iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: Issue **Issue:** ssue-1 **Month of publication:** October 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

Database Intrusion Detection Using Role Based Access Control System

Mrs. Antony Vigil[1], Mrinalini Shridhar[2], R Oviya[3]
[1, 2, 3]*Assistant Professor, Student SRM University*

Abstract- In this paper, we propose a different approach for the database intrusion detection (IDS). Database Management (DBMS) has become a key criteria in the information system (IS) storing valuable information of the system. We are urged to protect it to the fullest without losing any bit of information. Intrusion detection, which gathers and analyses the information system was one of the methods which protects the database the fullest with all sorts of rules. In this paper, we move into the Role based Access Control (RBAC) system which controls the administered databases for finding out sensitive attributes of the system dynamically. Role based Access Control is a method to restrict system access by authorized and unauthorized people directly. The access is based on the roles of the individual users within the organization. Important roles like administrator, access sensitive attributes and if their audit logs are mined, then some useful information regarding the attributes can be used. This will help to decide the sensitivity of the attributes. Since the models of the database intrusion detection has proposed a lot of rules , it is time to change the system to protect it more evidently with less rules and regulations which would be useful for detecting all sorts of transactions.

Keywords: Database intrusion detection, Role based access control system, Administered database, Audit logs, Sensitive and attributes.

I. INTRODUCTION

In past years, Database Management System (DBMS) have become an indispensible part of the life of the organizers and the users using it. Hence it was the primary priority to safeguard the DBMS, no matter how easy or difficult it was. The motive of the researches was first based on these ideas of protecting the DBMS and to prevent the leakage of data. The past years, Authentication user privileges , Auditing, Encryption and lots of methods have been used to protect the data and the system. Amending all the above methods, newer methods have come up to protect the same for daily operations and decision making in organizations. Database is a group or collection of data's which may contain valuable and sensitive information about the institution and organization, which is accessed by the people of the organization internally and externally every day.

Any leak of information in these systems will devastate the whole database system and the data's, leading to a great loss. Hence the data need to be protected and secured. The recent models of protection of DBMS were the dynamic threshold method and the data mining method of Intrusion detection system. Intrusion detection method is a process which analyses the unauthorized access and malicious behaviors and finds intrusion behaviors and attempts by detecting the state and activity of an operating system to provide an effective means for intrusion defend. In this paper, we will see how RBAC will help us to protect the database along with the intrusion detection with limited rules.

RBAC- Role based access control, also known as role based security is a method to restrict access of just one user, and also many users depending on the role of the users. The roles are prioritized like Example: Administrators access sensitive attributes and the DBMS and its attributes can be used. RBAC is a rich technology for authentication privileges and controlling the access of the information and data. It makes the administration of the security (work) much easier and simpler, though the process may be tedious and little vast. The possibility of adding newer application inside the secured system is much easier with the different access control mechanism. Extracting the data from the protected information system is much easier only by an authorized person. Talking about the sensitivity of the attributes we will have to refine the audit log to extract the data attributes.

In the past few years computer crime and security survey conducted by the Computer Security Institute(CSI) have seen a lot of drastic improvement in both the aspects ,but only thing was that there need to be a lot of adjustments in the rules given by each model. We are in the scoop of improving the database system and protecting it. In 2005, about 45% of the inquired entities have reported increased unauthorized access to information due to the poor system management. In 2007, financial application fraud was the leading cause and found it

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

double as compared to the previous year also 59% of the respondents outlined insider abuse as the security problem. In 2013, survey the number has dropped down and the security was much more than the past few years. The statistics being, the percentage threats due to insiders has been dropped to 20% and the financial fraud which was a cause before were eliminated in the upcoming years. Now only 10-20% are reported as unauthorized users. This shows that the database security has been improving day to day and researches have been conducted every time a model is proposed before implementing to action.

II. ROLE BASED ACCESS CONTROL MODEL

The Role based access control model proposes 3 relationships between the attributes given. They are:

a) USER-JOB: Which defines the relationship between the user and the task defined in that system.

b) JOB-ACCESS: Which defines the relationship between the job or the task of the person and the access to that particular work.

c) JOB-JOB: Which defines the job to job relationship between the users.

