International Journal of Computer Applications in Engineering Sciences
[VOL III, ISSUE II, JUNE 2013] [ISSN: 2231-4946]

Strategic Role Engineering Approach to Visual Role Based Access Control (V-RBAC)

M. Shubin Aldo

Department of Information Technology
DMI College of Engineering, Chennai, Tamil Nadu, India.

shubinaldo@gmail.com

***Abstract* -- Work on Role Based Access Control (RBAC) has emerged as the principle type of access control model in theory and practice. RBAC has frequently been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing application. This paper offers a new role engineering approach to Role-Based Access Control (RBAC), referred to as visual role mining. The key idea is to graphically represent user-permission assignments to enable quick analysis and elicitation of meaningful roles. In turn, we propose an idea of merging two algorithms in a hybrid fashion: ADVISER and EXTRACT. The former role structure is a heuristic used to represent the user-permission assignments of a given set of roles. The proposed hybrid approach is a fast probabilistic algorithm that, when used in conjunction with ADVISER, allows for a visual elicitation of roles even in absence of predefined roles. Results confirm the quality of the proposal and demonstrate its viability in supporting role engineering decisions.**

***Keywords*— Role Based Access control, Visualization, Role engineering, Role Mining.**

I. INTRODUCTION

Access Control is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. By leveraging on the observations made in the previous section, we now describe a viable, fast heuristic algorithm called ADVISER (Access Data Visualizer). Given a set of roles, this algorithm is able to provide a compact representation of them. In particular it reorders rows and columns of the user-permission matrix to minimize the fragmentation of each role.The more fragments in the visualization of a role, the higher the role visualization cost. Reordering users but not permissions only affects the number of gaps between columns, and so do Permissions (i.e., Rows and columns are sorted independently). According to our expectation, the visualization cost decreases as the number of samples increases. Finally, extensive applications over real and public data confirm that our approach is efficient, both in terms of computational time and result quality.

A. Role Based Access Control

Role Based Access Control also known as RBAC, [2] provides a popular model for information security that helps reduce the complexity of security administration and supports review of permissions assigned to users. This feature is critical to organizations that must determine their risk exposure from employee IT system access. The concept of [13] role-based access control (RBAC) began with multi-user and multi application on-line systems pioneered in the 1970s. The central idea of RBAC is that permissions are associated with roles, and users are assigned to appropriate roles. This greatly simplifies management of permissions. Roles permissions are created for the various job functions in an organization and users are assigned roles based on their responsibilities and qualifications.

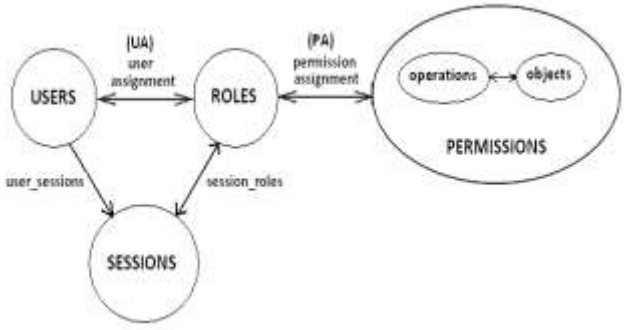


Fig. 1 Core RBAC

RBAC provides benefits in properly administered systems which enable users to carry out a broad range of authorized operations, provides great flexibility and breadth of application. System administrators can control access at a level of abstraction that is natural to the way that enterprises typically conduct business. This is achieved by statically and dynamically regulating users' actions through the establishment and definition of roles, role hierarchies, relationships, and constraints. Once an RBAC framework is established for an organization, the principal administrative

actions are the granting and revoking of users into and out of roles.

B. Visualization

Visualization is the study of the visual representation of data, meaning "information that has been abstracted in some schematic form, including attributes or variables for the units of information". Mainstream data mining techniques significantly limit the role of human reasoning and insight. Likewise, in data visualization, the role of computational analysis is relatively small. The power demonstrated individually by these approaches to knowledge discovery suggests that somehow uniting the two could lead to increased efficiency and more valuable results. *Information Visualization in Data Mining and Knowledge Discovery* is the first book to ask and answer these thought-provoking questions. It is also the first book to explore the fertile ground of uniting data mining and data visualization principles in a new set of knowledge discovery techniques. Leading researchers from the fields of data mining, data visualization, and statistics present findings organized around topics introduced in two recent international knowledge discovery and data mining workshops. Collected and edited by three of the area's most influential figures, these chapters introduce the concepts and components of visualization, detail current efforts to include visualization and user interaction in data mining, and explore the potential for further synthesis of data mining algorithms and data visualization techniques. This incisive, groundbreaking research is sure to wield a strong influence in subsequent efforts in both academic and corporate settings.

