International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Data Security Model using Artificial Neural Networks and Database Fragmentation in Cloud Environment

D.Suneetha, D.Rathna Kishore, G.G.S.Pradeep

Abstract: ***Data security is a one of the challenging issue in present scenario. In that one of the on demand service is cloud computing and it provides so many services for end users and also it provides a dynamic environment for end user to provide quality of services on data it leads to improve in the confidentiality of the data. The proposed work presents a new cloud data security model with the help of Artificial Neural Network. It improves the confidentiality and security in cloud environment. This proposed algorithm is implemented using dynamic hashing fragmented component. It is implemented for storing fragmented sensitive secret data. The neural network cryptographic proposed algorithm is used for data to deal with encryption process for secret and improve the confidentiality. This algorithm applied for various number of cloud databases and it shows high confidentiality on data security.***

Keywords: Cloud Data Security, Encryption, Fragmentation, Artificial Neural Networks, Confidentiality, Cryptography

I. INTRODUCTION

Cloud Computing is one of the buzz word especially used for to deploy application on internet. It provides so many services for end users and it has huge number of applications use large data centers and various numbers of efficient servers to host end user applications and providing various services [1]. It is a model for enabling various services on demand network access to shred various resources with minimum management efforts of various service providers. Cloud computing model consists of three models and those three are the important services of the cloud. Those are Infrastructure as a service, Platform as a service and Software as a service. In this environment we have four different types of model are composed those are private cloud, public cloud, community and hybrid cloud.

In this work we discussed about databases, data security and fragmentation. In general a cloud database runs on cloud computing platform. In this have two different types of databases i.e. the basic deployment model are two. One is run on independently with the help of virtual machine and another is a pay on service that means buy a database service for running on the cloud platform and it is maintained by the third party of cloud provider.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

D.Suneetha*, Associate Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.

D.Rathna Kishore, Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.

G.G.S.Pradeep, Professor, Department of CSE, Malla Reddy Institute of Science and Technology, A.P, India.

Every organization requires organizing data in systematic way and managing their own secret sensitive data in secured manner without accessing by unauthorized person. The main objective of this work is overcome the problem of critical cloud data security and to ensure safe or trustworthy cloud environment [13].This proposed approach mainly concentrates on one of the challenging issue confidentiality. Confidentiality means data us not relevant by unauthorized person or hackers. And it ensures improvement in the quality of service in cloud environment. For this improvement in this work apply fragmentation for cloud secret data. It is a one of distributed database design to divide a single relation into multiple classes or partitions without loss of original data. To increase the security in this a new data security model was proposed using neural networks. It is composed of highly interconnected networks called neurons. Those neurons are trained used supervised and in supervised learning. In supervised learning there was master for supervising and managing network related activities. In unsupervised learning there was a no master for these activities. In this one of the methods for learning neural network is counter propagation for various applications of cloud. This leads to guarantee for data to achieve improvement in confidentiality.

II. RELATED WORK

In this studied various security challenges and issues in cloud environment along with the limitations of various existing algorithms for various clod data security models. In the first focus Data confidentiality, relational databases with number of fragmentation techniques. Aleskandr[2] proposed a research work on the clod data privacy for various number of threats. In this use the concept of fragmentation along with relational database links to find out the locations and unlink the locations. The end user stores up the data to provide confidentiality along with the cloud service provider. This fragmentation is applied both vertically and horizontally on independent fragments. Vimmercat[3] had proposed fragmentation method to meet end user requirements. This algorithm has improved method in the data fragmentation and improves in the data manipulation process, storage requirements of data security. It mainly focuses on protecting on fragmented data.Cirrani[4] had proposed a new approach for data security. In this combine fragmentation with encryption process. This fragmentation is applied on the sensitive data for partitions. In addition to that this algorithm has decryption parameters based on the queries, attributes of the relevant relational database. Waang[6] proposed a secure cloud data storage model for secret data of end use.

