e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.327

Volume 7, Issue 10, October 2019

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

The Importance of Proactive Data Privacy and Cyber Security from Attacks

Dr. A. Anjaiah[1]
St. Peter's Engineering College
Hyderabad,TS – India

Nagre Dinesh Kumar[2]
IV B.Tech,Department of CSE
St. Peter's Engineering College
Hyderabad,TS – India

K. Prudhvi Raj[3]
IV B.Tech,Department of CSE
St.Peter's Engineering College
Hyderabad,TS – India

Ch. Hasini Reddy[4]
III B.Tech,Department of CSE
St. Peter's Engineering Colldyge
Hyderabad,TS – India

Abstract: In the health care systems, Patients routinely share personal information with health care providers. If the confidentiality of this information were not protected, trust in the physician-patient relationship would be diminished. Patients would be less likely to share sensitive information, which could negatively impact their care. This paper provides a solution to protect sensitive attributes of patients. It provides a method to share information only to the authorized users. It also provids a method to recover the data if it has been attacked. The attacked data might mislead the authorized users and recovering it is necessary.

Keywords: personal information, healthcare, confidentiality, sensitive data, attack, recovery.

I. INTRODUCTION

In today's data intense environments, data is being stored electronically rather than on papers. Though the techniques provide comfort, it has to be ensured that associated privacy and security issues are analyzed.[1]. Business and government agencies collect unprecedented amounts of data. Failure to keep this data secure can impact an organization immensely. But the price of data breeches is not only monetary. It also leads to loss of customer's trust that can devastate the organization. Now-a-days, datasets are considered a valuable source of information for the medical research, market analysis and economic measures. These datasets can include information about individuals that contain social, medical, statistical and customer data. It is necessary to protect this data as it might lead to several problems.

Ethical health research and privacy protections both provide valuable benefits to society. Health research is vital to improving human health and health care. As the information in these records has to be shared with multiple people, privacy should not be compromised [2]. All the authorized users need access to the data in order to arrive at right decisions[3]. Protecting patients involved in research from harm and preserving their rights is essential to ethical research. The primary justification for protecting personal privacy is to protect the interests of individuals. The objective of this project is to hide the sensitive data and make it available to authorized users using combination of attributes and keyword search. It also aims to recover attacked data.

II. LITERATURE SURVEY

k-anonymity: Some organizations attempt to remove explicit identifiers, such as name, address and telephone number,on the assumption that anonymity is maintained because and the resultant data set would look anonymous[4]. Each released record will have at least k-1 records that could not be distinguished from it.[5]. Similar data has to be grouped together in order to minimize information loss[6]. As mentioned in[7], there is a possibility of homogenity attack and background knowledge attack using k-anonymity. Hence l-diversity was proposed. L-diversity: This method requires that each equivalence class has at least l well-represented values for each sensitive attribute.[7]

