IMPLEMENTATION OF THRESHOLD BASED CRYPTOGRAPHIC TECHNIQUE OVER CLOUD COMPUTING FOR DATA AND KEY STORAGE SECURITY

M/S. Paurnima Ghugarkar 1, Prof.H.B.Jadhav2

[1]*Student, Dept. of Computer Engineering, VACOE, Ahmednagar, Maharashtra, India*
[2]*Professor, Dept. of Computer Engineering, VACOE, Ahmednagar, Maharashtra, India*

---***---

Abstract - *The Cloud domain is increasingly rapidly and being used to store and process big data. Due to the volume and complexity, outsourcing ciphertexts to a cloud is deemed to be one of the most effective approaches for big data storage and access. However, checking and verifying the access legitimacy or reality of a user and securely updating a ciphertext in the cloud based on a new access policy designated by the data owner are two major critical challenges to make cloud-based big data storage effective and practical. Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities. In this system, counter against cheating behaviors of the cloud and also enables (i) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (ii) a user to validate the information provided by other users for correct plaintext recovery. The implementation results depict that this system can prevent CSP from any data attack and safe eligible users from cheating and resist various attacks such as the collusion attack.*

***Key Words*: Client/server, Distributed applications, Distributed file system, Distributed databases, etc.**

1. INTRODUCTION

In computing, Data Security is a specialized data compression technique for eliminating unauthorized copies of repeating data. Related and somewhat synonymous terms are intelligent (data) compression and single-instance (data) storage. This technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. In the Security process, unique chunks of data, or byte patterns, are identified and stored during a process of analysis. As the analysis continues, other chunks are compared to the stored copy and whenever a match occurs, the redundant chunk is replaced with a small reference that points to the stored chunk. Given that the same byte pattern may occur dozens, hundreds, or even thousands of times (the match frequency is dependent on the chunk size), the amount of data that must be stored or transferred can be greatly reduced.

A Hybrid Cloud is a combined form of private clouds and public clouds in which some critical data resides in the enterprise's private cloud while other data is stored in and accessible from a public cloud. Hybrid clouds seek to deliver the advantages of scalability, reliability, rapid deployment and potential cost savings of public clouds with the security and increased control and management of private clouds. As cloud computing becomes famous, an increasing amount of data is being stored in the cloud and used by users with specified privileges, which define the access rights of the stored data. The critical challenge of cloud storage or cloud computing is the management of the continuously increasing volume of data. Architecture of cloud computing shown in figure 1. Data Security [3], [4] or Single Instancing essentially refers to the elimination of redundant data. In the Security process, unauthorized data is deleted, leaving only one copy (single instance) of the data to be stored. However, indexing of all data is still retained should that data ever be required. In general, the Data Security eliminates the unauthorized copies of repeating data. This encryption requires more time and space requirements to encode data. In case of large data storage, the encryption becomes even more complex and critical. By using the Data Security inside a hybrid cloud, the encryption will become simpler.

To avoid this duplication of data and to maintain the confidentiality in the cloud we using the concept of Hybrid cloud. It is a combination of public and private cloud. Hybrid cloud storage combines the advantages of scalability, reliability, rapid deployment and potential cost savings of public cloud storage with the security and full control of private cloud storage.

2. LITERATURE SURVEY

2.1 "Secure and Efficient Data Communication Protocol for Wireless Body Area Networks"

Wireless Body Area Networks (WBANs) are expected to play a major role in the field of patient-health monitoring in the near future, which gains tremendous attention amongst researchers in recent years. One of the challenges is to establish a secure communication architecture between sensors and users, whilst addressing the prevalent security and privacy concerns. In this system, we propose a communication architecture for BANs, and design a scheme to secure the data communications between implanted /wearable sensors and the data sink/data consumers (doctors or nurse) by employing Ciphertext-Policy Attribute Based Encryption (CP ABE) [1] and signature to store the data in ciphertext format at the data sink, hence ensuring data security. Our scheme achieves a role-based access control by employing an access control tree defined by the attributes of the data. We also design two protocols to securely retrieve the sensitive data from a BAN and instruct the sensors in a BAN. We analyze the proposed scheme and argue that it provides message authenticity and collusion resistance and is efficient and feasible. We also evaluate its performance in terms of energy consumption and communication/computation

Advantages:

1. This system provides message authenticity and collusion resistance and is efficient and feasible.

2. It achieves a role-based access control by employing an access control tree defined by the attributes of the data.

Disadvantages:

1. This system does not allow user verifiability based on access mechanism and therefore chances of unauthorized data access are more.

2.2 "Security and Privacy for Storage and Computation in Cloud Computing"

The Secure Data Sharing in Clouds (SeDaSC) methodology that provides: data confidentiality and integrity, access control, data sharing (forwarding) without using compute-intensive re-encryption, insider threat security, and forward and backward access control. The Secure Data Sharing in Clouds methodology encrypts a file with only a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats and the other key share is stored by a trusted and believable third party, which is called the cryptographic server. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations.

