Secure & Encrypted Accessing and Sharing of Data in Distributed Virtual Cloud: A Review

Ashish G. Ahuja
M.E. Scholar, Dept. of Computer Science & Enginnering,
Pote Engg/Sant. Gadge
Baba Amravati University, India.

Prof .Komal B.Bijwe
Assistant Professor, Dept. of Computer Science & Enginnering,
Pote Engg/Sant. Gadge
Baba Amravati University, India.

Abstract: - Cloud Computing has been accepted as the next generation architecture of IT Enterprise. The Cloud computing idea offers dynamically scalable resources provisioned as a service over and the Internet Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure Placing critical data in the hands of a cloud provider should come with the guarantee of security and availability for data and in use. various alternatives available for storage services, while data confidentiality is the solutions for the database as a service pattern are still undeveloped This architecture is supporting purely distributed clients to connect directly to an encrypted cloud database, and to execute simultaneous and independent operations including those modifying the database structure.

The Access control policy is set out in which only authorised users are able to decrypt the stored information. This scheme prevents from replay attacks and supports formation, modification, and reading data stored in the cloud. This unique attribute, however, creates many new security challenges which have not been well understood. Security is to protect data from danger and vulnerability. There are various dangers and vulnerabilities to be handle. Various security issues and some of their solution are explained and are concentrating mainly on public cloud security issues and their solutions. Data should always be encrypted in a time when stored and transmitted.

Keywords: Distributed computing, cloud, big data sharing, access control.

*****

I. INTRODUC0TION

Cutting in recent innovations, with Rapid development of information technologies and Network technologies, demand of information systems in government departments and organizations has increased to improve their business efficiency. However, in reality, it is common that establishing systems without a combined planning, mainly in medium and small organizations, so data sharing and integration among the independent systems has become a difficult[1][10]. But Businesses and organizations benefit through greater productivity and efficiency when big data is shared or exchanged with business partners around the world using Cloud technology . How to protect and make full use of data resources of the existing systems, in other words, how to realize data exchange and sharing, has become a determining factor in the success of establishing a new system[1][2].

Cloud is a large scale pool of computing service. The Cloud helps organizations are dynamically scalable abstracted computing infrastructure that is available on-demand and on a pay-per-use basis. Although the cloud Infrastructures are much more efficient and reliable, [4][8] . Most cloud computing providers offer a distributed data store/database. These distributed databases represent a data modelling standard that their consumers can use to cooperate with the cloud system. For example, Amazon Web Services offers DB Applications wishing to store their data in the cloud, can then define their tables, items and attributes as required by the distributed databases. Certainly, the sharing of the data is enabled through the use of common data models and common data protocols .Therefore, the use of a distributed database data modelling concepts, , e.g. Tables, Attributes, and Items is typically not sufficient for the sharing of data[3][7][9]. To make sure of the correctness of storage without the users possessing their own data, it is difficult to address all data security threats in cloud storage as all concentrated in single server scenario and not consider dynamically changing data and its operation. By using distributed protocols for maintaining storage correctness in the multiple server or peers . We use erasure- correcting code in the distribution of the file in the cloud to avoid redundancies which increases the data dependencies. It overcomes the communication overheads of the traditional replication based techniques of file distribution. [3][7][13]

In distributed computing, data is the likelihood of business enterprises and private users, especially data stored in mixed and independent data sources. The data sharing approaches such as Transaction Processing Monitor (TPM) [1] and Resource Description Frameworks (RDF) [2] attempt to

achieve this type of data sharing in different ways. . These approaches differ in the way they deal with the challenges that face users and companies during the development of data sharing systems. However, data sharing approach is realize data locked into various data sources and make them available for users In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality having paramount importance[10] With the development IT in concurrent and dynamic computing, cloud computing, grid computing and their related services computing in a distributed environment[04][15][16].

