An Elaborative Approach to Enhance Access Control Model: Demostrated by 7-Tier Architecture

Ankur Kumar Shrivastava, Abhinav Kumar, Richa Bhatnagar, Nidhi Chaudhary, Mariya Khurshid Ansari, Amod Tiwari

Abstract- Access control is a security process, which work as a facilitator between every initiated resource and access request to determine whether the system allows or deny the request. Access control is important for preventing theft of data and resources for ensuring that they are safe and well kept at all times. Thus in rapidly growing IT environment, unauthorized access becomes a form of threat. An organization or industry may possess a wealth of critical resources, but those resources are not at all available to each and every employee, customer or partner. Industries and organizations must implement access control mechanism to ensure that each user whether inside or outside of an organization had only necessary access to the required resources. We discuss here various architectures, policies and models for access control, which are trying to illustrate why they are so much crucial for any organizations. In this paper we are providing an elaborative approach to enhance access control architecture. Also we discuss some key aspect for designing access control architecture.

Keyword– MAC (Mandatory access control), DAC (Directory access control), RBAC (Role based access control).

I. INTRODUCTION

Is an information flow between an active entity and a passive entity. Active entity is a subject, which requests and access to an object or data within an object, and passive entity is an object that reside data or information inside it. So we can say that access control is an information security feature that can control the flow of information among a subject and an object. That is why access control becomes very important and a front line defense to prevent unauthorized access of the resources or data and securing the organizational resource and data against any unauthorized theft or tampering. Access controls are implemented at individual users system and different layers of a network.

Although different controls provide different functionality, they should all work together to keep the bad guys out and guys in, and to provide the necessary quality of protection.

Manuscript received September 02, 2012.

Ankur Kumar Shrivastava, CMJ University, Shillong, Meghalaya, India.
Abhinav Kumar, Mahindra SSG, Mumbai, India.
Richa Bhatnagar, Department of Information Technology MIET, Meerut, India.
Nidhi Choudhary, Department of Computer Science MIET, Meerut, India.
Mariya Khursid Ansari, Department of Computer Science MIET, Meerut, India.
Amod Tiwari, Department of Computer Science, PSIT, Kanpur, India.

A. The access control has basically four primary elements, i.e.:

- *Identification:* With the help of this we can ensure that a subject is a same entity as it is claiming. A simplest form of identification will be established with the employee id, user name or account number.
- *Authentication:* For proper authentication of himself, subject requires a second piece of credential and that is simply being a token, password or pin.
- *Authorization:* After proper identification and authentication of a subject, system checks into some access control matrix to verify the right of the subject. The process of verifying the rights of a subject is firmly known as authorization.
- *Accountable:* After authorization when a user grants access to the resources as per access control matrix it is important to record the action performed by the subject during access of a resource. With the help of this we can make a subject accountable.

Fig. 1 Primary elements of access control

B. Access control consists of three broad categories:

Each category has different access control mechanisms that can be enforced automatically or manually.

- *Administrative controls* can be responsible for following security goals and objective:
  - Policy and procedures
  - Personnel controls
  - Supervisory structure
  - Security-awareness training
  - Testing
- *Physical controls can be responsible for following security goals and objective:*
  - Network segregation
  - Perimeter security
  - Computer controls
  - Work area separation

- ❖ Data backups
- ❖ Cabling

➢ *Technical controls can be responsible for following security goals and objective:*

- ❖ System Access
- ❖ Network Architecture
- ❖ Network Access
- ❖ Encryption and Protocols
- ❖ Auditing

C. There are seven major different access control functionalities, which are as follows:

➢ *Deterrent:* Intended to discourage a potential attacker.
➢ *Preventive:* Intended to avoid an incident from occurring.
➢ *Corrective:* Fixes components or systems after an incident has occurred.
➢ *Recovery:* Intended to bring controls back to regular operations.
➢ *Detective:* Helps identify an incident's activities
➢ *Compensating:* Controls that provide for an alternative measure of control.
➢ *Directive:* Mandatory controls that have been put in place due to environmental requirements or regulations.

II. ARCHITECTURE, POLICY & MODEL

These three broad categories work together at different levels within their own segregations.

