing architecture [2] includes four distribution systems, five key features and three service prototypes. Better broadband suitability, different development in digital information and data, data storage requirements vary, and the presence of cloud computing is centered on the presence of cloud based databases. An indispensable objective of cloud computing [3] is to make available access to the pay-ons on computer-based resources such as networks, databases, applications and platforms. Services like electricity, water, telephony, and gas. Cloud-based computing is a group of rules for allowing a suitable, universal, on-ground network. Cloud based providers are also called cloud service manufacturers, and cloud consumers are also called clients or cloud service users, who are the main columns in the cloud computing database. Cloud users can either be software service providers / applications. Cloud service provider is a company that provides financially effective cloud-based services using tools and programs.

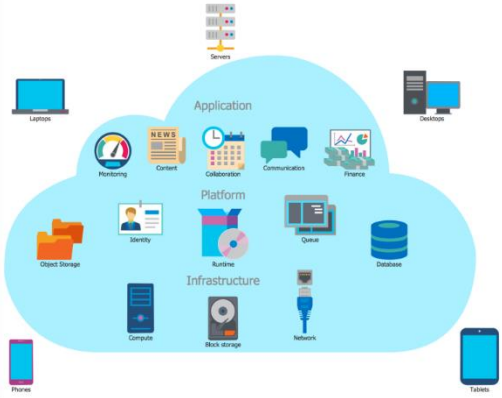

Figure 1.1 : Cloud Computing Environment [4]

There are 4 foremost types of cloud computing facility prototypes [5]. These models are DaaS Database as a Service[6], SaaS Software as a Service[7], IaaS Infrastructure as a Service[8] and PaaS Platform as a Service[9]. Database as a Service (DAAS)-Cloud database is aimed for virtualized computer based surroundings. It is none as modest as taking relational database management and positioning it over a cloud database server.

Platform as a service (PaaS), in platform as a facility ideal, service provider offers computer devices called hardware and software source programs that are also called as software towards the consumer that appeared for by him to database and web server. Software as a service (SaaS) Saas can be defined as the computer programs called software that is positioned over the network of network. Infrastructureas a service (IaaS) is the furthermost rudimentary cloud facility prototypical. It delivers computers virtual machines physical or and other resources. Figure 1.2 shows the cloud computing architecture.

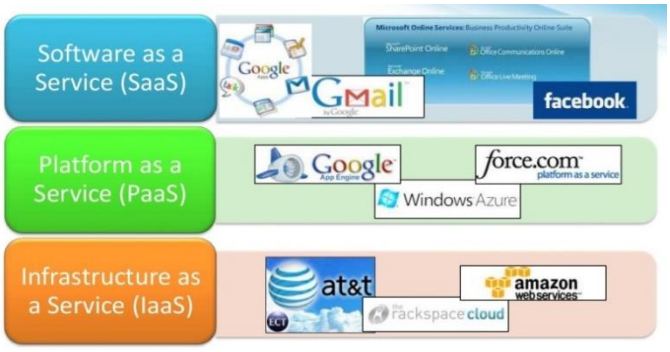

Figure 1.2 : Cloud Computing Architecture [10]

Cloud database security in one of the main issue in adoption of cloud database from customers view. Cloud database is basically public so anyone can access those databases. Audit, authentication and authorization are main security issues in cloud database. In cloud database information can be leaked due to various reasons. Privacy preservation of large organization cloud database from outside misuse is the main concern in adoption of cloud database.

II. RELATED WORKS

Boyang Wang et al. proposed a system which provides privacy protection for shared data in cloud computing using the public auditing method. The auditing method used the ring signature to provide verification process. This system includes public verifier, group of users and cloud servers. In this method, the specificity of the signer on each block in the collective data is kept private from the public verifier, validators are able to validate the truth of the shared information without retrieving the entire file. The method is capable of fulfilling all the inspection tasks at one place one by one, instead of confirming them. The method improves the efficiency and effectiveness of the method in auditing the shared information integrity. In some cases cloud database service providers may be financially motivated, so informing about this type of exploitation of information to inform users to protect their position and to circumvent subsequent revenue of their services can be informal. In privacy threats the uniqueness of the signer on every block in shared info is trustworthy and private to the group. All through during the method of auditing, a public auditor, who is merely permissible to verify the accuracy of shared info truthfulness, may try to expose the uniqueness of the signer on every block in shared info based on authentication metadata. When the public auditor exposes the uniqueness of the signer on every block, it can simply discriminate a great value object from others [11].

