ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Privacy and Confidentiality Issues in Healthcare Databases

Dr. P.Kamakshi

Professor, Department of I.T., Kakatiya Institute of Technology and Science, Warangal, India

ABSTRACT: With rapid development in technology, internet and efficient uses of computers, huge amount of information is regularly collected and shared by different users and organizations. It is a great challenge to protect database and maintain privacy and confidentiality of individual records. Especially in healthcare system which contains huge amounts of personal information about patient, patient treatment information needs privacy protection. It is the basic need to preserve privacy and confidentiality about relationship and association between patient and physician. The threat to privacy is more in situations where there is vast amount of personal and financial transaction information is available. Violation of privacy, confidentiality protection and security may cause numerous problems to a patient like social humiliation, impairment in their social and economic status. This paper focus on various privacy issues related to clinical database and possible ways to protect the privacy of patient information available in a healthcare database from malicious people.

KEYWORDS: Privacy; sensitive information; clinical database.

I. INTRODUCTION

Healthcare information systems provide numerous benefits to society. At the same time the users of such database must be warned and precautionary measures must be implemented so that there should not be any exploitation and use of such useful information for personal benefit at the cost of patient privacy. Confidentiality maintenance and protection of healthcare databases must be given highest priority. Health information system keeps the data regarding the past history of a patient [1] and such information is valuable and must be stored as secret document over a long period of time. There should be constant implementation of privacy preserving techniques to protect such electronic data records in healthcare system. Any leakage of sensitive information available in medical records creates threat to clients and patients who are part of health information system. Strong protection mechanism must be implemented to protect these medical records from data losses. Such protection mechanism provides security and confidence to a patient. Patient and client must be advised and proper guidelines should be provided to get benefit and efficient utilization from medical databases. Different parameters like the devices which collects medical data of patient, printed documents etc. should also be considered while providing privacy protection to medical records.

Two major qualities which need immense protection in healthcare databases are privacy and confidentiality.

II. RELATED WORK

In [3] the author expressed that valuable data resource holder like healthcare system, banks etc. have huge collection of e-records which can also be used and shared by researchers for research purpose. But the important thing here is that such database also includes sensitive information which personal specific. When the data holder releases such information to outside world for the benefit of the society, the data holder cannot guarantee the privacy protection of sensitive information related to a patient or financial information related to a customer. The individuals can be re-identified. This paper provides various anonymization techniques to provide security to e-data records.

In [6] the author focus on the need of protection required for e-data when large amount of data is available in the database records. This paper provides the techniques to provide computer security mechanism which protects the electronic data related to a patient disease or client's financial transaction. The suggested techniques e-data from intruders from malicious use and deteriorations of data.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

III. PRIVACY AND CONFIDENTIALITY

Privacy is generally considered as individual right to control the access of personal information. Any information which is personally identifiable is called personal information. A person considers information or something as private when it is really very special and sensitive to him. Such private and personal information needs protection of privacy, interference and interruption from an intruder. One important aspect of privacy [3]is the right to control information about oneself. For an individual or group, it is the ability to seclude themselves or information selectively. Privacy is treated as right of an individual to implement control over personal information to give consent or withhold, use or dissemination of information. The concept of consent is related to the right to privacy.

One of the main responsibilities in medical database is to maintain Confidentiality. It is the duty of healthcare system database provider to keep the patient's personal health information as confidential unless an approval is given by the patient to publicize the information. Generally the patients share their health problems and personal information with doctors and such information are kept as record in healthcare database. It is very important to protect the confidentiality of such information, otherwise the trust of patient on physician and healthcare system will be diminished. Once the confidence fade, the patients will not like to share sensitive information, which in turn will cause negative impact on their care. Hence it is very important to create a trusted environment showing importance to patient privacy which will encourage the patient to be free and honest to share the information during their interaction with doctor and visit to healthcare centre. The patient must be assured that without their consent information related to their medical treatment will not be disclosed to family or any outsider.

IV. PRIVACY VIOLATION IN HEALTHCARE DATABASES

In clinical database the information stored in the form of records is the detailed treatment information which a patient has revealed to hospital or doctor based on trust, expecting that his/her information will not be revealed to others without their consent. Though sharing of such information has potential advantages to the public, government and researchers, there is as an immense need to keep such personal information private. Emerging medical treatments and medical research essentially requires the information about patient disease, treatment and various health measures taken. But, still there should due to illicit leakage or disclosure of such collected information.

Now the question is how to protect sensitive information available in patient records in healthcare databases and find various facts which violate privacy of clinical database.