A. Security Architecture

Defines the lowest level hardware and software functions that implement controls imposed by the organization policies and well defined in the models. Basically there are three architecture that are followed at the lowest level:

➢ Systems wide or Network wide based Reference Monitoring:

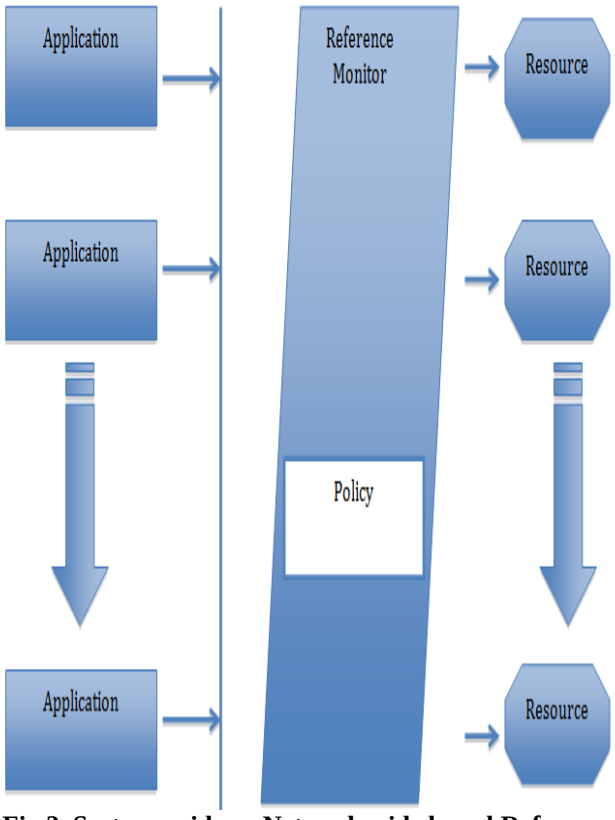

Fig.2. Systems wide or Network wide based Reference Monitoring

➢ Middle-Ware based Reference Monitoring:

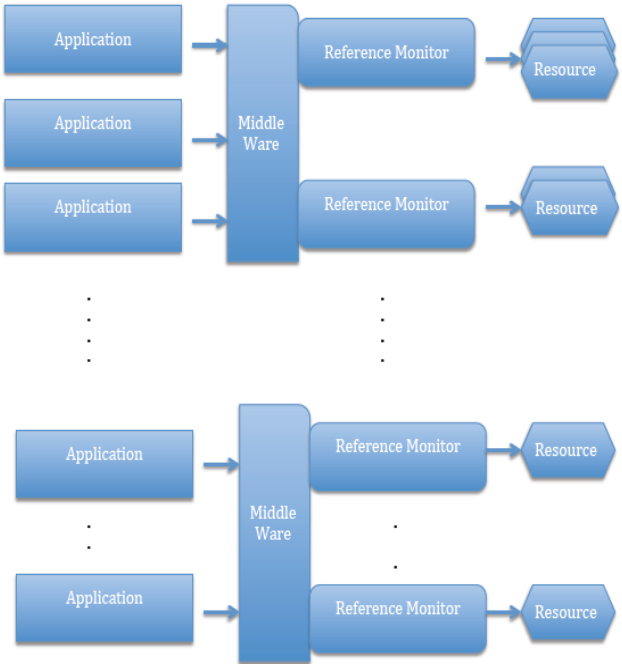

Fig.3. Middle-Ware based Reference Monitoring

➢ *Application based Reference Monitoring:*

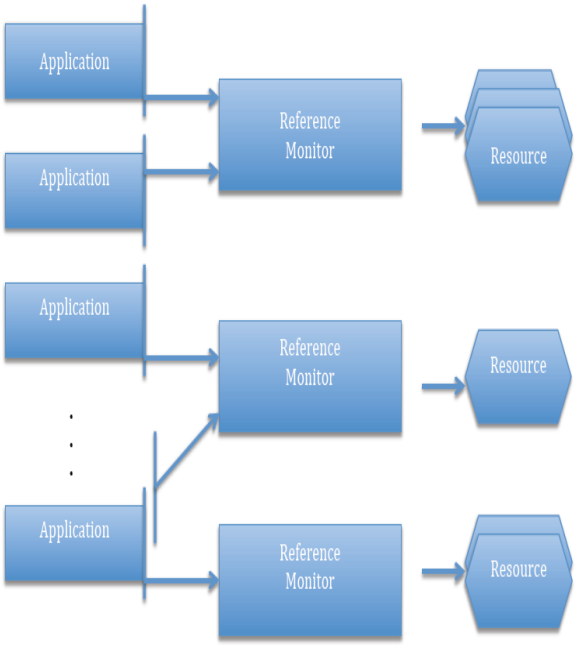

Fig.4. Application based Reference Monitoring

B. Access Policy

Provides a well representation of the various access control security policies and it's functioning. Some popular access control models are:

