Privacy - Preserving Cell Level and Incremental Data Access Control Mechanism

Madhuri Lambe\textsuperscript{1} and Vrunda Bhusari\textsuperscript{2}

\textsuperscript{1,2} Department of Computer Engineering, Savitribai Phule Pune University, BSIOTR, Wagholi, Pune, Maharashtra, India

\textsuperscript{1}madhuri.zade27@gmail.com, \textsuperscript{2}vrundabhusari82@gmail.com

ABSTRACT
Organizations, agencies distribute/publish sensitive data for research and other public benefit purposes. Prevent the misuse of sensitive data by the authorized/application users and provide both privacy and security of the sensitive data. The access control and privacy preservation these are two mechanisms protect the data from unauthorized or third party user. Normal/Application user to protect personal information as per they wants to do not share/disclose with others. The privacy preservation can be achieved through anonymized techniques from generalization. The objective of the work is to provide better security and minimum level of precision to the retrieved data, in this paper an accuracy constrained privacy preserving cell level access control mechanism is implement with extra constraint on each selection predicate this is called imprecision bound. Plan to extend the proposed system privacy preserving cell level access control in new approach. In fast growing world, the malicious intent or hacking purpose also increasing. So there is a need to provide a better security/protection to our system and provide dynamic access control.

Keywords: Query Evaluation, Cell Level Access control, Privacy preservation, Anonymity.

1. INTRODUCTION
The data is produced at an extraordinary rate, in recent years. So our ability to store data has grown. The data that is been stored can be analyzed for useful information. In order to make research useful, the data should be published. The data may contain personal details/information and sensitive attributes which an individual may not like to publish. The personal data may be misused for variety of different purposes. The protection against identity disclosure by satisfying some privacy/accuracy requirements [1]. Although the database has many security problems, such as authentication, integrity, access control, and privacy. There are several access Control mechanism [2]. Presenting a general methodology encryption technique, which allows encrypted data to the unauthorized-ed users without leaking information. It Provides anonymized format data to the unauthorized or authorized user. It Provides lots of security to the sensitive data according imprecision bound with user secured attributes.

2. LITERATURE SURVEY
On which a large amount of explore has been devoted, E. Bertino focus on access control mechanism systems, and explain the different access control mechanism models. A fine-grained access control mechanism model depend on authorization views that allows authorization transparent querying; user queries in terms of the database relations, and are valid if information contained in authorization views[3]. B.Fung[4] effort on Various Attacks Model and Privacy Models. They extend on authorization-transparent querying by introducing a new concept of validity, conditional validity. It give a powerful set of inference rules to verify for query validity. They display techniques by describing how an existing query optimizer can be extended to perform access control checks by incorporating inference rules. Enforcement of access control and privacy policies has been studied [5].

The privacy requirement in terms of k-anonymity shown by Li et al. [6] that k-anonymity offers similar privacy guarantees. The relation between the access control and the privacy protection mechanisms has been missing. Chaudhuri et al. have consider access control with privacy mechanisms [7].
3. PROPOSED SYSTEM

3.1 Design Goals and Objective

The goal of this system is to propose cell level access control mechanism this helps to normal user to protect personal information as per they wants to do not share with others.

The objectives of the project are as follows:

1) The project is to develop an application which is used to provide higher level security to any system. This can be made used by protecting sensitive data from an authorized user by using a new mechanism called as privacy protection mechanism.

2) New approach are going to implement new technique into this paper which is Cell level privacy protection mechanism. This help to user to secure his/her personal data it is extended feature in Privacy protection mechanism system.

3) Anonymous user can’t access single data without having permission. This functionality provided by Admin user to all other normal users.

3.2 System Architecture

Anonymization techniques are used to maintain the privacy of information/data. Access management and privacy protection mechanisms in our system provides a lot of security by applying encryption technique to sensitive information and information is retrieved during a custom made approach which will build users to access. Any access management concentrates on anomaly users to avoid privacy problems security.

ACM allows only license user predicates on sensitive information and PPM anonymized the information to satisfy privacy necessities and inaccuracy constraints on predicates set by the access control management Mechanism [8]. Anonymization techniques are used to impose the privacy and mainly generalization techniques are implemented. The proposed method works better in terms of tuple retrieval and privacy preservation. The system provides the dynamic policy management mechanism.

3.3 Module

In this system, there are two main entities first one is User and second one is Admin. User can be be Normal User or Application User. User can register in this system and update his/her profile. User can see normal user profile with getting security key. Admin is main entity in this system he/she grant roles and responsibility to other users also he /she can view sensitive data or anonymous data. Admin activate and deactivate other users.

There are mainly two module in this project.

1. User
2. Admin
1. User

1. Sensitive Data Retrieval: Sensitive information can still be misused by authorized users to compromise the privacy of consumers. The concept of privacy-preservation for sensitive data can require the enforcement of privacy policies or the protection against identity disclosure by satisfying some privacy requirements.

