IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Proposed Model for Ensuring More Security in Cloud by Data Fragmentation Method

V. Kiran Kumar[1*], E. Hari Prasad[2]

[1]Dept. of Computer Science, Dravidian University, Kuppam-517425, Chittoor dist, Andhra Pradesh, India
[2] Dept. of Science, Dravidian University, Kuppam-517425, Chittoor dist, Andhra Pradesh, India

Available online at: www.ijcseonline.org

Accepted: 16/Nov/2018, Published: 30/Nov/2018

Abstract— Cloud Computing is a latest technology where the usage of this service by different clients was increasing rapidly day by day. Cloud provides different services with best facilities to utilize it. Presently many small and large scale businesses were using Cloud services to meet their requirements. The one of the main service in cloud is cloud storage. The major requirements for achieving security in outsourced databases are confidentiality, privacy, integrity, availability. Now a day's many companies gives access their clients to store their data in remote storage server i.e. cloud .as well as one of the main issue in cloud is data security. In consideration with the cloud security, in this paper we proposed architecture for storing the data in cloud using the fragmentation method. The detail architecture is discussed in the paper.

Keywords— Security as a service, Cloud Models, Fragmentation, Database.

I. INTRODUCTION

Computing is one of the emerging technologies in Computer Science. Cloud provides various types of services to us. Database Outsourcing is a recent data management paradigm in which the data owner stores the confidential data at the third party service provider's site. The service provider is responsible for managing and administering the database and allows the data owner and clients to create, update, delete and access the database. There are chances of hampering the security of the data

Due to non reliability of service provider. So, to secure the data which is outsourced to third party is a great challenge. The major requirements for achieving security in outsourced databases are confidentiality, privacy, integrity, availability. To achieve these requirements various data confidentiality mechanisms like fragmentation approach, High-Performance Anonymization Engine approach etc. are available. In this paper, various mechanisms for implementing Data Confidentiality in cloud computing are analyzed along with their usefulness in a great detail.

IT businesses are migrating to the Cloud environment at a rapid elasticity. Security of information that is being processed by way of the purposes and finally getting saved in the data facilities are of gigantic issues of this newly evolving environment. The protection of the data is a quandary not most effective in the course of transferring of information by means of the wires but additionally for the duration of its storage. The architecture that is wanted to at ease the saved information is of so much value than whilst the information is getting transferred given that of the truth that the info resides fairly for a very long time within the storage subject than within the wires. To make certain the safety of the data stored within the knowledge facilities, a new methodology is proposed which would not thoroughly help in proscribing a hacker to access the information but will make the information worthwhile if it is extracted through a hacker but at the identical time ensures the best of the info that is being furnished to its respective proprietor or licensed consumer. A metadata based knowledge segregation, storage methodology and solutions is proposed to access this segregated information. This system ensures that data is important in the course of static house and positive aspects worth most effective for the duration of acquisition or updating.

II. FRAGMENTATION OF DATA IN CLOUD:

A disbursed database is a set of records that logically belongs to the same gadget but is spread over the websites of a pc community. Ceri (1984) and Ozsu et al (1999) defines a Distributed Database Management system (DDBMS) because the software machine that provides the control of the allotted database gadget and makes the distribution obvious to the customers. It isn't always vital that database device ought to be geographically allotted. The web sites of the allotted database could have the equal network address and can be in the identical room however the communication among them is performed over a community in preference to shared memory. The communication community is the simplest shared aid for DDBMS. As verbal exchange era, hardware, software protocols advances swiftly and prices of network equipments falls each day, developing dispensed database systems turn out to be more and more viable.

Design of efficient disbursed database is one of the major research troubles in database & records era areas.

Distributed processing on Database Management Systems (DBMS) is an efficient way of enhancing overall performance of programs that manage massive volumes of statistics. This may be carried out by using doing away with irrelevant information accessed for the duration of the execution of queries and by decreasing the information change amongst websites, which might be the two principal goals of the design of dispensed databases (Ceri 1984). Primary difficulty of distributed database gadget layout is making fragmentation of the family members in case of relational database or lessons in case of object orientated databases, allocation and replication of the fragments in one of a kind sites of the allotted system, and nearby optimization in every website online (Navathe 1995).

Fragmentation is a layout method to divide a single relation or class of a database into or more partitions such that the mixture of the partitions provides the unique database with none lack of information (Ozsu et al 1999). This reduces the amount of inappropriate records accessed by using the packages of the database, accordingly reducing the wide variety of disk accesses.

Fragmentation can be horizontal, vertical or mixed/hybrid. Horizontal Fragmentation (HF) lets in a relation or elegance to be partitioned into disjoint tuples or times. Vertical Fragmentation (VF) allows a relation or magnificence to be partitioned into disjoint units of columns or attributes besides the primary key. Combination of horizontal and vertical fragmentations to combined or hybrid fragmentations (MF) are also proposed (Navathe 1995). Allocation is the procedure of assigning the fragments of a database at the web sites of a distributed network. When statistics are allotted, it is able to either be replicated or maintained as a unmarried replica. The replication of fragments improves reliability and efficiency of read-handiest queries however will increase update price The major motives of fragmentation of the relations are to: growth locality of reference of the queries submitted to database, enhance reliability and availability of statistics and overall performance of the gadget, balance storage capacities and reduce communication costs amongst sites (Baio 2004).