A. *Causes of privacy violations:*

Following are different reasons of privacy violations in healthcare database:

- Sometimes people submit health related queries and their personal details through social networking sites. Intruders intercept such information and link it with other databases and utilize it for their personal benefit and immoral purposes without the knowledge of actual owner.
- Doctors during the interaction with patients collect past history of a patient to understand the disease in a better way and analyze such information it for better care and improved treatment. During interaction with doctors, patients also give identifiable information to healthcare centers regarding the treatment, drugs and their positive and adverse affects. Such medical database records are not only accessed by the doctors but are also accessed by many organizations like researchers, pharmaceutical companies to improve research in medicines. Many other organizations also access the healthcare database without the permission of patient.

When such information is misused by outsiders and unauthorized persons, patients have to face the negative impacts like privacy violation, employment problem, societal problems etc. Majority of the patient feel anxious about the disclosure of their treatment and past health information and refuse to reveal information further. Patients also deny for further diagnosis and tests. People try to change their regular activities and pretend in other way to protect privacy of their health information.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Ways to protect medical health database

Development in technology brought lot of improvement in Healthcare system. Today automated tools are used to coordinate the patient activities, their requirements for better care. Patient information is stored in the form of electronic records and is used to provide easy access to their health information. It is an uncomplicated method to make everyone comfortable and better informed about patient's health. Inspite of several benefits of health records, there are many queries regarding the privacy of health information which is considered as sensitive issue. The main anxiety of people is to ensure that their information should not be lost, theft, compromised or misused.

The possible ways to protect the privacy of healthcare database are:

- ***To obtain prior consent of patient***

One of major source of research area is electronic health records which stores enormous amount of patient related information. One solution to protect the privacy of patient information is to take the patient consent before the data is disclosed for any application or research. But acquiring approval from patient is challenging task. There may be negative effect on research and research outcome as patients may not come forward to give consent freely to do research on their personal and sensitive information. Further, because of large population it is not convenient and practical to collect the consent from individual patient. Extra time is required to spend for consent collection from large number of patients before performing research.

- ***De-identification***

The data in the electronic health records in clinical database can be used for research purpose or by government organizations in the form of consolidated reports for analysis purpose. Such consolidated reports provide valuable information to government for better care and providing better facilities to the population. Such records also contain sensitive information which is very private to a patient. To protect the privacy of the patient, the data curator who discloses the information must de-identify the sensitive information or personally identifiable data. The main anxiety of data curator is to identify various risks that can be initiated by an opponent to re-identify the original information. Before disseminating the information, Data curator de-identify the information by removing few variables in a given set of variables and get the authorization on data sharing document from the patient as well as the user of data like researchers or organizations.

Though the primary attribute like SSN is not disclosed in the disseminated information, an opponent can identify an individual by grouping few attributes information like place, age etc. Thus an opponent can easily re-identify the person as well as information about his/her diagnosis. In spite of various actions to de-identify health records, it is possible to re-identify the actual concerned person by means of linking the attribute information of separate databases like voter IDs, hospital transaction records, loan information in bank, insurance, etc.

Another possibility of de-identification is to present the details in aggregate from at higher level of [2]generalization.. Generalization lessens the accuracy of the available information. As an example, date of birth can be represented in the form of year of birth or individual age can be represented as a group with an interval of 10 years.Removal of many identifiers in a record and disclosing the information in aggregate form may provide the confidentiality, but this may not be very useful for research purpose where the minute details are also required.

- ***Cryptography***

Another way to protect the details of patient in healthcare database is by sharing the information in cipher form. Data encryption helps the healthcare provider to safeguard the sensitive health information stored in the electronic format.

Health care organization can protect the sensitive files from unauthorized person by encrypting the files. The database files are encrypted in the server using either software or hardware techniques .The files can be decrypted by only the administrator or authorized persons. Another way to protect the health records is to encrypt only the columns which are considered as most sensitive. The data in particular columns are completely scrambled and can be decrypted only by authorized users and unauthorized users can view only modified information which is not useful for analysis purpose.

The encryption process can also be applied on data by application before storing the data in database. Any queries submitted to databases return the result in the encrypted form and can be decrypted by the particular application only. The application or cryptographic engine supervises the key management and access management.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

V. PROPOSED MODEL TO PROTECT THE PRIVACY IN HEALTHCARE DATABASE

With the development of technology, today everyone can access suggestions related to their personal health through internet. With the evolution of mobile devices and amalgamation of information technology and medical field, people from anywhere and anytime can easily collect information about their health condition. Today people are more anxious about personal health care and frequently access health care services without any [4] restriction from anywhere and anytime. Mobile devices and mobile applications play the major role and support in accessing the health related information. Healthcare information system is treated as one of the most important asset to improve people health and in turn quality of nation health. But the major concern in healthcare system is privacy protection and security of sensitive information. Many users pay to utilize healthcare database for research purpose or for the benefit of their organization. As there is lot of information exchange between the patients, healthcare data providers and other users strong security mechanism is required to protect the sensitive information in healthcare system. Strong security mechanism can only prevent the leakage of sensitive information available in the records.

