A Privacy Preserving Access Control Model for Personal Health Record System

Omole, G.A[1], Adekunle, Y.A[2], Izang, A. A[3], and Omotunde, A.A[4]
[1-4]Department of Computer Science and Information Technology, Babcock University, Ogun State, Nigeria

***Abstract*– Personal Health Record (PHR) is an evolving patient-centric model for health information exchange and for storing patients' e-record in a centralized place. It permits patients to create, manage, control and share their health information with other users. Privacy and security in cloud computing is an important concern for both public and private sector. Cloud computing has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. While it offers these resources, it likewise poses risks for privacy preservation and the level of assurance required to sustain assurance in would-be users. The challenges in privacy protection are sharing data while protecting personal information. The confidentiality of the medical records is a major problem when patients use commercial cloud servers to store their medical records. In order to assure the patients' control over their own medical records, these records/ files should be preserved with high privacy and security and be encrypted before outsourcing them. In this dissertation, we propose a framework for privacy in a PHR of a patient; the design of a privacy-preserving that enables patients to keep their health information without disclosing their sensitive information to an unauthorized third party. The PHR was designed using Apache server, MySQL as the database in conjunction with PHPMyAdmin, CSS, HTML and JavaScript. The purpose of privacy is to anticipate privacy risks prior to the development of the system and assess its impact on individuals' privacy. This helps to prevent privacy intrusion events before they occur.**

***Keywords*– Attribute Based Encryption, Cloud Computing, Privacy and PHR**

I. INTRODUCTION

PHR is a patient-centric model of health information exchange. It's a service that allows a patient to create, manage, and control his/ her personal health data in a centralized place through the web; from anywhere and at any time so long there is a web browser and an Internet connection. Each patient has the full control of her medical records and can effectively share her health data with a wide range of users, including staffs from healthcare providers, family members or friends. In this way, the accuracy and quality of care are improved, while the healthcare cost is lowered [1].

A key application of data sharing in cloud environment is the storage and retrieval of PHR that maintains the patient's personal and diagnosis information. These records should be maintained with privacy and security for safe retrieval. The privacy mechanism protects the sensitive attributes. The data outsourced to service providers are largely consumed by wide variety of individuals. Hence the need of security and privacy in personal health records is an important issue [2].

The cloud enables patients to remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. As such, the PHR providers are increasingly willing to shift their PHR storage and application services into the cloud instead of structuring specialized data centres.

Online Personal Health Record (PHR) permits patients to manage their own medical records in a centralized way, which enormously simplifies the storage, access and sharing of personal health data. Regardless of this, issues on security and data confidentiality abounds. The cloud enables a convenient, on-demand network access to a shared pool of computing resources like networks, servers, storage, applications and services) that can be provided and released with less management effort or service provider interaction.

When a cloud user provides sensitive personal information (e.g., name, credit card number, phone number, driver's license number, etc.) while requesting services from the cloud, a trail of Personally Identifiable Information (PII), identity information, that can be used to uniquely identify a single person is left behind which—if not properly protected—may be exploited and abused [3].

It becomes more complex when Cloud Service Providers (CSP) use services from other providers to provide a service. Hence, there may be a chain and so, tracking the distribution of PII may not be simple.

Faced with these issues, the major problem regarding privacy in cloud computing is how to secure personal data and information from being used by unauthorized users, preventing attacks against privacy such as identity theft, even when a cloud provider cannot be trusted and maintaining control over private information [4].

A) Privacy in the Cloud

Privacy in cloud computing is defined as the ability of a user or a business to control what information they reveal about themselves over the cloud (or to a cloud service provider,) and the ability to control who can access that information [3]. Privacy is the ability of an individual or group to seclude themselves or information about themselves and also reveal themselves selectively [4].

Privacy is associated with the collection, use, disclosure, storage, and destruction of personal data (or Personally Identifiable Information, PII). Identification of private information depends on the specific application scenario and the law, and is the primary task of privacy protection [5].

In the commercial, user context, privacy entails the protection and applicable use of the personal information of users, and the meeting of expectations of users about its use. For organisations or firms, privacy entails the application of laws, policies, standards and processes by which personal information is managed [6].

Privacy varies from security, in that it relates to handling mechanisms for personal information, dealing with individual rights and aspects like fairness of use, notice, choice, access, accountability and security. Security on the other hand, applies to the provision of protection mechanisms which include authentication, access controls, availability, confidentiality, integrity, retention, storage, backup, incident response and recovery. Privacy only relates to personal information, whereas security and confidentiality can relate to all aspect of information [6].

