International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Privacy Preserving in Distributed Computation in Collaborative System

Ms. AnkitaBonde and Prof.Dr Rajesh Ingle

Department of Computer Engineering, Pune Institute of Computer Technology, Savitribai Phule Pune University, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Recently the databases are not in central location they are mostly distributed even geographically. Protecting the privacy over massive data that were store in different sites or in distributed systems are very important these days, because it will provoke serious consequences if the sensitive data get released without considering mechanism to protect this sensitive information. To overcome on the present issue the improvement can be done by separating patients identity from their medical data. The delicate data which needs to be uploaded to the system with the confidentiality constraints include major procedure namely data hiding. Privacy preserving distributed analysis of community health research data can be achieved by combining cryptography, suitable algorithms, constrain specification and enforcement.

Keywords*: Privacy, Distributed databases, Security, integrity, and protection, Database management, Data privacy, Collaborative data publishing.*

Introduction

In distributed system medical domains are increasing worldwide. There are plenty of awareness act is established to spread the medical healthcare high quality treatments. In healthcare- networks, the personal information of healthcare data is stored or kept at one place from where the data can be used to examine the patient. Some hospitals have their own storage. The electronic record system is an improvement to the traditional system, it improves healthcare outcomes for patients by minimizing clinical errors and cost. In this paper main aim to improve privacy of health data by using distributed attribute and hiding the personal details of the respective patients. The data storage and processing of system are distributed to maintain the privacy of the patient's identity from their healthcare data, separate the patient's identity from medical data and split the functionality.

Literature Survey

1.Paper name: Privacy-Preserving Distributed Information Sharing.
Author: Lea Kissner.
In many significant applications, a collection of equally distrustful parties must portion information, without cooperating their privacy. Currently, these requests are often performed by using some form of important third party (TTP); this TTP obtains all players' inputs, computes the desired function, and revenues the result. However, the level of trust that must be located in such a TTP is often inadvisable, unwanted, or even illegal. In order to a brand many applications applied and secure, we must eliminate the TTP, replacing it with well-organized protocols for privacypreserving distributed material sharing. Thus, in this thesis we explore techniques for privacy-preserving dispersed information sharing are effectual, secure, and applicable to many circumstances. As an example of privacy-preserving information distribution, we propose well-organized techniques for privacy-preserving processes on multi sets. By structure outline of multi-set procedures, employing the precise possessions of polynomials, we enterprise efficient, safe, and composable tactics to enable privacy-preserving cunning of the union, joining, and element discount procedures. We apply these techniques to a wide range of applied problems, including the Set Connection, OverThreshold Set-Union, Cardinality Set-Intersection, and Threshold Set-Union glitches. Additionally, the problem of decisive Subset relations, and even use our techniques to evaluate CNF Boolean formulations.
The projected system overwhelms the higher than restraint by preparation of WSN substructure for multiple weather applications maltreatment virtual device and overlap idea. Watching weather material and providing SaaS and social network disaster

warnings supported call ID3 method and supply cloud verification mistreatment secure shell. These factors recover and supply prime quality tragedy alters to users and weather forecasters at low cost.

2. Paper name: Preserving Privacy in Distributed Systems. **Author:** Yuriy Brun and Nenad Medvidovic, Member, IEEE Computer Society.
Here also with reference to the previous paper the s-tiles method is used for prediction of data which is from authorize network or from the unauthorized network. Once it detected it the homomorphic encryption algorithm is used to give a authorization to the data which belong to the patients health record. The personal data of the patients are stored in the encrypted part so that it can not reveal the personal information to the unauthorized person. The decrypted part of the data kept the information as it is and it will reveal to the belonging person only.
3.Paper name: Distributed Privacy Preserving Data Collection
Author:**MontherAldwairi, Ali Alwahedi .**
In this distributed data preserving data is a huge problem. Here in this paper the confidentiality of a data can be preserved from the untrusted party. The untrusted parties try to collect data which it will further used to dominate the patient. To keep it safe multi attribute function is introduced in this paper which have two factor one is sensitive data and the other one is unsensitive data. Sensitive data carries the
In this distributed data preserving data is a huge problem. Here in this paper the confidentiality of a data can be preserved from the untrusted party. The untrusted parties try to collect data which it will further used to dominate the patient. To keep it safe multi attribute function is introduced in this paper which have two factor one is sensitive data and the other one is unsensitive data. Sensitive data carries the information of persons particular disease from he-she suffering.

