Access control methodology for sharing of open and domain confined data using Standard Credentials

Dr. Nirmal Dagdee, Director
S.D. Bansal College Of Technology,
Indore, India
director@sdbct.ac.in

Ruchi Vijaywargiya, Asst. Professor
Department Of Computer Science
S.D. Bansal College Of Technology,
Indore, India
ruchivijaywargiya@yahoo.com

***Abstract*— Various credential based approaches have been proposed for realizing access control on shared data sources. These approaches use various types of credentials like identity certificates, attribute certificates, authorization certificates etc. Different credentials are found to be suitable in different conditions. The aim of this paper is to develop an access control methodology that not only enables immediate and open access to shared data by competent users but also provides fine grained access control on the domain confined data. The concept of standard credential is introduced which is a general purpose credential and can grant easy and fast access to variety of data sources across multiple domains. In this methodology, access control policy is defined using various types of credentials. Use of different types of credentials simplifies the specification of access control policy and provides more granular access control.**

Keywords- Access Control; credential; digital certificates; open access; attribute certificate; identity certificate; authorization certificate

I. INTRODUCTION

Web based technologies are gaining popularity not only to satisfy requirements of different businesses but also to enable availability of various data sources and services to general users. With the increasing use of these technologies, the present organizations in a typical corporate environment are not bound by geographical locations but their functioning is generally distributed across the globe. The decentralized and distributed information data sources each containing large volume of data and in variety of data formats, have posed difficult challenges for realizing access control on integrated data. Access to the shared and distributed data sources necessitates adoption of security and control measures against clandestine and unauthorized access yet facilitating easy access to legitimate user. There is a growing need for development of an architectural framework and appropriate methodologies for realizing open access systems that would enable easy access to shared resources for common users along with the fine grained access control in closed administrative domain.

Credential based access control approaches have been proposed for open access in which the user has to submit the required set of credentials for accessing the data source. The credentials that are commonly in use are identity credentials, attribute credentials, authorization credentials, etc. It has been observed that different credentials are appropriate for different types of access and thus need has been felt to have a general purpose and long lived credential which can grant access to various data sources across multiple domains. Also, as different credentials can grant access in different conditions, an appropriate system is required that uses different types of credentials for specifying the access control policy and making the system accessible to users having diversified access requirements.

II. CREDENTIAL BASED ACCESS CONTROL

Traditional access control approaches are based on identity based authentication where it is assumed that the users are known to the provider generally through a process of registration. In an open and distributed environment where data access is required by anyone spontaneously, centralized access control methodologies based on identity verification are not suitable. The credential based access control systems are found to be more appropriate in such environment [3,4,5,6,7]. In credential based approaches, user has to submit the required set of credentials for accessing the data source. The access decision depends on the properties the user may have, and can prove by presenting one or more credentials.

The credentials are realized as digital certificates that are verifiable and can be electronically transmitted. Credentials are issued by Certificate Issuing Authority (CIA) in much the same way as government agencies issue paper credentials like passport or driving license. A digital certificate works on the principle of Public Key Infrastructure (PKI)[9] and creates a binding between the certificate owner and his public key. The properties of the certificate owner which are asserted by the credential could be his identity or some attributes related to him. Depending on the capability, the user can acquire one or more credentials from various CIAs. In general, a CIA can issue multiple credentials and multiple CIAs can issue same type of credential. It is up to the data provider to decide that what type of credentials it can accept for granting access to his data source. Credentials are used to define access control policy

ISSN : 0975-3397

and anyone who possesses desired credentials is granted access to the shared data source.

The main advantage of credential based systems is that it does not require central control and allows users to specify their own trust specification. The certification authority can issue certificates to users and a user can prove his eligibility by showing an appropriate set of credentials to the resource provider. A resource provider acting as a verifier checks the shown set of credentials against the access control policy and grants or denies access accordingly.

Various types of credentials are being used by existing applications. Credential that is commonly used with single data source or a tightly coupled system is realized as Identity certificate [4,5,7,10,11]. An identity certificate is an electronic document used to recognize an individual, a server or some other entity and to connect that identity with a public key. Identity certificates are issued and certified by entities called certification authorities (CA). When a CA issues an identity certificate, it binds a particular public key to the name of the entity identified by the certificate. In addition to a public key, a certificate always includes information such as the name of the identity it identifies, a validity period, the name of the CA that issued the certificate, the digital signature of the issuing CA and so on. The Identity credential contains the identity of the user as known to the data source. Thus, it is assumed that the identity credential is usually issued by the owner or provider of the data source. User may possess multiple Identity credential one for each data source he is registered with. The identity based approaches that require registration of user with the data source provider helps in achieving access control in closed domain environment. But the necessity of prior registration of every user puts a limit on scalability of such systems and also makes the system unsuitable for open access.