➢ *DAC Policy:* In Directory access control policy individual users can set the access control to allow or deny the individual object access request. The DAC policy heavily relies on the object owner to allow or deny the access control. This policy is largely implemented in operating systems. Malicious software running on behalf of user is a major threat for this policy, because an owner can easily

change DAC policy, so any malicious program can run on the behalf of owner that can also implement the changes in policy. So we can say that humans are the weakest link in the security in such type of model.

- RBAC Policy: Role based access control policy relies on the roles that a user have within an organization and on the rules which clearly states what accesses are allowed for an individual user in that particular given roles.
- MAC Policy: In this system wide policy determines who are allowed to access and who are not. In this particular policy individual user are not allowed to set or change the access policy. In MAC policy no concept of ownership exists. Users are assigned the access on the basis of normal, confidential, secret and top secret. On the basis of this mechanism security labels are assign to all objects such as files, directories and devices with all its classification information. To get an
- access for an object, subject must have to gone with the security clearance.

C. Access Control Model

Defines the highest level of rules and regulation in order to which, access control must be imposed within an organization. Some popular access control models are such as:

- Bell-LaPadula Model: Bell and LaPadula propose this model in 1986. It is a multi-level model used for enforcing access control mechanism in government and military applications. This model only provides data confidentiality. The following two principles are the basics of this model:
  - *No-read-up:* A subject is permitted to a read access over an object if and only if the access class of the object is dominated by the access class of the subject.
  - *No-write-down:* A subject is permitted to a write access over an object if and only if the access class of the subject is dominated the access class of the object.

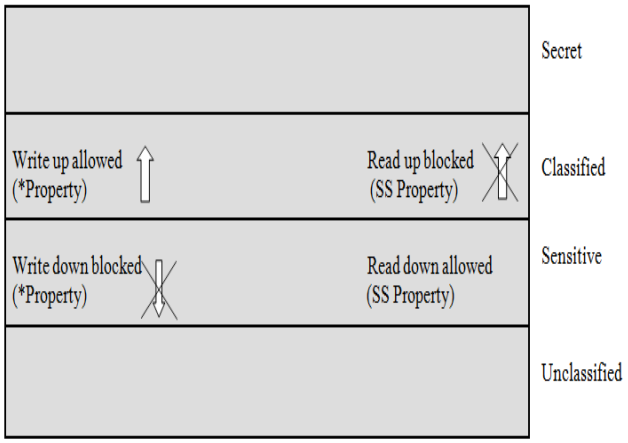

Fig.5. Bell-La-Padula Model

- Biba Integrity Model: Kenneth J. Bibaproposes this model in 1977. It is a multi-level model used for enforcing data integrity. It is in contrast to the Bell-La Padula model, which emphases only on data confidentiality. The following two principles are the basics of this model:
  - No-read-down: A subject is permitted to a read access over an object if and only if the access class of the subject is dominated by the access class of the object.
  - No-write-up: A subject is permitted to a write access over an object if and only if the access class of the object is dominated by the access class of the subject.