Lucca Ferretti et al. proposed a system that addresses both issues of cost and data privacy in cloud computing database as a services. These issues are very much necessary to adopt the cloud computing database. Although data encryption appears the ultimate in-built way out for data privacy. For performance point of view the SQL statements must be executed without decryption[12]. Some solution download the entire cloud database into native place and decrypt it. After decryption it execute SQL statements and encrypt it to store data in cloud

database. But this process have some performance problems. The proposed system also evaluate costs of encrypted as well as plaintext database. The information and data should be preserved and protected. Confidentiality of information data is additional safety issue connected with cloud computing environment. The database service cost can be legalized in instance of price variations and workload variations. Some encryption processes support comparison operations but do not select operators such as minus, union, intersect.

The disadvantage of encryption technology is that this plan is not suitable for long operations. This plan is also very complicated to implement because the database administrator does not perform every operation related to each database column [13].

R. N. Calheiros et al. proposed a system which is based on CloudSim that can support a database provider assessment of resource intakes and estimation of performance on one or multiple cloud data center. The information should not be visible to anyone at any cost. For performance point of view the SQL statements must be executed without decryption. Some solution download the entire cloud database into native place and decrypt it. After decryption it execute SQL statements and encrypt it to store data in cloud database. But this process have some performance related problems. The additional drawbacks of above scheme is that for every column different encryption technique must be adopted. The adaptive encryption technique, which was originally proposed for applications not mentioning to the cloud, encrypts every plaintext fields to numerous encrypted fields, and every value is enclosed in different layers of encryption. The outer layer provides better security than innermost layers. The outside layers are enthusiastically improved at execution time when new SQL statements are added to the amount of work [14].

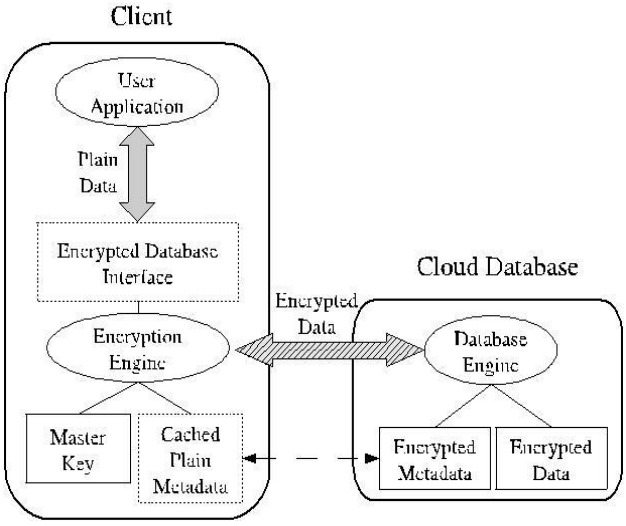

Figure 2.1 : Encrypted Cloud Database [14]

G. Wang, Q. Liu et al. proposed an attribute-based encryption (ABE) where attributes are the properties of user which represent various values related to profile. It permits each cipher text to be connected with an attribute. The system consists of master secret key for attributes. Depending on the policy of attributes master key holder get the top-secret key value and decrypt the desired data from database. The main anxiety in ABE is complicity resistance but not the compression of secret keys. The main issue is size of the secret key in ABE. Definitely, the size of the key frequently growths with the numerous attributes [15].

R. A. Popa et al. introduced a proxy re-encryption which is used to improve the decryption power. PRE is mainly used to delegate the decryption keys of cipher texts without circulation of the secret key to the receiver. A PRE system sanctions dispatcher to delegate to the cloud database server the capability to translate the cipher texts encrypted to receiver. PRE is fine and known to have many applications including cryptographic file system [16].

P. Paillier et al. suggested a protected architecture using encryption and single user key distribution for cloud database. Improving the privacy of data and information stored in cloud computing databases signifies an important involvement to the recognition

of the cloud system computing as the fifth usefulness because it addresses most user apprehensions. Identity-based Encryption (IBE) by Compact Keys: Identity-based Encryption is a category of public key encryption [17].

