ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Role-Based Access Control within RDBMS

Shilpa S. Shete, Prof.C.S. Kulkarni

M.E. Student, Dept. of Computer Science, Rajashree Shahu School of Engineering & Research, Pune , Maharshtra, India

Assistant professor, Dept. of Computer Science, Rajashree Shahu School of Engineering & Research, Pune , Maharshtra, India

ABSTRACT: Preserving Privacy in data-mining environment is a major challenge for organisations and individuals. Nowadays there is a rapid growth in mobile computing and digital networks, individuals like to do online shopping, online transaction for personal use or for business purposes. They are more serious about their data security and privacy. Therefore database security is important for all businesses and even home computer users. Our proposed system presents Role Based Access Control system, which controls access of unauthorized users and authorization of valid users, providing high security to database. It provides database security at table, row and column level. Our proposed system is independent of any domain specific database and can act as a standalone plug and play component.

KEYWORDS: database security, Role based Access Control, data authentication and authorisation.

I. INTRODUCTION

Organizations collect customer's personal information and some other details for business purposes. It is natural thing that the organization will use this information for different purposes, this leads to concern that the personal data may be misused. Many organizations collect, store and use huge amount of personal information. Data security is important for all businesses and even home computer users. Payment information, client information, bank account details and personal files - all of this information can be hard to replace and potentially dangerous if it is accessed by unauthorized users. Data lost due to disasters such as a flood or fire is overwhelming, but data loss due to hackers or a malware infection can have much large consequences. Therefore in order to achieve data quality and privacy, there should be clear compromise between customers and organization. Companies are setting good privacy policies thus trying to build up more customers. By considering the privacy of customers, an organization has to define secure privacy policies to remove the fear of customers. Therefore in an internal management system, an efficient, reliable, effective and secure privacy policy should be defined depending upon customers requirements.

II. RELATED WORK

Most of work is carried out to protect the privacy of person information and showed that the use of purpose should be used as the basis for access control for specifying a privacy policy. A privacy policy tells that data can only be used for its actual purpose (intended use of data) and an access purpose (Intention for accessing data) is compliant with the data's intended purpose.

'The Enterprise Privacy Authorization Language (EPAL)' [3], developed by IBM is used for specifying privacy policies to define data handling policies in IT systems. An EPAL policy defines a hierarchy of data categories, user categories and purposes. User categories are the entities (users/groups) that use collected data and data categories that define different categories of data. Purposes define the intension behind accessing the data. An EPAL policy also defines sets of actions, obligations and conditions. Actions define how data is used and obligations define actions that must be taken by the environment of EPAL. Conditions are Boolean expressions that evaluate the context. Privacy authorization rules are defined using these elements and each rule allows or rejects actions on data categories for specific purposes.

The main drawback of EPAL is that it does not provide support for linking data categories with the data stored in the database. Also it does not assure that it follows all the policies as per its definition.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

The W3C's platform for privacy preservation (P3P) is created for privacy preservation. It allows users to get control of their private information when they visit multiple web sites. P3P allows web sites to define their privacy policies in machine readable format, which specifies that what data is collected, who can access the data, for what purposes and how long the data will be stored by the sites. Browsers which support P3P can read these privacy policies automatically and compares to the customer's privacy preferences. These preferences are specified in the privacy preference language such as P3P Preference Exchange Language (APPEL) [2] which is designed by W3C.

The main drawback of P3P is that it does not provide any mechanism to assure that the compliance of privacy policies is consistent with the internal data processing. Thus P3P is not a reliable tool to keep information security and does not help organizations to keep their promises.

The concept of Hippocratic databases which suggests privacy protection is relational database systems was introduced by Agarwal et al.[9]. A Hippocratic database includes privacy policies and authorizations that associate with each attribute and each user's purposes. They presented privacy preserving database architecture called Strawman which was based on access control based on purposes. The architecture uses privacy metadata which consists of privacy policies and privacy authorizations stored in two tables.

Multilevel secure traditional databases [4, 5, 6, 7, 8] also suggests the policies for designing a fine grained secure data model. In multilevel relational database system, different security levels are defined and each type of data is classified into one security level. Every user has given a security right. The system ensures that the user can access only that data from that security level which he/she has a clearance. This ensures that there is no information flow from higher security level to lower security level.