B) Access Control

Access controls are security features that control how systems and users interact and communicate with one another. They are the collection of mechanisms that allows managers of a system to apply a directing or preventive influence over the use, behaviour and content of a system. Access control mechanisms can be grouped into four main classes: mandatory, discretionary, role based and attribute based [7], [2].

1. Mandatory Access Control (MAC) is a type of access control where the administrator alone manages the access controls. The administrator defines the access policy, which cannot be altered by users, and the policy will specify who has access to which programs and files.
2. Discretionary Access Control (DAC) permits the owner of the resource to specify which data users can access certain resources. The authorization rules clearly state which subjects can execute which actions on a particular resources.
3. In a Role-based Access Control (RBAC) model, access control is centred on a user's roles and on rules that defines which roles can be executed on a certain resource.
4. Attribute Based Access Control: This makes use of attributes as building blocks that describes access control rules and access requests. These attributes are sets of properties or labels that can be used to designate all the entities that must be measured for authorization purposes i.e., access is controlled by the attributes of the user and not by the rights possessed by the user. An attribute-based access control policy requires certain claims that must be satisfied in order to allow access to a resource [2].

In this paper, we provide a secure PHR framework which is to be integrated in a partially-trusted cloud environment so as to realize a fine grained, patient-centric access control.

The rest of the paper is organized as follows: Section two (II) deliberates on some related work in the methods for PHRs. Section three (III) presents the problem statement. Section four (IV) describes about the details of Proposed Framework. Section five (V) gives the conclusion and Section gives the future work.

II. RELATED WORK

In [8], the authors presented the detailed design of modules and implementation of proposed a novel framework for a scalable and secure sharing of personal medical records in cloud computing. They utilized various forms of ABE to encrypt the medical record files, so that patients can allow access not only by personal users but also several users from public domains with different professional roles.

The operations of their proposed medical record sharing system combined KP-ABE and MA-ABE with traditional cryptography which permits patients to share their medical records. These operations were classified into System Setup and Secret Key Generation where the system is divided into two domains; Encryption of Medical Records under a certain fine grained and role-based access policy for users; View Medical Records in order for a data reader to access files; and the revocation of Public domain user and or attributes.

Java Paring Based Cryptography library (JPBC) was employed for the implementation of KP-ABE and MA-ABE. Also, Net Bean-IDE for KP-ABE and Multi Authority API development, SQL Server and Microsoft visual studio 2012 for GUI development. The framework addresses the unique challenges brought by multiple owners and users, in that it reduces the complexity of key management while ensuring privacy.

However, key management is still an issue that needs to be focused upon.

In [9], they proposed a privacy- preserving public auditing system for data storage security in Cloud Computing by utilizing the homomorphic authenticator and random masking to guarantee that Third Party Auditor (TPA) would not acquire any information or knowledge about the data content stored on the cloud server during the efficient auditing process.

However the details of these purported analysis was not included in the work and thus the veracity of the conclusion about the security and efficiency of the schemes could not be verified.

Also, [10] introduced a decentralized access control system with anonymous authentication for secure data storage in the cloud. This gives clients revocation and prevents replay attacks and supports the creation, modification, and reading data stored in the cloud.

They proposed a policy based file access and policy based file assured deletion for better access to the files and delete the files which are no longer required. The main novelty of their model was the addition of key Distribution centres (KDCs).

Their method avoids storing multiple encrypted copies of the same data. This technique does not provide user authentication to users who want to remain anonymous while accessing the cloud. It prevents the cloud from having the

identity of the user who stores information and to verify the user's capability.

The cryptographic keys employed to protect data files stored in the cloud are Public Key, Private Key and Secret Key. This system is a secured system because it allows only authorized user to read, modify, delete, write and access the data which is stored in the cloud.

However in their work, how the algorithms were implemented was not analysed and access control structure was not achieved. Also, security of data storage was not properly addressed.

In [11], to achieve integrity, the authors proposed a novel framework for access control to PHRs within cloud computing environment. To support a flexible, fine-grained and scalable access control with integrity for PHRs, they leveraged on Hierarchical Attribute Set Based Encryption (HASBE) scheme with privacy preserving public auditing to encrypt each patients' PHR data before outsourcing it. In order to support public auditability without having to retrieve the data blocks themselves, the Homomorphic Linear Authenticator technique was integrated with random masking technique.

In the protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server. With random masking, the TPA, who has proficiency and capabilities that cloud users do not have and is trusted to assess the cloud storage service dependability on behalf of the user when it is requested, would not have the capacity to derive the user's data content, no matter how many linear combinations of the same set of file blocks can be collected.

