PRIVACY PRESERVING CLOUD STORAGE BASED ON A THREE LAYER SECURITY MODEL

Ajith Chandrasekar I[1], Aniruth K[2], Arjun KV[3], Udaya B[4]

[1,2,3]Dept. of Computer Science Engineering, Rajalakshmi Institute of Technology, Tamilnadu, India
[4]Professor, Dept. of Computer Science Engineering, Rajalakshmi Institute of Technology, Tamilnadu, India

---***---

Abstract – *The development of cloud computing technology with the explosive growth of unstructured data, cloud storage technology gets extra attention and better development. The cloud provider does not have suggestions regarding the information and the cloud data stored and maintained globally anywhere in the cloud. The privacy protection schemes supported encoding technology. There are several privacy protective strategies within the aspect to forestall information in cloud. We tend to propose a three-layer storage security in cloud. The projected framework will each take full advantage of cloud storage and shield the privacy of knowledge. Here we designed to divide data into different parts . If the one information is missing we tend to lost the information. In this framework we tend to use bucket thought based mostly algorithms and secure the information then it will show the protection and potency in our theme. Moreover, supported process intelligence, this algorithmic program will reckon the distribution proportion keep in cloud, fog, and native machine.*

***Key Words*: Cloud Computing, Cloud Storage, Fog Computing, Privacy Protection, Cryptography.**

1. INTRODUCTION

With the rapid development of network bandwidth, the Volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. For more powerful storage capacity, a growing number of users select cloud storage. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together coordinately. Nowadays there are lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies provide large capacity of storage and various services related to other popular applications. However, cloud storage service still exists a lot of security problems. The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. User uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user do not actually control the physical storage of their data, which results in the separation of ownership and management of data. The CSP can freely access and search the data stored in the cloud. Meanwhile the attackers may also attack the CSP server to get the user's information. The on top of 2 cases each build users fell into the danger of information outflow and data loss.

Traditional secure cloud storage solutions for the above problems are usually focusing on access restrictions or data encryption. These methods can actually eliminate most part of these problems. However, all of these solutions cannot solve the internal attack well, no matter how the algorithm improves. Besides, depending on the property of the Hash-Solomon code, the scheme can ensure the original data cannot be recovered by partial data. On another hand, mistreatment Hash-Solomon code can turn out a little of redundant information blocks which can be utilized in decipherment procedure. Increasing the number of redundant blocks can increase the reliability of the storage, but it also results in additional data storage. By reasonable allocation of the data, our scheme can really protect the privacy of user's data. The Hash-Solomon code needs complex calculation, which can be assisted with the Computational Intelligence (CI). Paradigms of CI are with success employed in recent years to deal with varied challenges, as an example, the issues in Wireless detector networks (WSNs) field. CI provides adaptative mechanisms that exhibit intelligent behavior in advanced and dynamic environments like WSNs. Thus in our paper, we take advantage of CI to do some calculating works in the fog layer. Compared with traditional methods, our scheme can provide a higher privacy protection from interior, especially from the CSPs.

2. TECHNIQUES AND METHODS

2.1. Advanced Encryption Standard:

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack.

2.2. Operations:

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It contains of a series of joined operations, a number of that involve substitution inputs by specific outputs (substitutions) and involve shuffling bits around (permutations).

apparently, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are organized in 4 columns and 4 rows for process as a matrix. Unlike DES, the amount of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

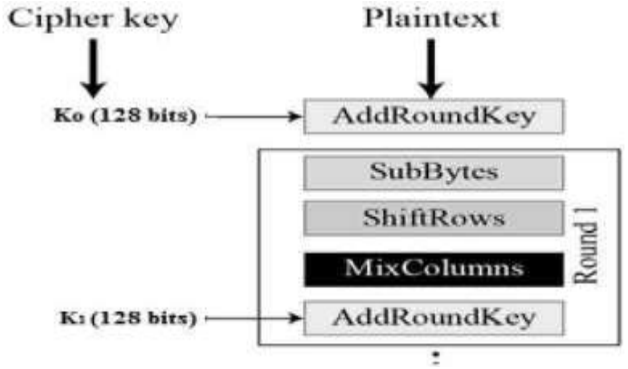

Fig -1: Advanced Encryption Standards

2.3. Triple Data Encryption Standards:

User first generates and distribute a 3TDES key K, which consists of 3 different key K1, K2 and K3.

