ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 7, July 2016

Performance Evaluation of A Role Based Access Control Constraints in Role Mining Using Cardinality

Yogita R. More[1], Dr. S. V. Gumaste[2]
PG Scholar, Dept.Of Computer Engineering, GES's R. H. Sapat COE, Nashik, Maharashtra, India[1]
Professor, Dept.Of Computer Engineering, GES's R. H. Sapat COE, Nashik, Maharashtra, India[2]

ABSTRACT- A Role Based Access Control (RBAC) is an extremely successful strategy for managing permissions assigned to a large number of users in an enterprise. This offers another approach to deal with RBAC, which is additionally called as visual role mining. Here the key thought or is to graphically represent the user permissions assignments for enabling fast analysis or examination and elicitation of meaningful roles with constraint. For implementing RBAC, within considered organization roles should be firstly identified. Normally the procedure of characterizing the roles is by a base up or bottom up methodology, a process which begins with the permission assignment to each user, is known as role mining. Here this system proposes a role mining problem definition under the cardinality constraints, which means restricting the most extreme number of authorizations or permissions that can be incorporated into the role. Constraints are critical part of RBAC and now and then contended to be the fundamental inspiration for RBAC. Permission usage cardinality constraint is also one of the cardinality constraint which restricts, greatest number of permissions that can be incorporated in a role. In this framework cardinality constraints on number of permissions incorporated into a role have been firstly considered in and Matrix Based Role Assignment (MBRA) algorithm and role miner algorithm has been proposed.

KEYWORDS - Role mining, Role based access control (RBAC), cardinality constraint.

I. INTRODUCTION

Role-based access control (RBAC) has long been recognized as a normative access control model. The essential notion of RBAC is to decouple users and permissions, and then associate both to roles respectively. This substantially simplifies the complexity of users and permissions management, widely perceived as onerous operations by system administrators. Employing RBAC is not only convenient but reduces the complication of access control since the number of roles in an organization is significantly smaller than that of users.

Moreover, the use of roles as authorization subjects, instead of users, avoids having to revoke and re-grant authorizations whenever users change their positions and/or duties within the organization. As a result, RBAC has been implemented successfully by numerous information systems. The trend is that RBAC will maintain its increasing prevalence since the growing demand for cost-effectiveness in management and security mechanism calls for it. Roles, users, permissions, objects and operations are constituents in RBAC where roles represent organizational agents that perform certain job functions within the organization, users are human beings and permissions are a set of many-to-many relations between objects and operations. According to the RBAC reference model , roles describe the relationship between users and permissions. Roles can be hierarchically structured, where senior roles generally inherit the permissions assigned to junior roles. Additionally, constraints such as separation of duties may be associated with the roles.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 7, July 2016

II. LITERATURE REVIEW

With the growing adoption of role-based access control (RBAC) in commercial security and identity management products, how to facilitate the process of migrating a non-RBAC system to an RBAC system has become a problem with significant business impact. Researchers have proposed to use data mining techniques to discover roles to complement the costly top-down approaches for RBAC system construction. It is possible to formulate the problem of role mining in presence of multiple cardinality constraints using the cost driven approach reported in [3]. Suitable penalty weights can be defined to account for constraint violations. It will also provide flexibility by allowing for imposition of soft constraints. For example, if the total cost comprises of, among others, a cost due to the number of roles and another due to violation of a constraint, relative weights can determine whether small violations would be allowed if there is a substantial reduction in the number of roles. The WSC metric used in [4] can be enhanced to include a suitably weighted sum of the number of constraint violations. It may be noted that the number of roles generated will depend on the optimization criterion chosen during role mining. For example, if the goal is to reduce the WSC metric, the number of roles itself might not get minimized. However, the proposed post-processing and concurrent frameworks can be used for any optimization criterion with appropriate modification in the greedy heuristic used for forming the next role at each step of the iteration. The ability of the concurrent processing approach to handle relatively smaller (tighter) values of constraints as compared to the post-processing approach is expected to be the same independent of the criteria. Frank et al.in [2] show that the role mining process can be formulated as multi-assignment clustering of Boolean data. In multi-assignment clustering, an object may belong to more than one cluster at the same time.In role mining, multi-assignments exist in the user-role assignment as well as in the role-permission assignment. The approaches can suitably be modified to enforce upper bounds on the number of assignments during the clustering process based on cardinality constraints.

