IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CLOUD AND FOG COMBINED GATEWAY ACCESS CONTROL FOR SECURE DATA DISTRIBUTION

[1]Santhanalakshmi K, [2]Gokul Prasanth G, [3]Hariharan K,[4]Mahanantham N

[1]Assistant Proffesor, [2]Student, [3]Student,[4]Student

Department of Computer Science and Engineering,

Paavai Engineering College, Namakkal, Tamilnadu, India

Abstract: Secure personal data sharing in the cloud is a crucial issue since it raises a number of security and data confidentiality challenges while using cloud services. Many obstacles still stand in the way of attaining practical fine-grained access control in the Personal Information Sharing system, including data privacy protection, flexible data sharing, effective authority delegation, and computing performance optimization. Before outsourcing to the cloud, personal records must be encrypted to safeguard privacy. Here, offer an effective data sharing system for healthcare data sharing that simultaneously protects data privacy, implements fine-grained access control, and delegated authority. It is suggested that a duplicate generation mechanism along with a two-server computing environment be used to secure patient MHRs in the healthcare cloud. The replica server acts as a second gallery for duplicate MHR, which gives the attacker the impression that it is the original data uploaded by data owner. A duplicate file will be kept on another server when a user uploads a file to the original server. The duplicate files are obtained from the beginning in our proposed methodology to ensure improved security. In this way, the decoy files are called when an intruder is identified accessing the system. The Elliptic Curve Cryptography (ECC) algorithm is being used in the suggested strategy to encrypt the medical records.

Index Terms - Public Key Generator (PKG), Elliptic Curve Cryptography (ECC), Architecture description languages (ADLs).

I. INTRODUCTION

Cloud computing technology consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security, as there is valuable and sensitive data in huge amount stored on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing.The e-Healthcare information offers unique security, privacy and confidentiality challenges that require a fresh examination of the mainstream concepts and approaches to information security. The significance of security and privacy in eHealthcare information raised the issues of individual consent, confidentiality and privacy, which are the main determinants in adopting and successful utilising the e-Healthcare information. Current trends in the domain of e-Healthcare information management point to the need for comprehensive incorporation of security, privacy and confidentiality safeguards within the review of e-Healthcare information management frameworks and approaches. This raises major challenges that demands holistic approaches spanning a wide variety of legal, ethical, psychological, information and security engineering. The e-healthcare information is varied and complex in nature. It is collected, maintained and utilised by a variety of players within the healthcare profession as well as in other sectors, where it is required for purposes such as insurance, employment and research. The structure of healthcare is multi-dimensional as it can be viewed in time-oriented, source-oriented and clinical problem-oriented terms with further dimensions being possible. In practice, health

information is scattered across and within organisations and countries. The period for utilising health information spans over a lifetime of an individual. There may be a statutory time period from the death of a person after whose expiry the deceased's healthcare information may be destroyed. The destruction of health information by a controller of such information is a legally regulated process. A key aspect of the nature of healthcare information is that it is personal It appears that this approach is increasingly being discarded in some places, where it seems legal ownership of health information is bestowed on the patient while the healthcare unit is designated as a controller with legal rights, interests and obligations over the information. Thus, use of health information always requires the consent of the individual owner. In practice, there is a separation between ownership and control of health information, the owner of healthcare information may not be the one who controls its collection, storage and processing.Therefore, this necessitates distinction between owners, the controllers, processors and users of healthcare information. The latter are governed by the laws on the protection of information to ensure the consent and preserve the owners' privacy and confidentiality. he proposed project aims to address the critical need for secure healthcare data sharing in the cloud by leveraging advanced encryption techniques, duplicate generation mechanisms, and a two-server computing environment. By utilizing Elliptic Curve Cryptography (ECC) for encrypting medical records, the system ensures that sensitive information remains protected from unauthorized access while stored in the cloud. The implementation of a fog server further enhances security by processing and encrypting data before it is uploaded to the primary cloud server. Additionally, a duplicate generation mechanism is employed to create fake copies of the original data on a secondary cloud server, ensuring that unauthorized users are directed away from accessing sensitive information. The scope of this project encompasses key aspects such as key generation and distribution, access control mechanisms, data processing, encryption, and retrieval, as well as monitoring and auditing functionalities to track and prevent unauthorized access attempts. By developing an extensible and robust system, this project aims to provide healthcare organizations with a secure platform for sharing sensitive patient data while maintaining privacy and confidentiality.

II. OBJECTIVES

Develop a robust cloud-based infrastructure capable of securely storing and sharing healthcare data while ensuring privacy and confidentiality.Set up a Public Key Generator (PKG) system responsible for generating system parameters and distributing public/private keys to authorized users for encryption and decryption purposes.Integrate ECC algorithm for encrypting medical records to ensure that sensitive information remains protected against unauthorized access.Utilize fog computing to process and encrypt data before uploading it to the cloud, enhancing security and reducing the risk of data breaches during transmission.Implement a mechanism for generating duplicate copies of the original data on a secondary cloud server to deter unauthorized access and maintain data integrity.Develop access control mechanisms to ensure that only authorized users can access the original data stored on the primary cloud server, while unauthorized users are redirected to the secondary server containing fake copies.