This system support public auditing of privacy preserving environment. It uses linear authentication and random number generation system for masking process to get efficient auditing results. It only supports auditing for single party it does not support for multi party.Abbaddi[7] proposed a new technique for data security by utilizing hashing technique. In this hashing technique is used to find out the locations of the direct data on the disk fragments. In this used dynamic hashing it provides some of the on demand services like data which are added or removes those details are provide whenever an end user requesting cloud service provider immediately it gives results to the end user. The dynamic hash structure is cloud environment uses an prominent and efficient for verifications of various data locations in cloud environment.Jiaawel[8-9] had proposed a new data security model for cloud environment. In this scheme each party encrypts his own data and place into the cloud. The cloud executes various operations on the cipher text without converting into the original data all the operations are directly performed on the cipher text. It uses doubly encryption algorithm for multiparty operation i.e. supporting it doesn't support one of the operations of multi party i.e. multiparty collaborative.Syamkumar[10] proposed one of the effective technique for data security. In this mainly focus of one of the challenging issues of data security i.e. Quality of service. In this proposed a flexible distribution technique for protecting secured data from unauthorized persons. This technique uses some of the pre requisition parameter like accessibility, tokens utilization for pre computing process. And also uses random number generation for providing integrity for end user secret data. This technique proved it is better than some of the existing algorithms to provide security for end users data.

Hung proposed [11] a encryption method which provides encryption/decryption process on data more than one technique is performed for end user secret data in parallel with one another. After encrypting the data either with public key or private key encryption algorithm again the cipher text is encrypted with other encryption algorithms that mean re-encryption process was done. This method which have various numbers of functions without decrypting original text. Itry[12] proposed a new fully homporphic algorithm to protect the form unauthorized person under cloud environment. This method has number of calculation and the method cost is high.

This paper mainly focuses on the data security for end users secret data in cloud environment and improves the confidentiality level for end user secret data. The idea is to limit the unauthorized person for accessing storage facilities of the cloud service providers. The fragmentation approach decreases the need of complex searchable operation and ensures the privacy for data and this process was managed by the cloud service providers. Confidentiality is provides with various data security techniques and describing query process relational model. The main limitations of existing database fragmentation are the entire database was fragmented. And it is difficult to access the end users also. The performance of the existing methods is poor related to data security and those are not applicable for multi party environment. To eradicate s the drawback of the old existing algorithm in this paper present a new "Neuron based security model" which will concentrate existing drawbacks and improve in the data security finally leads to improve in the confidentiality characteristics of data security.

I. PROPOSED ALGORITHM

The main objective of this proposed work is to identify and understand various security issues and challenges for cloud environment and also identify appropriate security algorithms which are used currently to protect data from unauthorized persons. The dynamic hashing component provides confidentiality for sensitive secret data and it also provides data isolation. It automatically extends during operations like insertion, deletion, updating including block insertion deletion and appending. The neural data security model is responsible for encryption and decryption process of cryptography. It uses public and private key cryptography using artificial neural networks. The proposed model is efficient and effective for different kinds of queries and the improvement in the confidentiality level of data security. This proposed model is less in expensive and higher performance with respect to security and storage.

The proposed work objective is achieving confidentiality for cloud data using fragmentation. The fragmentation is done both horizontally and vertically. It is a technique in which data can be stored for different cloud data centers by fragmenting the databases into several partitions called fragments. Confidentiality is achieved by dividing database into different fragments for identifications of different locations. The architecture of the proposed data security model presented in Figure 1. First the data is divided into different fragments. Such as F1, F2, F3 etc all the fragments are stored into the various data centers of the cloud. The sensitive data is M is encrypted separately. The fragments also stored using dynamic hashing mechanism in respective data centers.

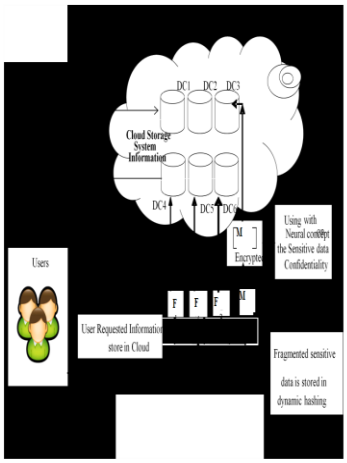

Fig.1. Proposed Data Security Model

Dynamic Hashing Fragmented Component:

In cloud data centers huge amount of data sets are stored. The structure of the dynamic fragments is dynamic in nature which increases or decrease the sized based on the supplied dataset automatically. The main of this is to divide large dataset into small number of fragments and store in into corresponding data centers.