II. LITERATURE SURVEY

Data storage in a cloud is where the user stores his data through a CSP (cloud service provider) into a set of cloud servers, which are running parallarly and in a distributed manner. The idleness of the data can be employed with technique of erasure-correcting code to further accept faults or server crash as user's data grows in size and importance . Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or recover his data[5]

It is of vital importance to guarantee users that their data are being correctly stored and maintains, as users no longer have their data locally, That is, users should be prepared with security means so that they can make continuous correctness

declaration of their data stored in Cloud Servers even without the existence of local copies[14].

D.Pratiba in 2002 proposed that Data mining in Cloud Computing is the process of extracting structured information from unstructured or semi-structured web data sources. The Data mining in Cloud Computing allows information from unstructured or semi- management of software and data storage, with the guarantee of efficient sharing of resources for their users.[16]

Zeng Dadan in 2003 proposed that an perfect computing platform aims at adapting to different kinds of computing applications. Different applications may prefer different storage systems for their specific needs. A distributed computing platform with broad usability can shorten the developing process distributed applications. If the application requirement changes then different storage systems can be used without the need for additional development or significant changes to the system, making the distributed application more flexible and efficient.[9]

Yu et al In 2005 proposed that Attribute-based encryption is by nature a tool for access control, and thus it is not surprising to see that the primitive is adapted to the setting of cloud computing, where fine grained access control is preferred so as to make the cloud a scalable and convenient platform for data sharing.[15]

Mao Tan in 2006 proposed that Distributed heterogeneous data exchange is an important research topic in the area of data sharing and integration, a significant difficulty in process of data exchange is to determine the problem caused by the heterogeneity of data the architecture of hardware or operating system may be different, which leads to differences in the structure of data storage, the acceptable technologies of data processing can also be different [1].

. Shucheng Yu in 2007 proposed that the data owner and cloud servers are very likely to be in two different domains. On one hand, cloud servers are not allowed to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of the owner. For the purpose of helping the data owner as like fine-grained access control of data stored on untrusted cloud servers, a feasible solution would be encrypting data through certain cryptographic primitive(s), and disclose decryption keys only to the authorized users. Unauthorized users, including cloud servers, are not able to decrypt because they do not have the data decryption keys.[18]

. Sundareswaran et al. in 2008 proposed that also bundles the data with an access policy. Additionally, a record file is also bundled with the data. Any operation the user carries out will be appended to the log file, and this record file will be from time to time sent to the Cloud. A data owner can then access the record files to check whether data is being used appropriately this prevents from man-in-the-middle attacks [19].

. Pengzhi Xu in 2009 proposed that, the distributed file systems make use of storage resource of product distributed file systems make use of storage supply of service machines to provide a large extensible cost capacity, low storage and high parallel transfer rate. However, our campus cloud is designed as access tools and a set of cloud middleware building upon the storage resources provided by these distributed file systems. Therefore, both works are critical to the personal storage and communities data sharing.[15]

. Kui Ren in 2010 proposed that, Address this open issue and propose a secure and scalable fine-grained data access control scheme for cloud computing. Our proposed scheme is partially based on our observation that, in practical application scenarios each data file can be related with a set of attributes which are meaningful in the perspective of their interest. The access structure of each user can thus be defined as a unique logical expression over these attributes to reflect the scope of data files that the user is allowed to access. As the logical expression can represent any desired data file set, fine-grainedness of data access control is achieved.[12]

. Yanjiang Yang in 2011 proposed on attribute-based encryption (or predicate encryption) and proxy encryption, two cryptographic primitives underlying our construction, as well as cryptographic access control mechanisms for cloud computing.[11]

. Ateniese et al. in 2012 proposed that at the time of encryptions we secure distributed storage system. Specifically,

the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate contents key(s) from the master public key to a granted user's public key.[17]

Luca Ferretti in 2013 proposed that Different approaches guaranteed some confidentiality by distributing data among different providers and by taking advantage of secret sharing . In such a way, they prevent one cloud provider to read its portion of data, but information can be reconstructed by colluding cloud providers.[8].

Chen et al. in 2014 proposed that bundle the data with an access policy and sending this bundle to authorized use untrusted applications this proposed Architecture called Data Safe. This Data Safe Mechanism allows only to the authorized user to set out the policy to the data so that it can accessible only from the trusted party[1].