The study aimed at proposing a privacy preserving auditing concept for the HASBE scheme, however it did not succeed in guaranteeing a very high level of data integrity in the cloud.

III. PROBLEM STATEMENT

The problem this dissertation solves is on the aspect of data confidentiality, preserving the privacy of cloud users, to safeguard the medical health record, before outsourcing to the cloud. In order to deal with the prospective risks of privacy disclosure, instead of permitting the service providers to encrypt patients' data, patients/medical record owners are given a full control over the sharing of their own medical data. The challenges in privacy protection are sharing data while protecting personal information.

In the course of seeking solution to these problems and to lower the complexity of encryption and user management for each owner, we adopt Attribute-Based Encryption which is the encryption technique that is used to resolve the problems on outsourced data. It is a technique for handling much number of users i.e., it increases the scalability and to secure sensitive data like patient record over outsourced data in cloud. This problem, if not properly addressed, may defeat the successful deployment of the cloud architecture.

IV. PROPOSED SYSTEM

A) Design Modules

The main goal is to provide a secured PHR framework to be integrated in a partially-trusted cloud environment so as to realize a fine grained, patient-centric access control. It also provides a secured PHR access that would ensure privacy of records and sharing amongst respective users. The system is divided into multiple security domains: public domains and personal domains.

It is assumed that the physical server of cloud-based system is semi trusted compared to centralized servers. As a result, this approach is designed to secure PHR records from the PHR data owner which is the point of origin to the PHR data user who is the recipient in an encrypted format [12].

Users in Public Domains (PUDs) obtain their secret keys without having to directly interact with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies for their PHR files.

Each data owner i.e. patient is a Trusted Authority of her own Personal Domain (PSD), who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD. Since the number of users in a PSD is often small, it reduces the burden for the owner.

When encrypting the data for PSD, all the owner is required to know is the basic data properties. The use of ABE makes the encrypted PHRs self-protective such that they can be accessed by only authorized users even when such data is stored on a semi trusted server and when the owner is not online [13].

The components required to make up the framework that have been proposed includes the following:

The browser, which is the interface that will be accessible by the users of the system; HTTP Server, which handles the http requests sent by a client; Web server clients; the cloud server which is to create interface between application and user. This consists of the Web Container also called Servlet Container/ Servlet Engine that interacts with Java servlets and other forms of files that include server-side code and supports the web components; Web-Service Engine which serves as the communication between two electronic devices over the network, Apache, and the Messaging Engine which is used to exchange clinical data btw several medical applications.

Lastly, is the PHR System which consists of the database which is where the record lies, and the operations that can be performed on it. The aim of the framework is to provide a secured PHR access that would ensure privacy of records and sharing amongst respective users. Authentication through username and password is required to gain access.

To ensure the privacy of patient information using an access control mechanism in which both cipher texts and user's authentication are associated with a set of attributes or a policy, an Attribute Based Access Control mechanism was employed for access control rules and access requests.

For encryption, four algorithms were employed namely: Setup, which is a random algorithm that is run by the central authority; Key Generation, which is a randomized algorithm that is run by the central authority and gives the output as user secret key; encryption which is a randomized algorithm run

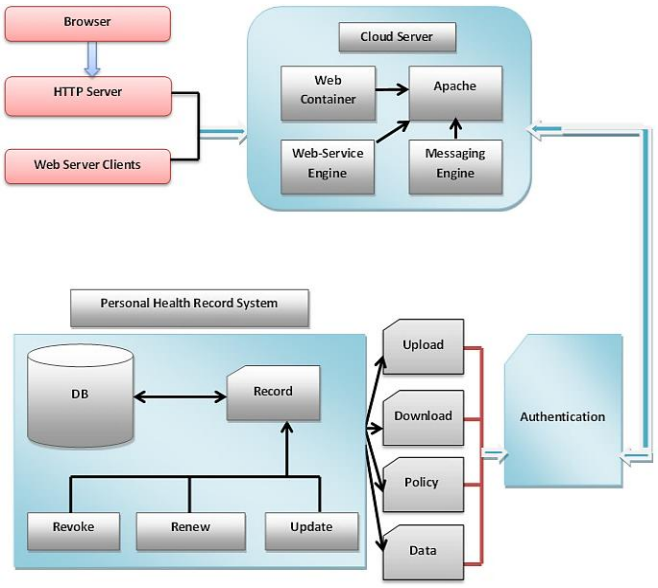

Fig. 1: The Developed Framework of Personal Health Record System

by a sender; and decryption which is a deterministic algorithm run by a user.

