Journal of Computer Science and Applications.
ISSN 2231-1270 Volume 6, Number 1 (2014), pp. 11-24
© International Research Publication House
http://www.irphouse.com

A Dynamic Access Control Framework for Database Security

V. Nirmalrani and P. Sakthivel

Department of Information Technology, Sathyabama University,
Chennai, Tamil Nadu, India
nirmalv76@gmail. com
Department of ECE, Anna University, Chennai, Tamil Nadu, India
psv@annauniv. edu

Abstract

In this era, database systems have become mandatory for the organizations to implement. Database security is under great risk. Therefore, it is highly important to specify a role based and environment based dynamic access control model for the database system in organizations to ensure information security and be dynamic. It provides the dynamic environmental check and assignment of permissions to a user of the database. Access level is predetermined by the database administrator to control user access. Considering most of unknown users attempting to access the information, we present a new framework for access control model that can handle both existing and unknown users of the database. The framework deals with three major algorithms, Environmental check, Roles and Permissions Check and finally the increment and decrement of permissions dynamically.

Keywords: Authentication; Access Control; Authorization; Security; Databases.

Introduction

Access Control is a mechanism to prevent the unauthorized use of a resource. The following are the requirements to ensure access control for database security.

- This service controls who can have access to a resource (Authorization)
- Under what conditions access can occur (Access Policies)
- And what those accessing the resource are allowed to do (Operations)

Organizations use access control mechanisms to mitigate the risks of unauthorized access to their data, resources, and systems. In recent years, vendors have begun implementing Role-Based Access Control (RBAC) features in their database management system, security management, and network operating system products.

Database systems have become mandatory for the organizations to implement. Database security is under great risk. Therefore, it is highly important to specify a role based and environment based dynamic access control model for the database system in organizations to ensure information security and be dynamic. It provides the dynamic environmental check and assignment of permissions to a user of the database. Access level is predetermined by the database administrator to control user access. Considering most of unknown users attempting to access the information, we present a new framework for access control model that can handle both existing and unknown users of the database. The framework deals with three major algorithms, Environmental check, Roles and Permissions Check and finally the increment and decrement of permissions dynamically.

Research Background

Access Control / Authorizations

Authorization is the process where requests to access a particular resource should be granted or denied. It should be noted that authorization is not equivalent to authentication - as these terms and their definitions are frequently confused.

Access Control is the method or mechanism of authorization to enforce that requests to a system resource or functionality should be granted.

Role Based Access Control (RBAC)

In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization or user base. The process of defining roles is usually based on analyzing the fundamental goals and structure of an organization and is usually linked to the security policy. For instance, in a medical organization, the different roles of users may include those such as doctor, nurse, attendant, nurse, patients, etc. Obviously, these members require different levels of access in order to perform their functions, but also the types of web transactions and their allowed context vary greatly depending on the security policy and any relevant regulations (HIPAA, Gramm-Leach-Bliley, etc.).

An RBAC access control framework should provide web application security administrators with the ability to determine who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances. http://csrc. nist. gov/rbac/ provides some great resources for RBAC implementation. The following aspects exhibit RBAC attributes to an access control model.

- Roles are assigned based on organizational structure with emphasis on the organizational security policy.
- Roles are assigned by the administrator based on relative relationships within the organization or user base. For instance, a manager would have certain authorized transactions over his employees. An administrator would have

certain authorized transactions over his specific realm of duties (backup, account creation, etc.)

- Each role is designated a profile that includes all authorized commands, transactions, and allowable information access.
- Roles are granted permissions based on the principle of least privilege.
- Roles are determined with a separation of duties in mind so that a developer Role should not overlap a QA tester Role.
- Roles are activated statically and dynamically as appropriate to certain relational triggers (help desk queue, security alert, initiation of a new paper, etc.)
- Roles can be only be transferred or delegated using strict sign-offs and procedures.
- Roles are managed centrally by a security administrator or paper leader

Dynamic Access Control is a set of features for Windows Server 2012 to manage authentication and authorization beyond Active Directory Groups.

Existing System

DAC leverages Windows Server 2012's improved file-level auditing and authentication to tag files based on criteria such as content and creator. Specific types of data can be identified; for example, social security numbers, bank account numbers or credit card numbers would be tagged as sensitive. Administrators could also designate that files of a certain type/extension all be tagged, or only documents that contain specific keywords might be tagged. Tagging and categorizing data is already familiar from Windows Server 2008, but Windows Server 2012 takes it to the next level.

