|| Volume 2 ||Issue 12 ||JULY 2017||ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Proposed Generalization, Suppression, Heuristic, Encryption Privacy Protection Module to Access Sensitive Information in Relational Database (Review Paper)

Miss Swati Abhimanyu Nase

Student, CSMSS Chh. Shahu College Of Engineering Aurangabad, Maharashtra ,India

***Abstract*— Database is important part of application. Its security is important. Sensitive information refers to privileged or proprietary information that only certain people are allowed to see and that is therefore not accessible to everyone. If sensitive information is lost or used in any way other than intended, the result can be severe damage to the people or organization to which that information belongs. To avoid identity disclosure .GSEHPPM module proposes which uses generalization, suppression, encryption, heuristic techniques to implement privacy protection mechanism. Heuristic used for fetch record from database without loss of privacy requirement of sensitive information**.

Abbreviation: GSEHPPM – Generalization , Suppression , Heuristic ,Encryption Privacy Protection Module

Keywords : Anonymity, L-diverse

I INTRODUCTION

Database security is serious problem from several years. It is necessary to protect database to maintain its Confidentiality, integrity and availability. There are three types of attribute namely identifier attribute, Quasi identifier and sensitive attribute. Action must take to protect sensitive information in relational database from unauthorized user. To implement this concept of anonymity is introduced, Where for L-diverse(multiple) record present containing sensitive information

II LITERATURE SURVEY

Accuracy Constrained Privacy preserving Access Control mechanism for Relational data paper present combination of access control & privacy protection mechanism for relational data. User query are modified by access control & only authorized tuple are return. RBAC i.e. Role Based Access Control gives permission based on role in organization. An equivalence class is set of tuples having same QI attribute values. If each equivalence class has k tuples then it satisfies k anonymity Property. Query impression is defined as numbers of tuple return by query evaluated in anonymize relation & number of tuple in original relation. Top down selection Mondrain in which whole tuple is space divided new partition meet privacy requirement. Different partition algorithm proposed [1]. An Efficient Cryptographic Approach For Preserving privacy in Data Mining paper present to protect privacy to the data owner cryptography technique proposed. In sensitive database user defined sensitive item placed. Sensitive database proceed by mining technique to obtain result. For Key generation cryptography techniques is used ,by using this key plain text converted into cipher text transform transaction database into sensitive database. In pattern discovery module original pattern from extracted pattern receive to data owner. This scheme useful in avoid attack on cloud database based on original item and its exact support [2].

A Study Survey of Privacy Preserving Data Mining paper present privacy preservation data mining is important aspect of data mining. Number of methods have been developed for implement this. In privacy preservation method noise can be used in conjunction in data mining method. This method is used to restrict query auditing. Cryptographic methods are used to get owners data distributed over different site without release sensitive information. In k-anonymization method uniquely identifying attribute are removed. For given k record at least k-1 record exists. In randomization method aggregate distribution recovered instead of individual record. Some matrix factorization technique has better performance than traditional method. Less significant data is removed. On negative matrix factorization is additive combination to original data[3].

III PROPOSED ARCHITECTURE

In this system concept of privacy protection mechanism is implemented using GSEHPPM proposed module. Based on privacy requirement how much queries to be retrieve are depends. This limit is called as imprecision bound. The GSEHPPM privacy protection mechanism uses generalization, suppression, encryption, heuristic technique to enforce security. The following figure shows architecture of proposed System. Where PPM is privacy protection mechanism, ACM is access control mechanism ,PR is privacy requirement, IB is imprecision bound, GSEHPPM is generalization ,suppression ,encryption and heuristic privacy protection mechanism, G is generalization ,S is suppression, E is encryption ,H is heuristic.

How It Works: Imprecision bound depends on number of tuple fetch from database, Privacy requirement based selection of type of attribute i.e. role identifier attribute, Quasi identifier attribute or sensitive attribute. Based of IB, PR particular role has access to access control mechanism .

Access control mechanism implemented using privacy protection mechanism In privacy protection mechanism GSEHPPM module proposed. It uses generalization, Suppression techniques to implement concept of anonymity, Encryption applied on sensitive attribute to display of sensitive information. Advance encryption standard algorithm used because it support concept of anonymity to retrieve l-diverse record containing sensitive information, privacy maintenance by partition technique done by heuristic techniques. By applying all these technique in GSEHPPM module , get the output without containing sensitive information.

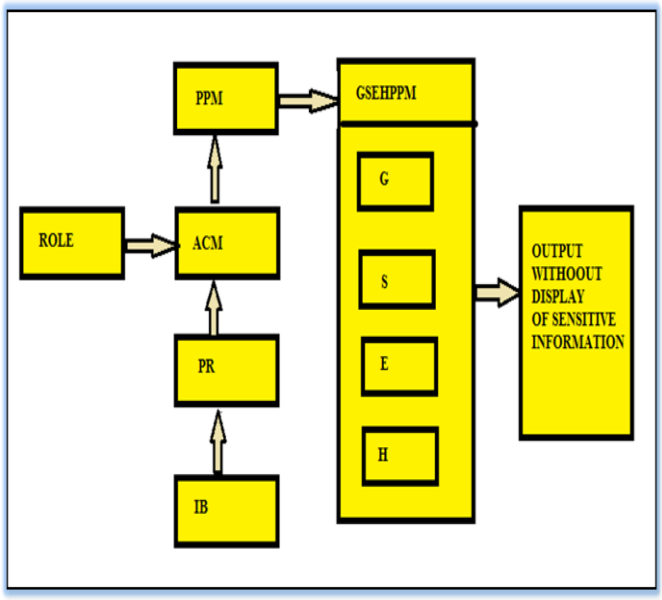

Figure 1 Architecture Of System With Proposed GSEHPPM Module

IV CONCLUSION

By understanding problem definition in field of database security to access sensitive information, with reference to literature survey carried out , GSHEPPM module to implement privacy protection mechanism to access sensitive information in relational database, if it is used by unauthorized use leads to identity disclosure, which can damage individual or organization.

REFERENCES

1] IEEE TRANSACTION ON KNOWLEDE AND DATA ENGINEERING VOL.26,NO 4,APRIL 2014 Accuracy-Constrained Privacy –Preserving Access Control Mechanism for relational data by Zahid Pervaiz ,senior Member, IEEE , Arif Ghafoor ,Fellow, IEEE ,and Nagbhushana Prabhu.

2] International Journal of Scientific & Engineering Research, Volume 4, Issue 10, October-2013 ISSN 2229-5518 1582 AN EFFICIENT CRYPTOGRAPHIC APPROACH FOR PRESERVING PRIVACY IN DATA MINING T.Sujitha1 V.Saravanakumar2 C.Saravanabhavan3.

3]International Journal of Research & Innovation in Computer Engineering , Vol 2, Issue 2 , April 2012, ISSN 2249-6580, (231-234) A Study Survey of Privacy Preserving Data Mining Shweta Shrma Hitesh Gupta Priyank Jain.