SECURE STORAGE OF PERSONAL HEALTH RECORD USING CRYPTO SYSTEM IN CLOUD

Mr. RUPENDRA SINGH, BULUSU SRI HARSHA

[1] **Assistant professor, CSE DEPT, VISAKHA INSTITUTE OF ENGINEERING & TECHNOLOGY , Vishakhapatnam, Andharapradesh**
[2]**PG Scholar of M.Tech, CSE DEPT, VISAKHA INSTITUTE OF ENGINEERING & TECHNOLOGY , Vishakhapatnam, Andharapradesh**

Abstract: The dispersed health data By distributing personal health information across healthcare professionals, the cloud computing technology significantly facilitates safe and effective patient treatment for medical consultation. The difficulty posed by this system should be maintaining patient identify privacy while also maintaining data confidentiality. Many access control and anonymous authentication methods now in use cannot be easily misused. An innovative authorised accessible privacy model (AAPM) is created to address the issue raised. By configuring an access tree that supports adjustable threshold predicates, patients can authorise doctors. A patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) is then proposed based on this, realising three levels of security and privacy requirements in distributed healthcare data Keyword cloud computing system by developing a new technique of attribute based designated verifier signature. By satisfying the access tree with their own attribute sets, the directly authorised physicians, the indirectly authorised physicians, and the unauthorised persons in medical consultation can, in turn, decrypt the personal health information and/or verify patients' identities. In order for only the client to see the contents of the stored data, confidentiality refers to the secrecy of the data. Data encryption techniques might be helpful to address the issue of confidentiality by giving consumers some control over the secrecy of storing data. Many recent studies have implemented this, enabling users to encrypt their data before outsourcing to the cloud. The searchable encryption technology combines security protection with advantageous operability features, and it can be quite useful for maintaining record systems. In this research, we offer a novel cryptographic primitive called key wrapping encryption technique that uses the sponge function to secure data storage and time-based conjunctive keyword search to limit guessing attacks.

Index Terms: - Authorised Accessible Privacy Model (AAPM), wrapping encryption, novel cryptographic

I Introduction

Using computer resources (hardware and software) that are provided as a service across a network is known as cloud computing (typically the Internet). The name is derived from the widespread use of a cloud-shaped symbol in system diagrams as a metaphor for the intricate infrastructure it holds. Cloud computing entrusts the data, software, and processing of a user to remote services. Hardware and software resources are made accessible via the Internet as managed third-party services in cloud computing. These services often give users access to cutting-edge server networks and sophisticated software programmes. The purpose of cloud computing is to apply traditional supercomputing, or high-performance computing power, typically used by military and research facilities, to consumer-oriented applications like financial portfolios, deliver personalised information, provide data storage, or power massively multiplayer online games.

To distribute data-processing tasks across a network of several servers running, typically, low-cost consumer PC technology and specialised connections, see cloud computing. Large networks of interconnected systems make up this shared IT infrastructure. Virtualization methods are Three main service models are included in cloud computing: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). An end user layer that encompasses the end user perspective on cloud services completes the three service models or layers. The following figure depicts the model. A cloud user can run her own applications on the resources of a cloud infrastructure if she accesses services at the infrastructure layer, for example, and is still in charge of the support, upkeep, and security of these apps. These responsibilities are usually handled by the cloud service provider if she uses a service that is accessible at the application layer. frequently employed to increase the power of cloud computing.

2. Literature survey

1)Cross-Domain Data Sharing In Distributed Electronic Health Record Systems

Cross-organization or cross-domain cooperation takes place from time to time in Electronic Health Record (EHR) system for necessary and high-quality patient treatment. Cautious design

Journal of Engineering Sciences
Vol 14 Issue 03,2023

of delegation mechanism must be in place as a building block of cross- domain cooperation, since the cooperation inevitably involves exchanging and sharing relevant patient data that are considered highly private and confidential. The delegation mechanism grants permission to and restricts access rights of a cooperating partner. Patients are unwilling to accept the EHR system unless their health data are guaranteed proper use and disclosure, which cannot be easily achieved without cross-domain authentication and fine- grained access control. In addition, revocation of the delegated rights should be possible at any time during the cooperation. In this paper, we propose a secure EHR system, based on cryptographic constructions, to enable secure sharing of sensitive patient data during cooperation and preserve patient data privacy

2)**Sage: A Strong Privacy-Preserving Scheme against Global Eavesdropping For E-health Systems**

The eHealth system is envisioned as a promising approach to improving health care through information technology, where security and privacy are crucial for its success and large-scale deployment. In this paper, we propose a strong privacy-preserving Scheme against Global Eavesdropping, named SAGE, for eHealth systems. The proposed SAGE can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. Extensive analysis demonstrates the effectiveness and practicability of the proposed scheme.