III. PROBLEM STATEMENT

Business data protection helps to customer details, financial information, sales figures and other key business data, protecting which is one of your most important assets. Good business data protection keeps information safe, as well as ensuring you comply with relevant data protection rules and legislation. You should think about business data protection alongside your backup options to ensure your data is safe, even if you suffer a data protection breach. When any company loses data it has to face the problems like loss of reputation if the sensitive data is leaked to the competitor, accidental loss of data prevent marketing activities or it may lead to legal action and substantial fine. Hence there is a need of a system who ensures that your information remains confidential and only those who should access that information and ensuring that no one can update the information so end users can rely on its accuracy. The need of this proposal is to design a system which allows role based access to the relational database system which will do authentication, authorization and audit. The system should provide the security at very low level like table, row and column level.

IV. OBJECTIVE

With the advent of tremendous growth in fields related to mobile computing and digital networks, the amount of personal and sensitive data which are processed and stored is rapidly growing. In such situation, database management systems play an important role which store data and provide tools to access and analyze that data. Although data protection via access control is becoming a key requirement for DBMS, currently many commercial DBMS systems include quite basic form of access control by defining user roles, access privileges at database and table level. Still there is a need of extending such securities at row and column level. Hence there is a need to design a system which will give access rights to users at very detailed level contributing a design of Role Based Access Control (RBAC) in database in which permissions will be associated with user roles and users will be members of appropriate roles.

V. MOTIVATION

In today's world, privacy becomes a major concern for both customers and organizations hence privacy preservation is a big challenge. Enterprises collect customer's private information along with some other factors during any type of marketing activities. It is a natural thought that the enterprise will use this information for different purposes, this leads to the thought that the personal data can be misused. As individuals are more anxious about their privacy, they are

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

using more online methods to carry out their businesses and hence many large organizations are losing major amount of potential profits. Hence a system is required which will grant access to data only to authorized users.

VI. EXISTING SYSTEM

An existing system contains three modules as follows.

1. Access Control Management module - This module is used for
1) Defining the set of purposes involved in policy specification and enforcement;
2) Specifying purpose-based authorizations
3) Classifying data stored into the target database into data categories used for access control purposes.

2. Policy Management module - It is used for fine-grained access control policy management. It can be used to serve users/administrators policy specification requests (e.g., add a policy), as well as to automatically handle updates to the specified policies as a consequence of modifications to the set of purposes or to the scheme of database tables.

3. Enforcement Monitor Module - It enforces access control by means of SQL query rewriting, issuing the rewritten.

VII. PROPOSED SYSTEM

Role Based Access Control (RBAC) system proposes creation of user, roles, groups, permissions. Access control is a means by which the ability is explicitly enabled or disabled in some way. Computer based access controls can suggest not only who or what process may have access to a specific system resource, but also the type of access that is permitted. With RABC, access decisions are based on the roles that are assigned to the users from organization. Roles bring together a set of users on one side and a set of permissions on the other whereas user groups are set of users. Permission is an association between a transformation procedure and object. Permissions are assigned to roles. Roles are assigned to users. The following figure shows the overview of this concept. It also gives an idea of the interconnection of all entities with each other.

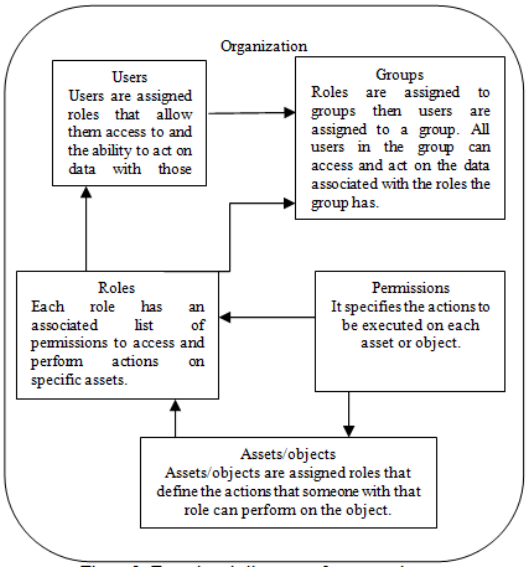

Figure 1. Functional diagram of proposed system

Proposed Algorithm – RBAC Algorithm

1. Check access groups of logged in user.
2. Parse the query. If it is syntactically correct then go to step 3 else stop further processing.
3. Do query derivation.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

1. Get all tables from query and store it in QueryTbl.
2. Get all columns from query and store it in QueryCol.
3. Get all row conditions for the tables mentioned in the query and store it in QueryRow table.

