ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Isolation Preserving Access Control Mechanism for Delicate Fitness Information

K.Priyadharshini [1], M.Geetha[2]

Research Scholar, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[1]

Associate Professor, Department of BCA, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: Micro data refers to series of records, each record with information on an individual unit like a patient or an organization. Access Control Mechanisms (ACM) protects the sensitive information from unauthorized users. Even authorized users may misuse the data to reveal the privacy of individuals to whom the data refers to. Privacy Protection Mechanism (PPM) anonymize the relational data to prevent identity and attribute disclosure. It is achieved by generalization or suppression. Role-based access control gives users the permissions to access the data based on their roles. The access control policies define selection predicates available to roles while the privacy requirement is to satisfy the k-anonymity or l-diversity. Imprecision bound constraint is assigned for each selection predicate. Top Down Selection Mondrian (TDSM) algorithm is used for query workload-based anonymization. The Top Down Selection Mondrian (TDSM) algorithm is constructed using greedy heuristics and kd-tree model. Query cuts are selected with minimum bounds in Top-Down Heuristic 1 algorithm (TDH1). The query bounds are updated as the partitions are added to the output in Top-Down Heuristic 2 algorithm (TDH2). The cost of reduced precision in the query results is used in Top-Down Heuristic 3 algorithm (TDH3). Repartitioning algorithm is used to reduce the total imprecision for the queries. The privacy preserved access control framework is enhanced to provide incremental mining features using R+-tree. Data insert, delete and update operations are associated with the partition management mechanism.

KEYWORDS: Personal health records; cloud computing; data privacy; fine-grained access control; attribute- based encryption.

I. INTRODUCTION

Current globally networked society greatly demand the sharing and propagation of information. While information released in the past was in tabular and pre-computed statistical form (macro data), there is a need for the release for specific data to perform statistical analysis on them (micro data). Micro data refers to series of records, each with information on an individual unit like a person or an industrial unit. It allows the recipient to perform a whole new analysis on them as needed. In order to protect the identity of individuals to whom the data refers to, when releasing micro data, data holders often remove or encrypt explicit identifiers, such as names and social security numbers. Removing certain identifying attributes provide no guarantee of anonymity. Released information often contains other data, such as race, birth date, sex and ZIP code that can be linked to publicly available information to re-identify respondents and to infer information that was not intended for release. For instance, a patient data can be linked to other publicly available data like voter registration data. Access Control Mechanisms are used to protect the sensitive information from unauthorized users. The privacy of individuals may still be subject to identity disclosure by authorized users. Privacy Protection Mechanism is used to preserve the privacy of data respondents. It can be achieved by either suppression or generalization or both. Anonymization due to PPM introduces some changes that affect the correctness or the accuracy of the data required. It introduces imprecision to the data.

The main aim of our work is to anonymize the data considering the imprecision bound for each of the query predicates. Role-based Access Control (RBAC) allows defining permissions on objects based on roles in an organization. We have considered the imprecision added to each permission in the anonymized micro data. We have used the concept of imprecision bound for each permission to define a threshold on the amount of imprecision that can

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

be tolerated. In recent years, personal health record has e- merged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1.Recently, architectures of storing PHRs in cloud computing have been proposed in .While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. However, the goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes.

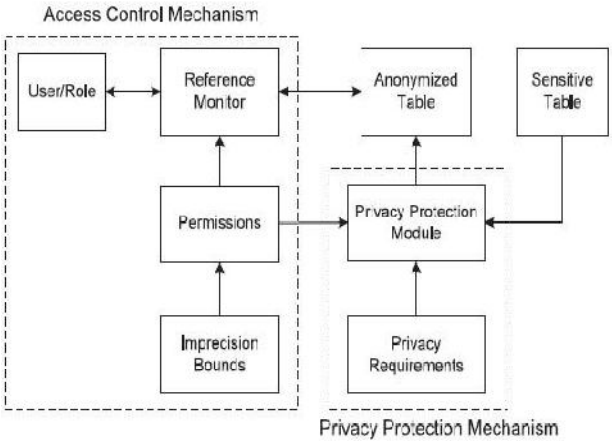

Fig 1.System Architecture

II. LITERATURE SURVEY

The collection of digital information by governments, corporations, and individuals has created tremendous opportunities for knowledge and information-based decision making. Driven by mutual benefits, or by regulations that require certain data to be published, there is a demand for the exchange and publication of data among various parties. Data in its original form, however, typically contains sensitive information about individuals, and publishing such data will violate individual privacy. The current practice in data publishing relies mainly on policies and guidelines as to what types of data can be published and on agreements on the use of published data. This approach alone may lead to excessive data distortion or insufficient protection. Privacy-preserving data publishing (PPDP) provides methods and tools for publishing useful information while preserving data privacy. Recently, PPDP has received considerable attention in research communities, and many approaches have been proposed for different data publishing scenarios. In this survey, we will systematically summarize and evaluate different approaches to PPDP, study the challenges in practical data publishing, clarify the differences and requirements that distinguish PPDP from other related problems, and propose future research directions.