The identification and tagging of the data is the first step. You could specify that all the data related to personnel be tagged with the Personnel tag, that financial data be tagged with the Finance tag, and so forth. Once that's accomplished, central policies can restrict access to those files based on different criteria. Specific users can be restricted, or all users within a particular group or department can be restricted. You can, for example, specify that only users who belong to the Finance group – and who have the appropriate NTFS and share permissions – will be able to access the Finance tagged files. Access can also be restricted based on devices instead of users.

Claims based access controls can also work in conjunction with other Microsoft technologies such as Rights Management Services (RMS). Tagged Office documents can be protected by RMS so that after they've been shared with others, you still maintain control over what those others can do with them. DAC protects the documents while they're on the Windows 8 server, and RMS protects them when they've been sent outside the organization.

Finally, audit policies can likewise be applied across all the servers in your organization, which work with the file tags and with user and device claims.

NIST Access Control Models

The following are the models standardized by National Institute of Standards and Technology (NIST) to ensure the access of the resources.

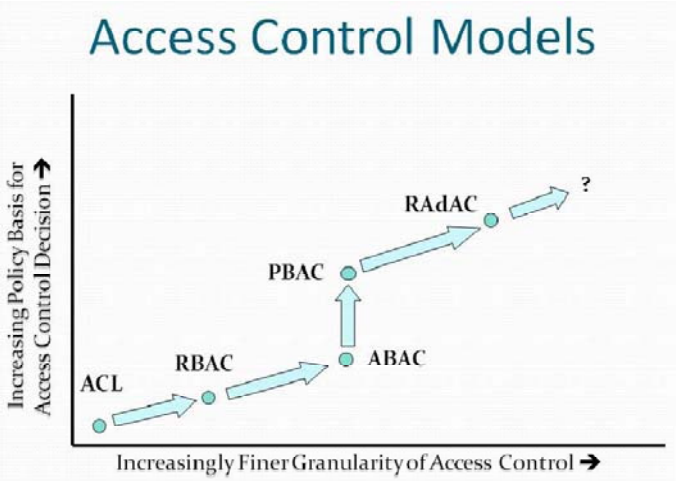

Access Control Models
Increasing Policy Basis for Access Control Decision →
Increasingly Finer Granularity of Access Control →
ACL
RBAC
ABAC
PBAC
RAdAC
?

Fig. 1. NIST – Access Control Models

ACL – Access Control List (Resource-centric, doesn't scale)

An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. When a subject requests an operation on an object in an ACL-based security model, the operating system first checks the ACL for an applicable entry to decide whether the requested operation is authorized. A key issue in the definition of any ACL-based security model is determining how access control lists are edited, namely which users and processes are granted ACL-modification access. ACL models may be applied to collections of objects as well as to individual entities within the system's hierarchy.

RBAC – Roles-Based Access Control (Lacks granularity, doesn't scale beyond broad categories of people)

Role-based access control (RBAC) is an approach for restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC). RBAC is sometimes referred to as Role-Based Security. Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Three primary rules are defined for RBAC:

- Role assignment: A subject can exercise permission only if the subject has selected or been assigned a role.
- Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

- Permission authorization: A subject can exercise permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

ABAC – Attribute-Based Access Control (scale leads to maintenance and consistency issues)

Attribute Based Access Control (ABAC) is an access control model wherein the access control decisions are made based on a set of characteristics, or attributes, associated with the requester, the environment, and/or the resource itself. Each attribute is a discrete, distinct field that a policy decision point can compare against a set of values to determine whether or not to allow or deny access. The attributes do not necessarily need to be related to each other, and in fact, the attributes that go into making a decision can come from disparate, unrelated sources. They can be as diverse as the date an employee was hired, to the papers on which the employee works, to the location where the employee is stationed, or some combination of the above. One should also note that an employee's role in the organization can serve as one attribute that can be (and often is) used in making an access control decision.

A key advantage to the ABAC model is that there is no need for the requester to be known in advance to the system or resource to which access is sought. As long as the attributes that the requestor supplies meet the criteria for gaining entry, access will be granted. Thus, ABAC is particularly useful for situations in which organizations or resource owners want unanticipated users to be able to gain access as long as they have attributes that meet certain criteria.

PBAC – Policy-Based Access Control

Policy-based Access Control (PBAC) is an emerging model that seeks to help enterprises address the need to implement concrete access controls based on abstract policy and governance requirements. In general, PBAC can be said to be a harmonization and standardization of the ABAC model at an enterprise level in support of specific governance objectives. PBAC combines attributes from the resource, the environment, and the requester with information on the particular set of circumstances under which the access request is made, and uses rule sets that specify whether the access is allowed under organizational policy for those attributes under those circumstances.