Figure1 below shows various kinds of security attacks and threats which can happen with the various users while accessing the information stored in healthcare databases. In healthcare databases the information stored may be sensed information, monitored information or analysed report information of a patient by a doctor. The stored information is shared or monitored through mobile services to check real time response of a patient. Figure below shows users from various fields accessing the healthcare databases for analysis or business purposes through mobile and electronic equipments. The actual purpose to access healthcare databases is to get more details regarding health and health related queries. Researchers can utilize patient medical records for their research. Pharmaceutical companies can use such information to understand the impact of drugs or medicines through the history of patient. Healthcare database is very useful to government and various organizations to collect and analyse the medical records and identify various diseases which are affecting the people health. Using such useful information, government can take necessary measures to release the funds or other facilities to the people.

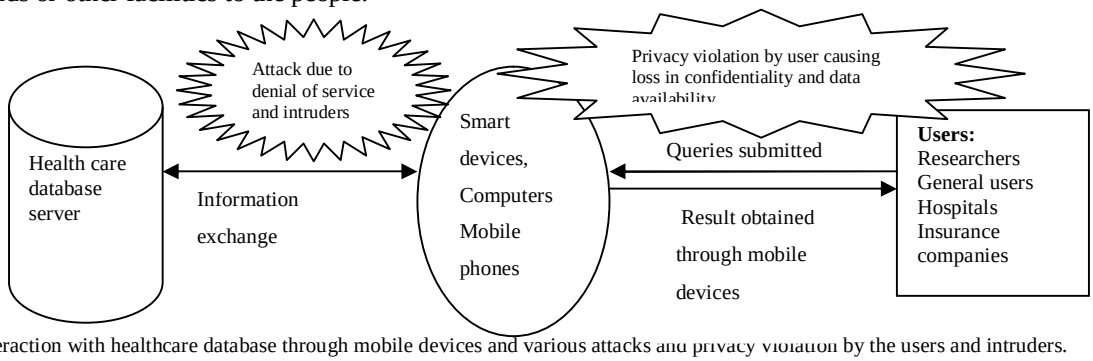

Fig. 1. User's interaction with healthcare database through mobile devices and various attacks and privacy violation by the users and intruders.

The attack which can happen through unauthorized access to database server is data manipulation or denial of service. The major threat to a patient is from the users under various categories who can access the data stored in healthcare database, and may identify the sensitive information related to a particular person. The major anxiety of a patient is that once the sensitive and private information is revealed, the fast spread and dissemination of sensitive data cannot be impended. It is very difficult to control the situation. The intruder can misuse such information for their personal benefit without the knowledge of patient.

The proposed model to protect the privacy of healthcare database system is shown in figure 2. Data collected from various hospitals are stored in centralized system called health database server. The attribute information either single attribute or group of attributes which helps the opponent to recognize a person are identified. When an opponent or ordinary user submits the query, such sensitive attributes data are de-identified [5] before it is revealed to the users. The modification process can use one of the processes like modification, cryptography, generalization or partial suppression of data or column modification.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

