Comparative Study of Conflict Management Strategies in Access Control Models

Gayatri Tirokar1[#1], Prof. GautamBorkar 2[#2].

#1Student at Rajiv Gandhi Institute of Technology, Versova, Andheri (West), 022-6113448,
#2 Professor at Rajiv Gandhi Institute of Technology, Versova, Andheri(West)

ABSTRACT

Creating, gathering, manipulating, distributing, using, interpreting, analyzing the data plays a vital role in decision making, interacting and communicating, carrying out various transactions, implementing various strategies to reach the desired goals, carrying out various activities efficiently and many such tasks in our daily routine. Such is the importance of data in all fields. Thus, this highly vital data must be protected from all threats, attacks by implementing various security strategies. Access control mechanism is adopted to monitor which entities in the society are permitted to access what part of the data. Accordingly, the permissions are granted or access is prohibited. This paper mainly concentrates on various security strategies adopted to prevent the conflicts occurring in access control mechanisms. Every strategy has its pros and cons so a comparative study of these discrete strategies will help us to better understand them.

Key words:access control mechanisms, conflict, permissions, security, threats.

INTRODUCTION

The data are raw facts and figures that can be stored and recorded in the system. After storing the data it is continuously processed which transforms data into information. There are many ways to accomplish this task. The stored information forms information assets. The individuals who access this stored data are called as subjects. Authorized subjects are called data owners. The access rights are provided to these data owners to access the required contents.

Information of any organization is highly secretive and confidential. If such vital data is manipulated or hacked by the hackers then it has adverse impacts on company's transactions which also might be beyond repairs. So it is very important to secure this data and protect it against all the possible attacks and threats. Thus, the data can be secured by controlling and monitoring who all are accessing which part of data. This can be achieved by controlling the

accesses made to the data. If any susceptible unauthorized access is encountered then access to data by such entity is blocked.

Access control is one such mechanism adopted to provide data security. It deals with the techniques used to guard the access points. Access points in any systems act as entry points from where the subjects can access the data. So security is required at this access points to block any unauthorized entry to the system. The access is granted only to the authorized entities on identification and verification of their identities. For example, no employee has right to access other employee's personal information. Thus, there are certain conditions set under which the access can be granted to a particular authorized data owner at a particular designation. This is one aspect of securing data.

The data in real world is always dynamic. With the time it continuously keeps on changing. The newer information goes on adding up. Thus modifications like continuous updating, inserting, deleting, altering the data must be practiced to keep data updated. Thus, with the continuous changes occurring in the data, the security policy used also needs to be changed accordingly. Also, these modifications allows the subjects to access certain data and at the same time prohibits them from accessing certain other data. The permissions are granted and prohibitions are imposed in the form of access rights. For example, in a database teacher is allowed to access as well as enter, modify the performance evaluation sheet of the students but at the same time teacher s prohibited to access modify the fee structure details. The account section is permitted to carry out modification in fee structure as and when required.

Thus, as the changes in the security policy occurs the access rights issued to the subjects also has to be changed. Sometimes these modifications gives rise to the conflicts in access control policy. The conflicts are the situations under which certain authorized subjects are given permission to access data but at the same time the access is prohibited as well. So, in this paper we will study and compare different access control models used to resolve these conflicting situations. For example, under certain circumstances the user A is allowed to access data set D but the group of users B, C, A (having user A as its member) are denied access to the same data.

Thus, it is very challenging to achieve access control as there are lot of variations occurring in the highly fluctuating data. So, it is very important to observe and analyze every variation and allow only the authorized users to access required data.

ACCESS CONTROL MODELS

Access control is gaining a lot of popularity as it plays a very important role to keep the data secured. Access control is a security mechanisms which helps to achieve all the basic security goals like confidentiality, integrity, availability of the information systems.