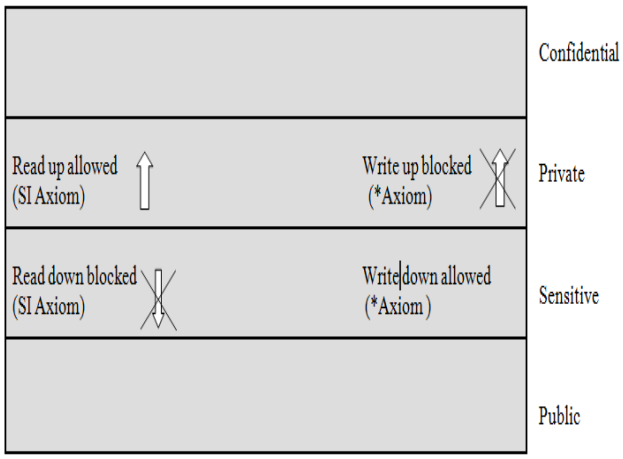

Fig.6. Biba Integrity Model

- Chinese Wall Model (Brewer and Nash): This model was proposed by David F.C. Brewer and Michael J. Nashin 1989. It is designed to provide control mechanism that mitigates conflict of interest in commercial organizations. Brewer and Nash refer to both confidentiality and integrity equally. The environment of an investment house or stock exchange is the best environment for this model.

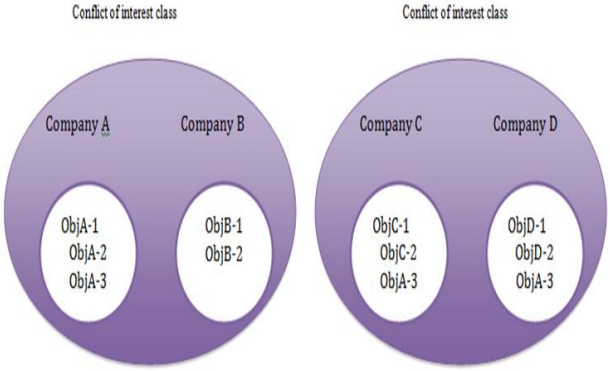

Fig.7. An example of Object organization

Three major concepts, which have been discussed above, provide conceptual partition between different levels of abstraction in the access control design.

III. SUGGESTED APPROACH

On the basis of above discussed architectures, policies and models which will be implemented by various organization for access control and secure interaction of a system, we are proposing here 7-tier architecture for access control when any user want to access restricted resources of the organization. Also we are suggesting here some important key, which must be taken into account before designing or implementing any access control mechanism.

A. The 7-tier proposed architecture is:

- Delegation and Identity Provisioning
- Centralize Authentication Process

- Enforcement of Authorization Policy
- Authorization Process
- Action Performed & Log Created
- Auditing for Accountability
- Maintainability

