IMPROVED ACCURACY-CONSTRAINED PRIVACY-PRESERVING ACCESS CONTROL MECHANISM FOR RELATIONAL DATA

[1]Seena Patel, [2]Ms. Ripal Patel
[1]P.G. Scholar, [2]Assistant Prof.
[1]Computer Engineering Department,
[1]Silver Oak College of Engineering and Technology, Ahmedabad, Gujrat

Abstract— The paper demonstrate on accuracy constrained privacy-preserving access control mechanism for relation data framework with multilevel anonymization techniques. Access control policy which define selection predicate on sensitive data and privacy requirement deals with anonymity. As privacy protection mechanism (PPM) provides less privacy protection and the data is shared so the user should compromise the with the privacy of data. The goal of the paper is to provide more security to the sensitive data along with minimal level of precision. The concept of accuracy constraints for permissions can be applied to any privacy-preserving security policy. Our goal is to solve problem of K-anonymity algorithm and provide solution by improving l-diversity algorithm.

Index Terms— Access control, privacy, k-anonymity, query evaluation

I. INTRODUCTION

ORGANIZATIONS collect and analyze consumer data to improve their services. Access Control Mechanisms (ACM) are used to ensure that only authorized information is available to users. However, sensitive information can still be misused by authorized users to compromise the privacy of consumers[1]. So we have to protect sensitive information from the misuse. Privacy preserving mechanism used to protect sensitive data. Organizations implement access control mechanism to assure that only sensitive information is available to authorized users. Sometimes confidential information is misused by authorized users to adjust the privacy of the customer. Organizations collect and analyze the data to improve the services [2].After removing the primary keys from the database of particular users ,the sensitive data may suffer from linking attacks from authorized users [6]. To improve the protection against identity discloser and support the privacy policy ,the concept of privacy preservation of sensitive data is introduced by satisfying some privacy requirements [7]. Every database have to maintain the sensitive information from privacy mechanisms, then also there is possibility that they suffer from linking attacks from authorized users. This problem has been studied in micro data publishing and privacy definitions like k-anonymity[6], l-diversity[2], variance diversity[2].

The concept of privacy-preservation for sensitive data uses anonymization techniques. Anonymization algorithm uses suppression or generalization of records to satisfy the privacy requirement with minimal distortion of micro data. This techniques can be used to ensure security and privacy of the sensitive information. The privacy is achieved at the cost of accuracy and imprecision is introduced in the authorized information under an access control policy [1].

Here in Fig.(1) represent An accuracy-constrained privacy-preserving access control mechanism. Arrows shows the direction of information flow. Here the PPM (privacy protection mechanism) ensures that the privacy and accuracy goals are met before the sensitive data is available to the access control mechanism. The permissions in the ACM (access Control mechanism) are based on the selection predicate on Quasi- identifier (QI) attributes.[1]