Confidentiality is a security goal which assures that the data is access only by the authorized subjects. No unauthorized access is made to the stored data. Integrity assures that all the modifications to the data are done only by the authorized subjects. Thus, data stored is always precise, accurate, consistent, unmodified or modified in proper authorized ways. Availability assures that the data requested and required by the authorized subject is made available to them in minimum time interval. This security goal prevents the denial of service (DOS) to the authorized users.

Authentication is other major and important aspect of security. It deals with the proper verification of subject's identity before allowing the access to the data in the system. The access control models accepts the requests from authorized subjects to access require data. It the checks

the specified rules and conditions for every received request. The request which satisfies the rules and conditions is given the access while others are denied.

If an unknown subject wants to access the data then such access request is denied by access control models. Also for an organization that follows hierarchical structure the access control models assign certain priorities to the employees. If request is made to access the same content at the same time the employee with the highest priority will be allowed to access the data.

CONFLICTS IN ACCESS CONTOL MODELS

Any access control model functions on positive and negative authorizations. If the access is granted to the authorized subject then it is called positive authorization. On the contrary, the access when denied results in negative authorization. The decision module is used in access control models to grant or deny the authorizations. Certain rules and conditions are set depending on which the access is either granted or denied. Thus, in many models under certain situation if the module determines conflicting rules where one is granting the access while other is denying it then it results in conflicts in the access control models.

The access control models thus function on specific rules and conditions. When these rules and conditions are satisfied the access is granted else it is denied. But the rule conflicts are the major issue that any access control model faces. For example, if s is an authorized subject who has been given the permission to access certain data d while g is certain authorized subject group for which the access is denied and s is one of the subject belonging to this group. So such contradictions result in the conflicting situations.

CONFLICT MANAGEMENT STATEGIES IN ACCESS CONTROL MODELS

Here, we will see some basic ideas and concept about the management of conflicts in various access control models. We will be studying the features as well as the weakness of the different strategies and then finally compare all the studied strategies. The various mechanisms are listed as follows:

1. ROLE BASED ACCESS CONTROL MODEL (RBAC)

The pioneer of this model was rooted in early 1970's. Role-Based Access Control model(R-BAC) is the most popular and widely used access control model to control the accesses made to the sensitive data. In this model the access is given to the authorized subjects on the basis of roles they perform.

This model comprises of four fundamental elements which are roles, subjects, permissions and sessions [1]. Roles are the jobs or functions that the subjects are authorized to perform. Subjects are the authorized users to whom the access is permitted. Permission are the approval given to the authorized users to perform specified operation on the data objects [1]. Sessions are established when user is active performing the specified role on the operations.

The entire functionality of this model depends on the relationships developed between these basic elements. The Fig.1 shows this relationship more efficiently. It depicts that the permissions constitute of the data objects and the operations to be performed on this objects.

From the diagram it is clear that the roles are in between the authorized subjects and the permissions.

So depending upon the role the permission will be given to perform some specific operations on the object. The R-BAC model is highly cost efficient and provides efficient mechanism to control accesses made to the sensitive data reducing complexity. Instead of all these advantages there are limitations which restrains the model from offering full-fledged solution for issues in access control. The fig. 1 depicts the core R-BAC model and the relationship between its various components.

Thus, RBAC is very simple and easy to use. It is best suited for static domain [5]. It has less complexity as the roles are well defined. It does not possess dynamicity. Modification of the roles have to be done in order to change the access rights of a particular entity. The policy specification is very simple. But it faces role explosion problem. Change of the priorities is complex as well as granularity is low in RBAC [5]. Manageability is simple but it has no flexibility so it faces mobility problems.

