JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Multi-authority Access Control with Anonymous Authentication for Personal Health Record

Bhavyashree R, Assistant Professor, Department of Computer Science
St. Joseph's First Grade College, Jaylakshmipuram, Mysore-570012

Abstract : **The Main aim of this project is to store and share the PHR data in a secure way of using cloud. Here we used to get the PHR data from the data owner like what are the details are need to fix the doctor appointments, that data only enter the owner, this detail will be convert in to a text file. And after this text file will be select and give a input as a Encryption process. Here we will use the Attribute Based encryption, then after complete the Encryption process, we will store the data to the cloud with a permission CSP. After uploading the file, the user get the notification to this appointments. So they will be accept this file and they will download the file with permission of CSP after they get the decryption key from the Central Authority and finally they will decrypt it.**

I. Introduction

In recent years, as an emerging technology, PHR has played a crucial role in data sharing. PHR can store medical records online and be accessed by patients and their doctors anytime, anywhere. However, when data sharing is implemented, PHR also brings problems such as privacy leakage. In order to protect the privacy of patients and enhance the control to their PHR, the fine-grained access control scheme over sharing data based on attribute-based encryption (ABE) is proposed and has been a hot topic at present. ABE defines an access policy through attributes associated with generating the private key or cipher text and only users whose attribute sets satisfy the access policy can access PHR. However, some previous schemes used a single centre to generate keys and authenticate users, which undoubtedly overburdened the system. Multi-authority encryption scheme requiring multiple authorities to jointly generate private keys for users solves such problem. We realized secure and efficient access control in a multi-authority environment, but the user's fuzzy authentication poses a threat to data security. In order to further ensure security, adding a searchable public key encryption scheme to a PHR system was presented and authentication technology was introduced to connect users of medical system to other trusted users. At the same time, some feasible solutions also effectively solve the problem of patient's privacy leakage and the confidentiality of the scheme. In these methods, the user's sensitive information, such as identity and attributes, is hidden during the system interaction.

II. PROPOSED SYSTEM

A PHR can provide convenient data storage and sharing. However, sensitive users' data on cloud devices may be stolen by unauthorized users, which causes serious privacy leakage issues. Patients will lose direct control over their PHRs. Therefore, a PHR system stored in the cloud suffers more external and internal attacks than a paper-based PHR. It is essential to provide a secure, privacy-protected PHR system with fine-grained access control. For example, a data owner defines an access policy, then encrypts a PHR and saves its cipher text to the cloud. A promising approach is to encrypt patients' confidential data to ensure security and privacy before outsourcing it to the cloud. It is worth noting that patients should be able to decide with which users to share their PHRs. As shown in Fig.2, only users who have the corresponding key can access the encrypted PHR. However, current schemes cannot guarantee data confidentiality, cipher textunforgeability or users' privacy in a PHR. First, patients' identities and attributes should not be disclosed during access and authentication. Second, the cipher text encrypted by the data owner should not be tampered with by the untrusted cloud. Third, during encryption and decryption, the amount of calculation on the client side should be minimized

An personal health record is a collection of patients' health related information to allow efficient, consistent and universal sharing of health information. Because of the sensitivity of health related information, providing secure storage and access to PHR is the main challenge in today's PHR systems are personal information protection and electronic documents act for health data are aimed at ensuring sufficient care is given to handling such data.

An increasingly popular approach in managing health data puts users at the centre of such systems and allows users to store and manage access to their own health information. PHR systems enable patients to selectively give access to their health data to healthcare providers and other.

The main contributions within this paper are:

- The PHR framework by combining attribute-based encryption with attribute-based signature to better the trade-off between protecting users' privacy and guaranteeing the data security.
- An anonymous authentication between the cloud and the user is proposed, which guarantees the data integrity in cloud and data cannot be forged. In addition, anonymity of the protocol keeps user's identities not to be exposed during authentication, which achieves the privacy-preserving of users.
- To achieve the lightweight computation, we use offline online technique and outsourcing decryption operations to help with authentication and partial decryption.

A. Advantages

- It will give a result of the problems like use multi-authority attribute-based encryption in a PHR, such as anonymous authentication outsourcing and cipher text enforceability, users and authorities collusion
- The experimental result is high when compared with existing system.
- It will be more secure compared with existing system.

III. LITERATURE SURVEY

A literature review is a text of a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources. Most often associated with academic-oriented literature, such as reviews are found in academic journals, and are not to be confused with book reviews that may also appear in the same publication. Literature reviews are a basis for research in nearly every academic field.