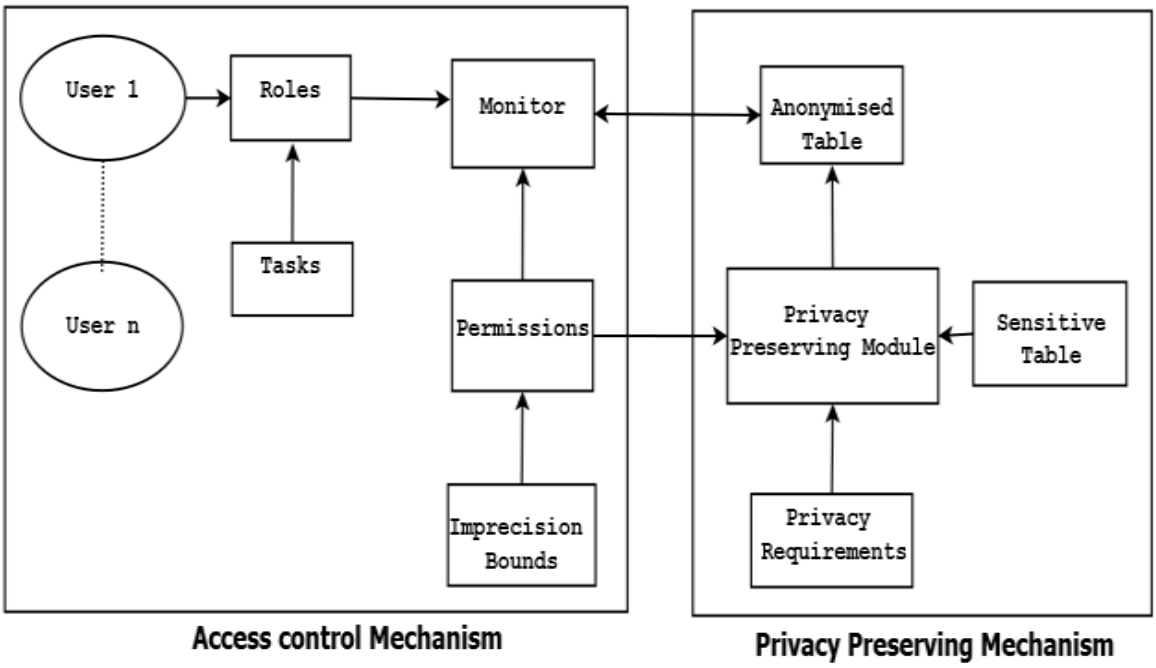

Fig. (1) Accuracy constrained privacy- preserving access Control mechanism

Disadvantage of system:

- System not able to retrieve data in a customized way.
- Privacy preserving uses only one anonymization technique.
- User's doesn't have efficient privacy and accurate constraints.
- System not able to retrieve data in customized way.

To overcome the disadvantages of existing system we proposed a system that provides more security and accuracy by providing heuristic to the system data. Data can be retrieved in a customized way that will make users to access in a more flexible way which will reduce user efforts. The advantage of proposed system are we are able to formulate the accuracy and privacy constraints. Due to use of heuristic algorithm system will provide security and accuracy to the users.

II. LITERATURE SURVEY

We have referred different papers regarding our research about access control mechanism, privacy preserving, k-anonymity, l-diversity. From this we came across the paper of Zahid Pervaiz, Walid G. Aref [1] in which they proposed an accuracy-constrained privacy-preserving access control framework for relational data. The framework is a combination of access control and privacy protection mechanisms. The access control mechanism allows only authorized query predicates on sensitive data. The privacy preserving module anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism. They formulate this interaction as the problem of k-anonymous Partitioning with Imprecision Bounds (k-PIB). They give hardness results for the k-PIB problem and present heuristics for partitioning the data to the satisfy the privacy constraints and the imprecision bounds. For this current work, they assumed static access control and relational data model.

As described above, [1] uses an accuracy-constrained privacy-preserving access control framework with only one technique that is Generalization. But Suhasini Gurappa .Metri [2] deals with multilevel anonymization techniques. She proposed an approach instead of using single Anonymization technique like generalization or suppression, a combined form of anonymization technique introduced like both generalization and suppression. Anonymization techniques replaces the data in the table with the some other values that is cannot be identified by the users. In generalization method individual values or attributes are replaced by some broader category. She also used suppression technique. In suppression certain values of the attribute are replaced by an asterisk '*'. Here Suppressed information of original table is used in the first level of anonymization, a generalized value is used in second level of anonymization.

To overcome the disadvantages of [1] Pratik Bhingardeve [3] proposed a system that provides more security by adding encryption to data. Data can be retrieved in a customized way that will make users to access in a more flexible way which will reduce user efforts. And access control concentrates on anomaly users to avoid privacy issues. The advantages of this system are they are able to formulate the accuracy and privacy constraints. Due to use of encryption system will provide security and privacy to users. Their defined additive approach of access management and privacy protection mechanisms in system provides a lot of security by adding cryptography to information and information is retrieved during a custom-made approach which will build users to access during as lot of versatile approach. Any access management concentrates on anomaly users to avoid privacy problems security .The ACM allows solely licensed user predicates on sensitive information and PPM anonymizes the information to satisfy privacy necessities and inexactness constraints on predicates set by the access management mechanism.

As a serious concern in data publishing and analysis, privacy preservation of individuals has received much attentions. Anonymity models via generalization can protect individual privacy, but often lead to superabundance information loss. Therefore, privacy preserving data publishing needs a careful balance between privacy protection and data utility. The challenge is how to lessen the information loss during anonymity. So, Gaoming Yang, Jingzhao Li, Shunxiang Zhang, Li Yu[4] proposed a (k, l, θ)-diversity model base on clustering to minimize the information loss as well as assure data quality. They take into accounts the cluster size, the distinct sensitive attribute values and the privacy preserving degree for this model. They proposed a (k, l, θ)-diversity model because some extent property is not enough for protecting sensitive attributes. They theoretically analyzed the hardness of this problem, and developed efficient algorithms to deal with them. The extensive experiments show that their proposed methods are effective and practical in real-world applications. Throughout the experiments, they found that the (k, l, θ)-diversity clustering algorithms uniformly outperformed the others.

