New York Science Journal

Websites:
http://www.sciencepub.net/newyork
http://www.sciencepub.net

Emails:
newyorksci@gmail.com
editor@sciencepub.net

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

Hierarchical Location Based Access Control & Delegation of Authority Model HLBAC-DOA

Waqar Ali, Fakhri Alam Khan

Department of Computer Science, Institute of Management Sciences Hayatabad, Peshawar 25000, Pakistan
Waqar.ms08@gmail.com, fakhri.alam@imsciences.edu.pk

Abstract: Access control to organizational resources is the central gravity of computer security. It deals with the fact that how persons, processes and machines access different resources in the system with different authority of access rights. A lot of work is on the way in this area and different models are in research with innovative ideas and concepts. As evolution going on from single user to group of users in computing systems, there is a necessity to shield the user processes and data from one another. This paper addresses the issue of shielding user data and processes using user location in the hierarchical form and protects the user resources from each other in indoor environment. In our model, we also show how in emergency situation the user accesses others resources in the form of delegation of access rights and usage control on the usage of resources by the user. In this paper we propose a new model of access control that gives access to the user on the basis of user location with the feature of usage control and continues-ongoing condition during access using hierarchical format.
[Waqar Ali, Fakhri Alam Khan. **Hierarchical Location Based Access Control & Delegation of Authority Model HLBAC-DOA**. *N Y Sci J* 2022;15(1):66-74] ISSN 1554-0200 (print); ISSN 2375-723X (online) http://www.sciencepub.net/newyork. 7. doi:10.7537/marsnys150122.07.

Keywords: Security, Access Control, Location, Zones, Delegation, Emergency, LRBAC, Usage Control

1. Introduction

Access control is the mechanism used by different organizations to limit the un-authorized users to access their data or systems and only allow the authentic users and authorized parties. Access control models are widely set apart into three main broad categories i.e. Mandatory Access Control Model (MAC) [1], Discretionary Access Control Model (DAC) [2] and Role Based Access Control Model (RBAC) [Sandhu et al., 1996].

In MAC the policies for the objects are defined by the central authority not by the owner of that file or the object. The permissions for an object are defined by the access control matrix. The decision for the protection of the file is not in the hand of the owner of that file but according to pre-defined rules of access matrix. Bell-LaPadula Confidentiality Model [Cankaya, E.C. 2011] and Biba Integrity Models [5] are the two use cases of MAC. The Bell-LaPadula Confidentiality Model gives confidentiality to the data while Biba Integrity Model is opposite to the Bell-LaPadula Model which gives Integrity to the data.

In contrast to MAC, in DAC the policies for the objects are defined by the owner/subject of that object. Access Control Lists (ACLs) [Cankaya, H.C. 2011], Lampson [Lampson, B.W. 1974] and Take-grant model [Snyder, L. 1980.] are the models uses the same DAC concept.

Alternative to both DAC and MAC is Role Based Access Control Model [Sandhu et al., 1996]. In RBAC the roles are created and permissions/privileges are assigned to the roles instead of users or central authority. There are different variants of RBAC which is also implemented by various Operating Systems like Windows 2000 and in latter OS in the form of "Groups" like Administrator Group, Power Users Group etc.

All the access control models have its own mechanism of access control but with some deficiencies in them like:

Lack of Delegation of Authority
No scenario for Emergency Situation
Usage Control unavailability

Delegation main idea is that when a user or an active entity transfer his or her authority to another entity or user for the purpose of performing some jobs on behalf of the delegated user in case of Emergency Situation. Delegation is a very important mechanism that gives flexibility to access control models which may be user to user, user to machine,

machine to machine and may be even machine to human. Capability-based Access Control Delegation Model on the Federated IoT Network [Anggorojati et al., 2012] presents the delegation method on the Federated IoT Network. xDAuth: A Scalable and Lightweight Framework for Cross Domain Access Control and Delegation [Alam et al., 2011] Model is the model for delegation but in cross domain environment not in the same domain.

In usage Control as given by the UCON $_{ABC}$ Usage Control Model [Park, J. and Sandhu, R. 2004.] the usage of the resources are controlled. The model integrated Authorizations (A), Obligations (B), and Conditions (C). Authorization decision is used on user's access to target resources. Obligations have to be fulfilled by obligation subjects for letting access. Conditions are subject and object-independent environmental condition or system requirements that have to be fulfilled for access to the resources.

