Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 03, March -2019

A SURVEY ON ROLE-BASED ACCESS CONTROL

A. Monisha[1], V. Manjula[2], S. Mahalakshmi[3]

[1]Department of Computer Science and Engineering, S.A. Engineering College
[2]Department of Computer Science and Engineering, S.A. Engineering College
[3]Department of Computer Science and Engineering, S.A. Engineering College

Abstract — *Role-Based Access Control (RBAC) is a methodology which is standardized for defining security policies and for which users are given the privileges, depending upon on roles as an abstraction representing a set of activities to be performed in an organization. The main advantages of role-based access control are, operational efficiency, IT work, and administrative work will be greatly reduced. Here, permissions are equated to roles instead of single users. Permissions granted to a role are strictly related to the data that are needed by a user in order to exercise the business activities of the role. Users are thus simply authorized to play the appropriate roles, thereby acquiring the roles' authorizations. Comparing with DAC, which the creator of a resource determines who can access the resource, the organization has central control over its resources. RBAC approach is a neutral policy, it has more advantages than DAC and MAC, especially when a flexible, policy-based, fine grained resource access control is required.*

Keywords-*Role-based access control, permission, access, role, user*

I. INTRODUCTION

(RBAC) emerged rapidly in the 1990s as a proven technology for managing and enforcing security in large-scale enterprise wide systems. Its basic approach is that permissions are related with roles, and users are attached to appropriate roles. This greatly simplifies security management. RBAC is a confirm substitute to traditional discretionary and mandatory access controls, as it ensures that only authorized users are given access to certain data or resources. It also helps three well-known security principles such as information hiding, least-privilege, and separation of duties. Access control policy is materializing in RBAC components as user-role, role-permission, and role-role relationships. These RBAC components size up if a particular user is allowed access a specific piece of system data. In specific, role-permission relationships can be predefined, making it not complicated to assign users to the predefined roles. Without RBAC, it is difficult to consider what permissions have been authorized for which users. The access control technique is essentially restriction of using resources and services, deciding whether the subjects are permitted to operate on the objects or not. It assures that only the authorized users can access to specific network information resources. Therefore, access control is the most important and basic security mechanism of computer systems and also one of the most important measures to protect the resources of the information systems. The main feature of RBAC is giving authorities to roles but not users. When a role is designated to a user, this user has all authorities of the role. Different users can be assigned different or same roles, and one more than one role a user can hold at the same time, and a role can belong to different users, and users access resources indirectly by roles.

II. RELATED WORKS

RBAC is not implemented in particular field. It has already placed its footprint in Bigdata, Blockchain, cloud computing. But these are the major places where security plays a major role. If security, then RBAC comes into action. It is not only implemented in these fields but also in other areas which have been discussed concisely.

The implementation of RBAC in ontology is discussed here [1]. They have used authorization and authentication as access. They have enacted this in university domain. By using role assignment, knowledge base, authentication and role set assignment they have implemented this work. They have introduced three algorithms for enacting namely Role delegation algorithm, assignment of single role algorithm, authentication and role set assignment. Their future enhancement is role auditing.

The attributes such as temporal, spatial and work flowed attribute are grouped together and the role is assigned to the as a whole. They have integrated pros of role-based access technique and UCON model [2]. Since this role doesn't well work with the distributed, they have combined all attribute and applied the role so that the user role assignment is updated automatically depending on subject attribute and object attribute. To assign the roles to the user supervisor entity is assigned. Supervisor entity alone supervises the attributes of the user as soon as the user login the system. Their future work is to focus on ubiquitous computing.

In the above-mentioned paper, we have seen all the attributes have been integrated and used. Here they proposed associated spatial and temporal role access in wireless heterogeneous network [3]. They overcome the difficulties in the conventional role access. To handle complex and large database they have proposed a new management scheme. All the user will be authenticated by the WTD server. The server has set of attributes associated with it. By introducing location and temporal constraint one can easily deploy in the wireless environment.

A separate paper has been proposed using temporal constraint [4]. An automata named Timed input output automata has been utilized here. This automata uses ? and ! as their beginning statements. These constraints are captured by two events namely Exp and Set. Set of rules had been enacted by them. They have proposed a fault model also by using mutation-based approach. They provide complete coverage of fault.