B) System Implementation

The System analyses on parameters were on security, scalability and efficiency i.e., should support users). I.e. in terms of storage, communication n computation cost. In the design of the system, the spiral lifecycle Model approach was employed as the developmental process which is ideal for large, costly, and complex projects. For the system testing, we did the component, integration and database testing for corrections and anomalies.

Fig. 2: Homepage

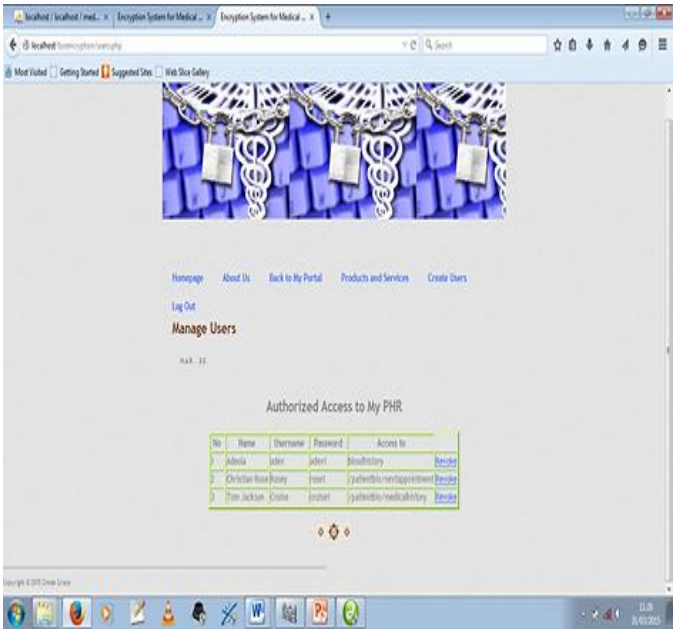

Fig. 3: Lists of Users

For the web based application, we employed the use of MYSQL from PHP MyAdmin to create the database for the application, Apache web server, HTML, CSS, and PHP to design the web pages, Adobe Dreamweaver CS6. Microsoft office 2010 was the modelling tool.

Fig. 3 depicts the lists of users that are present or are able to view a particular patient's record. The lists of what they can view are also shown. For instance, Christian Rose would be able to gain access to 'patient bio data' and 'next appointment' of the patient when she logs on to the record.

System Flowchart for Personal Health Record System:

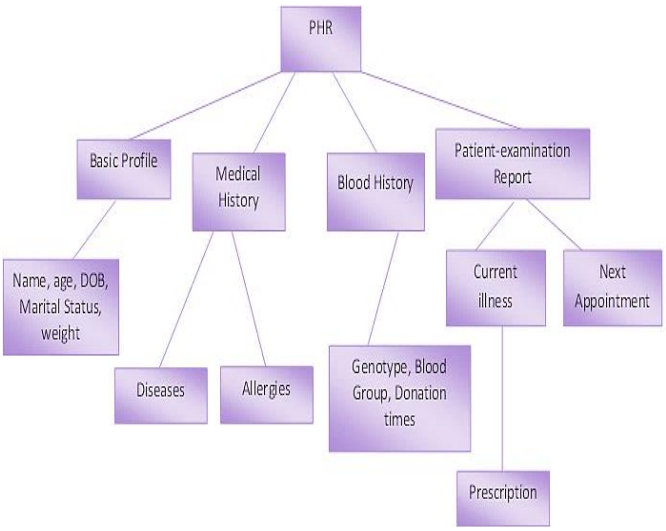

Fig. 4: An Attribute Hierarchy of Health Records

This diagram describes the hierarchy of Attributes that is to be encrypted and stored in Cloud.