C. Role Mining

Role mining is the process of analyzing user-to-resource mapping data to determine or modify user permissions for role-based access control (RBAC) in an enterprise. In a business setting, roles are defined according to job competency, authority and responsibility. The ultimate intent of role mining is to achieve optimal security administration based on the role each individual plays within the organization. Role mining can be done in three ways, called bottom-up, top-down and by-example. In bottom-up role mining, users are given pre-existing roles based on their skills or duties. In top-down role mining, roles are formulated to match the skills or duties of individual users. In by-example role mining, roles are matched with user skills and duties as defined by managers. Role mining (role discovery) uses expectation maximization and cobweb clustering algorithms to discover relationships between users based on similar access permissions that can logically be grouped to form a role.

The role mining process consists of three steps, first is the Setting role mining attributes, Second Creating and running a role mining task and finally Analyzing role mining results and configuring and saving roles.

II. Literature Review

Ravi S. Sandu, [15] introduces a family of references model for RBAC in which permissions are associated with role, and users are made member of appropriate roles. This greatly simplifies management of permissions. Roles are closely related to the concept of user groups in access control. However, a role brings together a set of users on one side and a set of permissions on the other, whereas user groups are typically defined as a set of users only. Longhua Zhang, et al [12], in their paper they introduce a systematic approach to specify delegation and revocation policies using a set of rules. They demonstrate the feasibility of their framework through policy specification, enforcement, and a proof-of-concept implementation on specific domains, e.g. the healthcare environment. They believe that their work can be applied to organizations that rely heavily on collaborative tasks.

David F. Ferraiolo et al provide a simple formal description in terms of sets and relations of role based access control.There is no commonly accepted formal definition and standards encompassing RBAC. Sabrina De Capitani di Vimercati et al, achieve a main security services (i.e) Data protection by the concept of Access control. But, There is incompleteness and inconsistency.

L. Wang, et al [11], introduce flexibility into the procedure of role assignment, ideas are borrowed from ABAC. In an ABAC system, permissions are associated with a set of rules expressed on measurable parameters and are granted to users who can prove compliance with these rules. Based on the analysis of Miao Liu, et al [9], the access control requirements for web services, this paper points out the limitation of current access control models for web services, and presents an attribute and role based access control model for web services. The model automatically produces the role set, accomplishes the mapping among users, permissions and roles, and unifies the access control for web services and data resources involved.

SHEN Hai-bo, et al [8], introduces a key challenge in Web services security is the design of effective access control schemes. However, most current access control systems base authorization decisions on subject's identity. Administrative scalability and control granularity are serious problems in those systems, and they are not fit for Web services environment. Lorenzo Cirio, et al [5], they show how Semantic Web

technologies can be used to build an access control system. They follow the role-based access control approach (RBAC) and extend it with contextual attributes. Their approach provides for the dynamic association of roles with users. A Description Logic (DL) reasoner is used to classify both users and resources, and verify the consistency of the access control policies. Finally, they provide a proof-of concept implementation of the system written in Java.

Ali E. Abdallah, et al [3], in their paper, they clarify the key role-based delegation concepts and define a number of RBAC delegation models with different characteristics. They start by introducing delegation to the simplest core RBAC model. They then refine the core RBAC model to support role hierarchy and show how to integrate delegation and revocation in the hierarchical model. Yonghe Wei, et al [2], presents an attribute and role based access control model for services oriented environment. They have described these components in detail and outlined their interactions. The proposed model introduces the notions of business role and service role, defines an automatically produces service role method based on attribute conditions to assign users to service roles, unifies the access control for web services and data resources involved. Finally, they give an access control algorithm for services. This model can provide fine-grained, supporting composite service access control and mechanism independent access control policy.

Ian Molloy et al, introduces a new role mining algorithm and two new ways for generating datasets for evaluation. But, here difficult to handle attribute information.

III. VISUAL ROLE BASED ACCESS CONTROL (V-RBAC)

This approach is used for setting the roles and permissions for the user working in the particular field. We are applying the visualization pattern to view the user's roles and permissions in the graphical form. To achieve this, a hybrid algorithm is proposed: Adviser and Extract. By implementing this algorithm visualization occurs. From this VRBAC will provide quick access of viewing the user's roles, permission and their complete details in no time.

A. System Architecture

The proposed design is to build a role structure along with the handlers into the Role Based Access Control where the roles and permissions be assigned to the trusted user.

1) Application Controller: User's details such as name, age, address, mail id, gender, phone number, educational qualifications, work experiences etc will be collected in the form of registration aspect and stored in database by the application controller. The privilege of the user will be analyzed according to his/her details in the database and then will be sent to the access control layer.

2) Task Scheduling: When the user login into the page, the application controller assign the roles and permission to the privileged users. The handlers will perform this process.