2.3. "Expanded Top Ten Big Data Security and Privacy Challenges"

Security and privacy issues are magnified by the velocity, volume, and variety of Big Data, such as large-scale cloud infrastructures, diversity of data sources and formats, streaming nature of data acquisition and high volume inter-cloud migration. There- fore, traditional security mechanisms, which are tailored to securing small-scale, static (as opposed to streaming) data, are inadequate. In this system, we highlight the top ten Big Data security and privacy challenges. Highlighting the challenges will motivate increased focus on fortifying Big Data infrastructures.

2.4 "Review Paper on Clustering Based Collaborative Filtering"

Big Data concerns large-volume, complex, growing data sets with multiple, autonomous sources. In Big Data applications data collection has grown tremendously and it is beyond the ability of commonly used software to capture, manage, and process that data. The most fundamental challenge for the Big Data applications is to explore the large volumes of data and extract useful information or knowledge for future actions. Recommender systems (RSs) are techniques and intelligent applications to assist users in a decision-making process where they want to choose some items among set of alternative products or services. RSs encounter two main challenges for big data application:

1) To make decision within acceptable time.

2) To generate ideal recommendations from so many services.

This system reports review on collaborative filtering which uses clustering algorithms. Nowadays Service relevant data become too big to be effectively processed by traditional approaches, so one solution to this challenge is Clustering Based Collaborative Filtering. This approach recruits similar services in the same cluster to recommend services collaboratively.

3. PROPOSED SYSTEM

3.1 System Architecture

The proposed system is a modified version of the existing system which addresses major issues such as Brute force attack or collusion attack. The cloud service providers are always considered to be dishonest and therefore files on cloud are encrypted. But If the CSP makes and attack on the encrypted files too, he can somehow get the sensitive data of users and compromise the user privacy. So the proposed system efficiently analyses this issue and proposes a system that will maintain security from unauthorized users as well as dishonest CSPs. Files stored on the cloud are not the whole, instead files are divided into threshold number of pieces (threshold i.e. count is decided by users), and each piece is encrypted and store don separate CSP such that none of the CSP has the idea whether the file is a complete file or a piece of file.

The proposed system can be widely made operational on university clouds in order to store the sorted questions of question papers and thereby avoid question paper leaks.

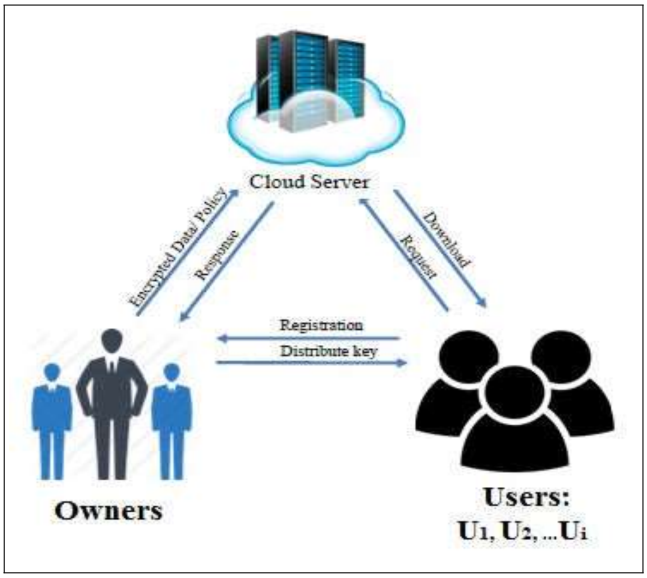

Fig -1: Architecture of Proposed System

3.2 ALGORITHM

1. AES ENCRYPTION ALGORITHM- FOR ENCRYPTING FILES

2. CHUNKING ALGORITHM- FOR DIVIDING FILES INTO PIECES

Step 1: select a file to upload

Step 2: Read the file into buffer reader.

Step 3: For all the data in the buffer reader

Step 4: Read each line till n size is detected.

Step 5: Consider the data till nth byte as a chunk

Step 6: While all the data is read select data till every 10nth byte as a chunk.

Step 7: Encrypt each chunk (piece) with the AES encryption algorithm and upload on different CSP.

Step 8: Send the decryption key to the authorized user on data request.

4. MATHEMATICAL MODEL

4.1 Set Theory

A set is defined as a collection of distinct objects of same type on class of objects. The object of a set are called elements or members of the set. Object can be number, alphabet, names etc.

Example: A = (1, 2, 3, 4, 5)

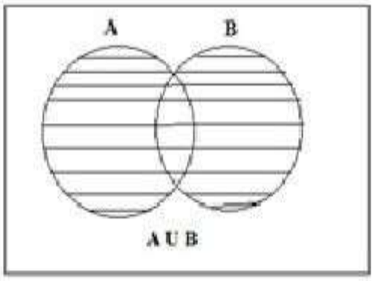

Fig -2: Union of Set

Union of two sets A and B is defined to be the set of all those elements which belongs to set A or set B or both and is denoted by A U B.

