International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

An Efficient File Hierarchy based E-System with Clinical Document Architecture in Cloud Computing

Archana. P
PG Student, Department of CSE, Mailam Engineering College, Mailam, Tamil Nadu, India

Prasanna. S
Associate Professor, Department of CSE, Mailam Engineering College, Mailam, Tamil Nadu, India

ABSTRACT

E- Healthcare system monitors the health condition and gives medical treatment through our web application. They collect the real time personal information (PHI) and patient's physical problem and transmitted it to the healthcare provider. To securely share the PHR information in cloud computing, a patient divides his PHR information M into two parts: personal information m1 that may contain the patient's name, social security number, telephone number, home address, etc. The medical record m2 which does not contain sensitive personal information, such as medical test results, treatment protocols, and operation notes. Then the patient adopts CP-ABE scheme to encrypt the information m1 and m2 by different access policies based on the actual need. Also we propose The Clinical Document Architecture (CDA). Our CDA document integration system integrates multiple CDA documents per patient into a single CDA document and physicians and patients can browse the clinical data in chronological order and historical wise.

I. INTRODUCTION

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Managing a private cloud requires software tools to help create a virtualized pool of compute resources, provide a self-service portal for end users and handle security, resource allocation, tracking and billing. Management tools for private clouds tend to be service driven, as opposed to resource driven, because cloud environments are typically highly virtualized and organized in terms of portable workloads. In hybrid cloud environments, compute, network and storage resources must be managed across multiple domains, so a good management strategy should start by defining what needs to be managed, and where and how to do it. Policies to help govern these domains should include configuration and installation of images, access control, and budgeting and reporting.

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers of the healthcare industry as they analyze and consider the implications

of cloud computing on their business. The paper includes guidance and strategies, designed to help these decision makers evaluate and compare cloud computing offerings in key areas from different cloud providers, taking into account different requirements from various actors including medical practices, hospitals, research facilities, insurance companies and governments.

When considering a move to use cloud computing, healthcare consumers must have a clear understanding of unique benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider. Consideration must be given to the different models of service delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as each model brings different requirements and responsibilities. Cloud deployment models (private, public, and hybrid) will also weigh heavily in strategic decisions.

The "Challenges to Leveraging Cloud Computing for Healthcare" section explains the critical barriers to cloud computing adoption for the healthcare industry with specific focus on the stringent security and privacy requirements that must be addressed including the impact of government and industry regulations. The "Benefits of Cloud Computing for Healthcare" section discusses specific IT trends in the healthcare industry that are addressed most effectively, both technically and economically, by cloud computing as opposed to traditional IT environments.

II. LITERATURE SURVEY

L.Gatzoulis and I. Iakovidis[1], in this paper Distributed m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality medical treatment. In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers equipped with their own cloud servers for medical consultant. A novel authorized accessible privacy model (AAPM) and a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system.

Vander Alves, Nan Niu, Carina Alves, George Valença[2] in this paper it defines the This paper discusses Cloud computing security related to the survival of cloud computing, has become a key factor in the development of cloud computing. This paper presents a data security model for cloud computing, and introduces agents to data security module in order to provide more reliable services. In further reducing the user waiting time, speeding up data access, and further increasing data availability. It is also planned to improve agents ability to satisfy the special demands of cloud computing.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter[3],

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains.

Milene Elizabeth Rigolin Ferreira Lopes, Carlos Henrique Quartucci Forster[4], This paper discusses a new cloud security management framework based on aligning the FISMA standard to fit with the cloud computing model, enabling cloud providers and consumers to be security certified. Our framework is based on improving collaboration between cloud providers, service providers and service consumers in managing the security of the cloud platform and the hosted services. In this paper we introduced a collaboration-based security management framework for the cloud computing model. Although the cloud computing model is considered to be a very promising internet-based computing platform, it results in a loss of security control over the cloud-hosted assets.

III. PROPOSED SYSTEM

The files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved. In this paper, efficient privacy-preserving fully heteromorphic data aggregation is proposed, which serves the basis for our proposed PPDM. Then, an outsourced disease modelling and early intervention is achieved, respectively by devising an efficient privacy-preserving function correlation matching PPDM1 from dynamic medical text mining and designing a privacy-preserving medical image feature extraction PPDM2. To protect patient data confidentiality, privacy preserving techniques are implemented to secure the PHI. And then to share data to the admin, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure which would reduce the encryption cost and increase the storage space. Also we propose The Clinical Document Architecture (CDA). We describe our CDA document generation and integration service based on cloud computing, through which hospitals are enabled to conveniently generate CDA documents without having to purchase proprietary software. Our CDA document integration system integrates multiple CDA documents per patient into a single CDA document and physicians and patients can browse the clinical data in chronological order and historical wise.