Now defining each attribute of the model we have the users of an organization represents an organizer or an agent of that field. The task or the job represents the responsibility or the functioning of the user within the organization. The access represents the approval or a permission to that particular task or event of that organization. The sessions box represents the overall relationship between the user and the task the contribution both has in the RBAC model. It does not point towards the access field as the access field is directed only by the task the user performs. Constraints represent the limitations or the boundary of each entity of that data that is, the user, task or job, access as well as the relationship between them is also restricted. The sessions represent the Divide and rule mechanism of the RBAC model. The fig 2 and 1 are interlinked process and each step of the data flow diagram will implement the following attributes of the user.

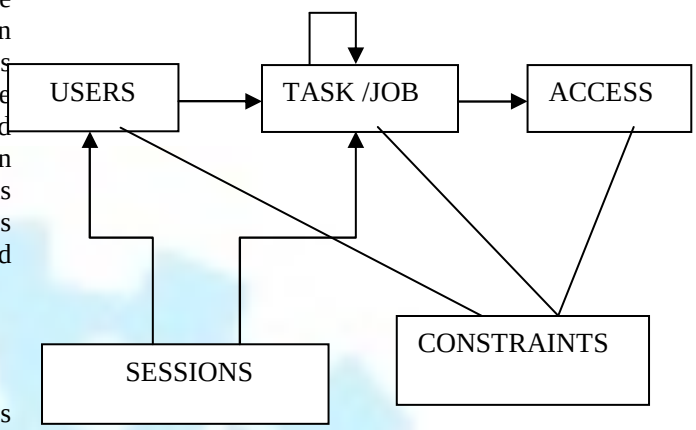


FIG 1. MODEL OF RBAC

III. RELATED WORKS

RBAC supports three well known principles and hence we work out our plan in 3 steps:

1. Principle of minimal authority
2. Divide and rule method of duties
3. Data abstraction

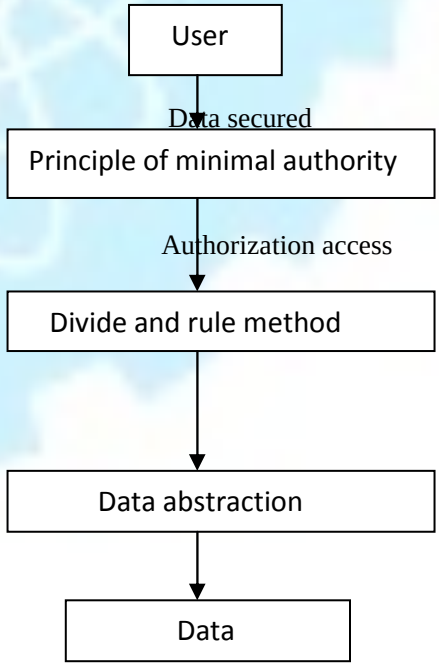


FIG 2. DATA FLOW DIAGRAM

Special Issue-1, October 2014
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

The sensitivity of an attribute is based on the database application. We have to divide the attributes into 3 divisions so as to protect the attributes according to the sensitivity or the position order they hold. Sensitivity refers to the position order a data has to be protected. If the data are least sensitive we can give it minimal protection. If the data are highly sensitive in the attribute set we need to protect it to the fullest. In some schematics we are not able to tell whether the data is sensitive or not. To give a clear picture of the attributes we have taken the Student Database Schema.

