Survey Of Privacy Preserving Technique For Improving Security In Cloud Computing Environment

Gayatri Patel
SDBCE Indore

Abstract- *Cloud Computing is in advance attractiveness and improvement day-by-day. The information storage in cloud computing environment has number of benefit. Users have a number of ways to access the cloud information without any validate its integrity. The main problem in the cloud environment security and integrity of data of user. But still the security threat hinders the achievement of Cloud Computing. In this paper, quantities of the privacy threats are address and the method to conquer them is surveyed. to afford a comprehensive study of state of-the-art method and techniques for protecting data confidentiality and access privacy, which create dissimilar tradeoffs in the proposed New model for privacy preserving technique for improving security in cloud computing environment be handle concomitantly which reduce communication and computing cost. In this paper we are going to study numerous methods to resolve these issues and to afford the privacy and security to the data in cloud.*

Keywords- Cloud Computing, Privacy Preserving, Access Control, Public Auditing.

I. INTRODUCTION

Cloud computing has elevated numerous security threats such as data gaps, data loss, DOS, and malicious insiders that have been widely studied in Numerous cloud security discover are information determined security aspects into, which reflect on privacy, dependability, and access control of outsourced information when they are put away in the cloud storage. To make certain Outsourced information privacy in the disseminated storage, now in these days the majority of the applications are developed based on internet and their use and also huge number of databases exists due to the quick development in communication and storing systems. Furthermore, due to the emergence of new technologies such as cloud computing increase the amount of data distribution between multiple entities. Therefore for satisfying the need of increasing demands new approaches are discovered for processing data in efficient and secure manner. In this context there are many applications available that needs a database services for storing data and each time required to fetch data from the data base. In addition of that there are some applications also available that needs more than one database services same time. In these applications the database storage is available in remote place and required connectivity between all the databases concurrently. We examine the problem of privacy-preserving correspondence join queries in this effort. As identified, strong data protection can be accomplished by encryption methods, but how to permit secure resemblance joins over encrypted data is a non-trivial task.

The system performance is found optimal but the time exploitation is considerably average in contrast to traditional algorithm. Thus the proposed technique is desirable to advance for their time utilization in near future. In adding of that in near prospect the technique is extendable for the hieratical data mining based privacy issues. To give data storage security in Cloud Computing with Third Party Auditor (TPA) Scheme. To intend a scheme which will afford a monitoring system for preserving the confidentiality of the data? To maintain data integrity & validation during confront and challenge verification. In these conditions the data models are applied to the databases for extracting the desired data efficiently. Thus to reduce the data access time and resource consumption the centralized manner of storage and processing is required. In this situation data mining techniques are help to provide data to more than one party at the same time. Here data model is referred to a high label data structure that incorporates the entire data in a same place. In this context the key issues is providing data with security by which the sensitivity of the actual data is maintained and the required other data release applications getting the benefits from the data.) near fuzzy keyword set building, this scheme construct the enhanced fuzzy keyword set composed of in general retrieval keywords, of course include the real keyword which is the genuine single to be searched by the user.

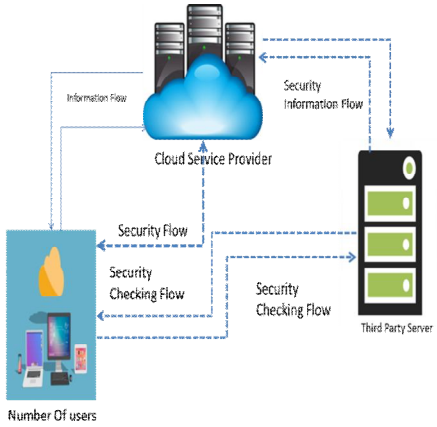

Figure 1. The architecture of cloud data storage service

Thus the proposed work is a privacy management and data security scheme that employed over the centralized data aggregation model and produces the data release with adding an amount of noise for securing the sensitivity of actual data of different parties. The databases consume the centralized approaches to reduce the complexity of data. But data in same place can generate the issues during the data access thus the proposed work is data privacy preserving, data analysis and release technique is simulated using vertically partitioned data. The rest of the paper is prepared as follows: Section II presents an summary of cloud computing, while section III describes the particulars of the research problem beside with current solutions and main challenges Privacy preserving. Section IV proposed methodology privacy-preserving Section V provide analysis and deliberations, and conclude this paper

II. RELATED WORK

In the privacy preserving Technique literature review is completed for data integrity scrutiny and data storage contrivances that are presently used in dynamic multi transactional applications. The structure of cloud and storing data in it has incredible benefits. It ease the authenticated and certified cloud users to way in massive resources that are outsourced and shared in the cloud. The common term of privacy within the general limits is the data that's leaked by the distributed computation to be the data that may be learned from the selected output of the computation.

Mr.V.Biksham in at al[1]To provide security to the encrypted data with computations, a secure encryption method called homomorphic encryption which provides calculations on encrypted data without decrypt the cipher text and enhance the performance of the cloud services.