The fragmented data has met the following requirements.The applied dataset should be n third normal before applying

Table. 1. Comparison of Proposed with un-fragmented data

Number of queries	Un fragmented Table	Fragmented Table	Improvement Percentage of fragmented table with proposed "Neural based Model"
Scalar Queries 400	78.3	64.2	14.10%
Range queires300	62.4	42.56	19.84%
Unique queries500	75.8	51.87	23.93%
Nested Querires500	69.7	41.37	28.33%

the fragmentation process It provides significant amount of confidentiality level for fragmented data. Extra demand or the user requirements are chosen by the end user. Before applying
fragmentation process for relevant database that can be normalized with normal forms. The first normal form removes the multivalve and it makes into the individual tables for relevant data. The second normal meets all the requirements of the end user and also it will separate the relations of the tables. The third normal removes transactional dependencies on data.

Algorithm1: Process for Fragmentations

Input: Data set from cloud database
Step1: Start
Step 2: Read required dataset form cloud database which will have relevant sensitive secure data
Step3: Fragment the sensitive data horizontally, vertically and hybrid
Step 4: Store the fragmented data in hashing and read the data using hash function key =m mod n
Step5: The data is encrypted using encryption algorithm using neural networks
Step 6: The encrypted data is stored into the cloud
Step 7: Stop

Algorithm 2: Process of Conventional encryption algorithm using Neural Networks

Input: Fragments from cloud data centers
Output: encrypted data
Step1: Start
Step 2: Read the fragments from the Data centers using hash function
Step3: Encrypt each fragment by using AES algorithm and obtain the cipher text
Step4: Obtained cipher texts is converted into binary format and give it to the input for cascading feed forward network
Step5: Train the binary values in cascading feed forward networks in three layers
Step6: Convert the data from binary to ASCII values and that is the cipher text and it will be stored into the relevant data centers of the cloud
Step 7: Stop

III. RESULTS

To identify performance of the propose algorithm we conduct four test each with 400 instances of sample data sets with different confidentiality levee i.e. low, medium and high These four tests done for different query operations like insertion , deletion etc. for analyzing we select the different types queries are taken into consideration like single, nested queries etc. Table 1 shows results of various un-fragmented data and fragmented data.

For the experiments of scalar query the percentage of query execution failures is very low. The success rate, failure rate is 94.65%, 6.45%.In horizontal fragmentation the success and failure rate for scalar queries 97.89%, 2.31%. In vertical fragmentation the success and failure rate for scalar queries are 98.13%, 2.87%. The maximum query execution failure rate is in the range o f 0 to 6% only. The results are scalar is high compared to remaining types of queries. The various results of queries for fragmented and un-fragmented data are shown in Table 2 and Table 3.

Table. 2. Performance analysis for unfragmented data

Fragmented Data

Type of query	Horizontal			Vertical			Hybrid		
	Success%	Failure%	Not Completed%	Success %	Failure%	Not Completed%	Success%	Failure%	Not Completed%
Scalar	94.35	4.63	1.02	95.45	2.66	1.89	93.42	4.02	2.56
Range	96.23	1.9	1.87	97.65	1.33	1.02	94.76	1.04	4.2
Unique	92.35	5.31	2.34	96.43	2.53	1.04	97.61	1.29	1.1
Nested	91.57	4.98	3.45	97.13	1.11	1.76	92.45	3.66	3.89