User Authentication:

Set (C) = {c0,c1,c2,c3}

C0= Get User Id

C1= Get Cloud Id

C2= Get Data Owner Info

C3= Get the User Privilege Information

C4= Get Key from Hash Table

Data Security

Set (T) = {c1,c2,d0,d1,d2}

d0= Get Data File Name.

d1= Data accessing user id.

d2= Get Cloud id

Union and Intersection of project

Set (P) = {c0,c1,c2,c3 }

Set (t) = {c1,c2,c3,d0,d1,d2}

5. ADVANTAGES

1. The security in terms of CSP is achieved as the CSP does not know which user stores or divides the file in how many chunks.

2. The security in terms of attacker users is achieved as the key is not stored completely, instead its divided into pieces and the access levels are checked before file access.

6. RESULT AND PERFORMANCE ANALYSIS

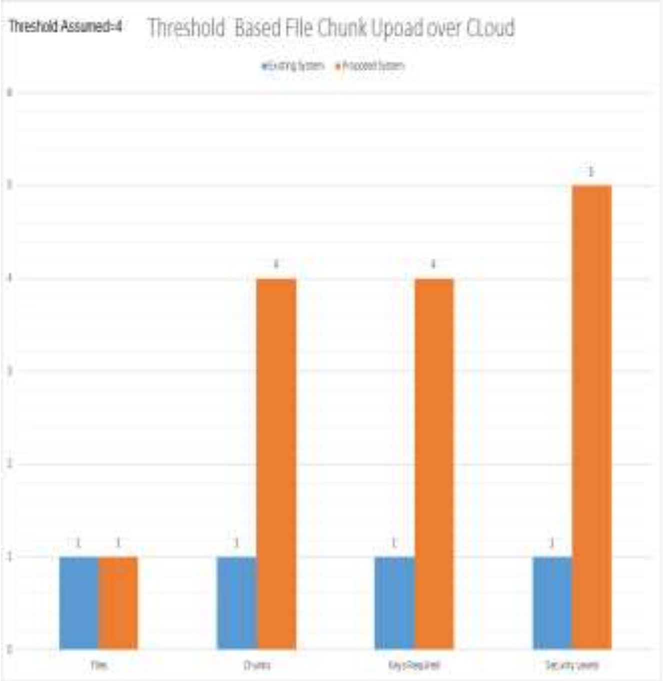

Fig -3: Performance Analysis

7. CONCLUSIONS

In this paper it is analyzed the notion of authorized Data Security is proposed to protect the data security by including differential privileges of users in the unauthorized check. It also presented several new duplication constructions supporting authorized unauthorized check in hybrid cloud architecture, in which unauthorized check is done and token of files are generated by private cloud server with private keys. The designing shows that how the actual flow of this project. Its constraints on designing of methods to achieve changeover and evaluation of change over methods.

In this proposed system provide the secure Security with the help of token generation, Secure upload/download of data and Authorized Data Security is proposed to protect the data security. Differential privileges of users in the unauthorized check are also provided. This technique more useful and accurate technique for Data Security. The current system is 98 Percent better than existing system.

ACKNOWLEDGEMENT

All faith and honor to the HOD for his grace and inspiration.

I would like to thank all my Friends and Family members They were always been there to support me. I sincerely thanks to my Department Head, PG coordinator and all other staff members to give me the guidelines for this paper.

REFERENCES

[1] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, “Secure and efficient data communication protocol for wireless body area networks,” IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94–107, 2016.

[2] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, “An attribute based signcryption scheme to secure attribute-defined multicast communications,” in Secure Comm 2015. Springer, 2015, pp. 418–435

[3] C. Hu, X. Liao, and X. Cheng, “Verifiable multi-secret sharing based on LFSR sequences,” Theoretical Computer Science, vol. 445, 2012.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” Public Key Cryptography–PKC 2011, pp. 53–70, 2011.

[5] Cheng Hongbing 1,2, Rong Chunming 3, Hwa ng Kai 4, Wang Weihong 1, LI Yanyan 1, ”Secure Big Data Storage and Sharing Scheme for Cloud Tenants ” China Communications June 2015.

[6] SHUI YU, ”Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data”, Digital Object Identifier 10.1109/ACCESS.2016.2577036.

[7] Chunqiang Hu, Hongjuan Li, Xiuzhen Cheng, Xiaofeng Liao, ”Secure and Ef- ficient data communication protocol for Wireless Body Area Networks, IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS, VOL. , NO. , 11. 2015.

[8] Z. Eslami and J. Z. Ahmadabadi, ”A verifiable multi-secret sharing scheme based on cellular automata,” Information Sciences, vol. 180, no. 15, pp. 28892894, 2010.

[9] Sheetal Thokal and Vrunda Bhusari, ” Review Paper on Clustering Based Col- laborative Filtering, Volume 2, Issue 11, November 2014, International Journal of Advance Research in Computer science and management studies.

[10] M. A. Beyer and D. Laney, ”The importance of big data: a definition,” Stamford, CT: Gartner, 2012.