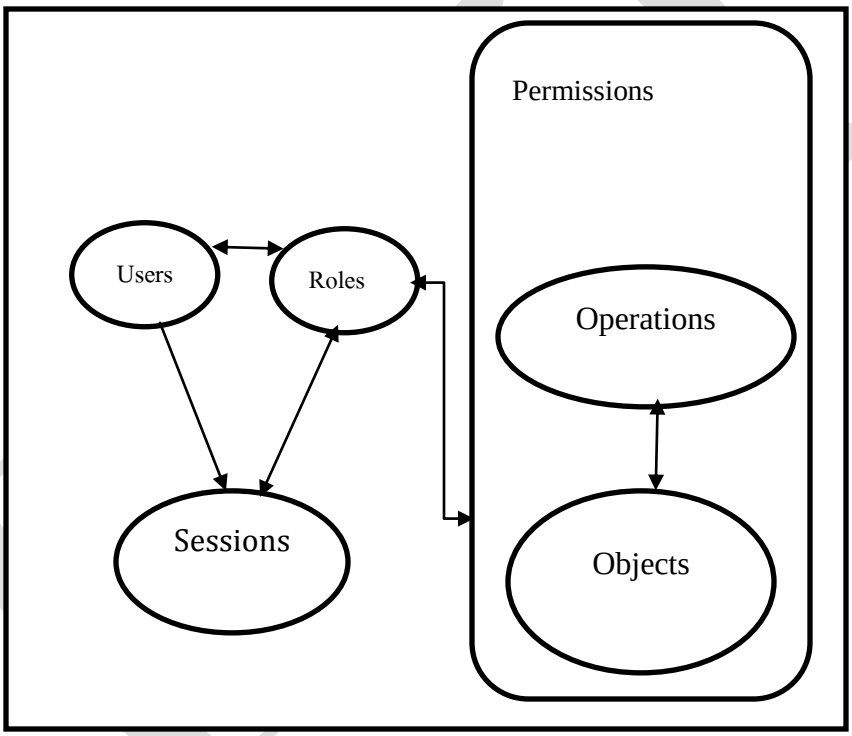

Fig. 1. RBAC Model

2. ORGANISATION BASED ACCESS CONTROL MODEL (Or-BAC)

The major component of this model is organization. The organization comprises of various subjects which are the active users or data, sub-organizations and other entities whose cooperation and coordination leads to smooth functioning of an organization. The organization consists of all authorized subjects who operate in the organization and carry out all required organized activities. Thus, every subject plays certain role in the organization. In simple words, role acts as a link between subjects and organization.

In organizations the hierarchical format is followed for smooth, efficient and organized functioning. The positions of the subjects are in the hierarchical format. Example, clerk is at the lowest level, the employee is above clerk, manager above employee and so on. The subjects are assigned roles depending on the position they have in the organization.

The basic elements of Or-BAC model comprises of organization, role, activity, view, subject, action, object and context [2]. Organization is collection of several authorized officials employed to perform certain specified task. Role is the function the subjects carry out. Activity is the set of operations to be carried out to accomplish the job assigned to the subject. The set of objects that satisfy common properties comprises of views. They are used to add new object to the system. Subjects are authorized users and action is the activity they perform on the objects. The context are the logical rules to derive certain conclusion.

This model functions in two levels. The first level is abstract level which specifies the permissions and prohibitions between role, activity and view [2]. The other level is concrete level which specifies permissions and prohibitions between subject, action and object.

