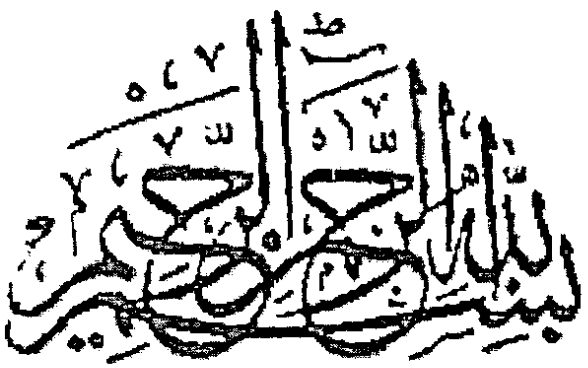
DEVELOPMENT OF RS-XACML BASED ACCESS CONTROL MODEL FOR WEB 2.0

Tehsin Kanwal
Registration # 354-FBAS/MSCS/F07

Supervised by:
Ms.Muneera Bano
Mr.Mata-Ur-Rehman

Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad
2009



In The Name of

ALLAH ALMIGHTY

The Most Merciful, The Most Benefic——ent

To

The Holiest Man Ever Born,

Prophet Muhammad (صلى الله عليه وسلم)

&

To

My Parents and Family

I am most indebted to my parents and family, whose affection has always been the source of encouragement for me, and whose prayers have always been a key to my success.

&

To

My Honorable Teachers

Who have been a beacon of knowledge and a constant source of inspiration,
for my whole life span.

A dissertation Submitted To

Department of Computer Science,

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

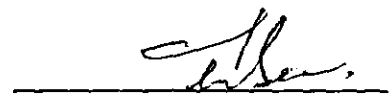
As a Partial Fulfillment of the Requirement for the

Award of the

Degree of *MS Computer Science.*

Declaration

I hereby declare that this Thesis *"Development of RS-XACML Based Access control Model For Web 2.0"* neither as a whole nor as a part has been copied out from any source. It is further declared that I have done this research with the accompanied report entirely on the basis of my personal efforts, under the proficient guidance of my teachers especially my supervisors *Mr.Mata-ur-Rehman and Ms.Muneera Bano* If any part of the system is proved to be copied out from any source or found to be reproduction of any project from any of the training institute or educational institutions, we shall stand by the consequences.



Tehsin Kanwal

Registration#354-FBAS/MSCS/F07

Acknowledgement

I bestow all praises to, acclamation and appreciation to Almighty Allah, The Most Merciful and Compassionate, The Most Gracious and Beneficent, Whose bounteous blessings enabled me to pursue and perceive higher ideals of life, Who bestowed us good health, courage, and knowledge to carry out and complete my work. Special thanks to my Holy Prophet Muhammad (SAW) who enabled us to recognize our Lord and Creator and brought me the real source of knowledge from Allah (SWT), the Qur'ān, and who is the role model for me in every aspect of life.

I consider it a proud privileged to express my deepest gratitude and deep sense obligation to my supervisors ***Mr.Mata-ur-Rehman and Ms.Muneera Bano*** whom kept my morale high by their suggestions and appreciation. Their motivation led me to this success. Without their sincere and cooperative nature and precious guidance; i could never have been able to complete this task.

Finally I must mention that it was mainly due to my parent's moral support and financial help during my entire academic career that enabled me to complete my work dedicatedly. I am also thankful to my loving brothers, friends, and class fellows who mean the most to us, and whose prayers have always been a source of determination for me.

Tehsin Kanwal

Registration#354-FBAS/MSCS/F07

Project In Brief

Project Title:	**Development of RS-XACML Based Access control Model For Web 2.0**
Undertaken By:	**Tehsin Kanwal** **Registration#354-FBAS/MSCS/F07**
Supervised By:	***Mr.Mata-ur-Rehman*** ***Ms.Muneera Bano***
Start Date:	***October,2008***
Completion Date:	***August,2009***
System Used:	Pentium IV

Abstract

A growing need of Access control in Web 2.0 sites demands a serious effort towards finding related research issues and development of Access control Models for access control and authorization. Our aim is to investigate and analyze Traditional Web services and existing web 2.0 access control models to find research issues in access control mechanisms and to develop access control model on the basis of our investigation. We conducted a literature survey for finding the gaps in literature and then evaluate access control models on basis of security requirements. Relation based model, XACML based model and semantic based access control model have potential to express the challenging needs of web2.0 access control requirements.

Our proposed model RS-XACML Based access control model will be interoperable, fine grain, Relation based and semantically descriptive. As a practical realization of our access control model, in future we will test our proposed model at mostly used social networking site Face book.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1 INTRODUCTION

1.1 Motivation and challenges

Nowadays, most of us are using the Web 2.0 applications like face book, you tube, Mashups etc. Web 2.0 sites are based on a particular set of technologies that encourage user-generated content in the form of text, video, and photo postings etc. Any participant can be a content creator in Web 2.0. As User interaction with web changes due to web 2.0 it create new technical requirements for access control mechanisms. This kind of access control must take care of some special requirements created as a result of large amount of web 2.0 user generated contents and their related authorization issues.

Existing web service standards for access control and authorization like XACML why till now not used in access control for web2.0.most of web2.0 access control mechanisms are not fine grained and interoperable. To the best of our knowledge no single web2.0 application is adopting standard access control and authorization model. So why not investigate what is the real obstacle in using web service access control standards in web2.0

Main challenges faced were that Traditional web service Environment and dynamic web 2.0 environment is totally different having different constraints and requirements e.g. in web 2.0 any user can be content creator so can edit and modify contents but in traditional web user were not content creator. In Access control and authorization standard like XACML there is no concept of relations and semantic description of policies created under XACML environment. .There is also need for using web2.0 access control model that should use XACML standard model so as to fill gap between traditional and dynamic environment of web 2.0 there is need of model specifically created for web 2.0 having strong base of design requirement arise after systematic literature survey and requirement analysis process.

1.2 Background

Web 2.0 sites are based on a particular set of technologies such as AJAX and encourage user-generated content in the form of text, video, and photo postings along with comments, tags, and ratings .any participant can be a content creator in Web 2.0. its applications include Face book, You tube, Mash ups etc. eXtensible Access Control Markup Language XACML is also a Web services Security Standards to make the access control decisions including policy creating environment and protocol for exchange of access control information.

Various models exist for access control in web services e.g. Role based, Identity based, Rule based, Attribute based etc. however in order to satisfy the need of web 2.0 related social networking sites Relation based and content based models are proposed but these are not utilized successfully in today's web2.0 environment.

1.2.1 Access control models: web services

Various models exist for access control in web services e.g. Role based, Identity based, Attribute based access control model. Access control decisions on resources are usually taken depending up on information obtained from the identity of the requesting party and the context of the resource. If access control decision depends only on the identity itself, e.g. the user name, it is called Identity-based Access Control (IBAC). If additional information, such as subject roles or task assignments, is considered for access control decision, it is called Role-based or Task-based Access Control (RBAC or TBAC). While making access control decision Attribute-based Access Control (ABAC) models, combine identity, role Information of subject and related resource attribute as characteristics. [4, 5]

1.2.2 Web services: security standards

In web services security standards exists for access control and authorization but unfortunately in web 2.0 we have no such standards Security Assertion Markup

Language SAML is a Web services Security standard that handles the user authentication and also carries attribute information of involved entities.

eXtensible Access Control Markup Language XACML is an OASIS Standards for Web services Security to make the access control decisions. It includes policy creating environment and protocol for exchange of access control information.

The policy language is used to describe general access control requirements and has standard Extension points for defining new functions, data types, combining logic, etc. The request/ Response language makes it possible to form a query to ask whether or not a given Action should be allowed. The response includes an answer about whether the request should be allowed using values: Permit, Deny, Indeterminate (an error occurred or some required value was missing, so a decision cannot be made), or Not Applicable.

Architecture of XACML

User sends access request to the Policy Enforcement Point (PEP). The PEP creates an XACML request and sends it to the Policy Decision Point (PDP), which evaluates the request and sends back a response. The response includes either access permitted or denied, with the appropriate actions performed.

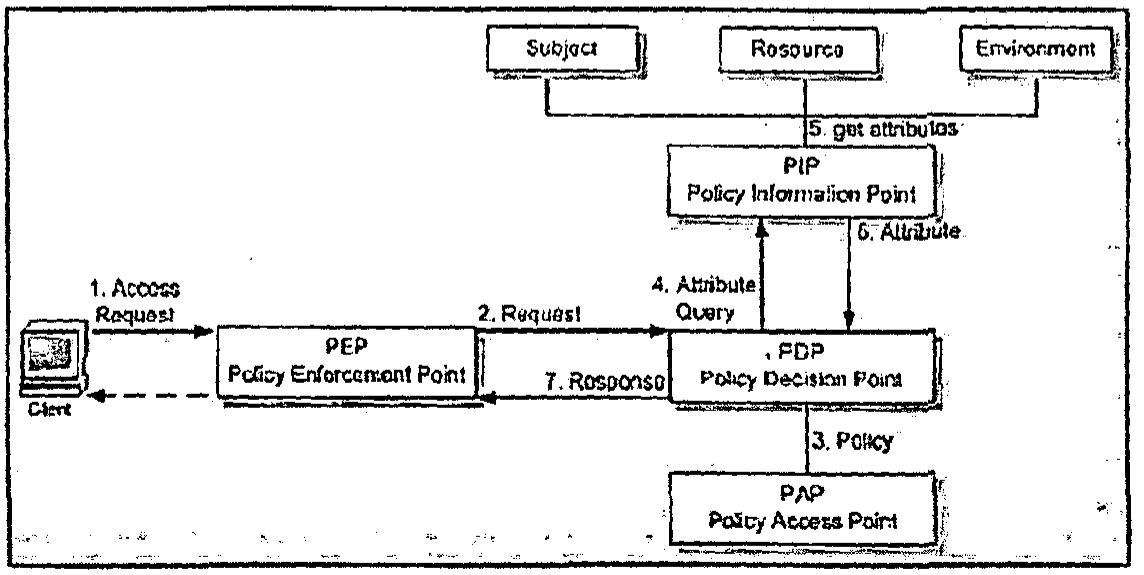


Figure 1-1: XACML Architecture adapted from [22]

The PDP arrives at a decision after evaluating the relevant policies and the rules that are storedwithin it. Number of policies may be available but the PDP does not evaluate all only the relevant ones are chosen for evaluation, based on the policy target. The policy target contains information about the subject, action properties etc. PDP uses the Policy Access Point (PAP), which writes policies and policy sets, and makes them available to the PDP.

The PDP may also invoke the Policy Information Point (PIP) service to retrieve the Attribute values related to the subject, the resource, or the environment.

The authorization Decision arrived at the PDP is sent to the PEP. The PEP fulfills the obligations or necessary actions, based on the authorization decision that is sent by the PDP, it either permits or denies access to the resource. [22]

1.2.3 Access control models: Web 2.0

In order to satisfy the need of some web 2.0 related sites Trust based, content based and more recently Relationship based access control models are proposed but these are not utilized successfully in today's social networking sites. Trust based access control models use notation of trust to grant access to resources. Trust can be computed on basis of type, level, and depth of relationship. Content based access control use object e.g. content attribute in making decision to grant access to a resource that can be any thing including text, photograph, video, etc but content based access control model is not suitable for representing complex security policies

RelBAC splits subjects from objects by defining permissions as relations .RelBAC models permission as relations between subject and objects representing it as an Entity Relationship (ER) model. RelBAC model is developed specifically for new web 2.0 access control requirements but it is still not implemented and till at this time it is not used in web2.0 specific scenarios work is in progress towards refinement of this model [6, 9, 12, 14]

Some Web 2.0 application are using FOAF with the help of FOAF, we can help machines understand our home page, and through doing so, learn about the relationships that connect people, places and things described on the Web. FOAF uses W3C's RDF technology used to Integrate information from our home page with that of our friends, and the friends of our friends, and their friends [13]

There is also research in semantic web direction in order to make access control policies machine interpretable so as to make semantically descriptive policies. Ontologies in OWL can be specified to represent access control models e.g. RBAC, RelBAC etc. [19, 21, 22]

1.3 Research Domain

Access control and authorization in web 2.0 is an area of research that is not well established in terms of standard development of Access control models. Research that is carried out in web2.0 access control is in initial phases as at present no single solution for web 2.0 access controls and authorization solve the problem in standard way.

Our research domain mainly focuses on investigation of web service standard (XACML) to check its feasibility to use in web2.0 environment. Aim of our research is to find the gaps between existing web 2.0 based access control and traditional web services standards and investigate all access control requirement reported in [1] in previous work also keeping in our own view about access control and authorization in web 2.0 scenarios.

We are not redeveloping already established security standards like XACML but try to extent it to include that portions that are among solid web2.0Access control requirements e.g. Relation based, fine grain and semantic interoperability etc.

We will not work at the authentication aspect of web2.0 instead we assume that Authentication had already been done by web2.0 Authentication standard like OpenID. Our focus will be on Access control rather than Authentication.

Web2.0 Access control models like RelBAC and other semantic based access model SBAC will be studied in order to develop a model for access control and authorization. It is used inside XACML standard model with the intent to develop standard interoperable and semantically enriched access control model for web 2.0.

In today's web environment where there is large amount of user generated contents no single existing mechanisms satisfy authorization and content related issues so our access control model will do some improvement in that direction.

1.4 Proposed Approach

Access control and authorization in web2.0 is different from traditional web service access control mechanism. in order to develop a generic conceptual model all the requirements are studied well and deep analysis is carried out in order to find important requirements that most of access control model are missing.