Although PBAC is an evolution of ABAC, it is a much more complicated model. Since the attributes have to be maintained across the enterprise, it is necessary to design and deploy enterprise-level systems to accommodate PBAC.

RAdAC – Risk-Adaptive Access Control (Complex to implement, requires a lot of computing resources)

The Risk-Adaptive Access Control (RAdAC) model was devised to bring real-time, adaptable, risk-aware access control to the enterprise. RAdAC represents a fundamental shift in the way access control is managed. It extends upon other earlier access control models by introducing environmental conditions and risk levels into the access control decision process, in addition to the concept of "operational need. " RAdAC goes beyond the traditional reliance on static attributes and policies. It combines information about a person (or machine's) trustworthiness, information about the corporate IT infrastructure, and environmental risk factors and uses all of this information to create an overall quantifiable risk metric. RAdAC also uses situational factors as input for the decision-making process. These situational inputs could include information on the current threat level an organization faces based on data gathered from other sources, such as CERTs or security vendors. After all of this information is gathered, it is compared against access control policy. The access control policy could include directives for how access control should be handled under a variety of situations and with a variety of risk levels.

RAdAC system will use previous decisions as one input when determining whether access will be granted to a resource in the future.

Problem Definition and Proposed System

Scope of the proposed system

The scope of the proposed system is to secure databases from unauthorized access using RBAC. In RBAC privileges are assigned based on the roles (Static). The privileges need to be made dynamic in some conditions. So the static permissions are incremented or decremented based on the conditions.

Proposed System

Proposed permissions enable an administrator to more accurately model the impact of potential changes to access control settings without actually changing them.

In the proposed system, the user puts his/her request to enter the database; his/her log information is checked in an existing log file. If the user is found new user, his/her platform/software interface is checked, if it matches with the database software then the roles and permissions are assigned to user. The permissions are dynamically increased or decreased when the user puts the request; also the system checks its role match and existing permissions. The permissions are increased accordingly with all this process the system automatically generates a routine that creates a backup table that is kept hidden from user. If the changes that a user makes in a table are not suitable or a user is deleting or modifying some critical data then the system will not allow him to save the data rather than it will over write the changed table with backup table. If it does so keeps this operation as threat and decreases the permissions.

Anatomies of proposed system

Security Domain

Each user has a security domain—a set of properties that determine such things as:

- The actions (privileges and roles) available to the user
- The table space quotas (available disk space) for the user
- The system resource limits (for example, CPU processing time) for the user

Each property that contributes to a user's security domain is discussed in the following sections.

Privileges

A privilege is a right to run a particular type of SQL statement. Some examples of privileges include the right to:

1. Connect to the database (create a session)
2. Create a table in your schema
3. Select rows from someone else's table
4. Run someone else's stored procedure

Roles

Roles are named groups of related privileges that you grant to users or other roles.

Implementation of Dynamic Access Control

User and Device Claims

User claims are properties about the user such as what department they work in. Likewise the physical device can have claims associated with it. This can be used to prevent sensitive information from being exposed to an untrusted machine even if the user would otherwise be allowed to access the file. Claims support a variety of data types including strings, Booleans, and integers.

Expression-Based Access Control Lists

Expression based ACLs operate on user claims, device claims, and resource properties.

The expression has two part, applicability and permission. The applicability check would usually be against the resource properties, such as “Resource. SecurityLevel = Secret”. If this returns true, then the permission expression is evaluated to see if the user/device pair can access the resource. Continuing the example, we would use “(User. SecurityClearance = TopSecret or User. SecurityClearance = Secret) and (Device. Location = SecureLab)”.

Expression-based Access Control Lists also extend existing group-based policies. Previously there was no concept of an “and” operator for groups. If a user needed to be in two or more groups in order to access a resource then a new group that represented both would need to be created. This “group bloat” is a leading problem among many large companies with dozens or hundreds of sites. Now an expression that translates to “user is in Group A and Group B” can be written.

Users and developers can manage expression based ACLs using many different ways including APIs such as AddConditionalAce, Power Shell, or LDAP.

File Classification Infrastructure

The File Classification Infrastructure is used to assign resource properties to files. FCI supports both built-in and third party classifiers. In Windows Server 2008 R2, the file classifiers were run on a timer, usually late at night. With Windows Server 2012 they are run in near-real time. There is still going to be a small delay between creating a file and classifying it, making local permissions also important.