III. Proposed System

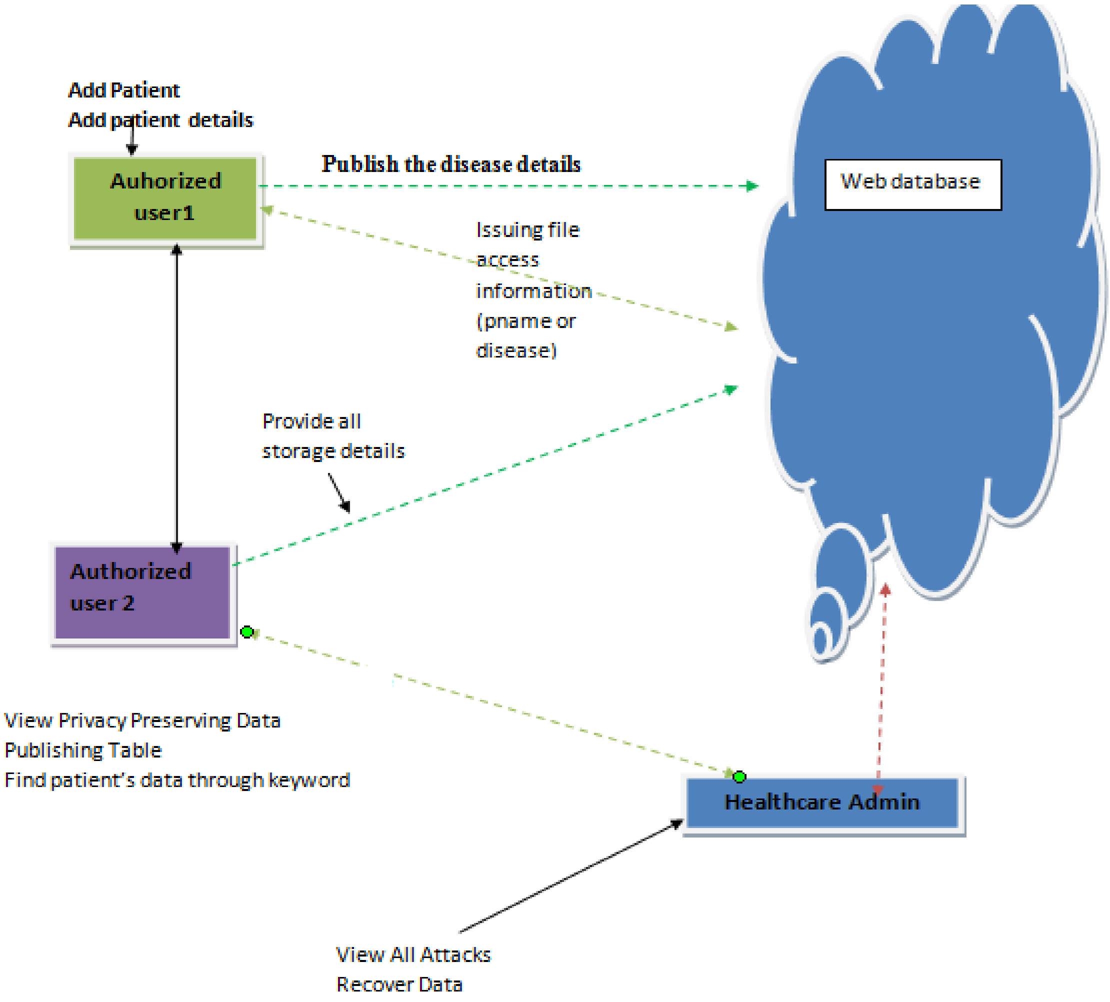
Add Patient
Add patient details
Auhorized user1
Publish the disease details
Web database
Issuing file access information (pname or disease)
Provide all storage details
Authorized user 2
View Privacy Preserving Data
Publishing Table
Find patient's data through keyword
Healthcare Admin
View All Attacks
Recover Data

Figure 1: Architecture Diagram

With the advent of technology, hospital management systems have started depending on electronic systems in order to store large amount of data. This method also reduces human intervention to a large extent thereby providing monetary benefits. The only issue using this technique is security. The data that is being stored has to be secure. Efforts have to be made to protect the confidentiality of data during its transit. It has to be made sure that the data that is stored or is being transferred should not be modified or deleted. If the data is changed, there are chances of severe loss not only to the owner of data but also to the organization that is managing the records of patients. Trust of the patients in the organization is lost and the organization's reputation is threatened. Hence, the issue has to be addressed and a better solution has to be designed in order to secure the data in storage area as well as in transit.

