International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

Application of Advance Encryption Algorithm To Implement Access To Sensitive Information In Relational Database

Swati Abhimanyu Nase

[1]Master of Engineering, Computer Science & Engineering ,CSMSS CHH , Shahu College Of Engineering , Aurangabad, Maharashtra ,India

---

Abstract - Role based access control system depending upon role of individual has permission to access the system to authorized user. Role assignment, role authorization, permission authorization are major three rules in role bases access control system. Sensitive information of individual able see by only the person having authorization rights in authorization policy.t This paper represent application of advance encryption algorithm to implement access to sensitive information in relational database.

Keywords : Role based access control, Role assignment, Role authorization, Permission authorization, Authorization policy, Access, Relational database

1. INTRODUCTION

Advance encryption standard algorithm uses for convert plaintext into cipher text. Encryption uses when true value of information is hidden. The retrieve true information secret key required. Secret key preset to only authorize user. AES is symmetric key encryption algorithm. When same key is used for encryption and decryption then it is called symmetric key encryption algorithm. Advantages of advance encryption standard algorithm are it helps to maintain data in secure manner by Secure manner by using encryption technique. Algorithm can be applied to sensitive information to maintain user privacy. Algorithm works fastest. It uses annonymization technique to retrieve L-diverse record. Algorithms software implementation possible in programming languages. During restricting unauthorized access to data is to encrypt data even somebody was able to reach data it is not discerned by simple query.

2. LITERATURE SURVEY

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 [1]. Proposed NIST Standard for Role-Based Access Control paper present standard for role based access control. RBAC access control model implemented in various application such as database management, security management .Need standardization of RBAC feature. National institute of standard and technology has conducted and sponsored market analysis not alone recognize potential benefits of RBAC technology and research has done. Concept of role used in software application from many years. The root RBAC is use group in UNIX and other operating system include privilege grouping in database management system. It is useful to provide security feature in multi domain digital government infrastructure. RBAC is open ended technology which range from simple to extreme fairly complex. RBAC reference model defined collection of model component defines set of basic element user, role, permission, Operation as type and function that are implemented in standard. RBAC system and administrative functional specification feature fall in three category administrative operation, administrative review and system level functionality .First function defines capability to create, delete and maintain RBAC element and relation to create and delete use role assignment. Second function performs query operation on RBAC element and relation. System level functionality defines feature for creation of user session to include role activation, deactivation .RBAC gives common benchmark provide researcher with well-defined foundation for new and innovative access control and authorization management tools and technique. Standardization for developing specific application program interface. Rational RBAC defines feature required for core RBAC which is deal with common permission. General hierarchical RBAC

support concept of multiple inheritance permission of and user membership among role limited hierarchical RBAC are limited to simple structure such as trees. NIST RBAC model define in term of four component core RBAC, hierarchical RBAC, static Separation of duty relation and dynamic separation of duty relation. Static separation of duty relation related to disjoint user assignment with respect to set of role prevent authorization due to conflict roles. Dynamic separation of duty relation gives least privilege to user has different level of permission at different time depending role being performed. Package consist of different function for relevant requirement for product development, system evaluation or system acquisition specification [19].

3 . ADVANCE ENCRYPTION STANDARD ALGORITHM

Steps:
1)Byte Substitution (Sub Bytes).
2) Shift rows
3) Mix columns
4) Add round keys.

128 bits (16 bytes) plaintext converted into 128 bit(16 bytes) cipher text by using 128 bit(16 bytes) secret key.16 bytes plaintext substituted by another text by using S-box substitution. In shift row operation First row is not shifted. Second row is shifted one (byte) position to the left. Third row is shifted two positions to the left. Fourth row is shifted three positions to the left. Each column of four bytes is now transformed using a special mathematical function. The 128 bits(16 bytes) of the matrix are XOR to the 128 bits of the round key. If this is the last round then the output is the cipher text. 10 rounds required for 128 bit key size.

3.1 How it works on sensitive information in relational database

Table1-Original table.

Registration No	Name	Mobile No	Disease
100	R.S.Sen	9999999***	Heart disease
250	P.V.Kumar	2322221***	Fever
310	Z.N.Jain	1555551***	Dibetis
455	K.S.Das	5454442***	Tified

Table2-Original table after applying advance encryption algorithm on sensitive attribute

Registration No	Name	Mobile No	Disease
100	R.S.Sen	9999999***	xYmee7kxe25hYFCRr696wq==
250	P.V.Kumar	2322221***	3L48W9T0Try4z90egtg==
310	Z.N.Jain	1555551***	MR0ztJ173PR2RWtJaAj0q==
455	K.S.Das	5454442***	qsNC89xzFJhkJWpgdcyq==

Consider Table1-Original table contains field's Registration No, Name, Mobile No and Disease. Here Registration No and Mobile No are in annonymized form using generalization and suppression technique and Disease is sensitive information.In Table2-Original table after applying advance encryption algorithm on sensitive attribute contains field's Registration Number, Name, Mobile Number and Disease. In which first three fields same as in Table1.Disease is sensitive information. Advance encryption algorithm applied on Disease attribute which only individual have authorization rights in hospital management system are able to see.

4. CONCLUSION

How Advance encryption standard algorithm can be applied to access sensitive information in relational database system is studied .By using this only authorized person able to access sensitive information in role base access control system. Unauthorized person see the sensitive information in encrypted form which hides the true information.

REFERENCES

[1] 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.
[2] D. Ferraiolo, R. Sandhu , S. Gavrila , D. Kuhn, and R. Chandramouli ,"Proposed NIST Standard for Role-Based Access Control," ACM Trans. Information and System Security, vol. 4, no. 3, pp. 224-274, 2001.