Xiaokui Shu et al. proposed a two factor security system with data recoverability. The system used USB as a security device. The receiver only decrypt the data if he/she has security device and secure key. Without both of the authentication success the receiver will not access the database. The receiver should have proper device and key to decrypt the data file. If the device is stolen then it will revoke the device and receiver will not decrypt the database. This system also used identity based system for authentication. The difficulty of info safety in cloud database storage, which is principally a distributed storage structure. To make certain the truthfulness of users' info in cloud database storage, and truthfulness of users who can used the cloud database server. They scheduled flexible and effective distributed structure with explicit dynamic info support, including authentication service and Kerberos. Kerberos responsible for a centralize authentication security service whose utility is to validate user to cloud database server. Any user to access the cloud database server first ought to make profile and authentication password. Then it can use the cloud database server with increase the qualify Fig. 2.2 shows the privacy preserving data leak detection model [18].

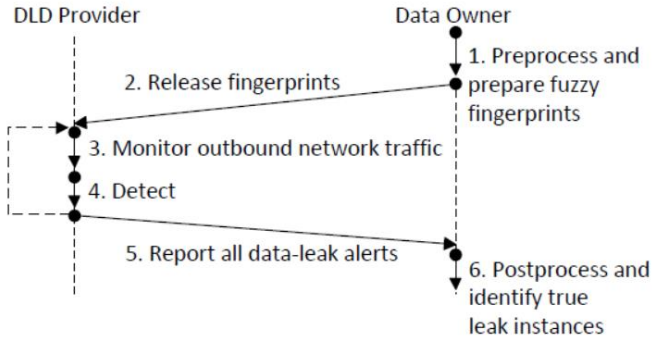

Figure 2.2 : Privacy Preserving Data Leak Detection Model [18]

Giuseppe Ateniese et al. explored proxy re-encryption as of both a realistic theoretical perspective. They defined the security and traits guarantees of formerly recognized methods, and as related them to a group of treaded forward re-encryption methods. These pairing-primarily based methods recognise serious new abilities, comprising of protection the major private key of the cloud user from a colluding delegate and proxy. One of the maximum favourable applications on behalf of proxy re-encryption is providing proxy proficiencies to the main key server of a trustworthy distributed database system; this method the main key server necessity not be unquestionably depend on by means of all the secure keys of the organisation and the storage for every cloud user also can be condensed [19].

M.R. KalaiSelvi1 et al. provides the method to secure cloud database for large and dynamic groups in untrusted cloud. The cloud user can share data with other cloud users at some intervals. As well, it also supports cost-effective new user connation and revocation. The whole public key will not change if new cloud members square measure a little to the cluster. The method even obscure the scale of the cluster. The sizes of the definitive signatures and the public key, likewise as outcomes of the method effort for sign language and validating, ad hoc of the number of cloud group members. In addition, the database storage overhead, key computation are reduced [20].

G. Suganyadevi et al. additionally includes digital signature to provide integrity towards the user's data. Considering the pragmatic issue of security saving information sharing framework taking into account open cloud stockpiling which obliges an information proprietor to appropriate a substantial numeral of keys to clients to provider them to get to her/ his info [21].

Y. Harshada et al. represents a ranking created share authority confidentiality preservative authentication

protocol. This protocol provides ranking at the cloud admin level allocate to file on the base of how often that file retrieved. In this access control method undercover access demand matching is providing without unveiling user's info. Cloud database user can access their info by the feature based access control procedure. Widespread compos capability model is used to offer safety for the info when dissimilar protocols are used throughout the method. A ranking is allot at the admin level to indicate that how numerous interval that file accessed. Cloud database user can see that in their control panel. That enriches the safety of the system and offers knowledge about the susceptibility of the file [22].

Jianyongchen et al. represents an on-demand safety architecture for cloud database system. In this structural design three level layers are there one is input level, second is policy level, and third level is safety mechanism layer. In input level three checks is completed first is safety level, in this only certified user can be permissible to access the service illegal cloud user doesn't have approval to access data. Second is category of service, in this, what kind of service cloud database user want to use or access is checked for the reason that dissimilar kind of service needs different safety. Access system network risk, in this the risk when service permits by the server is checked. Safety policy in this level info is checked and safety considerations are implemented on the base of safety level. Third level is security mechanism level, in this each domain offers different safety mechanism, like decryption/encryption in storage area, IP safety in the network domain, and honey pot in service domain [23].