1. Accountable privacy preserving attribute-based framework for authenticated encrypted access in clouds

Author:Sana Belguith&NesrineKaaniche&Maryline Laurent&Abderrazak&Rabah Attia

YEAR:2020

Findings

In this paper, propose an accountable privacy preserving attribute-based framework, called InsPAbAC, that combines attribute-based encryption and attribute-based signature techniques for securely sharing outsourced data contents via public cloud servers. The proposed framework presents several advantages. First, it provides an encrypted access control feature, enforced at the data owner's side, while providing the desired expressiveness of access control policies. Second, Ins-PAbAC preserves users' privacy, relying on an anonymous authentication mechanism, derived from a privacy preserving attribute-based signature scheme that hides the users' identifying information. Furthermore, our proposal introduces an accountable attribute-based signature that enables an inspection authority to reveal the identity of the anonymously-authenticated user if needed. Third, Ins-PAbAC is provably secure, as it is resistant to both curious cloud providers and malicious user's adversaries. Finally, experimental results, built upon OpenStack Swift testbed, point out the applicability of the proposed scheme in real world scenarios.

2. Privacy Preservation for Outsourced Medical Data with Flexible Access Control

Authors: Xingguangzhou1 ,Jianwei liu1 , Qianhong wu1 and Zongyangzhang.

YEAR:2020

Findings

Electronic medical records (EMRs) play an important role in healthcare networks. Since these records always contain considerable sensitive information regarding patients, privacy preservation for the EMR system is critical. Current schemes usually authorize a user to read one's EMR if and only if his/her role satisfies the defined access policy. However, these existing schemes allow an adversary to link patients' identities to their doctors. Therefore, classifications of patients' diseases are leaked without adversaries actually seeing patients' EMRs. To address this problem, we present two anonymous schemes. They not only achieve data confidentiality but also realize anonymity for individuals. The first scheme achieves moderate security, where adversaries choose attack targets before obtaining information from the EMR system. The second scheme achieves full security, where adversaries adaptively choose attack targets after interaction with the EMR system. We provide rigorous proof showing the security and anonymity of our schemes. In addition, we propose an approach in which EMR owners can search for their EMRs in an anonymous system. For a better user experience, we apply the "online/offline" approach to speed up data processing. Experimental results show that the time complexity for key generation and EMR encapsulation can be reduced to milliseconds.

IV. Software requirement specification

A. Functional Requirements

- Data Owner and Data User Login
- PHR Uploading
- Key Generation
- Data Encryption and Upload
- Cloud Server
- Decryption
- Download Healthcare records.

B. Hardware Requirements:

• Processor	: Intel Core i5
• Hard Disk	: 200 GB
• Monitor	: 18' LED color
• Mouse	: DELL.
• Keyboard	: 110 keys enhanced
• RAM	: 3GB