In traditional access control mechanisms, a user accesses a resource through direct permission given on that resource. In organizations with tens of thousands of users and permissions, the number of user-permission assignments becomes very large, making security administration quite challenging. Over the last few years, there is an increasing trend of using role based access control (RBAC) [5], [6]. In RBAC, permissions are assigned to roles. Users obtain permissions by acquiring the required roles. Since the number of roles is significantly smaller than the number of permissions, RBAC makes security administration more manageable and flexible. In many business scenarios, a more interactive role engineering approach is preferred in which the effort is to formulate meaningful roles by studying the organizational role structure [4], [8], [9]. Hybrid role mining combines both top-down and bottom-up approaches.

III. PROBLEM DEFINITION

Here variety of role mining problems are defined each of which has a different objective which is both meaningful and in the in the perspective of the whole collection of roles in contrast to one single role. So this is first time to introduce the concept of objective into the role mining problems. To the best of knowledge, the notion of an objective which aims to optimize a criterion does not exist in previous research works in role mining paradigm even from the perspective of one single role.

On the other hand, the extensive applications of RBAC urgently call for the association of meaningful and diverse objectives with the role mining problem, therefore, system administrators can choose a specific role mining problem which has a suitable objective in order to meet the specific organizational needs. Roles can be assigned overlapping permissions. This also implies that a particular permission might be held by members of different roles. That is,

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 7, July 2016

permissions are not exclusive to roles nor they elite to a hierarchy. A user may play several different roles, and the user may have a specific permission because of more than one of those roles (since multiple roles may include the same permission).

IV. SYSTEM ARCHITECTURE

We propose a system in which user permissions, roles, constraints are taken as an input. Then we apply two heuristics such as Matrix Based Role Assignment (MBRA) and Role Miner Algorithm. And at final stage we get the best representation of User Permission Assignment (UPA) as an output.

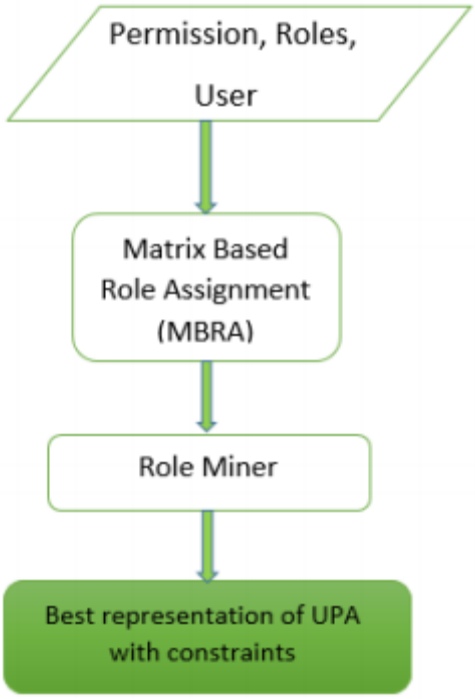

Fig.1 System Architecture Diagram

Snapshot of the GUI is as shown in Fig.2 . It shows the front page of the system in which there are 3 buttons Permissions defined, Roles defined, User type, Files and Upload Dataset