4. If group Id of logged in user is in among the assigned groups of column list, then show that column in result set else show NULL values for that column.
5. If logged in user group id is among the assigned row group ids then only add those rows in result set else exclude it.
6. If tables from the query are among the prohibited access table list, then reject the execution of query.
7. If query derivation process satisfies all the above three conditions, then execute the query and display results.
8. Stop.

Complexity of this algorithm is O(n).

Proposed System UI Design

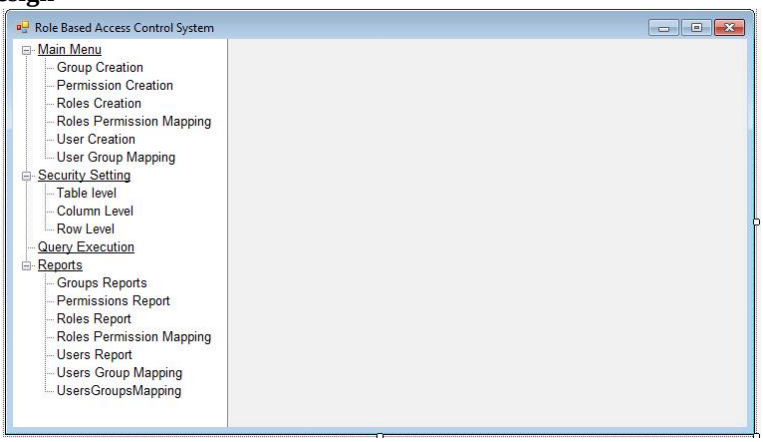

Figure 2. Main Screen of RBAC system

RBAC system has following modules.

1. **Main Menu** – It has following sub menus.
   1. **Group Creation** – Allows creating, editing, deleting new groups in the system. For example developer Group, tester Group, system analyst Group, designer Group, project manager Group, team leader Group, HR Group etc.
   2. **Permission creation** – Allows creating, editing, deleting new permissions in the system. For example 'can execute test cases', 'can execute INSERT query on LIVE DB', 'can access staging database'etc.
   3. **Roles Creation** – Allows creating, editing, deleting of roles in the system. For example developer, tester, system analyst, designer, project manager, team leader, HR etc.
   4. **Roles Permission Mapping** – Allows to map roles to permission. It can map multiple permissions to a single role. Then role can be assigned to group. It saves time to assign permissions to individual user. For example permissions 'can execute INSERT query on LIVE DB', 'can access staging database' can be assigned to role 'developer'.
   5. **Roles Group Mapping** – Allows mapping roles with groups. For example, assigning of 'developer' role in above example to 'developer group'. It will help to assign similar role to multiple users at a time.
   6. **User Creation** – Allows creating, editing, deleting of users.
   7. **User Group Mapping** – Allows mapping of users to groups. For example, assignment of multiple users to developer group.
2. **Security Setting –** It allows setting security on database objects mainly table, column and row. It is the core part of RBAC system. It has three sub menus as follows.

Table Level – It allows setting security rights at table level. Following screen shows the details.As shown in Fig 3.,administrator has to select particular group among the predefined groups from the first drop down. Second drop

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

down shows the list of tables available in the application. Selected group will have prohibited access for the selected table. It is logical to set list of prohibited access than setting list of allowed access for tables because there can be very few tables for which access can be denied.

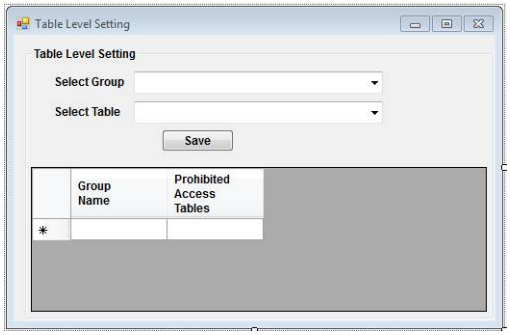

Figure 3. Table Level Setting

1. **Column Level Setting -** It allows setting of security rights at column level. Following screen shot gives the details.