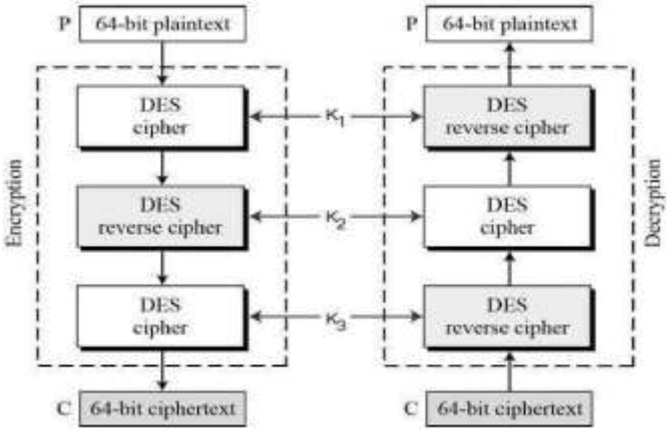

Fig -2: Triple DES

The encryption-decryption process is as follows

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES. Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Triple DES systems are significantly more secure than single DES.

2.4. MD5:

The MD5 hashing rule may be a unidirectional science operate that accepts a message of any length as input and returns as output a fixed-length digest worth to be used for authenticating the first message. The MD5 hash operate was originally designed to be used as a secure science hash rule for authenticating digital signatures. MD5 has been deprecated for uses apart from as a non-cryptographic confirmation to verify information integrity and sight unintentional information corruption. Although originally designed as a science message authentication code rule to be used on the web, MD5 hashing isn't any longer thought of reliable to be used as a science confirmation as a result of researchers have incontestible techniques capable of simply generating MD5 collisions on industrial ready-to-wear computers. The rule takes as input a message of capricious length and produces as output a 128-bit 'fingerprint' or 'message digest' of the input. it's conjectured that it's computationally impracticable to provide 2 messages having a similar message digest, or to provide any message having a given pre-specified target message digest. The MD5 rule is meant for digital signature applications, wherever an outsized file should be 'compressed' during a secure manner before being encrypted with a personal (secret) key underneath a public-key cryptosystem like RSA. The IETF suggests MD5 hashing will still be used for integrity protection, noting "Where the MD5 confirmation is employed inline with the protocol alone to safeguard against errors, associate MD5 confirmation continues to be a suitable use." However, it additional that "any application and protocol that employs MD5 for any purpose has to clearly state the expected security services from their use of MD5."

2.5. Security:

The goal of any message digest operate is to provide digests that seem to be random. To be thought-about cryptographically secure, the hash operate ought to meet 2 requirements: 1st, that it's not possible for associate degree wrongdoer to get a message matching a particular hash value; and second, that it's not possible for associate degree wrongdoer to form 2 messages that turn out a similar hash value.

2.6. Sha 256:

The SHA-2 family of cryptographic hash functions was first designed in 2001 by United States NSA and is patented under US patent 6829355. SHA-2 is an improved version of algorithm compared to the previous MD-5 or SHA-1. The SHA-2 set of algorithms consists of six hash functions with hash values of 224, 256, 384 or 512 bits, acknowledged as SHA-224, SHA-256, SHA-384, SHA-512/224, SHA512/256. The SHA-256 with 32-bits and SHA-512 with 64-bit are widely used hash functions. Although both of these hash functions have virtually identical basic structures but they differ in use of shift amounts, additive constants, and number of rounds. The generation of initial values using SHA-512/224 and SHA-512/256 are done according to the procedures described in Federal Information Processing Standards PUB 180-4. It is designed to function with enhanced security provided by the AES cipher. According to a report published in 2017, it was no longer recommended to use SHA-1 in applications that depend on collision resistance, such as digital signatures, as it was more prone to collisions than intended. But SHA-2 remained unbreakable against these attacks.