3) Data Access Control: Access control is the process of mediating requests to data and services maintained by a system, determining which requests should be granted or denied.

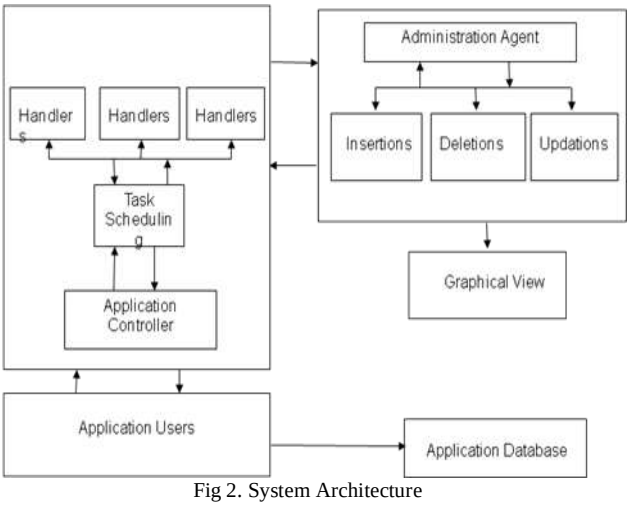


Fig 2. System Architecture

4) Content Manipulation: In our Role Mining concepts with out using database administration we try to perform manipulations. But we couldn't perform entire operation based in files only few operation are consider as a role because of security reasons we play a manipulations like inserting, deleting as well as setting permissions to their employees.

5) Administrator Agent: The system admin is one who maintains the database and controls the overall process being done in the architecture. The admin will collect the user details and stores it in database for later references, the admin will analyze about the user and provide privilege and assign a role for the particular user. Also admin will set predefined rules for an attribute which cannot be modified by anyone else. The admin will provide access control for the users so that the user should perform the action which is only assigned to him. Admin will also maintain the role structure of the organization so that even if a user

leaves, immediately the roles and permissions will be set for the next privileged user according to the delegation constraint.

B. Matrix Representation

The role mining objective is to analyze access control data in order to elicit a set of meaningful roles that simplify RBAC management. Various business information can be analyzed but user-permission assignments are the minimal data set required. A natural representation for this information is the binary matrix, where rows and columns correspond to users and permissions, and each cell is "on" when a certain user has a certain permission granted.

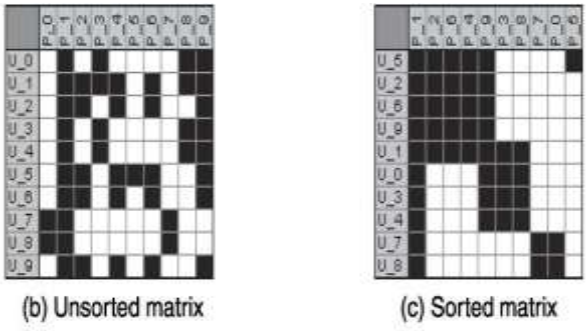


Fig 3. Role Matrix

C. Algorithm Description

We propose hybrid algorithms merging ADVISER and EXTRACT. In ADVISER algorithm, it reorders rows and columns of the user permission matrix. Reordering users but not permissions only affects the number of gaps between columns, and so do Permissions. In EXTRACT algorithm, it extracts the particular user-permission assignments.

ADVISER:

In this algorithm, it reorders rows and columns of the user permission matrix. Reordering users but not permissions only affects the number of gaps between columns, and so do Permissions.

1. Procedure ADVISER(USERS, PERMS, ROLES, UA, PA)
2. $\sigma_U \leftarrow$ SORTSET(USERS, UA, ROLES)
3. $\sigma_P \leftarrow$ SORTSET(PERMS, PA, ROLES)
4. return σ_U, σ_P
5. end procedure

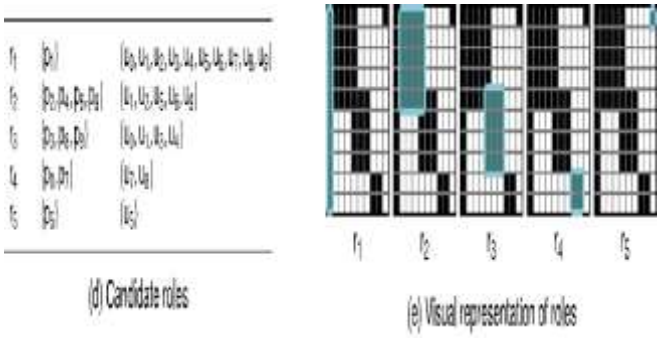
EXTRACT

In this algorithm, it extracts the particular user-permission assignments.