- XACML model for authorization is studied to find the gap that is what should be in it in order to use it in web 2.0.
- At parallel various new and traditional accesses control models like RelBAC, CBAC, and SBAC etc are viewed from point of view of standard web2.0 access control requirements.
- New access control model Rel-Semantic based will be developed to satisfy Relation based and semantic interoperability.
- XACML will be extended as it provide extension in its main authorization purpose so we did extend it and propose Rel-Semantic access control model based XACML architecture is developed.

- XACML also has strong basis for fine grained policy language and providing authorization mechanism so we try to adjust its benefits with deficiencies e.g. with the help of our Rel – Semantic model.

1.5 Thesis Outline

The organization of this thesis has the following structure:

Chapter 2: Literature Survey is given as a mean to Survey existing and previous Access control models of web services and web 2.0.important findings are extracted and shaped at the end in form of Finding Table.

Chapter 3: Requirement Analysis gives an Analysis of previous web services access control models and existing web 2.0 Access control models. It analyzes on basis of standard web2.0 access control requirements.

Chapter 4: System Design explains in detail the Design requirements and proposed architecture.

Chapter 5: Conclusion and out look summarizes the contributions and outlines open issues or rather directions for future research.

Chapter 2

LITERATURE SURVEY

2 LITERATURE SURVEY

2.1 Introduction

In this chapter literature survey is given main aim is to provide a solid base for what we are trying to investigate. We will find the gaps between access control requirements for today's most advance web 2.0 applications especially social networking sites and standard access control mechanisms for web services like XACML.

In Section 2.2 Research Related to Traditional Access control models for web Services and existing new Access control models of web 2.0 is given. Main emphasis is given towards generating useful findings from related research. Section 2.3 organize research findings in tabular form Section 2.4 give limitations of Access control models investigated in previous sections.Section2.5 summaries whole literature survey process.

2.2 Related Research

2.2.1 Attribute based access control model

Attribute based access control model deals with authorization aspect of web services. IBAC and RBAC are not suited in today's collaborated environment the core RBAC model limits user function to roles only; Further, RBAC generally doesn't take into account the characteristics of resources (other than their identifiers); also not contain any security relevant information of the environment .Attribute based access control combine identity and role information of subject as characteristic of subject and resource attribute are also taken while making access control decisions.

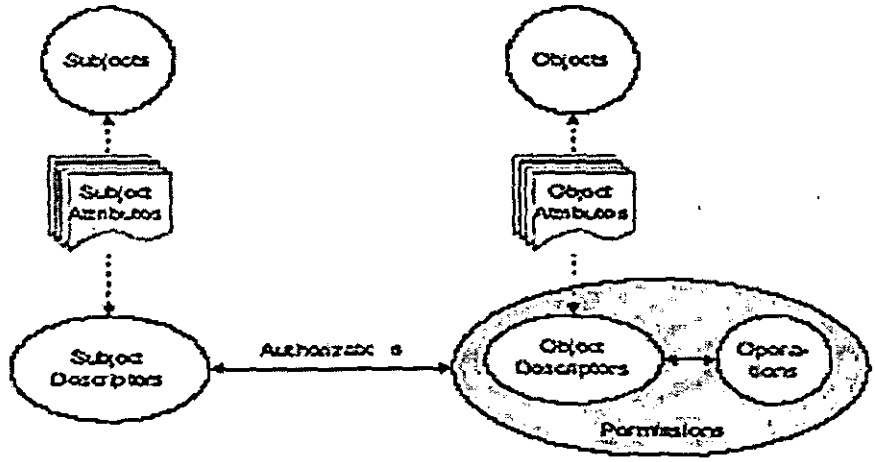


Figure 2-1: Overview of ABAC Model adapted from [24]

policy representation in ABAC is more fine grained and richer semantically due to its rich expressive ability to represent subject resources and environment attribute , so ABAC model is capable of modeling much richer access control semantics [5].

Finding1 : ABAC model is capable of modeling much fine grain and richer access control semantics related to policy representation, but at the same time it fails to satisfy other access control requirements

2.2.2 XACML based access control model

If we move towards web services An XACML based access control model that uses SAML to provide authentication process.

Finding 2: Access model is interoperable across different authorization systems. XACML provides the means for resource administrators to express complex access control policies also allows standard evaluation of access control requests across heterogeneous resources and external subjects [8]

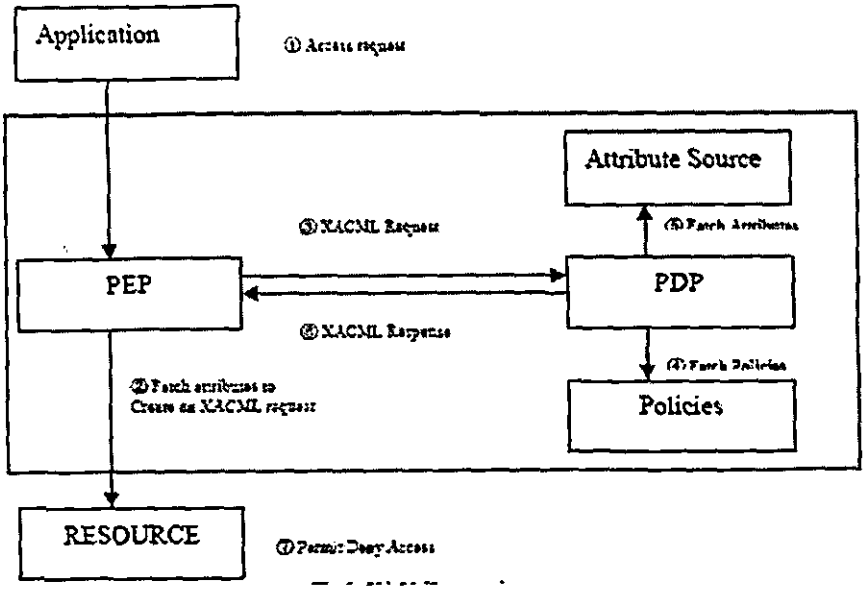


Figure 2-2: XACML overview adapted from [8]

2.2.3 XACML/ SAML based access control model

We can find lot of such examples where use of XACML/ SAML is more than satisfactory in Web services e.g. portals used by different organizations to combine different type of information with the help of remote web services. As portals don't convey the identity of invoker to back end services so to do this a SAML/XACML based access control and authorization mechanism based on PERMIS IS given. XACML RBAC profile is used to define role based policies stored in XML data base. [7]

2.2.4 Access control mechanisms in Web based social networks WBSN

There is growing need of access control in web based social networks. An access control and enforcement mechanism for Web based social networks WBSN is given in[9]. It uses the rule based model for Policy creation and trust based model for granting access to requester. In order to make it reliable certificate server is used for issuing certificates for relationship proof. Its semi decentralized. it give access to resources on the basis of type, depth and trust level of relationship and proof in form of relationship certificate in order to avoid vulnerabilities.

Finding3: work can be done towards representing access control rules in more expressive language like XACML and concept of content based access control [9]

2.2.5 An access control mechanism for online social network OSN

Moving ahead towards online social network OSN an access control mechanism for images is given , no online social network provide this type of feature first to their knowledge .user can specify a relation who could have access to the their contents .Image that a user posts is locked to set of relations specified by user. Only specified relations can view original while others see the fake image. Open ID Authentication mechanism is used and System Implemented Using Firefox Extension. Approach is given experimentally as what user feel when gain such fine grained access control but in long run it is suggested to use ordinary ACL mechanism used in most of OSN Avoiding Browser Extension Need [10]

2.2.6 Milestones based architecture for Web 2.0 Security

In order to protect information on Social web some milestones based architecture combining existing and new technologies is proposed in [4]. Emphasis is given toward introducing semantic description of security mechanisms. they argue that this type o arrangement will be needed if social web users want control on their generate contents .and more importantly for business transactions. A tag-based access control is given, using OWL ontologies (Web Ontology Language) and SWRL rules (Semantic Web Rule Language).usability is given further using user friendly tag based approach handled by users their self.

Finding 4: Security policies for access control can use security standards like XACML In Backend And Express simple semantic description of these using tag based approach.

Finding 5:security policies for access control can be expressed in OWL and SWRL FOAF model is used for user to be a friend according to the information of the Web site's or resource's owner to form a basis for an interoperable security architecture [4].

2.2.7 Privacy Enhanced Access Control Model for web3.0

The user privacy issue in existing web 2.0 access control methods is also highlighted, with the help of this model user can define specific relations with ability to manage and preserve personal information. It's different from existing membership management used in web Applications in sense that it preserves user privacy with the help of WS-Security. FOAF is used to form social network. It also uses 'Folksonomy' with the help of which we can create and manage tags used in content categorization.[3]

Finding6: user defined relationships and content categorization concept is used to build social network or community with the help of subject, object, and permissions giving to users based on the content categorization.

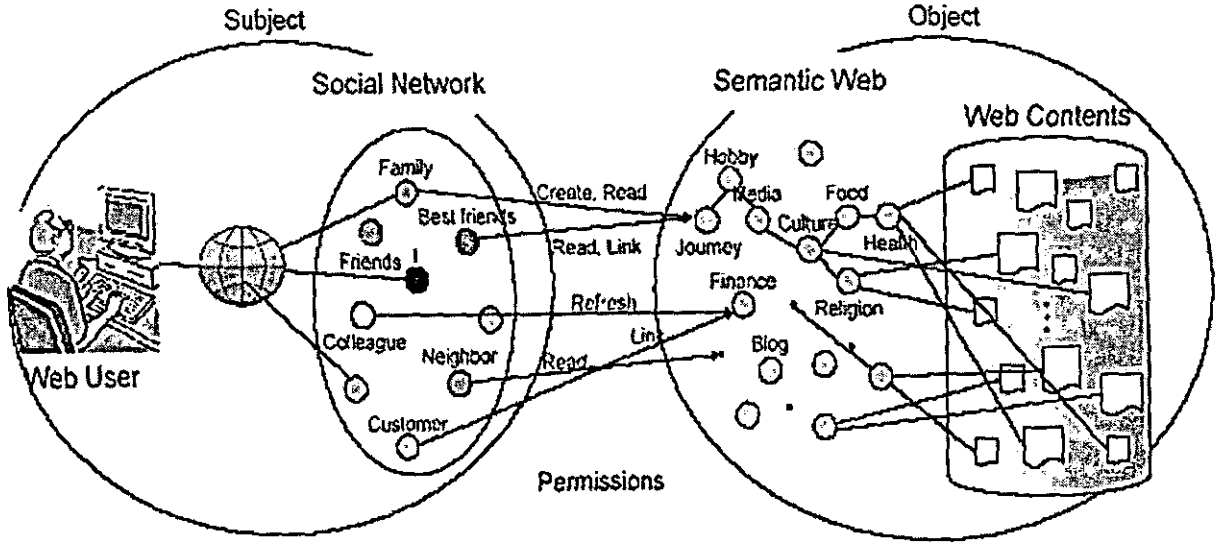


Figure 2-3: Architecture of the Privacy Enhanced Access Control Model adapted from [3]

2.2.8 RelBAC: Relation Based Access Control Model

RelBAC model and its logic is given main difference from other models (RBAC) is that it models permission as relations between subject and objects representing it as an Entity Relationship (ER) model .While access control rules are their realizations with logic on subject and objects. ER diagrams is Translated into Description Logics (DL). RelBAC Logic, allows us to express and reason about users, objects, and

permissions RelBAC splits subjects from objects by defining permissions as relations. Translation of ER diagrams into Description Logics allows for a direct formalization of the RelBAC model into a RelBAC Logic, its done by modeling Subjects (Users) and Objects as Concepts and permissions as DL Roles. ER diagrams provide high level semi-formal specifications of Description Logics. A policy is stated in a logical specification, instead of embedding it into the code, it is good as it can be (easily) changed, contrarily to the RBAC case where the policy is hardwired in the system code.

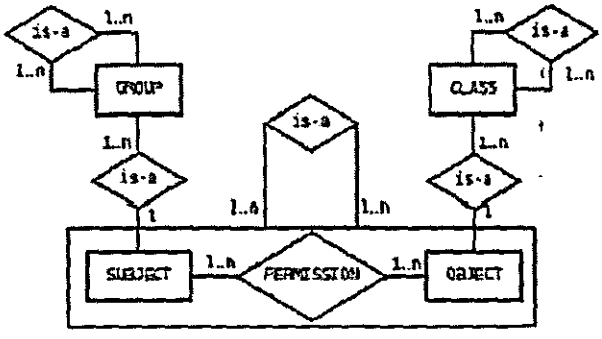


Figure 2-4: The ER Diagram of the RelBAC Model adapted from [12]

Finding 7: RelBAC models permissions as ER relations and allowing for logic aware access control policies. It allows for a direct embedding on policies into a (Description) Logic which allows to reason about them. For addressing the complication of the current new Web open, highly dynamic applications RelBAC is necessary. It will be possible to use RelBAC as some kind of enhanced RBAC [12]

In their first implementation of RelBAC, they have implemented user and object directories as Lightweight Ontologies and performed some preliminary evaluations of the possibility of automatically classifying users and objects in directories and of automatic generation of permissions based on the user interests, using the Semantic Matching technology. This direction give some hint towards sharing access control policies using Web standard languages, e.g., OWL. BelBAC allows for a direct embedding on policies into a (Description) Logic that make possible to reason about them. RelBAC provide

mechanism to address the complication of the current new GRID and Web open, highly dynamic applications. Make hope that in the end it will be possible to use RelBAC as some kind of enhanced RBAC

There is an approach to integrate policy based and reputation based approaches into a versatile trust management language. Both approaches establish trust in distributed and decentralized systems. This approach is proposed in the context of open and distributed services architectures. Emphasis is on trust management mechanisms having different policy languages and engines for specifying and reasoning on rules for trust establishment. Argument is given that policy based decisions can be enhanced by numerical-based ones and vice versa. An integrated approach is needed for real world scenarios. Trust management framework capable of addressing the variety of semantic web scenarios. [6].

