POTENTIAL COVERT CHANNEL IN DISTRIBUTED DATABASE

Richa Punia[1] , Dr. Sona Malhotra[2]

[1](Department of CSE , UIET KURUKSHETRA, Kurukshetra University INDIA)

[2](Department of CSE , UIET KURUKSHETRA, Kurukshetra University INDIA)

Abstract: *In today's Environment. There is need of distributed database in communication. This provides a faster access and remove delays throughout the system .The paper will examine the features of distributed database architecture. The learning of distributed database management system will lead us for successful design. The design will improve scalability ,accessibility and flexibility while accessing data .In distributed System there is conflicts in real time performance and security can be unsolvable .This issue is Improved by allowing database to provide partial security violation so that real time performance is improved such as a covert channel at the time of failure. The main aim is to provide a efficient communication in efficient manner .This design also provide a non blocking communication between different levels. This design will improve a response time and delays throughout the system . In this paper we discuss partial security issues for a DDBMS*

Keywords -- *Distributed database System security, distributed database, distributed database management system, distributed database retrieval problems, discretionary security in distributed database, query processing and multilevel security.*

I. INTRODUCTION

*In today's Environment. There is need of distributed database in communication***.** This provides a faster access and remove delays throughout the system. that improves the system performance and improves a single point of failure problem . the distributed system provides a better way of communication environment to the system

Distributed Database System

Distributed database system provides an improvement in communication and data processing due to its data distribution throughout different network sites.[3] A distributed database is a collection or gathering of databases that can be stored at different computer network sites. Every database may involve different database management systems and different architectures that distribute the execution of transactions. The main objective of a distributed database management system (DDBMS) is to control the management of a distributed database (DDB) in such a way that it appears to the user as a centralized database. There is eight transparencies are believed to incorporate the desired functions of a distributed database system.

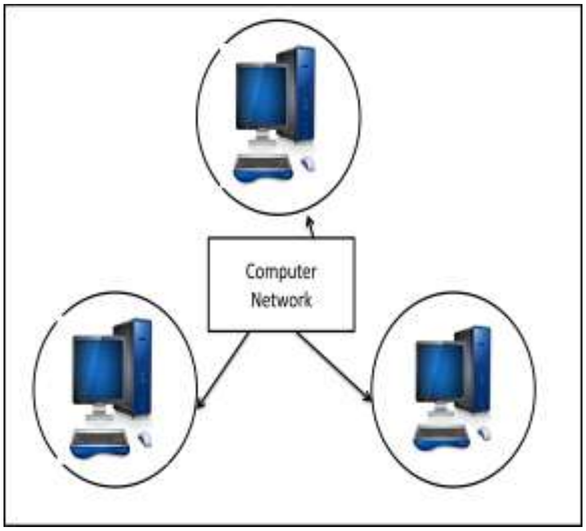


Fig : Distributed System

Classification of Distributed Database Management System (DDBMS)

A collection of multiple, logically interrelated databases that distributed throughout a network. A distributed database management system is the software system that permits the management of the distributed database and makes the distribution transparent to the users. A distributed database system consists of loosely coupled sites that involve no sharing of physical component **distributed database system** allows applications to access data from local and remote databases. In a **homogenous DDB system**, each of database is an Oracle based Database. In a **heterogeneous DDB system**, at least one of the database is not Oracle based Database. Distributed databases use client/**server** architecture is used to process information requests.

Main Characteristics of distributed database

- Data is used at one location only (other than centralized).
- Data accuracy and, confidentiality, and security is a local responsibility of DDB
- Files are very simple and used by only a few applications. In this case, there is no benefit of maintaining complex centralized software. Cost of updates is too much high for a centralized storage system.

Security Issues in Distributed Database

Database security is the system, and processes, and procedures that protect a database from unauthorised activity. Unauthorised activity can be categorized like authenticated misuse of system, malicious attacks or inadvertent mistakes made by authorized individuals and processes.