2.7. Applications:

SHA-2 hash functions are widely implemented in security applications and protocols such as SSL, TSL, PGP, S/MIME, SSH and IPsec. SHA-256 is used in DKIM message signing standard and authenticating Debian software packages. SHA512 was used to authenticate a video from International Criminal Tribunal of the Rwandan genocide. SHA-256 and SHA-512 are recommended to be used in DNSSEC, and are also used for secure password hashing in Unix and Linux. SHA-256 is used for verifying transactions and calculating proof-of stake in several crypto-currencies like Bitcoin. SHA-2 is extensively used in cryptographic algorithms and protocols, and for protection of sensitive unclassified data by the U.S. Government.

2.8. METHODOLOGY

Fog computing is an extended computing model based on cloud computing which is composed of a lot of fog nodes. These nodes have a certain storage capacity and processing capability. In our scheme, we split user's data into three parts and separately save them in the cloud server, the fog server and the user's local machine.

3. RELATED WORKS:

3.1. A Model for Preserving cloud computing Privacy:

The widespread target the Cloud Computing has necessitated the corresponding mechanisms to make sure privacy and security. Varied makes an attempt are created within the past to safeguard the privacy of the individual or agency attempting to utilize the services being provided by the cloud. The foremost difficult task is to produce services to the users whereas additionally protective the privacy of the user's data. during this paper a model that includes a three level design, protective cloud computing Privacy (PccP) model is projected that aims to preserve privacy of knowledge bearing on cloud storage.

3.2. Data Privacy Preserving Mechanism Based on Tenant Customization for SaaS:

As a newly software delivery model, software as a service, SaaS for short, is the best way for small and medium enterprise to adopt the newly technology. However trustworthiness is greatest challenge in the wide acceptance of SaaS. In the absence of trustworthiness in SaaS applications, data privacy is the primary and the most important issue for tenants. How to protect the data privacy when software service and database are both hosted the service provider's client is still an open issue.

3.3. On the Design and Analysis of the Privacy Preserving SVM Classifier:

The support vector machine (SVM) is a widely used tool in classification problems. The SVM trains a classifier by solving an optimization problem to decide which instances of the training data set are support vectors, which are the necessarily informative instances to form the SVM classifier. Since support vectors are intact tuples taken from the training data set, releasing the SVM classifier for public use or shipping the SVM classifier to clients will disclose the private.

3.4. A Survey on the Privacy-Preserving Data Aggregation in Wireless Sensor Networks:

Wireless sensor networks (WSNs) consist of a great deal of sensor nodes with limited power, computation, storage, sensing and communication capabilities. Data aggregation is a very important technique, which is designed to substantially reduce the communication overhead and energy expenditure of sensor node during the process of data collection in a WSNs. However, privacy-preservation is more challenging especially in data aggregation need to perform some aggregation.

3.5. Efficient Multi-Party Privacy Preserving Data Mining For Vertically Partitioned Data:

The data in computational domain stored in digital format. This format of data, consumes less effort and storage. Thus a number of organization and institutes are preserving their information in this format. In this presented work the data and their privacy is the main area of study. In the proposed work an organization is considered where the decisions are made with the different department based data and their attributes. Additionally to make decisions the attributes of all the departments are required. But the departments are not able to disclose the privacy of data owner.