Another change to FCI is where the classifications are stored. Previously this was placed in a secondary file stream. This meant that it could be edited by anyone with write access to the file. With Server 2012 this has been moved into the file's ACL. The list of possible file classifications is stored in Active Directory.

Central Access and Audit Policies

Central Access Policy combines file classification with Expression-Based Access Control. This allows the IT department to setup high level rules such as financial documents (as classified by the FCI) can only be accessed if the user is in the finance department and in the paper's group. These rules are pushed onto the file servers using group policies.

Central Access Policies are checked after the share ACL is checked. If the CAP rules are also passed, then the files NTFS-based local file ACL is checked.

In order to reduce problems caused by misconfigured security settings, Central Access Policies can be staged. This allows the InfoSec manager to see who will lose access to a file and what rules are causing the problem.

Access Denied Assistance

In a nut shell, Access Denied Assistance helps users figure out why they were denied access to a given resource. It can do things like remind them to insert a physical passkey or tell them what access violation rule they at this time. It can also be configured to send an email to the resource owner so that their access request can be reviewed and potentially granted.

DAC Architecture

In the proposed architecture, every actor is assigned with a role and privileges are assigned based on the roles. When the roles are accessing the database the following constraints are verified

- Environment Check
- Role Verification
- Permission Verification

If the role satisfies all the constraints, the access to the database is given to those roles. Based on the environment the privileges are either incremented or decremented. This can be done at when a user tries to connect to the database. This factor checks the URL from which the user accesses the database. After the user has passed the initial check, he/she can start using the database. If he/she attached the database for long time the access pattern will be evaluated. The access pattern that the system still will look for will be in terms of security threats. All the threats that are highlighted in the table refer to the access control of database.

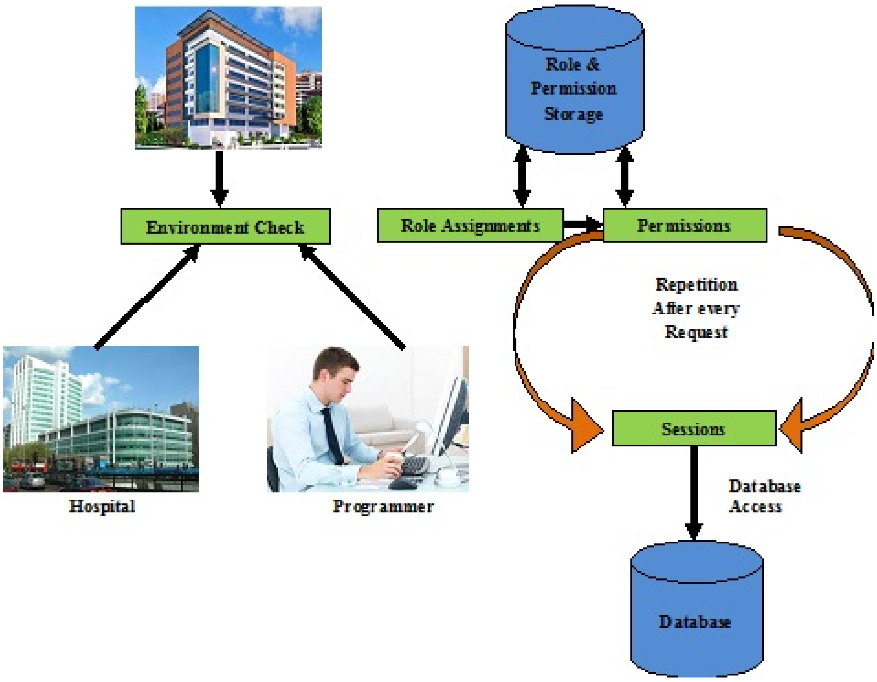


Fig. 2. DAC Architecture

Module Description

The following are the modules used for implementing the Dynamic Access Control for Database Security.

- Administration Module
- Dynamic Access Control
- Role Based Access Control
- Dynamic Permission Assignment

Administration Module

This is the module which is the master and base module for all other Sub-modules. It provides the overall functionality to the software and maintains its integrity. This module includes the following functions. It provides an authorization to carry out some operation on the system. It allocates user name and password for every role. It includes an authorization to carry out some operation on the system. It allocates user name and password for every role. Allocation of Rooms is explained in this module. It ensures the allocation of patients to various departments according to their Requirements. It provides access to every sub module.