Table 1: Proposed Methodologies

Sr.No	Year	Author	Proposed Work
1	2002	D.Pratiba	The cloud computing allows to access information from structured or semi-unstructured ,semi-structured web data sources
2	2003	Zeng Dadan	A distributed computing platform Allows different types of computing Applications so that any kind of data from any kind of storage system must be Accessible
3	2005	Yu et al	An Attribute Based Encryption scheme Allows to access fine grained data or bundle of data by setting the cloud computing platform
4	2006	Mao Tan	Data exchange is to determine the problem caused by the heterogeneity of data the architecture of hardware or operating system may be different.
5	2007	Shucheng Yu	The data owner and cloud server both are different the data owner not allows to access confidential data while cloud server not allowed to decrypt the data.
6	2008	Sundareswaran et al	After bundle the all data ,at the time of sending the data to cloud additionally log file will sent so that or system can identify kind of changes & update file will sent to the owner time to time.
7	2009	Pengzhi Xu	The distributed file systems make use of storage supply of service machines to provide a large extensible cost capacity, low storage and high parallel transfer rate
8	2010	Kui Ren	A secure and scalable fine-grained data access control scheme for cloud computing as the logical expression can represent any desired data file set, fine-grainedness of data access control is achieved.
9	2011	Yanjiang Yang	An attribute-based encryption (or predicate encryption) and proxy encryption, two cryptographic primitives underlying construction, as well as cryptographic access control mechanisms for cloud computing.
10	2012	Ateniese et al	A distributed storage storage system Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key.
11	2013	Luca Ferretti	Different approaches guaranteed some confidentiality by distributing data among different providers and by taking advantage of secret sharing.
12	2014	Chen et al	Bundle the data with an access policy and sending this bundle to authorized user untrusted applications this proposed Architecture called Data Safe

III. PROPOSED WORK

In this system, hybrid cloud architecture is introduced in which we are going to create number of virtual clouds in the main cloud. There will be different type of virtual cloud will be created like Encrypted cloud in which encrypted data or files of the stored. To access that files user has to take access key from the owner of that file. Next one is the public cloud in this all the data will be access by the user publicly without any authentication and another cloud will be the Virtual dedicated private cloud in this cloud the user will create the group and that data is access by the authenticated group members. In this cloud system some speculated user are going to use that cloud data that are only those one which are mansion at the time of virtual dedicated cloud creation.

When the user request for the file uploading then data is stored in private cloud, if the user request to the public cloud the user can access the data without authentication or if the user want to access data of the encrypted public cloud user has to use the key to decrypt the data. And if the third party wants access to the encrypted data then that third party will ask

for the key to authorized user to the data. But the third party can access the public cloud publicly without any permission.

IV. CONCLUSION

A Developed innovative architecture that guarantees confidentiality of data stored in a cloud databases because day by day their demand is going to be increases when dealing with the data sharing in a distributed environment so for the purpose of security. Privacy is essential for the data available in a cloud hence whatever the data to be illegally distributed kept it to be highly confidentially and in a future set out those policy so that it can identify who is the owner of the data and who is another and also

Our scheme accomplishes the integration of storage correctness insurance and data corruption has been detected during the storage correctness verification across the distributed servers. Our scheme is highly efficient to provide private and shared cloud which can be used to provide ease of access to share data from different users. Here we had proposed the environment in which user can able to share their data into public cloud which gives ease of access to all other user to get that data and to use it.

V. FUTURE SCOPE

Existence of Internet will improve its future:

The cloud computing will change into everything the greater outstanding in the company of ubiquity of high-speed, broadband Internet. Easily but quickly may be we are becoming nearer to each other in the form of data sharing and data accessing from the cloud or sending data to the cloud. Most part of the computer specialist spends lots of their time and creation downloading distinct variants of software so that they can approach the distinct programs and data with brief efforts. Using our proposed system we can make a global cloud which can be used to share a data among all the other clouds and to all the users for next generation.