Information sharing has become part of the routine activity of many individuals, companies, organizations, and government agencies. Privacy-preserving data publishing is a promising approach to information sharing, while preserving individual privacy and protecting sensitive information. In this survey, we reviewed the recent developments in the field. The general objective is to transform the original data into some anonymous form to prevent from inferring its record owners sensitive information. We reviewed and compared existing methods in terms of privacy models, anonymization operations, information metrics, and anonymization algorithms. Most of these approaches assumed a single release from a single publisher, and thus only protected the data up to the first release or the first recipient. We

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

also reviewed several works on more challenging publishing scenarios, privacy protection and privacy preserving mechanisms.

III. EXISTING SYSTEM

Predicate based fine-grained access control has been proposed, to protect the sensitive information from the unauthorized users. However, sensitive information can still be used improperly by correct users to compromise the privacy of users. Sensitive information can still be used improperly by correct users to compromise the privacy of users. This difficulty has been studied widely in the area of micro data publishing and privacy definitions.

Disadvantages of existing system:

Disadvantage occurs in this method that is important datas can still be abused by authorized users to surrender the privacy of users.

IV. PROPOSED SYSTEM

In this work, we inquire privacy and protection from the anonymity view. The important data, even after the deleting of sensitive variable, is still inflexible to linking attacks by the correct users. This problem has been studied widely in the area of micro data publishing and privacy definitions, e.g., k-anonymity, l-diversity, and variance diversity .Suppression and generalization methods are used by anonymization algorithm to satisfy privacy necessity with low mistakes of micro data. The privacy of individuals may still be subject to identity disclosure by authorized users. Privacy Protection Mechanism is used to preserve the privacy of data respondents. It can be achieved by either suppression or generalization or both.

Anonymization due to PPM introduces some changes that affect the correctness or the accuracy of the data required. It introduces imprecision to the data. The main aim of our work is to anonymize the data considering the imprecision bound for each of the query predicates. Role-based Access Control (RBAC) allows defining permissions on objects based on roles in an organization. We have considered the imprecision added to each permission in the anonymized micro data. We have used the concept of imprecision bound for each permission to define a threshold on the amount of imprecision that can be tolerated.

ADVANTAGES OF PROPOSED SYSTEM:

The system reduces the imprecision rate in query processing. Hence precision is improved and time complexity is reduced in the system. Privacy preserved data access control mechanism is improved with incremental mining model. Access control mechanism is adapted for incremental mining model.

V. IMPLEMENTATION

The policy administrator expects the imprecision bound for the least number of queries be violated by PPM. The administrator may able to change the imprecision bounds for queries if it seems that large number of queries violate the bounds and access request for roles will be denied. It is assumed that given n tuples are uniformly distributed in the domain space of the QI attributes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

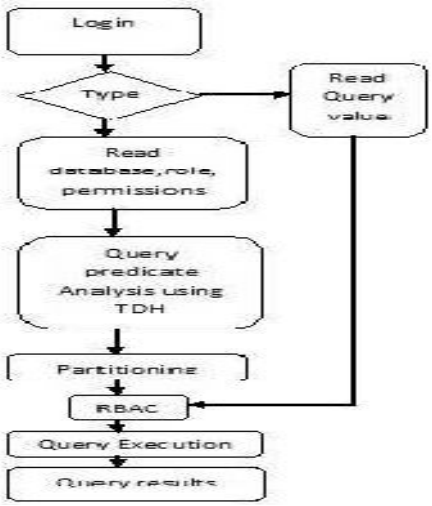

Fig2. System Flow Diagram

For finding the expected imprecision for a query, first find the expected number of partitions Over lapping the query.

VI. TOP-DOWN HEURISTIC ALGORITHM

In TDSM, the partitions are split along the median. Consider a partition that overlaps a query. If the median also falls inside the query then even after splitting the partition, the imprecision for that query will not change as both the new partitions still overlap the query. In this heuristic, we propose to split the partition along the query cut and then choose the dimension along which the imprecision is minimum for all queries. If multiple queries overlap a partition, then the query to be used for the cut needs to be selected. The queries having imprecision greater than zero for the partition are sorted based on the imprecision bound and the query with minimum imprecision bound is selected. The algorithm for TDH is listed in Algorithm 2. There are two differences compared to TDH1. First, the kd-tree traversal for the for loop in Lines 2-14 is preorder. Second, in Line 14, the query bounds are updated as the partitions are being added to the output (P). The time complexity of TDH2 is O(d|Q|2n2), which is the same as that of TDH1. In Section 4.3, we propose changes to TDH2 that reduce the time complexity at the cost of increased query imprecision.

VII. COMPUTATION

Algorithm
Input: T,k,Qand
Output: *P*

Initialize Set of Candidate Partitions(*CP*←*T*)
for(CPi € CP) **do**
Find the set of queries *QO* that overlap *CPi*
Select query from *QO* with smallest
Create query cuts in each dimensions
Reject cuts with skewed partitions
Select dimension and cut with least overall imprecision for all queries in *Q*
if(*Feasible cut found*) **then**
Compact new partitions and add to *P*
Else
Split recursively along median till anonymity

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

requirement is satisfied

Compact new partitions and add to *P* Update according to,

return(*P*)

VIII. RESULT ANALYSIS

Role Based Access Control (RBAC) scheme provides security to the data by allowing access based on permissions. K-Anonymi model is integrated with minimum imprecision based data access control mechanism. Partitioning using R+-trees results in less number of overlapping partitions. Hence precision is improved and time complexity is reduced in the system. Privacy preserved data access control mechanism is improved with incremental mining model. The system reduces the imprecision rate in query processing. Access control mechanism is adapted for incremental mining model.