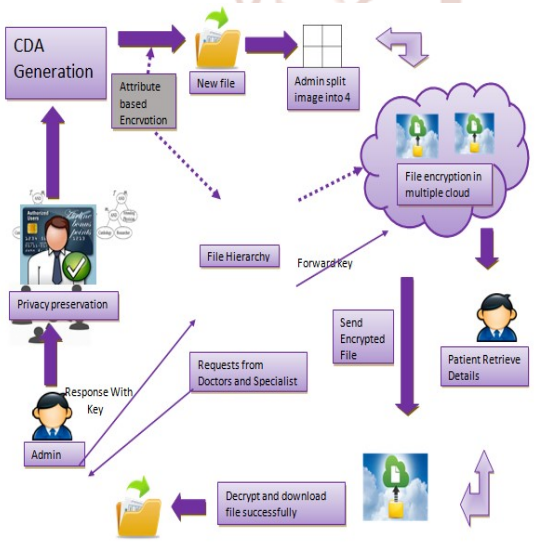

Fig: Overall Architecture

IDENTITY AND AUTHORITY

Indirectly authorized admins and unauthorized admins cannot correctly distinguish the identities of the user from each other. Only the admins directly authorized by the users can only access the user's personal health information and sensitive information's and authenticate their identities simultaneously. The various admins indirectly authorized by user cannot authenticate the user's identities but recover the personal health information. Unauthorized persons can obtain neither.

USER INFORMATION

A user divides his information M into two parts: personal information m1 that may contain the user name, social security number, telephone number, home address, etc. The official record m2 which does not contain personal information, but sensitive information's. Then the users adopts CP-ABE scheme to encrypt the information m1 and m2 by different access policies based on the actual need.

FILE HIERARCHY

We propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure. we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA

An attending physician needs to access both the patient's name and his medical record in order to make a diagnosis, and medical researcher only needs to access some medical test results for academic purpose in the related area, where a doctor must be a medical researcher, and the converse is not necessarily true.

Suppose that the patient sets the access structure of $m1$ as: $T1$ {("Cardiology" AND "Researcher") AND "Attending Physician"}. Similarly, $m2$ is termed as: $T2$ {"Cardiology" AND "Researcher"} the information needs to be encrypted twice if $m1$ and $m2$ are encrypted with access structures $T1$ and $T2$, respectively. The two structures could be integrated into one structure T. the computation complexity of encryption and storage overhead of ciphertext can be reduced greatly.

PRIVACY PRESERVING

SLICING ALGORITHM:

Several anonymization techniques, such as generalization and bucketization, have been designed for privacy preserving micro data publishing. Recent work has shown that generalization loses considerable amount of information, especially for high dimensional data. Bucketization, on the other hand, does not prevent membership disclosure and does not apply for data that do not have a clear separation between quasi-identifying attributes and sensitive attributes.

In this paper, we present a novel technique called slicing, which partitions the data both horizontally and vertically. We show that slicing preserves better data utility than generalization and can be used for membership disclosure protection. Another important advantage of slicing is that it can handle high-dimensional data. We show how slicing can be used for attribute disclosure protection and develop an efficient algorithm for computing the sliced data that obey the ‘-diversity requirement.

Our workload experiments confirm that slicing preserves better utility than generalization and is more effective than bucketization in workloads involving the sensitive attribute. Our experiments also demonstrate that slicing can be used to prevent membership disclosure.

THIRD PARTY AUDITOR

In this module, Auditor (TPA) views all List of Files Uploaded by User. Auditor directly views all user data without key. TPA has privileges to encrypt the user’s data and save it on cloud. Also auditor can view data which is uploaded by various users. TPA can encrypt data and send it to Cloud service provider (CSP) for storage and auditor can view encrypted data of every user.

CLINICAL DOCUMENT ARCHITECTURE

Nowadays in Hospital management, doctors have to share the patient information from one hospital to another hospital by using charts and papers. Doctor’s haven’t maintain any database. For example: a patient has a family doctor for his/her regular treatment from their childhood. Suddenly he/she have a severe attack like heart attack or cancer, the family doctor have to refer the specialist. To overcome this problem we propose the Clinical Document Architecture (CDA).

In existing system patients carry all their medical treatments, slips and bills manually. Moreover it won’t be in an order. We describe our CDA document generation and integration service based on cloud computing, through which hospitals are enabled to conveniently generate CDA documents without having to purchase proprietary software. CDA documents per patient into a single CDA document and physicians and patients can browse the clinical data in chronological order and historical wise. So it’s easy for the doctors to see the patients disease from the initial stage and medicines been taken and symptoms in a single file.