To address the issues discussed, we propose a new model in this paper for an access control to organizational resources. Major contributions of this paper include:

i. Proposed HLBAC-DOA Model
ii. Delegation of Authority
iii. Usage Control
iv. Implementation of the HLBAC-DOA model

Rest of the paper is organized as follows. Section 2 deals with the existing techniques of different access models, Section 3 with the Existing Approach and its Limitations, Section 4 with the Proposed Model i.e. HLBAC-DOA and Section 5 with the implementation of the HLBAC-DOA.

2. Existing Techniques

Access Control Lists (ACLs) [Cankaya, H.C. 2011] is one of the oldest access control technique mostly used by the Operating Systems like Microsoft Windows NT, Mac and some hardware companies like CISCO. In ACLs rights are assigned to each subject for their respective object but the limitation of ACL is that each and every user of an organization is treated as a separate subject so a lot of human manual effort is required resulting in inefficient use of resources. In Contrast to ACLs, we have the RBAC Model [Sandhu et al., 1996]. RBAC Model minimizes the human effort in which the administrator of an organization creates "Roles" "Permissions" and "Users". Users are assigned to Roles. When a user access a resource, the permissions of the relevant role is automatically applied on the user as shown in the Fig.1

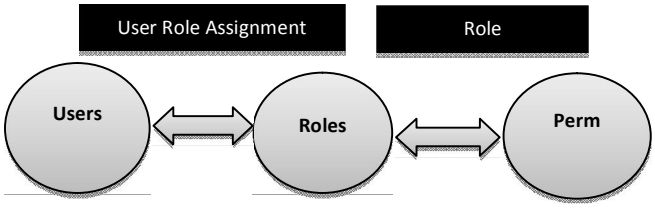

Fig. 1 Role Based Access Control Model

There are different variants of RBAC which is also implemented by various Operating Systems like Windows 2000 and in latter OS in the form of "Groups" like Administrator Group, Power Users Group etc.

The main deficiency of RBAC is that it does not give granular control of access to the users so there is a need to differentiate group members one by one and allow/deny access to each user independently. To fill this gap we have Attribute based Access Control (ABAC) [Yuan, E. and Tong, J. 2005]. In ABAC model attributes of the requester, environmental condition and the properties of the resources are checked during access. Similarly Capability-based delegation model in RBAC [Hasebe et al., 2010] is the concept which covers the limitation of basic RBAC Model which is the delegation of access rights. In CRBAC if a user wants to access the resources to which he/she is not entitled then a "Capability" is created by the allowed user which is then delegated to the user who wants to use the resources for which he/she is not entitled. The same emergency situation is also dealt by the Rumpole: a Flexible Break-Glass Access Control Model [Marinovic et al., 2011]. GEO-RBAC A Spatially Aware RBAC [Bertino et al., 2005] gives the concept of spatial roles which represent geographically bounded organization function. According to Geo-RBAC When a user is in its real Position then Role will be enabled only and when the user logical position is conformed using a function called "MAPING FUNCTION" then the Role will be activated for him/her only. Enforcing Spatial aware RBAC Systems [Kirkpatrick, M.S. and Bertino, E. 2010.] is one of the extensions of RBAC Model. It focuses mainly on authentication of user's claim about location and verification of user's position continuously. It's based on GEO-RBAC [Bertino et al., 2005] and combines the element of UCON $_{ABC}$ Model [Park, J. and Sandhu, R. 2004.] with GEO-RBAC.

3. Problems in the Existing Approach

A location-aware role-based access control model [Ray et al., 2006] is the model that dealt with the location of a user i.e. from where the users access the relevant resources keeping in view the concept of RBAC Model [Sandhu et al., 1996]. This model extended and integrates the notion of location in RBAC Model. In this paper different components in the RBAC model are correlated with location and showed how this location evidence can be used to decide whether a subject has right of entry for a given object or not. This model is suitable for applications comprising of static and dynamic objects, where position of the subject and object must be taking before access. The different components of the LRBAC model are Users, Roles, Locations, Objects, Sessions and Permissions as shown in the Fig 2. When the user is checked and verified. After that concerned role is assigned to the user to access the resources. But there are some deficiencies in the LRBAC Model wants to access the resources then 1st his/her location.