- **Access control**
- **Auditing**
- **Authentication**
- **Encryption**

There is conflicts in real time performance and real time system can be unsolvable. This issue is improved by providing partial security violation to the system. such as a covert channels. this improve performance of the system.

II. Partial security violation

In distributed database, a partial security is used to improve the performance of system. Systems that are partially secured allows potential security violations as such like covert channel used in certain situations. Here We describe the basic idea of requirement specification that allows the system designer is used to specify important properties of the database at a suitable level. In many distributed system , the security is one of important constraint, since the system maintains sensitive information to be shared by multiple users with different levels of security clearances.. It is important to define the exact meaning of partial security, for security violations of secured or we can say sensitive data must be strictly controlled by the system. A security violation here indicates a potential covert channel, i.e., the transaction may be affected by a transaction at a higher security level. One main approach is to define the security in terms of a percentage of security violations allowed in the system. However, the value of this definition is questionable. In fact a system may allow a very low percentage of security violations, this fact alone reveals nothing about the security of individual data. For example, a system might have a 99% security level, but the 1% of insecurity might allow the most sensitive piece of data to leak out from the system database as per permitted by higher authority. A more precise parameter would be necessary for the applications where security is a serious concern. Thus in partial security the violation is allowed in certain security level.

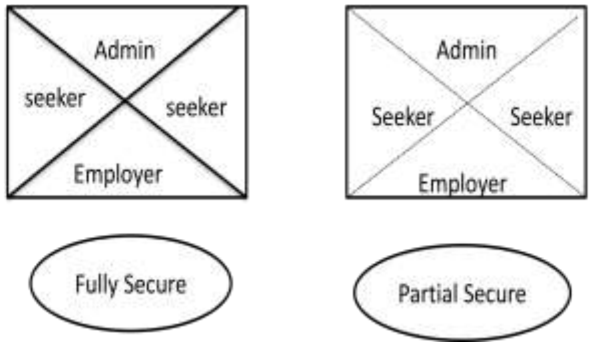
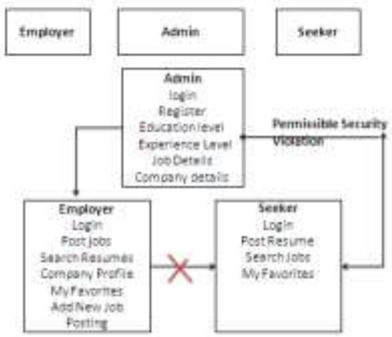


Figure: full and partial security in Distributed database

Thus in partial security the violation is allowed in certain security levels shown in above figure. The solid line indicates that the system is fully secure whereas doted lines defines that the system can violate security under certain circumstances

A. Framwork of proposed solution:



The below mentioned discussion depicts the overall security breaches in different layers of the layered framework displayed above.

At Admin level:-

This layer is in fully protected mode; here all the permission and validations are imposed at different levels. Security is not compromised at this very level. The security is very high as compared to other levels.

At Employer level:-

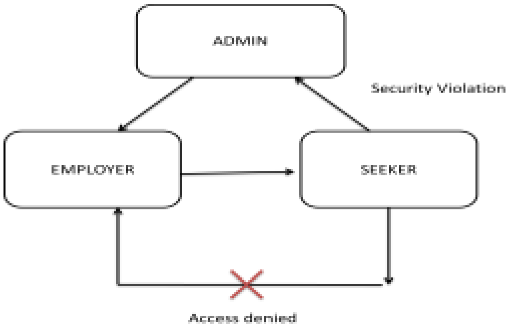
This layer is in partially protected mode; here all the permission and validations are imposed in such way that only few of the information areas can be accessed at lower levels up to some extent..

At Seekers level:-

This layer is also in partially protected mode; here all the permission and validations are imposed in such way that only few of the information areas can be accessed from upper level up to limit/range at 1 or from upper level to limit/range at 2 .

