Configuring Role Based Security with traditional Access Control Models for ERP System

Swapnaja A. Ubale
Research Scholar Computer Science and Engineering Department
Research Center - Walchand Institute of Technology , Solapur Maharashtra, India

Dr. S.S. Apte
Research Guide (Ph D) Computer Science and Engineering Department
Walchand Institute of Technology Solapur, Maharashtra, India

Abstract: For Security Access control models have been traditionally proposed. Most traditional models include mandatory access control (MAC) and discretionary access control. Now a days , role-based access control (RBAC) has been introduced, keeping in mind that it has been easy to implement along with both traditional models. In this paper configuring role based security along with manadatory and discretionary model for making application to be more secure is proposed. This configuration is also used with new DC encryption algorithm. DC Encryption algorithm after analysis found to be more secure. For this paper, this simulation is done for the ERP which is at the heart of many organizations.

Keywords : ERP, Access Control, RBAC, MAC, DAC,DC

I. INTRODUCTION TO GENERAL ERP SYSTEM

For many organizations it needs to store data, manipulate data, and produce It whenever requited in front of users. There are hundreds of such data tables which store data generated as a result of diverse transactions. These rather integrated for the speedy and accurate results required by multiple users, for multiple purposes, for multiple sites, and at multiple times.

Therefore, ERP solution implies that it be:

Flexible: An ERP system has to have modular application architecture. This means that various functionalities are logically clubbed into different business process and structured into a module which can be interfaced or detached whenever required without affecting the other modules. Comprehensive: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

ERP is the part of the interlinked processes that make up the total impact of any organization.

For making ERP system to be very efficient and secure Access control models plays important role. Working of these models in introduced shortly and then simulation of these models is presented for ERP system.

In RBAC importance is given to roles, principle or the rules etc. To clarify the notions here is simple formal description, in terms of sets and relations, of role based access control.

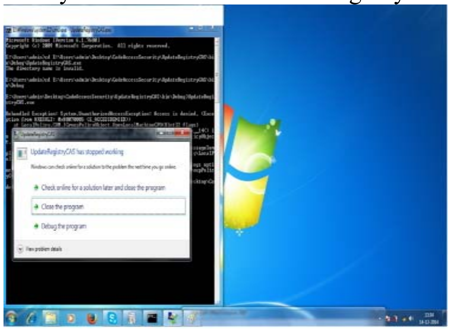
- Subject and object of the system are defined first
- For each subject, the active role is the one that the subject is currently using so define the active role for subject.
- Each subject may be authorized to perform one or more roles so define authorized roles for subject.
- Each role may be authorized to perform one or more transactions so define transactions authorized for role.
- Subjects may execute transactions. The predicate is true if subject *s* can execute transaction *t* at the current time, otherwise it is false.

Basic rules required are as:

1. Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a role. The identification and authentication process (e.g. login) is not considered a transaction. All other user activities on the system are conducted through
transactions. Thus all active users are required to have some active role.
2. Role authorization: A subject's active role must be authorized for the subject:
Thus rule ensures that users can take on only roles for which they
are authorized.
3. Transaction authorization: A subject can execute a transaction only if the transaction is authorized for the. subject's active role

II. DAC

In DAC Discretionary protection policies govern the access of users to the information on the basis of the user's identity and authorizations (or rules) that specify, for each user (or group of users) and each object in the system, the access modes (e.g., read, write, or execute) the user is allowed on the object. Each request of a user to access an object is checked against the specified authorizations. If there exists an authorization stating that the user can access the object in the specific mode, the access is granted, otherwise it is denied. As shown in the following snapshot owner can restrict access to any file. Here it is shown for registry.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

E:\Users\admin>cd E:\Users\admin\Desktop\CodeAccessSecurity\UpdateRegistryCAS\bi
n\Debug\UpdateRegistryCAS.exe
The directory name is invalid.