TABLE 1.TEACHER'S SALARY DATABASE SCHEMA

TABLE NAME	ATTRIBUTE NAME
STAFF	Name [i], Staff-id [j], Address [d], Phone no [a]
ACCOUNT	Account-id [b], Staff-id [c], Status [g], Month [e], Year [f], Amount [h]
SALARY TYPE	Salary-type [k], LOP and Deductions [l]

TABLE 2. TYPES OF SENSITIVE ATTRIBUTES

SENSITIVITY	ATTRIBUTE	WEIGHTS
Light sensitivity	a, b, c, d, i, ,j ,k	I
Medium sensitivity	e, f	II
High sensitivity	g, h, l	III

The sensitivity of the attributes can also be given by the entity-relationship model [E-R]. But with relation to the RBAC model , an administrator is required to control the database for its sensitivity. It is a perception of the real world. It is the diagrammatic representation of how the attributes are considered. The * represents if the attributes are sensitive or not. The model represents a collection of entities or data's and the contribution to the system. To maintain the account and the staff system we need a main administrator. Hence the RBAC system proposed in this E-R model .Thus E-R model is modified as:

STAFF + ACCOUNT + SALARY TYPE = ACCOUNTS ADMINISTRATOR

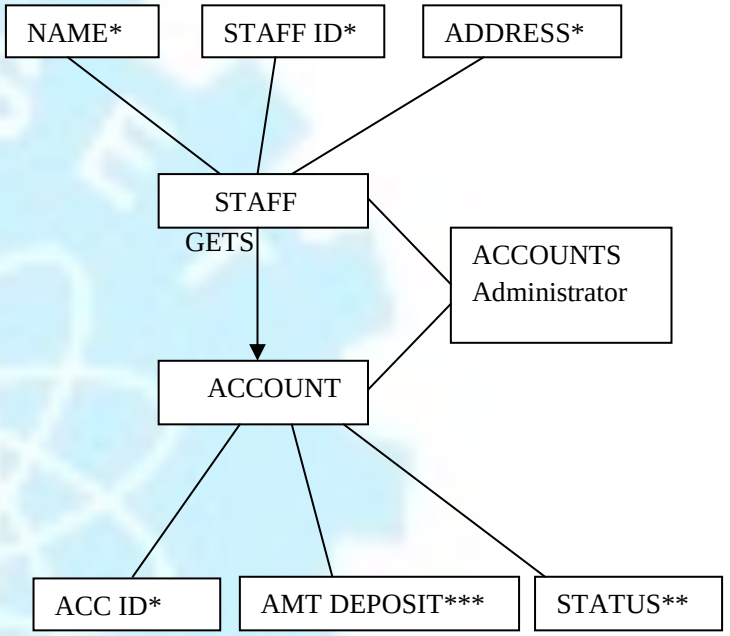


FIG 3.RBAC MODEL USING E-R MODEL

a) Principal of minimal authority- Also known as the principle of least privilege means that the access to the information system or its resources for only its own legitimate purpose by every user or the module. In simple words, we can say that an authorized user can access that information system or the resource only for their own privileged purpose. Privileged/ Authority refers to the right a user has or granting access to the user to use a particular system. For example, the user defined in its domain can access only its domain and its attributes. The person accessing a bank account can go through only their bank procedures and account. The system does not access or grant permission to access other accounts. Similarly an admin user accessing a computer can go into only the admin user account all other password accounts are blocked for the admin user.

b)Divide and rule method of duties- it can also be termed as the separation of duties among the users. It helps the task to be

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

completed faster. A mutual exclusive role is achieved to complete a particular set of task. RBAC brings this advantage of time management. the database is secured as well as the data are given to the authorized people easily with security.

c)Data abstraction- Data abstraction is a simple concept of accessing the data whenever we want to but with the permission of authorized people. It has different modes to it.

i)Public Mode- The access to the data by any user of the domain, but limited to a particular organization. This requires a common security where only the users of the organization can access it.

ii)Private Mode- The access of the data is limited only to the key user of that particular search of interest. That is only the accountants can handle the accounts of the organization and hence access to that particular class is given only to that particular user. A manager accessing the accounts of the company will be denied from accessing it.

iii)Protected Mode- The user in that particular domain and the senior user that is one or maximum two users who has to write to access that domain can access it with ease. Example only the accountants and the chief of the company can check the accounts of hat particular institution and make changes in that. The others have no right to access these without their permission. For the others the domain remains in blocked state.