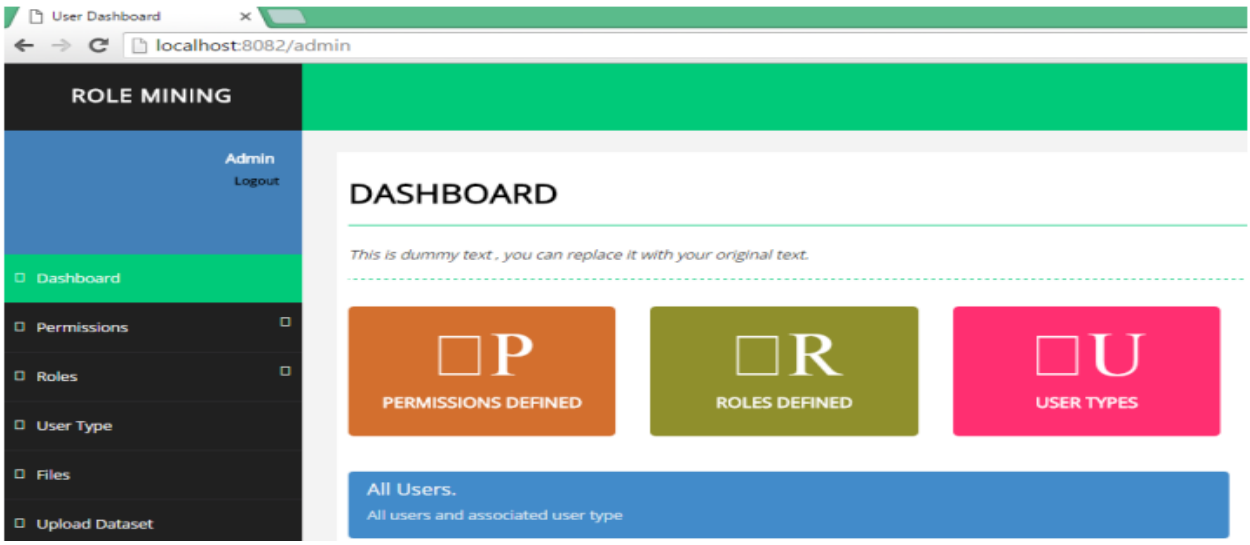

Fig.2 Snapshot of User Interface

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 7, July 2016

V. RESULTS AND DISCUSSION

Snapshot of loading of permission dataset is shown in Fig. 3. In this figure there is upload dataset button for loading the permission dataset, this will load the permission dataset. Here we are assigning file permissions like r for read and w for write and e for execute.

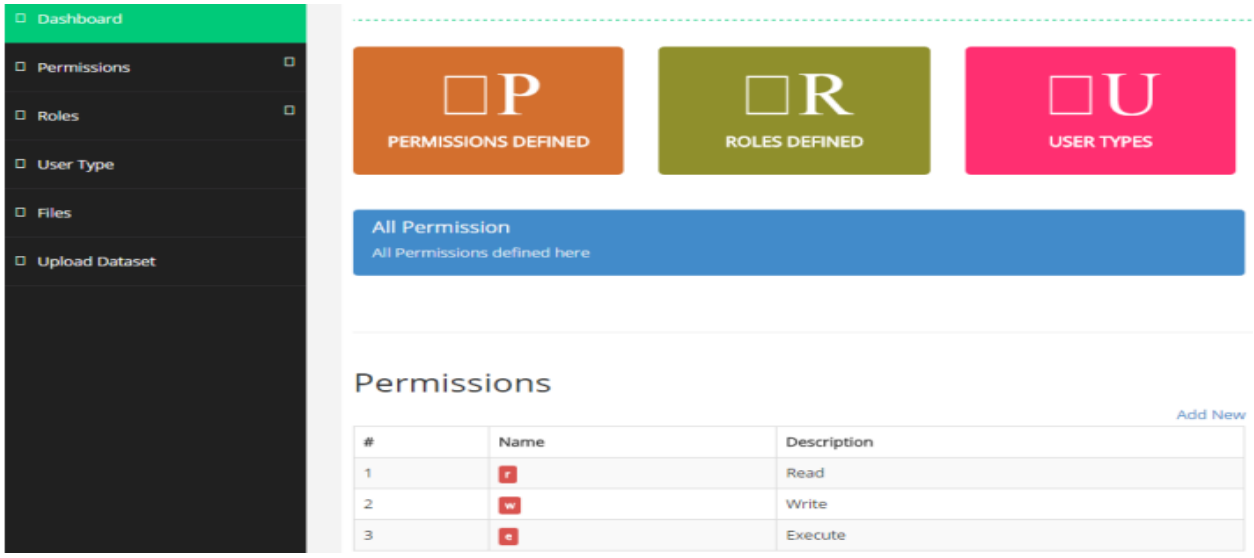

Fig. 3 Snapshot of loading of permission dataset

Snapshot of loading of roles dataset is shown in Fig. 4. In this figure there is upload dataset button for loading the roles dataset, this will load the role dataset. Here we are assigning previous permissions to the roles. And this result will be represented in the form of matrix.