3)**Privacy-Preserving Query Over Encrypted Graph-Structured Data in Cloud Computing**

In the emerging cloud computing paradigm, data owners become increasingly motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. For the consideration of users' privacy, sensitive data have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. In this paper, for the first time, we define and solve the problem of privacy-preserving query over encrypted graph-structured data in cloud computing (PPGQ), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Our work utilizes the principle of "filtering-and- verification". We prebuild a feature-based index to provide feature-related information about each encrypted data graph, and then choose the efficient inner product as the pruning tool to carry out the filtering procedure.

4)**Securing Personal Health Records In Cloud Computing:** Patient-Centric and Fine-Grained Data Access Control In Multi-Owner Settings

Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In this paper, we propose a novel framework for access control to PHRs within cloud computing environment.

3 Implementation Study

In a healthcare data Keyword system data confidentiality is much important but in existing system framework it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data

confidentiality and identity privacy in the distributed healthcare data Keyword cloud computing scenario under the malicious model was left untouched. Public key encryption scheme with keyword search (PEKS) allows a user to search on encrypted information without decrypting it, which is suitable to enhance the security of EHR systems. In some situations, a patient may want to act as a delegator to delegate his search right to a delegatee, who can be his doctor, without revealing his own private key. The proxy re-encryption (PRE) method can be introduced to fulfill the requirement. The server could convert the encrypted index of the patient into a re-encrypted form which can be searched by the delegate. However, another problem arises when the access right is disseminated. When the patient recovers and leaves the hospital or is transferred to another hospital, he does not want the private data to be searched and used by his previous physicians anymore.

DISADVANTAGES

Data confidentiality is low.

Data redundancy is high.

There is a violation in data security.

The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems

3.1 Proposed Methodology

Proposed system for a privacy-preserving authentication scheme in anonymousP2P systems based on Zero-Knowledge Proof. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed healthcare data Keyword cloud computing systems where the computational resource for patients is constrained. Suggested patients have to consent to treatment and be alerted every time when associated physicians access

Journal of Engineering Sciences
Vol 14 Issue 03,2023

their records and also our proposed system is a patient-centric and fine-grained data access controlling multi-owner settings is constructed for securing personal health records in cloud computing.

Our proposed healthcare data Keyword system mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in healthcare data Keyword cloud computing system. in distributed healthcare data Keyword cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes. They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained.

In this paper, we aim to solve the problem with a novel mechanism for Storing and searching of the data using the key wrap and sponge function cryptography. With a novel searchable encryption scheme supporting secure conjunctive keyword search function. Compared with existing schemes, this work can achieve Better re-encryption with effective delegation revocation. And Searching technique will avoid the Guessing Attacks.

Advantages:

Healthcare data Keyword system is fully controlled and secured with encryption standards.

There is no data loss and data redundancy.

System provides full protection for patient's data and their attributes.

The beauty of the proposed system is the re-encryption phase and sponge construction which give more security in Data Storage information and Data Retervial using key Word Search for avoiding the attacks.

