Client-Centric Proxy Re-Encryption for Outsourced Data in the Cloud

Mr. M. Sathyanarayanan, M. E, (*Author*)
Assistant Professor,
Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India.

Mr. S. DineshKumar, B. Tech.,
Student, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India.

Mr. N. Tamilarasu, B .Tech.,
Student, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India.

Mr. R. Yasvanth, B. Tech.,
Student, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India.

Abstract*—In this paper, we introduce a new cryptographic primitive, called autonomous path proxy re-encryption (APPRE), which is motivated by several application scenarios where the delegator would like to control the whole delegation path in a multi-hop delegation process. Compared with traditional encryption, it provides much better fine-grained access control to the delegation path. Briefly speaking, the delegator designates a path of his preferred delegates. The delegation, for ciphertexts of a delegator, can only be carried out on the autonomous path designated by the delegator, in the sense that re-encrypted cipher texts along the autonomous path cannot branch off with meaningful decryption, and original ciphertexts generated a path differently and cannot be inserted into (i.e., cannot be transformed along) the autonomous path with meaningful decryption. We give the formal definition, as well as the formal security model, for this cryptographic primitive. Under this concept, we construct double masking and blockchain to secure the files that have been generated to the server. Our scheme is with the useful properties of proxy re-encryption, i.e., uni-directionality and multi-hop. Data sharing is a depriving user's direct control over the outsourced data, which inevitably raises security concerns and challenges. Client-Centric Proxy Re-Encryption scheme gives a concrete solution for secure data sharing in which deprives user's direct control over the outsourced data. Enriches data privacy and confidentiality with highly grained access and prevents user data from third-party access. Increases privacy and confidentiality by providing a double masking technique to the user files that are stored distributed. Highly enhances user data with a double masking technique that encrypts data in a bidirectional manner. With double masking, data that has been stored in CSP will be highly confidential, where zero knowledge about files has been provided to CSP. Along with that blockchain, the mechanism has been proposed to prevent data from anomaly attacks. In addition to blockchain periodically verifies user data to maintain trust management of every file in the system.

Key words-- Encrytion, cloud providers, Decryption, key generation center, proxy re-encryption, ip address.

I. INTRODUCTION

When one is too busy to interpose with all his encrypted files, he may wish to delegate his decryption rights to someone he trusts. This delegation of the power to decrypt the cipher text can be easily done if the delegator is online – simply decrypts the cipher text and re-encrypts the plaintext with the public key of whom he trusts. However, this is not always real, for the delegator may not be online all the time. And, it is undesirable to just disclose the secret key to some untrusted server to do the transformation of the cipher text. To solve the above mentioned problems. Firstly proposed the concept of proxy re-encryption (PRE). In a PRE scheme, a semi-trusted proxy with some additional information (re-encryption key, which is computed by the delegator in advance) can convert a cipher text computed under Alice's (delegator's) public-key into one intended to Bob (delegatee) with the same plaintext. If the cipher text can be transformed more than one time, For example, if a delegate happens to be very busy, or just cannot be online when he receives a re-encrypted cipher text from his delegator, he would like to delegate his decryption rights to other delegatees. If the PRE scheme is single hop, then the delegate cannot transform the re-encrypted file furthermore. The multi-hop property of a PRE scheme is described. We note that, the delegator with public key pk0 designates his delegatee pk1. The delegatee pk1 designates his own delegatee pk2. There is maybe no relationship between pk0 and pk2, since no restrictions are specified when pk1 selects his delegatee. The delegator may want to designate another delegatee by himself if his delegatee pk1 is unable to decrypt the ciphertext. In order to meet the above discussed applications, in this work we introduce a new cryptographic primitive, called autonomous path proxy re-encryption (AP-PRE). Briefly speaking, in an AP-PRE scheme, the delegator designates a path of his preferred delegates. The path consists of several delegates with the privilege from high to low. The delegation, for cipher texts of a delegator i, can only be carried out on the self and own path Pai designated by the delegator i, in the sense that re-encrypted cipher texts along the autonomous path Pai cannot branch off Pai with meaningful decryption, and original cipher texts generated under pkj for j≠ i (i.e., for a path Paj different from Pai) cannot be updated into (i.e., cannot be formed along) the autonomous path Pai with useful decryption. Under this concept, we construct an IND-CPA secure AP-PRE scheme under the decisional bilinear Diffie-Hellman

(DBDH) assumption in the random oracle (RO) model. The re-encryption key is used for the proxy to transform the re-encrypted ciphertext under one of his delegatee's public key to another delegate, while the delegator actually does not know the private key of any of his delegates.