Roles

Add New

#	Role	Description	r	w	e
1	117961	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
2	118219	ROLE_ROLLUP_1 (company role grouping category 1)1	No	No	Yes
3	117929	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
4	117951	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
5	118079	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
6	117902	ROLE_ROLLUP_1 (company role grouping category 1)1	No	No	Yes
7	118315	ROLE_ROLLUP_1 (company role grouping category 1)1	No	No	Yes
8	91261	ROLE_ROLLUP_1 (company role grouping category 1)	Yes	No	No
9	118216	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
10	118090	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
11	118752	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
12	119134	ROLE_ROLLUP_1 (company role grouping category 1)1	No	No	Yes
13	117926	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
14	117890	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
15	117916	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
16	118212	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
17	118256	ROLE_ROLLUP_1 (company role grouping category 1)1	No	No	Yes
18	118555	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
19	118602	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
20	118269	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
21	118106	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No
22	117975	ROLE_ROLLUP_1 (company role grouping category 1)1	No	Yes	No
23	118573	ROLE_ROLLUP_1 (company role grouping category 1)1	Yes	No	No

Fig.4 Snapshot of loading of roles dataset

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 2, Issue 7, July 2016

Snapshot of loading of user type dataset is shown in Fig. 5. In this figure there is upload dataset button for loading the user type dataset, this will load the user type. Here we are assigning previous roles to these user type. Make sure that we have already assigned permissions to the roles in previous steps. And this result will be represented in the form of matrix.

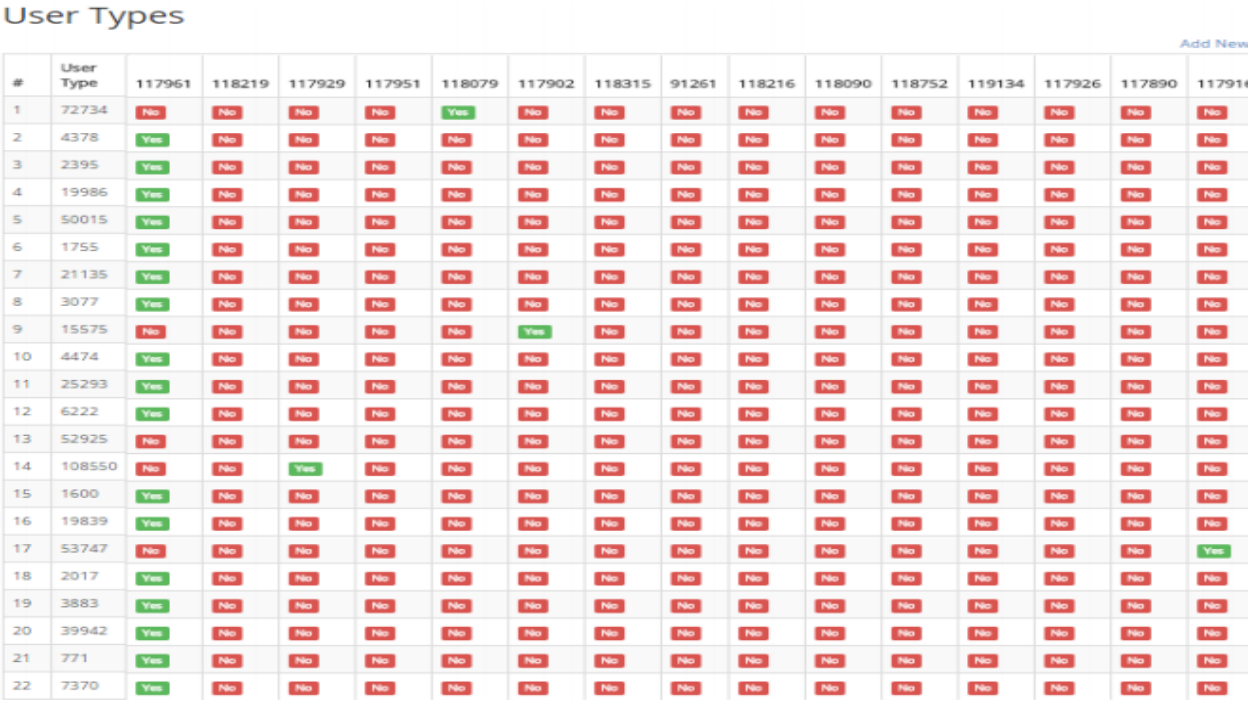

Fig.5 Snapshot of loading of user type dataset

Snapshot of adding new users is shown in figure. 6. In this figure there is a button Add new. U sign this button we add new users by adding their first name, last name, email ID, user type. And here system will automatically generate new User ID and password for each user, which user will user to login into his session.