2.2.9 CBAC: Content- Based Access Control Model

The CBAC models are similar to ABAC, as it can be implemented by assigning attributes, and granting access based on an object's attributes.

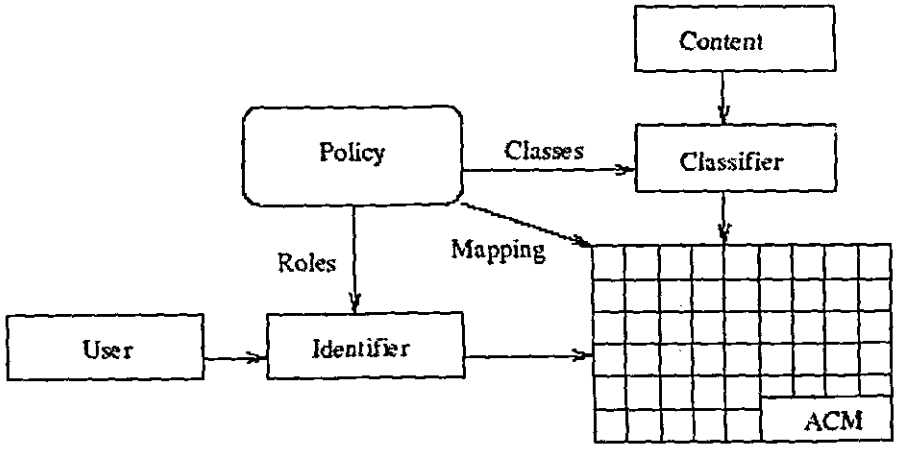


Figure 2-5: architecture for implementing CBAC adapted from [14]

Architecture for implementing CBAC Use a set of roles for users, a set of classifications for objects in the system, and an access control matrix relating roles and classes, and an Enforcement mechanism.

Finding 8: Content based access control share similarities with ABAC and like RBAC concept of roles is used in creating policies, that kind of access control is needed for social net workers but not for complex security requirements.

Finding 9: Friend's model adopted by face book sites needs to be revised as it is not expressive enough. Although it is working but fails to provide fine grain access control concept [14].

2.2.10 XACML: need in Web based social networks WBSN

In literature need of XACML in social networks is also reported emphasis is given to authorization.

Finding 10: social network members should made fine grain access control policies that meet their specific needs. There is a need for expressive language for fine grain access control. We can write policies using XACML defined functions and also it's extended functionality.

Data sharing principles are also applicable to social networking sites.

"Requirement 1: Who can see what is clearly the responsibility of the data owner. In both cases, however, the inability to consider some friends differently from others results in rather cumbersome models. Requirement 2: As one cannot predict a priori what policies particular data owners might wish to impose, support for flexible and fine-grained models is essential"

Finding 11: In face book simple access control related to profiles, contact information is given we are not able to view information by friends of particular .there is no facility

now e.g. in face book if we want that our photograph is only viewed by our female friends.

According to them e-health and social network data sharing requirements are similar but specifically their concern is with trust relationship and with utilization of XACML. its side effect is complexity, policy creation language should be expressive but we should keep in mind that users of social networking site are all not so trained to understand the complex mathematical logic while representing its needs for creating access control policies [11].

2.2.11 Extended RBAC profile of XACML

There is need for platform independent light weight communication mechanisms to facilitate interoperability for web services and some may also be true for web2.0 application One of these security policy languages is an OASIS standard XACML describes both a policy language and an access control request/response language.

Finding 12: XACML like standard language to express the access control is essential but it is just a way to write policies and rules. Question is how we can use the access control models model within these existing access control languages

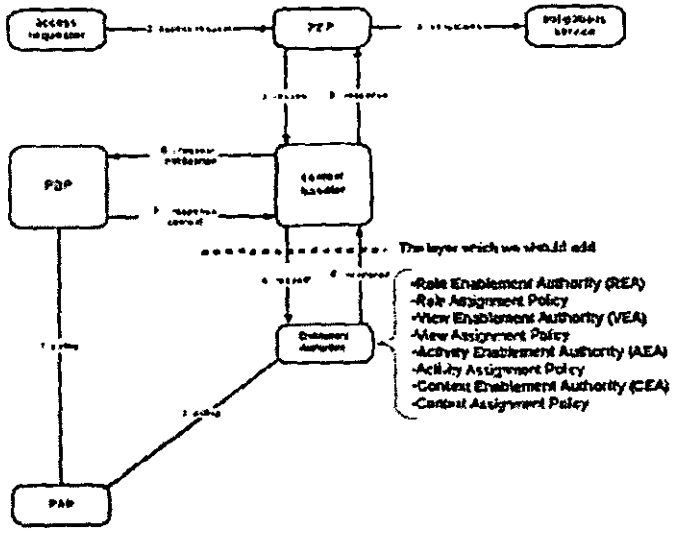


Figure 2-6: The extended profile architecture adapted from [15]

e.g. The RBAC profile of XACML expresses a way to use the standard XACML access language within the RBAC model As XACML is an extensible language where we can add new attributes to the elements defined in the standard,. low level access control models like ABAC are ignored that is very close to the XACML language but complex to use to express some security rules, in particular, constrained and contextual ones the extended profile can meet the requirement of general access control models DAC to more sophisticated one like ABAC the same process of role assignment as proposed in the RBAC profile of XACML is used, There are no publicly available implementations of the RBAC profile of XACML. It give us some intuition that why not we try to introduced Relationship based access control model concept as thy use XACML profile for extended Role based access control model (we can say relationship based model as natural extension of Role based model[15]

Finding 13: RBAC profile of XACML use standard XACML access language within the RBAC model [15], we can say RelBAC as enhanced form of RBAC model [12]. We can introduce RelBAC model in XACML access language. [Self generated].

Finding 14: Face book restrict information availability to specified networks, Face book users are still unable to define their own.

2.2.12 Use of RDF metadata to specify and enforce access control policies

In [16] an approach to use subject, object attribute to perform access control in web environment is given. New thing is about using RDF metadata to specify and enforce access control policies by defining subject and object attribute in access control mechanism. Their architecture mainly consists of PEP; PDP, Attribute validator, RDF parser, policy management tool. RDF parser is applied to extract the respective attribute values from the document. Policy management tool used to define policies in PDP .Attribute validator is used to validate attribute integrity if attributes are presented as XML/RDF statements, the XML-Signature standard can be applied to validate these attributes. Their Architecture is based on existing and tested components and they use it

according to their specific needs. e.g. RDF parser, and web server components provided by the ActiWeb framework. An overview of architecture and a prototype implementation using RDF-based attribute documents is given.

Finding14: RDF metadata can be used specify and enforce access control policies in Web-based environment as RDF is flexible and can be integrated in a semantic web context.

2.2.13 Privacy Preserving Trust Authorization Framework Using XACML

In [17] a trust authorization framework (TAF) that builds on the Capabilities of XACML to support the bilateral exchange of policies and credentials with the help of trust Negotiation is proposed. To make the services and resources available to legitimate users an authorization infrastructure requires the users' attributes, at the same time users may not be ready to disclose their attributes to a remote service provider without confirming exactly the providers identity and how their personal attributes will be used. In this paper approach that is used for addressing these privacy concerns is to employ a bilateral exchange of policies and credentials between the parties involved in the transaction.

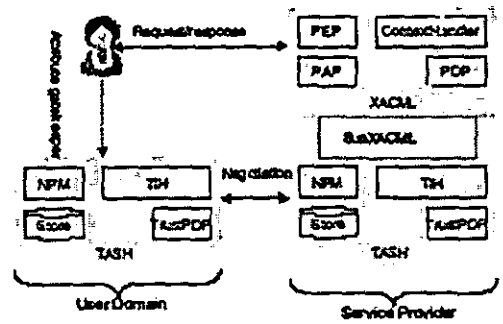


Figure 2-7: XACML Trust Authorization Architecture adapted from [17]

Proposed XACML Trust Authorization Framework (XTAF). XTAF is a loosely coupled architecture with a trust component that protects authorization information (policies and credentials). A Trust Authorization Service Handler (TASH) to handle trust and privacy of authorization information is added in core XACML. In TASH, the Negotiation Protocol Module (NPM) handles the trust negotiation protocols and ordering of messages in building a trust relationship. The Trust Information Handler (TIH) is responsible for the canonical representation f the inputs consumed by the TrustPDP and the outputs from

it. The TrustPDP handles trust access management decisions. Their model optimistically addresses the problem of probing attacks so that the risk to which a party is exposed at any point in the negotiation can be minimized. Framework has the capabilities to protect resources, policies and credentials in distributed environment for users with or without pre-existing trust relationships. The proposed framework is implemented in SunXACML and the PERMIS Attribute Verifier subsystem.

Finding15: XACML model can be used in providing privacy and trust that is gradually incremented using bilateral exchange of policies protecting resources, policies and credentials in distributed environment.

2.2.14 Enforcing Privacy by Means of an Ontology Driven XACML Framework

Different from the conventional form of usage the ontologies are taken to generate access control policies. Why we use ontologies and convert them in to standard policies? The implemented rules are represented in a transparent and comprehensible form. XACML policy language provide this way, third persons have the opportunity to comprehend the system. Moreover, if the legal situation about privacy rules changes the affected entities can easily be modified. In their case this is done by the data protection officer. Working mechanism of policy generation is shown in detail.

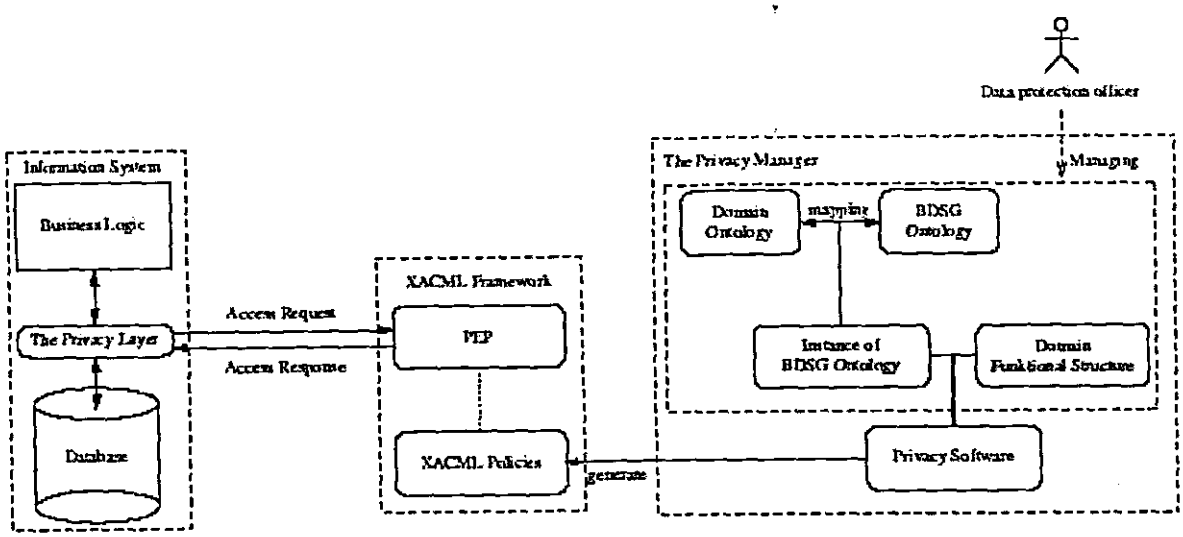


Figure 2-8: A conceptual architecture to adapt privacy directives adapted from [18]

The Privacy Manager generates the XACML policies used by the XACML Framework. it is managed by the data protection officer. It consists of an ontology that represents the German Federal Data Protection Act BDSG. Ontological technology was used because we have through this a mechanism to map law statements to a machine interpretable language without losing any aspect of its meaning. Data protection officer running the system provide the missing Meta and world knowledge, XACML provide a mechanism that offers much finer granular access control than simply denying or granting access in addition to its own benefit of providing a portable and standard system. The ontology represents the collectivity of the policies the transformation from the ontology's native format into XACML conform policies can be done the XACML policies are derived from the ontology .a query is submitted and is evaluated e.g. to check the legality of an action checks all paragraphs and action is allowed if conforms from paragraph. the result of query is transformed in to XACML policy.

Finding16: Ontologies can be used to provide transparent and machine interpretable language and result of ontologies can be transformed in to XACML standards mechanism.

2.2.15 ROWLBAC - Representing Role Based Access Control in OWL

In [18] relationship between the Semantic Web based policy languages (OWL) and the Role Based Access Control (RBAC) model is investigated. it confirms the use of OWL not as a web ontology language but also for expressing authorization policies. Two different ways are given to represent RBAC model in OWL. Emphasis is given on the need to develop parallel access control models and semantic web based policies languages to produce verifiable security properties for emerging open and dynamic environments. Roles are represented as classes and as attributes. when represented as classes queries are evaluated efficiently and reasoning can be done in DLL through subsumtion reasoning .in representation of role as attributes or values specification is simpler as compare d to class representation but DLL reasoner is unavailable to determine subsumption relationship between query and class of policy.

Finding17: RBAC Model can be represented in OWL either representing Role as classes or representing as attributes. ABAC can be modeled using OWL.

Finding18: XACML as a standard mechanism for authorization and policy language still have limitation of no considering the semantics of policies that are created although it do repreent ABAC and RBAC.

2.2.16 Design and Run Time Reasoning with RelBAC

RelBAC model is computed with its reasoning ability as a fact that RelBAC model as ER Diagram can easily convert to Description logic DL that is Rel based logic. Rel Based model is used and its applicability is shown to SFA scenario also ontologies were created in RDF/OWL to describe the scenario. The benefit of representing policies in RelBAC model is that we have the ability to reason about them .Run time reasoning and Design time reasoning are explained in context of RelBAC. Design time reasoning support policy writer at design time to write policies also checks redundancy, conflicts and separation of duties SOD about policies. Run time decision applies for Access control decisions at run time and dynamic separation of duties. System Architecture for implementing RelBAC model is also given.