Dynamic Access Control

When an unknown user wants to access the database the permissions assigned to him/her are dynamically changed based on his/her pattern. The permissions can dynamically be incremented or decremented after analyzing the access pattern of the user after interval of every minute. Secondly this model is flexible enough to increase or decrease the access permission of user based on the security checks. The environment checking will be done at two places. Once, at the beginning access stage when a user tries to connect database. The environment factors that are going to be checked will be among others the origin of the user.

Role Based Access Control

Roles are created for a variety of job purpose. The permissions to carry out definite operations are assigned to precise roles. A user has access to an object base on the assigned role.

Dynamic Permission Assignment

Suitable roles are turned on according to user's existing environment. Dynamically permissions are assigned to a task. Incompatible bodies in organization should be carefully measured to produce work catalog.

Algorithms Used

In DAC architecture the following algorithms are used

- Role Based Access Control Algorithm
- Dynamic Access Control Algorithm

Role Based Access Control Algorithm

```
cvl1 ← Sort context variables used in cva1 according to their name
cvl2 ← Sort context variables used in cva2 according to their name
i = j = 1; result = false
while i ≤ |cvl1| do
while j ≤ |cvl2| do
if cvl1[i]. name = cvl2[j]. name then
if disjointTest(cvl1[i]. value, cvl2[j]. value, op1, op2) then
if cvl1[i]. SCV = true then
return false
else result = true
end if
else i++; j++
end if
else if cvl1[i]. name < cvl2[j]. name then i++
else j++
end if
end while
end while
return result
```

Dynamic Based Access Control Algorithm

```
IF (U e)
IF (R=1)
```

```
P=p+1
Routine called, Table backup
ELSE Access Denied
IF (Op=L)
Update Database, Update Log file
ELSE Replace table with backup Table
P=P-1
ELSE IF(R=1)
P=P+1; Routine called, Table Backup
ELSE Access denied
IF (Op=L)
Update Database, Update Log file
ELSE Replace Table with Backup Table
P=P-1
ENDIF
```

Implementation Results of DAC

Dynamic Access Control model for Database Security has been implemented using Wamp Server. Coding has been written in PHP and the database connectivity has been done through MySQL.

Hospital Database

The records of the actors are stored in the database. Only the administrator can access the database. The tables are Administrator, Medicine, Patients, Roles, Staffs, Tests and Wards.

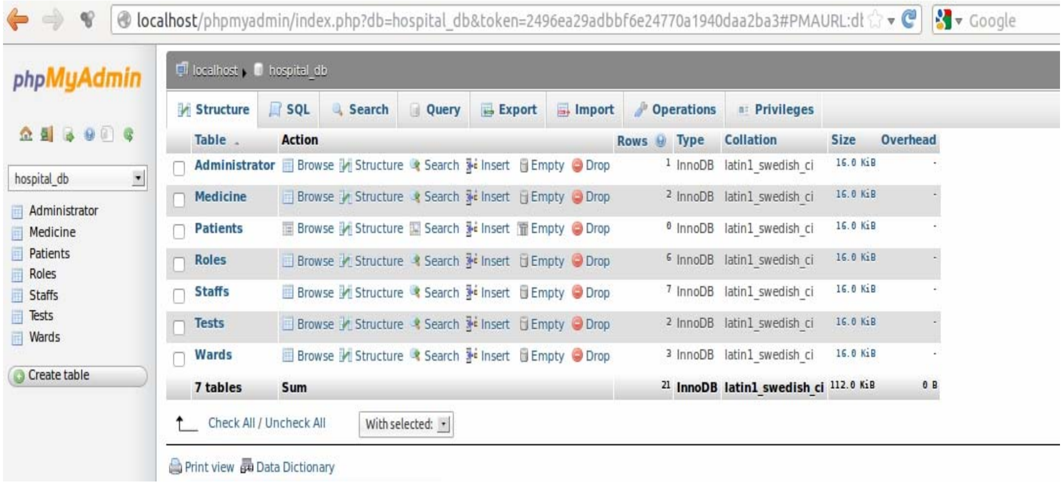
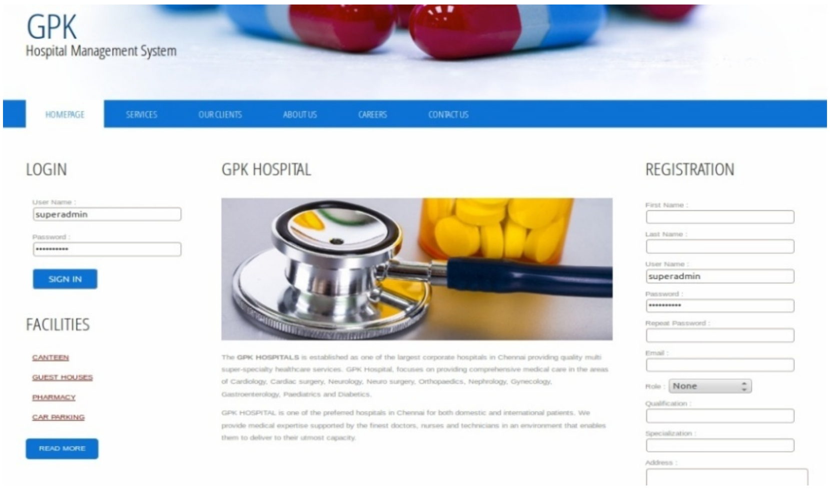