III. EXISTING SYSTEM

With fog, availability of a service can be increased. When a fog gathers data from the underlying nodes and sends it to the cloud in a bottom-up communication, the cloud has an opportunity to create value-added services out of it. On the other hand, in a top-down communication where a cloud provides its resources to the underlying nodes, a fog can extend the reach of the sensors and nodes lying underneath to more powerful computing resources. In this way, services can be scaled up both horizontally as well as vertically. Various scenarios involving fog or cloud can be applied on the data collected from the sensors and IoT nodes. Fog's resources can be used to perform big data analytics and more complex value-added and smart services can be created for the relevant stakeholders. Sensors and IoT nodes generate unstructured data that may be used for several extended services. Nevertheless, the data must be collected and analyzed extensively to create customized and complex services. Several machine learning and artificial intelligence techniques can be used in this case. This process of data collection and analysis can be more efficient by using fog computing without which, thousands of sensors and nodes will be sending data directly to the cloud or central servers, consuming scarce network bandwidth. For a quick and location-aware task, fog can facilitate in performing then necessary computation. For a task that requires fog to perform immediate actions but delegate the rest to the cloud, a fog-cloud collaborative scenario will be created. In the same way, for tasks that require even more computation or storage capabilities, cloud-only scenario will be suitable.In existing system implemented a three-tier IoT-fog-cloud model. We argue that with distributed

task execution, we can achieve high scalability of IoT services, and manage the global energy consumption as well. As a proof-of-concept, we evaluate our three-tier architecture by taking into account computational tasks for various applications in IoT related to medical, multimedia, location-based, and text. Here provide an implementation of the three-tier CoT architecture with different workloads and assess power consumption and performance based on different data handling and queuing policies run on a middleware. We differentiate among the noteworthy middleware technologies used in cloud-IoT, and elaborate the role of fog computing in this regard. Present three-tier CoT architecture and a task offloading mathematical model for handling incoming tasks from an underlying IoT and decide whether to offload to a fog, a cloud, or collaboratively to fog-cloud. In our architecture, the tasks are received at a gateway (Global Gateway) from where they get distributed elsewhere.

IV. PROPOSED SYSTEM

Proposed system adopt two different public cloud servers to achieve secure outsourced computation, such as outsourced key generation/encryption/re-encryption key generation/ decryption. Actually, one public cloud server (e.g., public cloud 2) is sufficient for outsourced decryption, but not enough for other operations, because the entire secret will be exposed to the unique cloud server. The access control model consists of five entities: private key generator (PKG), public cloud 1, public cloud 2, data owners and data consumers. Proxy Re-encryption is used to re-encrypt the data before sending it to the data consumer. Here propose an efficient data sharing mechanism for Personal Data Sharing, which not only achieves data privacy, fine-grained access control and authority delegation simultaneously, but also optimizes the computation efficiency and is suitable for resource constrained servers. Most of the data consumers are honest, while few of them are corrupt and will leakage their secret keys in the collusion. On the contrary, PKG and data owner are assumed to be fully trusted. Besides, cloud and fog cannot collude with each other. The non-collusive assumption is reasonable, because the client can demand that two cloud servers cannot reveal users' information by contract. This approach has modules like Framework Creation, Medical files uploading, Data Encryption, duplicate Storage, File access and alert system. Input process has file storage and output was providing secure to medical files using two clouds.

V. FEASIBILITY STUDY

The purpose of this chapter is to introduce the reader to feasibility studies, project appraisal, and investment analysis. Feasibility studies are an example of systems analysis. A system is a description of the relationships between the inputs of labour, machinery, materials and management procedures, both within an organisation and between an organisation and the outside world.During the planning and execution stages of an audit, it's important to have a clear understanding of what the objectives of the audit include. Companies should strive to align their business objectives with the objectives of the audit. This will ensure that time and resources spent will help achieve a strong internal control environment and lower the risk of a qualified opinion.

5.1 Technical Feasibility

Technical Feasibility assessment focuses on the technical resources available to the organization. It helps organizations determine whether the technical resources meet capacity and whether the technical team is capable of converting the ideas into working systems. In technical feasibility the following issues are taken into consideration. Whether the required technology is available or not. Whether the required resources are available - Manpower- programmers, testers & debuggers, Software and hardware. Once the technical feasibility is established, it is important to consider the monetary factors also. Since it might happen that developing a particular system may be technically possible but it may require huge investments and benefits may be less. For evaluating this, economic feasibility of the proposed system is carried out.