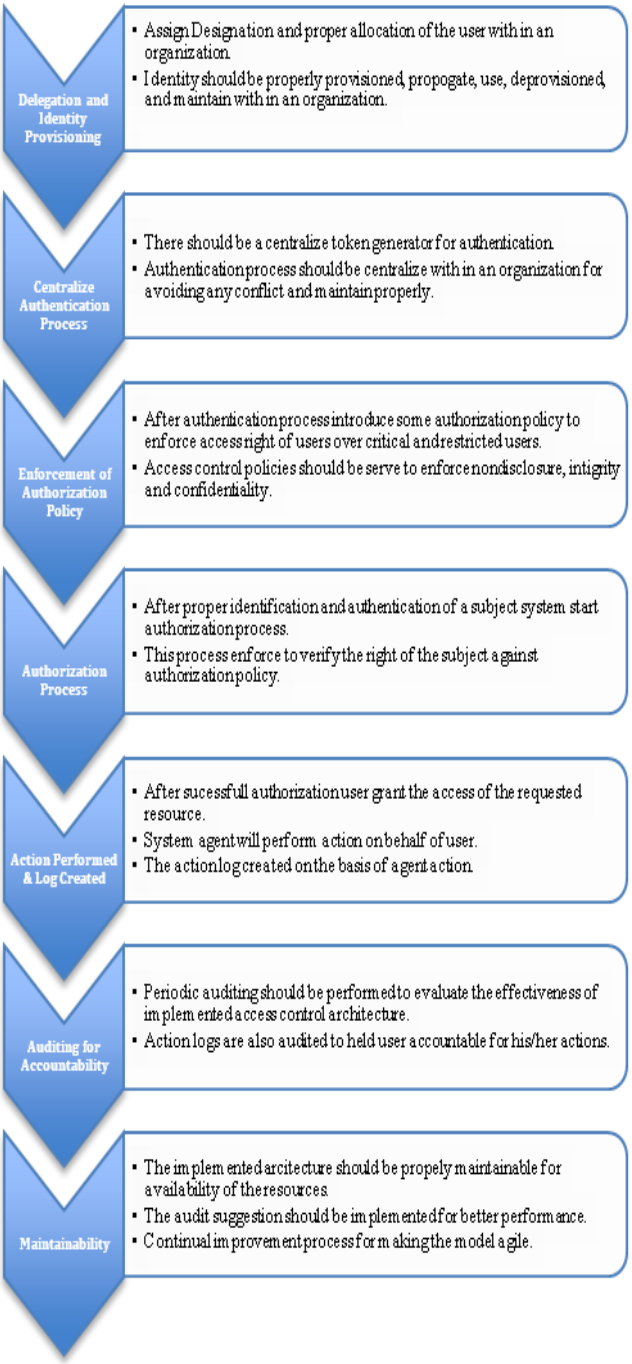

Fig.8. 7-tier of proposed architecture

IV. KEY ASPECT OF DESIGNING ACCESS CONTROL MODEL

There are some key aspect, which an organization must focus before designing and implementing the access control model with in an organization. First of all we have to identify the scope i.e. need and purpose of the access control model with in an organization. Then we have to understand the security requirements for access control and according to the need of our organization access control security requirement chose access control policies (such as DAC, MAC, RBAC) for proposed model. In the adequacy check we can set different level of abstraction for secure access control model, and define how it will provide secure interaction with the system. In next step we examine that whether the proposed model is sufficient enough to enforce all the security policy requirements or not. We should also clearly define the rule and regulation for secure execution of operation within proposed model.

Fig.9. Key Aspect of Designing Access Control Model

In further step (validation of consistency) of design access control model we have to exhibit that the proposed model can be used with any system, which obeys the defined rules of operations and also satisfies the access control model definition of security. Periodic auditing should be performed to evaluate the effectiveness of the model and identified if any security threats or loopholes exist into the implemented access control model. The last but very important key aspect is continual improvement of the model based on audit and testing suggestion and properly maintains the model for keeping it agile in changing and growing environment.

V. CONCLUSION

Our proposed 7-tierarchitectural models facilitate qualitative and quantitative access control security and other dependable attributes. Validation can be conducted at multiple level and provide diverse planes of conformity. The overall objective of a secure access control system implies that security clearances are given conservatively (as opposed to generously). With role based access policy we also implement the same in our recommended architecture. We also discussed some important key aspect of access control designing in this paper. Also this paper throw some light on the various mechanism used in secure access control. Till now due to time constraints we are not able to evaluate the correctness and effectiveness of proposed model but in future we must implement this model and evaluate the result and performance on the basis of its result calculations.

REFERENCES

1. M. Abadi, M. Burrows, B. Lampson, and G. Plotkin. A calculus for access control in distributed systems. ACM Transactions on Programming Languages and Systems, 15:706–734,1993.
2. R. Ahad, J. David, S. Gower, P. Lyngbaek, A. Marynowski, and E. Onuebge. Supporting access control in an object-oriented database language. In Proc. of the Int. Conference on Extending Database Technology (EDBT), Vienna, Austria, 1992.
3. G. Ahn and R. Sandhu. The RSL99 language for role-based separation of duty constraints. In Proc. of the fourth ACM Workshop on Role-based Access Control, pages 43–54, Fairfax, VA, USA, October 1999.
4. P. Bonatti, S. De Capitani di Vimercati, and P. Samarati. A modular approach to composing access control policies. In Proc. of the Seventh ACM Conference on Computer and Communications Security, Athens, Greece, 2000.
5. D.F.C. Brewer and M.J. Nash. The Chinese wall security policy. In Proc. IEEE Symposium on Security and Privacy, pages 215–228, Oakland, CA, 1989.
6. D.D. Clark and D.R. Wilson. A comparison of commercial and military computer security policies. In Proceedings IEEE Computer Society Symposium on Security and Privacy, pages 184–194, Oakland, CA, May 1987.
7. D. Ferraiolo and R. Kuhn. Role-based access controls. In Proc. of the 15th NIST-NCSC Naional Computer Security Conference, pages 554–563, Baltimore, MD, October 1992.
8. http://spdp.dti.unimi.it/papers/sam-fosad.pdf.
9. http://www.fas.org/irp/nsa/rainbow/tg10.pdf.
10. http://en.wikipedia.org/wiki/Access_control.
11. http://www.eit.lth.se/fileadmin/eit/courses/eit060/lect/Lect8.pdf.

