Integrating basic Access Control Models for efficient security along with encryption for the ERP System

Prof. Swapnaja A. Ubale
Research Scholar (Computer Science & Engineering Department)
Research Center - Walchand Institute of Technology , Solapur Maharashtra, India
Email – swapnaja.b.more@gmail.com

Dr. S.S. Apte
Research Guide (Ph D) (Computer Science & 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 (DAC). Currently, 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 mandatory and discretionary model for making application to be more secure is proposed. 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 BASIC STRUCTURE OF A GOOD 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 should 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 MAC model central system is governed by central control. In DAC owner can control access to objects created by it only. In RBAC according to role hierarchy access is provided. For ERP these three access control models are integrated along with new encryption algorithm data crypt. Data crypt is explained and compared with other encryption algorithm as AES in following sections.

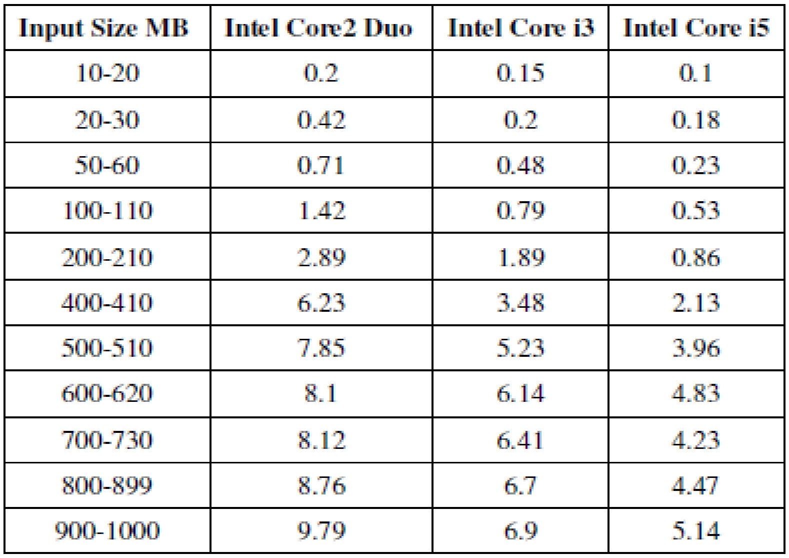
II PERFORMANCE ANALYSIS OF ENCRYPTION ALGORITHMS

Table 1 Key Size of encryption algorithms

Algorithm	Key Size (Bits)	Block Size (Bits)
DES	64	64
Rijndael(AES)	256	128
Data crypt	448	64

Table 1 shows the Key Size used in this experiment. Longer key lengths mean more effort must be put forward to break the encrypted data security. For Data Crypt (DC), key length used is more as compared with AES and DES. Encryption algorithms are compared on different processors as given below.

Table 2: Performance Result of DC algorithm



Input Size MB	Intel Core2 Duo	Intel Core i3	Intel Core i5
10-20	0.2	0.15	0.1
20-30	0.42	0.2	0.18
50-60	0.71	0.48	0.23
100-110	1.42	0.79	0.53
200-210	2.89	1.89	0.86
400-410	6.23	3.48	2.13
500-510	7.85	5.23	3.96
600-620	8.1	6.14	4.83
700-730	8.12	6.41	4.23
800-899	8.76	6.7	4.47
900-1000	9.79	6.9	5.14