The enactment of role-based access is done in IoT also. They have proposed this paper for multidomain MIoT [5]. They have used optimal authorization route for the best authorization route. To overcome the problem of authorization they have deployed intelligent planning theory. Using this efficient and quick authorization is achieved. A new algorithm called PGAO is designed. It helps the admin to make most accurate decision which increases the access safety and reduces the workloads in sharing the resources. Although their system has many merits, the core drawback is they lacked performance. They have suggested authorization decision support system as a remedy to the drawback with a powerful interactive capability. Their future enhancement is automatic authorization.

In web-based environment assigning roles and permission is very tedious task. Such an arduous task is carried in e government sector [6] They fully rely on web. This role assigning will be very helpful for the e government sector to maintain their security and privacy. They enhanced the permission management flexibility. Separated the duties to meet the permission management. The main theme of this paper is to enhance the security of the web documents in the information resource. They have achieved this with the help of web services. It will be very helpful in multi-tie web application. Their future work is to deploy it in the e government sector.

Task based model existed earlier. They have proposed user, task and role constrained which they have described formally [7]. They have implemented in such a way that they have assigned access privilege of one to one mapping that is one user to one task. They have implemented this paper in real time and proved that the access control is efficient and also the cost is reducing greatly.

Healthcare is a major application in which the world moves on. By using role as access control in healthcare application they have collaborated Chinese and western medicine [8]. By collaborating these medicine patients would be more profited. Patients can acquire self – assurance by integrating these medicines. But the main flavor of the paper deals with the patient record. Maintaining or transferring their records is one of the arduous problems. They have introduced this idea to overcome this problem. This paper clears all the past patient incorrect diagnosis record and provide fullest authorization. The main drawback is by integrating these two they may arise some side effect or it may not be suited for some people Their future enhancement is to deploy this application practically.

Role based access formal model was developed by a team of researchers [9]. They have used a special language called Z language to implement. They have contributed three things to develop this model. First is they have totally used the Z language for compassable approach. Secondly, they have identified the various relationships between various inheritances. Thirdly they have contributed three different notions between various role access systems. Their future enhancement is to focus on permission expansion.

Financial sector also gets benefitted with this [10]. A three-layer role access is developed here. The three layers are data, operations and web pages. They have used access control using coarse and fine grain. The anonymous attacks are avoided by using access control called coarse grain. The user privilege is restricted in access control called fine grain. The privilege checking has been overlapped in first and second layer. They have presented a report on performance testing. Assurance of security in information had been provided by them. Their future enhancement is optimization.

Administration management is very mandatory. Managing the user and assigning the roles to the user is very arduous. Wei huang and his partner introduced a decentralized technology [11]. With this user assigned in an efficient way. By using graph, they have solved this problem. The user assignment problem had been solved by using breadth first search with the help of role based access technique. To improve the performance of user assignment problem they have used A* search technique.

The discretionary model was the earliest most of role-based access model. The drawbacks of discretionary model were overcome by role-based access technique. For business application these two models are very important. So, Kathrin Lehman and Florian Matthes has integrated these two models and proposed a meta model using path expressions [12]. Here the access control is represented by using path. The have used many associations such as one – one, one - many, many – many. The main pros of the paper are simple grammar which is being proposed. Their future enhancement is to implement the path expression in reverse order and to provide access control demand resource-oriented access.

By using Peer to peer John S park and his partner have implemented access control for tailoring role access [13]. Here all the decisions will be only made by the peer. They take the decision based on various factors such as community, peer policies, enterprise. It is only suited for individual peer but also deemed peer. They work in collaboration and have provided and efficient access control for utilizing peer to peer. User and permission role assignment is utilized here. The main pros of this paper are it is cost efficient and reliable. Their future work is to implement in computing resource.

Smart grid is a very new invention which collaborated the electrical power and information technology. To overcome the drawback of the existing smart grid they have implemented a paper based on role access [14]. They have introduced a model called AOR model. All the security requirements provide by the national institute of smart grid had been met. They have proposed in such a way that they overcome all the existing critical requirements. It provided an efficient and consistent way of accessing.