Table	Action	Rows	Type	Collation	Size	Overhead
□ Administrator	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	16.0 KiB	-
□ Medicine	Browse Structure Search Insert Empty Drop	2	InnoDB	latin1_swedish_ci	16.0 KiB	-
□ Patients	Browse Structure Search Insert Empty Drop	0	InnoDB	latin1_swedish_ci	16.0 KiB	-
□ Roles	Browse Structure Search Insert Empty Drop	6	InnoDB	latin1_swedish_ci	16.0 KiB	-
□ Staffs	Browse Structure Search Insert Empty Drop	7	InnoDB	latin1_swedish_ci	16.0 KiB	-
□ Tests	Browse Structure Search Insert Empty Drop	2	InnoDB	latin1_swedish_ci	16.0 KiB	-
□ Wards	Browse Structure Search Insert Empty Drop	3	InnoDB	latin1_swedish_ci	16.0 KiB	-
7 tables	Sum	21	InnoDB	latin1_swedish_ci	112.0 KiB	0 B

Fig. 3. Database

Homepage

In the homepage, the user can login to his / her account and is allowed access to the records. The new users can register into the system by entering the details for registration. The services provided by the hospital are Sponsorship from the clients, detailed information about the hospital, the careers that is offered by the hospital and the details for contacting in order to post queries and enquire about the facilities provided by the hospital. All these services can be accessed in the homepage.



User Name : superadmin
Password : ••••••••••••

The **GPK HOSPITALS** is established as one of the largest corporate hospitals in Chennai providing quality multi super-specialty healthcare services. GPK Hospital, focuses on providing comprehensive medical care in the areas of Cardiology, Cardiac surgery, Neurology, Neuro surgery, Orthopaedics, Nephrology, Gynecology, Gastroenterology, Paediatrics and Diabetics.

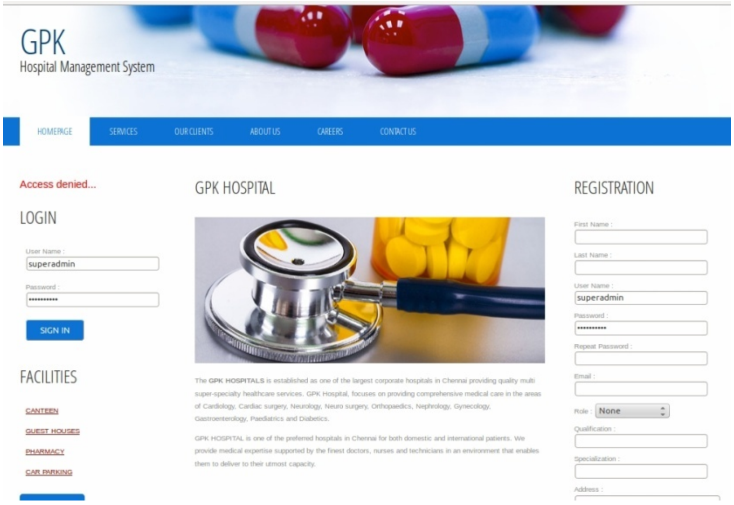
GPK HOSPITAL is one of the preferred hospitals in Chennai for both domestic and international patients. We provide medical expertise supported by the finest doctors, nurses and technicians in an environment that enables them to deliver to their utmost capacity.

First Name :
Last Name :
User Name : superadmin
Password : ••••••••••••
Repeat Password :
Email :
Role : None
Qualification :
Specialization :
Address :

Fig. 4. Home Page

Access Denied

At the time of login, if the username / password provided by the user is incorrect or if the user does not belong to the hospital i. e. the user detail is not stored in the database, then his access is denied. An alert message is displayed to warn the user that his / her access is denied.



Access denied...