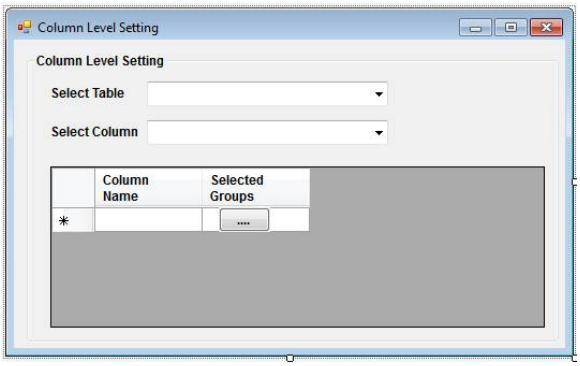

Figure 4. Column Level Setting

Administrator has to select the table from first drop down and all the columns from selected table are displayed in second drop down. In the following grid `Selected Groups0 column has command button which opens the screen which shows all the available groups. Administrator has to select groups. It means that only for those groups, that column is accessible.

Row Level Setting - It allows setting of row access for particular value. Administrator has to select the table and column from that table. In the following grid, under “Column Value” column hardcoded value of selected column is mentioned. “Allowed Access Groups” column shows the list of all allowed groups who can view that column.

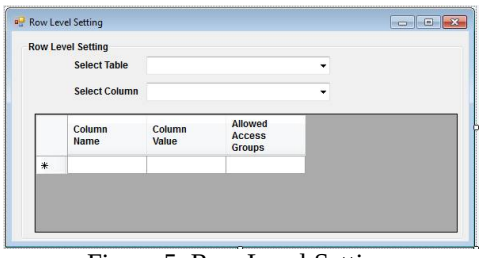

Figure 5. Row Level Setting

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

1. **Query Execution** – It allows user to write and execute the query.

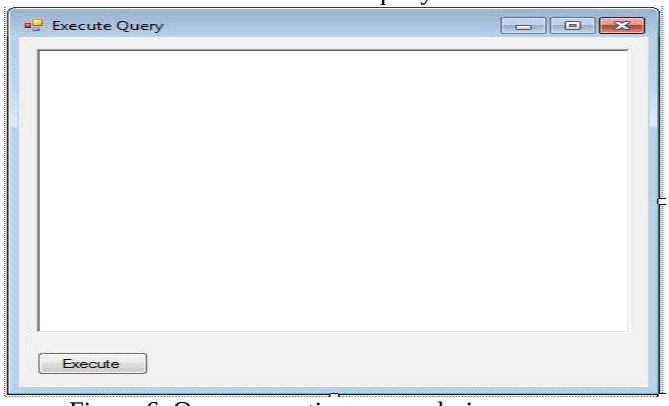

Figure 6. Query execution screen design

VIII. EXPECTED RESULTS

The RBAC system can be tested on multiple live databases. Hence it can be used as a standalone component which can be used in plug and play fashion. Different databases like patient database, university database and sales database can be used for testing this system.
Following screen shots shows the expected results. Following query is executed on AdventureWorks 2012 database of sql server.

```
SELECT
        e.BusinessEntityID, p.FirstName, p.LastName, e.JobTitle, pp.PhoneNumber,
        pnt.Name AS PhoneNumberType, ea.EmailAddress, a.AddressLine1
FROM
        HumanResources.Employee AS e INNER JOIN
        Person.Person AS p ON p.BusinessEntityID = e.BusinessEntityID INNER JOIN
        Person.BusinessEntityAddress AS bea ON bea.BusinessEntityID = e.BusinessEntityID INNER JOIN
        Person.Address AS a ON a.AddressID = bea.AddressID INNER JOIN
        Person.StateProvince AS sp ON sp.StateProvinceID = a.StateProvinceID INNER JOIN Person.CountryRegion
        AS cr ON cr.CountryRegionCode = sp.CountryRegionCode LEFT OUTER JOIN
        Person.PersonPhone AS pp ON pp.BusinessEntityID = p.BusinessEntityID LEFT OUTER JOIN
        Person.PhoneNumberType AS pnt ON pp.PhoneNumberTypeID = pnt.PhoneNumberTypeID LEFT OUTER JOIN
        Person.EmailAddress AS ea ON p.BusinessEntityID = ea.BusinessEntityID
```

For example, for user ‘ABC’, the administrator has set the security rights as follows.