In the proposed system, the electronic health record management system would consist of two authorized users and an admin. Admin would be responsible for adding hospitals in the application. One of the authorized users would be an operator in the hospital who would take charge of adding patient data in the storage. The other authorized user would be a doctor who will view patient data. Initially, the doctor will view the table of data that would contain the details of patients in varied format. With the help of this data, doctor will figure out which patient details have to be searched for. Using these details, he will perform keyword search and retrieve the details of the patient that is required. During transit, the sensitive attributes are hidden and forwarded. The details duing the keyword search are retrieved through local storage. Hence the data is secure in storage and during transit

If the attacker has any information about the quasi-identifiers of the victim, then he can find out the victim and target the victim easily using that data.[8][9]. l-diversity attempts to solve attribute disclosure problem that may occur using k-anonymity[10]. The sensitive attributes are encrypted and grouped together. Whenever an authorized user wants to access the data, he would first see the encrypted and hidden data table. This data table does not display the sensitive attributes and hides few of the quasi identifiers. The authorized user is facilitated with a keyword search mechanism which helps him retrieve the data that he needs from the server. Hence, the data is secured while the authorized user still having access to it.

In some cases, the attacker might make an attempt to modify the existing data of the patients. This modification can be done due to several reasons and can affect the patients' health adversely. Hence, the problem has to be addressed. We provide a solution to this by notifying admin whenever the data is being updated in the storage area. As soon as any update operation is being performed on the data, the admin of the application would get notified. The admin now makes an attempt to retrieve the original data. This retrieval is possible with the backup of data that was created during the insertion of patient records. Whenever the authorized user adds patient data, its backup will be immediately created.

IV. Conclusion

In this project, we have majorly focused on tranfering the data in a way such that sensitive attributes are not at risk. Patient data is very vital and its security is important. Any changes in the data of the patient can not only lead to loss of data but also risk the health of patient. It would also bring monetary as well as reputation loss to the organization. Hence security of data is vital. Here, we have proposed a solution to transfer data without any threat to patients' sensitive attributes. We also provide a solution to detect attacks made on patient data and also provide a method to recover them. Our work also opens door to variety of research. It does not notify when the attacker only reads the data and does not modify it. It should provide more security and prevent the data from being accessed.

References

1. M. Meingast, T. Roosta and S. Sastry, "Security and Privacy Issues with Health Care Information Technology," 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY, 2006, pp. 5453-5458.
2. P. Ray and J. Wimalasiri, "The Need for Technical Solutions for Maintaining the Privacy of EHR," 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY, 2006, pp. 4686-4689.
3. k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. International Journal of Uncertainty, Fuzziness and Knowledge-Based SystemsVol. 10, No. 05, pp. 557-570 (2002)
4. Machanavajjhala, J. Gehrke, D. Kifer and M. Venkitasubramaniam, "L-diversity: privacy beyond k-anonymity," 22nd International Conference on Data Engineering (ICDE'06), Atlanta, GA, USA, 2006, pp. 24-24.
5. Latanya Sweeney, "Achieving k-anonymity Privacy Protection Using Generalization And Suppression", International Journal of Uncertainty, Fuzziness and Knowledge-Based SystemsVol. 10, No. 05, pp. 571-588
6. Jun-Lin Lin *, Meng-Cheng Wei ,"An efficient clustering method for k-anonymization", PAIS '08 Proceedings of the 2008 international workshop on Privacy and anonymity in information society, Pages 46-50 .
7. The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Zhou, B. & Pei, J. Knowl Inf Syst (2011) 28: 47.
8. Privacy and Security of Personal Information in a New Health Care System.Lawrence O. Gostin, JD; Joan Turek-Brezina, PhD; Madison Powers, JD, PhD; et alRene Kozloff, PhD; Ruth Faden, PhD; Dennis D. Steinauer. JAMA. 1993;270(20):2487-2493
9. The Hardness and Approximation Algorithms for L-Diversity, Xiaokui Xiao, Ke Yi, Yufei Tao. Proceedings of   the 13th International Conference on Extending Database Technology. Pages 135-146.
10. Domingo-Ferrer and V. Torra, "A Critique of k-Anonymity and Some of Its Enhancements," 2008 Third International Conference on Availability, Reliability and Security, Barcelona, 2008, pp. 990-993.