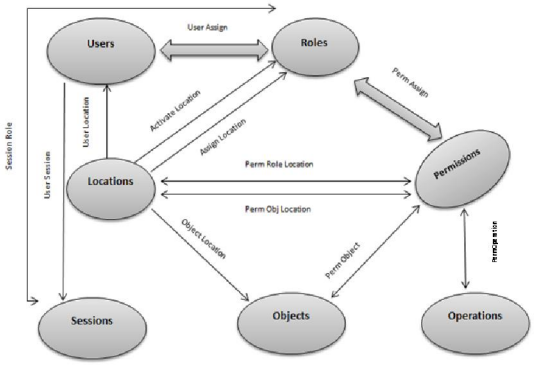

Fig 2. Location Role Based Access Control Model

The 1st main deficiency of LRBAC is the emergency situation i.e. if a user is abroad from the location in which he/she is not registered then how he/she will be allowed to access the resources. In LBAC no solution for this scenario exists.

Similarly in LBAC there are no constraints on the usage control of resources by users but only location is taking into account.

Another limitation of LRBAC Model is that if a user wants to delegate his/her rights to another user which may be from different location then no dealing exists for such a scenario in the Model.

4. Proposed Model (HLBAC-DOA)

In our approach of access control we segregate the location of an organisation in hierarchical form and called it "*Hierarchical Location Based Access Control and Delegation of Authority Mode (HLBAC-DOA)*". In HLBAC-DOA we address the issues of LRBAC model and also add extensions such as delegation of Authority for emergency situation and usage control.

In our approach of Access Control we assume the location of the user for accessing their allowed resources. The user location is logically placed in hierarchical form as shown in the Fig.3.

In the Fig.3 we have a Hospital System in which the user's location is 1st identified, then after that the user is allowed to access the desired zone according to the pre-defined rules of access matrix. On the top we have an admin zone and each zone is assigned to a separate role as shown in the table 1. Each parent node will access only their child nodes (Read, Write and Execute) and their same level nodes (Only Read). The lower level zones will never read or write up except in the "Emergency Situation".

Roles	Zones
Role 1	Zone 1
Role 2	Zone 2
Role 3	Zone 3
Role 4	X-Ray
Role 5	ECG
Role 6	CT-Scan

Roles	Permissions
Role 1	R, W, E (All)
Role 2	R (R3) R, W, E (R2,R4, R5,R6)
Role 3	R (R2) R,W,E (R3)
Role 4 (X-Ray)	R (R5, R6) R,W,E (R4)
Role 5 (ECG)	R (R4, R6) R,W,E (R5)
Role 6 (CT-Scan)	R (R4, R5) R,W,E (R6)

Table. 1 To Zones to Role & Role Permission Assignments

According to Fig.3 a hospital is divided logically into zones E.g. In zone#1 we have the "Admin" of the hospital, in zone#2 we have the "Radiology Department" similarly "Surgical Department" in Zone 3 and so on for other departments.

4.1 Access Matrix for Zone#2

According to the rules given, the access matrix will be like as shown in the table 2. Each row of the access matrix states subjects and each column of the access matrix states objects of the model. According to the below access matrix for example if we take radiology admin or user belongs to the radiology role in Zone#2 it has full access of resources of itself, technicians and nurses and has read only access on surgical role.

Similarly nurses have read only permissions only for their concern department role and no permissions for others.

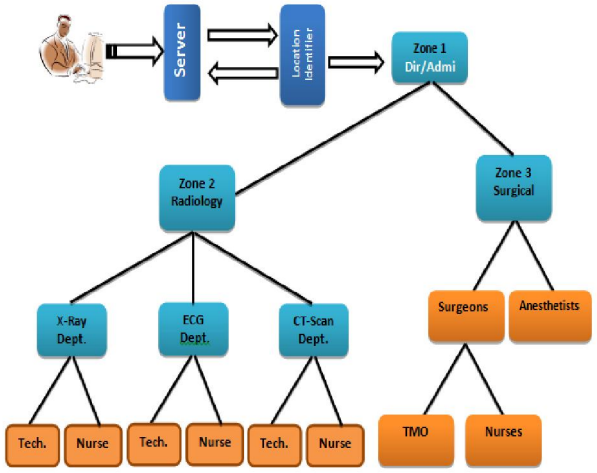

Fig. 3 Hospital System in Hierarchical Form

Subjects	Resources/Objects				
	Zone: 2 Radiology	Zone: 3 Surgical	Zone: 4 X-Ray	Zone: 5 ECG	Zone: 6 CT-Scan
Radiology Admin	Read Write Execute	Read	Read Write Execute	Read Write Execute	Read Write Execute
Surgical Admin	Read	Read Write Execute	-	-	-
X-Ray Tech	Read	-	Read Write Execute	Read	Read
ECG Tech	Read	-	Read	Read Write Execute	Read
CT-Scan Tech	Read	-	Read	Read	Read Write Execute
X-Ray Nurse	-	-	Read	-	-
ECG Nurse	-	-	-	Read	-
CT-Scan Nurse	-	-	-	-	Read