1. Table Level Setting –
   Prohibited table – HumanResources.Employee
2. Column Level Setting –
   PhoneNumber, PhoneNumberType, EmailAddress, AddressLine1
3. Row Level Setting –
   Job Title = Buyer
   Job Title = Vice Precident of Production

Following screen shot shows results in normal conditions when user ‘ABC’ will execute this query from SQL query analyser. i.e. when no security settings are done.

Busin...	FirstName	LastName	JobTitle	PhoneNumber	PhoneNumber...	EmailAddress	AddressLine1
259	Ben	Miller	Buyer	151-555-0113	Work	ben0@adventure-works.c...	101 Candy Rd.
278	Garrett	Vargas	Sales Representative	922-555-0165	Work	garrett1@adventure-work...	10203 Acorn Av...
204	Gabe	Mares	Production Technician - ...	310-555-0117	Work	gabe0@adventure-works....	1061 Buskrik Av...
78	Reuben	D'sa	Production Supervisor - ...	191-555-0112	Work	reuben0@adventure-wor...	1064 Slow Cree...
255	Gordon	Hee	Buyer	230-555-0144	Cell	gordon0@adventure-wor...	108 Lakeside C...
66	Karan	Khanna	Production Technician - ...	447-555-0186	Work	karan0@adventure-works...	1102 Ravenwood
270	François	Ajenstat	Database Administrator	785-555-0110	Cell	françois0@adventure-wor...	1144 Paradise Ct.
22	Sariya	Harnpadoun...	Marketing Specialist	399-555-0176	Work	sariya0@adventure-works...	1185 Dallas Drive
161	Kirk	Koenigsbauer	Production Technician - ...	669-555-0150	Work	kirk0@adventure-works.c...	1220 Bradford ...

Fig. 7 Result screen shot before applying any security settings

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

In above screen shot, data from "HumanResources.Employee" table is displayed for user 'ABC' for which this user has prohibited access. Also he should not view the column data for PhoneNumber, PhoneNumberType, EmailAddress, and AddressLine1. Similarly he should not view the rows with job title 'Buyer' and 'Precident of Production'. When user executes this query from sql , no restrictions are made for hiding some data.

Following screen shot shows results when query is executed from RBAC system from 'Execute Query' screen. Consider three scenarios.

1. **Only Table Level setting is done.** (i.e. prohibited access is set on HumanResoucres.Employee table) In this case query is straightaway rejected.

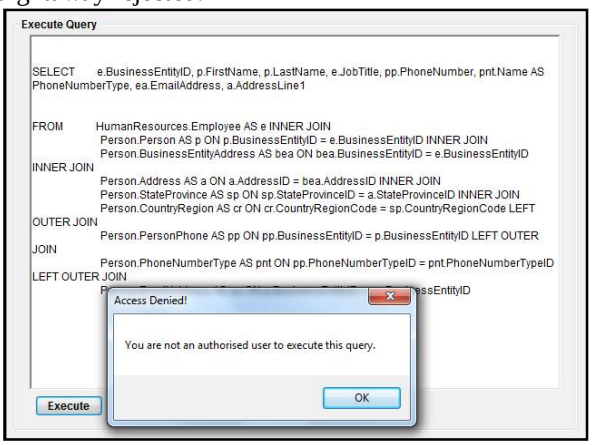

Fig. 8 Expected outcome for Table Level setting

1. **Only Column Level settings are done.** (i.e. PhoneNumber, PhoneNumberType, EmailAddress, and AddressLine1 are not displayed for user 'ABC')

	Busin...	FirstName	LastName	JobTitle	PhonenNumber	PhoneNumber...	EmailAddress	AddressLine1
▸	1	Ken	Sánchez	Chief Executive Officer	NULL	NULL	NULL	NULL
	2	Terri	Duffy	Vice President of Engineer...	NULL	NULL	NULL	NULL
	3	Roberto	Tamburello	Engineering Manager	NULL	NULL	NULL	NULL
	4	Rob	Walters	Senior Tool Designer	NULL	NULL	NULL	NULL
	5	Gail	Erickson	Design Engineer	NULL	NULL	NULL	NULL
	6	Jossef	Goldberg	Design Engineer	NULL	NULL	NULL	NULL
	7	Dylan	Miller	Research and Developme...	NULL	NULL	NULL	NULL

Fig 9. Expected outcome for Column level setting

1. Only Row Level Settings are done. (i.e. rows with column value 'JobTitle = Buyer' and 'JobTitle = Precident of Production' should not be displayed in result set for user 'ABC')

