www.ThePharmaJournal.com

The Pharma Innovation

ISSN (E): 2277- 7695
ISSN (P): 2349-8242
NAAS Rating 2017: 5.03
TPI 2017; 6(10): 408-411
© 2017 TPI
www.thepharmajournal.com
Received: 05-08-2017
Accepted: 06-09-2017

Ishwarya MV
Research Scholar, HITS,
Assistant Professor, CSE
Department Sri Sairam
Engineering College,
West Tambaram, Tamil Nadu,
India

Saptha Maaleekaa S
4th year CSE Department,
Sri Sairam Engineering College,
West Tambaram, Tamil Nadu,
India

Swetha G
4th year CSE Department,
Sri Sairam Engineering College,
West Tambaram, Tamil Nadu,
India

Anu Grahaa R
4th year CSE Department,
Sri Sairam Engineering College,
West Tambaram, Tamil Nadu,
India

Correspondence
Ishwarya MV
Research Scholar, HITS,
Assistant Professor, CSE
Department Sri Sairam
Engineering College,
West Tambaram, Tamil Nadu,
India

Secure communication on cloud for health care monitoring

Ishwarya MV, Saptha Maaleekaa S, Swetha G and Anu Grahaa R

Abstract
In prior, stages data investigation and security were the primary factors for the improvement of the efficacy and seclusion. Efficacy plays a dominant role in monitoring the health. For the preservation of database documents the algorithms should be effective. The important problem on information prediction and list of patients and privacy preserving health care monitoring system to protect the privacy of the involved clients and their data health care investigation poses a consistent challenge to doctors and is the area of research in which trillions of amounts are being spent by all countries. Different mining algorithms have been applied on the voluminous health records to aid decision making process. In our paper, the patient health conditions and the details of the patients are analyzed and sliced using a new slicing technique called Shingle slicing. Patient analysis report is generated and it is monitored by the doctors and other users and the details of the patients are sliced according to the users.

Keywords: Privacy preservation, Data mining, Shingle slicing

1. Introduction

In the growing technology, peculiar information is used in most of the aspects. Examples are newsletter, banking, website registration, patients detail in hospital management database and goes on. More databases are created daily. For this process, most management goes for data mining. There may be a risk of private information getting exposed. For Example consider the hospital management database, where it contains a column "birth date". When analyzing the database, the age of the patient should not be revealed. In this, we implement some algorithms and the birth date gets manipulated (for example 19**). In this process, the exact patient age is kept secret.

2. Related Works: Our works are related to the security issues and privacy proficiency and cloud based instruction avoidance of healthcare records duplication.

2.1 cloud assisted privacy proficiency

The emerging cloud technologies for interconnected medical devices had played a vital role in the upcoming-generation healthcare industries for privacy patient care. As the number of increasing in inpatient and outpatient people, there is an urgent need for a real-time health monitoring environment for preventing the data firmly. So that the third person can't see the required details of patients' healthcare data.

These documents were sold as commodities to various companies by other person. The individual can sell documents from where the data is stored by using cloud. The individual privacy gets affected. The documents should be anonymized to produce without the privacy getting affected. The data should be anonymized before introducing. The privacy model is shown in fig 1.

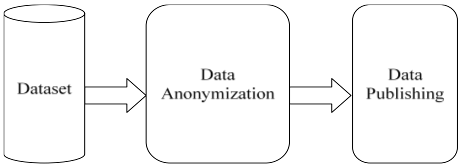


Fig 1: Privacy Model

The main motive behind this paper is to produce the information for different purposes without the individual’s privacy getting affected. Sensitive Attributes are in the sensitive information to a particular person where one must avoid disclosure and Non-Sensitive Attributes includes all attributes that are not considered above.

3. Existing System

For databases which are divided in a vertical manner there is a privacy preserving solution of frequent item set mining which is cloud aided. In addition to this there is another method where there is also a privacy preserving method for data mining techniques like association. Both the above mentioned methods are used by people who outsource their encrypted data to miners and fear of privacy breach.