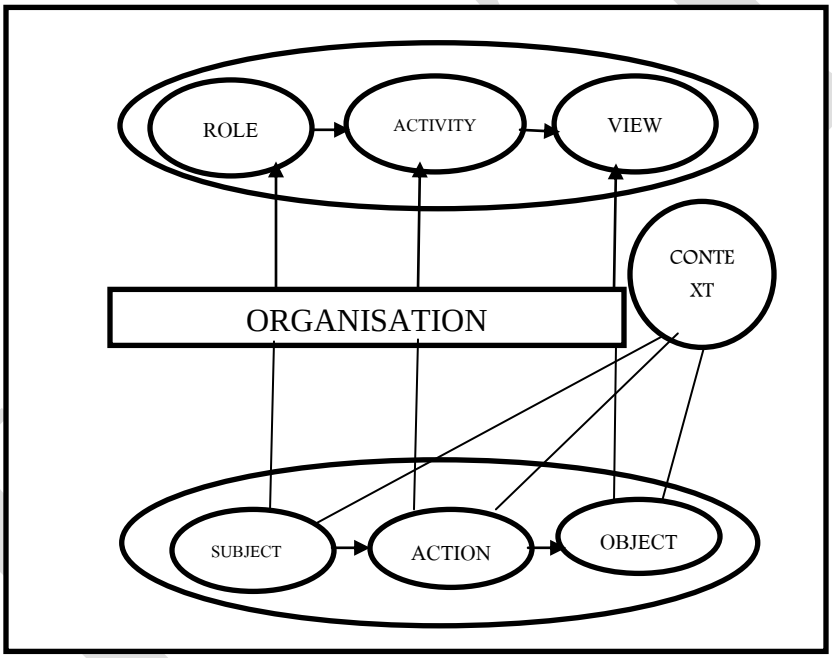

Fig. 2. Or-BAC Model

In the fig. 2 we see the Or-BAC model which shows the relationship between the various components. The context is guiding the subjects performing the actions on the various objects present in the system.

3. PRIVACY AEWARE ROLE BASED ACCE CONTRO MODEL (P-RBAC)

The system administrator is the sole entity who creates and manages the roles and authorized permission. This causes the hindrance and prevents the R-BAC model from offering the full- fledged solution to the access control mechanism in certain situation. This limitation of

R-BAC model is overcome by the core P-RBAC model [3]. It works on the core components of R-BAC model which are privacy, policies and agents. This results in efficient handling of private policy in access control.

The basic components of P-RBAC model are users, role, actions, purposes, obligations and conditions [3]. Thus as seen more components are been added as a result of which more restrictions are imposed on the permissions and this increases the efficiency of access control model.

The users are the authorized subjects permitted to access the objects which are the sensitive data stored in the system. Role is the authorized function that subject access on the objects. Actions is the set of operations of subjects implement. Purpose defines the motto of the subjects to perform the desired actions. Obligation defines the set of responsibility of the subjects and conditions are set to authenticate the subjects before granting the access.

To resolve the conflicts this model uses pair-wise conflict detection mechanism [3]. But this mechanism fails to detect conflicts in more than two policies which acts as a major drawback. To overcome this drawback multi-policy conflict detection algorithms are used.