AUTHORS PROFILE

Ankur Kumar Shrivastava: Born in 1981 in Ghazipur distict (Uttar Pradesh). Phone Number +919335092777 & E- Mail Id: ankurshrivastava16@gmail.com. He completed his B.Tech. (Information Technology) from Allahabd Agriculture Institute Deemed University, Allahabad, M.B.A. (Marketing) from Sikkim Manipal University, Sikkim, M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad, and currently pursuing Ph.D..He had 2 years Industry Experince from Reliance (RIPL, DAKC), Mumbai. He had more than 1 year Teaching Experience fromMeerut Institute of Engineering & Technology, Meerut. Ankur has published his research work in Springer International Conference of Computer Networks and Intelligent Computing in August, 2011, IT-BHU National Conference of Artificial Intelligence in December,2011 and International Journal of Innovative Technology and Exploring Engineering of Computer Science in August,2012. His major field of Study AreasareInformation Security, Forensic Science, Cryptography, Network Security, Vullnerability Assesment and Penteration Testing, ISO 27001 and Software Engineering.

Abhinav Kumar: Born in 1986 in Ghazipur distict (Uttar Pradesh). Phone Number +919920423488 & E-mail Id: er.abhinavshrivastava@hotmail.com. He completed his B.E. (Computer Science Engineering) from University of Rajasthan, and then attained his M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad. He has more than two years of Industry Experience. Currently he is working with Mahindra SSG as an analyst. He worked with NII Consulting (Mumbai), MG Techno Savvy Pvt. Ltd (Jaipur), and Tryst Technologies Ltd (Jaipur). He has also held a position of a lecturer with Meerut Institute of Technology (Meerut) for four Months. Abhinav has published his research work in Springer International Conference of Computer Networks and Intelligent Computing in August, 2011, IT-BHU National Conference of Artificial Intelligence in December,2011 and International Journal of Innovative Technology and Exploring Engineering of Computer Science in August,2012. He is a certified Lead Auditor for ISO27001, ISO20000, and BS25999. His major fields of work areas are ISMS, BCMS, IT Audit, Risk Assessment, Current State Assessment, Artificial Intelligence and Computer Networks.

Richa Bhatnagar: Born in 1988 in Meerut Distict (Uttar Pradesh). Phone Number +919456019431 and E-mail Id: bhatnagar.richa1@gmail.com. She completed her B.Tech. (InformationTechnology) from Uttar Pradesh Technical University and currently pursuing M.Tech. She had 1.5 year Teaching Experience from Meerut Institute of Engineering & Technology, Meerut. Meerut International Institute of Technology, Meerut. Her major field of study areas are DBMS and Software Testing.

Nidhi Choudhary: Born in 1989 in Saharanpur Distict (Uttar Pradesh). Phone Number +918171532851 and E-mail Id: frmnidhichoudhary@gmail.com. She completed her B.Tech. (Computer Science And Engineering) from Uttar Pradesh Technical University and currently pursuing M.Tech. She had 1.5 year Teaching Experience from Meerut Institute of Engineering & Technology, Meerut. Her major field of study areas are Distributed Systems and Mobile devices communication.

Mariya Khurshid: Born in 1989 in Kanpur Distict (Uttar Pradesh). Phone Number +918791277359 and E-mail Id : khurshid.mariya@gmail.com. She completed her B.Tech. (Computer Science And Engineering) from Uttar Pradesh Technical University and currently pursuing M.Tech. She had 2.0 year Teaching Experience from Meerut Institute of Engineering & Technology, Meerut. College Of Engineering and Rural Technology, Meerut. Her major field of study areas are Data Mining and Warehousing.

Dr. Amod Tiwari: Born in 1974 in Kannouj district (UttarPradesh). Phone Number +919415539025 & E-mail Id: amodtiwari@gmail.com. He acquired his Bachelor degree in Mathematics and Science from CSJM Kanpur University Kanpur and master degree in Computer Science and Engineering from Bilaspur Central University Bilaspur