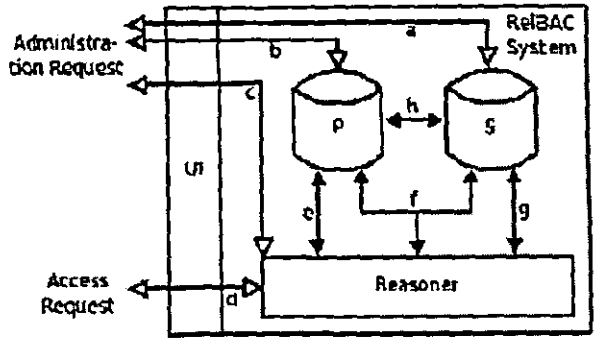


Figure 2-9: The System Architecture using RelBAC adapted from [19]

Finding19: RBAC Model Require a logical Framework for policy reasoning on top of it but RelBAC has its own description logic for reasoning purpose

2.2.17 Ontology-Based RBAC Specification for Interoperation in Distributed Environment

This paper proposes ontology specification to describe Role-based Access Control model. Ontologies are defined to describe the concepts and a declaration of rules to clear the relationship between concepts. The ontology based approach can express security policy with semantic information. It has benefit to provide a machine interpretation for descriptions of policy in open and distributed environment.

Both XACML and X-RBAC are based on XML; However, XML does not provide a machine interpretation of policy specification. Application domain has to agree on the meanings of terms. Machine interpretation for descriptions of security policy specification in distributed environment is very important for avoiding security vulnerabilities.

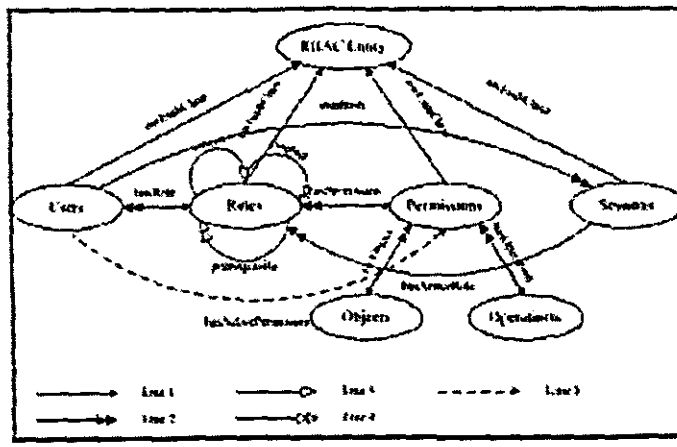


Figure 2-10: Ontology for RBAC model adapted from [20]

With RBAC, users associate with permissions through roles. Permissions must be authorized for roles, and roles must be authorized for users. A user assigned to a role can activate the role in a session and acquire all the permissions assigned to it.

The ontology for RBAC model is designed to help expressing concepts and relationships, and their formal meanings can be interpreted by machine. The classes Users, Roles, Permissions and Sessions are defined to express key concepts in RBAC, and several types of property are defined to describe relationships among them.

The ontology based approach of RBAC specification is the starting point to achieve semantic interoperability among the different components of access control systems in open distributed environment.

Finding20: Ontologies can be specified to represent RBAC Model It has benefit to provide machine interpretation for descriptions of policy in open and distributed environment

2.2.18 SBAC: "A Semantic–Based Access Control Model"

Semantic Web aims at automation, integration and reuse of data among different Web applications. Semantic Web applications create new requirements for the access control models Access to resources can not be controlled in a safe way unless the access decision consider the semantic relationships among entities in the data model. Decision for access control by assuming entities in isolation and not considering their interrelations results in security violations.

In this paper, Semantic Based Access Control model (SBAC) is proposed. SBAC considers semantic relations among entities in all domains of access control, e.g. subject domain, object domain and action domain. To facilitate the propagation of policies in these three domains, semantic interrelations can be reduced to the subsumption problem reducing the space and time complexity of the access control mechanisms which are based on SBAC.

Ontologies are used for modeling the entities along with their semantic interrelations in three domains of access control, namely subject, object and action domain. Decision

making in SBAC for granting or denying an access request is automated by inference processes according to the semantic relation among entities. Based on the OWL ontology language, it is shown how semantic interrelations can be effective in the authorization process; and for enhancing the expressiveness of authorization rules defined in SBAC, rule languages like SWRL can also be applied.

Future access control systems like client based access control systems work with undecidable but more expressive logics than Description Logic under OWL.

SBAC makes its decisions on three domains: Subject, Object and Action. SBAC consists of three basic components: Ontology Base, Authorization Base and Operations. Ontology Base is a set of ontologies: Subject-Ontology (SO), Object-Ontology (OO) and Action-Ontology (AO).Authorization Base is a set of authorization rules in the form of (s, o,±a) in which s is an entity in SO, o is an entity defined in OO, and a is an action defined in AO. Predefined access rights can be saved in Authorization Base in the form of authorization rules for making decision for incoming requests. Inference is done based on the semantic relationships between the requested authorization and the explicit authorization rules in Authorization Base.

Finding21: Future access control systems e.g. web2.0 access control models can use semantic based access control concept and Logic under OWL [self generated]

Finding22: Semantic web languages e.g. OWL are not more expressive so more expressive language SWRL can be used but it can't be done automatically at machine level and require reasoning that human can provide in form of rules.

Finding Table Extracted from literature survey

Table 2-1: "Findings" from Literature

Finding	Text	Reference
1	Fine grain and richer access control semantics related to policy representation. Can be done with ABAC model.	[5]
2	XACML provides the means for resource owner to express complex access control policies also allows standard evaluation of access control requests across heterogeneous resources and external subjects in web services	[8]
3	Access control rules can be representing in more expressive language like XACML. concept of content based access control can be used to develop fine grain access control model	[9]
4	Security policies for access control can use security standards like XACML In Backend And Express simple semantic description of these using tag based approach.	[4]
5	security policies for access control can be expressed in OWL and SWRL, FOAF is used for user to be a friend according to the information of the Web site's or resource's owner to form a basis for an interoperable security architecture	[4]
6	user defined relationships and content categorization concept is used to built social network using subject ,object ,and permissions giving to users based on the content categorization	[3]
7	RelBAC can be viewed as some enhanced RBAC. RelBAC models permissions as ER relations and allowing for logic aware access control policies and policies reasoning done with Description logic. These points are needed for addressing the complication of the Web open, highly dynamic applications	[12]

Finding	Text	Reference
10	There is a need for expressive language for fine grain access control. We can write policies using XACML defined functions and also it's extended functionality Social network members should made fine grain access control policies in order to satisfy their needs	[11]
11	In face book simple access control related to profiles is given, with given contact information we are not able to view information by friends of particular	[11]
12	XACML like standard language is essential but it is just a way to write policies and rules. How we can use the access control models model within these existing access control languages? RBAC profile of XACML expresses a way to use the standard XACML access language within the RBAC model	[15]
13	Face book restrict information availability to specified networks ,Face book users are still unable to define their own relationships that is user centered relationship groups	[1]
14	RDF metadata can be used specify and enforce access control policies in Web- based environment as RDF is flexible and can be integrated in a semantic web context.	[16]
15	XACML model can be used in providing privacy and trust that is gradually incremented using bilateral exchange of policies protecting resources, policies and credentials in distributed environment.	[17]
16	Ontologies can be used to provide transparent and machine interpretable language and result of ontologies can be transformed in to XACML standards mechanism	[18]

17	RBAC Model can be represented in OWL either representing Role as classes or representing as attributes. ABAC can be Modeled using OWL.	[19]
18	XACML as a standard mechanism for authorization and policy language still have limitation of no considering the semantics of policies that are created although it do represent ABAC and RBAC.	[19]
19	RBAC Model Require a logical Framework for policy reasoning on top of it but RelBAC has its own description logic for reasoning purpose. RelBAC can be represented in Ontologies.	[20]
20	Ontologies can be specified to represent RBAC Model. It has benefit to provide machine interpretation for descriptions of policy in open and distributed environment.	[20]
21	Future access control systems e.g. web2.0 access control models can use semantic based access control concept and Logic under OWL [self generated].	[20]
22	Semantic web languages e.g. OWL are not more expressive so more expressive language SWRL can be used but it can't be done automatically at machine level and require reasoning that human can provide in form of rules.	[21]

2.3 Limitations

2.3.1 Attribute based access control model

Attribute based access control model is not refined enough to satisfy requirements of today's web environment e.g. Relation Based, Interoperability .when Access control language is used to represent model access control decision is carried on basis of subject ,object attributes but how machine interpret them means semantic interoperability is not present[5,19].

2.3.2 XACML based access control model

XACML model shows its applicability on a scenario but no implementation is given although solidify use of XACML for web services scenarios [8]. XACML based models do provide interoperability and standard mechanism for evaluation of access control policies but fails if its satisfiability for web2.0 access control environments is investigated [Table 2].

2.3.3 XACML/ SAML based access control model

XACML/SAML based models are interoperable. XACML/SAML based models fit well for previous web services requirements but for today's web demands some special need as users and also contents are not like before.

2.3.4 Access control mechanisms in Web based social networks WBSN

It can be seen that access control mechanism of WBSN is not interoperable and fine grain. Policies creation is not content or data dependent .they use authorization based model to grant access to resources to user some new access control models e.g. RelBAC model if used then have the inherent ability of reasoning about access control policies at run time as they use N3 that is an RDF based compliant language having advantage of integrating it in Cwm reasoner [9,12]

2.3.5 An access control mechanism for online social network OSN

As to give fine grained access control feel this approach fail to give any solid solution in this direction just help us to think this type of solutions but should have ground reasons for using any particle approach as they are not comparable to standard. Access control mechanism. OSN is not interoperable and polices are also not content dependent because user can define relations that are eligible to view image other users not in these relations are not eligible to view the image .

2.3.6 Milestones based architecture for Web 2.0 Security

It does give some ideas of how to handle identity management on social web, trust assurance. Security and access control is handled by giving idea of relating these to semantic description. Some real world scenarios are also given. But its interoperable architecture still lack implementation.

2.3.7 Privacy Enhanced Access Control Model for web3.0

Although this paper give a view of using user defined relationships and content categorization concept but propose model is not supported with the help of scenarios [3] ,also not supported with the help of any implementation they just give their idea how to manage relationship and formal definition of access control model is also not given[14].

Their model still lack interoperability because not adopting standard policy creating and access control language e.g. XACML.

2.3.8 RelBAC: Relation Based Access Control Model

Author gives an idea of introducing permissions between subject and object as binary Relations. Model is given at introductory level how to apply it to dynamic web 2.0 scenarios is not described. Reasoning about policies at runtime and design time is not introduced just tell that RelBAC model have the advantage of having DLL reasoning and not need to introduce separate logical frame work above core RBAC model. [12, 20]

2.3.9 Approach to integration of policy based and reputation based approaches

Although the concept is applied to an e business scenario to show its applicability as such no formal representation model is given like we have in RBAC and RelBAC models.

2.3.10 BAC: Content- Based Access Control Model

CBAC system seems to be effectively solve the fine grain access control requirement and ease of policy creator to apply same policy to categorized objects but techniques used for this purpose still have some issues to their applicability. CBAC model still lack interoperability

CBAC alone do not provide effective solution for web.2.0 scenario's there should be a system that be interoperatible keeping in mind relation between subject and objects participating in access decisions although suit to some web applications that do not have excessive content s and where content management is not a big problem. CBAC [14]

2.3.11 XACML: need in Web based social networks WBSN

There are no relations and policies are not created by keeping in mind contents or data so fails to satisfy relationship based and sticky policies requirements of web2.0 access control [Table2].

2.3.12 Extended RBAC profile of XACML

Extended RBAC profile of XACML do solve some problem in terms of contextual and constrained extension but there is still need further extension if one want to investigate its suitability in web 2.0 environment e.g. relationship concept used in most of OSN is not present also semantic Description of policies is also not handled wit any mechanism only context is not broad enough to satisfy [10, 21].

2.4 Summary

Different access control models are deeply investigated in literature survey some of these are XACML based, Role based, Attribute based, Relation Based, Semantic Based access control Model etc.

XACML based access control models for web service successfully uses it in order to make interoperable access models across different domains. Use of XACML as a standard access control mechanism and policy creating environment is reported in literature.

Next different Access control models for new web 2.0 scenarios some attempt to satisfy web2.0 requirements in form as some user defined relations and content based access was given some research work emphasize on the use semantic web as mean to make access control models machine interpretable and to give meaning to access control policies .there is also work toward generating ontologies and then convert them in to XACML policies but they use them to their respective requirement of their scenarios not for web2.0 . Finding table is generated on the basis of findings obtained from literature survey generated finding table have all findings some of them in summarize way are described here but more can be find in a precise and compact form in finding table.

Some main limitations in previous research work are that all interoperable web based access control models lack mechanisms for providing new web 2.0 requirements as Relation based semantic interoperability are among some of them. Moreover policies are not created keeping in mind specific contents as like in CBAC but it have its own limitation in using Artificial intelligence techniques for content categorization.

Chapter 3

REQUIREMENT ANALYSIS

3 REQUIREMENT ANALYSIS

3.1 Introduction

In order to perform requirement analysis first of all a deep understanding of underlying web 2.0 technologies/applications is needed. The reason why there is need of investigation if one wants to introduce web services standards for access control like XACML is that web 2.0 due to its dynamic nature not only demands some special requirements but also most of its applications to the best of our knowledge are not under standard access control mechanisms or models.

We will investigate all requirements reported in [1] in previous web services and web2.0 related work also keeping in minds our own perspective and requirements about access control and authorization in web 2.0 scenarios.