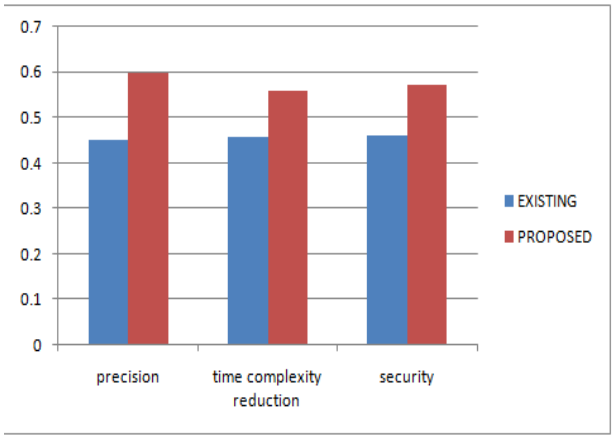

Fig 3.Result Analysis Graph

IX. CONCLUSION AND FUTURE WORK

In this paper made a survey on the Improving the Security on Public Health Record System in Cloud Computing. And also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. It is efficient in the Conjunctive Property. But somewhat limitations on MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation. Because it can be affect the non-revoked users. So move to the Attribute Based Broadcast Encryption. It satisfies the Disjunctive Property also and handles the revocation perfectly. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. Homomorphic encryption with data auditing is used to verify the trust worthiness of third party auditor.

The personal health record system needs security against attackers and hackers. Scalable and Secure sharing includes basic securities to protect the information from unauthorized access and loss. This paper proposed the new approach for existing PHR system for providing more security using attribute based encryption which plays an important role because these are unique and not easily hackable. We are reducing key management problem and also we enhance privacy guarantee.

REFERENCES

[1] S. Chaudhuri and Sudarshan, "Fine Grained Authorization through Predicated Grants," Proc. IEEE 23rd Int'l Conf. Data Eng.., 2007.

[2] R.Agrawal,P.Bird,T.Grandison,J.Kiernan,S.Logan and W.Rjaibi,"Extending Relational Database Systems to automatically Enforce Privacy Policies,"Proc.21st Int'l Conf. Data Eng.,pp.1013-1022,2005.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

[3] S. Chaudhuri, Kaushik and R. Ramamurthy, "Database Access Control & Privacy: Is There a Common Ground?" Proc. Fifth Biennial Conf.Innovative Data Systems Research, 2011.
[4] G. Ghinita, P. Karras, P. Kalnis and N. Mamoulis, "Fast DataAnonymization with Low Information Loss," Proc. 33rd Int'l Conf.Very Large Data Bases, pp. 758-769, 2007.
[5] N.Li,W.Qardaji, and D.Su,"Provably Private DataAnonymization:Or,k-Anonymity Meets Differential Privacy," Arxio preprintarXiv:1101.2604,2011.
[6] X. Xiao, G. Bender, M. Hay and J. Gehrke, "Ireduct: Differential Privacy with Reduced Relative Errors," Proc. ACM SIGMOD Int'lConf. Management of Data, 2011.
[7] Zahid Pervaiz,Walid G.Aref,Arif Ghafoor,NagabhushanaPrabhu, "Accuracy-constrained Privacy Preserving Access Control Mechanism for Relational Data, "IEEE Trans. Knowledge and Data Engineering,vol.26,no.4,pp. 795-807,2014.
[8] K. LeFevre, D. DeWitt and R. Ramakrishnan, "Workload-Aware Anonymization Techniques for Large-Scale Datasets," ACM Trans. Database Systems, vol. 33, no. 3, pp. 1-47, 2008.

REFERENCES

K.PRIYADHARSHINI was born on 20-06-1990 in Tamilnadu, India. She received B.sc Computer Science 2010 degree from Vivekanandha college of Arts and Science for Women, Namakkal, Affiliated to Periyar University, Salem, and Tamilnadu, India. She received Master of Computer Application 2013 degree from *Info* Institute of Engineering , Coimbatore, Affiliated to Anna University-Chennai, Tamilnadu, India. She is Pursuing M.Phil (full time) degree from Mutha yammal College of Arts & Science, in Periyar University Salem,Tamilnadu, India. She interested research area is Datamining.

M.GEETHA. She received her B.sc Computer Science degree from Bharathidasan University and MS(IT)., degree from Bharathidasan University.She has completed her M.Phil at Annamalai University. She is having 10 years of experience in collegiate teaching and she is the Associate Professor, Department of BCA in Muthayammal College of Arts and Science, Rasipuram affiliated by Periyar University. Her main research interests include Datamining and Warehousing.