# Bi-Layer Access Control Model (BLAC) to handle insider threats in E-health Systems

**Done by:** Shruthi Prakash(sxp3768@rit.edu)  
**Guided by:** Prof Dr. Rajendra Raj(rkrics@rit.edu)  
**Rochester Institute of Technology, Computer Science**

## Overview

- Health care systems need the most secure information sharing methodology  
- An access control model helps to protect the confidentiality, integrity and privacy of e-health systems  
- The biggest challenge is the insider attacks which has been happening over the years.  
- Solution is to create a Bi-Layer access control model to protect the e-health systems against insider threats.

## RBAC and ABAC

- RBAC is a good approach, however the main focus on data access is based on the role. A subject of a particular role will be able to access all the data under that role which can lead to insider threat.  
- ABAC handles the limitations of RBAC, however as and when the data increases the policy becomes more complex and difficult to manage. It gets too expensive and leads to poor performance.

## Methodologies

- The BLAC model incorporates the advantages of RBAC and ABAC and handles the limitations of these two, giving a 2-layer protection to the e-health systems from the insider attacks.  
- Pseudo roles will be created for the subject (users) and the objects will have policies defined which includes the pseudo roles as well.

## Goals

- The main goal of the project is to create a bi-layer access control model which overcomes the limitations of RBAC and ABAC.  
- The model should give a better performance compared to the previously defined models such as ABAC and RBAC.  
- The model should be able to handle all kinds of insider threats which is one of the major goals.

## Proposed Solution

### BLAC Model

![BLAC Model Diagram](Image)

### Pseudoroles

![Pseudoroles Diagram](Image)

## Results

### BLAC model performance against normal access

<table>
<thead>
<tr>
<th>Number of Rows</th>
<th>Time taken by BLAC model in ms</th>
<th>Time taken by normal access in ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>50</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>100</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>500</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>1500</td>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>

## Conclusion

- The model describes a bi-layer access control mechanism where pseudoroles are created dynamically.  
- When the subject requests an access, the pseudoroles are fetched for that particular subject and passed to decision maker, which in turn verifies the roles in policies and then goes to the next layer of verification where subject id, object id, action specifiers are checked.  
- The model proves to be very effective when it comes to handling insider attacks as any access request has to clear the two layer verification.  
- The model was tested for performance against normal access and proved to be really effective.  
- The model was also run against ABAC changing the number of rows and it shows how complex ABAC can get. BLAC model again proves to be very effective.  
- The overall performance of the model is good and handles the limitations of both RBAC and ABAC.

## Acknowledgement

Thanks to Prof. Dr. Rajendra Raj for guiding me throughout and Prof. Leon Reznik for valuable advice.

## References

- Alshehri, Suhair; Mishra, Sumita; and Raj, Rajendra, "Insider threat mitigation and access control in healthcare systems" (2013). Accessed from [RIT ScholarWorks](http://scholarworks.rit.edu/article/1401/).  
- Raj, Rajendra and Suhair; Mishra, "Secure Access Control with Pseudorole for Health Information Sharing System" (2013). Accessed from [RIT ScholarWorks](http://scholarworks.rit.edu/article/1401/).