Challenges & Privacy Concerns

The following is a list of challenges that exist within the healthcare landscape despite the benefits of the of electronic health records:
1) Patient's health records exist in multiple locations which results in:

a) Physicians being unable to have a holistic view of the patients' prior or current treatments

b) Data silos result in sub-optimal targeted treatment and population management.

2) Privacy & EHR Access Challenges include:

a) Patients having little control over the sharing of their health data: there is a growing demand for consumer mediation and control.

b) Healthcare providers, clearinghouses and insurance providers process/store patient data and claims in centralized locations: a patient's privacy is completely violated when an one of these entities is compromised.

3) Healthcare and insurance providers use different formats for the EHRs and insurance claims forms. These formats depend on the vendors selected healthcare providers.

Propose Methodology

Registering Patient & Uploading Data

In order to make use of the distributed electronic health record a patient must first register. Registration involves the patient personal details such as name, age, contact details, etc. Once patient registered to the portal all details will automatically save to EHR.
At another level doctor also need to register for the same portal with the corresponding details.
Processing & Data Access Goals

Following list shows the processing and data access goals:

1) Patient can access data from any location 2) Doctor must be able to access patient's medical
Data history and other information

Design & Privacy Assumptions

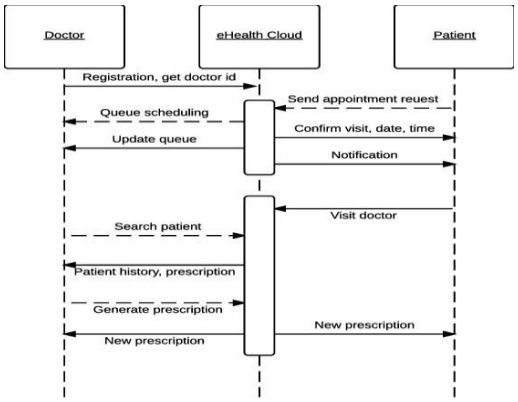
The following shows the assumptions for work:

1) Healthcare providers are trusted not to disclose any information because of strict regulations.
2) A patient's personal devices and personal information (e.g. mobile phone,name) are remain secured. 3) Data partitioning can be done to prevent privacy.

Privacy Method a) Digital Envelope

A digital envelope is a random number only known by the owner of private data used to hide the private data. Sender encrypt the data with a symmetric cipher using a session key. Then, sender encrypts its session key with the help of receiver's public key by using an asymmetric cipher. The encrypted key and the encrypted data are sent to the receiver, who is the only one that can decrypt a session key with his private key and use the decrypted key for decrypting the data.

b) RSA Public-Key Cryptographic Algorithm
A client (for ehr browser) sends his\her public key to the server and requests for some data. The server encrypts the data using client's public key and then sends the encrypted data. Client receives the data and then decrypts the data. Since there is asymmetric, no one rather than browser can able to decrypt the data even if a other party has a public key of browser.



A Scheme Providing Strong Anonymity

In the following, we propose a solution that provides strong anonymity. Our scheme follows closely the lines of the previous scheme, yet overcomes its limitations by the following main ideas:

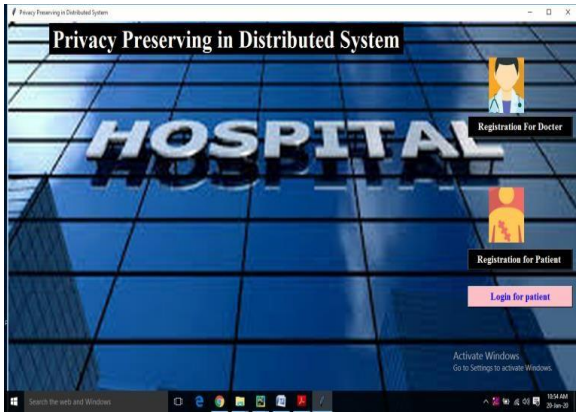
In the previous scheme, the data collector not only collects the data, but also takes on the role of the recovery authority and data analysts. We factor these specific tasks out of the data collector, and assign them to the corresponding entities. This is essential to establish strong anonymity.