3.1.1 Web 2.0: Technologies and Environment

Web 2.0 sites encourage user generated contents in form of text video photo posting along with tags comment and ratings. Strong social component e.g. user profiles, friend links web based social networks are incorporated in web 2.0

Web 2.0 sites based on particular set of technologies such as Ajax stands for Asynchronous JavaScript and XML act as a mixture of several technologies used to integrate web page presentation, interactive data exchange between client and server side take place.

IFRME is a programming technique allows additional contents to be embedded in web page. Are often used to display banner ads or information from different sites on a single page.

RSS Really simple syndication, user gets updates automatically from web site whenever changes occur in web site. Its uses include news reports, weather reports, and blogs on social networking sites like Face book.

Flash objects also offer similar functionality that is after download they can communicate asynchronously with server. e.g. in case of you tube user download flash object it download small prefix of video and start playing it while asynchronously loading the remainder of the video.[web 2 create sec challenge, understand web 2]

3.1.2 Web2.0: lacks standard Access control Mechanisms

Web 2.0 applications include most of social networking sites (e.g. Orkut and Face book), photo-sharing sites (e.g. Flickr and SmugMug), and video sharing sites (e.g. YouTube and Google Video) have a look at their under laying access control features or models all fall under following categories.

Private/public. Access control systems support private and public objects.

Friends. Private/public scheme is added with a feature that users create a list of "Friends." User can restrict some of his or her content to be visible only to friends. Face book automate the process through invitations to friends The Orkut social network introduce some level of trust among its users by requiring new users to have an invitation from an existing user.

Password-protected Posts. SmugMug and WordPress allow users to create password-protected posts. Although extremely flexible access control policies are possible but, user have to manage the access control policies.

Mostly adopted is friends model because it is flexible in terms of ease of use and les complicated or easy to manage by non technical user but it is not suited if we Talk about

Having some mechanism to judge friendship by trust level parameter although some sites do some work towards this direction but not noticeably enough [14].

Friend's model fails to provide fine grain access control both in terms of Relationships and fine granularity of access control mechanism. as user have to rely on his pre defined list of friends user is not able to introduce his own defined relation ships. for users personal objects like photos, videos, posts are not protected by fine grain access control policies.

Traditional access control models for Web Services e.g. Role Based Access control Model (RBAC) ,Attribute Based Access control Model ABAC,XACML, were not created by keeping in mind web 2.0 Access control Requirements.

3.1.3 Web2.0: New security requirements

Web 2.0 access control requirements are not fully addressed As most of mechanisms related to Access control and authorization were developed by keeping in mind traditional Web services having pre-defined set of users and also data or resources on web were not such that to be generated dynamically.

Web 2.0 systems are open and it is not possible to predict about user, data at design time also policies created need to be reason about at run time [15]

New challenging requirements include some Relationship based access control as some of social networking sites deals heavily with Relationship concept like friends, Real Relationships etc Policies created for Access control are not fine grained. Due to large amount of user generated data there is need for some kind of content management system or some access control mechanism based on content categorization. Models should be interoperable among different sites there should be some standard interoperable mechanisms for access control in web 2.0.Semantically descriptive models to address the need of relationships and also web contents should be arranged with the help of contents semantic meanings.

3.1.4 Where problem exists

??????????????

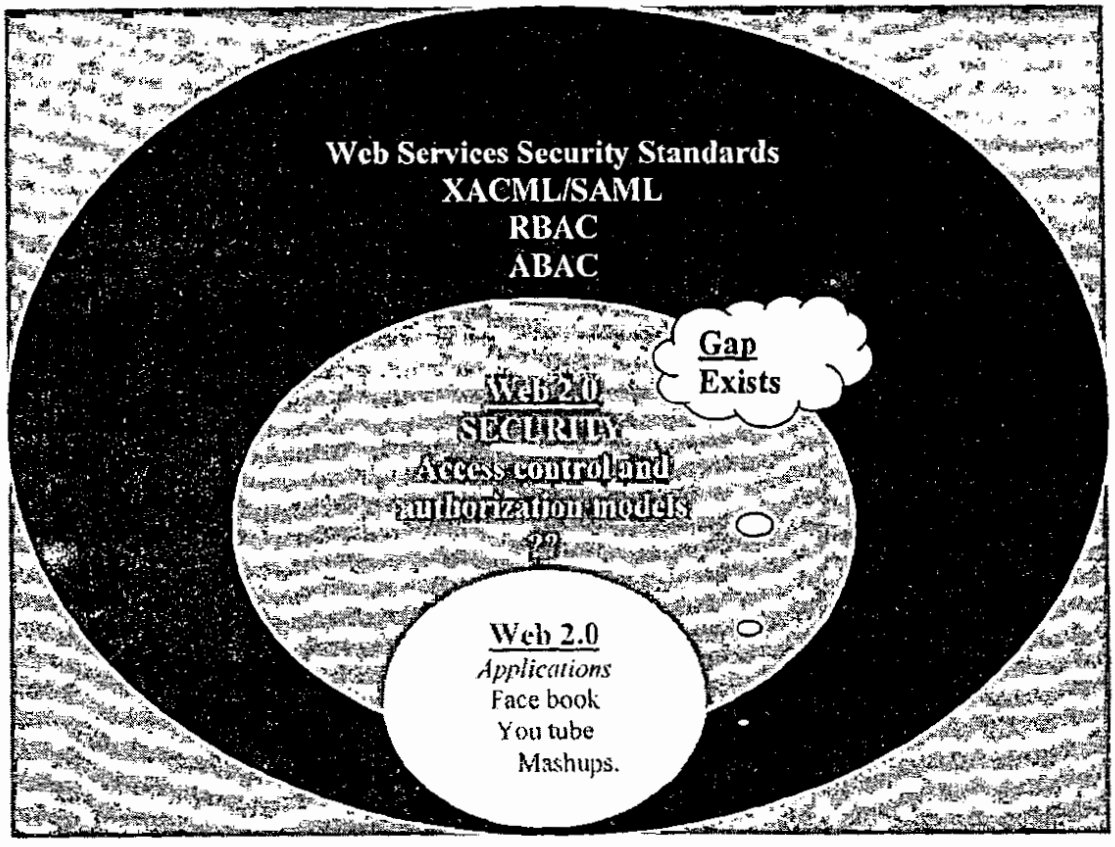


Figure 3-1: Problem description in Web services and Web 2.0 context

3.2 Requirement Analysis with critical Problem Scenarios

3.2.1 Role based access control model

Role based access control model mainly deals with Roles access control permissions are assigned to roles and roles are assigned to users but in web 2.0 environment as users roles, identities are not pre-defined same as with the access objects as not fixed and pre-defined .So in traditional Organizations scenario RBAC work well but RBAC as it is not satisfying Web 2.0 Access control requirements.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Role based access control model	partially satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied

3.2.2 Attribute based access control model

Attribute based access control model is not refined enough to satisfy requirements of today's web environment. ABAC although fine grained but it lacks semantic interoperability and also policies are not created by keeping in mind contents that is sticky policies are not created. ABAC

Is not relationship based there is no concept like this as it concentrate more towards attributes of involved entities.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Attribute based access control model [5]	Not Satisfied	Satisfied	Not Satisfied	Partially Satisfied	Not Satisfied

3.2.3 *XACML based access control models*

XACML model shows its applicability on web services scenarios XACML based models do provide *interoperability* but fails to satisfy other web2.0 access control requirements. XACML have strong policy language and access control or authorization mechanism but certain special requirements e.g. Relation based, Content based, semantic interoperability demands its extension to accommodate the new scenarios need.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
XACML-based Access Control Model [8]	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied

3.2.4 XACML/ SAML based access control model

It does provide some hint how we can use it in advanced web 2.0 scenarios involving authentication and access control. XACML/SAML based models do provide interoperability but fails to satisfy other web2.0 access control requirements.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
XACML/ SAML based access control model [7]	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied

3.2.5 Access control mechanisms in Web based social networks WBSN

It can be easily seen that except relation ship based requirement no other is satisfied because access control mechanism of WBSN is not interoperable and fine grain. Policies creation is not content or data dependent

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Enforcing Access Control in Web-based social networks[9]	Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied

3.2.6 An access control mechanism for online social network OSN

OSN is not interoperable and polices are also not content dependent because user define relation that can view image other users not in these relation are not eligible to view the image .

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Attribute based access control model [5]	Not Satisfied	Satisfied	Not Satisfied	Partially Satisfied	Not Satisfied

3.2.7 Milestones based architecture for Web 2.0 Security

Security and access control is handled by relating these to semantic description. Relationship based and fine grained access control requirements are not satisfied as it use

concept of already established web service security standards semantic interoperability aspect is not full adopted as specific ontologies are not created [11,12, 21]

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Milestones based architecture for Web 2.0 [4]	Not Satisfied	Not Satisfied	Satisfied	Satisfied	Not Satisfied

3.2.8 Privacy Enhanced Access Control Model for web3.0

Their model still lack interoperability because not adopting standard policy creating and access control language e.g. XACML also semantic interpretation of policies is not handled in their architecture they try to extend social network with the help of user defined relationships.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Privacy Enhanced Access Control Model for web3.0[3]	Satisfied	Satisfied	Not Satisfied	Satisfied	Not Satisfied

3.2.9 RelBAC: Relation Based Access Control Model

RelBAC model is developed by keeping in mind web 2.0' special dynamic security requirements but still it's not semantically descriptive. Policies are not specifically created by keeping in mind contents or objects involved in access scenario.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
RelBAC: Relation Based Access Control Mode l [12]	Satisfied	Satisfied	Not Satisfied	Not Satisfied	Not Satisfied

3.2.10 CBAC: Content- Based Access Control Model

Although CBAC system seems to be effectively solve the fine grain access control requirement but its policies are nit semantically descriptive and CBAC model is interoperable as like XACML like models.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
CBAC: Content-Based Access Control Model [14]	Partially Satisfied	Satisfied	Not Satisfied	Satisfied	Not Satisfied

3.2.11 XACML: need in Web based social networks WBSN

There is no relations concept in XACML and policies are not created by keeping in mind contents or data. XACML is not inherently semantically descriptive.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Attribute based access control model [5]	Not Satisfied	Satisfied	Satisfied	Not Satisfied	Not Satisfied

3.2.12 Use of RDF metadata to specify and enforce access control policies

This approach introduce RDF metadata to specify access policies RDF meta data can be easily integrated in semantic web context .there is no way described how relation based fine grained policies are create.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Use of RDF metadata to specify and enforce access control policies	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Satisfied

3.2.13 Privacy Preserving Trust Authorization Framework Using XACML

XACML is used in building model for trust based authorization model except interoperability no other requirement is fulfilled if we investigate in web 2.0 scenario.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Privacy Preserving Trust Authorization Framework Using XACML	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied

3.2.14 Enforcing Privacy by Means of an Ontology Driven XACML Framework

Architecture is not fine grained and policies created deal with specific domain not object centric.Ontologies created so they satisfy semantic interoperability requirement of web 2.0.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Enforcing Privacy by Means of an Ontology Driven XACML Framework	Not Satisfied	Not Satisfied	Satisfie5 6 d	Not Satisfied	Satisfied

3.2.15 OWLBAC - Representing Role Based Access Control in OWL

Except semantic requirement no other web 2.0 requirement is satisfied.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
ROWLBAC - Representing Role Based Access Control in OWL	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Satisfied

3.2.16 Ontology-Based RBAC Specification for Interoperation in Distributed Environment

Semantic Description requirement is satisfied but lot of work needed towards fulfillment of other s like fine grained, relation based etc.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
Ontology-Based RBAC Specification for Interoperation in Distributed Environment	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Satisfied

3.2.17 SBAC: "A Semantic–Based Access Control Model

SBAC focus mainly on semantic interpretation of policies with the help of SBAC model but it is not Interoperability, Relationship-based etc. so in order to develop a model that is semantically descriptive at he same time inter operable and relation based need addition of some web2.0 specific needs.

Referenced paper	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description
SBAC: "A Semantic–Based Access Control Model"	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied	Satisfied

Table 3-1Evaluation Table of existing Access control models /Technologies on basis of Web 2.0 Access control Requirements

Referenced papers	Requirement 1 Relationship-based	Requirement 2 Fine-grained	Requirement 3 Interoperability	Requirement 4 Sticky policies	Requirement 5 Semantic Description	Evaluation Column
Attribute based access control model [5]	Not Satisfied	Satisfied	Not Satisfied	Partially Satisfied	Not Satisfied	
XACML/ SAML based access control model [7]	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied	
XACML-based Access Control Model [8]	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied	
Enforcing Access Control in Web-based social networks[9]	Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	
Using Subject- and Object-specific Attributes for Access Control in Web-based K MS [16]	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Satisfied	
Privacy Preserving Trust Authorization Framework Using XACML	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied	
Enforcing Privacy by Means of an Ontology Driven XACML Framework	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Satisfied	
ROWLBAC - Representing Role Based Access Control in OWL	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Satisfied	
Ontology-Based RBAC Specification for Interoperation in Distributed Environment	Not Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	Satisfied	
Fine Grained Access Control in Online Social networks[10]	Satisfied	Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	
On the need for user-defined fine grained access control [11]	Not Satisfied	Satisfied	Satisfied	Not Satisfied	Not Satisfied	
RelBAC: Relation Based Access Control Mode l [12]	Satisfied	Satisfied	Not Satisfied	Not Satisfied	Not Satisfied	
Milestones based architecture for Web 2.0 [4]	Not Satisfied	Not Satisfied	Satisfied	Satisfied	Not Satisfied	
Use of RDF metadata to specify and enforce access control policies	Not Satisfied	Not Satisfied	Satisfied	Not Satisfied	Satisfied	
SBAC: "A Semantic–Based Access Control Model"	Not Satisfied	Satisfied	Not Satisfied	Not Satisfied	Satisfied	
Privacy Enhanced Access Control Model for web3.0[3]	Satisfied	Satisfied	Not Satisfied	Satisfied	Not Satisfied	
Design and Run Time Reasoning with RelBAC	Satisfied	Satisfied	Not Satisfied	Partially Satisfied	Not Satisfied	
CBAC: Content- Based Access Control Model [14]	Partially Satisfied	Satisfied	Not Satisfied	Satisfied	Not Satisfied	

3.3 Summary

Requirement analysis is carried up on existing and previous Access control mechanisms. Main aim of requirement analysis in our work is to find exact status of most of existing Access control models either they satisfy all web2.0 access control requirements or not. After analysis an Evaluation table is generated. Evaluation table will help us if we want to know quickly what are the web 2.0 access control requirements still not satisfied by existing models.