3.6. Toward Privacy-Assured and Searchable Cloud Data Storage Services:

Cloud computing is envisioned as the next generation architecture of IT enterprises, providing convenient remote access to massively scalable data storage and application services. While this outsourced storage and computing paradigm can potentially bring great economical savings for data owners and users, its benefits may not be fully realized due to wide concerns of data owners that their private data may be involuntarily exposed or handled by cloud providers. Although end-to-end encryption techniques have been proposed as promising solutions for secure cloud data storage, a primary challenge toward building a full-fledged cloud data service remains: how to effectively support flexible data utilization services such as search over the data in a privacy-preserving manner. In this article, we identify the system requirements and challenges toward achieving privacy-assured searchable outsourced cloud data services, especially, how to design usable and practically efficient search schemes for encrypted cloud storage. We present a general methodology for this using searchable encryption techniques, which allows encrypted data to be searched by users without leaking information about the data itself and users¿ queries. In particular, we discuss three desirable functionalities of usable search operations: supporting result ranking, similarity search, and search over structured data. For each of them, we describe approaches to design efficient privacy-assured searchable encryption schemes, which are based on several recent symmetric-key encryption primitives. We analyze their advantages and limitations, and outline the future challenges that need to be solved to make such secure searchable cloud data service a reality.

3.7. Cooperative Fog-Cloud Computing Enhanced by Full-Duplex Communications:

Full-duplex (FD)-fog nodes with wireless backhaul can improve the flexibility of deployment for 5G ultra density networks. However, under computation-intensive environments, the insufficient computing resource of fog nodes leads to the increase of backhaul for cloud computing. In this letter, we introduce in-band full-duplex communications to cooperatively integrate the fog computing and cloud computing. By considering the statistical variation of the computation delay caused by co-located and concurrent workload, we construct an M/M/1 queuing to model the computing delay. We comprehensively analyze the outage performance for both the communication and the computing procedure, which is close to actual systems. Moreover, ergodic computation rate is proposed to investigate the computation capability of the FD-fog computing systems. Simulations results verify the accuracy of our analysis, and the cooperative fog-cloud computing framework outperforms the existing fog computing system.

4. SECURE CLOUD STORAGE BASED ON FOG COMPUTING

The security degree is an important metric to measure the quality of cloud storage system. Furthermore, data security is the most important part in cloud storage security and it includes three aspects: data privacy, data integrity and data availability. Ensuring data privacy and integrity has always been the focus of relevant researches. On another hand, data privacy is also the most concerned part of the users. From a business perspective, company with high security degree will attract more users. Therefore improving security is an crucial goal no matter in academia or business. In this section, we will detailedly elaborate how the Transport Layer Security framework protects the data privacy, the implementation details of work flow and the theoretical safety and efficiency analysis of the storage scheme.

4.1. Fog Computing

Our scheme is based on fog computing model, which is an extension of cloud computing. Fog computing was firstly proposed by Ciscos Bonomi in 2011.In Bonomi's view, fog computing is similar to the cloud computing, the name of fog computing is very vivid. Compared to highly concentrated cloud computing, fog computing is closer to edge network and has many advantages as follows: broader geographical distributions, higher real-time and lowlatency. In considering of these characters, fog computing is more suitable to the applications which are sensitive to delay. On another hand, compared to sensor nodes, fog computing nodes have a certain storage capacity and data processing capability, which can do some simple data processing, especially those applications based on geographical location. Thus we can deploy CI on the fog server to do some calculating works. Fog computing is usually a three-level architecture, the upmost is cloud computing layer which has powerful storage capacity and compute capability. The next level is fog computing layer. The fog computing layer serves as the middle layer of the fog computing model and plays a crucial role in transmission between cloud computing layer and sensor network layer. The fog nodes in fog computing layer has a certain storage capacity and compute capability. The bottom is wireless sensor network layer. The main work of this layer is collecting data and uploading it to the fog server. Besides, the transfer rate between fog computing layer and other layers is faster than the rate directly between cloud layer and the bottom layer. The introduction of fog computing can relief the cloud computing layer, improving the work efficiency. In our scheme, we take advantage of the fog computing model, adopt three-layer structure. Furthermore, we replace the WSNs layer by user's local machine.