E:\Users\admin>cd E:\Users\admin\Desktop\CodeAccessSecurity\UpdateRegistryCAS\bi
n\Debug

E:\Users\admin\Desktop\CodeAccessSecurity\UpdateRegistryCAS\bin\Debug\UpdateRegi
stryCAS.exe

Unhandled Exception: System.UnauthorizedAccessException: Access is denied. (Exce
ption from HRESULT: 0x80070005 (E_ACCESSDENIED))
   at [illegible]
```

UpdateRegistryCAS has stopped working

Windows can check online for a solution to the problem the next time you go online.

Figure 1: DAC to restrict access

So in DAC also can be called as code access security owner of the file can restrict access to its own resources. Different modules can be protected against unauthorized access, So here it is possible to keep user data safe and avoid theft of data or resources.

III. MAC

With mandatory access control, this security policy is centrally controlled by a security policy administrator; users do not have the ability to override the policy and, for example, grant access to files that would otherwise be restricted. In strict Government applications or for Military purpose it has been used dominantly. It is most traditional and most secure model.

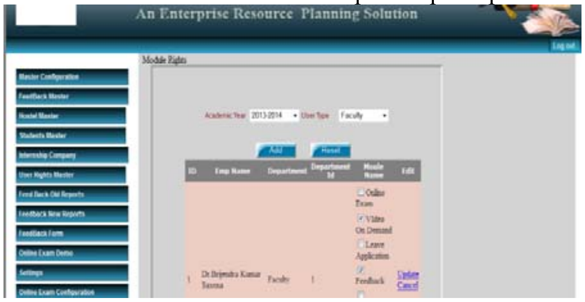
But when flexibility in considered role based approach is better than MAC. With RBAC it can deal with more number of users easily. So for ERP system RBAC model is configured to work with MAC and DAC.

IV. SIMULATION FOR ERP SYSTEM

In ERP consider for any educational institution, SuperAdmin suppose in the of main manager who is responsible for assigning the role and deciding the principle for assigning the duties to the different roles. As in MAC SuperAdmin is going to govern centrally but each role as per the principle have the freedom to do necessary changes whenever required. Consider the example for the role of faculty. Supipose XYZ faculty has permission to access Video On Demand Application. Then XYZ faculty can upload any video or delete video in his own account. But it is governed by principles of SuperAdmin as the Manadatory Access Control.

In ERP each role can do its own activity assigned to that role and has role level security. Work done by that role is kept secure. One role person can not see changes done by other role. Also in one role category , one member of the same role cannot see changes done by other member of the same role as it is provided unique ID and password. For each member of each role password generated by each member is also secured. superAdmin also cannot see password because it is encrypted form. Thus any other member of another role cannot make changes in other member’s domain. Thus Role Based Security is provided for ERP system.

In Code access Security as code is secured by authority who is responsible for that code. Similarly in ERP different modules are assigned to different roles with the permission of SuperAdmin. As per the principles and rules SuperAdmin decide modules which can be accessed by different roles. SuperAdmin can change modules assigned to dofferent roles at any time. In this case modules are generated runtime for each role. Every day SuperAdmin can assign different modules to different roles as per the principles as shown in following snapshot.



Module Rights

Academic Year 2013-2014 User Type Faculty

ID	Emp Name	Department	Department Id	Module Name	Edit
1	Dr.Brijendra Kumar Saxena	Faculty	1	☐ Online Exam ☑ Video On Demand ☐ Leave Application ☑ Feedback ☐	Update Cancel

Figure 2: DAC for ERP System

Thus simulating ACL based modules and configuring role based model with manadatory and discretionary user can provide high level security for any application and resources and data effectively.

V. ENCRYPTION ALGORITHM

Configuration also can be used with encryption algorithm for more security. While implementing ERP system new DataCrypt Encryption algorithm is used. It is compared with other exiting algorithm as given in following table.

Table 1 Key Size of encryption algorithms

Algorithm	**Key Size** **(Bits)**	**Block Size** **(Bits)**
DES	64	64
Rijndael(AES)	256	126.2
Data crypt	448	64

Table shows the Key Size used in this experiment. Longer key lengths mean more effort must be put forward to break the encrypted data security.

In following table and graph, it shows the performance of cryptographic algorithms in terms of encryption time. Here, it compares the encryption time of DES, 3DES, AES, DC, AES and RSA algorithm over different packet size. DC algorithm takes less time for encryption and decryption as compared with other other algorithms and is more secure than AES and AES - RSA used combinely.

Table 2: Comparative Analysis of Different cryptography techniques

Input Size in KB	**DES**	**3DES**	**AES**	**DC**	**AES and RSA**
200	25.0	70.8	14.2	10.3	16
557	58.2	146.2	38.2	28.3	52.38
1024	110.0	276.3	72.2	53.5	99.0
2,030	187.0	469.7	122.7	90.9	168.3
5,120	542.3	1362.2	355.9	263.7	488.1

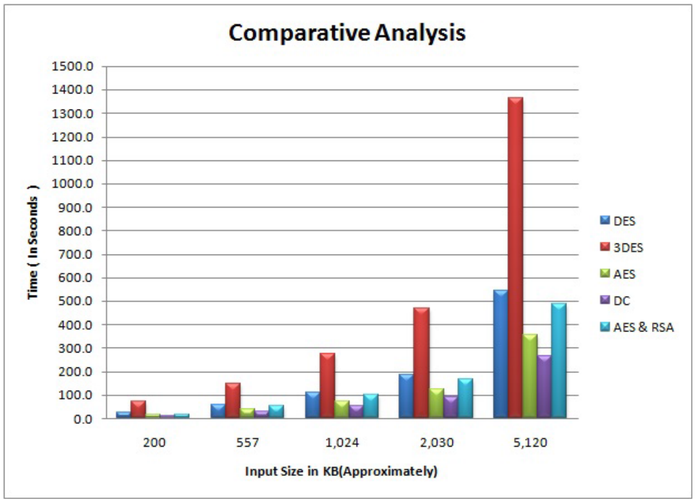


Figure.3: Performance of different algorithms.

For DC although it is more secure, resource utilization is also more as compared with other algorithms.

VI. CONCLUSION

Configuring role based model with traditional model provides efficient security and it can also be implemented with encryption algorithm. In this work new Data Crypt algorithm is implemented which provides strong security as shown in analysis.

Acknowledgement
For the implementation of this ERP system, special Thanks to Prof. Ganesh Ingale (IGB Systems), without his support it is not possible to complete this work.

REFERENCES

[1] Lan Zhou, Vijay Varadharajan, and Michael Hitchens,” Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12, DECEMBER 2013 1947

[2] Sylvia Osborn, Ravi Sandhu George Mason University,” Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies”, ACM Transactions on Information and System Security, Vol. 3, No. 2, May 2000, Pages 85–106.

[3] Bakry, A. H. and Bakry, S. H. (2005). “Enterprise resource planning – a review and a STOPE view,” International Journal of Network Management 15. pp. 363-370.

[4] Prof. S.A.Ubale and Dr. S.S. Apte, “Study and Implementation of Code Access Security with .Net Framework for Windows Operating System”, International Journal of Computer Engineering & Technology (IJCET), Volume 3, Issue 3, 2012, pp. 426 - 434, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375

[5] Prof. S. A. Ubale, Dr. S. S. Apte, “Comparison of ACL Based Security Models for securing resources for Windows operating system “, IJSHRE Volume 2 Issue 6 Page No 63.

[6] Tingyuan Nie, and Teng Zhang ,A Study of DES and Blowfish Encryption Algorithm, IEEE publications, 2009.

[7] Singh, S preet, and Maini, Raman Comparison of Data Encryption Algorithms, International Journal of Computer science and Communication, vol.2,No.1,January–June 2011,pp.125- 127.A.