5.2 Economic Feasibility

Economic feasibility analysis is the most commonly used method for determining the efficiency of a new project. It is also known as cost analysis. It helps in identifying profit against investment expected from a project. Cost and time are the most essential factors involved in this field of study. For any system if the expected benefits equal or exceed the expected costs, the system can be judged to be economically feasible. In economic feasibility, cost benefit analysis is done in which expected costs and benefits are evaluated. Economic analysis is used for evaluating the effectiveness of the proposed system.

5.3 Operational Feasibility

Operational Feasibility is depend on human resources available for the project and involves projecting whether the system will be used if it is developed and implemented. Operational feasibility is a measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements analysis phase of system development. Operational feasibility reviews the willingness of the organization to support the proposed system. This is probably the most difficult of the feasibilities to gauge. If the request was initiated by management, it is likely that there is management support and the system will be accepted and used. However it is also important that the employee base will be accepting of the change.

Equations

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. The key distribution algorithm is used to share a secret key, the encryption algorithm enables confidential communication, and the digital signature algorithm is used to authenticate the signer and validate the integrity of the message:

Private Key = an integer, x, selected from the interval [1, p-1] (1)

Public Key = product, Q, of private key and base point (Q = x*B) (2)

Both parties agree to some publicly-known data items, The elliptic curve equation, Values of a and b,Prime, p.The elliptic group computed from the elliptic curve equation,A base point, B, taken from the elliptic group,Similar to the generator used in current cryptosystems,Each user generates their public/private key pair.

VI. MODULE DESCRIPTION

6.1 Medical Cloud Framework

There is a significant volume of healthcare data generated daily. The data are important and vital for decision making and delivering the best care for patients. Cloud computing is a cost effective method that facilitates real-time data collection, data storage and exchange between healthcare organizations. Cloud infrastructure is characterized with a high throughput and a high volume storage; two important factors for efficient data analysis of large patients' population. Security and privacy are of the major concerns for using cloud-based healthcare services. Healthcare organization should have electronic medical records in order to use the cloud infrastructure. In order to cope with the rapid advancements in information technology and the utilization of cloud based services, efforts should be dedicated to move healthcare data form the traditional paper based to the electronic format. Then, regional legislation and policies should be enacted to regulate and control the usage of healthcare data.

6.2 Upload Medical Files

Cloud computing allows data collection and transfer to healthcare organizations. Data are collected from hospitals in the form of patient details, doctor details, medical reports and prescription details and then transmitted wirelessly to healthcare external processing units where patient's physician monitor and analyse those data. Administrator should maintain the doctor details and also enter the patient details. Then allocate the patients to the doctor based on their disease. Doctor should login and view the allocated patient details. Then doctor can add patient's medical reports and prescriptions for allocated patients. These medical details and files are securely stored in health care cloud.

6.3 Data Encryption

In this module, in order to make health data's more secure use multi party in cloud computing system. The data's encrypted with identity policy can be decrypted only if the identity policy is satisfied. Where the health data is encrypted using attributes and key policy. And the user with a particular attribute and key policy alone will be able to decrypt the health data after it is verified by "key distribution centre" and the "secure data distributor". This technique can be used in medical field for secure storage of patient details and limiting to particular doctor access. It's used to achieve fine–grained access control. A user can decrypt the ciphertext if only his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encryptor holds the ultimate authority about the encryption policy.

6.4 Duplicate Storage

This technique can be considered as an illusion technique, as it makes the attacker believe that he/she has accessed the user's original medical files while in fact it is just a duplicate file. Thus, both authorized and unauthorized users will be referred to the Duplicate Storage as the first step, while authorized legitimate users, as a second step, will be referred to the Original Cloud after being verified. We believe that by setting the default value of the as shown and the OMBD as hidden, we keep the original MBD more secure. Also, we believe that verifying that the user is legitimate is much easier than detecting the attacker, which is why we tried to deal with the attacker in the first place by offering the DMBD as the first step.