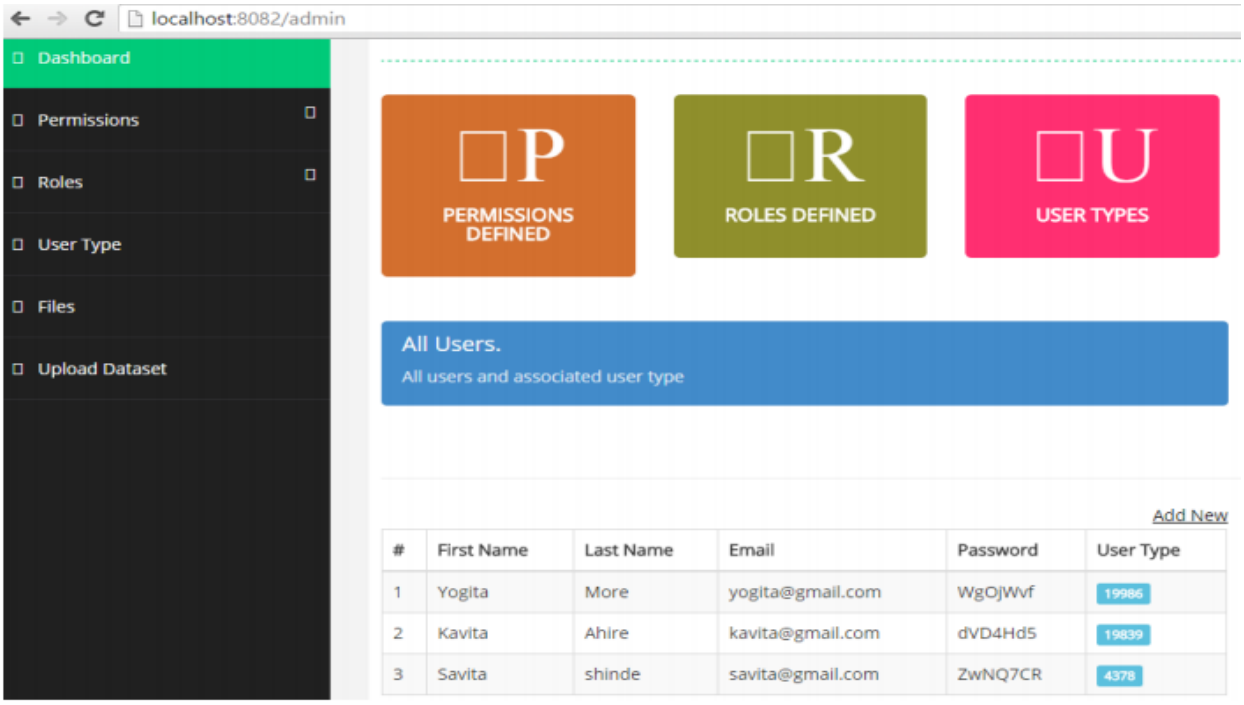

Fig.6 Snapshot of adding new users

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
Volume 2, Issue 7, July 2016

Snapshot after login through user session, user will add his own file is shown in fig. 7. In this figure there is a button Add new. User will be able to add, download or delete this file. Also he can view which permissions are assigned to which roles. But he will not be able to delete files of another user.