5. Three-Layer Privacy Preserving Cloud Storage Scheme

The framework can take full of cloud storage and protect the privacy of data. Here the cloud computing has attracted great attention from different sector of society. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms. In our system we using a bucket concept so reduce the data wastages and reduce the process timings. We are using a BCH (Bose–Chaudhuri–Hocquenghem) code algorithm. It's High flexible. BCH code are used in many communications application and low amount of redundancy. The Bucket Access manage resource represents the Access Control Lists (ACLs) for buckets inside Google Cloud Storage. ACLs let you specify who has access to your data and to what extent. The three layer cloud storage stores into the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.

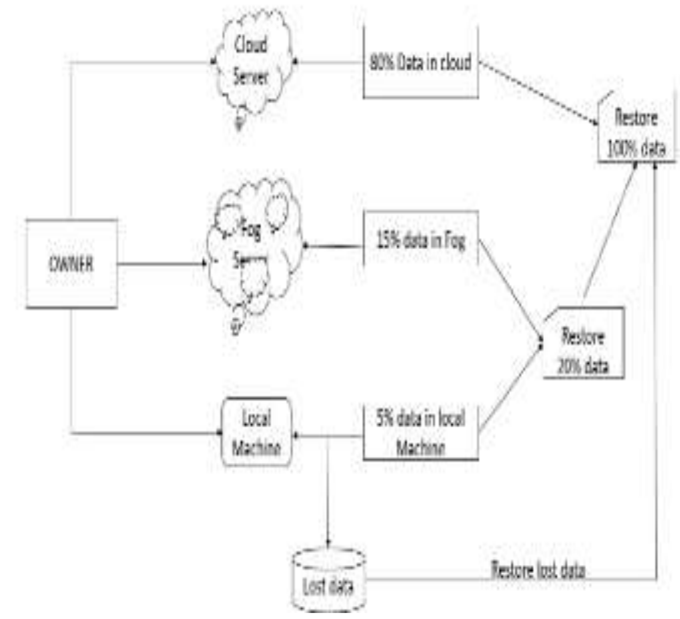

Fig -3:System Architecture

6. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to resolve the matter of privacy protection in cloud storage, we have a tendency to propose a three layer privacy protective secure cloud storage methodology framework supported fog computing model and style. By allocating the magnitude relation of knowledge blocks keep in several servers fairly, we will make sure the privacy of knowledge in every server. On another hand, cracking the encryption matrix is not possible in theory. Besides, using hash transformation will shield the fractional info. Through the experiment take a look at, this theme will efficiently complete encryption and coding while not influence of the cloud storage efficiency.

REFERENCES

[1] J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloud assisted urban data sharing framework for ubiquitous cities,Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.3.013

[2] Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., & Zhang, Z. (2018). Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2018.2793350

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[5] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014,pp. 2969–2974.

[6] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7,pp. 1397–1409, 2014.

[7] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016,pp. 130–143.

[8] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[9] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[10] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[11] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," IEEE Commun. Surv. Tuts.,vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[12] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,pp.2594–2608, Nov. 2016.

[13] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Comput., vol. 41, pp. 219–230, 2017.

[14] Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884,Aug. 2017.

[15] J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.

[16] Q. Hou, Y. Wu, W. Zheng, and G. Yang, "A method on protection of user data privacy in cloud storage platform," J. Comput. Res. Develop., vol. 48, no. 7, pp. 1146–1154, 2011.

[17] P. Barham et al., "Xen and the art of virtualization," ACM SIGOPS Oper.Syst. Rev., vol. 37, no. 5, pp. 164–177, 2003.

[18] G. Feng, "A data privacy protection scheme of cloud storage," vol. 14, no. 12, pp. 174–176, 2015.Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Trans. Inf. Forensics Security, vol. 11, no. 12, pp. 2706–2716, Dec. 2016.