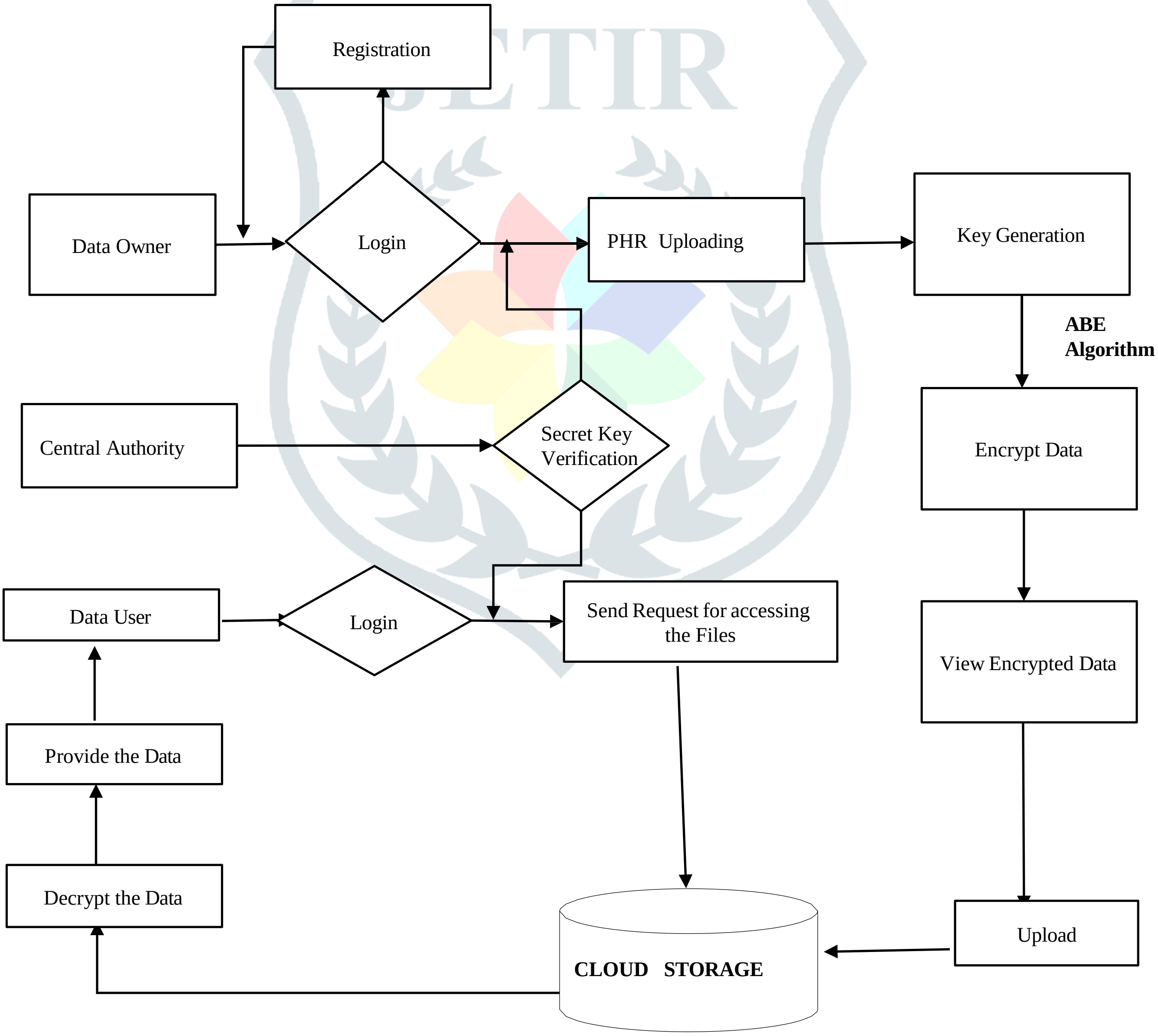
C. Software Requirements

•	Operating System	: Windows 7 / 8 / 10
•	Language Used	: Java
•	Database	: My SQL
•	User Interface Design	: JFrame