In Job site starter kit (jssk) in this system the Employer post jobs, Search resumes and add new jobs for the seeker. But if seeker is not getting any job details from Employer/Provider in that case seeker has ability to access to admin with partial security violation which is permissible by admin.

III METHODOLOGY & ASSUMPTIONS



Assumptions Taken

User is authorized to access the data depending upon user access levels. Four levels of users have been proposed depending upon the access permissions given to each user.

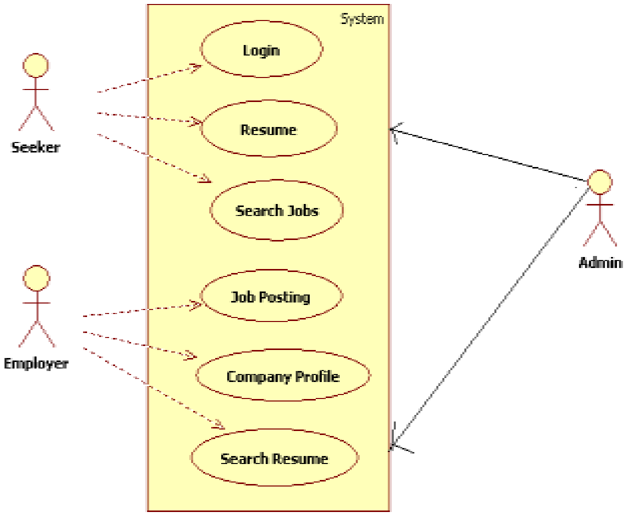
At Admin level:-
1. By restricted its services, if it not fulfills some security criteria.

At job Employer level:-
1. Upload resumes and access Job details updated by Employer

At job seekers level:-
1. If unable to get the Job details can check it at super user level
2. By restricted its viewing fields if he/she not fulfill some security constraints.

Proposed Architecture

Depending upon the above assumptions we have proposed an architecture that will display the above mentioned methodology layers defined. The proposed architecture consists of three basic layers ADMIN, JOB EMPLOYER and JOB SEEKER. Depending on the levels the security violation is defined in the following architecture. At the top level is ADMIN, next level is owned by JOB EMPLOYER, last level is obtained by JOB SEEKER.



This depicts the partial security violation at the SEEKER level as levels mentioned in the methodology proposed.