User Name : superadmin
Password : ••••••••••

The **GPK HOSPITALS** is established as one of the largest corporate hospitals in Chennai providing quality multi super-specialty healthcare services. GPK Hospital, focuses on providing comprehensive medical care in the areas of Cardiology, Cardiac surgery, Neurology, Neuro surgery, Orthopaedics, Nephrology, Gynecology, Gastroenterology, Paediatrics and Diabetics.

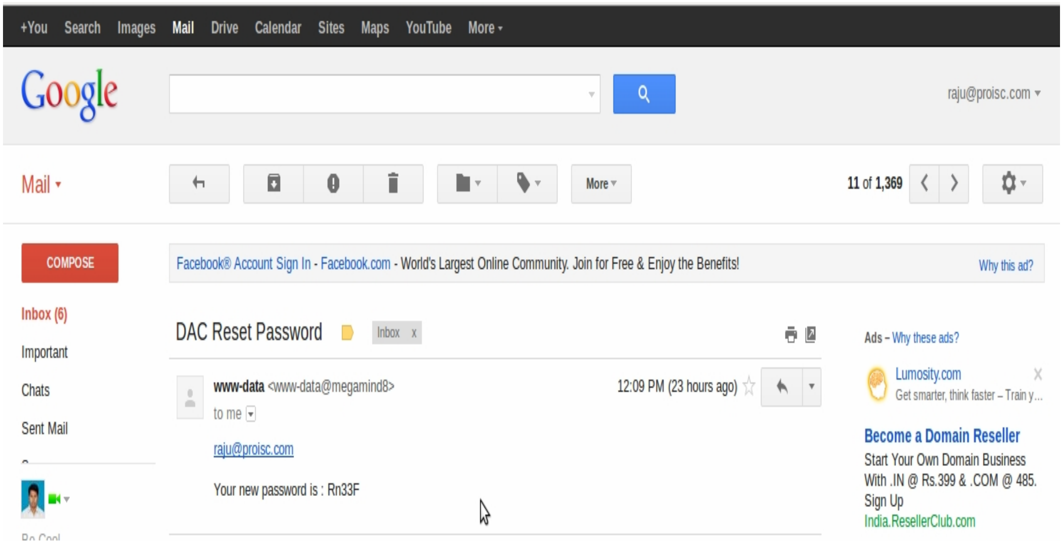
GPK HOSPITAL is one of the preferred hospitals in Chennai for both domestic and international patients. We provide medical expertise supported by the finest doctors, nurses and technicians in an environment that enables them to deliver to their utmost capacity.

First Name :
Last Name :
User Name : superadmin
Password : ••••••••••
Repeat Password :
Email :
Role : None
Qualification :
Specialization :
Address :

Fig. 5. Access Denied

Password Recovery

In order to ensure maximum security, the password of the user is changed every time the user login to the system. The new password stored in the database is sent to the corresponding users for verification and can be recovered. Mail configuration is done so as to ensure that every user receives a mail whenever the password is changed.


+You Search Images Mail Drive Calendar Sites Maps YouTube More
Google
raju@proisc.com
Mail
More
11 of 1,369
COMPOSE
Inbox (6)
Important
Chats
Sent Mail
Facebook® Account Sign In - Facebook.com - World's Largest Online Community. Join for Free & Enjoy the Benefits!
Why this ad?
Inbox x
Ads – Why these ads?
Lumosity.com
Get smarter, think faster – Train y...
Become a Domain Reseller
Start Your Own Domain Business With .IN @ Rs.399 & .COM @ 485. Sign Up
India.ResellerClub.com