IV. IMPLEMENTATION

RBAC is a complex system that involves a strategic process prepared by an expertise. RBAC is best implemented by applying a structured and detailed procedure. The use of divide and rule method is very essential to implement these process. Each task or step is broken down into sub tasks for the work and implementation to be easier and more efficient. The steps involved are:

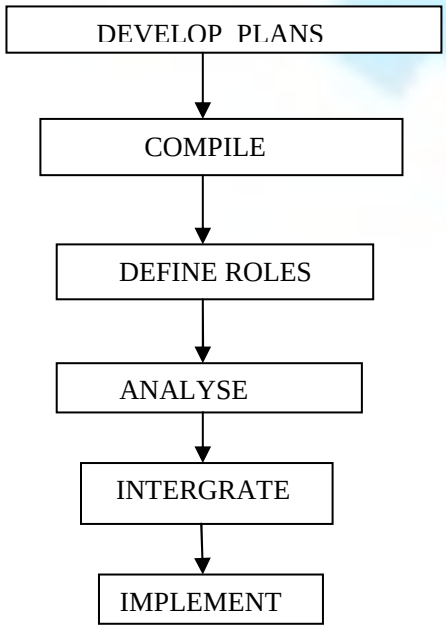


FIG 4.PROCESS

a)Develop Plans- To make best use of RBAC we can develop and plan for the RBAC system into best work in an organization or for a project's security of data. Example to extract the maximum security from RBAC a development plan including a project, etc. should be developed along with the deadline , budget etc.

b)Compile- This step involves the collection and putting together of all data , files , projects, etc. so as to identify the level of security needed to implement it. Sensitivity of the attributes should be determined so as to segregate and compile the system to one to provide the highest security possible.

c)Define Roles- As we have discussed that operation of database system is first best used only by the key user or the important user of that organizer or a system. Hence assigning a particular role to that person for the easy access of the software to access the data with ease and implement any kind of proper change within the system.

d)Analyze- this is a main step for any kind of system to know and to formulate RBAC. This would bring about the betterment of the system so that the next stage of implementation would be easier to execute. Any changes needed in the system should be done in this stage so that no further disputes arise at the later stage.

e)Integrate- Before any problem occurs in the system like system failure, we need to transfer each application's security system to a centralized security system so as to provide a secured companywide information access. this would be the last step of the process and would be the final stage without making any changes.

e)Implement- To put forth whatever we have executed these many steps without any errors or any types of problems. These are the best ways to protect a data from the external user.

Thus refining the system and protecting it according to the steps followed would give a better result. Always the principle of divide and rule method is followed in RBAC which is the key principle of the system.

V. PROCESS USING A FORMULAE

Each datum is a process streamline flow of information which is guarded by security. These syntaxes along with the formula help

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

in the security purpose. This formula was implemented in the Web Based technology, now it is time to implement it in Database to ensure its safety.

P1=>| (staff)P| name(P).X | staff id(P).X | phone(P).X
P2=>| (account)P | account id(P).X | amount deposited(P).X | status(P) .Y
P=>| P1||P2

Syntax:

P=>0 no process
| P | P composition of the process
| O(P).X output value of the process, X is the outcome.
| I(P).Y input value/ getting input from the user of the process, Y is the input variable.
| !!I(P).Y repetition of the input variables.

P=> run the process
| D(P) main data or the attributes
| read(P) read the data or the attributes
| change(P) change the data or the attributes
P=>enable(R).D gives permission to R to access a data
P=>disable(R)>D gives permission to R to disable the data or remove or stop the process till R.

For the above E-R diagram of the process ,the interaction between the staff salary and the account we can create a formula based on the process.

P=>| {(staff)P | name(P).X | staff id(P).X | phone(P).X} || {(account)P | account id(P).X | amount deposited(P).X | status(P).Y}

The other way of representing it is to split the process:

Where staff and the account have no sensitivity and hence it's just an attribute of the system, where as the other attribute-name, staff id, phone, account, account id, amount deposited are the inputs and the output is the status.
The two processes can be divided and then later combined to form a single equation. If the process needs to be changed or read or any other kind of operations, they can be done by the given formula which would be useful for the later run.