All existing web2.0 access control models are not adopting interoperability and semantic description although some have fine grained access control to some extent. As Rel BAC is developed specifically for web 2.0 scenarios so except it no other models are Relation based .Content are in large amount in number and un predictable as they are changed dynamically at web 2.0, if it is said that access control policies should follow the contents then except Content based access control no other model is developed keeping it in mind except one or two.

The requirement analyses will emphasis at requirement those need to be in access control mechanisms of web2.0 but most of existing models are not emphasizing on them. Some of the main requirements will act so as input to our access control model as main design requirements.

Chapter 4

SYSTEM DESIGN

4 SYSTEM DESIGN

4.1 Introduction

In this chapter proposed Model with its details are given. In order to develop Access control model an investigative process is adopted. Form extensive literature survey gaps were identified between web services security standard for access control and authorization (XACML) and open and dynamic nature of today's web2.0.As a result of literature survey finding table is developed its main aim of construction is to support our model with valid issues that arise as a result of finding table. Support of finding were required is given in explaining the design requirements

Chapter organization is given below.

Section 4.2 Describe in detail the Design requirements obtained after Requirement analysis phase and are named as Interoperability, Fine grained, Semantic Description, Relation Based and Sticky Policies. At the end of section design requirement with it s supported concept is given in tabular form.

In Section 4.3 proposed architecture is given it is divided in to subsections 4.3.1 describe flow diagram of proposed architecture then in 4.3.2 Main architecture diagram with its flow descriptions given.4.3.3 describe in detail architectural components. Section 4.5 gives summary of whole design architecture.

4.2 Design Requirements

Design requirements are explained below in detail in order to increase the understandability of the proposed Architecture.

4.2.1 INTEROPERABILITY

Interoperability is one of the main design requirements in creating architecture for web2.0 access control and authorization. Proposed architecture should be interoperable across different domains, so that without the need of redeveloping model for different domains one standard model use for solving access control and authorization problems related to web 2.0.so standard XACML architecture and policy language is extended to fulfill new web 2.0 scenarios requirements

- XACML is a standard for access control and authorization systems. Most of the current systems implement access control and authorization in application-specific manner .XACML Provide a standard and interoperable model and policy language.
- XACML: Benefits over other access control policy languages
- One standard access control policy language replaces many application-specific languages.
- XACML inherits all XML benefits; particularly it is vendor and platform independent.
- XACML is flexible enough to accommodate most access control policy needs and it is extensible So that new requirements can be supported.
- One XACML policy can cover many resources so prevent inconsistent policies on different resources.

XACML: data flow and key components

A typical XACML scenario is given with data flow as well as the key components involved in a XACML exchange.

e.g XACML: data flow and key components

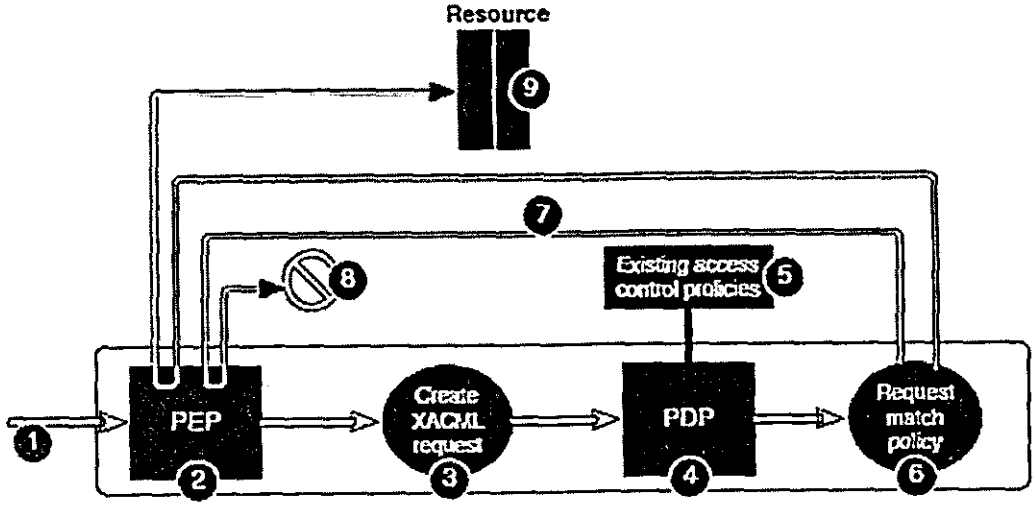


Figure 4-1: XACML Key components and data flow diagram adapted from [23]

Step 1 A user request access to a specific network resource e.g. a file system, database Or web service.

Step 2 The request goes to the entity Policy Enforcement Point (PEP). PEP is defined as a system entity that performs access control, by making decision requests and enforcing authorization decisions.

Step 3 The PEP uses the XACML request language to create a request based on the user, Action and the resource.

Step 4 PEP sends this request to a Policy Decision Point (PDP). A PDP is an entity That accepts XACML access requests and evaluates them against one or more Policies to produce an access decision.

Step 5 The PDP retrieves applicable policies from a policy store also called Policy Administration Point (PAP). A PAP is the system entity that creates a policy or a collection of policies.

Step 6 The PDP compares the request against policies retrieved in step 5, and determines Whether access should be granted or denied.

Step 7 The decision is sent back to the PEP. The Decision is usually either "Permit" or "Deny".

Step 8 If the decision is deny, The PEP denies the user access to the resource.

Step 9 If the answer is permit, the user is granted access to the resource [23].

4.2.2 FINE-GRAINED

There is a need for expressive language for fine grain access control in web 2.0. We can write policies using XACML defined functions and also it's extended functionality. But it has its own limitations [finding 3].Social network members should made fine grain access control policies in order to satisfy their needs

Finding 10: social network members should made fine grain access control policies that meet their specific needs. There is a need for expressive language for fine grain access

control. We can write policies using XACML defined functions and also it's extended functionality

Its side effect is complexity, policy creation language should be expressive but the users of social networking site are all not so trained to understand the complex mathematical logic while representing its needs for creating access control policies[9,11]

4.2.3 SEMANTIC DESCRIPTION

Semantic Web is the extension of current Web which gives information a well defined meaning capable of interpreting and processing the information. A semantic aware access control mechanism should assure that only eligible users are authorized to be granted an access right and each eligible user must be able to access all the resources that s/he is authorized for.

Traditional access control models like MAC, DAC and RBAC, ABAC, RelBAC fail to address these issues since they do not consider the rich semantic relations in the data model under Semantic Web. Decision is made based on isolated entities while ignoring the semantic interrelationships among them results in illegal inferences by unauthorized users and incomplete grant of access rights.

In semantic web ontologies are created to make the isolate entities understandable. Ontologies are used significantly in different access control models e.g. RBAC, ABAC. At the same time use of XACML is also reported so as we can convert ontologies generated policies in to XACML context [Findings: 16, 17, 18, 20, 21].

To overcome these challenges, there is a need for semantic aware access control systems consistent with the semantic data model under the Semantic Web.

4.2.4 STICKY POLICIES

Policies created for access control should be such that when created follow the data or Objects In access control terminology. Access control policies should be created based on contents.

In web 2.0 application majority of contents are in form of text, videos, and photos so it is the contents that are more important in access control environment.

Content based access control CBAC follow the concept of categorizing the contents before access decision or during policy creation but CBAC can also use manual access control. But even in this case, CBAC can help users mediate access by aggregating similar content to reduce overhead involved without categorizing the contents.

Content-Based Access Control is based on the convergence of different technologies, such as text summarization and machine vision, and inherits their weaknesses and is not perfect in terms of precisely identifying features or classifying content [14]

So in order to use CBAC concept should be used such that gain benefit from content categorization concept with out involving in complex artificial intelligence techniques

Sr#	DESIGN REQUIREMENT	CONCEPTS USED IN PROPOSED MODEL
1	Interoperability	XACML
2	Fine-grained	XACML+RelBAC
3	Semantic Description	SBAC
4	Relationship-based	RelBAC
5	Sticky policies	CBAC

Table 4-1Concepts used in Proposed Model

4.3 Reference Architecture

4.3.1 General Flow Diagram for Proposed Authorization model in Web 2.0

Main purpose of presenting flow diagram at start of proposed model is to provide ease of understanding whole mechanism of model at abstract level.

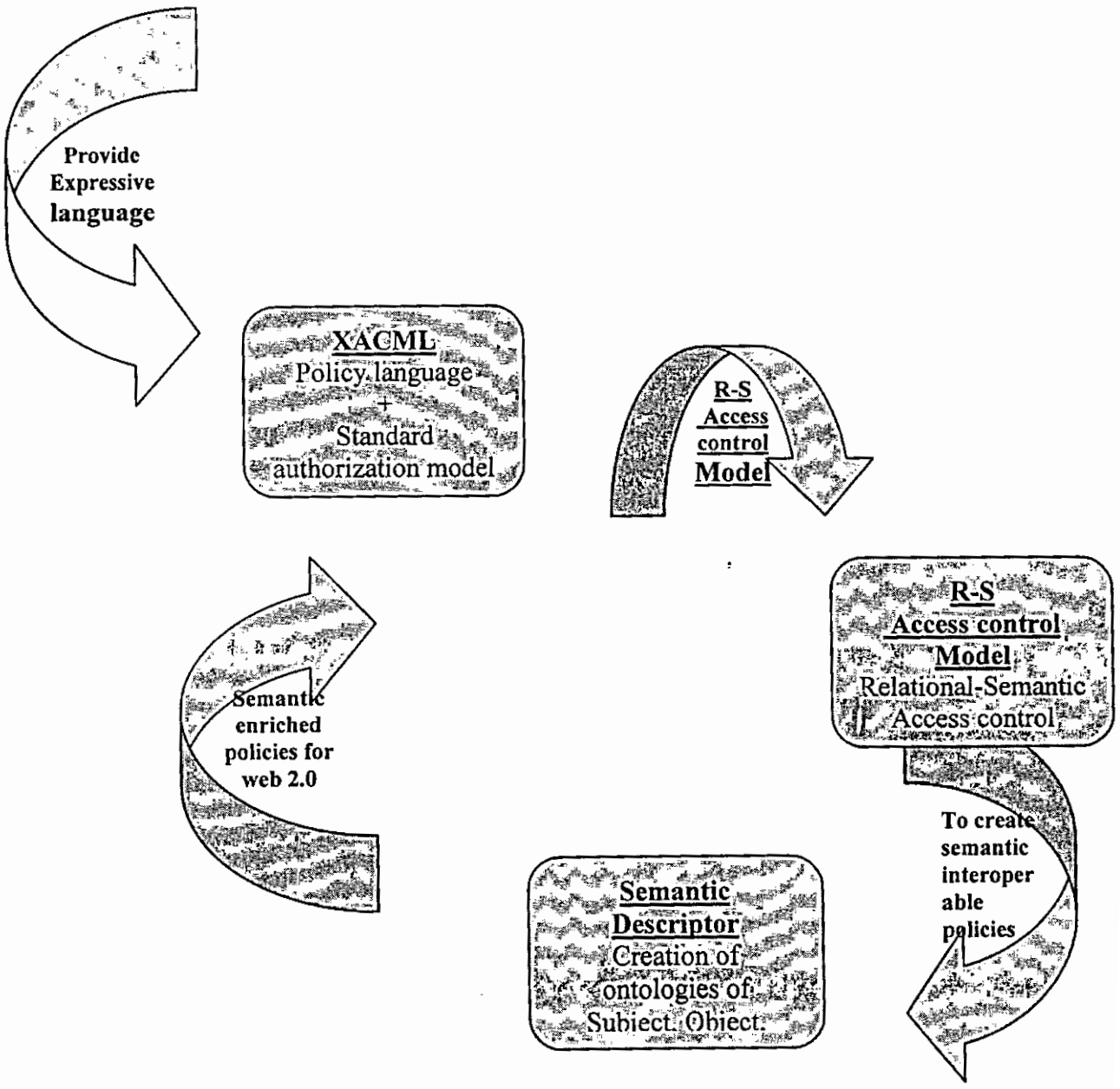


Figure 4-2: General Flow Diagram for Proposed Authorization model (RS-XACML BAC Model)

Flow Diagram: Detailed flow with explanation

- XACML is used for dual purposes in proposed model as it is a standard mechanism for authorization in addition to Expressive policy language construct.
- XACML is used here as standard interoperable model for authorization flow and final decision for authorization. As a Policy language its selection is limited due to lack of semantic meaning while making authorization decisions.
- As model for access control need language to represent so new model for authorization Rel-S BAC model is used as policy creation environment.
- Up to this point there is no semantic meaning exists among entities participating in access control so here in Semantic descriptor Ontologies are created in OWL for(Subject, Object, Operations) and inference is made through inference engine for authorization decisions
- Semantically enhanced policies are converted on to native XACML format and cycle continues in this manner for every request processing.

