International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Enhanced Security Model in Cloud Using Neural Networks

Ms. A.Anto Viji[1], Dr. J. Jasper[2], Dr. T. Latha[3]

[1]Assistant Professor, Department of Computer, Science and Engineering, CSI Institute of Technology, Tamil Nadu, India

[2]Professor, Department of Electrical and Electronics Engineering, Ponjesly College of Engineering, Tamil Nadu, India

[3]Professor, Department of Electronics and Communication Engineering, St. Xavier's Catholic College of Engineering, Tamil Nadu, India

ABSTRACT

In order to improve redundancy elimination security is an important factor to be considered. To increase the security of cloud storages a new method of neural network based security enhancement has to be provided. Data confidentiality with sensitive data sets and provides data isolation. The dynamic fragmented component automatically extends and shrinks during insertion and deletion, respectively, and also provides explicit dynamic data support, including block update, delete, and append. The Neural Data Security model is used to encrypt and decrypt the sensitive data by using cryptography. It attains data security for public and private keys using cryptography using Neural Networks. The Data Security Model is more efficient and effective for all kinds of queries, and performance is high at the data confidentiality level. This model provides less expensive, higher performance and an expandable storage system to enhance the security.

KeyWords: Confidentiality, Neural Networks,, Security, Redundancy, Fragmentation

I. INTRODUCTION

Cloud computing is a group of ideas of distributing huge amount of applications over internet. Cloud enables global access among multifaceted heterogeneous networks over internet as pay as you service from a shared pool of resources. Resources in cloud computing are managed without the direct active management by user. A large amount of redundant data stored in cloud data leads to inefficient use of exquisite cloud resources. Traffic redundancy leads inefficient use of shared pool network. A long dreamed computing vision as utility based on remote server storage. End user generates traffic redundancy during higher usage of cloud resources. Several traffic redundancy schemes have been introduced and security cloud provide by HMAC. Confidentiality [3] in cloud is based on the encryption techniques. Main issues in cloud that owner losses the control over the data stored in the cloud. Data confidentiality is implemented using the owner's private key along with cryptographic technique applied. Users are allowed to perform

security privileges and check the replicated data files in the network.

Security on cloud networks is high when compared to the existing approaches. Storage cost and computation cost reduces on neural network based approach. Integrity and Confidentiality of Data present in cloud are maintained Security is the most important factor in cloud computing and also in a major concern. Mutual cooperation concern and neural network scheme increases the redundancy [1] elimination and Security in homogeneous as well as heterogeneous cloud. Combination of both sender and receiver based elimination provide a better solution for network traffic and redundancy elimination. Cloud security is also a major factor for data storage in cloud environment, convergent encryption based technique used in mutual cooperation of sender and receiver to remove replica data in communication channels and optimize the bandwidth and cost in cloud.

Redundancy in cloud is the process of sending replicated data stored in various parts of cloud, when a cloud computing system fails to send or receive data the entire files in cloud cannot be accessed. This redundancy is made available by having fully replicated data several times on multiple computers or units involved in the same data center leads to higher costs. Differential privileges with deduplication[2] is one of the major issues in cloud computing . To avoid such problems in cloud a secure duplication scheme is used along with neural networks. this can be one among the largest challenge once applying information deduplication to cloud storage that have often changed knowledge. It demands an effective and efficient way to eliminate redundancy among frequently changed and therefore similar information. An economical approach to removing redundancy among similar information blocks is delta compression that has gained a giant attention in storage systems

II. RELATED WORK:

Cloud users store the user data remotely and attain a high quality of services on the various cloud applications. The mechanism used to store data in cloud needs to be efficient and confidential. Cloud data using horizontal and vertical fragmentation. Fragmentation is the technique in which the data can be stored in different cloud data centers by fragmenting the whole database into several pieces called fragments. Data confidentiality is achieved by relational databases into independent fragments and then processing them into different locations. The architecture describes the flow of the Neural Data Security Model. This model is used to store data in cloud in an efficient and confidential way.

The user data are first fragmented into small fragments and stored in different data centers in the cloud storage. The sensitive data are encrypted as separately. The Fragmented data are stored efficiently using the dynamic hashing mechanism. These sensitive data are encrypted using cryptographic algorithm with neural network and are stored in order to achieve a higher level of confidentiality. In this research work, we propose a new model called, “A Cloud Data Security Model: Ensure High Confidentiality and Security in the Cloud Data Storage Environment” .It implements high data confidentiality and security [7] for sensitive data in a cloud environment. The sensitive fragments are encrypted using cryptographic algorithm with neural network and are stored in different server locations. The unique features of dynamic hashing include orders of magnitude faster than other schemes and allows the client to read, update, insert and modify.