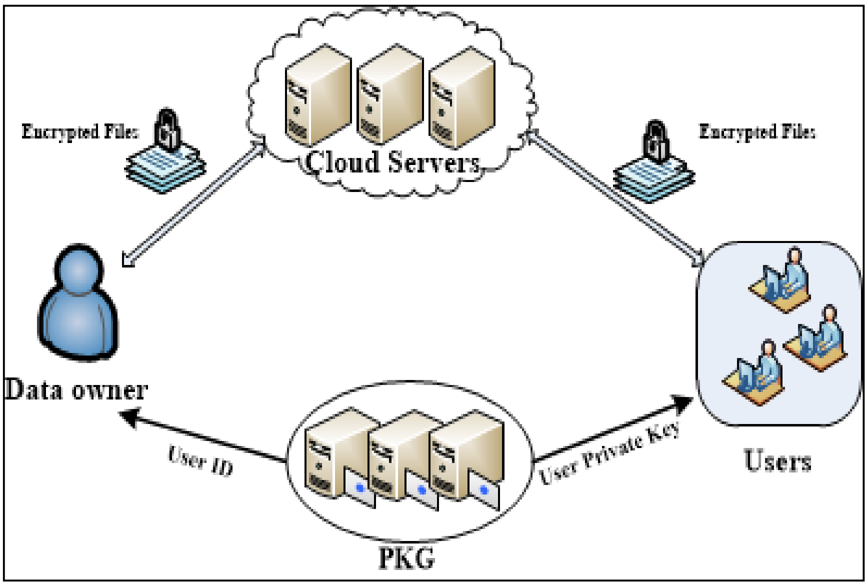


Fig 2: System model of outsourced data mining on joint database.

3.1 Disadvantages of Existing System

In high-dimensional data, the considerable amount of information is lost in Generalization for k-anonymity losses. The membership disclosure is not prevented in bucketization. As the QI values are produced in the original forms in bucketization, the data is not secured.

Table 1: Illustrates the Existing Slicing Technique

NAME, AGE	ZIPCODE, AGE
Babe,36	(14589, 36)
Babe,22	(14586, 22)
Cherry,39	(14587, 42)
Frank,42	(14588, 56)
Frank,33	(145587, 33)
Mark,56	(14788, 56)
Olga,60	(14566, 60)

The Table has the following tuple where (Babe, 22) can have 4 possible ways to correlate with. Therefore, a set of 4 tuple can have 16 possible ways to correlate with the other tuple.

4. Proposed system

In proposed system we introduced novel concept “Shingle slicing”. When compared to generalization the data utility is better in this type (shingle slicing). Attribute correlations are protected with the new technique than bucketization. High-dimensional data can also be handled. Attribute disclosure is prevented using Shingle slicing. All stored patient information have two category, one for search index another privacy table. Search index contain only searchable keywords, so that encryption keys are common to all patient. Privacy table are maintained by network admin that contain unique encryption keys for all patient Those key only provide authorized request, that means patient can set instruction for access our key, instruction have any type there may be Ip address or unique id. We develop web application for outpatient interface, using this application doctor and patient can register the provided details in the application. Patient and the doctor can view our prescription information from our web application.

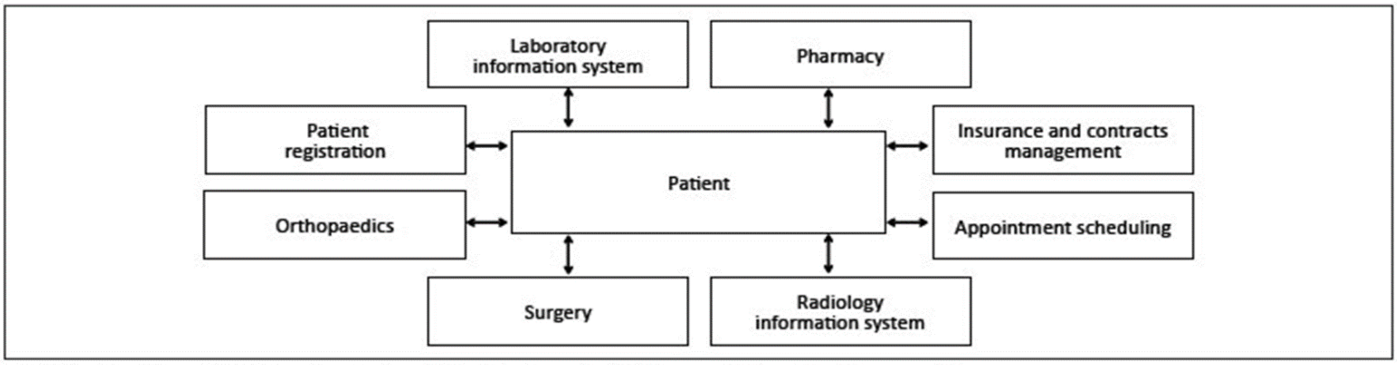

Laboratory information system
Pharmacy
Patient registration
Insurance and contracts management
Patient
Orthopaedics
Appointment scheduling
Surgery
Radiology information system

FIGURE 1: A depiction of the information sharing relationships (ecosystem) between patients and health-care services.