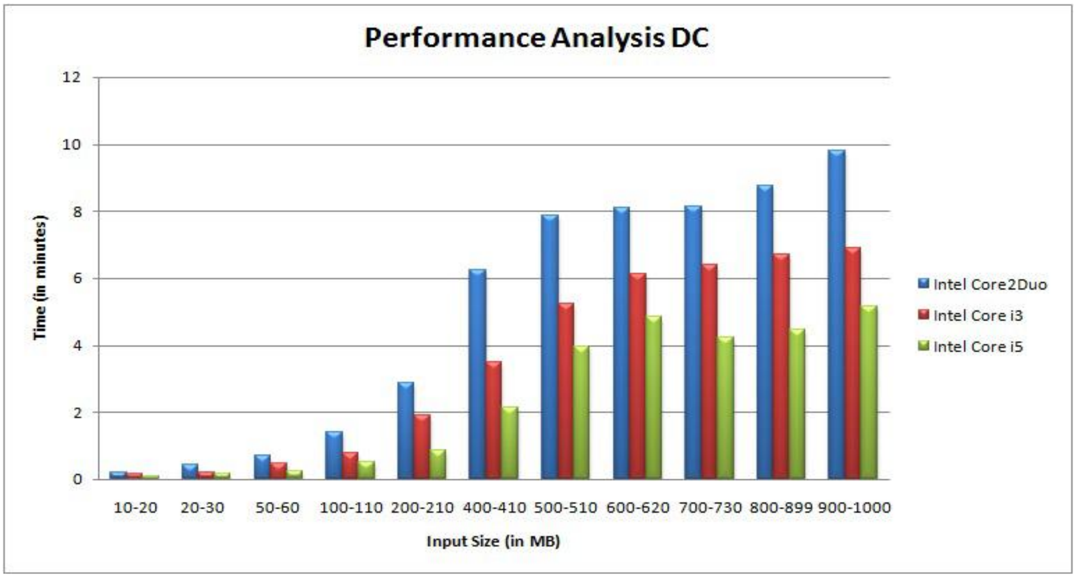
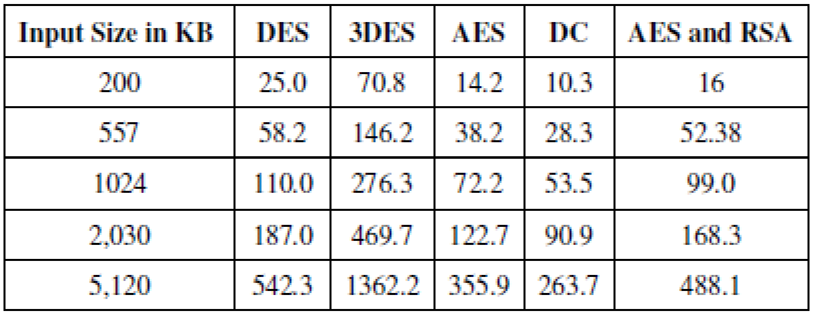


Figure 1: Performance Graph of DC Algorithm.

From above analysis, it is observed that for DC algorithm, for encrypting 10-20 MB of data it requires 0.2 minutes on Intel Core2Duo, 0.15 minutes on Intel Corei3, 0.1 minutes on Intel Corei5. DC is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption. This algorithm produces a stream of pseudo-random values. For generating pseudo-random values key is used as seed or base. XOR of the input stream and these values is calculated, bit by bit. The encryption and decryption process is the same as the data stream, is simply apply XOR with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version. This implementation works for the individual client and it is quick in software. So time comparatively less as compared with other algorithms as AES, RSA.