6.5 File Access

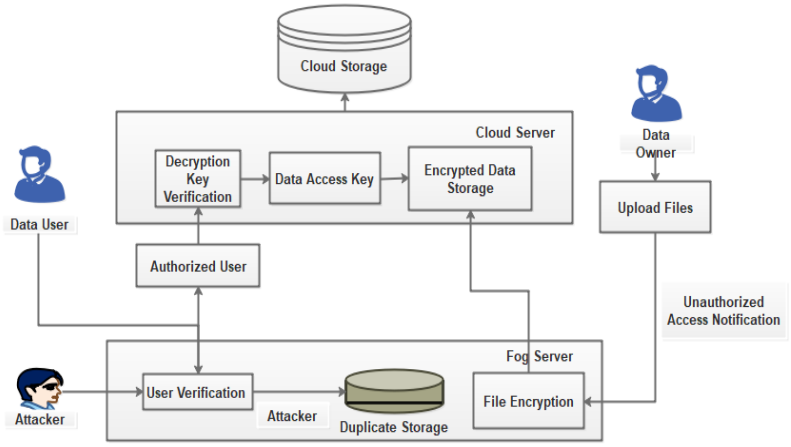
User profiling is a familiar technique that can be applied to model in what way, at what time, and how considerable users access their information in the healthcare cloud. This method of behavior-based security is commonly used in fraud detection application. In our proposed system, once the user accesses his/her account, by default the duplicate storage is shown. The legitimate user already knows that the gallery he/she accessed is not his/her original one, so would move on to the next step. Moving to the next step, the legitimate user can access his/her original medical files after being verified by passing the key verification. The key verification is the process of verifying the secret key by authorized user. Thus, if he/she passes the key verification, that means he/she is the authorized user, so will be able to access the original medical files which are located on the cloud computing layer.

6.6 Alert Intimation

One of the key issues is to effectively detect any unauthorized data access in cloud. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data access occurs. Finally provide SMS alert to data owner regarding the file access in duplicate storage. The intimation will be send to the form of mobile SMS.

VII. SYSTEM ARCHITECTURE

System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. Software architecture must describe its group of components, their connections, interactions among them and deployment configuration of all components. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).



VIII. RESULTS AND DISCUSSION

7.1 CONCLUSION

In this project proposed a new mechanism is proposed to protect the healthcare data in the cloud. This system has a double layer protection in which the EHRs are stored in the cloud. Encryption/ Decryption will be done in one layer and in the other layer; duplicate files will be created and stored. To this end, two cloud storages are generated for different purpose. The original medical files are kept secretly in the cloud and the duplicate cloud is used as duplicate file storage. Therefore, instead of retrieving the duplicate medical files only when any unauthorized access is discovered, the user, by default, accesses the duplicate files in cloud 2. The original server is only accessible by a user after verifying the authenticity of the user. Thus, the original multimedia data become more secure by setting the default value of the duplicate storage, while the original medical files are kept in a secure hidden cloud.

7.2 FUTURE ENHANCEMENT

In future work, we can extend the framework to implement the system with various encryption algorithms and also other cryptographic approaches in real time images and medical videos. Implement Stenography based approach to hide the Medical Data inside the Medical Image or other Images to provide secure sharing.

REFERENCES

[1] Hahn, Changhee, Jongkil Kim, Hyunsoo Kwon, and Junbeom Hur. "Efficient iot management with resilience to unauthorized access to cloud storage." IEEE Transactions on Cloud Computing 10, no. 2 (2020): 1008-1020.

[2] Abdollahi, Sina, Javad Mohajeri, and Mahmoud Salmasizadeh. "Highly Efficient and Revocable CP-ABE with Outsourcing Decryption for IoT." In 2021 18th International ISC Conference on Information Security and Cryptology (ISCISC), pp. 81-88. IEEE, 2021.

[3] Fugkeaw, Somchart. "A lightweight policy update scheme for outsourced personal health records sharing." IEEE Access 9 (2021): 54862-54871.

[4] Yang, Kan, Xiaohua Jia, Kui Ren, Ruitao Xie, and Liusheng Huang. "Enabling efficient access control with dynamic policy updating for big data in the cloud." In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, pp. 2013-2021. IEEE, 2014.

[5] Yu, Jiguo, Suhui Liu, Shengling Wang, Yinghao Xiao, and Biwei Yan. "LH-ABSC: A lightweight hybrid attribute-based signcryption scheme for cloud-fog-assisted IoT." IEEE Internet of Things Journal 7, no. 9 (2020): 7949-7966.

[6] Xiong, Shuming, Qiang Ni, Liangmin Wang, and Qian Wang. "SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage." IEEE Internet of Things Journal 7, no. 4 (2020): 2914-2927.

[7] Qi, Saiyu, Youshui Lu, Wei Wei, and Xiaofeng Chen. "Efficient data access control with fine-grained data protection in cloud-assisted IIoT." IEEE Internet of Things Journal 8, no. 4 (2020): 2886-2899.

[8] Ullah, Zia, Basit Raza, Habib Shah, Shahzad Khan, and Abdul Waheed. "Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment." IEEE Access 10 (2022): 36978-36994.

[9] Saini, Akanksha, Qingyi Zhu, Navneet Singh, Yong Xiang, Longxiang Gao, and Yushu Zhang. "A smart-contract-based access control framework for cloud smart healthcare system." IEEE Internet of Things Journal 8, no. 7 (2020): 5914-5925.

[10] Alshehri, Suhair, Omaimah Bamasaq, Daniyal Alghazzawi, and Arwa Jamjoom. "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment." IEEE Internet of Things Journal 10, no. 5 (2022): 4239-4256.