Table. 2 Access Matrix for Zone 2

4.2 Delegation of Access Rights in Emergency Situation

For emergency situation the delegation process will be applied but on the basis of social relationship.

For example in normal situation the "X-ray Tech" i.e. Zone 4 is not allowed to access the "ECG Tech" department or "Zone#5" but in emergency the "X-ray Tech" are allowed to access the resources of "ECG" department i.e. Zone 5.

The following steps are taken for "X-ray Tech" to access the "ECG" as shown in the control sequence diagram of Fig.4.

1. "X-Ray" department sends request to access the resources of "ECG Tech" i.e. Zone# 5.
2. Zone# 5 denied the access as lower level zones or same level zones are not allowed to access the upper level zones or same level zones.
3. Zone# 5 will ask for the guarantor that on what basis i allow you or who will be your guarantor.
4. "X-Ray" department then send request to zone#2 i.e. admin for guarantee him/her.
5. Zone#2 will authenticate the X-Ray and delegates access rights to him/her.
6. Access is then given to "X-Ray Tech" to access the zone 5 resources foe specific period of time.

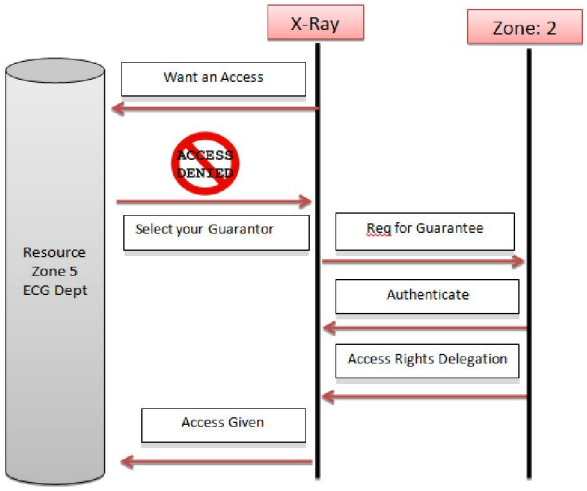

Fig 4. Control Sequence Diagram in Emergency Situation

4.3 Usage Continuity

Suppose Group 2 user used laptop to access database and during the usage he/she moves to other location in which he/she is not registered and also not allowed to access the database.

For such a Scenario in our model there is continuous on-going condition which is applied continuously on the user location and signal time difference is checked between the user and base station.

Suppose user to base station: 1-----10 msec

1-----20 msec

If greater than 10 msec or 20 msec then access will be revoked.

4.4 Environmental Condition

In our model we have environmental condition that should be satisfied during the usage of resources. Before the requested right is exercised condition should be evaluated as shown in the Control Sequence Diagram of Fig.5.

i. First the User send request to the Admin

ii. Before the request is exercised Pre-Condition is checked that either the user is allowed for authorization or not. If Pre-condition fails then the user request is rejected otherwise access is given.

Pre-Condition

Att(s) = {member/User}

Allowed (s,o,r) = PreCon (get PreCond(s,o,r))

get PreCon(s,o,r)={(User Loc∈Pre-defined Area)}

E.g Sub/Surgeon ∈ Zone3

iii. During Access Ongoing condition checks usage of object by the subjects continuously. If any current right violates the Pre-defined restrictions, the allowed rights are revoked and exercise is stopped.