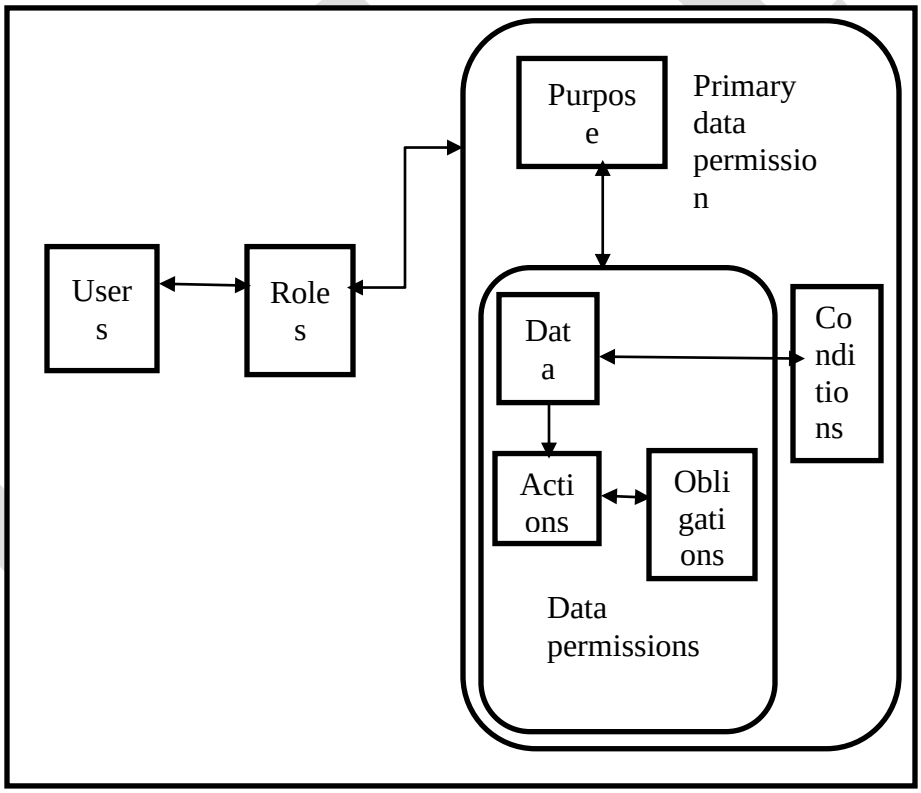

Fig. 3. P-RBAC Model

The fig. 3 shows extension of the fig. 1. The fig. 3 shows the additional components like conditions and obligations being added.

4. ADMINISTRATION MODEL FOR RBAC (ARBAC)

This model is the extension of RBAC model. The major activities carried out by A-RBAC model is to manage the organization, roles, activities, views and context and assign the users to the roles, permissions to the roles and users to the permissions [4]. This model gives a new approach for conflict management by defining various administrative functions by considering various views and the organizations deals with these varied views.

Here we define various administrative functions. Every function deals with the various roles required to access the views. There are two separate roles specified in this model. These are the administrative role which carries out administrative functions and the regular role which carries out the regular functions other than the administrative ones [4].

The fig. 4 shoes the A-RBAC model. Here the users are given the permissions based on their roles. The administrative model controls the permission-role administration, user-role administration and role-role administration.

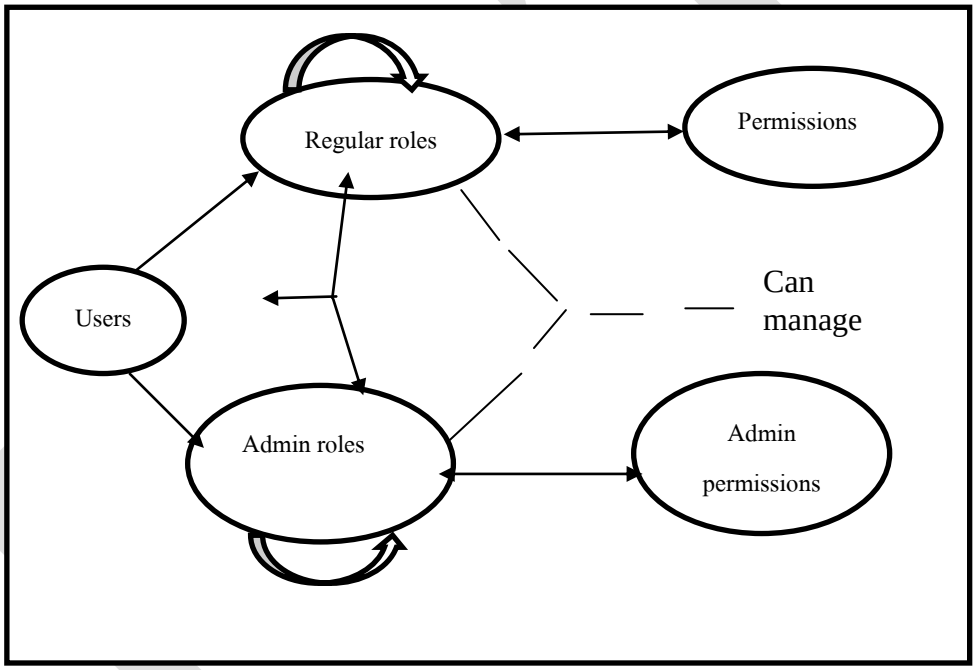

Fig. 4. A-RBAC Model

5. ATTRIBUTE BASED ACCESS CONTROL MODEL

RBAC model faces the user role assignment problem. To avoid this the ABAC model is developed. This model avoids the direct assignment of permissions between users and objects. ABAC is very flexible and is most efficient than RBAC model. It functions on the attributes of the users which can me age, name, address or any other information. Some of these attributes are static while some are dynamic.