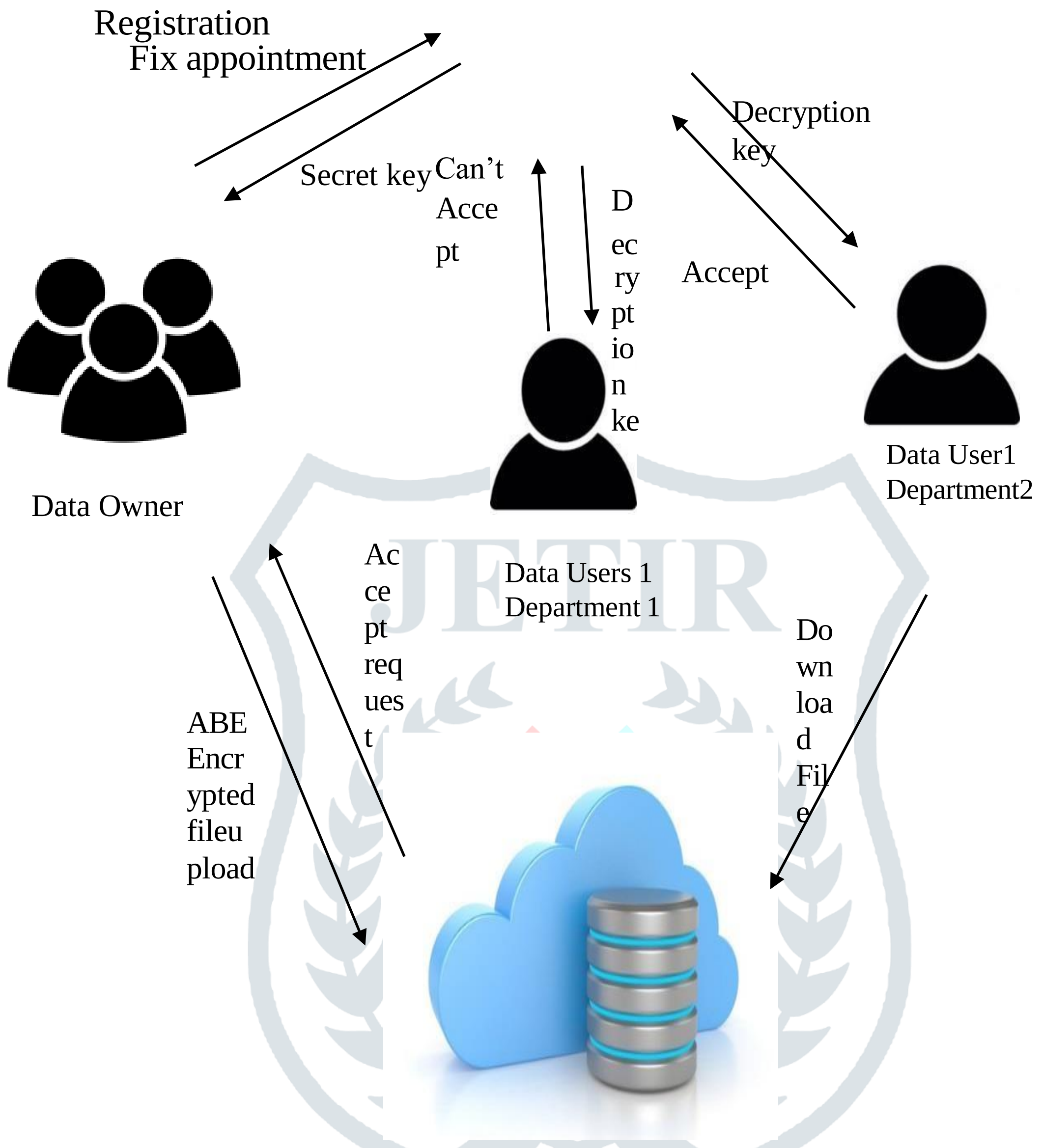
V. SYSTEM DESIGN

a) Flow Diagram

A flowchart is a type of diagram that represents a workflow or process. A flowchart can also be defined as a diagrammatic representation of an algorithm, a step-by-step approach to solving a task. The flowchart shows the steps as boxes of various kinds, and their order by connecting the boxes with arrows. Any drawing program can be used to create flowchart diagrams, but these will have no underlying data model to share data with databases or other programs such as project management systems or spread sheet. Many software packages exist that can create flowcharts automatically, either directly from a programming language source code, or from a flowchart description language. There are several applications and visual programming languages21 that use flowcharts to represent and execute programs. Generally these are used as teaching tools for beginner students. A flowchart is described as "cross-functional"' when the chart is divided into different vertical or horizontal parts, to describe the control of different organizational units. A symbol appearing in a particular part is within the control of that organizational unit. A cross-functional flowchart allows the author to correctly locate the responsibility for performing an action or making a decision, and to show the responsibility of each organizational unit for different parts of a single process.



b) SYSTEM ARCHITECTURE



VI. Conclusion

In this Process, we proposed as a secure sharing framework based on multiauthority attribute-based encryption for PHRS system. In this scheme, the identity and attributes of the user are hidden and known only to the trusted central authority. To prevent cloud server from tampering with cipher text or spoofing end users, an anonymous authentication based on attribute-based signature is proposed. In the whole access-control process, only authorized users can access and obtain messages. And the data owner will be store their PHR data in Cloud in the encryption format. The data use to Encrypt the ABE Algorithm and the data user wants to download this file must verified by the central authority and CSP and after they will be decrypt the file.

VII. Future Enhancement

- As a future work, it would be interesting to modify or advanced algorithm are used to encryption process and store more securely in cloud .
- In the future, we should like to combine different algorithms and evloluate the process one to another like compare the accuracy and security of those algorithms.
- Future extension of this article includes extending the proposed model to more and more efficient process to implement in online as such as an real-time process also.

VIII. REFERENCES

- L. Tbraimi, M. Asim, M. Petkovi, “Secure management of personal health records by applying attribute-based encryption, In Proceeding of the International Workshop on Wearable Micro and Nano Technologies for Personalized Health(pHealth),” in Oslo, Norway, Jun.2009, pp.71– 74.

- J. Akinyele, M. Pagano, M. D. Green, “Securing electronic medical records using attribute-based encryption on mobile devices,” in Proceeding of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Oct.2011, pp.75–86.

- S. Narayan, M. Gagne´, R. Safavi-Naini, “Privacy preserving EHR system using attribute-based infrastructure,” in proceeding of the ACM Cloud Computing Security Workshop, Chicago, Oct.2010, pp.47–52.

- J. Lai, R. H. Deng, Y. Li, “Fully secure ciphertext-policy hiding CPABE,” in Proceedings of the International Conference on Information Security Practice and Experience, Jun.2011, pp.24–39.

- J. Sun, Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” in IEEE Trans.ParallelDistrib.Syst., Jun.2009, pp.754–764.

- M. Li, S. Yu, Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption,” in IEEE Trans.ParallelDistrib.Syst., 2013, pp.131–143.