Cloud Encrypts user data or the owner’s data and issue identity to each and every user from the third party identity service provider. Users can access the data from the service provider by the identity issued by the service provider. Access control policies are used for the outsourced data in the cloud. Single

linear encryption uses convergent encryption technique that is planned to encipher information for confidentiality. This method user identity, and also the key is obtained by computing the crypto graphical hash value of the content of the message. After the completion of key generation and encoding, users retain the keys to personal cloud then send the cipher text to the cloud [5].

Deterministic encoding operation from the info content, alike information files produces exactly same user identity and therefore same cipher text. A secure proof of possession protocol

[3] is additionally needed to supply the proof that the user indeed owns. Duplicate files are pointed out by the pointers referencing the files in public cloud. Single linear encryption allows cloud to perform de-duplication of files by preventing unauthorized access to files.

Physical copy of data generates pointers referencing other redundant data technique called deduplication. To secure the confidentiality of private data throughout deduplication, the convergent cryptography technique is used to encode the information before uploading it onto the general public cloud. A duplicate-adjacency info for likeness detection wherever we've got to consider any information blocks to be similar provided that their respective adjacent information blocks are duplicate. Network traffic redundancy illustrated in a large-scale study of real-life traffic redundancy is accessible in [12], [13]. Packet-level TRE [1] techniques are compared. A new technique builds on their findings that an end to end redundancy elimination using neural schema has been established to obtain most of the bandwidth [10] savings results in benefit of low cost software end-to-end solutions.

A large-scale distributed computing hierarchy implicit a new significance in the promising era of Cloud. It is widely expected that most of data generated by the massive number of cloud storages must be processed locally at the users or at the edge, for otherwise the total amount user data for a centralized cloud would crush the communication network bandwidth[6]. A distributed computing hierarchy offers opportunities for system scalability, data security and privacy in cloud storages. The dynamic hash structure is cloud environment uses prominent and efficient for verifications of various data locations in cloud environment. TRE system [4] for the developing world where storage and WAN [9] bandwidth are scarce. It is a software-based middle-box replacement for the expensive commercial hardware. In this scheme, the sender middle-box holds back the TCP stream and sends data signatures to the receiver middle-box. The receiver checks whether the data is found in its local cache.

Data chunks that are not found in the cache [13] are fetched from the sender middle-box or a nearby receiver middle-box. Naturally, such a scheme incurs a three-way-handshake latency for noncached data. EndRE [2] is a sender-based end-to-end TRE for enterprise networks. It uses a new chunking scheme that is faster than the commonly used Rabin fingerprint, but is restricted to chunks as small as 32–64 B. Unlike PACK, EndRE requires the server to maintain a fully and reliably synchronized cache for each client. To adhere with the server's memory requirements, these caches are kept small (around 10 MB per client), making the system inadequate For medium- to-large content or long-term redundancy. EndRE is server-specific, hence not suitable for a CDN or cloud environment. Inorder to overcome the drawbacks of traffic redundancy and data security in cloud a novel technique of using dynamic hashing along with neural networks has been implemented.

III. PROPOSED WORK:

Neural Networks are a recent type of linear and convolution layers called binarized neural networks uses 0 and 1 layers initially represented as -1 and 1. Standard floating-point neural network while using less memory and reduced computation due to the binary format extends BNNs to allow the network to

fit on embedded devices by reducing floating point temporaries through reordering the operations in inference. There are three approaches are used to find out system accuracy and traffic redundancy elimination.

Fragmentation:

Maximum Fragments represents the max of fragments present in the fragmented data files. Maximum fragments can be written as

Mj = Max(Mij)

1≤n≤j

Where n is the number of users and Mij is j-th fragment of the input vector and Mj output vector fragments.

Average number of fragments can be calculated as

$$Mj = \sum_{i=1}^{n}(Mij/n)$$

After calculation of the average fragments present in cloud storage concatenate each and every encrypted files present in the entire storage to extract the higher level fragments present in cloud.

Z=fexitn (x;θ)

where fexitn is a function representing the computation of the neural network layers from an entry point to the n-th exit branch and θ represents the network parameters such as weights and biases of those layers.

Files present in the cache storage are splited into fragments by means of linear convolution layers. Each user send the information to the local cache storage. The local cache storage send sum of combined files present in cache to the data base, now the exact file location for the user has been identified. If the local cache storage find the exact location of files no information will be send to cloud otherwise it sends an information about file for retrieving.