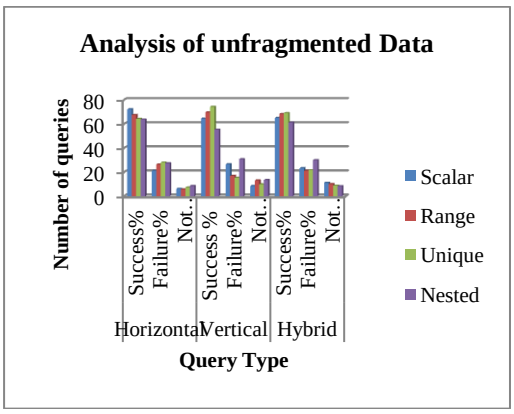

Fig.2. Analysis of un-fragmented data

Table. 3. Performance Analysis For Un-Fragmented Data

Un-fragmented Data

Type of query	Horizontal			Vertical			Hybrid		
	Success%	Failure%	Not Completed%	Success %	Failure%	Not Completed%	Success%	Failure%	Not Completed%
Scalar	72.34	21.29	6.37	64.56	26.77	8.67	65.23	23.43	11.34
Range	67.64	26.47	5.89	69.76	17.04	13.2	68.45	21.27	10.28
Unique	64.35	28.22	7.43	74.35	15.51	10.14	69.23	21.8	8.97
Nested	63.89	27.44	8.67	55.46	30.87	13.67	61.34	30.1	8.56

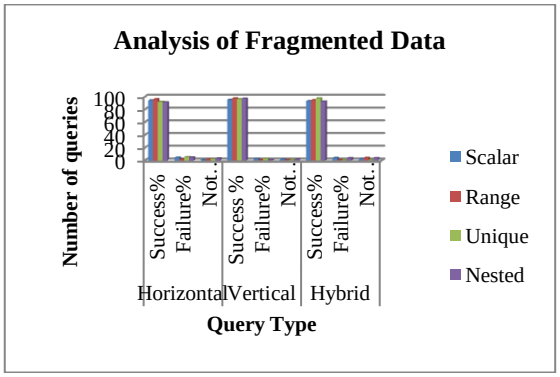

Fig 3. Analysis of Fragmented data

IV.CONCLUSION AND FUTURE SCOPE

One of the major aspects of cloud is to provide the confidentiality with high security level while accessing data from cloud database by the end user. The proposed security model improves the confidentiality level of data with the help of Artificial Neural Networks which also improves the security of data over cloud environment. The Dynamic fragments model stores highly sensitive fragments in the corresponding data center over the cloud and also use encryption algorithm in combination with cascading feed forward network to obtain relevant cipher text. This work is tested using various datasets of different confidentiality level and is shows better improvements with respect to confidentiality level and data security over the datasets of cloud environment.

REFERENCES:

1. Aggarrwal, Baiwa, , “Two can keep a secret: A an architecture for distributed architecture for secure database services,” in Proc. of the 2nd (CIDR’05), Asilomar, California, USA, pp. 186–199, January 2015.
2. Aleskandr., Peteer Kieeseberg., Edguar R. Weipppl, “Confdendailty using fragementation ” International Journal of Pervsasive Computing using neurons , 2016.
3. Vimmercat Cireiani, , “Enforcing confidentiality and integrity with Conference on Data and Applications Security and Privacy (DBSec’11), Springer- Verlag, vol. 6818, pp. 47–59, 2014
4. Cirrani S. Paraboscchi, and P. Samuarati, “Fragmentationand encryption techniques , LNCS, vol. 4734. Springer-Verlag, pp. 181–189 Octomberber 2017.
5. S. Forestti, , “ Combining data fragmentation and data encryption to for secured storagestorage”, ACCM Trans. Inf. Syst. Secure, Vol:15, 2018.
6. Waang., Shermanu., “Privacy-Preserving and Auditing for Storage under cloud environment ,” IEEE Transactions, Vol:5 , Issue: 2, 2016.
7. Abbaddi ,Bondee, , ‘Techniques for back propagation using neural networks”, IJEAR, Volume 3, Issue 1, February 2015
8. Ziswsis. Jiaawel, “Addressing cloud computing challegngig issues,” Next Generation Computer Systems., Elsevier journal., 2016.
9. E Damiani., Simercati., ajodia., Jiaawel., “Balancing data Confidentiality and Efficiency in trusted Relational DBMSs,” ACCM Transaction 2013.
10. Huidic. V, Sihareeful “Data Condentiality using un- Fragmentation in Cloud Computing” IJCNDS , Vol. 2, pp 3, 2014.
11. Imaad., “Towards Un- Trustworthy Resource Scheduling and security in Clouds,” IEEE Transactions, Vol. 8, No. 7, July 2014.
12. hiansekhar and Balajji, “An Efficient indexing” ICIET’15, 2015.
13. Montreeal, “Fragmentation design for query execution over non sensitive distributed databases,” 29th ICDCS 2009), , pp. 36–42, 2015.