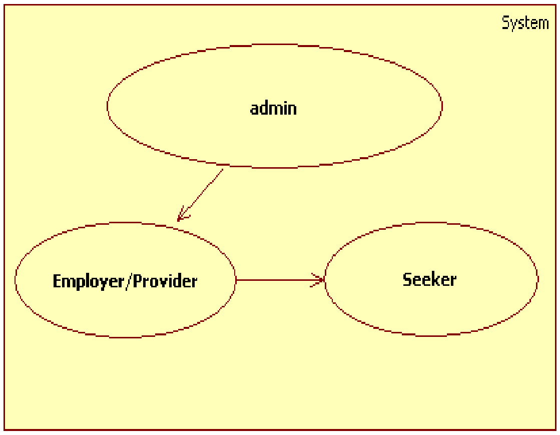


Fig: Security violations for Job Seeker

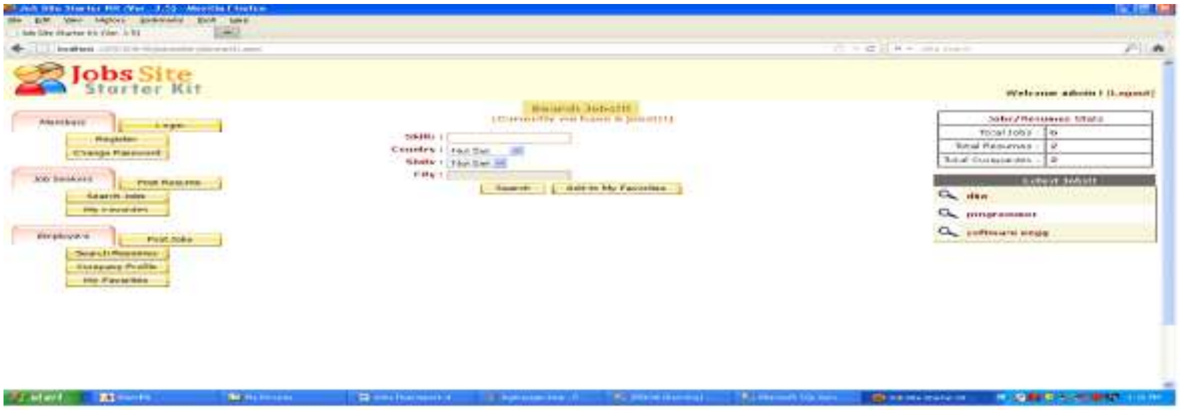
This JSSK is designed by keeping in mind both parties Job providers and Job seekers. JSSK allows Job seekers to register themselves then get details like job details with skills and experience within the system, and then on the other hand even it allows job providers to post their requirements with the system through resume.

Job Site Starter Kit is helpful for the job seeker which are in need of jobs. This violation provides a better way to access the system. There is no blocking and delays in the system This portals main aim is to provide the job details available for the job seekers without taking any charge from them in IT technologies and provides a profile details regarding company. JSSK will automatically provide access to all job details to job seekers whose skills are matched with the requirement or not

This improves Transaction time and response time.

Resultant Screenshot:

Admin login page:



Search Jobs!!!

Skills :

Country : Not Set

State : Not Set

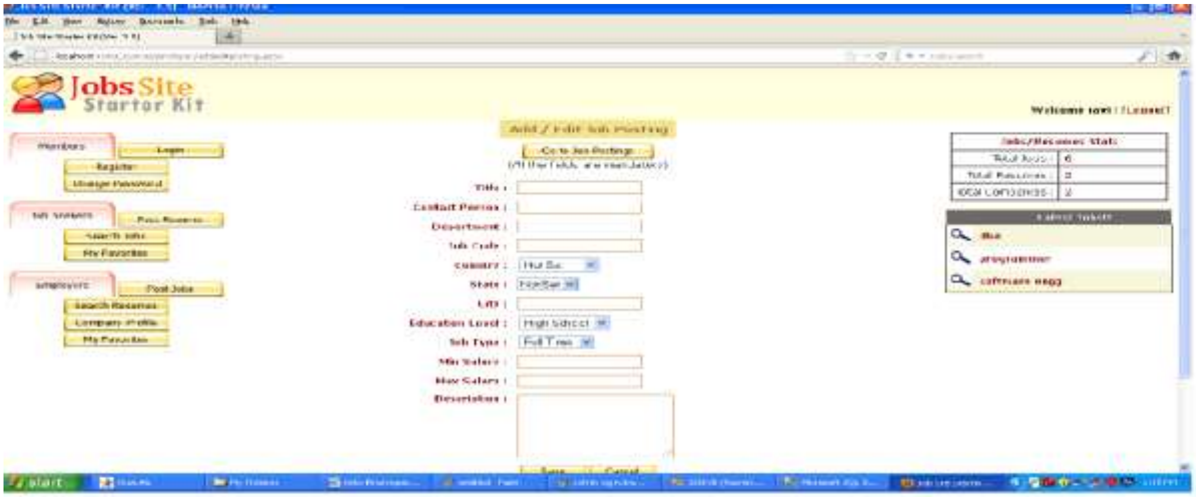
City :

Jobs/Resumes Stats	
Total Jobs :	6
Total Resumes :	2
Total Companies :	2

Latest Jobs!!!