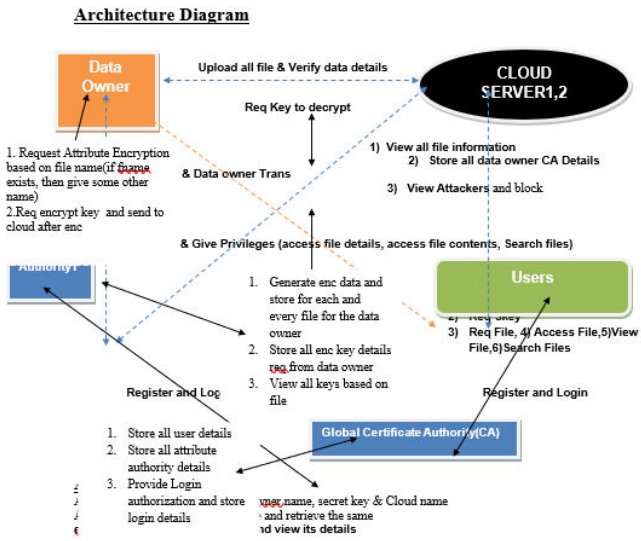

Figure 1: System Architecture

4. Methodology

SPONG CONSTRUCTION

The sponge construction builds a function [f,pad,r] with domain Z2∗ and co domain Z2∞ using a fixed-length transformation or permutation f, a sponge-compliant padding rule "pad" and a parameter bitrate r.A finite-length output can be obtained by truncating it to its ℓ first bits. We call an instance of the sponge construction a sponge function.

The transformation or permutation f operates on a fixed number of bits, the width b. The sponge construction has a state of b bits. First, all the bits of the state are initialized to zero. The input message is padded and cut into r-bits blocks. Then it proceeds in two phases: the absorbing phase followed by the squeezing phase. In these phases the first r bits of the state and the remaining b − r bits of the state s are treated differently. We denote the former by the outer part s and the layer by the inner part or inner state s. The length of the inner state is b − r and is called the capacity c . The two phases are:

Absorbing phase

The r-bit input message blocks are XORed into the outer part of the state, interleaved with applications of the function f. When all message blocks are processed, the sponge construction switches to the squeezing phase.

Squeezing phase

The outer part of the state is iteratively returned as output blocks, interleaved with applications of the function f. The number of iterations is determined by the requested number of bits ℓ. Finally the output is truncated to its first ℓ bits. The c-bit inner state is never directly affected by the input blocks and never output during the squeezing phase. The capacity c actually determines the ainable security level of the construction, as proven in Chapters 5 and 6. We use the term random sponge to denote a sponge function with f a random transformation or permutation.

•Definition

An ack on a sponge function is a generic a ack if it does not exploit specific properties of f. The sponge construction is illustrated in Figure 2.1, and Algorithm 1 provides a formal definition. In our original paper on sponge function we treated a more general case with the outer part and message blocks being elements of an arbitrary group and the inner part elements of an arbitrary set. Because of its practical relevance, we abandon this generic representation to the more specific case where the state is a binary string of a given length b and the message blocks are r-bit strings.\

The sponge construction Z =[f,pad,r](M, ℓ)

The duplex construction

Like the sponge construction, the duplex construction [f,pad,r] uses a fixed-length transformation or permutation f, a padding rule pad and a parameter bitrate r to build a cryptographic scheme. Unlike a sponge function that is stateless in between calls, the duplex construction results in an object that accepts calls that take an input string and return an output string that depends on all inputs received so far. We call an instance of the duplex construction a duplex object, which we denote D in our descriptions. We prefix the calls made to a specific duplex object D by its name D and a dot.