Ongoing Condition

Att(s) = {member/User}

Allowed(s,o,r)=OngoingCon(getOngoingCon(s,o,r))

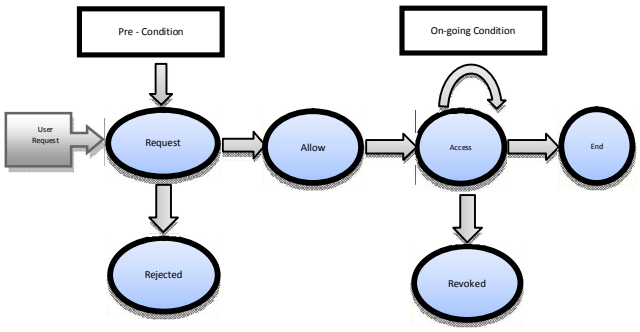

Fig. 5 Usage Continuity Control Sequence Diagram

5. HLBAC-DOA Implementation

The very first look of the front end of HLBAC-DOA model is shown in the snapshot of Fig.6.

The internet explorer is used as front end communication medium for the clients to the database. First when the user request for a resource then her location is identified, if the user satisfied the required location from which she applied for resource execution then she will be allowed for the recourses and assigned to the specific Roles otherwise will be rejected.

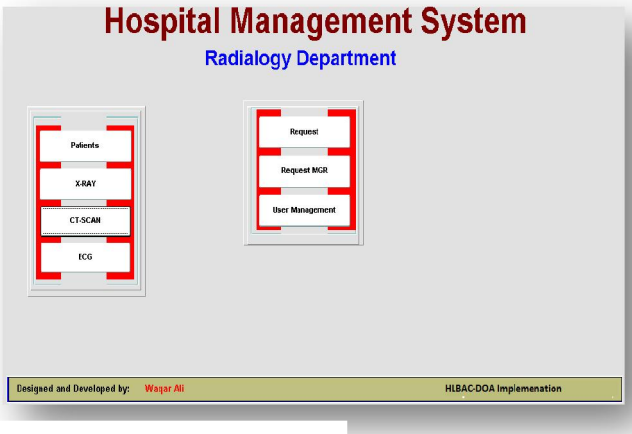

Fig. 6 HLBAC-DOA Front End

5.1 Roles Creation and Permission Assignments for Zone 2

To Create the role
create role X_RAY_NURSE;
To Grant/Revoke object privileges

{ Current (T) ∈ Day H/Night H if user ∈ Day/Night
Current (Loc) ∈ Pre-Assigned Loc if user ∈ Pre-Assigned Location } grant select on PATIENTS to X_RAY_NURSE;
grant select on X_RAY to X_RAY_NURSE;

To Create the role
create role X_RAY_TECH;
To Grant/Revoke object privileges
grant select on CT_SCAN to X_RAY_TECH;
grant select on ECG to X_RAY_TECH;
grant select, insert, update, delete, alter on X_RAY to X_RAY_TECH;

TO Create the role
create role ECG_NURSE;
To Grant/Revoke object privileges
grant select on ECG to ECG_NURSE;
grant select on PATIENTS to ECG_NURSE;

To Create the role
create role ECG_TECH;
To Grant/Revoke object privileges
grant select, insert, update, delete, alter on CT_SCAN to ECG_TECH;
grant select, insert, update, delete, alter on ECG to ECG_TECH;
grant select on X_RAY to ECG_TECH;

To Create the role
create role CT_NURSE;
To Grant/Revoke object privileges
grant select on CT_SCAN to CT_NURSE;
grant select on PATIENTS to CT_NURSE;

To Create the role
create role CT_TECH;
To Grant/Revoke object privileges

grant select, insert, update, delete on CT_SCAN to CT_TECH;
grant select on ECG to CT_TECH;
grant select on PATIENTS to CT_TECH;
grant select on X_RAY to CT_TECH;

To Create the role
create role RADIALOGY;
To Grant/Revoke object privileges
grant select, insert, update, delete, alter on CT_SCAN to RADIALOGY;
grant select, insert, update, delete, alter on ECG to RADIALOGY;
grant select, insert, update, delete, alter on X_RAY to RADIALOGY;

When the normal user want an access of the other level zones then he/she will send request to the admin by clicking on the "Request" button and then in "Request Manager" the admin will allow or deny the required request from others.

