Sub-Sahara African Academic
Research Publications
September, 2020, Editions

JPAS
Journal of Pure and Applied Science
Vol..16, No.9, ISSN 2318-9315

SECURED SHARING OF PERSONAL HEALTH RECORD (PHR) USING ATTRIBUTE BASE ENCRYPTION

***ISHAQ MUHAMMAD; *ABDULRAHMAN ABDULKARIM; *SUBERU YUSUF; **UMAR SAIDU ABASHE; * LELE MOHAMMED**

**Department of Computer Science, the Federal Polytechnic, Bauchi (Nigeria) **Department of Multimedia Technology, Katsina State Institute of Technology and Management, Katsina (Nigeria)*

ABSTRACT

Personal health record (PHR) has e- merged as a patient-centric model of health information exchange. It enables patients to store, share, and access personal health data in centralized way that it can be accessible from anywhere and anytime. One major problem is to manage and secure data from the unauthorized persons. The security schemes are used to protect personal data from public access. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing but 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. Attribute based Encryption is proposed in this work to secure PHR and also provides many functionalities such as accountability, revocation of user, searching over encrypted les, delegation of other user access, searching over encrypted les and multi-authority.

Keywords*: Personal health records; data privacy; fine-grained access control; attribute-based encryption.*

INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control his personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of his medical records and can share his health data with a wide range of users, including healthcare providers, family members and friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed in .While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to expo- sure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. In this paper, we endeavor to study the patient- centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date.

RELATED LITERATURE

Overview

The PHR refers to a representation of health records related to the care of a patient that is managed by the patient (Tang et al., 2006). There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the surge in recent attacks and legal pressure faced by such services. One method for alleviating some of these problems is to store data in encrypted form (Abdulkarim & Souley, 2017). Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at an engrained level.

Attribute-Based Encryption

Attribute-Based Encryption (ABE), is a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that various users who gain proper keys can decrypt. In their work, (Sahai & Waters, 2005) made some initial steps to solving this problem by introducing the concept of Attributed-Based Encryption (ABE). In an ABE system, a user's keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. ABE schemes come in two complimentary forms, namely, Key-Policy ABE (KPABE) schemes and

Cipher text-Policy ABE (CP-ABE) schemes (Bobba et al., 2009). As the name indicates in KP-ABE scheme, attribute policies are associated with keys and data is annotated with attributes (Goyal et al., 2006; Sahai & Waters, 2005). The schematic overview of CP-ABE and KP-ABE is shown in Figures 2.1 and 2.2.

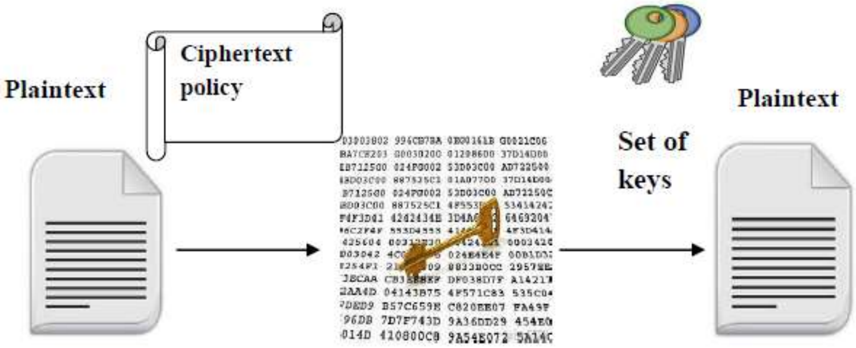

Figure 1 Schematic overview of CP-ABE

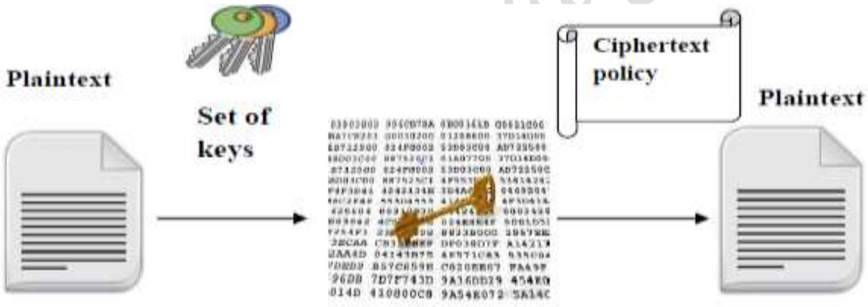

Figure 2 Schematic overview of KP-ABE

Methodology

A Methodology is a structured sets of methods, practices, processes and procedures used to attain (*Master of Project Academy | What is Methodology?*, n.d.). There is no on precise approach to develop a system, every development method has its strength and drawbacks. It depends on the circumstances they did, applied and people who involved in the development activities. Among all the methods, Rational Unified Process methodology was selected to develop task management system to manage hardware and software as it is appropriate for project web based applications. The major concern of this work is to secure user data in the

PHR system during upload or download of data using Attribute-Based Encryption (ABE).

