Secure File Sharing On Cloud Using Cellular Automata Based Encryption

Mrs.D.Thamizhisai[1], Abarna.V[2], Charumathy.K[3], Monisha.S[4]
[1, 2, 3, 4]RAAK COLLEGE OF ENGINEERING AND TECHNOLOGY, PUDUCHERRY

Abstract- *Data Lake was architected from the ground up for cloud scale and performance. With Azure Data Lake Store any organization can analyse all of its data in a single place with no artificial constraints. The Data Lake Store can store trillions of files where a single file can be greater than a petabyte in size which is 200x larger than other cloud stores. This means there is no need to rewrite code as there is increase or decrease of the size of the data stored or the amount of compute being spun up. Data Lake also takes away the complexities normally associated with big data in the cloud, ensuring that it can meet your current and future business needs.*

In this project we are creating the azure account to use the data lake and were, we are storing the data in the data lake. Data Lake can store data of any type. And we are using the Cellular Automaton encryption algorithm and PSEUDO-RANDOM NUMBER GENERATOR (PRN) to solve the problem in the existing system and this algorithm verifiable file search problem and develop protocols to enable verifiable file search for enterprise-scale cloud storage applications. And, alsowe are propose a multiple key based-secure key encryption scheme with low overhead cipher texts and aggregate keys. which can flexibly extend the number of participants in associate degree passing cloud surroundings the structure of the Group style.

This protocol is applied in cloud computing to support secure and economical information sharing. The data can also be deleted if the user don't need the data or in case of change is systems.

Keywords- PSEUDO-RANDOM NUMBER GENERATOR (PRN) ,Data outsourcing, searchable encryption, SSE, verification,

I. INTRODUCTION

Nowadays, millions of websites are hosted on the web in the Internet era. A stack of servers is needed to maintain the hosted site, which is very costly. The servers' traffic rates must be steady and must be regularly checked and maintained. Need to hire more people to organize and maintain the servers. All of the data will be stored in data centres. As a result, continual attempts to maintain the server issue and the workers may detract from our ability to meet our business objectives using "Cloud Computing" to prevent time-consuming upkeep.

"Cloud computing is a practice of employing a network of remote servers to store, manage, and process data from anywhere within the world." it's utilized in place of a local server or a personal computer. The service like storing data and applications is delivered to the organization's devices through the internet. Cloud computing provides many benefits through the services combining the data centers, resources, and servers through the internet. Cloud Services are based on pay-per-use regulations. The services are accessible from anywhere in the world at a greatly reduced cost, allowing employees to collaborate more effectively.

II. EXISTING METHODS

We aim to develop an Efficient, Secure, Verifiable Symmetric Searchable Encryption scheme (ESVSSE). The data owner uploads the encrypted documents, authenticator and the security index using the B+-Tree to the cloud server. This scheme allows the user to verify the integrity and freshness of the search results. Our ESVSSE scheme is defined as follows: ESVSSE is a three-party model where data owners store secure indexes, authenticators, and encrypted documents on the cloud server. The data owner can authorize users to query the cloud servers. The authorization procedure is similar to. The cloud server provide storage and search capabilities. Authorized users can initiate query and verification operations.

Cellular Automation Algorithm:

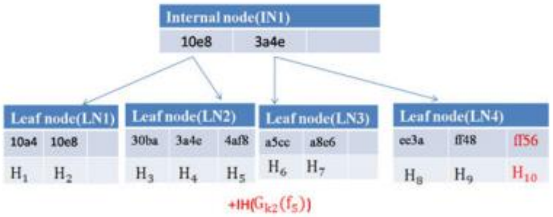
A discrete parallel computation model built of a finite array of n cells is known as one dimensional cellular automation. In a discrete amount of time (t), each cell communicates with its neighbors. Each center cell x updates its state s12 {0, 1} by applying a local ruleand a radius(r1). For radius r1, the neighborhood consists of a total of 2*r1+1 numbers of**:**

Gen (1k) →{K1; K2; K3;(ssk; spk)}: is a probabilistic algorithm that takes as input a security parameter k and outputs private keys K1; K2; K3, and a random signing key pair (ssk, spk) and it is executed by the data owner.

Init(K1; K2; K3; ssk; D) → {I; p; pbf ; C }: is an algorithm executed by the data owner. It takes as input the secret keys K1; K2; K3, the signing private key ssk, and the document set D, and outputs the secure index I, encrypted documents C, the authenticator p and the authenticator of Counting Bloom Filter pbf . The pbf is an authenticator, which can provide proof when the keyword queried by the user does not exist. The data owner stores the I and pbf locally and meanwhile sends I, C, p, and pbf to the cloud server. PreUpdateðK1; K2; K3; ssk; pbf t; p; pbfg: is an algorithm that takes as private keys K1; K2; K3, and the signing private key ssk, and the file f to be updated, and outputs the update tokens tv and the authenticator p. The data owner runs the algorithm and sends tv, pbf , and authenticator p to the cloud server.