- dba
- programmer
- software engg

Employer login page:



Add / Edit Job Posting

(All the fields are mandatory)

Title :

Contact Person :

Department :

Job Code :

Country : Not Set

State : Not Set

City :

Education Level : High School

Job Type : Full Time

Min Salary :

Max Salary :

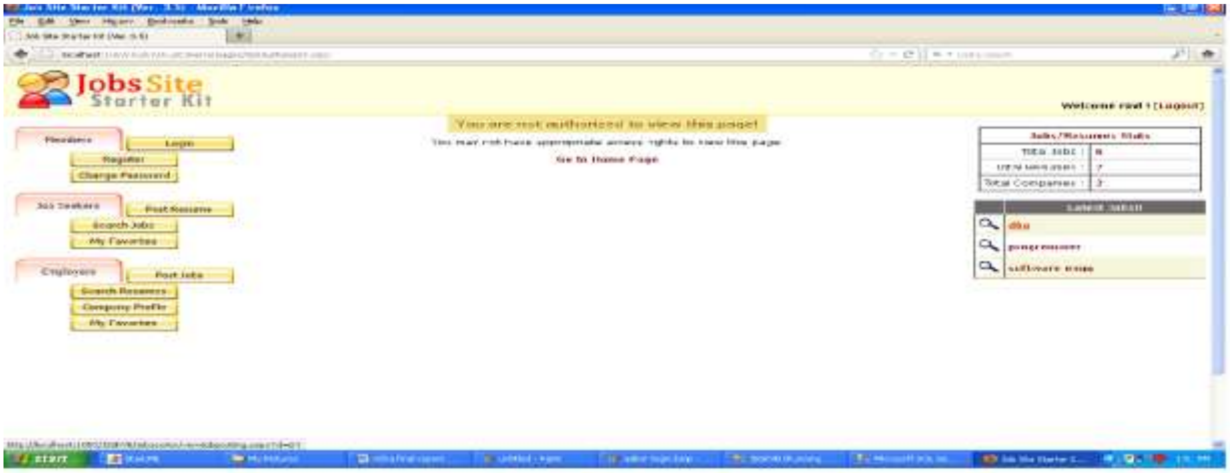
Description :

Jobs/Resumes Stats	
Total Jobs :	6
Total Resumes :	3
Total Companies :	2

Latest Jobs!!!

- dba
- programmer
- software engg

Employer Don’t access because admin is not permitted for accessing data :



You are not authorized to view this page!

You may not have appropriate access rights to view this page.

