RESEARCH ARTICLE OPEN ACCESS

PATIENT DETAILS ON DISTRIBUTED MEDICAL HEALTHCARE APPLICATION

R.Selvakumar[1], S.Rajeshwaran[2]

[1]Assistant professor Department of Computer Science Ponnaiyah Ramajayam Institute of Science & Technology (PRIST) Vallam, Thanjavur.

[2]Master of computer application Department of Computer Science Ponnaiyah Ramajayam Institute of Science & Technology (PRIST) Vallam, Thanjavur.

Abstract:

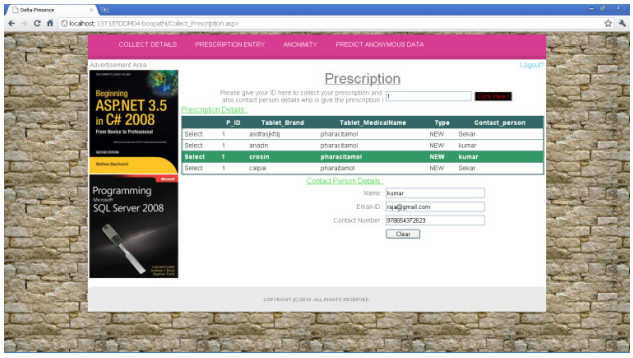
In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers equipped with their own cloud servers for medical consultant. And also it gives the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering. In this paper, the security and anonymity level of our proposed construction is enhancing by number of patients' attributes to deal with the privacy leakage in patient sparsely distributed cloud system. Data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. Data mining is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations.

Keywords — **Data mining, Networks, healthcare**.

INTRODUCTION

THE increasing ability to collect, manage, and share information is raising ever-increasing privacy concerns. This poses a challenging trade-off between the value (both to society, and to individuals) from the knowledge available from ubiquitous, shared information, and the risk to individuals posed by disclosure and misuse of private data. One solution to this problem is anonymity: ensuring that disclosed data cannot be linked to the individual whom the data are about. The European Community Directive This paper looks at a basic, and yet common and practical, problem: the risk is simply from identifying that an individual is (or is not) in an anonym zed data set. This could occur when there is a desire to publish a data set to support research on a specific condition, but identifying individuals meeting that condition is damaging. Examples could range from counterterrorism, publishing a database containing information about suspected terrorist groups to support research in automated support for discovering terrorism; to medical research, such as a database of patients with a particular type of cancer. In both cases, identifying that an individual is present in the database is damaging, both to the individual, and in the terrorism example by disclosing to real terrorist groups that their "cover organization" is suspect .

Data collection information process:



Module Description:

This project mainly focuses the concept which is secure the user data's from the hackers. To solve this problem, we are proposing a Delta presence technique to make the anonymized data and mainly it focuses how to predict the anonymized data with the following modules,

- Authentication
- Details submission
- Create anonymized data
- Predict anonymized data

CURRENT PROCESS ACTION:

Existing system works on objects shared by Byzantine processes consider that the access to operations in these objects is protected by ACLs. In this model, each operation provided by an object is associated to a list of processes that have access to that operation. Only processes that have access to an operation can execute it. This model requires a kind of reference monitor to protect the objects from unauthorized access. The implementation of this monitor is not problematic

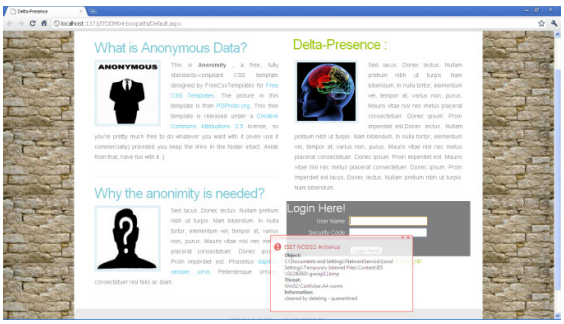
PROPOSED PROCESS ACTIONS:

The proposal for distributed computing with shared memory accessed by Byzantine processes presented in this paper differs from the previous model where objects are protected by ACLs. Our approach is based on the use of fine-grained access policies that specify rules that allow or deny an operation invocation to be executed in an object based on the arguments of the operation, its invoker, and the state of the object. The constructions presented in this paper (consensus and universal objects) demonstrate that this approach allows the development of simple and elegant algorithms, at the cost of defining access policies for the shared memory objects they use.

Medical processing

Future Enhancement:

The delta-presence definition can be revisited by assuming an adversary with varying levels of background knowledge; an adversary who knows more (e.g., the weight of an individual) gains in their ability to identify an individual, but also in their prior estimation of sensitive data. For example, knowing an individual is obese may make them easier to identify than not knowing their weight, but even without the anonymized data an adversary would have a strong reason to believe the individual was at risk for diabetes. As adversary prior knowledge increases, the probability of disclosure increases but the cost from disclosure decreases; giving a cost-utility trade-off (instead of simply privacy-utility).



CONCLUSION

We have presented a problem where anonymization is an appropriate solution, and a metric delta-presence that correlates to the real risk/cost of a privacy violation. Data sets anonymized directly to meet the delta-presence standard distort data less than k-anonymization to comparable privacy levels, and provides a clear risk-based guarantee of privacy. We have shown that the delta-presence measure first introduced in [1] not only provides a more meaningful approach to privacy than competing metrics, but with this paper we show that it can be practically achieved.

Reference:

1. N. Li and T. Li, "t-Closeness: Privacy Beyond k-Anonymity and l- Diversity," Proc. 23rd IEEE Int'l Conf. Data Eng. (ICDE '07), Apr. 2007.

2. Q. Zhang, N. Koudas, D. Srivastava, and T. Yu, "Aggregate Query Answering on Anonymized Tables," Proc. 23rd IEEE Int'l Conf. Data Eng. (ICDE '07), pp. 116-125, Apr. 2007.

3 R.J. Bayardo and R. Agrawal, "Data Privacy through Optimal k-Anonymization," Proc. 21st IEEE Int'l Conf. Data Eng. (ICDE '05), pp. 217-228, 2005.

4 Y. Tao, X. Xiao, J. Li, and D. Zhang, "On Anti-Corruption Privacy Preserving Publication," Proc. 24th IEEE Int'l Conf. Data Eng. (ICDE), pp. 725-734, 2008.