DAC Reset Password

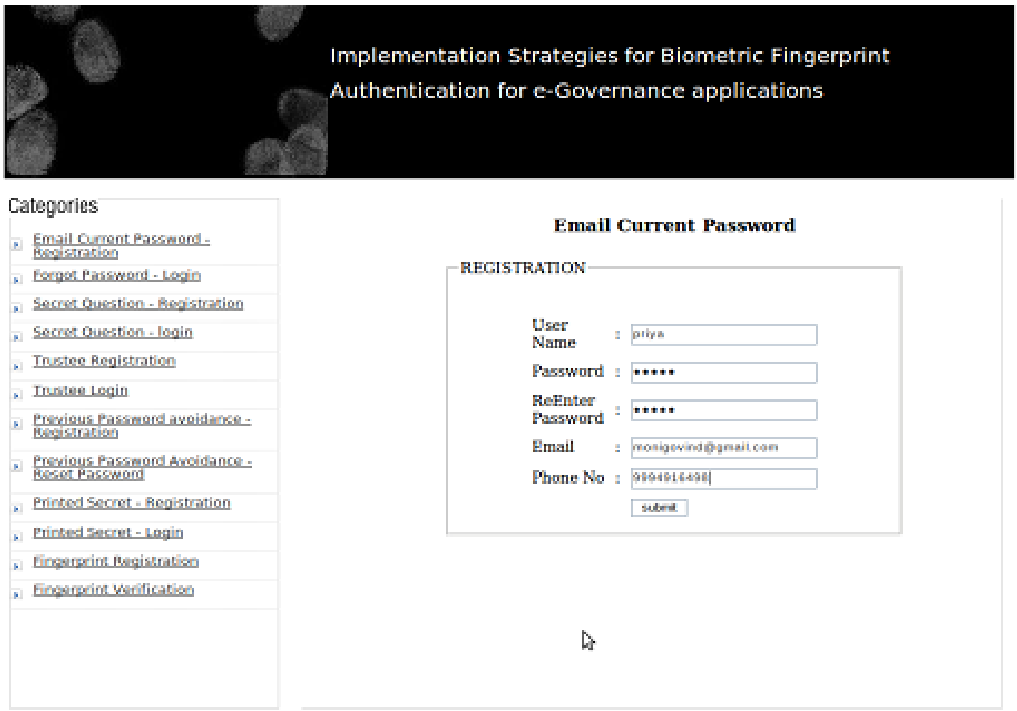
www-data <www-data@megamind8> 12:09 PM (23 hours ago)

to me

raju@proisc.com

Your new password is : Rn33F

Fig. 6. Password Recovery through Mail


Implementation Strategies for Biometric Fingerprint Authentication for e-Governance applications
Categories
Email Current Password - Registration
Forgot Password - Login
Secret Question - Registration
Secret Question - login
Trustee Registration
Trustee Login
Previous Password avoidance - Registration
Previous Password Avoidance - Reset Password
Printed Secret - Registration
Printed Secret - Login
Fingerprint Registration
Fingerprint Verification
submit

Email Current Password

REGISTRATION

User Name	:	priya
Password	:	•••••
ReEnter Password	:	•••••
Email	:	monigovind@gmail.com
Phone No	:	9894916498

Figure 7. Biometric Fingerprint Authentication Interface

Conclusion

This paper presented the dynamic access control that provides the dynamic environment check and assignment of permissions to users of the database. It is the extension of the existing RBAC model and dynamically adjusts the role assignment and permission assignment based on the environment and the access pattern of the user and automatically decides whether the user should continue its access to database or not. On the other hand it also decided that the user may get its permissions increased based on its safe and sound access pattern.

In future, the system will automatically generate a routine that can create a backup table that is kept hidden from the user. More security can be ensured by giving the finger print, eye retina as password. The essential details of the patient can be sent through online itself. More security can be ensured by sending random password to their respective mobiles. Other hospital information and their patient's information can be connected to the database. Real time objects can be used instead of sample objects in the database.

References

[1] Ahmad S, Ahmad R, "Environmental-based Dynamic Access Control Model for Database Systems" 2011 3rd International Conference on Machine Learning and Computing (ICMLC 2011), 978-1-4244-925, pp. 3 – 4 / 11.

[2] Chaoyi. P, H. David, M. Anthony, "Managing RBAC States with Transitive Relations" ASIACCS 07, March 20 – 22, 2007 ACM.

[3] Hua. H, L. Ande, "Actor and Trust Based Dynamic Access Control Model in Universal Computing Environment", IEEE Second International Symposium on Intelligent Information Technology Application (IITA '08), 2008.

[4] Lingli. Z, L. Shuai, L. Junsheng, X. Haicheng, "A Dynamic Access Control Model Based on Trust", 2nd IEEE Conference on Environmental Science and Information Application Technology, ESIAT 2010, pp. 548 – 551.

[5] Sajjad Ahmad and Rohiza Ahamad, "Design of Algorithm for Environment Based Dynamic Access Control Model for Database Systems", International Journal of Computer Applications, Vol. 21, No. 10, May 2011.

[6] Sandhu. R. S, E. J. Coyne, H. L. Feinstein, C. E. Youman, "Role-Based Access Control Models", IEEE Computer, vol. 29, issue 2, pp. 38 – 47, 1996.

[7] http:// blog. techwheels. net / send – email – from – localhost – wamp –server using sendmail.

[8] http:// en. wikipedia. org / wiki / Role-based-access-control.