2. Encryption: Encryption is the conversion of data into a encrypted form, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

3. Request for Permission: User want to convert the encrypted data to original format then user request for permission.

4. Retrieve from Encrypted Database: The process of decoding data that has been encrypted into a secret format. Decryption requires to display the user data.

5. Anonymous Data Retrieval: User can retrieve data in anonymized format. This table provides security to the user.

2. Admin

1. Impression Bound: It is based on number of k attributes.

2. Query Cut and Medium Cut: A query cut is defined as the splitting of a partition along the query interval values. For a query cut using Query , both the start of the query interval and the end of the query interval are considered to divide a partition and In Medium cut, Partition created by TDSM have dimension along the medium.
3.4 Mathematical Module

User:
Registration: Name, Password, mail-id, mobile number, Disease, age, location etc
Login: Username, Password
If (success)
Login Successfully And Get Permissions from admin for View Sensitive data with status about user Disease.
(Fail)
User is not authorized. Login Failed.

Doctor:
Registration: Name, Password, location etc.
Login: Username, Password.
If (success)
Search Disease: View two tables:
1. Sensitive Data
2. Anonymous Data

Sensitive Data:
Display data in encrypted format.
View Particular user:
Search particular user after permission is granted from Admin and status to particular user

Anonymous Data:
This table gives information in Partition.

Admin:
Username, Password
Grant Permissions to Doctor for view Sensitive data which is Encrypted format.

Take Permission to view user data:
Permission_Key=GetAccessKey()
Permission_Key < ------- > Valid=show User data

Create Query_Work load:
Q={q1,q2,………,qn}
K={k1,k2,k3,k4,k5}

=Qi ← Ki

3.5 Algorithm

1) Top-Down Heuristic 1
Input: T, K value, Query and BQj.
Output: Partition (P).
1. Initialize set of CP.
2. for (CPi ∈ CP)
3. Find the set of queries that overlap CP.
4. Arrange queries in ascending order of BQj.
5. while (feasible cut is not found)
6. Find query from QO.
7. Make query cuts according dimension.
8. Choose dimension and cut having least overall imprecision.
9. Test feasible cut found or not if feasible cut then
10. Make new partitions and add to CP.
11. otherwise
12. Divide candidate partitions recursively along median upto anonymity requirement is fulfilled.
13. Shrink new partitions and add to P
14. return (P)

2) Cell level protection
Input: T, K value, Query and BQj
Output: Queryset and Resultset.
1. Initialize CP.
2. for each cpi in cp {
   Find the queries that find overlap Result and add to the Queryset.
   Choose Query from Queryset with small Resultset.
   Make querycut with each dimension.
   Choose Imprecision for all queries into queryset.
   Check (feasiblecut is found or not)
   If ( test with usersecured attributes)
   add it into CP
   Else
   do recursively till anonymity requirement is not fulfilled.
   Add into Resultset.
   Renew BQj
3. Return (Resultset)

4. RESULT

Here, consider one data having large numbers tuples of the proposed heuristics. In proposed system, Any User want to access data, it will get result in two table. First one is sensitive table and Other is Anonymized Table. Unauthorized user can’t access sensitive data, if user want to access encrypted data into origional format that time user request for permission. After getting permission, user
can access with user secured attributes. And for anonymized table, it will check imprecision bound and query workload, it is based on k number of attributes according to the user secured sensitive information.

Following fig. shows cell level graph.

Create number of queries randomly as the workload/permissions for the data set. In this query set, remove all queries which have empty value. Find randomly queries, store it into Query set and divide it into an equal intervals Which is Query set. Fix the value of k and change the query imprecision bounds from 5 to 20 value with increments of value 5. Then, select the number of queries whose bounds have not been satisfied by each algorithm for the uniform query workload.

5. CONCLUSIONS

The framework is a combination of Cell level access control and privacy Preserving mechanism. Presenting a general methodology encryption techniques, which allows encrypted data to the unauthorized users without leaking information. TDH1 and Cell level protection algorithm are used. It Provides anonymized format data to the unauthorized or authorized user. It Provides lots of security to the sensitive data according imprecision bound with user secured attributes. To prevent anonymous user to access Unauthorizeds data. The System provides lots of security and information is retrieved according to the customized format. Proposed system has investigate privacy-preservation from the anonymity aspect and provide Security.
ACKNOWLEDGMENTS

This is a great pleasure and immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in my project work successfully. I express my gratitude towards project guide Prof. V.K. Bhusari, and Prof. G.M. Bhandari, Head of Department of Computer Engineering, Bhivarabai Sawant Institute of Technology and Research College of Engineering, Pune who guided & encouraged me in my project work in scheduled time. I would like to thanks our Principal Dr. T.K. Nagraj, for allowing us to pursue my project in this institute.

REFERENCES