Working Principle of ABE algorithm

The attribute based encryption (ABE) algorithm introduce by (Sahai & Waters, 2005) for access control using public key cryptography aimed to provide scalability, security, flexibility and fine grained access control. Attribute encryption algorithm is the public key encryption that allow user to encrypt and decrypt the message based on user attributes. In ABE algorithm the user secret key and cipher text are related with a set of attributes. A user is able to decrypt the cipher text if and only if the number of attribute verify between the cipher text and user secret key.

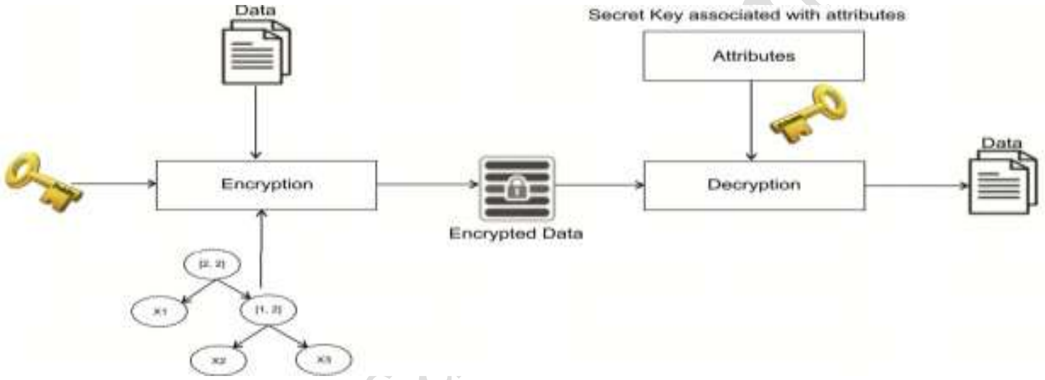

Figure 3 ABE algorithm example

Proposed System Architecture

This work is aimed at providing security when using Personal Health Record system that will secure user data in the cloud using Attribute Base Encryption as discussed above. Personal health records (PHR) allows patients to build lifelong Personal health records. The records can be shared by the patient with any stakeholder interested in those. PHR allows the controlled sharing of application software that is required to view and analyze health records.