Fig 3: System architecture

5. Module Description: In this software we have developed some forms. The brief description about them is as follows.

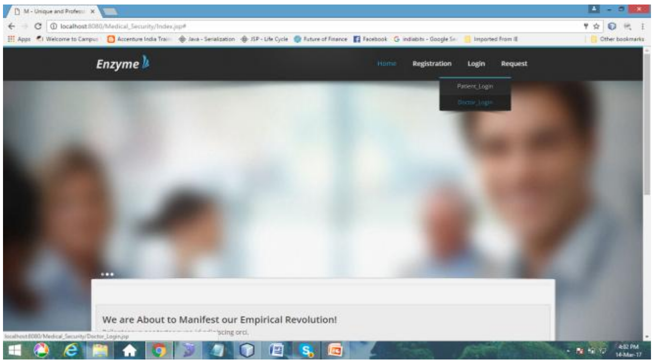
5.1. Profile Creation.

For each person a profile is created containing his identity information. A profile is nothing but those information that can distinctly refer to a person. But this data can have privacy breach by systems using and storing the persons' information. For the registration of user have to submit their details. Then the trust authority creates the database for patients. After the registration, user obtains a username and password. Every information stores in the database of MYSQL server.

5.2. Login Details: A user logs in using certain details, and upon authentication he is granted access to some confidential information according to his access rights.

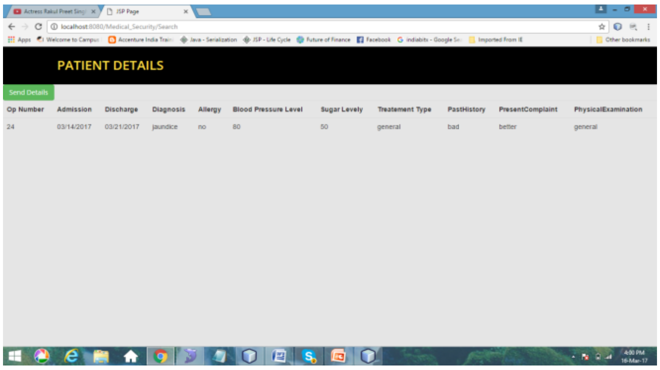
Sub modules: [a].Doctor login [b].Patient Login

Data base
Login
View details



We are About to Manifest our Empirical Revolution!

5.3 Shingle Slicing Technique: In this model, system will provide the information depends on the role of access. Data set will be same for all the users, but it will change to provide to the user based on authority level. Clinician and Customer they are the major roles played here. Data set will be sliced by the authority and role of the user. When Clinician want to see the medical record, first it will check the specialization, based on it will provide the relevant information. If patient want to be search, it will provide the data depends on his/her authority level. Data always in term of slicing, every time user want to be given a right key pair to decrypts the data.

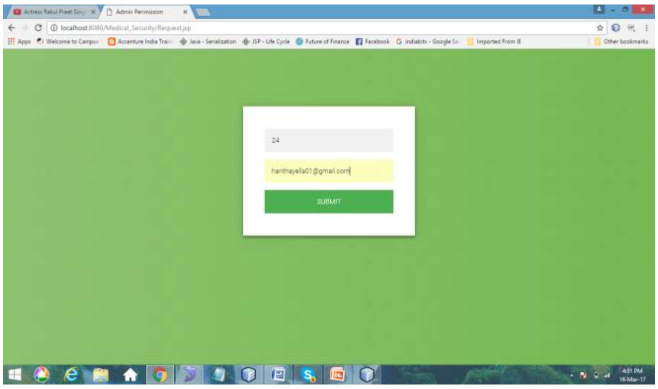

Actress Rakul Preet Singh
JSP Page
localhost:8080/Medical_Security/Search
Send Details
4:00 PM
14-Mar-17

PATIENT DETAILS

Op Number	Admission	Discharge	Diagnosis	Allergy	Blood Pressure Level	Sugar Levely	Treatement Type	PastHistory	PresentComplaint	PhysicalExamination
24	03/14/2017	03/21/2017	jaundice	no	80	50	general	bad	better	general

5.4. Otp Request: A one-time password (OTP) is a kind of password and it can be used by the user to login to the system only once.

- OTPs ensure that even if the password is known to unauthenticated user it cannot be used to log in to the system as it is valid only once for logging in.