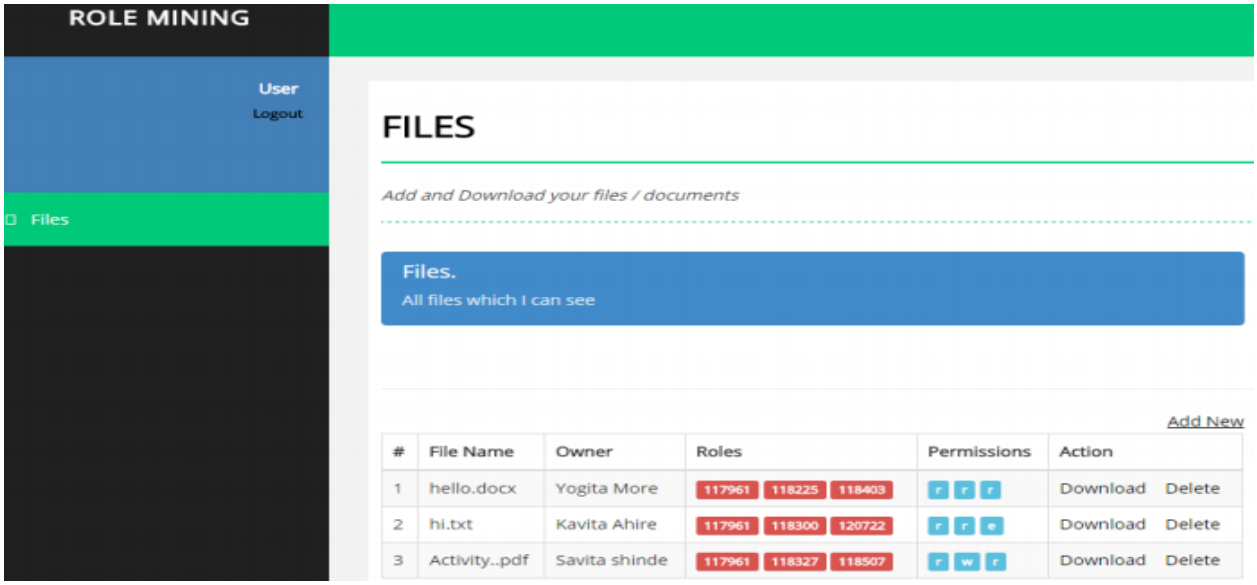

Fig.7 Snapshot of user adding new files

Fig. 7.10 shows search event analysis. When we click on files button on dashboard, Search option is provided over there. Using this search option administrator can search by permissions or roles. In fig. 8 the time required to search in milliseconds is represented on Y-axis against the number of trials (T1, T2, T3) taken on dataset represented on X-axis.

Fig. 8 Snapshot of search event analysis

VI. CONCLUSION

In organizations with tens of thousands of users and permissions, the number of user-permission assignments becomes very large, making security administration quite challenging. Hence over the last few years, there is an increasing trend of using role based access control(RBAC). Devising a complete set of roles is necessary to

implement a RBAC system. This is accomplished by bottom up approach called Role Mining. The bottom up approach starts with existing user permission assignments and attempts to derive roles from them. Visual approach to role mining simplifies the role engineering process. All prior work so far only considers role mining with a single constraint at a time. Here in this system we can impose multiple constraints at a time. Matrix Based Role Assignment (MBRL) algorithm is implemented to represent the user permission assignments in a better way. This representation in matrix format enables quick analysis and elicitation of meaningful roles. Role miner algorithm is also implemented here successfully.

REFERENCES

[1] **Pullamsetty Harika, Marreddy Nagajyothi, John C. John, Shamik Sural, Jaideep Vaidya, and Vijayalakshmi Atluri , " Meeting Cardinality Constraints in Role Mining " , IEEE transaction on dependable and secure computing vol. 12, No. 1, January / February 2015.**

[2] **M. Frank, A.P. Streich, D. Basin, and J.M. Buhmann , " MultiAssignment Clustering for Boolean Data " , J. Machine Learning Research, vol. 13, pp. 459-489, Feb. 2012.**

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

[4] **I. Molloy, H. Chen, T. Li, Q. Wang, N. Li, E. Bertino, S. Calo, and J. Lobo, " Mining Roles with Semantic Meanings " , Proc. 13th ACM Symp. Access Control Models and Technologies (SACMAT), pp. 21-30, 2008.**

[5] **R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, " Role Based Access Control Models " , Computer, vol. 29, no. 2, pp. 38-47, Feb. 1996.**

[6] **D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, and R. Chandramouli, " Proposed NIST Standard for Role-Based Access Control " , ACM Trans. Information and System Security, vol. 4, no. 3, pp. 224-274, 2001.**

[7] **C. Blundo, S. Cimato, " Constrained Role Mining " ArXiv eprints,Mar. 2012.**

[8] **M. Frank, A.P. Streich, D. Basin, and J.M. Buhmann, " A Probabilistic Approach to Hybrid Role Mining " , Proc. 16th ACM Conf. Computer and Comm. Security (CCS), pp. 101-111, 2009.**

[9] **Yogita R. More1, Dr. Shyamrao V. Gumaste, "Survey Paper On A Role Based Access Control Using Cardinality Constraint Of Role Mining" in IJARSMT Volume 1, Issue 6, 2016.**

[10] **D. Zhang, R. Kotagiri, and E. Tim, " Role Engineering Using Graph Optimization " , Proc. 12th ACM Symp. Access Control Models and Technologies (SACMAT), pp. 139-144, 2007.**

[11] **M. Frank, J.M. Buhman, and D. Basin, Role Mining with ProbabilisticModels, ACM Trans. Information and System Security, vol. 15, article 15, Apr. 2013.**

[12] **For dataset : https://www.kaggle.com/c/amazonemployee- access challenge/data.**