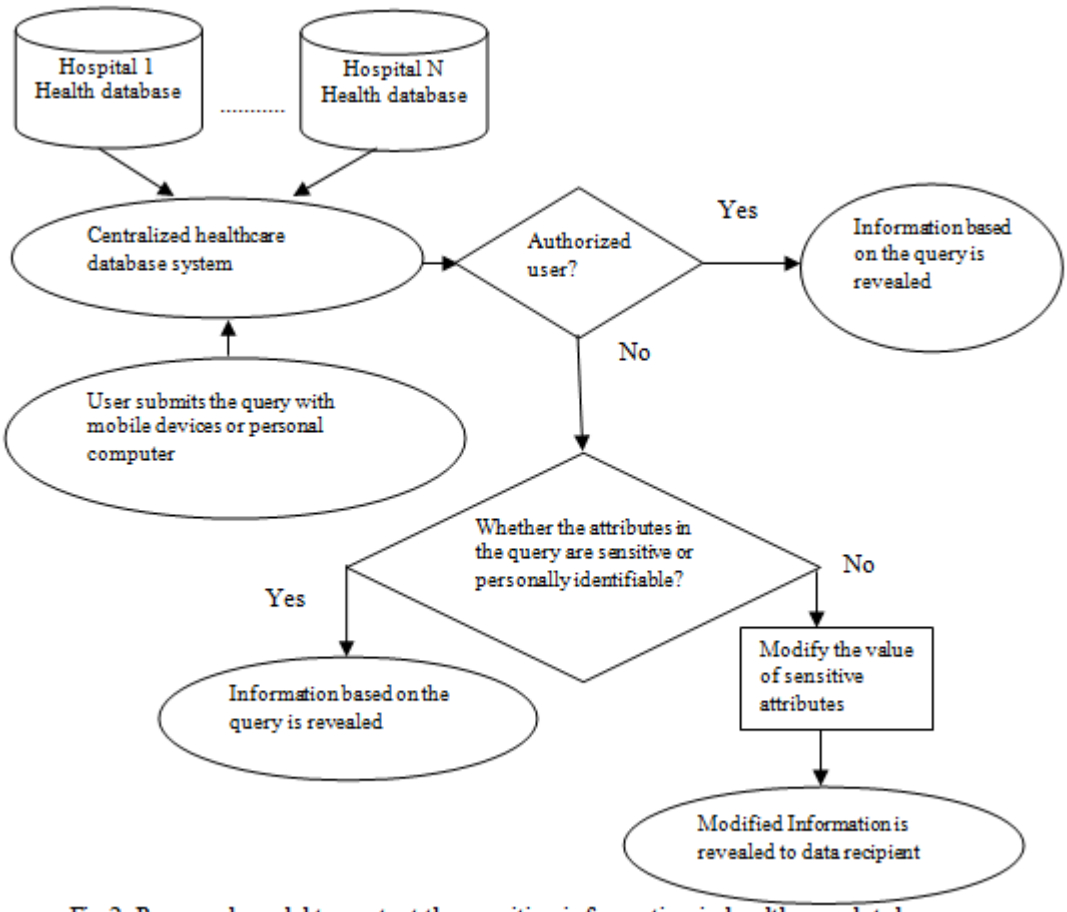

Fig 2. Proposed model to protect the sensitive information in healthcare database

VI. CONCLUSION

With the rapid development of technology people can access any information at anytime and from anywhere. Today people are more anxious as well as interested in accessing health related information and try maximum to deal with their personal health. The development of mobile technology and mobile applications facilitate the people to access the desired information from web based healthcare database system. The healthcare database consisting of patient records and medication helps the users to understand the disease and drug effects. Researchers can access the patient records and their medical history for the development of new medicines. On other side, as the healthcare database consists of sensitive information, leakage of such information can cause violation in patient privacy.

In this paper, various causes of privacy violation in healthcare databases are discussed. Various privacy protection mechanisms are suggested to protect the sensitive information available in healthcare database records. Such privacy protection mechanism not only protect the privacy of patient information but also provides the necessary information needed by ordinary people as well as researchers to access the precious healthcare databases

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

REFERENCES

1. Yung-Wang Lin, Li-Cheng Yang, Luon-Chang Lin, and Yeong-Chin Chen,'PreservingPrivacy in Outsourced Database', International Journal of Computer and Communication Engineering, Vol. 3, No. 5, September 2014 ,pp361-366,2014.
2. Asmaa Hatem Rashid and Norizan Binti Mohd Yasin ,'Generalization technique for privacy preserving of medical information', International Journal of Engineering and Technology, Vol. 6, No. 4, August 2014,pp.262-264,2014.
3. L. Sweeney. K-anonymity, 'A model for protecting privacy', International Journal on Uncertainty ,Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570,2002.
4. Tamas S. Gal, ,Zhiyuan Chen,Aryya Gangopadhyay, 'A Privacy Protection Model for Patient Data with Multiple Sensitive Attributes', International Journal of Information Security and Privacy, 2(3), pp.28-44, July-September 2008.
5. McGraw D. , 'Building,Public Trust in Uses of Health Insurance Portability and Accountability ActDe-identified Data'. JAMIA (Journal of the American Medical Informatics Association) 2013;20(1):pp29-34. 2013.
6. Dr. Vladmir Simovic,Matija Varga, Marin Milkovic,'Supervision and protection of e-data in sensitive information systems', Proceedings in International conference on Technology Innovation and industrial management , 2013, pp.s3-1-s-22

BIOGRAPHY

Dr. P.Kamakshi is a Professor in the Information Technology Department, Kakatiya Institute of Technology and Science, Warangal. She received Ph.D. degree in 2013 from JNTUH, Hyderabad, India. Her research interests are Data mining, security and privacy preservation techniques in data mining. etc.