The total communication cost for local cache and cloud can be calculated as

$$m=4x|M|+(1-l)gxf$$

8

whereas l is percentage of sample files in cache, M Set of all files in cache, g number of filters and f output size of single layer filter.

Dynamic Hashing:

Convergent key encryption is considered as the best way to ensure secure data deduplication. But it has been observed that convergent key encryption has various drawbacks. Hence convergent key encryption mechanism should not be used to protect data privacy; the better mechanism is needed to ensure secure and efficient data storage A Dynamic hash function will map a collection of distinct entries into a set of n integers. It is a technique to reduce the collisions when a huge number of insertions, deletions, and search operations are to be performed on a huge number of data items. The time complexity for performing insertion, deletion and search operations is very efficient in cloud. Main strategy of dynamic hash divide the input data items into various buckets with a small number of data elements, identify a collision free mechanism for the buckets separately. The average number of data elements in each bucket can be changed as we execute the algorithm. We can also choose the load factor, which is the percentage of occupied positions in the hash table dynamically. The complexity involved in developing the dynamic perfect hashing is linear, can be calculated in constant time. The generation of dynamic hashing is possible even when we have a large pool of data items. to make the mechanism secure, we can make use of the one-way hash functions like Secure Hash algorithm(SHA-2) so that it will be impossible to figure out the data item based on the identifier of the data item.

IV. CONCLUSION

Providing secure cloud storage and redundancy has been the necessity of the day, as every computer user wants to make use of the cloud storage. We have considered the client side deduplication considering

the variable level of security demands for the data items and leveraged the advantage of the hash function in indexing the data items. Data related to the popularity of data items has been maintained by a partially trusted key server that will help the user in knowing which data items are unpopular. Our further work is in providing the secure and efficient data storage in the cloud computing environment and making cloud storage a key choice for storing valuable data in a secure way.

V. REFERENCES

[1]. Eyal Zohar, Israel Cidon, and Osnat Mokryn "PACK: Prediction-Based Cloud Bandwidth and Cost Reduction System" IEEE, 2014.

[2]. B. Agarwal, A. Akella, A. Anand, A. Balachandran, P. Chitnis, C. Muthukrishnan, R. Ramjee, and G. Varghese, "Endre: An end-system redundancy elimination service for enterprises," in NSDI, 2010, pp. 419– 432.

[3]. Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou "A Hybrid Cloud Approach for Secure Authorized Deduplication" IEEE, 2014.

[4]. Lei Yu, Haiying Shen, Karan Sapra, Lin Ye and Zhipeng Cai "CoRE: Cooperative End-to-End TrafficRedundancy Elimination for Reducing Cloud Bandwidth Cost" IEEE, 2016.

[5]. Swathi Kurunji, Tingjian Ge, Benyuan Liu, Cindy X. Chen "Communication Cost Optimization for Cloud Data Warehouse Queries" IEEE, 2012.

[6]. Lluis Pamies-Juarez, Pedro Garc a-L_opez, Marc S_anchez-Artigas, Blas Herrera, "Towards the Design of Optimal Data Redundancy Schemes for Heterogeneous Cloud Storage Infrastructures" Computer Networks, 2011.

[7]. A. Gupta, A. Akella, S. Seshan, S. Shenker, and J. Wang, "Understanding and exploiting network traffic redundancy" UWMadison, Madison, WI, USA, Tech. Rep. 1592, Apr. 2007.

[8]. Zhifeng Xiao and Yang Xiao, Senior Member, IEEE, "Security and Privacy in Cloud Computing", IEEE 2013.

[9]. S. Ihm, K. Park, and V. Pai. Wide-area Network Acceleration for the Developing World. 2010.

[10]. E. Zohar, I. Cidon, and O. O. Mokryn, "The power of prediction: cloud bandwidth and cost reduction," in ACM SIGCOMM, 2011, pp. 86–97.

[11]. N. T. Spring and D. Wetherall, "A protocol-independent technique for eliminating redundant network traffic," in ACM SIGCOMM, 2000, pp. 87–95.

[12]. A. Anand, C. Muthukrishnan, A. Akella, and R. Ramjee, "Redundancy in network traffic: findings and implications," in SIGMETRICS /Performance, 2009, pp. 37–48.

[13]. L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker. Web caching and zipf-like distributions: Evidence and implications. In IEEE Infocom, 1999.