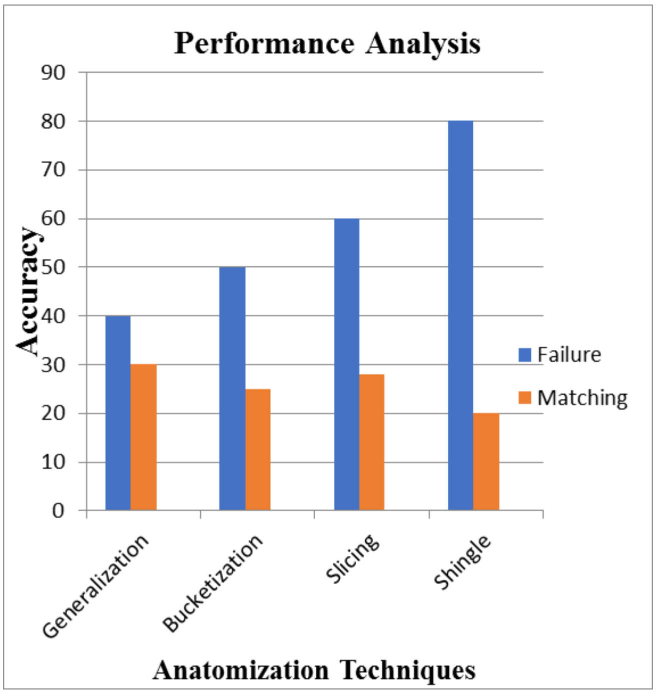

Actress Rakul Preet Singh
Admin Permission
localhost:8080/Medical_Security/Request.jsp
SUBMIT
4:01 PM
14-Mar-17

24

harithayella01@gmail.com

6. Performance Analysis

To determine the definitiveness of data the better accuracy is shown by Shingle Slicing Techniques which executes more when compared to other techniques.



7. Conclusion

To realize our solutions, realize our solutions, the concept of Shingle Slicing overcomes the drawback of overlapping slicing thus by improving the privacy of data. Shingle-slicing enhances the ability to hold huge information. This slicing enhances data utility as well preserves privacy threat and it does not divide quasi and sensitive attributes. This technique have potential usage in other secure computation applications, such as secure data entirety, beyond the data mining solutions described in this paper.

8. References

1. Privacy-Preservation-Outsourced Association Rule Mining on Vertically Partitioned Databases Lichun Li, Rongxing Lu, Senior Member, IEEE, Kim-Kwang Raymond Choo, Senior Member, IEEE, Anwitaman Datta, and Jun Shao, IEEE Transactions On Information Forensics And Security, 2016; 11(8).

2. A Secure Model for Medical Data Sharing. Wong Kok Seng1,1,Myung Ho Kim1, Rosli Besar 2, Fazly Salleh2 1Department of Computer, Soongsil University, 156-743 Sangdo-dong, Dongjak-Gu, Seoul, Korea 2 Faculty of Engineering, Multimedia University, Jalan Ayer Keroh Lama, 75450 Bukit Beruang Melaka Malaysia 1 {kswong, kmh}@ssu.ac.kr, 2 {rosli, fazly.salleh.abas } @mmu.edu.my; In International Journal of Database Theory and Application, 2014.
3. Privacy Preserving Data Mining In Health Care Applications First A. Dr. D. Aruna Kumari, Ph.D.; Second B. Ch.Mounika, Student, Department Of ECM, K L University, chittiprolumounika@gmail.com; Third C. A. Sai Kavya, Student, Department Of ECM, K L University, akaveetikavya@gmail.com; Fourth D. M. Anvesh Babu, Student, Department Of ECM, K L University; In International Journal of Advanced Computer Technology (IJACT), 2013.
4. Hiding Individual Detail In Publishing Data Using Overlapping Slicing1 Sucheta Nikam, 2rajesh Bhise 1ME Student, 2Asst. Professor, Department Computer Engineering, PHCET E-mail: 1 snikam@mes.ac.in, 2 rbhise@mes.ac.in, 2012.
5. Privacy preserving association rule mining in vertically partitioned data P. Kamakshi, Dr. A. Vinaya Babu Journal Of Computing, 2010; 2(4). April ISSN 2151-9617.
6. Yu H, Vaidya J, Jiang X. Privacy preserving SVM Classification on vertically partitioned data PAKDD conference, 2006.
7. Agrawal R, Srikanth R. Information sharing across private databases", In Proc.of ACM SIGMOD, 2003.
8. Kargupta H, Datta S, Wang Q, Sivakumar K. On the privacy preserving properties of random data perturbation techniques", In Proceedings of the 3rd IEEE International Conference on Data Mining, Melbourne, Florida, 2003, 99-106.
9. Kargupta H, Datta S, Wang Q, Sivakumar K. On the privacy preserving properties of random data perturbation techniques, Proc. of Intl. Conf. on Data Mining (ICDM), 2003.
10. Agrawal D, Aggarwal CC. On the Design and Quantification of Privacy Preserving Data mining algorithms. ACMPODS Conference, 2002.