4.3.2 Relational-Semantic-XACML Based Access control Model for web2.0

RS-XACML BAC Model:

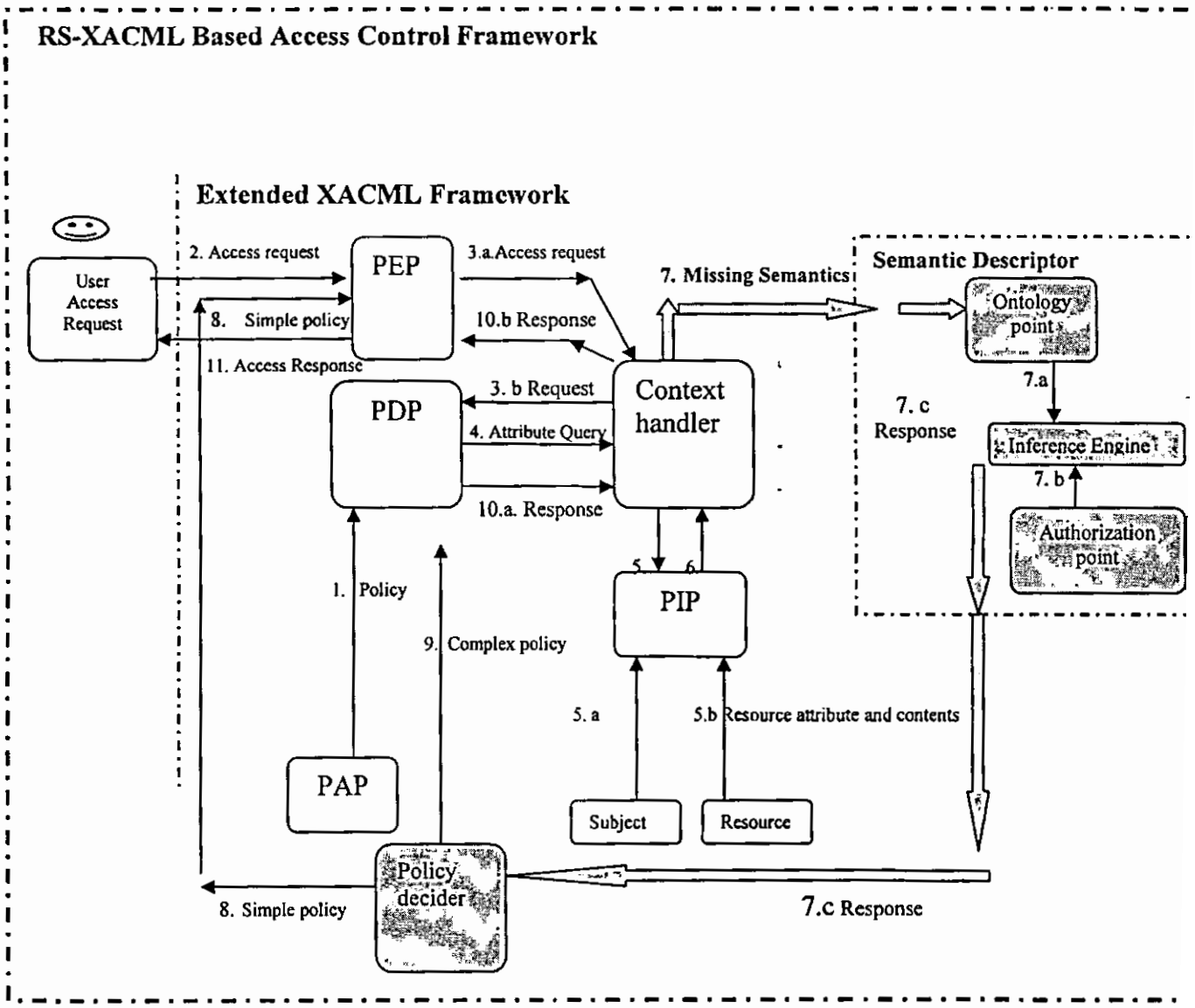


Figure 4-3: RS-XACML BAC Model

4.3.3 Relational-Semantic-XACML Based Access control Model for web2.0

4.3.3.1 Basic component flow: RS-XACML BAC Model

The architecture is depicted in fig.4.our extensions are emphasized using grey shading. An access control decision and enforcement is performed according to the following steps.

1.) The policy access point PAP provides XACML policy created by policy administrator and user as the owner of resource e.g. text, photos, videos etc, to the policy decision point PDP.

2.) The user sends a resource request to the policy enforcement point PEP.

3.) PEP forwards this request to the context handler and context handler create XACML request and send it to PDP.

4.) PDP requires additional subject and resource attribute so it send attribute query to the context handler.

5. Context handler requests those attributes from Policy information point PIP.

PIP collect attribute from subject and resource and send it to context handler.

6.) XACML lack semantic interpretation so at this point attributes semantic meaning and semantic inference is added with the help of semantic Descriptor.

7. a) from ontology point ontologies for subject Object, Permissions are created in OWL.

7. b) Authorization point has authorization rules Inference Engine make inference about access decision to grant access or not.

7. c) Response about access request is given to Policy decider.

8.) Policy decider in case of simple policy forward access decision that it receive from Semantic Descriptor to the PEP.

9.) Policy decider in case of complex policy sends decision to the PDP it Re- consider decision and make access decision according to complex policy requirement.

10) PDP gives its response to context handler that cover request in its native format.

10.a)Context handler sends its response to PEP

10.b) If access is allowed then PEP give access to resource Otherwise Access is denied.

4.3.4 Main component description: RS- XACML Based Access control Model

Main RS- XACML Based Access controls Model component s are given below.

- **Extended XACML Framework**
- **Semantic Descriptor**
- **Policy Decider**

4.3.4.1 Extended XACML Framework

XACML standard framework is extended with the help of semantic web technology in form of module introduced as Semantic Descriptor.

XACML is used here as standard access control and authorization Mechanism. RelBAC [12] is introducing at introductory level in it as we are introducing concept of relations among subject and object entities.

RelBAC logic

RelBAC has the following components.

SUBJECT (or USER): a subject is a user that requests an access to some resources. In XACML it is taken as subject.

OBJECT: an object is any resource of the system a user requests access. In XACML objects are expressed as Resources.

PERMISSION: PERMISSION is an operation that users can perform on objects. To capture this intuition PERMISSION is named with the name of the operation it refers to, e.g., Write, Read operation or some more high-level operation, e.g., Assign or Manage.

As in XACML based RBAC PERMISSIONS are associated with ROLES and ROLES are expressed using one or more Subject attributes so taking advantage of these we said that here in RelBAC we model PERMISSIONS in XACML as a Relation between Subject and Object or as a operation a subject want to do on object as a PERMISSION

RULE: associates PERMISSION to a specific set of (SUBJECT, OBJECT) pairs.

Membership

Similar to what RBAC does with roles, Adding or deleting an individual user from an existing subject group means only adding or deleting an assertion to or from the knowledge base .it is just as the assignment of a role in RBAC

Propagation

As in RBAC user assignments and permission assignments propagate through role hierarchy.

Membership Propagation

Different Relations such as IS-A, composed of, responsible for, etc. can form various hierarchies

The 'IS-A' relations can be represented as partial order '≥' in RelBAC to form the

Hierarchy not only among groups but among classes and permissions.

User membership propagation depends on group 'IS-A' hierarchy only. Given any two groups Ui; Uj such that Ui '≥' Uj and u is a member of Ui then the membership of u to Uj can be automatically implied.

.Permission Propagation

The permission propagation is more complex because in RelBAC permission is a binary relation that links a subject to an object. So it has three paths to propagate: 'IS-A' hierarchy of subjects, objects and permissions.

In addition to the group hierarchy which simulates the role hierarchy in RBAC model, RelBAC provides object class and permission hierarchy with partial order '≥' applied on classes and on permissions as '$O_i \sqsubseteq O_j$' and '$P_i \sqsubseteq P_j$'.

Permissions can propagate through the permission hierarchy as well. The partial order among permissions describes subsumption between sets of (u; o) pairs.

.The extent we apply RelBAC is at introductory level as detail concept in RelBAC e.g. Static and dynamic separation of duties SOD are not included as our emphasis is at giving conceptual Architecture here only in next level when we implement our architecture we will describe RelBAC in its full Capability .XACML is extended to here

as to include RelBAC at introductory level and semantic interoperability along with its inherent interoperability and authorization mechanism.

4.3.4.2 Semantic Descriptor

Main components are Ontology point, Inference Engine and Authorization point.

Concepts and detail representations are taken from [22].We use it as module to introduce semantic description in our XACML based Relational framework. In [22] it's described in more detail where emphasis is given toward development of Semantic based access control model not on its usage in dynamic scenarios like web2.0 as we are using it in our proposed architecture.

Ontology point

Ontologies are defined as in [22] $Ont = (C, T, \leq_C, \leq_T, R, A, \sigma_A, \sigma_R, \leq_A, \leq_R)$

"C is a set of concepts, $\leq_\sigma$ is the subsumption relation between concepts. The other semantic relations are presented by $\sigma_R : R \rightarrow C \times C$, $\leq_R$ shows the hierarchy among Object Properties,

Meaning one property is sub property of another property. T is a set of data types with a hierarchy of data types, $\leq_T$. Data Type Properties are presented by $\sigma_A : A \rightarrow C \times T$"

Ontology point creates subject object and action ontologies.

OO: is an Object Ontology for describing objects or resources. Objects are entities which are Accessed and/or modified. Object-Ontology Shows the structure in which the objects (Concepts, Individuals and Properties) are organized along with the semantic relationships among them.

SO: is the Subject Ontology where subjects or users are active entities which require Access to objects. Subjects are concepts or individuals in Subject-Ontology.

AO: Actions depend on the type of the actions that subjects or users aim to execute on An object or resource. All the ontologies can be represented in OWL due to its well defined structure that let machines automatically process the knowledge described in it.

Inference Engine

Inference is done based on semantic relation among entities in ontology point e.g. Subject Object and action. Semantic inference can be done on three levels in OWL based on fundamental structure: concept–level, individual–level and property–level where the semantic authorization flow can occur in each level or between different levels.

Concept-Concept (C-C): Inference can be between two concepts in ontology.

Concept-Individual (C-I): The authorization flow from the concept level to the individual level is usual since all the individuals are influenced by the access conditions enforced on the concept they belong to.

Individual-Individual (I-I): authorization flow include the 'same as' axiom states that two individuals are semantically equal, hence the access conditions on each of them should be applied equally.

Property-Concept (P-C): This semantic authorization flow occurs when an access right on a property is granted. A property is a set of ordered pairs of individuals where the first individual is in the domain and the latter is in the range of property. Any access right on a property can result in the same access right on the domain and range of the property.

Property-Property (P-P): Semantic relations between various properties can result in new properties needed for decision making but are not explicitly mentioned in the ontology.

Property-Individual (P-I): The semantic authorization flow from a property to its individuals is inevitable because all the individuals are influenced by the access conditions enforced on the property that they belong to.

Authorization Point

Authorization point includes explicit authorization rules. Oprs are the operations that can be performed on the Authorization point

$$AP = \{(s, o, +a \mid s \in SO \wedge o \in OO \wedge a \in AO\}$$

$$Oprs = (CA, Grant, Revoke)$$

Access rights are stored in Authorization Point AP in the form of Authorization rules where:

$$AP \subseteq S*O*A$$

The operations are executed on AP for making decision about a request, Granting an access right or revoking an access right the formal definition is

$$Oprs = (CA, Grant, Revoke)$$

CA(s,o,a) is a function of decision making such that

$$CA: S* O*A \rightarrow \{true, false\}$$

4.3.4.3 Policy Decider

It decides about policy as it is a simple one or complex. A policy is simple if it lack arithmetic comparison operators other wise it is a complex policy. In semantic languages like OWL we don't have expressive power in case of arithmetic comparisons operators [25].So here we need XACML policy help so as to cover the deficiency Simple policies are not evaluated by PDP in extended XACML framework as access decision is already made in semantic descriptor module. In case of complex policies PDP make decision about access request and policies are processed in XACML policy language if some arithmetic comparison or decision is needed.

4.4 Summary

In this chapter proposed RS- XACML Based Access control Model is given. the whole process of model development follow a systematic process of investigation starting from literature survey important findings were obtained for providing valid base for our proposed model.

The design requirements obtained from requirement analysis phase were taken as input to our proposed model. Design requirements interoperability semantic description Relation based are main requirements. XACML standard framework for access control is extended and its policy language is used to achieve interoperability and fine grained requirement of web2.0

Semantic interoperability is achieved through semantic web concepts for access control like SBAC model .Relation based access control concept is used in order to satisfy one of main requirement.

Proposed model is divided in to three main components namely Extended XACML framework, Semantic Descriptor, Policy decider. XACML standard model is extended in order to use it in web2.0 scenarios as it lack semantic description of access policies and decision so it is achieved through semantic descriptor module in it Ontology point create Ontologies for entities participating in access control like subject ,object ,actions .Inference for authorization rule stored in authorization point is done through inference engine. Policy decider decides about the nature of policies required for access control either simple or complex. Policy decider in case of simple policies forward it to PEP so as a final to convey the decision about resource as access is given or denied. In case of complex policies XACML expressive language is used to construct policy complex policy and PDP decide about it.

Chapter 5

CONCLUSION AND OUTLOOK

5 CONCLUSION AND OUTLOOK

5.1 Introduction

In this chapter some concluding remarks are given. Achievements in form of what we really succeed in doing. Improvements and Future work as what still need to be done as there is always some space exists for improvement in any research work.