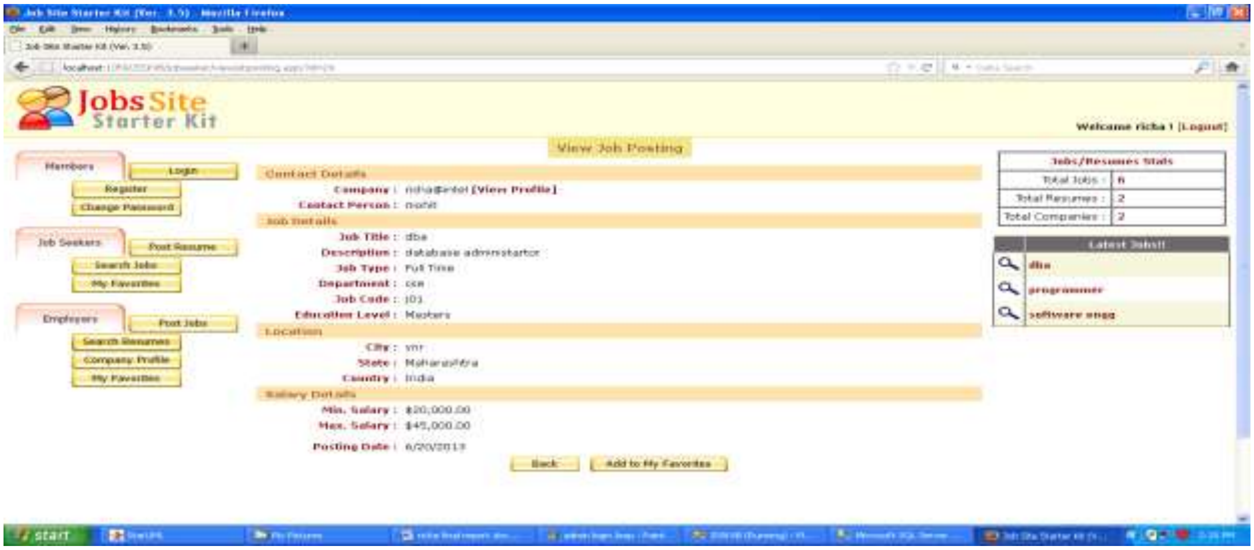
Go to Home Page

Jobs/Resumes Stats	
Total Jobs :	6
Total Resumes :	2
Total Companies :	2

Latest Jobs!!

- dba
- programmer
- software engg

Seeker view job Posting:



View Job Posting

Contact Details

Company : richa@intel [View Profile]
Contact Person : mohit

Job Details

Job Title : dba
Description : database administartor
Job Type : Full Time
Department : cce
Job Code : j01
Education Level : Masters

Location

City : vnr
State : Maharashtra
Country : India

Salary Details

Min. Salary : $20,000.00
Max. Salary : $45,000.00

Posting Date : 6/20/2013

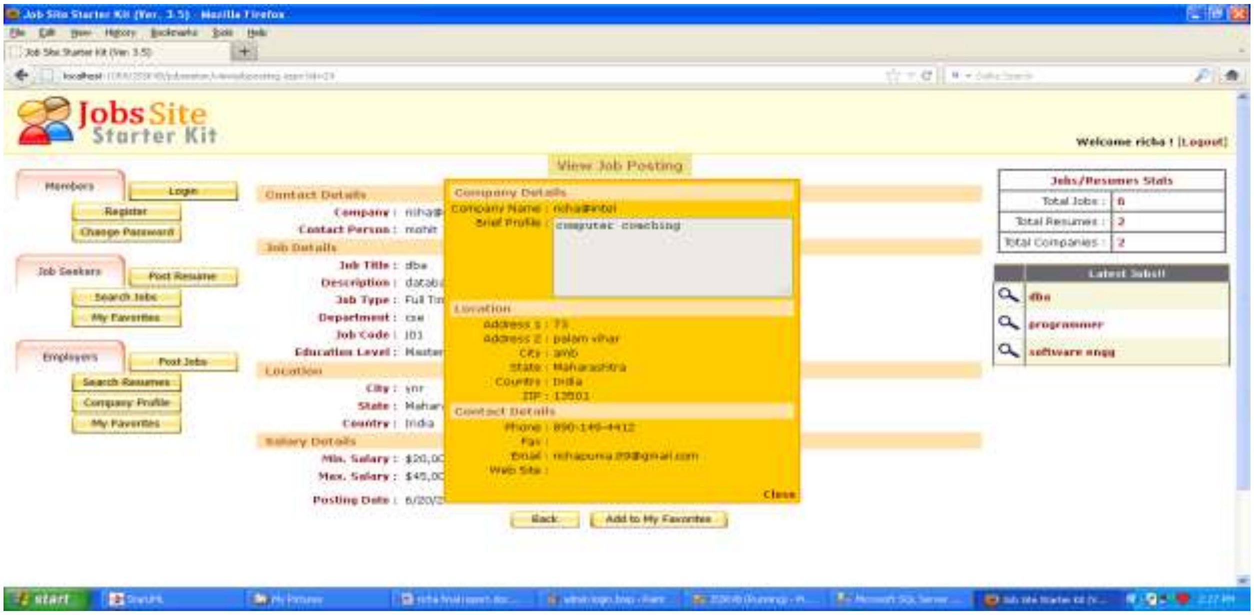
Back | Add to My Favorites

Jobs/Resumes Stats	
Total Jobs :	6
Total Resumes :	2
Total Companies :	2

Latest Jobs!!

- dba
- programmer
- software engg

Seeker view job profile details which is not accessible by employer that is permissible by admin to seeker i.e it provide a partial security violation to the system when employer is not responding to seeker.