Giuseppe Ateniese et al. proposed a system which is based on Provable Data Possession (PDP) that permits an auditor to check the exactness of a client's info stored at an untrusted database server. By applying RSA-based homomorphic sampling strategies and authenticator, the auditor is capable to publicly verify the truthfulness of info without recovering the complete data. Inappropriately, their method is only proper for auditing the truthfulness of personal info [24].

Kevin D. et al. defined an additional model named Proofs of Retrievability (POR), which is also capable to check the accuracy of info on an untrusted database server. The main file is added with a group of randomly-valued data check blocks called sentinels. The auditor challenges the untrusted database server by stipulating the situations of a gathering of sentinels and enquiring the untrusted database server to coming back the connected sentinel values [25].

III. CONCLUSION & FUTURE SCOPE

A good amount of research on cloud database security is found in literature. Many of them show good security and encryption accuracy. The different encryption and description algorithms are also studied. In this paper, related works with their advantages and disadvantages have been mentioned. The different audit, data leak detection techniques are also studied and found their flaws. A system can be developed in future that can prevent the confidentiality of information or data that can not violate at any cost.

IV. REFERENCES\

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future GenerationComput. Syst., vol. 25, no. 6, pp. 599–616, 2009.

[2] Peter Mell,Timothy Grance,"The NIST definition of cloud computing",http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] RajkumarBuyya,"Introduction to the IEEE transactions on cloud computing" vol 1,januarry-june 2013.

[4] http://www.conceptdraw.com/How-To-Guide/cloud-computing-architecture

[5] M.Armbrust, "A view of cloud computing, communications of the ACM", vol 53, no. 4, (2010).

[6] H. Hacig€um€u¸s, B. Iyer, and S. Mehrotra, "Providing database as a service," in Proc. 18th IEEE Int. Conf. Data Eng., Feb. 2002, pp. 29–38.

[7] B. Sosinsky, "Cloud Computing Bible" Wiley Publishing, Inc., Indianapolis, Indiana 2011.

[8] R. Buyya, C. Vecchiola, S. T. Selvi, "Mastering Cloud Computing" Tata McGraw Hill Education Private Limited New Delhi.

[9] Harshitha. K. Raj "A Survey on Cloud Computing"International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7, July 2014.

[10] http://www.infoa2z.com/Technology/Cloud/cloud-computing-services-igwdyd_0.html

[11] Boyang Wang, Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditingfor Shared Data in the Cloud", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014, pp.43-57

[12] Lucca Ferretti,FabioPierazzi,MichelColajani and Micro Marchetti "Performance and cost evaluation of an adaptive encryption architecture for cloud databases" IEEE transactions on cloud computing, vol 2,no.2,April-June 2014.

[13] K. Rajasrika, P.S. Smitha "Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015.

[14] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. Buyya, "Cloudsim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," Software: Practice and Experience, vol. 41, no. 1, pp. 23–50, 2011.

[15] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. 17th ACM Conf. Comput. Commun. Security, 2010, pp. 735–737.

[16] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting confidentiality with encrypted query processing," in Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011, pp. 85–100.

[17] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. CryptographicTech., May 1999, pp. 223–238.

[18] Xiaokui Shu, Danfeng Yao, and Elisa Bertino, Privacy-Preserving Detection of Sensitive Data Exposure, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 5, MAY 2015, pp-1092-1112

[19] GIUSEPPE ATENIESE KEVIN FU MATTHEW GREEN and SUSAN HOHENBERGER "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage" ACM Transactions on Information and System Security, Vol. 9, No. 1, February 2006, Pages 1–30.

[20] M.R. KalaiSelvi1 "Secure Data Sharing for Dynamic and Large Groups in the Cloud "International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014

[21] G. Suganyadevi1 S. PunithaDevi " Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Special Issue 6, May 2015

[22] Y. Harshada, K. Janardhan, "Ranking Based Shared Authority Privacy Preserving Authentication protocol in cloud computing" IJIRCCE, May 2015.

[23] Jianyongchen, Y. Wang, X. Wang, "On-demand Security Architecture for cloud computing" IEEE, 2012.

[24] Giuseppe Ateniese, Randal Burns† Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song, "Provable Data Possession at Untrusted Stores", ACM 2007, pp. 598-612

[25] Kevin D. Bowers, Ari Juels, and Alina Oprea, "Proofs of Retrievability: Theory and Implementation", RSA, 2008.