To calculate the sensitivity or to know the sensitivity of the attributes, automatic capitalization would be invoked to represent the highest sensitive attributes in the given set of data or the formula generated at the end of the process typed. The least sensitive are given in small letters. The medium sensitive might be in italic letters. The ones inside brackets represents that it is a secured data and hence it is the start of the process and that the data must be protected fully. Hence we cannot find the sensitivity of the attribute at the mid stage of the process. The same process with a change to denote the sensitivity is represented as :

P=>| {(staff)P | name(P).X | staff id(P).X | phone(P).X} || {(account)P | account id(P).X | AMOUNT DEPOSITED(P).X | STATUS(P).Y}

The other way is:

P1=>| (staff)P| name(P).X | staff id(P).X | phone(P).X
P2=>| (account)P | account id(P).X | AMOUNT DEPOSITED(P).X|STATUS(P).Y
P=>| P1||P2

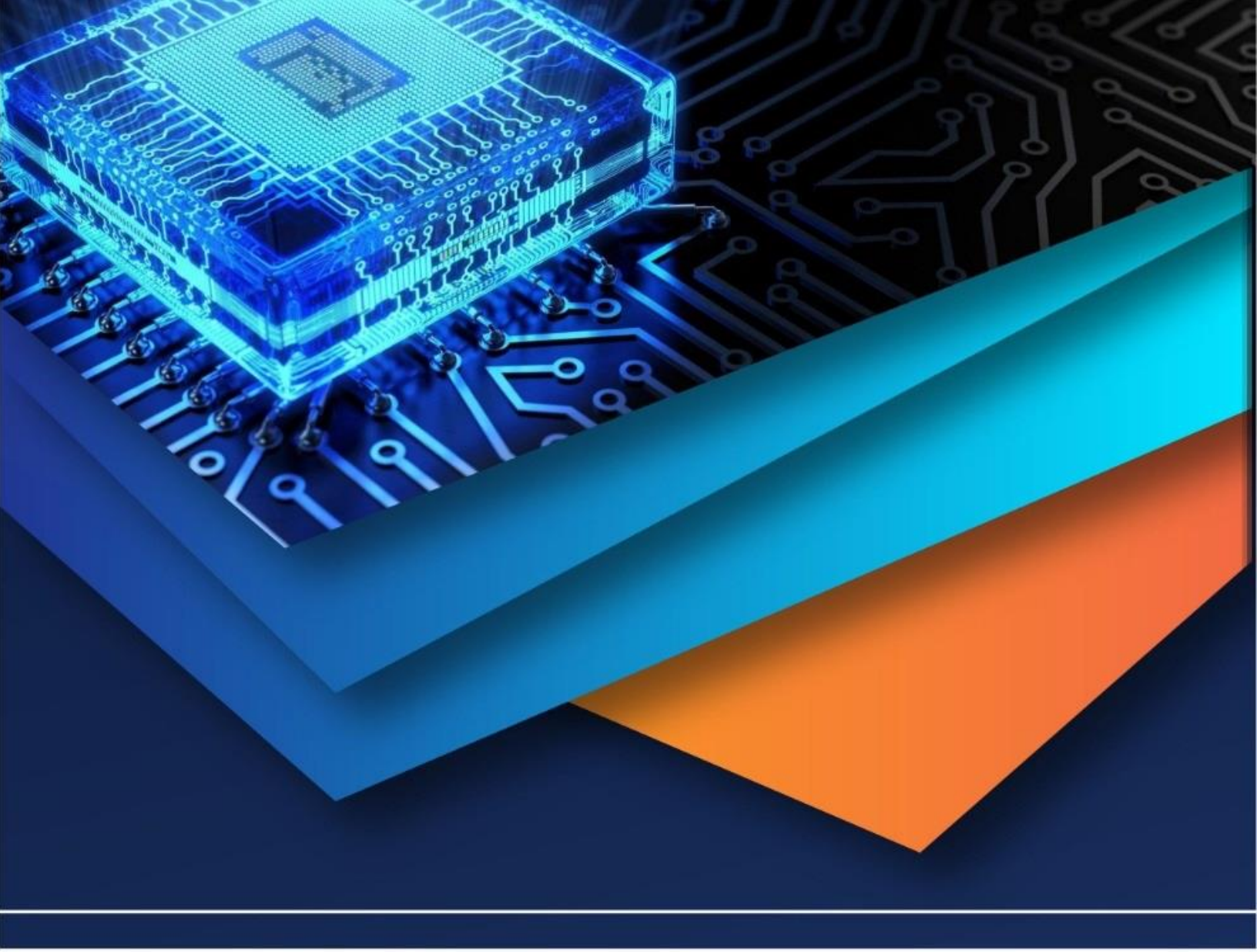
Thus this formula would be easy for the generation of large sets of data and to secure the data and hence even if there is a small change in the capitalization or the attributes or the brackets or any syntax mistake there would be an error generated in the system which would spoil the whole set of data. This is done for just a small set of data. We can proceed this for a huge one. An outsider seeing this would not understand the type of data or the importance of the data and hence would hesitate to meddle with it.