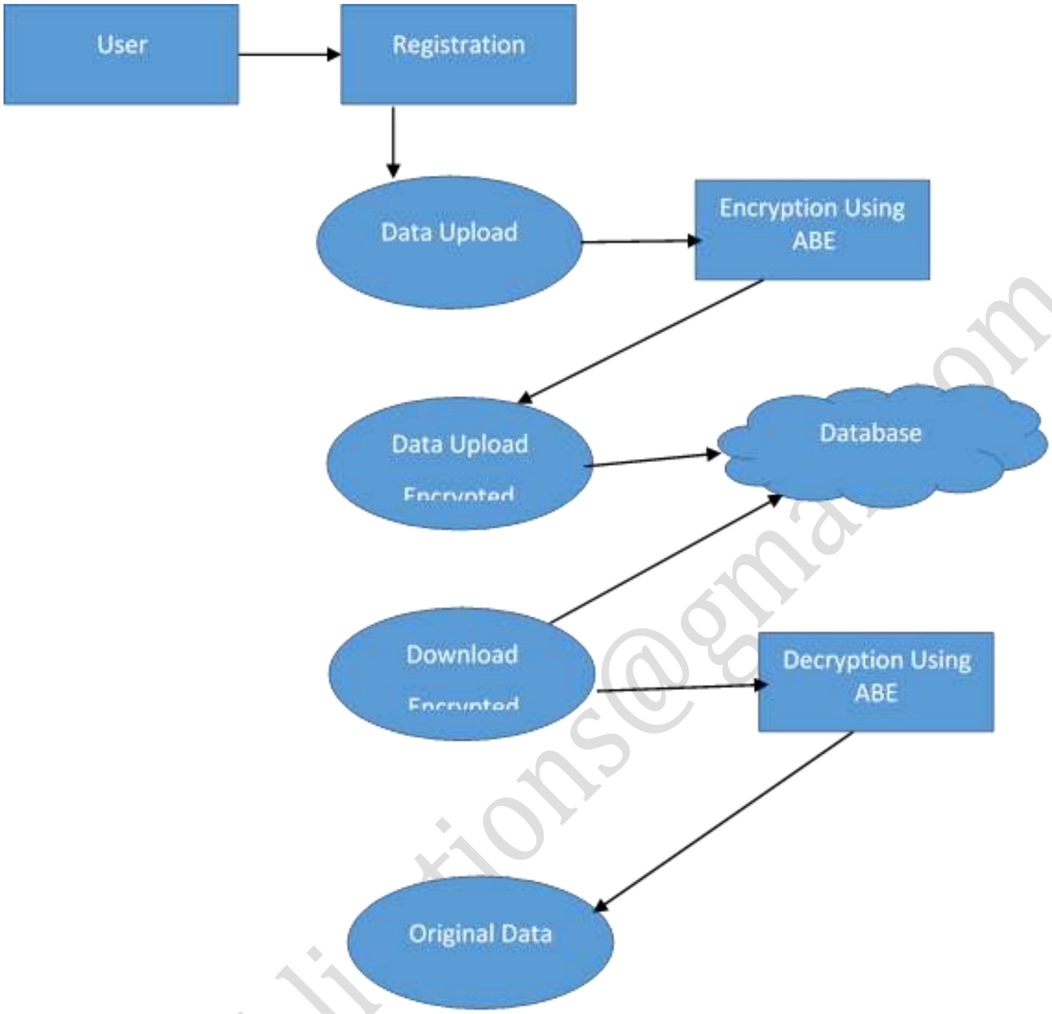

Figure 1 : System Architecture

Proposed ABE Algorithms

In the proposed system, multi-authority CP-ABE is use to provide unique global identity to every user in system that helps to identify misbehaving user of PHR that gives decryption key to other unauthorized user (Maheswari & Gudla, 2017). Our proposed scheme uses the following algorithms;

Setup:

- Input: security parameter λ∈ N total number of Attribute Authority.

- Output: params as system parameters and N number of {public key, private key} pair.

AttKeyGen: run by every Attribute Authorities

- Input: private key of AA, list of attributes and global identity of user for which they created key.
- Output: decryption key according to given attribute list for user with unique identity.

Encrypt: run by PHR owner

- Input: massage and policy for encryption to generate cipher text where policy contains some attribute that are subset of total attribute.
- Output: encrypted data cipher text with respect to access structure.

Decryption: run by PHR user

- Input: cipher text that is encrypted with some access policy and secret key of PHR user according some attributes.
- Output: they gets original message or not on bases of what attributes they have and it's satisfy the access policy that embedded in cipher text or not.

Trace:

- Input: public parameters, cipher text policy
- Output: global identity of misbehaving user

Simulation Tools

The proposed system will be implemented using java programming as language and Net Beans IDE 8.0.2 as the programing environment. A HP lap-top System with Core i (TM) i5-4200U, 2.30GHz CPU and 8GB RAM as hardware requirement will be used as well.

Conclusion and Future Work

This work proposed a technique to protect user data when uploading and downloading the data from the cloud using Attribute Base Encryption as cryptography by transforming the data to unreadable form from unauthorized users in order to achieve a secure communication in the cloud. After the work has been achieved successfully, Steganography and

Cryptography will be combined in the future to provide a high level of security in Personal Health Record (PHR).

References

Abdulkarim, A. I., & Souley, B. (2017). *An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography*. *8*(7), 1512–1517.

Bobba, R., Khurana, H., & Prabhakaran, M. (2009). Attribute-sets: A practically motivated enhancement to attribute-based encryption. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5789 LNCS*, 587–604. https://doi.org/10.1007/978-3-642-04444-1_36

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the ACM Conference on Computer and Communications Security*, 89–98. https://doi.org/10.1145/1180405.1180418

Maheswari, S., & Gudla, U. (2017). Secure sharing of personal health records in Jelastic cloud by attribute based encryption. *2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017*, *7*(1), 1–8. https://doi.org/10.1109/ICACCS.2017.8014725

Master of Project Academy | What is Methodology? (n.d.). Retrieved August 13, 2020, from https://masterofproject.com/blog/3457/what-is-methodology

Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. *Lecture Notes in Computer Science*, *3494*, 457–473. https://doi.org/10.1007/11426639_27

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, *13*(2), 121–126. https://doi.org/10.1197/jamia.M2025