II.EXISTING SYSTEM

Type Based PRE provides semantic protection and cipher-text privacy control. But in the other way encoding operations over encrypted messages is not possible limiting in its overall use. Key-Private PRE provides security against cipher-text attack but privacy proof of this scheme is more difficult than plaintext attack. Identity-based PRE is secure against an adaptive CCA but it is difficult to find such constructions that are multi-use, efficient and secured. Provides fine grained access control data by limiting decryption based on attributes of receiver but it has an average efficiency and flexibility. Current PRE schemes provide an efficient mechanism but it is very difficult to design and secure. Time based PRE is a more recent modification of PRE schemes which provides a defineable user revocation and reduces the workload of data owners. Drawback is that it requires effective time to be same for attributes and threshold PRE enables data forwarding efficiently but requires high access control which is difficult to provide.

II. DISADVANTAGES OF EXISTING SYSTEM

- Due to the lack of using an asymmetric key in the existing system, we can not be able to provide more secure than systems and it can easily accessible by the attackers to breach the data.
- In the existing system, there will be low-security control for the user information, the user is not able to receive any authentication message.
- Data that consists of various information can be damaged or processed by unauthenticated users.

III. PROPOSED SYSTEM

Due to isolated population of candidate solutions, it brings a typical limitation called premature convergence. In this the evolution falls into a local optimum too early, resulting in a solution far from the global optimum. It is known that multi-population genetic algorithm can efficiently overcome this

limitation by using multiple populations to evolve together. We propose to use multi-population co-evolution to enhance the robustness of data. We provide a Robustness Optimization with multi-population Co-evolution which introduces operators to rewire network topologies to enhance the robustness against malicious attacks. In addition we propose a block chain paradigm that if an attacker attacks single node our proposed methodology restricts the attacker. To modify the data from the single node we have to modify every node that has been present in the system. It increases the security and efficiency of the network that has been processed. along with attackers IP and MAC can be retrieved for better privacy preservation schema.

IV. ADVANTAGES

- Secured sharing of sensitive encrypted data" — with multiple third parties, be it a customer, partner, supplier or even a regulator.
- No Computational Overhead.
- CC-proxy re-encryption technology provides the customers to give the ability to manage access controls without needing to provide full access to the data.
- It can remove any isolated point of failure (i.e. via an admin will have full access control to all of the data).
- No internet is needed either for encrypt or decrypt.

V. FEASIBILITY STUDY

Depending on the results of the initial investigation the survey is currently distended to a a lot of elaborated feasibleness study. "FEASIBILITY STUDY" may be a check of system proposal in step with its workability, the impact of the organization, ability to satisfy desires and effective use of the resources. It focuses on these major questions:

- What square measure the user's demonstrable desires and the way will a candidate system meet them?
- What resources square measure offered for a given candidate system?
- What square measure the doubtless impacts of the candidate system on the organization?
- Whether it's price to resolve the problem?

During the feasibleness analysis for this project, the subsequent primary square measureas of interest are to be thought of. Investigation and generating concepts a few new system will this.

a)TECHNICAL FEASIBILITY

A study of resource convenience that will have an effect on the power to attain a suitable system. This analysis determines whether or not the technology required for the planned system is offered or not.

- Can the work for the project be through with current instrumentality existing software system technology & out there personal?
- Can the system be upgraded if developed?
- If new technology is required then what is developed?

b)ECONOMIC FEASIBILITY

Economic justification is mostly the "Bottom Line" thought for many systems. Economic justification includes a broad vary of considerations that features a analysis. In this, we have a tendency to weight the price and therefore the advantages related to the candidate system and if it suits the essential purpose of the organization i.e. profit-making, the project is creating to the analysis and style part. The money and therefore the economic queries throughout the preliminary investigation square measure verified to estimate the following:

• The price to conduct a full system investigation.
• The price of hardware and software system for the category of application being thought of.
• The advantages within the type of reduced price.
• The planned system can offer the minute data, as a result, the performance is improved that successively could also be expected to produce enhanced profits.

c)OPERATIONAL FEASIBILITY

It is in the main associated with human organizations and political aspects. The points to be thought of are:

- What changes are brought with the system?
- What structure structures square measure disturbed?
- What new skills are required?
- Do the present workers members have these skills?
- If not, will they be trained in due course of time?