REFERENCES.

[1] Mao Tan, Youzhi Li, "Design and Implementation of General Distributed Heterogeneous Data Exchange System" 978-1-61284-486-2/11 2011 IEEE.

[2] Danan Thilakanathan, Rafael Calvo, Shiping Chen, Surya Nepal," Secure and Controlled Sharing of Data in Distributed Computing ",2013 IEEE 16th International Conference on Computational Science and Engineering.

[3] Marwan Sabbouh, Kenneth McCracken, Geoff Cooney," Data Sharing for Cloud Computing Platforms" ,2014 IEEE International Congress on Big Data

[4] R. Nithiavathy,"Data Integrity and Data Dynamics with Secure Storage Service in Cloud", Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, February 21-22.

[5] Zhe Zhang1,2, Min Song3, Daxin Liu1, Zhengxian Wei2 , Hongbin Wang1, Jun Ni4," Data-Structure-Model for Data Integration in Distributed Systems" 978-0-7695-3430-5/08 $25.00 © 2008 IEEE DOI 10.1109/IMSCCS.2008.45 194

[6] Danan Thilakanathan, Rafael Calvo, Shiping Chen, Surya Nepal", 2013 IEEE 16th International Conference on Computational Science and Engineering", DOI 10.1109/CSE.2013.125

[7] S. Tu, S. Niu, H. Li, Y. Xiao-ming, M. Li (2012)" Fine-grained Access Control and Revocation for Sharing Data on Clouds.m Parallel and Distributed Processing Symposium Workshops &PhD Forum (IPDPSW)", 2012 IEEE 26th International: 2146-2155

[8] Luca Ferretti, Michele Colajanni, and Mirco Marchetti,," Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[9] Zeng Dadan, Zhou Minqi, Zhou Aoying," A Data Accessing Method in Distributed Massive Computing", 978-0- 7695-3745-0/09 2009 IEEE DOI 10.1109/HIS.2009.203

[10] G.Ateniese, K. Fu, M. Green, and S. Hohenberger," Cloud-Enabled Data Sharing Model" 978-1-4673-2104- 4/12/$31.00 ©2012 IEEE

[11] Jian YANG, Huijia TANG, Linfu SUN and Shengyin WANG. N Research and Realization of Heterogeneous Data Exchange System Based on XML. Computer Engineering, 31 (19) : 195-197, 2005.

[12] Kui Ren," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS FEBRUARY 2014.

[13] Pengzhi Xu ," Campus Cloud for Data Storage and Sharing", 2009 Eighth International Conference on Grid and Cooperative Computing.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. Of CCS'06, 2006

[15] Yu, C. Wang, K. Ren, and W. Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing, Proc. IEEE International Conference on Computer Communications, INFOCOM'10.

[16] R. Buyya, C. S. D.Pratiba Yeo, and S. Venugopa, "Market-oriented cloud computing:Vision, hype, and reality for Delivering it services as computing utilities", Proc. the 10th IEEE International

Conference on High Performance Computing and Communications (HPCC 08), 2008, pp. 5-13.

[17] G.Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy reencryption schemes with applications to secure Distributed storage. In NDSS. The Internet Society, 2005.

[18] Bethencourt, J.; Sahai, A.; Waters, B. (2007): Ciphertext- Policy Attribute-Based Encryption. Security and Privacy, IEEE Symposium: 321 – 334.

[19] Sundareswaran, S; Squicciarini, A.C.; Lin, D (Jul/Aug 2012): Ensuring Distributed Accountability for Data Sharing in the Cloud". IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 4: 556 - 568

BIOGRAPHY

Ashish G.Ahuja Received Bachelor of Engineering in Information Technology from SGB Amravati University & Pursuing Master of Engineering in Computer Science and Engineering from P.R.Pote (Patil) College of Engineering and Management, Amravati.

Assistant Prof. Komal B. Bijawe Received Master of Engineering in Computer Science and Engineering from SGB Amravati University. Working as Assistant professor in P.R.Pote (Patil) College of Engineering and Management, Amravati.