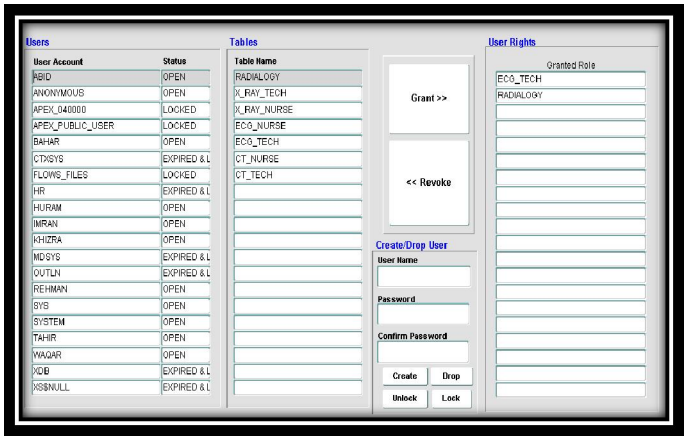

Fig. 7 HLBAC-DOA User Management

6. Conclusions

Access Control on the basis of user location is one of the unique concept in nowadays. With the advancement in technology and wireless growing industries the location of a user is an important issue i.e. from where the user wants to access the resources. This paper deals with the same approach which overcomes the issues of LRBAC Model and adds extensions in the existing model like Delegation of Authority, Usage Control, Usage Continuity and Environmental Condition. In the approach we assume the location of a user for accessing their allowed resources which is logically placed in hierarchical form and is assigned to the specific zone according to the pre-defined rules of access matrix which is also implemented in this paper using Oracle 11*g*.

In future work, one of the most interesting and worthwhile direction is to verify the model HLBAC-DOA using a formal method and also to implement the model in commercial applications.

Corresponding Author:
Mr. Waqar Ali
MS-CS (Information Security)
IMSciences Hayatabad, Peshawar 25000, Pakistan
Waqar.ms08@gmail.com

References:

[1]. [cited 2013 26 December]; Available from: http://en.wikipedia.org/wiki/Mandatory_access_control.
[2]. [cited 2014 2 January]; Available from: http://en.wikipedia.org/wiki/Discretionary_access_control.
[3]. Sandhu, R.S., COYNE, E.J., FEINSTEIN, H.L. and YOUMAN, C.E. 1996. Role-based access control models. *Computer 29*, 38-47.
[4]. CANKAYA, E.C. 2011. Bell-LaPadula Confidentiality Model. In *Encyclopedia of Cryptography and Security* Springer, 71-74.
[5]. [cited 2013 18 December]; Available from: http://en.wikipedia.org/wiki/Biba_Integrity_Model.

[6]. CANKAYA, H.C. 2011. Access Control Lists Springer.
[7]. LAMPSON, B.W. 1974. Protection. *ACM SIGOPS Operating Systems Review 8*, 18-24.
[8]. SNYDER, L. 1980. Theft and conspiracy in the Take-Grant protection model.
[9]. ANGGOROJATI, B., MAHALLE, P.N., PRASAD, N.R. and PRASAD, R. 2012. Capability-based access control delegation model on the federated IoT network. In *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on* IEEE, 604-608.
[10]. ALAM, M., ZHANG, X., KHAN, K. and ALI, G. 2011. xDAuth: a scalable and lightweight framework for cross domain access control and delegation. In *Proceedings of the 16th ACM symposium on Access control models and technologies* ACM, 31-40.
[11]. PARK, J. and SANDHU, R. 2004. The UCON $_{ABC}$ usage control model. *ACM Transactions on Information and System Security (TISSEC) 7*, 128-174.
[12]. YUAN, E. and TONG, J. 2005. Attributed based access control (ABAC) for web services. In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on* IEEE.
[13]. HASEBE, K., MABUCHI, M. and MATSUSHITA, A. 2010. Capability-based delegation model in RBAC. In *Proceedings of the 15th ACM symposium on Access control models and technologies* ACM, 109-118.
[14]. MARINOVIC, S., CRAVEN, R., MA, J. and DULAY, N. 2011. Rumpole: a flexible break-glass access control model. In *Proceedings of the 16th ACM symposium on Access control models and technologies* ACM, 73-82.
[15]. BERTINO, E., CATANIA, B., DAMIANI, M.L. and PERLASCA, P. 2005. GEO-RBAC: a spatially aware RBAC. In *Proceedings of the tenth ACM symposium on Access control models and technologies* ACM, 29-37.
[16]. KIRKPATRICK, M.S. and BERTINO, E. 2010. Enforcing spatial constraints for mobile rbac systems. In *Proceedings of the 15th ACM symposium on Access control models and technologies* ACM, 99-108.
[17]. RAY, I., KUMAR, M. and YU, L. 2006. LRBAC: A location-aware role-based access control model. In *Information Systems Security* Springer, 147-161.

11/22/2021