M. Thangavel et al[2] we also explore solution to handle single identity to be used with all service providers to make user free from maintaining separate credentials. To strengthen privacy preservation, we recommend usage of anonymous authentication based on Zero Knowledge Proof[3] which will help user to access the service anonymously.

Most researchers have proposed some encryption techniques which helps to ensure privacy for a particular level in cloud. Based on the survey done by various researchers, No complete privacy preservation system is available in today's world. In this paper, comparative study on privacy preservation schemes in cloud provides a clear view on the privacy issues and methods to preserve in the cloud data storage

Dishant Soni in et al[3] also discover solution to handle single identity to be used with all service providers to make user free from maintaining separate credentials. To strengthen privacy preservation, we recommend usage of anonymous authentication based on Zero Knowledge Proof[4] which will help user to access the service anonymously. The present progressive paradigm for privacy-preserving knowledge analysis is differential privacy [5] that permits un-trusted parties to access personal knowledge through combination queries.

Table 1.

Author Name	**Algorithm**	**Advantage**	**Limitation**
Noman Mohammed et al.[5]	Two-party algorithm	Effectively preserve information for a data mining task	Not work properly in cloud environment
N. Cao et al.[6]	Significantly improved MRSE schemes	Low overhead on computation and communication	Number of Stage is high then increasing the data set then become the problem

M. Li et al.[7]	Hierarchical predicate encryption (HPE),	efficiently support multi-dimensional, multiple keyword searches	Not supports Huge Number of data set
C. Wang et al.[8]	Order-preserving symmetric encryption (OPSE)	efficiency of the proposed solution	This approach to required crypto techniques, such as attribute-based encryption

Xingliang Yuan et al.[9] In this research they have been focus on the problem of privacy-preserving resemblance join queries over encrypted high-dimensional data. Start from the state-of-the-art methods that combine LSH and SSE to realize secure relationship search. In specific, three dissimilar secure query schemes are proposed to resolve the problem regarding dissimilar practical requirements on security, effectiveness, accuracy and deploy capability.

III. PRIVACY PRESERVING DATA MINING

We proposed a new approach for privacy-preserving public auditing system for data storage security in cloud computing. In our approach the computational time is reducing and efficiency should be increasing in different number of datasets. To store in data cloud environment using our proposed approach very efficient and secure manner. to utilize and row and column based scheme with homogenous encryption linear authenticator technique to guarantee that the TPA would not study several knowledge about the data content stored on the cloud server during the efficient auditing process, we not only eliminates the load of cloud user improving the security of the user dataset for storing the outsourced server.

IV. PROPOSED METHODOLOGY

Based on the earlier deliberations and findings, it become evident that there is a exchange among how much data is creature outsourced and the security level of big data analysis. Conventional secure outsourcing method often times cannot grip the processing of such large data. In addition, no practical solution is yet accessible for conduct the task of splitting the computation so that the private data is securely reserved in an organization's private cloud, being done so as part of a cloud. It guarantees data privacy, resolve uselessness of key source, reduces the encumbrance of encryption and decryption, can be able to accomplish frequent keys, protects owners storage space, decrease run-time overheads of the system, provides outstanding privacy security and can relate to numerous users, data owners and service providers. in addition, as one of the nearly all complex computing environment, cloud computing will definitely occupy unforeseeable confront in privacy protection and preservation. Therefore, it is essential to analyze cloud privacy risk, and intend cloud privacy protection and preservation technique. For example, for cloud clients, previous to they join in cloud environments, a number of actions and procedures applied at client side can provide them confidence to utilize cloud services. For cloud service provider, presently similar to other service providers in existing computing environment, spiteful customers or attackers are the most important concerned intention in privacy fortification and protection. For nearly all service provider, existing in the cloud ecological surroundings, it is essential to converse or assist with every other. So, other malicious service provider might be privacy attackers or thieves. For service providers, interior control and running in privacy protection and preservation are essential to avoid some unintended privacy leakages, and so on. Therefore the following consideration is placed for aggregation, generalization and release operations.

- Find a method by which the different parties can aggregate their private data on same place.
- Required to develop a generalized method by which the distribution of their own data becomes feasible.
- Implement a method by which the generalized data is prepared to use in different applications.

We propose a technique comprises an Identity Management Server with anonymous authentication mechanism, which aim to maintain user's identity based on service provider's profile or category of application which needs users' information. Data mining is a technique or a utility by which the analysis of raw data is performed. The analysis of data is performed in such manner by which either the key factors from the data are recovered or by using the mining procedure obtain some conclusion from the data. The data mining techniques can be different types and nature that can be dependent on the data format or the data sources. In this presented work, the main aim is to study the distributed nature of data. In this environment, the data either organized in form of vertical partitions or horizontal partitions. In this work the vertical partitioning of data is considered for experimentation. The vertically partitioning of data contains a

part of the complete set of data and after combining different parts the entire dataset can be recovered.