ABAC is most suitable to function in dynamic environments owing to its flexibility and efficiency. The subjects, objects and environment attributes form the basic components of the

ABAC model [5]. The diagram shows ABAC model in which objects and subjects both define attributes and their values.

Sometimes heterogeneity in the information supplied by user increases the complexity of this model. To resolve this problem a centralized database is maintained which connects all the attributes in the same format [5]. It's a very complex task to maintain this model also it has lower degree of expressiveness.In this model the authorization decisions are taken globally depending on the users credentials which are dynamically given [5].

The complex task of changing the privileges is overcome by granting access on the attribute basis as a result of which there is no need to change the privileges of the users.

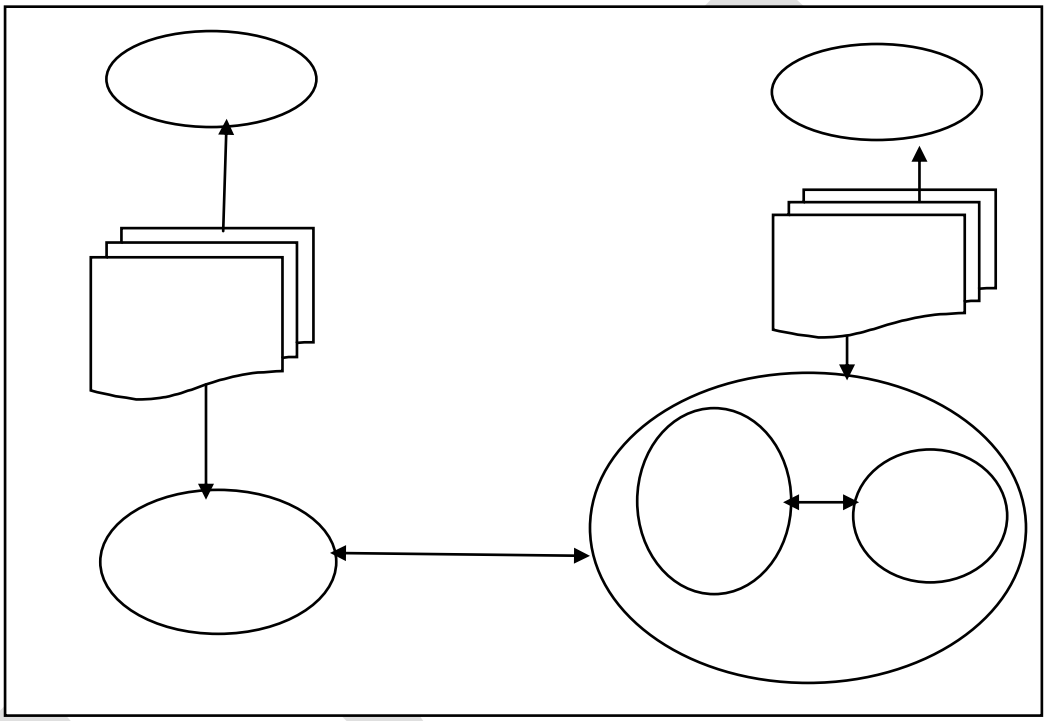

Fig. 5. ABAC Model

COMPARITIVE TABLE FOR CONFLICT MANAGEMENT STRATEGIES IN ACCESS CONTROL MODELS

Table.1. comparative table for conflict management in access control models

SR.NO	PAPERS	RESOURES	YEAR	MODEL	COMPOENTS	FEATURES	CONFLICT MANAGEMENT STRATEGY	DEFECTS
1.	High level conflict management	Journal electronic Notes in Theoretic			Roles, subjects,	Access permissions are associated with roles and ten users are made subjects in	Assigns higher priorities to certain access rules to manage conflicts [1].	Potential to manage current conflicts but fails to manage