III. PROPOSED WORK

PROPOSED MODEL FOR STORING SECURED DATA IN CLOUD USING METADATA FRAGMENTATION MODEL:

The design of distributed database is an optimization problem and the resolution of several sub troubles as information fragmentation (horizontal, vertical, and hybrid), statistics allocation (without or with redundancy), optimization and allocation of operations (request transformation, choice of the exceptional execution strategy, and allocation of operations to web sites). There are some distinct processes to resolve every trouble, which means that that the design of the dispensed databases has grown to be hard enough. There are many researches connected to the records fragmentation and they are provided each in the case of relational database and within the case of item-oriented database.

This version is based on the reality that any records are precious most effective so long as the fragments of the facts are related to each other. When associated data aren't to be had in a mapped way, its miles of no use. For instance, facts approximately a credit card number without its corresponding

Facts like card holder call, validity date and Card Verification Value (CVV) is precious and so is it's vice versa. And a similar instance is the mapping of username and password. A username on my own isn't always treasured and so is the statistics about the password by myself. The records become treasured handiest when those fragments of statistics are mapped. The mapped data about elements is needed only for authenticated customers and proprietors of the respective facts. A widely known example of intrusion of person records is the one recorded by Sony PS Network in recent times (Dan 2011).

In one of this scenario, there's no necessity that facts have to be stored in a mapped manner. But mapping is needed on the point of usage. Juels et al (2007) described a proper "Proof of Irretrievability" (POR) model for ensuring the faraway records integrity. Their scheme combines spot-checking and error-correcting code to make sure each possession and irretrievability of files on archive provider systems. The time of usage of the records is apparently very much less in assessment to the time that statistics is gift at the storage vicinity. Thus two varieties of safety concerns stand up. One issue is during facts utilization, i.e. In the course of transmission and secondly, static section of the data, i.e. during dwelling at storage centres.

The model defined deals handiest with the facts security at the storage centres. This in turn has two issues: One issue is about the actual physical unit wherein the facts are stored and the alternative one is the intrusion into the facts. The proposed model specifically focuses in presenting security to avoid intrusion. This model does not prevent hackers from getting maintained of the data. Rather it makes the records precious although its miles accessed by means of an interloper. To adhere to this version, care needs to be taken right from the design segment of the facts storage. Data needs to be segregated into Public Data Segment (PDS) and Sensitive Data Segment (SDS). The SDS has to be further fragmented into smaller units till every fragment does now

not have any value individually. The fragmentation want now not be of a couple of stages. Instead, effort is required to perceive the key element that makes the data touchy and should be fragmented one after the other. Below Figure explains this fragmentation.

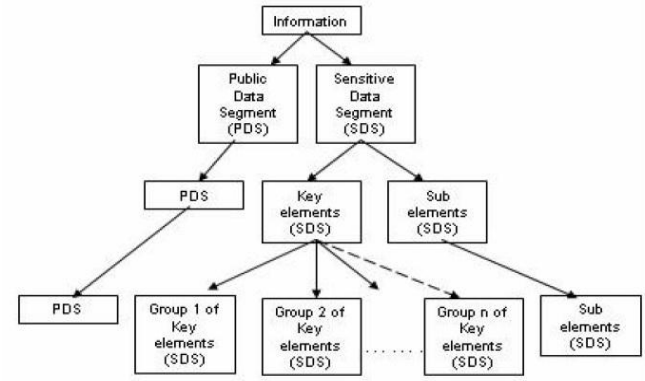

Fig. 1

The proposed methodology is quite unique from commercially available sliced records garage answers like Symform and Clever safe which was evaluated by Paul (2011). In those answers, the statistics is considered in byte formats. In a typical state of affairs, data is broke into 64MB chunks and each bite is encrypted with AES 256 bit encryption and then these chunks are saved in distinct locations. These solutions are applicable for raw facts, but this could not be powerful for data stored in relational databases that have records interdependencies and are logically saved based on schemas.

Our version enforces that the associated records should be saved at extraordinary places and ought to be mapped runtime either during replace or question. Consider that this complete version is migrated to our proposed version through the DME. The user has to supply the schema information of those tables to the DME and together with its metadata. Let us consider only 3 classes of metadata for this case. The record that is having low value is taken into consideration as 'Normal'. The records that is having high cost is considered as 'Critical' and the data which has cost while mapped with different information is taken into consideration as touchy. The fact which maps 'Sensitive' or 'Critical' records to 'Normal' information is also taken into consideration 'Sensitive'.

The DME now has to fragment these facts. The DME have to be able to be configured or custom designed with appreciate to the level of safety required. Considering the desired example, if DME desires to provide medium degree protection, it needs to fragment most effective records which are of 'Critical' criteria. And if excessive stage safety is required, it should fragment facts present in each 'Critical' and 'Sensitive' standards. The DME isn't always privy to the real statistics residing within these tables. Hence alongside the metadata of the tables, the number one key column call needs to be provided in addition to it. This is without problems available with the schema statistics of the database tables. The specific levels of protection wanted and their corresponding metadata need to be configured with the DME.