Table 3: 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

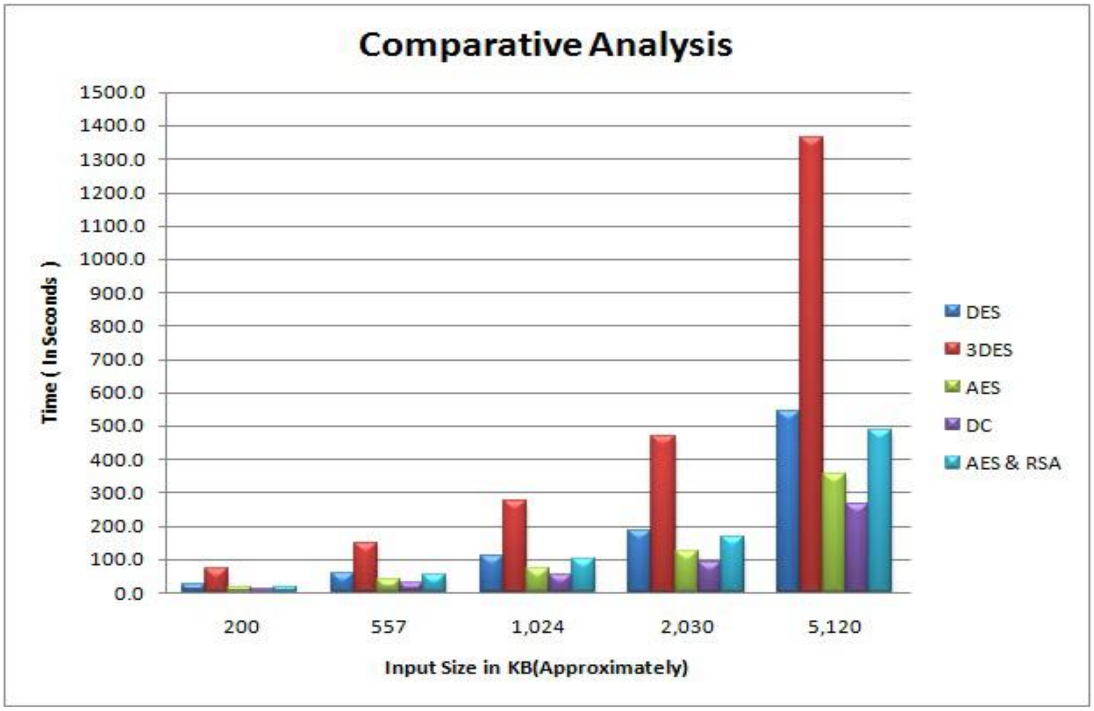
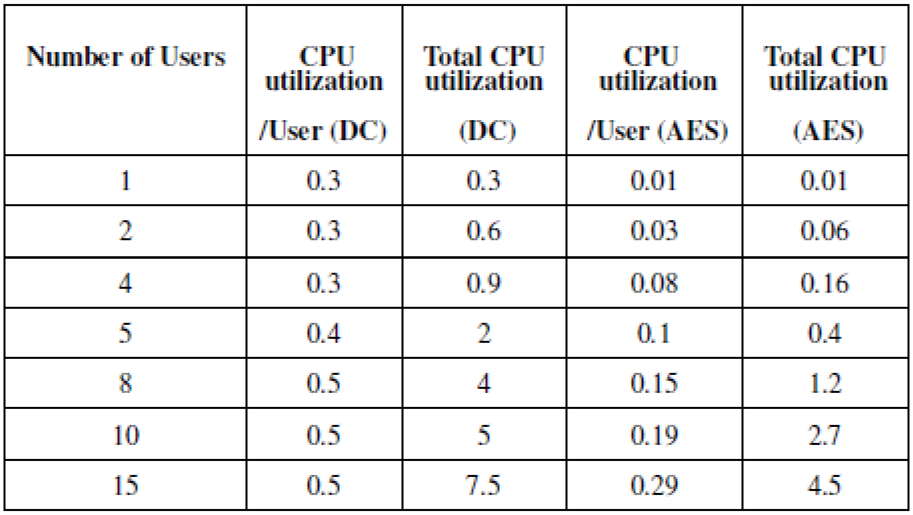


Figure 2: Performance of different algorithms.

From Comparative analysis, as shown in Table 3, it is observed that, DC requires less time as compared with other encryption algorithms as AES, integrated AES –RSA as it is discussed earlier.

Further analysis is done based on CPU utilization, for each algorithm, on Core 2 duo processor and 2 GB ram.

Table 4: CPU utilization of DC and AES Algorithm



Number of Users	CPU utilization /User (DC)	Total CPU utilization (DC)	CPU utilization /User (AES)	Total CPU utilization (AES)
1	0.3	0.3	0.01	0.01
2	0.3	0.6	0.03	0.06
4	0.3	0.9	0.08	0.16
5	0.4	2	0.1	0.4
8	0.5	4	0.15	1.2
10	0.5	5	0.19	2.7
15	0.5	7.5	0.29	4.5