The key issue arises when the data sources are quite different but having some similar contents or attributes which are required for use and conclude some decisions from the data. To understand more clearly suppose an organization has some different departments and each department maintain some kind of their client's data. But here the complexity is that nobody wants to disclose the sensitive or private data of a user (end-client). On the other hand for organizational point of view that much essential to make audit on data. Therefore there is need to implement some privacy preserving technique by which the sensitive contents from the data is normalized. Additionally, the data can be used for organizational assessment purpose

In the development stage, the information proprietor build the correspondence metric article from the primary raw information, sends these resemblance metric items to a resemblance cloud for indexing and the basic information to information storage. In the searching stage, several accepted customer can inquisition the comparability cloud to acquire IDs of the relevant items alluding to exclusive information protests that can be accordingly recovered from the crude information storage. General goals of outsourced secure comparability detection can be outline as takes after. To established security for user's outsourced data without learning knowledge of data contents. New technique using the experience of available techniques is propose and implementation for demonstrating the entire scenario of data aggregation and their privacy preserving data mining. Comparative Performance between Proposed Technique and Traditional Technique: In this phase the performance of the proposed secure data mining model is computed and their comparative study with the traditional algorithm is provided. In this paper, we tackle the concern of fuzzy keyword set construction and enhancement of the systems usability as well as the user retrieval acceptable degree from retrieval effectiveness and accuracy perspective. Our approach of the sensible mixture of fuzzy keyword set construction proposed in and to build a full-scale fuzzy Keyword set near the huge compensation of additional applicable fuzzy keywords to fill in the fuzzy keyword set so as to create additional precise keyword searches for the trapdoor matching process. In adding, during feedback method by interactions among the retriever and the cloud, statistically simple misspelled keywords rank in a convinced fuzzy keyword set applicable to the input keyword is dynamic since of the supple pointer which straight the one whose rank is a great deal advanced so as to put the files enclose more applicable fuzzy keyword in facade of the retrieval consequences. Thorough theoretical analysis and we will improve can efficiently increase the systems usability and acquire higher users acceptable degree, and the accuracy as well as its security analysis of the proposed method is sensible and precise.in this paper to study a number of algorithm and approach for privacy preservation drawbacks of the existing system by securing data dynamics and performance improvement. To Common analysis illustrations that our schemes are provably secure and extremely effective.

V. CONCLUSION

This paper is on concern of one of the key issue - privacy that happen in the situation of cloud computing and analyze the numerous works being done to resolve the issues in privacy and thus to ensure privacy to outsourced data on cloud storage. Therefore security and privacy are becomes a primary concern in different data mining applications. In this presented work the security concern in centralized data mining techniques are investigated and a new lightweight solution is introduced for improving the traditional privacy preserving data mining techniques.

REFERENCES

[1] Mr.V.Biksham , Dr. D.Vasumathi ," Query based computations on encrypted data through homomorphic encryption in cloud computing security" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[2] M. Thangavel, P. Varalakshmi, S. Sridhar ," An Analysis of Privacy Preservation Schemes in Cloud Computing" 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

[3] Dishant Soni , Hiren Patel," Privacy preservation using novel identity management scheme in cloud computing" 015 Fifth International Conference on Communication Systems and Network Technologies.

[4] Shweta Taneja, Shashank Khanna and Sugandha Tilwalia, "A Review on Privacy Preserving Data Mining:Techniques and Research Challenges", International Journal of Computer Science and Information Technologies, Volume 5, Issue 2, PP. 2310-2315, 2014

[5] Noman Mohammed, Dima Alhadidi and Benjamin C.M. Fung, "Secure Two-Party Differentially Private DataRelease for Vertically Partitioned Data", IEEE

Transactions On Dependable and Secure Computing, Vol. 11, No. 1, January/February 2014.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou. Privacy-Preserving Multi-Keyword RankedSearch over Encrypted Cloud Data. In INFOCOM, 2011 Proceedings IEEE, pages 829–837, April 2011.

[7] M. Li, S. Yu, N. Cao, and W. Lou. Authorized Private Keyword Search over EncryptedPersonal Health Records in Cloud Computing. In Proceedings of ICDCS 2011, 2011.

[8] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou. Secure Ranked Keyword Search over EncryptedCloud Data. In Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems, ICDCS '10, pages 253–262, Washington, DC, USA, 2010.IEEE Computer Society.

[9] Xingliang Yuan, Xinyu Wang , Cong Wang, Chenyun Yu , and Sarana Nutanong ," Privacy-preserving Similarity Joins Over Encrypted Data" DOI 10.1109/TIFS..2721221, IEEE-2017.

[10] Yang, K., & Jia, X. 2012. Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web, 15(4), 409-428.

[11] R. Lomotey and R. Deters, "Saas authentication middleware for mobile consumers of iaas cloud," in Services (SERVICES), 2013 IEEE Ninth World Congress on, pp. 448–455, June 2013.

[12] H. Kim and S. Timm, "X.509 authentication and authorization in fermi cloud," in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 732–737, Dec 2014.

[13] B. Tang, R. Sandhu, and Q. Li, "Multi-tenancy authorization models for collaborative cloud services," in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.