	Busin...	FirstName	LastName	JobTitle	PhoneNumber	PhoneNumber...	EmailAddress	AddressLine1
▸	278	Garrett	Vargas	Sales Representative	922-555-0165	Work	garrett1@adventure-work...	10203 Acorn Av...
	204	Gabe	Mares	Production Technician - ...	310-555-0117	Work	gabe0@adventure-works....	1061 Buskrik Av...
	78	Reuben	D'sa	Production Supervisor - ...	191-555-0112	Work	reuben0@adventure-wor...	1064 Slow Cree...
	66	Karan	Khanna	Production Technician - ...	447-555-0186	Work	karan0@adventure-works...	1102 Ravenwood
	270	François	Ajenstat	Database Administrator	785-555-0110	Cell	françois0@adventure-wor...	1144 Paradise Ct.
	22	Sariya	Harnpadoun...	Marketing Specialist	399-555-0176	Work	sariya0@adventure-works...	1185 Dallas Drive
	161	Kirk	Koenigsbauer	Production Technician - ...	669-555-0150	Work	kirk0@adventure-works.c...	1220 Bradford ...
	124	Kim	Ralls	Stocker	309-555-0129	Work	kim0@adventure-works.c...	1226 Shoe St.
	10	Michael	Raheem	Research and Developme...	330-555-2568	Work	michael6@adventure-wor...	1234 Seaside Way

Fig.10 Expected outcome for Row level setting

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IX. PERFORMANCE MEASURES

Performance measures for RBAC system can be as follows.

1. Number of columns, rows, tables with different security settings and WHERE or HAVING conditions – If security settings are more, then algorithm evaluation time is more. Hence the performance will depend on number of conditions evaluation. It also depends on total number of columns, tables from query and total rows returned by query.
2. Execution Time – Performance can also be measured by the execution time of the query.

X. FUTURE SCOPE

We are using Microsoft SQL 2012 as a back end database and Microsoft .Net 2012 for front end development. The future scope of the proposed system can be extended by developing the system in other platforms and with other database system. RBAC is a rich and open ended system, which ranges from very simple at one end to more complex and sophisticated at each other.

XI. CONCLUSION

The effect of the proposed system can be useful for internal access control within an organization as well as outside the organizations who shares the information. This technique can be used by the enterprises to enforce the privacy policies they define and to allow their customers to control their data.

REFERENCES

1. Platform for Privacy Preferences (P3P),World Wide Web Consortium (W3C),Available at www.w3.org/P3P.
2. A P3P PreferenceExchange Language 1.0 (APPEL 1.0),World Wide Web Consortium (W3C), Available at www.w3.org/TR/P3P-preferences.
3. (EPAL), Available at www.zurich.ibm.com/security/enterpriseprivacy/epal
4. D. E. Bell and L. J. LaPadula. Secure computer systems: mathematical foundations and model. Technical report,MITRE Corporation,1974.
5. Elisa Bertino, Sushil Jajodia, and Pierangela Samarati, Database security: Research and practice,In Information Systems,1996.
6. Dorothy Denning, Teresa Lunt, Roger Schell, William Shockley,and Mark Heckman.,The seaview security model, In The IEEE Symposium on Research in Security and Privacy, 1988.
7. Ravi Sandhu and Fang Chen., The multilevel relational data model,In ACM Transaction on Information and System Security, 1998.
8. Ravi Sandhu and Sushil Jajodia, Toward a multilevel secure relational data model,In ACM International Conference on Management of Data (SIGMOD), 1991.
9. Rakesh Agrawal, Jerry Kiernan, Ramakrishman Srikant, and Yirong Xu,Hippocratic databases,In Proceedings of the 28th International Conference on Very Large Databases (VLDB),2002.

BIOGRAPHY

Shilpa S. Shete received the diploma in computer science degree from Shivaji Univercity in 2002,received bacholor's of engineering degree in computer science from Shivaji University in 2005. She is persuing masters of engineering in computer science from Savitribai Phule Univercity. She has 6 years of software industry experience.

Prof.C.S.Kulkarni
B.E.(COMPUTER SCINCE & ENGG.) from A.D.C.E.T,Ashta Shivaji University.
M.TECH(COMPUTER SCINCE & ENGG.) from Bharati Vidyapeeth College of Engineering, Pune.