The system is operationally possible because it is extremely simple for the tip users to control it. It solely desires basic data concerning the Windows platform.

d)SCHEDULE FEASIBILITY

Time analysis is that the most significant thought within the development of the project. The time schedule needed for the event of this project is extremely vital since additional development time result machine time, price and cause a delay within the development of different systems. A reliable Hospital Management System is developed in an exceedingly hefty quantity of your time.

VII.PROJECT DESCRIPTION

Modules

- Cloud Framework
- File System Analysis
- Key Generation
- Double Masking
- Performance evaluation

a)Cloud Framework

Storage policies and an increasing cloud usage environment square measure dynamic needs the necessities for the way users want to access and store information. The cloud storage service is usually initiated by individual users United Nations agency store information and transfer it to set and collaborate. Therefore, additional and additional cloud-based storage platforms suppliers avail storage for his or her users to store information.

b)File System Analysis

Initially VM disk stores the files and analyzes sets to see storage and therefore the information hold on within the CSP. solely files square measure hold on within the Cloud Service suppliers, and so there's no data concerning the keys generated to the files within the CSP.

c)Key Generation

Cryptosystem, many schemes are designed. every user con tains a secret-key. There exists an economical thanks to derive a descendant's key from the owner in accordance with the partial order relation. therefore every user are given a secret key supported the Key Generation algorithmic rule to stop information.

d)Double Masking

KGC will increase the efficiency of the system by providing double encryption schema, that is termed as double masking. It re-encrypts the files that square measure hold on and provides zero data concerning the keys to the cloud service suppliers.

e)Performance evaluation

We tend to assess the performances of the projected schemes supported information measure, user's storage, computation prices and therefore the variety of keys. The system parameters may be chosen to support the measurability with relevancy the mumbled roles, the amount of users, the role of KGC, etc. KGC will increase the performance analysis of the whole system.

VIII.SYSTEM ARCHITECTURE

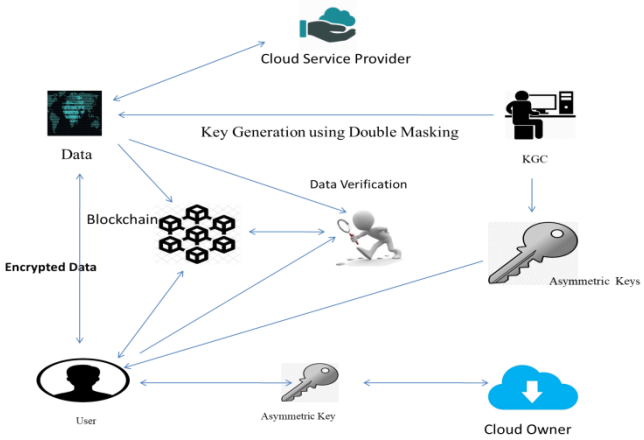

Fig. Architecture diagram for client-centric proxy re-encrytion for outsourced data in the cloud

In the above system diagram, every cloud users have to get authorized by a certain organization. The Cloud storage has provided by the cloud service provider who has authority to authority to provide and access the cloud data. When cloud users have logged into the cloud user portal to access the data, through using blockchain technology we have ale to track the activities that have done by the cloud user. The uploaded data have accessed by the cloud users using a request-response methodology, each and every process has been processed based on the request-response strategy. The files that have been getting encrypted using the public key which has provided by the

key generation center. The key generation center will be responsible people for authenticating the cloud users as well as the cloud owner. The random key generation can not be viewed by cloud service providers. The random key may get generated using a certain algorithm. The key generation center has generated the asymmetric key for the security to the cloud data. Certain files will be provided to the user when the private keys get matched with the provided private keys. If the private key does not matched, it alerts the cloud owner and the cloud user through electronic mail or text message which are get registered in the portal with the attackers' IP address and the MAC address. And then, there will re-encryption process has been done using double masking to secure the files.

Information security is the process of securing data information from unauthorized access not to use, modification, tempering, or disclosure. With the increased use of electronics media in our usual lives as well as business, the way of security breach and its major impact has increased. The theft of personal identity, credit card information, and other important data is hacked by using user names and passwords have become common in nowdays. In addition to this, the theft of confidential business data also leads to loss of business in commercial organizations.

In this free network security tutorial, we'll learn:

- Security Policies and Procedures
- Implementing Good Security Measures
- Information Security Processes
- Implementing Security Policy
- Access Control
- Authentication & Authorization
- Wireless Security
- Encryption & Hashing
- Intrusion Detection
- Physical Security

a)Active Attacks
An active attack is a network to make use of in which attacker attempts to make changes to data on the target or data on the way to the target.