III. COMPARISON TABLE

Paper No	Methodology used	Advantages	Disadvantages
1	Authentication and authorization	Ease of access and efficient	No access for role auditing
2	Integrated role-based access and UCON model	High security	Not suitable for ubiquitous computing
3	Spatial and temporal access	Easily used in wireless environment	Performance is not up to the level
4	Timed - input output automata	Fault is reduced	No implementation
5	Optimal authorization route	Highly authorization	Automatic authorization has to be implemented
6	Role based access technique	High secure to web documents	Bug detection hasn't developed
7	Task based access	Cost efficient	No updates
8	Security based access	High authorization	Not yet implemented
9	Z language	Three contributions which improved security	Permission is not fully enhanced
10	Three-layer role access control	High performance	Poor in optimization
11	Decentralized technology	Highly secure	No performance updates
12	Meta model using path expression	Simple grammar	Cannot use the expression in reverse order
13	Peer to peer technology using web services	Reliable and efficient	Not yet implemented for computing power
14	AOR method	Consistent and reliable way of access	No bug reporting technique is introduced

IV. CONCLUSION

RBAC is one of the best mechanisms for providing access and role permission. It introduced a major shift from user-based access control to role-based access control. The number of rules for implementing the access and role permission had reduced to a greater extent. The major powerful advantage of RBAC is, it provides security to the fullest in which many organizations are being benefitted. Although it suffers some drawbacks, many researchers had overcome the issue in RBAC and had made it to gain its strength. It not only provides security to the cloud but also had played its part well in other fields like webservices, e-government, etc. By all the above surveyed paper we conclude that RBAC has proved its potential in providing secure role and access permission.

V. REFERENCES

[1] Avita Katalt, Pranjal Gupta, Mohammad Wazid, R.H. Goudar, Abhishek Mitta1, Sakshi Panwar and Sanjay Joshi, Authentication and Authorization: Domain Specific Role Based Access Control Using Ontology, Proceedings of7'h International Conference on Intelligent Systems and Control, 2013

[2] Guoliang Tanga, Feng Yangb, Zhiyong Zhangc, Jiexin Pud, A Extended Role-based Access Controls Model Temporal, Spatial, Work flowed and Attributed Role-based Access Controls Model, 2010 Fourth International Conference on Genetic and Evolutionary Computing

[3] Hsing-Chung Chen, Yung-Fa Huang, Syuan-Zong Lin, A Generalized Associated Temporal and Spatial Role-Based Access Control Model for Wireless Heterogeneous Networks, 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing

[4] Qiang Liu1, Hao Zhang1, Jiafu Wan2, Xin Chen1, An Access Control Model for Resource Sharing Based on the Role-Based Access Control Intended for Multi-Domain Manufacturing Internet of Things, IEEE Access, volume 5, 2017.

[5] Ammar Masood, Arif Ghafoor, Fellow, IEEE, and Aditya Mathur, Member, IEEE, Conformance Testing of Temporal Role-Based Access Control Systems, Ieee Transactions on Dependable and Secure Computing, Vol. 7, No. 2, April-June 2010

[6] Zeng Zhongping, Zhang Yi, E-Government information security in the web environment based on Role Based Access Control technology, 2008 International Seminar on Business and Information Management
[7] Liu Sainan, Task-role-based access control model and its implementation, 2010 2nd International Conference on Education Technology and Computer (ICETC)
[8] Mei-Yu Wu, Yao-Bao Fong, Applying Role-based Access Control in Combining the Chinese and Western Medicine Systems, 19th International Conference on Systems Engineering
[9] David Power, Mark Slaymaker and Andrew Simpson, On Formalizing and Normalizing Role-Based Access Control Systems", The Computer Journal, Vol. 52 No. 3, 2009
[10] Zhichao WEN, Bo ZHO, Di WU, Three-Layers Role-based Access Control Framework in Large Financial Web Systems, 2009 IEEE
[11] Wei Huang, Yang, Planning User Assignment in Administrative Role-Based Access Control, 2009 ISECS International Colloquium on Computing, Communication, Control, and Management
[12] Kathrin Lehmann, Florian Matthes, Meta Model Based Integration of Role-Based and Discretionary Access Control Using Path Expressions, Proceedings of the Seventh IEEE International Conference on E-Commerce Technology, IEEE 2005
[13] Joon S. Park and Junseok Hwang, Role-based Access Control for Collaborative Enterprise in Peer-to-Peer Computing Environments, Conference Paper · January 2003
[14] Daniela Rosic, Ugljesa Novak, Srdjan Vukmirovic, Role-Based Access Control Model Supporting Regional Division in Smart Grid System, 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks