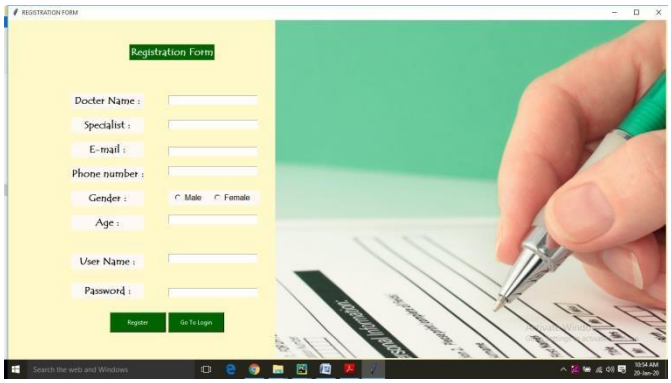
The previous scheme exported data directly from the data collector's database. We use a special export protocol, which anonymizes these records for every export, there by making it harder for two data analysts to merge their sets and augment their respective views on individual medical histories.

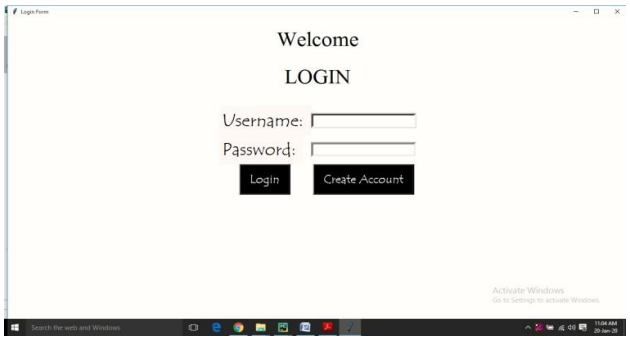
The previous scheme did not authenticate sources. We base our system on a public key infrastructure that allows us to authenticate all involved entities. This way, our scheme guarantees integrity of the data.

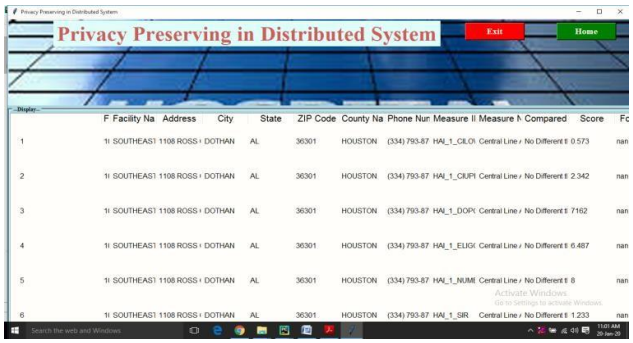
Results and Discussion

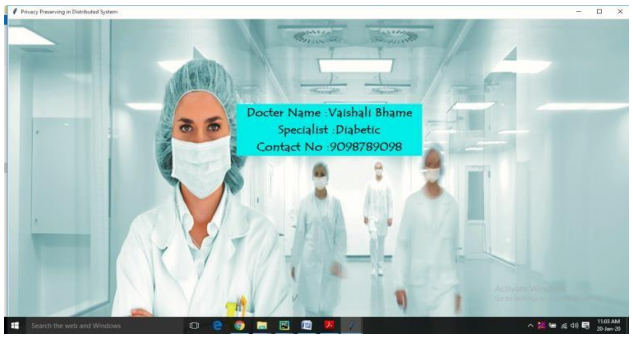
The system is aims are to provide confidentiality in the distributed data. To design a method which allows the sharing of data amongst all participants while at the same time values of the qualities remains private. The propose system are develop using python and pycharm .The pycharm for the backend coding, It is used for give authentication and authorization to patient and Doctor.











Conclusion

In this paper, we focus on confidentiality in Big Data which is related to the medical healthcare. The privacy of the data can be maintained and the valid suggestion is provided to the patients without reveling personal data. In future works, we will come with more privacy related aspect and some other implementations.