After fragmentation is finished, the DME segregates the schema, separating out the information changed by means of DME, 'Originally Sensitive' information and 'Normal' information.

The DME then actions the 'Normal' data to at least one database and 'Originally Sensitive' statistics to any other database and AD of 'Sensitive DME' information to another database at exclusive vicinity and MD of 'Sensitive DME' to the database with 'Normal' statistics. With recognize to the AD, if DME creates its very own desk, then this desk will be the more secured records and may be saved in a exclusive vicinity. Different region here states the both specific server on the same geographical location or at different geographical vicinity. Additionally one extra mapping is required for mapping the original desk with the fragmented facts set. This can be saved in a separate table.

Now each database includes statistics which does no longer have price in itself. The whole mapping is performed handiest throughout runtime and the price is built up quickly for the duration of get right of entry to and replace and later its cost is destroyed. An intruder who receives get entry to to the statistics in the course of the static section of the lifestyles cycle of the statistics can't use the statistics to exploit the information with the aid of any way. The integrity between the unique schema and the brand new schema may be taken care with the aid of deploying a database runtime migration environment so as to deploy all the logics required for the runtime technology of schema and its corresponding drop after its lifecycle.

IV. CONCLUSION

To make sure that the facts is at ease in the course of the stored segment of the existence
cycle of the data, a metadata based records fragmentation version became advanced the use of which the records living at statistics center are robbed in their values and the values are temporarily constructed up at some stage in runtime after which destroyed once its utilization scope is finished. This makes the data precious despite the fact that an intruder receives access to this information. Though this version will take a few quantifiable efforts to be implemented in actual time, it gives vital answer for surroundings just like the Cloud that's showing an unfavorable ability to come to be the subsequent era employer environment. Implementing such a version in the course of the earlier stages of the evolution of the machine can be exceedingly simpler with recognize to

imposing it after lot of records take refugee inside the cloud. This version in aggregate with the multi-tier protection model for securing facts over transmission will offer proper go bars in the wires of malicious users.

REFERENCES

[1]. Foster, I., Zhao, Y., Ioan, R. and Lu, S. "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, 2008.

[2]. Azzam, S., Wesam, A., Samih, A. and Abdulaziz, Y. "A Dynamic Object Fragmentation and Replication Algorithm in distributed database systems", American Journal of Applied Sciences, pp. 613-618, 2007.

[3]. Balachandra, R., Ramakrishna, P.V. and Atanu, R. "Cloud Security Issues", In IEEE international Conference on Services Computing, pp. 517-520, 2009.

[4]. Ceri, S. and Pelagatti, G. "Distributed Databases Principles and System", 1st ed., New York: McGraw-Hill, 1984.

[5]. Cong, W., Qian, W. and Kui R., "Ensuring Data Storage Security in Cloud Computing", Cryptology ePrint Archive, Report, http://eprint.iacr.org/, (accessed: 18 October 2009), 2009.

[6]. Jay, H. "What you need to know about Cloud Computing Security and Compliance", Gartner, Research, ID Number: G00168345, 2009.

[7]. Katja, H. and Ralf, S. "Distributed Database Systems-Fragmentation and Allocation," Cluster of Excellence MMCI, October 2010.

[8]. Gibbs, M.R., Graeme, S. and Reeva, L. "Data Quality, Database Fragmentation and Information Privacy", Surveillance and Society, http://www.surveillance-and-society.org/articles3 (1)/data.pdf, (accessed on 11 January 2012), pp. 45-58, 2005.

[9]. Navathe S., Karlapalem, K. and Ra, M. "A mixed fragmentation methodology for initial distributed database design," Journal of Computer and Software Engineering Vol. 3, No. 4 pp 395-426, 1995.

[10]. Ozsu, M.T. and Valduriez, P. "Principles of Distributed Database Systems", 2nd ed., New Jersey: Prentice-Hall, 1999.

[11]. Weiss, A. "Computing in The Clouds", In ACM networker, pp. 16–25, 2007.

[12]. Ch.V.B.Neeraja1*, S.S.S.N.Usha Devi N2, "A Novel Two Level Search Scheme to Provide Security and Privacy of Encrypted Spatial Data," International Journal of Scientific Research in Computer Science and Engineering Vol.6, Issue.6, pp.01-05, October (2018),

[13]. Kodge B. G.," Information Security: A Review on Steganography with Cryptography for Secured Data Transaction", International Journal of Scientific Research in Network Security and Communication, Volume-5, Issue-6, Dec 2017.

Authors Profile

Dr. V.Kiran Kumar, Working as a Associate Professor in the Dept of Computer Science, Dravidian Uniersity, Kuppam. Chittoor Dist. A.P. His Research area are Semantic Web, Web Technologies, Programming.

Mr. E.Hari prasad, Working as Academic Consultant in the Dept of Computer Science, Dravidian Uniersity, Kuppam, Chittoor Dist, A.P. He is doing his research in domain of Cloud Computing in Dravidian University, Kuppam.