5.2 Achievements

- In this thesis first we did an informative deep analysis of existing web2.0 Access control models and Traditional web service models for access control on basis of standard access control requirements that we investigate .we also add some useful one like semantic description in these requirements. Evaluation table is constructed that at itself do provide an overview of today's and traditional access control model in terms of web2.0 requirement satisfaction.
- On basis of Evaluation table we are able to find the exact situation as how many requirements of web2.0 Access control models are satisfying and what are those not satisfying.
- We did develop a conceptual framework for access control and authorization in web2.0. Our model has the maximum support for web2.0 requirements as compared to existing and traditional models for access control.
- XACML is investigated in order to find how it can be used in new and dynamic paradigm of web2.0 as XACML has strong basis for providing interoperability and fine grained access control policies. We also extend XACML model to make it semantically interoperable and use Rel BAC model that is specifically developed for web 2.0 inside XACML standard model.

Our s is first model for access control and authorization in web 2.0 to the best of our knowledge that is XACML based so inherit its interoperable, fine-grained policy representation and standard mechanism for access control. It is made semantically descriptive with the help of Semantic web Technologies.

5.3 Future Recommendations and improvements

- A conceptual framework for Access control in web 2.0 is developed in this thesis. We plan to implement proposed framework in next step and test it at mostly used web2.0 site like face book to the best off our knowledge it is not adopting any standard mechanism for access control.
- XACML is extended to make it semantically interoperable but we can also use it as policy representation and authorization mechanism to represent new Access control model means that to develop new one instead of using RelBAC or SBAC access control models although these like RelBAC are newly developed and not used till now in any access control standard authorization model.
- Semantic web technologies like SWRL instead of OWL can be used inside access control model to make more expressive access control policies but it also has its own disadvantages. [Finding 22.[22]].
- RDF metadata can be used specify and enforce access control policies in Web-based environment as RDF is flexible and can be integrated in a semantic web context.[finding 14. [16]].

References

6 REFERENCES

[1] C. E. Gates, Access Control Requirements for Web 2.0 Security and Privacy, Proc. of Workshop on Web 2.0 Security & Privacy (W2SP 2007), Oakland, California, 2007.

[2] G. Cormode and B. Krishnamurthy. Key differences between web 1.0 and web 2.0.at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/ar ticle/view/2125/1972 , June 2008.

[3] E. Choi, An Approach to Privacy Enhancement for Access Control Model in web3.0. Proc. 3rd IEEE Conf. on Convergence and Hybrid Information Technology, Busan , Korea 2008, 1046-1051.

[4] M. Quasthoff, H. Sack, C. Meinel, Who Reads and Writes the Social Web? A Security Architecture for Web 2.0 Applications. Proc. 3rd IEEE Conf. on Internet and Web Applications and Services, Athens, 2008, 576-582.

[5] E. Yuan and J. Tong. Attribute based access control (ABAC) for web services. Proc .of the 3rd IEEE Conf. on Web Services, Orlando, Florida, 2005. 569

[6] P. A. Bonatti, C. Duma, D. Olmedilla, and N. Shahmehri.An integration of reputation-based and policybased trust management.Proc.4th International conf.on Semantic Web and Policy Workshop, Galway, Ireland, 2005.

[7] Hao Yin1,Jiliu Zhou1, Huilin Wu Liang Yu1, A SAML/XACML based Access Control between Portal and Web Services. Proc. 1st IEEE Symposium. On Data,Privacy and E-Commerce, Chengdu, China, 2007, 356-360

[8] Tao, H,A XACML-based Access Control Model for webService.Proc.IEEEConfon Wireless Communications, Networking and Mobile Computing, Wuhan, China ,2005,1140- 1144.

[9] Barbara Carminati, Elena Ferrari, Andrea Perego, Enforcing Access Control in Web-based Social Networks, Technical Report, 2007

[10] Amin Tootoonchian, Geoffrey Salmon, Ahmad Ziad Hatahet ,fine Grained Access Control in Online Social Networks,2007.

[11] Andrew Simpson, on the need for user-defined fine grained access control policies for social networking applications. Proc. Conf. on Security in Opportunistic and SOCial networks, Istanbul Turkey 2008, article no.1

[12] Fausto Giunchiglia, Rui Zhang, Bruno Crispo,RelBAC: Relation Based Access Control. Proc. 4th IEEE Conf.on Semantics, Knowledge and Grid (SKG), Bijing , 2008 , 3-11

[13]Leigh Dodds. An Introduction to FOAF .at http://www.xml.com/pub/a/2004/02/04/foaf.html February 04, 2004.

[14] Content-Based Access Control. At www.cs.sunysb.edu/~mhart/cbac.pdf , 23 Oct 2006

[15] D. Abi Haidar, N. Cuppens-Boulahia, F. Cuppens, and H. Debar. An Extended RBAC Profile of XACML.Proc. 3rd ACM Workshop. On Secure Web Services, Alexandria, VA,, USA, 2006, 13 - 22.

[16] Use of RDF metadata to specify and enforce access control policies

[17] U. M. Mbanaso, G. S. Cooper, D. W. Chadwick, S. Proctor. Privacy Preserving Trust Authorization Framework Using XACML.in Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks WOWMOM '06, 2006.

[18] Finin, T., Joshi, A., Kagal, L., Niu, J., Sandhu, R., Winsborough, W.H., Thurais ngham, B.: ROWLBAC: Role Based Access Control in OWL. In: ACM Symposiumon Access Control Models and Technologies (SACMAT). (June 2008)

[19] Fausto Giunchiglia, Rui Zhang, Bruno Crispo, "Design and Run Time Reasoning with RelBAC",Technical Report noDISI-08062,November 2008.

[20] Wu, D., Chen, X., Lin, J., Zhu, M.: Ontology-Based RBAC Specification For Inter-operation in Distributed Environment. Lecture Notex in Computer Science 4185 (2006) 179

[21] Javanmardi, S., et al. SBAC: "A Semantic-Based Access Control Model". in NORDSEC-2006. 2006.

[22] Simone Heil, Development and Implementation of an AJAX framework for Dynamic context injection in Web 2.0 applications, Diploma Thesis, Hochschule Fulda University of Applied Sciences, December 2006

[23] Asem Hassan ,Conceptual Design of Identity Management in a profile-based access contro, Masters Thesis in Information and Communication Systems, Hamburg University of Technology, 2006

[24] T. Priebe, W. Dobmeier, and N. Kamprath., "Supporting Attribute-based Access Control with Ontologies," Proc. of the 1st International Conference on Availability,

Reliability, and Security (ARES 2006), IEEE, pp. 465-472

[25] XACML profile for WS- Policy Constraints. Working draft06, OASIS, October, 2005.

Appendix

7 APPENDIX

XACML Sample policy

```
<? xml version=" 1.0 " />
<Policy Policy I d=" . . ."
   Rule Combining Alg Id= " identifier: rule –combining –algorithm: deny –overrides ">
   <Target />
<Rule Rule Id=" . . ." Effect=" Permit " / " Deny " >
<Target>
    <Subjects>
      <Subject>
       <Subject Match
       MatchId=" urn: oasis :name s : t c : xacml :1 .0 : function : string –equal ">

  <Attribute Value
    Data Type=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g ">
<! Any attribute Value Subject e.g email id e.g. Alice@ company .com or Role or Group
information of user>
</ Attribute Value>
<Subject Attribute Designator
Attribute I d=" urn:oasis :name s : t c : xacml :1 .0 : s u b j e c t –category "
      DataType=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g ">
         </ Subject Attribute Designator>
     </ Subject Match>
    </ Subject>
</ Subjects>
<Resources>
    <Resource>
    <Subject Match
Match Id=" urn:oasis : name s : t c : x a cml :1 .0 : f u n c t i o n : s t r i n g –equal ">
  <Attribute Value
        DataType=" h t t p : //www.w3. org /2001/XMLSchema#AnyURI ">
<! Any resource URL e.g. http: //company. com/ java / docs / tutorial . htm>
        </ Attribute Value>
   <Resource Attribute Designator
  Attribute I d=" urn:o a s i s :name s : t c : xacml :1 .0 : resource : resource –id "
         DataType=" h t t p : //www.w3. org /2001/XMLSchema#AnyURI ">
        </ Resource Attribute Designator>
        </ Subject Match>
         </Resource>
    </ Resources>
    <Ac t ions>
   <Ac t ion>
```

```
      <Action Match
      MatchId=" urn: oasis :name s : t c : x a cml :1 .0 : f u n c t i o n : s t r i n g –equal ">
        <Attribute Value
        DataType=" h t t p: //www.w3. org /2001/XMLSchema#s t r i n g ">
<! Any action user wants to take on resource e.g. Read, Write, update>
        </ Attribute Value>
<Action Attribute Designator
 A t t r i b u t e I d=" urn: oasis :name s : t c : xacml :1 .0 : a c t i o n : a c t i o n –id "
 DataType=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g " />
                  </Action Match>
                </Ac t ion>
             </Ac t ions>
          </ Target>
    </Rule>
</ P o l i c y>
```

XACML Sample Request

```
<Request>
    <Subject>
        <Attrib u t e
         At tribute I d=" urn:oasis :name s : t c : xacml :1 .0 : s u b j e c t : s u b j e c t –id "
        Data Type=" urn: oasis: names: t c : xacml :1 .0 :data–type:rfc822Name ">
        <Attribute Value>
                              Subject email id e.g. Alice@ company .com
       </ Attribute Value>
        </ A t t r i b u t e>
        <At t r i b u t e
            Attribute Id=" urn: oasis :name s : t c : xacml :1 .0 : s u b j e c t –category "
            DataType=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g "
           Issuer=" admin @ company . com">
           <Attribute Value>developer s</ Attribute Value>
           </ A t t r i b u t e>
 </ Subject>
 <Resource>
 <Attribute
        Attribute I =" urn: oasis :name s : t c : xacml :1 .0 : resource : resource e–id "
        DataType=" h t t p : //www.w3. org /2001/XMLSchema#anyURI ">
             <Attribute Value>
<! Any resource URL e.g. http: //company. com/ java / docs / tutorial . htm>
                 </ Attribute Value>
              </ Attrib u t e>
            </Resource>
          <Action>
            <At t r i b u t e
                Attribute Id=" urn: oasis: names: t c: xacml :1 .0 : action : action –id "
                 DataType=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g ">
                <Attribute Value>read</ Attribute Value>
```

```
            </ A t t r i b u t e>
        </ Ac t ion>
</Request>
```

XACML Sample Response

```
<XACML AuthzDecision Statement>
<Response>
<Result>
<Decision>Permit</Decision>
<Status><StatusCode Value=" urn: oasis: names: tc: xacml: 1.0:
status: ok"/></Status>
</Result>
</Response>
</XACML AuthzDecision Statement>
```

Semantic Descriptor

XACML Request

```
<Request>
   <Subject>
       <Attrib u t e
        At tribute I d=" urn:oasis :name s : t c : xacml :1 .0 : s u b j e c t : s u b j e c t –id "
       Data Type=" urn: oasis: names: t c : xacml :1 .0 :data–type:rfc822Name ">
       <Attribute Value>Subject attributes e.g. email id </ Attribute Value>
       </ A t t r i b u t e>
       <At t r i b u t e
           Attribute Id=" urn: oasis :name s : t c : xacml :1 .0 : s u b j e c t –category "
           DataType=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g "
         Issuer=" admin @ company . com">
         <Attribute Value>developer s</ Attribute Value>
         </ A t t r i b u t e>
</ Subject>
<Resource>
<Attribute
       Attribute I =" urn: oasis : name s : t c : xacml :1 .0 : resource : resource  e–id "
       DataType=" h t t p : //www.w3. org /2001/XMLSchema#anyURI ">
<Attribute Value>
       Resource attributes e.g any URI of resource h t t p: //company. com / java / docs /
       tutorial
        </ Attribute Value>
          </ Attrib u t e>
</Resource>
       <Action>
         <At t r i b u t e
```

```
            Attribute Id=" urn: oasis: names: t c: xacml:1 .0 : action : action –id "
             DataType=" h t t p : //www.w3. org /2001/XMLSchema#s t r i n g ">
            <Attribute Value>read</ Attribute Value>
            </ At t r i b u t e>
      </ Ac t ion>
</Request>
```

7. a *Ontology point:*

<Subject>-> SO

<Resource>-> OO

<Action>-> AO

7. c Authorization Point:

AP $\subseteq$ S*O*A

Oprs = (CA, Grant, Revoke)

CA(s,o,a) is a function of decision making such that

CA: S* O*A -> {true, false}

CA: S* O*A -> {true} -> Permit

CA: S* O*A -> {false} ->Deny

7. c XACML response with Semantic Authorization point Decision to Policy decider

<XACML Authz Decision Statement>
<Response>
<Result>
<Decision>

CA: S* O*A -> {true} -> Permit

CA: S* O*A -> {false} ->Deny

</Decision>

<Status><Status Code Value=" urn: oasis: names: tc: xacml: 1.0: status: ok"/></Status>

</Result>
</Response>

8. Policy decider

It decides about policy as it is a simple or complex .A policy is complex if it involves arithmetic comparison operators and complex functions not supported by semantic web language. Complex policies are evaluated by XACML constructs e.g. PDP

Policy-> p
Simple policy-> sp
Complex policy-> cp
PD (p, sp, cp) is a function of policy decider such that
PD (p, sp, cp) -> {true} -> sp

PD (p, sp, cp) -> {false} -> cp

Sp -> XACML response to PEP

<XACML AuthzDecision Statement>
<Response>
<Result>
<Decision>
"Permit"
"Deny"
</Decision>
<Status><Status Code Value=" urn: oasis: names: tc: xacml: 1.0:
status: ok"/></Status>
</Result>
</Response>

9. Cp ->XACML response to PDP

PDP evaluate policy on basis of complex policy requirement.

10.a ,10.b. XACML response from PDP to Context handler and PEP.

<XACML AuthzDecision Statement>
<Response>
<Result>
<Decision>
"Permit"
</Decision>
<Status><Status Code Value=" urn: oasis: names: tc: xacml: 1.0:status: ok"/></Status>
</Result>
</Response>