SECURITY ANALYSIS:

In this section, we will conduct a security analysis for our scheme. On the one hand, we should analyse the security and confidentiality of data on the cloud servers. On the other hand, we also make sure that users authorized by the data owner can verify the search results correctly. Confidentiality means that an attacker cannot learn any useful information



Pseudo Random NumberGenerator(PRNG):

PRNG an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers. A PRNG starts from an arbitrary starting state using a seed state. Many numbers are generated in a short time and can also be reproduced later, if the starting point in the sequence is known. Hence, the numbers are deterministic and efficient.

$$\mathbf{X_n}+1 = (aXn + c) \bmod m$$

where X is the sequence of pseudo-random values

m, $0 < m$ - modulus

a, $0 < a < m$ - multiplier

c, $0 \leq c < m$ - increment

x0, $0 \leq x0 < m$ - the seed or start value

III. PROPOSED SYSTEM

We propose a multiple key based-secure key encryption scheme with low overhead cipher texts and aggregate keys. We demonstrate how the multiple key framework may be efficiently extended and combined with broadcast encryption schemes for distributing the aggregate key among receiver data users in a real-life data sharing environment.In this project, we formalize the Cellular Automata based encryption with verifiable file search problem and develop protocols to enable verifiable file search for enterprise-scale cloud storage applications. The proposed protocols also protect the privacy of filenames. In addition, the proposed protocols are provably secure under malicious clouds. And we are using the Pseudo Random Number Generator to generate the key for the decryption.

OUR PROPOSED PROTOCOLS HAVE TWO KEY FEATURES:

They enable a cloud storage user to verify the correctness of a search result when searching for a file on the cloud;

They enable different users with different security privileges to only access data with the matching and appropriate security level, i.e., they support access control inherently.

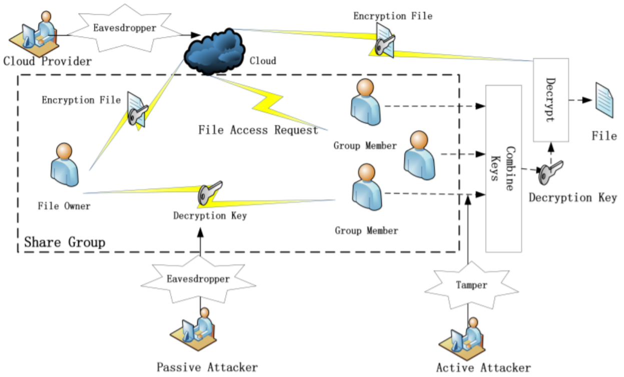
ADVANTAGE OF THE CELLULAR AUTOMATA:

Truly equal peers: decentralized, no dependency on seed or core nodes

Simple rules: easy to implement, simpler code, less errors, consume less resource so potentially working on billions of mobile devices.

Native parallel processing: highly scalable Dynamic: network topology can evolve with a touch of randomness, difficult to detect network traffic pattern, more resistant to attacks
Decentralized: local decision, global impact
Open and expandable

IV. SYSTEM ARCHITECTURE



V. CONCLUSION

In this paper we are using the **CELLULAR AUTOMATA (CA)** algorithm for the encryption file once the file is stored in the azure the searching of the file will be impossible and the is solved using the CA. and the **PSEUDO-RANDOM NUMBER GENERATOR (PRN)** for the random key generation and this key will be useful in the decryption of the stored file and hence random key generated every time is difficult for the hacker to hack the file. And, the proposed protocols are provably secure under malicious clouds.

VI. FUTURE ENHANCEMENT

As the future enhancement we can use any other security based algorithm to improve security in the cloud and then we can combine it with the deep learning algorithm the data separation.

REFERENCES

[1] B. Waters . J. Bethencourt, and A. Sahai, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Secur. Privacy, 2007, vol. 10, pp. 321–334.

[2] Tadjer, “What is cloud computing,” ACM, vol. 51, pp. 9–11, 2011.

[3] A. K. Iyengar, “Enhanced clients for data stores and cloud services,” IEEE Trans. Knowl. Data Eng., vol. 31, no. 10, pp. 1969–1983, Oct. 2019.

[4] X. Ge, Y. Wang, J. Fu, J. Wu, and L. Ping, “Cloud storage as the infrastructure of cloud computing,” in Proc. IEEE Int. Conf. Intell. Comput. Cogn. Informat., 2010, pp. 380–383.

[5] L. Weng, L. Amsaleg, and T. Furon, “Privacy-preserving outsourced media search,” IEEE Trans. Knowl. Data Eng., vol. 28, no. 10, pp. 2738–2751, Oct. 2016.

[6] S. Kamara, C. Papamanthou, and T. Roeder, “CS2: A searchable cryptographic cloud storage system,” Microsoft Technical Report, pp. 380–383, 2011.

[7] K. Ren, B. Zhang, R. Xie, K. Yang, and X. Jia, “Effective data access control for multi-authority cloud storage systems,” IEEE Trans.

[8] L. M. Gupta, K. A. Nielsen, M. G. Borlick, and L. M. Gupta, “Method, system, and computed program product for distributed storage of data in a heterogeneous cloud,” Int. Bus. Machines Corporation, vol. 10, 2019, Art. no. 171.

[9] H. Ancin, X. Chen, A. Jassal, D. H. Jung, G. B. Neustaetter, and S. H. Puttergill, “Systems and method for facilitating access to private files using a cloud storage system,” U.S. Patent 9251114, Feb.2016.

[10] K. Lauter and S. Kamara, “Cryptographic cloud storage,” in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2010, pp. 136–149.

[11] K. Kurosawa and Y. Ohtaki, “UC-secure searchable symmetric encryption,” in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2012, pp. 285–298.

[12] K. Kurosawa and Y. Ohtaki, “How to update documents verifiably in searchable symmetric encryption,” in Proc. Int. Conf. Cryptology Netw. Secur., 2013, pp. 309–328.

[13] C. Papamanthou, E. Stefanov, and E. Shi, “Practical dynamic searchable encryption with small leakage,” in Proc. Netw. Distrib. Syst. Secur. Symp., 2014, pp. 23–26.