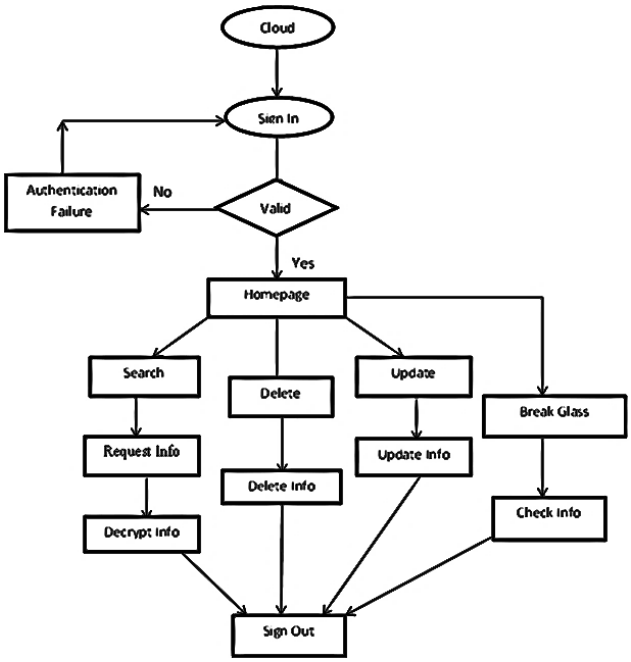

Fig. 5: A System Flow Diagram of PHRs

V. CONCLUSION

In conclusion, this work addresses privacy concerns of cloud-based Personal Health Record system by integrating cryptographic technique and access policy into the PHR system. Considering partially trustworthy cloud servers and privacy control measures, patients are able to control of their own privacy through the encryption of their medical record files to allow fine-grained access which means being able to do as you want i.e., patient. Data owner is able to state n enforce expressive and flexible access structure for each user.

Only users with proper access alone are able to secure access to records of patients and handle them. In addition, emergency data is prevented from being accessed in normal daily situations to prevent the misuse of data.

Generating an emergency report from a patient data to be accessed in emergency situation is an added measure to preserve patient's privacy and confidentiality. This depends mostly on the cooperation between the patient and medical provider. If the patient does not mark the emergency data and marks the whole record, the system becomes inadequate and a major security breach in the system.

VI. FUTURE WORK

This work focuses on securing sharing of medical records and also provides a means whereby a patient's authentication and information can be preserved while accessing the cloud against intrusion from an unwanted party.

We all seek for our private lives to be ours only and not for general consumption. This is made sure and data confidentiality is certain and the control of ones' own records is assured. Hence, I'll recommend that it is importance to set in place schemes that can check against, protect and avoid intrusions, attacks or in any of its forms from occurring. By so doing, trust and increase in the use of the cloud would be at its fullest.

Also, this research recommends Nigeria hospitals to use the cloud as a means of sharing records from a centralized place in a secured way. It is better and safer that way and can also be kept for future references. It can also be adopted and incorporated in other fields that regard and take into consideration security in their daily day-to –day activities.

For further duties, other forms of encryption would be employed and also fine grained access control can be enhanced in cloud computing with a third party auditor to confirm the cloud server that stores and process the PHRs.

REFERENCES

[1] M. Li, S. Yu, K. Ren & W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," 2010.

[2] S.A. Abraham & R. Gokulavanan, "Ensuring Privacy and Security in Data Sharing under Cloud Environment," International Journal of Computer Applications Technology and Research 2 (2), pp. 188 – 194, 2013.

[3] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien & L.B. Othmane, "A User- Centric Approach for Privacy and Identity Management in Cloud Computing," IEEE International Symposium on Reliable Distributed Systems, 2010.

[4] R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim & M. Kang, "An Approach for Preserving Privacy and Protecting Personally Identifiable Information in Cloud Computing," 2010.

[5] D. Chen & H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing, "International Conference on Computer Science and Electronics Engineering, 2012.

[6] S. Pearson, "Privacy, Security and Trust in Cloud Computing," Computer Communications and Networks, Springer, pp. 3-42, 2013.

[7] X. Liang, R. Lu, X. Lin & X.S. Shen, "Ciphertext policy attribute based encryption with efficient revocation, Technical Report, University of Waterloo, 2010.

[8] B.R. Madnani & N. Sreedevi, "Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation," International Journal of Innovative Research in Computer and Communication Engineering, 1(3), 2013.

[9] A. Ansari & C. Bawankar, "Privacy and Data Integrity for secure Cloud Storage," International Conference on Advances in Engineering & Technology – (ICAET-2014), pp. 69-72, 2014.

[10] A.N. Madde, M.J. Joshi, S. Gutte, S. Asawa & P. Jawalkar, "Decentralized Access Control To Secure Data Storage On Clouds," Bimonthly International Journal, ISSN 2347-6680 (E), 2(5&6), pp. 124-128, 2014.

[11] J.P. Resshma & H. Stanly, "Scalable and Secure Data Access Control in Cloud Computing," Proceedings of IRF International Conference, ISBN: 978-93-82702-71-9, 2014.

[12] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," A dissertation, 2011.

[13] S. Musthafa & D.B. Sudarsa, "Patient–Centric Secure Data Sharing Frame Work for Cloud-Based PHR Systems," International Journal of Engineering Science Invention, ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726. 2 (5), pp. 17-26, 2013.