Ebin P.M, Brilley Batley. C[5] proposed a system that consider suppression based anonymous database. A secure protocol is presented for privately checking whether K-anonymous database retains its anonymity once a new tuple is being inserted. QI is a minimal set of attributes used to uniquely identify individuals. Attack is mainly using Quasi-Identifier. Attacks may be re-identification or linking attack. To prevent the attack, masks the values of Quasi-Identifiers using either suppression based or Generalization based Anonymization methods. They have proposed secure protocol to check that if new tuple is being inserted to the database, it does not affect anonymity of database. It means when new tuple get introduced, k-anonymous database retains its anonymity. Database updates has been carried out properly using proposed protocol. This is useful in medical application. If insertion of record satisfies the k-anonymity then such record is inserted in table and suppressed the sensitive information attribute by * to maintain the k-anonymity in database. Thus, by making such k-anonymity in table that makes unauthorized user too difficult to identify the record.

Comparison Table

Sr No.	Description	Approach	Pros	Cons
1	Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data	Access control, privacy, k-anonymity, query evaluation	give hardness results for the k-PIB problem and present heuristics for partitioning the data to the satisfy the privacy constraints and the imprecision bounds	static access control and Relational data model has been assumed
2	Security Management Methods in	Access control,	Used multilevel	-----

	Relational Data	Anonymity, privacy preservation	anonymization technique	
3	A Survey on Security and Accuracy Constrained Privacy Preserving Task Based Access Control Mechanism for Relational Data	Access control, privacy, l-diversity.	Use encryption system that will provide security & privacy to user	Depends on custom based approach where cryptography can be effected
4	An Enhanced l-Diversity Privacy Preservation	privacy preservation, k-anonymity, l-diversity, clustering	proposed a (k, l, θ)-diversity models against sensitive attribute is effective	(k, l, θ)-diversity clustering algorithms works uniformly
5	Privacy Preserving Suppression Algorithm for Anonymous Databases	Privacy, Anonymization, Secure Computation, Suppression	k-anonymity in table makes unauthorized user too difficult to identify the record	problem of anonymity when initially table is empty

III. CONCLUSION

The paper discuss about the how to improve the efficiency of the security system. Anonymization techniques are used to maintain the privacy. We proposed a system that provides more security and accuracy by providing heuristic to the system data. Data can be retrieved in a customized way that will make users to access in a more flexible way which will reduce user efforts. The advantage of proposed system are we are able to formulate the accuracy and privacy constraints. Due to use of heuristic algorithm system will provide security and accuracy to the users. That will improve the efficiency of accuracy constrained privacy preserving access control mechanism for relational data.

IV. REFERENCES

[1] ZahidPervaiz, Walid G. Aref, ArifGhafoor, and NagabhushanaPrabhu, Accuracy-Constrained Privacy-Preserving Access Control Mechanismfor Relational Data", IEEE Transactions On Knowledge And Data Engineering, Vol. 26, NO. 4, April 2014.

[2] Suhasini Gurappa .Metri PG Student, CSE Dept Cambridge institute of technology ,Bangalore ,India, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 4

[3] Pratik Bhingardeve1, 2 Pune University, Smt. Kashibai Navale College of Engineering, Vadgaon (BK), Pune-411041, India, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[4] Gaoming Yang, Jingzhao Li, Shunxiang Zhang, Li Yu school of computer science and engineering anhui university of science and technology Huainan, 2013 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)

[5] Ebin P.M, Brilley Batley. C, AMIE, Assistant Professor Department of Computer Science & Engineering, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[6] Samarati, "Protecting Respondents' Identities in Microdata Release," IEEE Trans. Knowledge and Data Eng.,vol. 13 , no. 6, pp. 1010-1027 , Nov.2001.

[7] A. Rask, D. Rubin, and B. Neumann, "Implementing RowandCell-Level Security in Classified Databases Using SQL Server2005," MS SQL Server Technical Center, 2005.

[8] S.V.G.REDDY**,**Associate professor, ,Dept.of CSE, GIT, GITAM UNIVERSITY, 'Introduction to Data Mining

[9] K. LeFevre, D. DeWitt, and R. Ramakrishnan, "Workload Anonymization Techniques for Large-Scale Datasets,"ACMTrans. Database Systems, vol. 33, no. 3, pp. 1-47,2008.

[10] Femi Olumofin and Ian Goldberg "Preserving Access Privacy Over Large Databases", University of Waterloo, Ontario, Canada N2L 3G1, 2012

[11] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002.

[12] Machanavajjhala, D. kifer, j. Gehrke, and M.Venkitasubramaniam,"L-Diversity: Privacy Beyond kanonymity," ACM Trans.Knowledge Discovery from Data, vol. 1, no. 1, article 3, 2007.