For example, Meet Alice and Bob. Alice wants to interact to Bob but distance is a problem. So, Alice want to send an electronic mail to Bob via a network which is not secure against attacks. There is an another person called Tom, who is in the same network with Alice and Bob. Now, the data flow is open to everyone on the network, Tom will alter some portion of an authorized message to produce an unauthorized effect. For example, there is a message meaning "Allow BOB to read hidden file X" is modified as "Allow Smith to read cofidential file X".

Active network attacks are often aggressive, binding attacks that injured person immediately become aware of when they occur. Active attacks are highly destructive in nature, often locking out users, destroying memory or files, or forcefully gaining access to a targeted system or network.

b)Passive Attacks

A passive attack is a network attack in which a system is monitored and sometimes scanned for unlocked ports and susceptibility, but it does not affect system resources.

For example, Alice sends an electronic mail to Bob via a network which is not safe against attacks. Tom, who is in the same network with Alice and Bob, monitors the data transfer which is taking place between Alice and Bob. Suppose, Alice sends some sensitive information such as bank account details to Bob in the form of plain text. Tom can easily access the data and use the data for intensioned purposes.

So, the purpose of the passive attack is to gain access to the computer system or network and to access data without any detection.

So, network security includes the implementation of different hardware and software techniques necessary to guard underlying network architecture. With the proper network security in place, we can detect emerging threats before they gradually access your network and compromise your data.

IX.CONCLUSION

This paper is proposed a proxy re-encryption for the outsourced data in the cloud. By using our proposed system, the maximum level of security to the data files will be provided and there will be asymmetric secret keys that have been used to provide the maximum level of security to the data files. The data files have been getting encrypted twice using double masking that may have improves the security level. There will no need for internet connectivity for encrypting as well as decrypting the data files. Our proposed system may eliminate a single point of failure and it may decrease the risks to the data.

X.REFERENCE

[1] R. Ahlswede and I. Csisz´ar, "Common randomness in information theory and cryptography. i. secret sharing," IEEE Trans. Info. Theory, vol. 39, no. 4, pp. 1121–1132, July 1993.
[2] U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Info. Theory, vol. 39, no. 3, pp. 733–742, May 1993.
[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Communications Surveys Tutorials, vol. 16, no. 3, pp. 1550–1573, Third 2014.
[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 240–254, June 2010.
[5] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with a low probability of detection on AWGN channels," IEEE Journal of Selected Areas in Communications, vol. 31, no. 9, pp. 1921–1930, September 2013.
[6] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in Proc. of IEEE International Symposium on Information Theory, Istanbul, Turkey, July 2013, pp. 2945–2949.

[7] M. R. Bloch, “Covert communication over noisy channels: A resolvability perspective,” IEEE Trans. Info. Theory, vol. 62, no. 5, pp. 2334–2354, May 2016.
[8] L. Wang, G. W. Wornell, and L. Zheng, “Fundamental limits of communication with a low probability of detection," IEEE Trans. Info. Theory, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.
[9] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion, and stealth,” in Proc. of IEEE International Symposium on Information Theory, Honolulu, HI, July 2014, pp. 601–605.
[10] B. Wu, B. J. Shastri, P. Mittal, A. N. Tait, and P. R. Prucnal, “Optical signal processing and stealth transmission for privacy,” IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1185–1194, Oct. 2015.
[11] K. Shahzad, X. Zhou, and S. Yan, “Covert communication in fading channels under channel uncertainty,” in 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), June 2017, pp. 1–5.
[12] S.-H. Lee, L. Wang, A. Khisti, and G. W. Wornell, “Covert communication with channel-state information at the transmitter,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2310–2319, 2018.
[13] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, “Covert communication in the presence of an uninformed jammer,” IEEE Transactions on Wireless Communications, vol. 16, no. 9, pp. 6193– 6206, 2017.
[14] Q. Zhang, M. Bakshi, and S. Jaggi, “Covert communication over adversarially jammed channels,” arXiv preprint arXiv:1805.02426, 2018. [15] M. Tahmasbi and M. R. Bloch, “Covert secret key generation,” in 2017 IEEE Conference on Communications and Network Security (CNS), Oct 2017, pp. 540–544.
[15] M. Tahmasbi and M. R. Bloch, “Covert secret key generation,” in 2017 IEEE Conference on Communications and Network Security (CNS), Oct 2017, pp. 540–544.