Contact Details

Company : nihag

Contact Person : mohit

Job Details

Job Title : dba

Description : datab

Job Type : Full Tin

Department : cse

Job Code : 101

Education Level : Master

Location

City : ynr

State : Mahar

Country : India

Salary Details

Min. Salary : $20,0C

Max. Salary : $45,0C

Posting Date : 6/20/2

Company Details

Company Name : nihaa#intel

Brief Profile : computer coaching

Location

Address 1 : 73

Address 2 : palam vihar

City : amb

State : Maharashtra

Country : India

ZIP : 13501

Contact Details

Phone : 890-149-4412

Fax :

Email : nihapuma.89@gmail.com

Web Site :

Jobs/Resumes Stats	
Total Jobs :	6
Total Resumes :	2
Total Companies :	2

	Latest Jobs!!
🔍	dba
🔍	programmer
🔍	software engg

IV. CONCLUSION

For many applications, it is important to provide more secured, efficient and reliable access to multilevel databases stored at different sites. At last we can say that with this proposed solution allows the security violation with security aspect of system performance. This will increase system performance by improving the response time and transaction access time.

VIII. REFRENCES

[1] Steven P. Coy-"*Security Implications of the Choice of Distributed Database Management System Model: Relational vs. Object-Oriented*".(2010)

2] Ghazi Alkhatib-"Transaction Management in Distributed Database Systems: the Case of Oracle's Two-Phase Commit" Journal of Information Systems Education, Summer (2002)

[3] Sang H. Son and Craig Chaney "Supporting the requirements for multilevel secure and real-time database in distribute environments", pp.136—147(1997).

[4] Bhavani Thuraisingham -"Multilevel Security Issues in Distributed Database Management System II"-Computers & Security, 10 (1991) 727-747(2007).

[5] Moses Garuba-"Performance study of a COTS Distributed DBMS adapted for multilevel security" Consultant scientist, U.S. Government, Washington DC, (2004).

[6] Charles P. Pfleeger, Shari Lawrence Pfleeger "Security in Computing", www.studytemple.com/.../2830-security-computing-charles-p-pfleeger,4th Edition (2008).

[7] T. F. Keefe, W. T. Tsai, and J. Srivastava. "*Multilevel Secure Database Concurrency Control*," In Proceedings of the Sixth International Conference on Data Engineering, pp 337-344, Los Angeles, CA, February 1990.

[8] Davidson, M.A. "*Security in an Oracle data base environment*". Information Systems Security (2007).

[9] P. C. Clements, C. L. Heitmeyer, B. G. Labaw, and A. T. Rose. "*MT: A Toolset for Specifying and Analyzing Real-Time Systems*," Real-Time System Symposium, Lake Buena Vista, FL, December 1990.

[10] D. E. Bell and L. J. LaPadula. "*Secure Computer Systems: Unified Exposition and Multics Interpretation*," The Mitre Corp., March 1976.

[11]Newman, "*A. Database Security Best Practices Security*". Retrieved April 1, 2007 from Business Source Premier database. Palmquist, M., Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B., (2005).

[12] Andre N. Fredette and Rance Cleveland. "*RTSL: A Language for Real-Time Schedulability Analysis*," Real-Time System Symposium, Raleigh-Durham, NC, December 1993.

[13] Luftman, J., Managing the Information Technology Resource: Leadership in the Information Age. Upper Saddle River, NJ. Pearson Education, Inc. (2004).

[14] Millen /Lunt, A.Tamaru, F.Gilham, R.Jagannathan, C.Jalali, P.Neumann and H.Javitz, "Security for Object-Oriented Database ",IT-security and privacy-design and use of privacy"-enhancing (1992)

[15] Thuraisingham, B. "Database and Applications Security: Integrating Informations Security and Data Management". Boca Raton, FL: Auerbach Publications (2005).

[16] Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review (2007) .