VI. CONCLUSION

Intrusion detection mechanism helps to secure the data in an organization. In this paper we have discussed in detail how the database could be secured by using Role Based Access Control System. The key benefits of RBAC are high efficiency and low maintenance cost for any type of organization be it big or small. Also RBAC system could be designed and used to improve the operational performance and strategic business value. This system could streamline and automate any business procedures, thus providing high/ better/ faster benefits to the user. It also helps to maintain privacy and confidentially of the employees in any organization. Thus we can conclude that mission to protect any key business process is a main vision of RBAC system in database intrusion detection.

REFERENCES

[1] Intrusion detection database system with dynamic threshold value By Khomlal sinha and Tripti Sharma
[2] Database Intrusion Detection using Weighted Sequence Mining Abhinav Srivastava1, Shamik Sural1 and A.K. Majumdar2
[3] J. Han, M. Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann Publishers (2001).
[4] U. Fayyad, G. P. Shapiro, P. Smyth, The KDD Process for Extracting Useful Knowledge from Volumes of Data, Communications of the ACM, pp. 27-34 (1996).
[5] R. Bace, P. Mell, Intrusion Detection System, NIST Special Publication on Intrusion Detection System (2001).
[6] A. Srivastava, S. Sural, A.K. Majumdar, Weighted Intratransactional Rule Mining for Database Intrusion Detection, Lecture Notes in Artificial Intelligence, Springer Verlag, Proceedings of Pacific-Asia Conference in Knowledge Discovery and Data Mining, pp. 611-620 (2006).
[7] W. Lee, S.J. Stolfo, Data Mining Approaches for Intrusion Detection, Proceedings of the USENIX Security Symposium, pp. 79-94 (1998).
[8] D. Barbara, J. Couto, S. Jajodia, N. Wu, ADAM: A Testbed for Exploring the Use of Data Mining in Intrusion Detection, ACM SIGMOD, pp. 15-24 (2001).
[7] C. Y. Chung, M. Gertz, K. Levitt, DEMIDS: A Misuse Detection System for Database Systems, IFIP TC-11 WG 11.5 Working Conference on Integrity and Internal Control in Information System, pp. 159-178 (1999).
[8] V.C.S. Lee, J.A. Stankovic, S.H. Son, Intrusion Detection in Real-time Database Systems Via Time Signatures, Real Time Technology and Application Symposium, pp. 124 (2000).
[9] Intrusion detection database system with dynamic threshold value By Khomlal sinha and Tripti Sharma
[10] Database Intrusion Detection using Weighted Sequence Mining Abhinav Srivastava1, Shamik Sural1 and A.K. Majumdar2
[11] S.Y. Lee, W.L. Low, P.Y. Wong, Learning Fingerprints for a Database Intrusion Detection System, Proceedings of the European Symposium on Research in Computer Security, pp. 264-280 (2002).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY