RESEARCH ARTICLE OPEN ACCESS

Survey on Algorithms and Techniques for Secure Cloud Database

Sanjay Kumar Sharma [1], Dr. Manish Manoria [2], Prof. Dr. Sarvottam Dixit [3]
PhD Scholar [1], Advisor to Chancellor [3] Mewar University, Rajasthan
Director [2], Sagar Institute of Research Technology and
Science, Ayodhya Bypass Road Bhopal, M.P
India

ABSTRACT

Cloud computing is a style of computing where massively scalable information technology-enabled capabilities are conveyed ‘as a service’ using computer and Internet technologies to numerous clients. The different safety problems in cloud are scalability, data truthfulness, heterogeneity, data intrusion, non-disclaimer, access control, authentication and authorization. Detecting and preventing data privacy requires a set of different technique, which may include data-privacy recognition, surreptitious malware detection data locking up, and policy enforcement. For cloud database security many techniques and algorithms are provided. This paper reviews different algorithms and techniques to secure cloud computing database.

***Keywords*:-** Cloud Database, Security, Privacy Preservation, Audit, Data leak Detection

I. INTRODUCTION

The objective of cloud computing is to permit users to take advantage from all of cloud related technologies, without the essential knowledge about or proficiency with each one of them. Improving the secrecy of data stored in cloud based databases denotes an important contribution to the acceptance of the cloud computing as the fifth helpfulness because it addresses utmost user apprehensions. There are four foremost types of cloud computing prototypes [2]. These models are DaaS Database as a Service [3], SaaS Software as a Service[4], IaaS Infrastructure as a Service[5] and PaaS Platform as a Service[6]. Database as a Service (DAAS)-Cloud database is aimed for virtualized computer based environments. 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 service, service provider offers computer devices called hardware and software programs called as software to the consumer which is looked-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. Infrastructure as a service (IaaS) is the furthermost rudimentary cloud facility prototypical. It delivers computers virtual machines physical or and other resources.

Cloud computing architecture consists of end users, Internet and cloud providers. The end users can be mobile devices, applications and different computer software’s, Internet with high speed, and different cloud service providers. PaaS provides computers physical or virtual machines and other resources. The providers like Amazon, Rackspace are the examples of infrastructure as a service.

There are four types of cloud models. These are Private, Community, Public and Hybrid Cloud. Cloud Structure pooled by numerous setups for a shared cause for certain community is called community cloud. A cloud structure is providing to numerous clients and is consummate by a third cloud structure is called a public cloud. Cloud based structure only used by particular client is called private cloud. A cloud structure of more cloud delivery service models is called hybrid cloud.

The security related issues are-

(i) How to obey with present and forthcoming security and danger supervision compliance

(ii) How to automate storage provisioning, network, and compute

(iii) How to do on-demand services

(iv) What type of safety services are accessible through the cloud computing

(v) How to achieve external and internal reviews of cloud security

(vi) How the cloud will save data protected and accessible.

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 database. Audit, authentication and authorization are main security issues in cloud database. The information should be preserved and protected. Confidentiality of information is additional safety issue connected with cloud computing environment. For cloud computing database security numerous techniques and algorithms are provided.

The paper is organized as follows. Section 2 represent the problem statement related to cloud security. Section 3 represent the literature survey. Section 4 concludes the paper.

II. PROBLEM STATEMENT

The cloud based database as a service is a pioneering architecture that can support various internet-based applications. The main problem for adoption for cloud database is the information privacy complications. Database as a service (DBaaS) that poses several research challenges in relations to safety and price assessment from an occupant's point of view. Cloud database is basically public so anyone can access those database. Cloud services, analogous to various other services, are consumable in nature and cannot be stored for future sale. Privacy preservation of the cloud database from malicious attack is also main task in cloud database security. The data leak detection in large organization is also necessary in cloud database. The different encryption techniques that allow the execution of SQL operations on encoded data have some performance limits. And different types of encryption techniques must be implemented for every database SQL operation and database column. Most of the encryption technique regarding encryption for cloud-based database services are inappropriate to the database prototype. The recommendation organization system used by the association must be combined or incorporated with those used by the cloud database services. Intentionally scheduled attacks, unintended leaks such as accelerating trustworthy emails to unclassified email account. The attacks may also include human faults such as passing on the erroneous privilege main reason of the data-privacy occurrences. The three level of security should be provided in cloud database as a service. If any reason the data leaked then it should be detected and report should be provided to the cloud system with audit report. How to design a host assisted privacy preservation cloud database which ensures security of the information from unauthorized access. How to design and keep large organizations cloud database from data leak and misuse is the cloud security issues. The various techniques are reviewed in this paper related to cloud database security.

II. LITERATURE SURVEY

Attribute-based encryption (ABE) [7] Attributes are the properties of user which represent various values related to profile. It permits each ciphertext 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.

Proxy re-encryption[8] 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.

Predefined Hierarchy based Cryptographic Keys: Cryptographic key assignment systems [9] intention to minimalize the overhead in managing and storing secret keys for universal cryptographic use. In this method a secret key for a given node can be used for its sibling's nodes. The author in this proposed work provides a method using hierarchical system. This scheme uses tree structure which consists of nodes. The secret key is assigned to the parent node the all nodes under parent node automatically grants the secret keys to all other nodes. This scheme produce a tree grading of symmetric-keys with the help of recurring assessments of pseudorandom block cipher on an immovable secret. The concept can be used in graph.

Additional innovative cryptographic key assignment systems provision access strategy that can be demonstrated by cyclic graph and an acyclic graph. Maximum of these systems produce keys for symmetric-key cryptosystems. This scheme is more expensive then symmetric keys.

Key circulation and key storing are more challenging issue in the cloud database. Cloud storage is a virtual system storage that empowers customers to store objects and documents. Cloud system database should provision of cloud computing and traditional relational databases for extensive satisfactoriness. The probable encounters connected with cloud database are high availability and scalability. The further challenges are data reliability and truthfulness, confidentiality and many more. P. Paillier 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. D. Song et al in[11] annoyed to make IBE with secure key accumulation. IBE scheme also uses random oracle. In this IBE scheme, key combination is inhibited in the all keys should be taken from dissimilar identity divisions. The advantage of this schemes are security and cipher text size.

Shu et al. in [12] proposes 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.

To make sure info security in cloud database storage, a unique triple encryption structure[13] is suggested. In the triple encryption scheme, big data HDFS files are encrypted by using the integrated encryption constructed on RSA and DES, and the user's RSA security key is encrypted with the help of IDEA method. The triple encryption scheme is integrated and implemented in Hadoop-based cloud database storage.

[14]The practical downside of privacy conserving information sharing

system maintained public cloud database storage which necessities an information vendor to allocate an oversized range of keys to users to change them to access his/her documents The key-aggregate searchable cryptography (KASE) scheme allot one key to a cloud user once sharing numerous documents with the other cloud user, and also the user merely must submit and access once she/he demands over all documents shared by cloud owner .

Susan et al. in [15] 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.

Outsourcing database to cloud servers has become an increasing development for many organizations to relieve the liability of local database maintenance and storage. In[16] provides various methods of outsourcing database storage: mutual trust, block-level info dynamic, access control and newness. The author proposed a cloud based database storage structure which provides outsourcing of dynamic info, where the data owner is proficient of not only accessing and archiving the info stored by the cloud database providers, but also scaling and inform this info on the remote cloud servers. The recommended scheme facilitates the legal users to make sure that they are getting the fresh and recent version of the outsourced info.

M.R. KalaiSelvi in [17] 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.

Due to the characteristic of lesser maintenance, cloud computing make available efficient and financially suitable group network resource amongst cloud database users. The method[18] is lot flexible, and it can be merely protracted to support further advanced probing database query. Here author achieve that this provide a spectacular constructing block for the creation of secure services in the cloud database storage which are not trustworthy by cloud user. As user will share only single private key. The database storage space necessary will become a smaller amount of and more proficient.

To split information flexibly is an important role in cloud computing. User favour to upload their data on cloud and among dissimilar users. Outsourcing of information to server may guide to drip the confidential info of cloud user to everyone. Encryption is a one outcome which make available to share particular info with desired cloud user. Sharing of decryption private keys in protected way act important role. Key Aggregate Cryptosystems provides allocation of secret keys for different files stored in cloud storage in the form of single aggregate key. The [19] 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. [20] surprisingly offer the idea of secure key-aggregate searchable encryption (KASE) and progress a solid KASE plan.

In [21] plan a multi-keyword rank explore scheme to allow correct, capable and safe search over encrypted mobile cloud information. Security examination has established that this scheme can efficiently achieve privacy of documents and trapdoor privacy, index, trapdoor conceal access prototype, unlink ability, and of the search user. Extensive concert estimation has revealed that this method can accomplish better effectiveness in terms of the computation overhead and functionality. Still access control and authentication concerns need to be inspected.

In[22], a semantic more than one keyword ranked search scheme over the encrypted cloud database information is suggested, which all together come across a group of strict secrecy requirements. This system employ secure K-nearest neighbour (K-NN) to complete safe search functionality. The method could return not merely the particular identical files, but as well the file including the terms latent semantically linked to the query keyword. As for future they will think on the encrypted info of semantic keyword examine in command that they can confront with the more difficult search.

Mathew Green et al. in [23] is almost outsourcing the decryption of ABE Cipher texts, a new concept for ABE that largely eliminate the overhead of complication of use or access method for users. If ABE cipher texts are put in storage in the cloud, the paper demonstrate how a client can make available the cloud database with a single conversion key that allow the cloud to decode any ABE cipher texts fulfilled by the user feature into a EI Gamal-style cipher text, with no the cloud being able to convert any portion of the users communication. Additionally this methodology has a negligible impression on performance.

Y. Harshada et al. in [24] 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.

Jianyongchen et al. in[25]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.

S. Sankarashewari et al in , [26] represents an access control mechanism for shared data over cloud database. This procedure a decentralize access control method is used, in that there are numerous no of key circulation centres KDCs to share key amongst the cloud database user. In present method an integrated key distribution method is used, which occasionally leads to the difficulty of single point let-down. To avoid replay attacks which used to perform to get use or access for the cloud user's database. In this if a cloud user once constrained by the set of rules then she/he cannot back stale their info. Uniqueness of the cloud database user is also not revealed to the cloud database server throughout the whole procedure. In this a SHA constructed encryption is applied to hide the info of the cloud database user. In this info of the cloud user not revealed to the cloud database server but cloud database server recognises the access method for each info that stored in the cloud database server.

Provable data possession (PDP), suggested by [27], 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.

Kevin D. Bowers et al. in [28] 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.

To support active data, offered proficient PDP method built on symmetric keys. This method can support delete and update procedures on info, however, insertion operations are not presented in this method. For the reason that it exploits symmetric keys to audit the integrity of info, it is not public auditor and only make available a user with a restricted number of authentication requests.

The method utilized BLS signatures and Merkle Hash Tree to sustenance dynamic info in a public verifying method and presented dynamic provable data possession (DPDP) with the help of genuine dictionaries, which are constructed on rank information.

Enormous progression in digital information and data, better broadband conveniences, altering data storage necessities, and Cloud system computing commanded to the appearance of cloud databases. The adoption of cloud computing database as fifth utility is failure because of cost, information and data privacy. provides privacy preservation for shared data in cloud computing using public auditing method. The auditing method used ring signature to provide verification process. The system consists of public verifier, group of users and cloud server. In this method the distinctiveness of the signer on every block in collective data is retained private from public verifiers, the verifiers are able to capably validate shared info truthfulness without reclaiming the complete file. The method is able to accomplish numerous inspecting tasks all together in its place of confirming them one by one. The method improves the efficiency and effectiveness of method in auditing shared info integrity.

The data owner in the beginning generates shared info in the cloud. The info is shared through group users. Both the group users and original user are associates to the group. Every single member of the created group is permissible to modify and access shared info. Shared info and its authentication metadata are both put in storage in the cloud database server. A public authenticator, such as a third party examiner providing professional info inspecting services or a info user external to the group expecting to make use of shared data, is capable to openly validate the truthfulness of shared info stored in the cloud database server. When a public verifier needs to check the truthfulness of shared info, it primarily directs an inspecting challenge to the cloud database server. Afterward acceptance the auditing challenge, the cloud database server answer back to the public auditor with an inspecting evidence of the ownership of shared info. Then, this public auditor checks the precision of the complete info by confirming the precision of the auditing proof. Principally, the method of public auditing is a challenging task and reply protocol amongst the cloud database server and a public verifier.

Two categories of security threats associated to the integrity of shared info are possible privacy and integrity threats. In integrity threats an opponent may attempt to corrupt the truthfulness of shared info or the cloud database service provider possibly will carelessly remove or even corrupt the info in its storage because of human errors or to hardware failures.

In some cases the cloud database service providers can economically inspired, that is it might be unenthusiastic to notify users about such exploitation of info in order to protect its status and circumvent trailing revenues of its services.

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.

IV. CONCLUSIONS

The cloud computing resources are storage, networks, applications, servers, and services. The cloud system database as a facility is the pioneering archetype that can support various web based software's.The prospective encounters connected with cloud system database are high availability, scalability data consistency and fault tolerance, integrity, confidentiality and many more. Although data encryption appears the ultimate in-built way out for data privacy. The different security schemes related to cloud database security are reviewed in this paper. The major research gap provided in techniques and algorithms are lack of three level security issues.

REFERENCES

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

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

[3] 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.

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

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

[6] 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

[7] 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.

[8] 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.

[9] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st ACM Symp. Theory Comput., May. 2009, pp. 169–178.

[10] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc.

17th Int. Conf. Theory Appl. Cryptographic Tech., May 1999, pp. 223–238.

[11] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, May 2000, pp. 44–55.

[12] 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

[13] Chao YANG, Weiwei LIN*, MingqiLIU "A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security" Fourth International Conference on Emerging Intelligent Data and Web Technologies 2013

[14] Baojiang Cui, Zheli Liu_ and Lingyu Wang "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 6, NO. 1, JANUARY 2014

[15] 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.

[16] AyadBarsoum, Anwar Hasan,"Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems", IEEE Transactions on Parallel and Distributed Systems, IEEE 2013, pp. 37-42

[17] 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

[18] Sharayu.J.Lande, Prof. N.B.Kadu "A Review of Research on An Aggregate Key Sharing Mechanism For Sharing Data Between Different Groups Via Cloud" IJEDR | Volume 3, Issue 4 2015

[192] 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

[20] Salman Mujawar "A Paper On secure multi-owner group data search by using aggregate key" Innovation in engineering science and technology (NCIEST-2015)

[21] Hongwei Li, Dongxiao Liu, YuanshunDai,Tom H. Luan and Xuemin(Sherman) Shen "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage",March 2015

[22] Li Chen, Xingming Sun, *Zhihua Xia and Qi Liu "An Efficient and Privacy- preserving Semantic Multi-Keyword Ranked Search Over Encrypted Cloud Data", International Journal of security and its application, 2014.

[23] Mathew Green (Johns Hopkins University), Susan Hohenberger (Johns Hopkins University), Brent Waters (University of Texas at Austin), "Outsourcing the decryption of ABE Ciphertexts". IEEE, 2008,pp.34-45

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

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

[26] S. Sankareswari, S. Hemanth "Attribute Based encryption with privacy preserving using asymmetric key in cloud computing" IJCSIT, 2014.

[27] 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

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

[29] Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018.