1. Procedure EXTRACT(UP, K)
2. P-ROLES,P-UA, P-PA ← 0
3. For i = 1 ....k do
4. Pick (u,p) € UP uniformly at random
5. U ← users(p)
6. P ← perms(u)

IV. Results and Analysis

A visual representation can highlight potential exceptions within data in an effective manner and a textual role representation reports on information about role-user and role-permission relationships in a less communicative fashion than a graphical representation.



The graph shows the roles assigned for each user.

Also this proposed work will support for dynamic attributes since delegation constraint is added which are used to determine the user permissions and the ability to quickly determine the maximum permissions available to each user, also separate roles are not needed to be framed since the attribute itself will grant the access decisions and assign all conditions needed to the user. By analysing we believe this is an appropriate approach that will retain the benefits of RBAC while extending its utility to today's important distributed applications.

V. Conclusion and Future Work

Role Based Access Control is the best among all access control techniques. But still there are few issues in the Role Engineering criteria. To overcome this problem we have proposed an idea by proposing a hybrid algorithm that supports role mining and role visualization techniques which in turn gives an effective and flexible role engineering approach. Thus this work concludes that the algorithm used in the proposed system represents easy access for applications like banking information system, payroll system, large organizations etc where large number of users involved. This work can be further enhanced by applying various constraints.

References

[1] Alessandro Colantonio,et al"Visual Role Mining:A Picture Is Worth a Thousand roles" IEEE Transactions on Knowledge and Data Engineering Vol 24,June 2012.

[2] I. Molloy, N. Li, T. Li, Z. Mao, Q. Wang, and J. Lobo, "Evaluating Role Mining Algorithms," Proc. 14th ACM Symp. Access Control Models and Technologies (SACMAT '09), pp. 95-104, 2009.Yonghe Wei, Chunjing Shi and Weiping Shao. 'An attribute and role based access control model for service-oriented environment' Control and Decision Conference (CCDC '10), 2010, pp. 4451 – 4455.

[3] Ali E. Abdallah and Hassan Takabi 'Formalizing Delegation and integrating it into Role Based Access Control' Journal of Information Assurance and Security, Issue: 5, pp. 21 - 30, 2010.

[4] Manachai Toahchoodee, Xing Xie and Indrakshi Ray 'Towards Trustworthy Delegation in Role-Based Access Control Model', Information Security, Volume 5735, pp. 379-394, 2009.

[5] A. Colantonio, R. Di Pietro, A. Ocello, and N.V. Verde, "A Formal Framework to Elicit Roles with Business Meaning in RBAC Systems," Proc. 14th ACM Symp. Access Control Models and Technologies (SACMAT '09), pp. 85-94, 2009.

[6] A. Colantonio, R. Di Pietro, and A. Ocello, "A Cost-driven Approach to Role Engineering," Proc. ACM Symp. Applied Computing (SAC '08), pp. 2129-2136, 2008.

[7] Lorenzo Cirio, Isabel F. Cruz and Roberto Tamassia. 'A role and attribute based access control system using semantic web technologies' Proceedings of the 2007 OTM, Volume Part II, pp. 1256-1266.

[8] Zhu Yi-qun, Li Jian-hua and Zhang Quan-hai. 'A General Attribute based RBAC Model for Web Service' Services Computing, SCC '07, 2007, pp. 236 – 239.

[9] N. Li, J. Byun and E. Bertino. 'A Critique of the ANSI Standard on Role-Based Access Control', IEEE Security & Privacy, pp. 41-49, Nov. 2007.

[10] Miao Liu, He-Qing Guo and Jin-Dian Su. 'An attribute and role based access control model for Web services' Machine Learning and Cybernetics, 2005, Volume: 2, pp.1302 – 1306.

[11] L. Wang, D. Wijesekera and S. Jajodia. 'A logic-based framework for attribute based access control'. In ACM Workshop on Formal Methods in Security Engineering (FMSE), 2004, pp. 45–55.

[12] Longhua Zhang, Gail-Joon Ahn and Bei-Tseng Chu 'A role-based delegation framework for healthcare information systems', SACMAT '02 Proceedings of the seventh ACM symposium on Access control models and technologies, 2002, pp. 125-134.

[13] Al-Kahtani M.A. and Sandhu R. 'A model for attribute-based user-role assignment' Computer Security Applications Conference, 2002, pp. 353 – 362.

[14] E. Barka and R. Sandhu 'Framework for role-based delegation models', Proceedings of the 16th Annual Computer Security Applications Conference ACSAC '00, 2000, pp. 168-176.

[15] Sandhu, R.S., Coyne E.J., Feinstein H.L. and Youman C.E. 'Role-based access control models' Computer Volume: 29, Issue: 2, pp. 38 – 47, Feb. 1996.

[16] E.J. Coyne, "Role-Engineering," Proc. ACM Workshop Role-Based Access Control (RBAC '95), pp. 15-16, 1995.