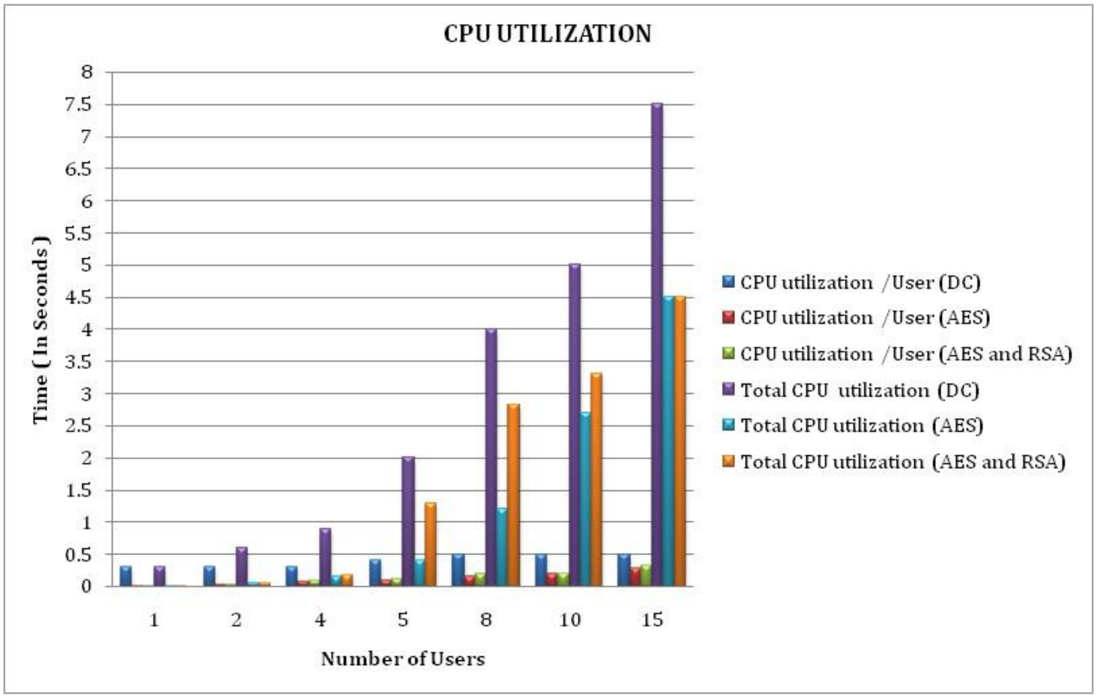


Figure 3: CPU Utilization

From Table 4, it is observed that CPU utilization of DC algorithm is more than AES. CPU utilization increases as number of users increase. As for 1 user, DC utilizes CPU for 0.35 seconds, AES utilizes CPU for 0.03 seconds. Data Crypt works for the individual client. The key stream is completely independent of the plaintext used. Key length is used to generate state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream. Apply XOR on the generated stream with the plaintext to give the cipher text. And this implementation works for individual client. It is going to generate different pseudo code for different client, as per the state table. So resource utilization and memory requirement for DC is more as compared with AES, RSA encryption algorithms. So it is observed that although, DC takes less time for encryption, CPU utilization for DC is more as compared with other encryption algorithm. With integrated ACL models and data Crypt algorithm ERP become more secure

III. CONCLUSION

Integrated access control model MAC, DAC and RBAC 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. As key length used for data crypt is more than other algorithms, it is stronger in security but CPU utilization of data crypt is more than other encryption algorithms (AES). So according to requirement of application security, encryption algorithm can be chosen.

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.

IV. REFERENCE

[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.

[8] R. Sandhu. “The next generation of access control models: Do we need them and what should they be?”, In SACMAT –01, May 2001, page 53.

[9] W. Stallings, “Cryptography and Network Security Principles and Practices”, Fourth Edition, Pearson Education, Prentice Hall, 2009.

[10] Daemen, J., and Rijmen, V. ,Rijndael: “The Advanced Encryption Standard”. Dr. Dobb 's Journal, March 2001.

[11] R.L.Rivest, A.Shamir, and L.Adleman, A Method for Obtaining Digital Signatures and Public–Key Cryptosystems, Communication of the ACM, Volume 21 No. 2, Feb. 1978.