ATTRIBUTE BASE ENCRYPTION

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver’s public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver.

ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

CLOUD STORAGE

Patients can store their personal data and upload records on cloud storage. For security reasons, all data must be encrypted. It uses ABE algorithm for encryption. For Cloud storage we have configured public cloud named CloudMe cloud storage. CloudMe is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration. The service provides 2 gigabytes (GB) of storage for free and up to 100 GB on various for-fee plans. CloudMe is cloud storage service that enables users to store

files on remote cloud servers and the ability to share files within a synchronized format.

CloudMe provides an online storage solution powered by cloud computing service model of infrastructure as a service (IaaS). CloudMe users are provided by an online storage space hosted on CloudMe accessible anywhere via the Internet. The storage space provides storage for virtually any kind of fie type from documents, images, videos etc.

IV. SYSTEM IMPLEMENTATION

The system output is mainly based on privacy preserving method. It will be evaluated using attribute based encryption. Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The FH-CP-ABE scheme consists of four operations: **Setup**, **KeyGen**, **Encrypt** and **Decrypt**. It is described as follows:

1) PK,MSK)←**Setup**(1κ).The probabilistic operation takes asecurity parameter κ as input and outputs publickey PK and master secret key MSK.

2) (SK)←**KeyGen**(PK,MSK,S).The operation inputs PK, MSK and a set of attributes S and creates a secret key SK.

3) (CT) ← **Encrypt**(PK , ck, A). The operation inputs PK, ck={ck1,. . . ,ckk}and a hierarchical access tree A as shown in the Fig.2. Atlast, it creates an integrated ciphertext of content keys CT

4) (cki(i∈[1,k])) ← **Decrypt**(PK,CT,SK). The algorithm inputs PK , CT which includes an integrated access structure A, SK described by a set of attributes S. If the S matches part of A, some content keys cki (i ∈ [1, k]) can be decrypted. If it matches the whole A, all the content keys can be decrypted. Then, the corresponding files mi (i ∈ [1, k]) will be decrypted with the content keys by the symmetric decryption algorithm.

V. CONCULSION AND FUTURE WORK

In this project, a secure and efficient privacy-preserving dynamic medical text mining and image feature extraction scheme PPDM and File Hierarchy in cloud-assisted e-healthcare systems is proposed. Firstly, an efficient privacy-preserving fully homomorphic data aggregation from any one-way trapdoor function is proposed, which serves the basis for our proposed PPDM. Then, an outsourced disease modeling and early intervention is achieved, respectively by devising an efficient privacy preserving function correlation matching PPDM1 from dynamic medical text mining and designing a privacy-preserving medical image feature extraction PPDM2.

Finally, the formal security proof and extensive performance evaluation demonstrate our proposed PPDM achieves a higher security level (i.e. information-theoretic security for input privacy and CCA2 security for output privacy) in the honest but curious model with optimized efficiency advantage over the state-of- the-art in terms of both computational and communication overhead.

VI. REFERENCES

1) M. Quwaider and Y. Jararweh, “Cloudlet-based efficient data collection in wireless body area networks,” Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.

2) K. Dongre, R. S. Thakur, A. Abraham et al., “Secure cloud storage of data,” in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.

3) M. S. Hossain, G. Muhammad, M. F. Alhamid, B. Song, and K. Al- Mutib, “Audio-visual emotion recognition using big data towards 5g,” Mobile Networks and Applications, pp. 1–11, 2016.

4) J. Chen, K. He, R. Du, M. Zheng, Y. Xiang, and Q. Yuan, “Dominating set and network coding-based routing in wireless mesh networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 423–433, 2015.

5) L. M. Kaufman, “Data security in the world of cloud computing,” Security & Privacy, IEEE, vol. 7, no. 4, pp. 61–64, 2009.

6) R. Lu, X. Lin, and X. Shen, “Spoc: A secure and privacy-preserving Oportunistic computing framework for mobile-healthcare emergency,”

Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 3, pp. 614–624, 2013.

7) J.-J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, Q. Wang, and H. Pan, "Emerging information technologies for enhanced healthcare," Computers in Industry, vol. 69, pp. 3–11, 2015.

8) J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.

9) A. Andersen, K. Y. Yigzaw, and R. Karlsen, "Privacy preserving health data processing," in e-Health Networking, Applications and Service (Healthcom), 2014 IEEE 16th International Conference on. IEEE, 2014, pp. 225–230.

10) K. Rohloff and D. B. Cousins, "A scalable implementation of fully homomorphic encryption built on ntru," in Financial Cryptography and Data Security. Springer, 2014, pp. 221–234.