	strategies in advanced access control models	al Computer Science(ENTCS) volume 186	2007	R-BAC	permission and sessions	administrative way thus simplifying authorization process. It is a non-discretionary access control model. Provides greater productivity, fewer errors and greater operational security.		potential conflicts [1]. Results in generation of redundant rules [1].
2.	Organization Based Access Control.	IEEE 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Come, Italy.	2003	Or-BAC	Organization, role, activity, view, subject, action, object and context.	Specifies different security polices for various sub-organizations [2]. Security policy comprises of permissions, prohibitions, obligations and recommendation	Logic is used to directly derive the priority of subject automatically depending on security policy.	Administrative model for administrating the security policy is not suggested.
3.	An obligation model bridging access control policies and privacy	Third International Workshop on Policies for Distributed	2004	P-RBAC	Users, role, actions, purposes, obligations and conditions	It's an extension of R-BAC model which supports access control polices and privacy policies separately	Pair wise conflict detection mechanism is used for conflict management [3]	Fails to detect the conflicts occurring in two or more policies.

	policies.	Systems and Networks (POLICY 2002)						
4.	Policy Analysis for Administrative Role Based Access Control	Computer security foundation workshop	2006	A-RBAC	Senior security officer (SSO), junior security officer (JSO) user role administration policy, permission role administration policy, role-role administration policy [4].	It is a decentralized administration for RBAC policies [4]. It specifies authorities of administrators and thus depicts the way in which organization RBAC policy may change.	Administrative functions are define to monitor various roles assigned to require to access views. The SSO is core administrator who divides the policy into to 2 sections and assigns each section to JSO.	
5.	Comparative analysis of Role Base and Attribute Base Access Control Model in Semantic Web	International Journal of Computer Applications (0975 – 8887) Volume 46– No.18	2012	ABAC	Subjects, objects, environment, attributes	Overcomes user role assignment problem of RBAC. Grants access based on the attributes of the user. Highly flexible as works efficiently in distributed and dynamic environments.		Highly complex due to maintenance and specification of policies. Sometimes attributes the user possess don't match with the one's that

								service provider provides [5].

CONCLUSION

We have completed the comparative study of various access control models on the basis of conflict management strategies. We also studied various features of these models and the mechanism they adopt to grant or deny the access.Every model has its pros and cons. We studied the defects and also have seen the models that overcome these defects. The table. 1 indicates the comparison and details of the comparison study.

REFERENCE

[1] High level conflict management strategies in advanced access control models, Journal electronic Notes in Theoretical Computer Science (ENTCS) volume 186, 2007.

[2] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Mi`ege, C. Saurel, and G. Trouessin. Organization Based Access Control. In Proceedings of IEEE 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Come, Italy, 2003.

[3] C. Bettini, S. Jajodia, X. S. Wang, and D. Wijesekera. Obligation Monitoring in Policy Management. In Third International Workshop on Policies for Distributed Systems and Networks (POLICY 2002), 2004.

[4] Policy Analysis for Administrative Role Based Access Control, Computer security foundation workshop, 2006.

[5] Comparative analysis of Role Base and Attribute Base Access Control Model in Semantic Web, International Journal of Computer Applications (0975 – 8887) Volume 46– No.18, 2012.

[6] David F. Feccialo, Janet A. Cugini, D. Richard Kuhn- Role Based Access Control Model: Features And Motivations- National Institute of Standards and Technology U.S. Department of Commerce Gaithersburg md 20899.