5 Results and Evolution Metrices

Fig2: Home Page

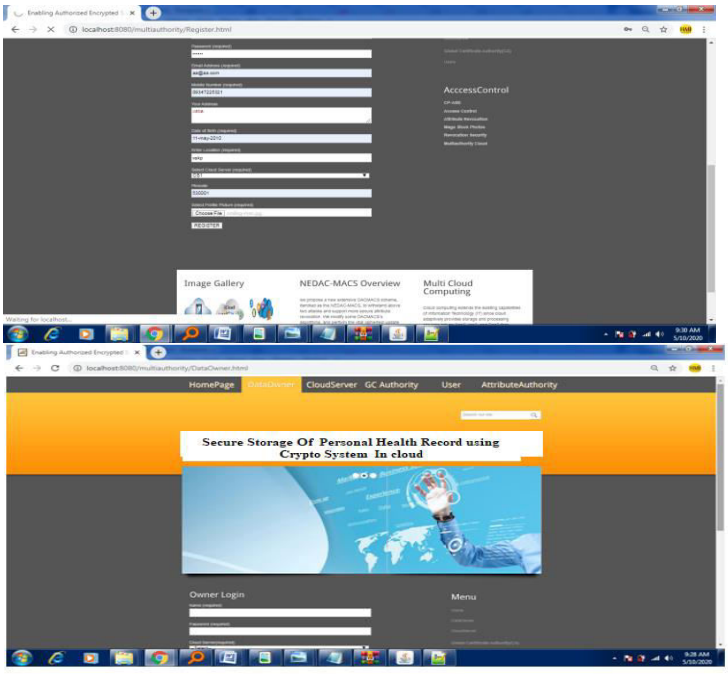

Fig3: Owner Login Page

Fig4:Registration Module

Fig5:Cloud Login

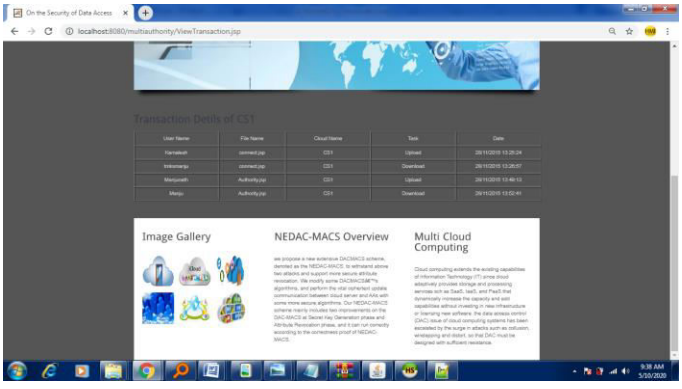

Fig6: Cloud Server Home page

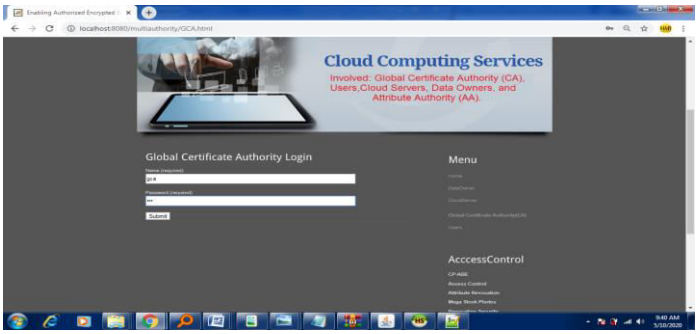

Fig7: Certificate Authority Login

Fig8: Authority Home Page

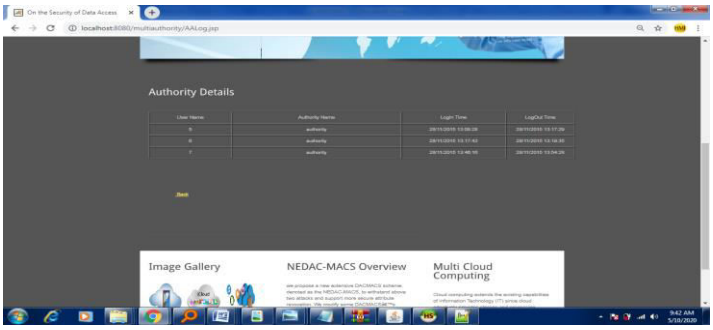

Fig9: Log Details

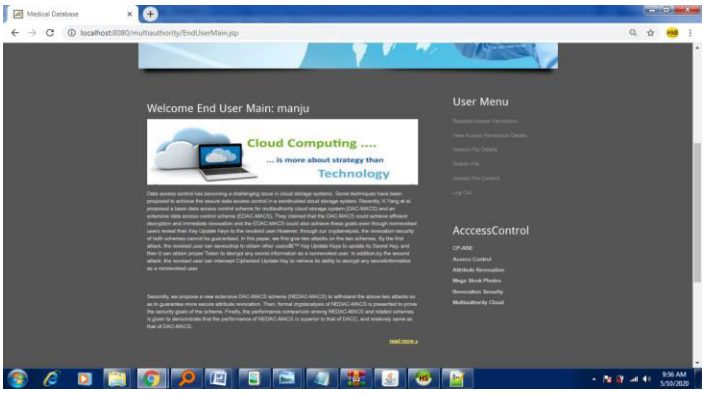

Fig10: End User home page

Fig11: Access permission details

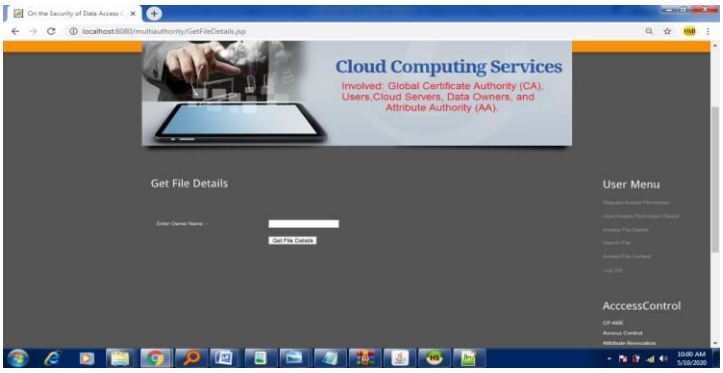

Fig12: Getting file detail

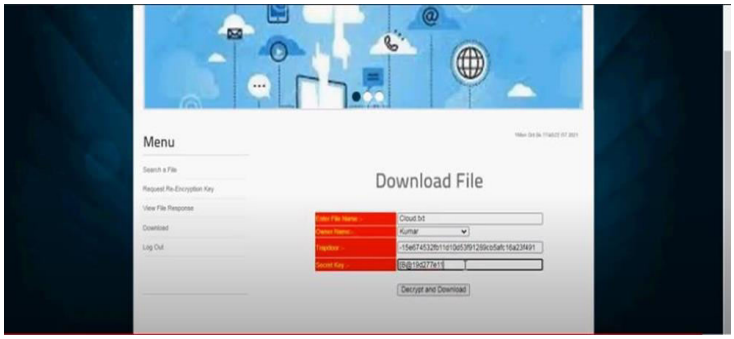

Fig13: Download The File After Re Encryption

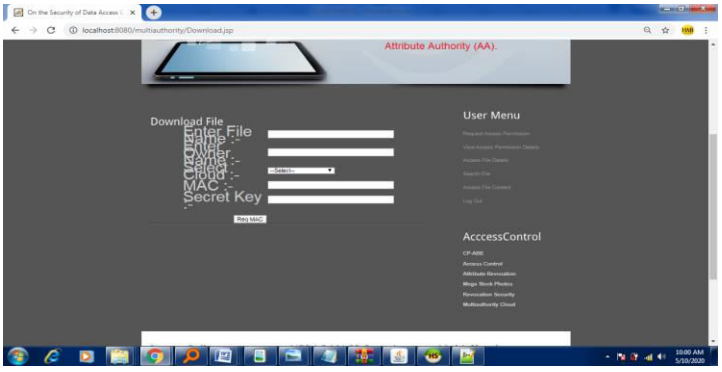

Fig14: Accessing file using secret key

Fig15: Generate Encrypt keys

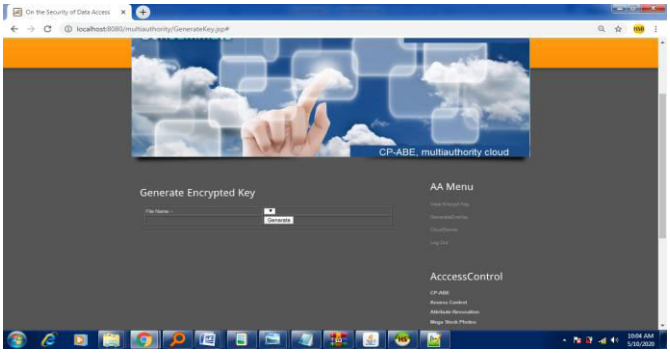

Fig16: Generate Key for cloud servers

6 Conclusion

A novel authorized accessible privacy model and a patient self-controllable multi- level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed healthcare data Keyword cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

7 References

[1] I. J. Misic and V. B. Misic, "Implementation of security policy forclinical information systems over wireless sensor network," AdHoc Netw., vol. 5, no. 1, pp. 134–144, Jan. 2007.

II. J. Misic and V. Misic, "Enforcing patient privacy in healthcare WSNs through key distribution algorithms," Security Commun. Netw. J., vol. 1, no. 5, pp. 417–429, 2008

III. M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Proc. 6th Int. ICST Conf.Security Privacy Comm. Netw., 2010, pp. 89–106.

IV. J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record
system," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 6, pp. 754–764, Jun. 2010.

V. R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms- matching for mhealthcare social network," J. Mobile Netw. Applications, vol. 16, no. 6, pp. 683–694, Dec. 2011.