ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

An Integrated Framework for to Protect Sensitive Information from Authorized Users

M.Venkateswarlu[1], M.M.Venkata Chalapahi[2], Dr.N.Kasi Viswanath[3]

M. Tech, Computer Science Engineering, Annamacharya Institute of Technology and science,
Rajampet (m), Y.S.R Kadapa, A.P[1]

Assist Prof, Dept of Computer Science and Engineering, Annamachrya Institute of Technology and Science,
Rajampet (m), Y.S.R Kadapa, A.P[2]

Professor& Head, Dept of CSE G.Pullareddy Engineering College, Kurnool, AP[3]

Abstract: In Previous days to protect the Sensitive information from unauthorized users generally by using Access control mechanism. The integrated framework is a combination of Access control policies and Privacy Protection Mechanism (PPM). However, when sensitive information is shared and a Privacy Protection Mechanism (PPM) is not in place, an authorized user can still compromise the privacy of a person leading to identity disclosure. A PPM can use suppression and generalization of relational data to anonymize and satisfies privacy requirements, e.g., k-anonymity and l-diversity, against identity and attribute disclosure. In this paper, we propose an Integrated framework it s a combination of accuracy-constrained privacy-preserving access control framework. The access control policies define selection predicates available to roles while the privacy requirement is to satisfy the k-anonymity or l-diversity. An additional constraint that needs to be satisfied by the PPM is the imprecision bound for each selection predicate. The techniques for workload-aware anonymization for selection predicates have been discussed in the literature. However, to the best of our knowledge, the problem of satisfying the accuracy constraints for multiple roles has not been studied before. In this paper the focus is on a static relational table that is anonymized only once. To exemplify our approach, role-based access control is assumed.

Index terms: Access control polices, privacy, Anomity methods, Query evaluation

1. INTRODUCTION

In generally in world numbers of originations are there. Examples are hospital, college, and government etc…The consumer data in these organizations are day-to-day increases. The consumer data is mainly used for analyzes and improves their services. . Access Control Mechanisms (ACM) is 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. 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 [1]. In this paper, we investigate privacy-preservation from the anonymity aspect.

The sensitive information, even after the removal of identifying attributes, is still susceptible to linking attacks by the authorized users [2]. And privacy definitions, e.g., k-anonymity [2], l-diversity [4], and variance diversity [5]. Anonymization algorithms use suppression and generalization of records to satisfy privacy requirements with minimal distortion of micro data. Anonymity techniques can be used with an access control mechanism to ensure both 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.

2. Integrated Framework Architecture

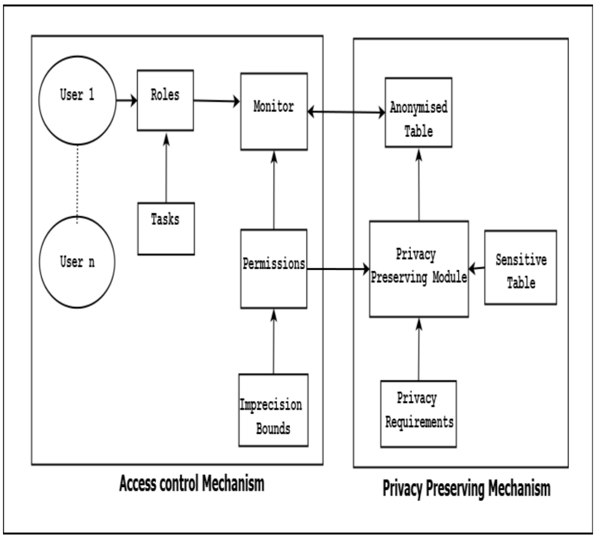

Fig: architecture of ACM and PPM

An accuracy-constrained privacy-preserving access control mechanism. (arrows represent the direction of information flow), is proposed. The privacy protection mechanism ensures that the privacy and accuracy goals are met before the sensitive data is available to the access control mechanism.

DOI 10.17148/IARJSET.2015.2706

3. ACCESS CONTROL POLICY

Access control policy is given in that allows he roles to access the tuples under the authorized predicate, e.g., Role CE1 can access tuples under PermissionP1. Access control across its networks, IT systems and services in order to provide authorized, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy.

This policy covers all LSE networks, comms rooms, IT systems, data and authorised users. According to the population density in a county, an epidemiologist can advise isolation if the number of persons reported with influenza are greater than 1,000 and quarantine if that number is greater than 3,000 in a single day. Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within LSE's Active Directory domains.

Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation encryption and other methods as necessary. The anonymization adds imprecision to the query results and the imprecision bound for each query ensures that the results are within the tolerance required. If the imprecision bounds are not satisfied then unnecessary false alarms are generated due to the high rate of false positives.

4. ANONYMITY

Anonymity means that the real author of a message is not shown. Anonymity can be implemented to make it impossible or very difficult to find out the real author of a message. Anonymityis prone to homogeneity attacks when the sensitive value for all the tuples in an equivalence class is the same. To counter this shortcoming, l-diversity has been proposed and requires that each. Here, for any combination of selection predicates on the zip code and age attributes, there are at least two tuples in each equivalence class.

5. ANONYMIZATION WITH IMPRECISION BOUNDS

We formulate the problem of k-anonymous Partitioning with Imprecision Bounds and present an accuracy-constrained privacy-preserving access control framework. Imprecise data means that some data are known only to the extent that the true values lie within prescribed bounds while other data are known only in terms of ordinal relations. The optimistic strategy pursues the best score among various possible scores of efficiency and the conservative strategy seeks the worst score.

6. CONCLUSION

The Integrated framework is a combination of access control and privacy protection mechanisms. So access control mechanism allows only authorized query predicates on sensitive data. The PP Manonymized the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism. In the current work, static access control and relational data model has been assumed. For future work, we plan to extend the proposed privacy access control to incremental data and cell level access control.

REFERENCES

[1] E. Bertino and R. Sadhu, "Database Security-Concepts, Approaches, and Challenges," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 1, pp. 2-19, Jan.-Mar. 2005.

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

[3] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments," ACM Computing Surveys, vol. 42, no. 4, article 14, 2010.

[4] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-Diversity: Privacy Beyond k-anonymity," ACM Trans. Knowledge Discovery from Data, vol. 1, no. 1, article 3, 2007.

[5] 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.

[6] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "A Framework for Efficient Data Anonymization Under Privacy and Accuracy Constraints," ACM Trans. Database Systems, vol. 34, no. 2, article 9, 2009.

[7] X. Xiao, G. Bender, M. Hay, and J. Gehrke, "Ireduct: Differential Privacy with Reduced Relative Errors," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2011.

BIOGRAPHIES

M.VENKATESWARLU: Has been received a B.TECH Degree in Information Technology from Vaagdevi Institute of Technology and Science , Proddtur, A.P JNTU ANANTAPUR University. Present Pursuing M. Tech in Computer Science Engineering from Annamacharya Institute of Technology and science. Rajampet (m), Y.S.R KADAPA, A.P.

M.M.VENKATA CHALAPAHI: Assistant professor in Dept of Computer Science and Engineering at Annamachrya Institute of Technology And Science. Rajampet (m), Y.S.R KADAPA, A.P.

N.KASI VISWANATH: Professor and Head of CSE DEPT. G.Pullareddy Engineering College, Kurnool, AP.

DOI 10.17148/IARJSET.2015.2706