It has been observed that all access control decisions are not identity based. In open environments such as the Internet, resource requesters are not identified by unique names but are identified by their attributes to gain accesses to resources. For example, requester being a member of the library is more important than his identity in order to provide him the access on the shared electronic books. Similarly, a doctor submitting a proof of being a doctor is more relevant than his identity while providing him access to the shared medical records of some person. Here the user is required to submit the proof of bearing the membership of the library or having the degree of medical professional. The credential that certifies the specific properties of the user rather than his identity is realized as Attribute Certificate. In Attribute Based Access Control [1,4,5,6,7,8,11,14], the access policy is based on the various attribute values related to the user, resource or environment. The Attribute certificate is issued by Attribute Authority (AA) and has a structure similar to the Identity certificate. However, in place of public key, the attribute certificate contains the name value pairs of the various attributes. Basing authorization on attributes provides flexibility and scalability that is essential in the context of large distributed open systems. However, attribute being generally domain specific and lack of attributes suitable for multiple domains make the system not purely open access [8]. Also, the requirement of acquiring the credentials before submitting the data access request introduces considerable delay especially when immediate access to data is required in some critical situation [12]. Privilege Management Infrastructure (PMI)[13] defines appropriate framework for issue and management of user privileges in the form of attributes of attribute certificates.

Recent research developments have resulted into another kind of digital certificate called as the authorization certificate which is based on the principle of delegation of rights and responsibilities [2,4,5,7,15]. The authorization certificate is issued by the authority called as authorization authority which itself has rights to access the specific resource and thus can delegate full or subset of his rights to other users. The authorization certificate usually contains the identity of the resource, identity of the user as can be proved by the user, action on the resource which is allowed to the user, evidence that the issuer has the rights to access the resource, etc The advantage of this approach is that the user is authenticated by his own domain and hence change in organizational structure has no effect on the access control policy [2].

The rest of this paper is organized as follows. Section 3 explains the proposed access control methodology suitable for open and domain confined data. Section 4 describes the design considerations and in section 5 system architecture and prototype implementation of the proposed system are discussed. In section 6, we have summarized the salient advantages of the proposed work and specified the future work.

III. PROPOSED METHODOLOGY

It has been observed that various kinds of credentials are being used by existing applications and different credentials are found suitable in different environment. The Identity certificate is more appropriate in closed domain access whereas in open access environment, attribute certificates are more suitable. Authorization certificates can be used where limited time access is to be granted and thus the access rights can be delegated by one user to other user. However, in today's corporate environment, an access policy is required which can grant access to users ranging from employees to customers, registered to unknown users and the users from different domains. Identity credential is usually issued by the data source provider and thus user is expected to acquire multiple identity certificates one each for the data sources it accesses. Attribute credentials are usually domain dependent and thus one attribute certificate may not be useful for accessing other data source or may be data source in different domain. Thus user has to acquire various different types of credentials from various CIAs in order to gain access on various data sources. Acquiring various credentials on one hand provides access on various data sources but on the other hand complicates the task of credential handling and management. Also, the verification of multiple credentials issued by various CIAs at data source provider introduces delay and increases complexity. The need has been felt to develop some general purpose and long lived credentials which can gain access to multiple data sources across multiple domains.

ISSN : 0975-3397

A. *Standard Credential*

The popular paper credentials that are used commonly to perform various tasks or access various resources are passport, driving license, academic degree, society/club membership etc. These credentials grant a status to the bearer like a license issued by Vehicle Control Authority certifies that the bearer is a skilled driver for certain types of vehicles. Another example may be that of a university who issues a credential to certify that the owner is a 'Medical Student' in that university. These credentials are issued by specific authorities and contain specific attributes organized in a specific format. These credentials are trusted and accepted by various resource providers not only because they have specific attributes organized in fixed format but also because they are issued by specific agencies which usually everyone trusts. Therefore a professor of one country is generally accepted as 'Professor' in another country. In this paper, we propose a kind of digital credentials which are similar to the paper credentials commonly in use. We named these credentials as standard credentials. These credentials contain the values of those attributes that grant a 'status' to the bearer of the credential. For example, the attributes like name of university, name of course, year of admission, duration of the course, specialization area etc. in standard credential gives a rank of 'student' to the bearer. These credentials are named as standard as they have standard logical structure and can be issued by specific agencies only. This information is published and thus known to everyone. A registered authority identifies and publishes the list of standard credentials which the data source providers usually require in order to provide access on their data sources. The users can acquire and preserve these credentials and can use them as and when needed to access any data source. Using these credentials user can get access on most of the data sources.

The data source provider makes use of one or more of these credentials to define the access policy. Use of standard credentials simplifies the specification of access control policy as provider need not have to specify the values of various attributes as is the case with attribute certificates rather can specify the policy in terms of one or more standard credentials. This in turn reduces the number of credentials the user has to submit for data access. Even if the access policy is defined in terms of attributes, this credential enables user to submit multiple attributes together all being part of one or at least few credentials. Verification of standard credential is simpler than any other traditional credential as one has to verify only that the person sending the credential is himself the owner of the credential. Use of Standard credential also relaxes the issue related to privacy of various user attributes whose values the user may not wish to disclose. User can have the freedom of selecting the attributes which he wishes to be present on the credential and which he does not. Life of standard credential is comparatively more than that of attribute credential but is generally less than that of identity credential.

B. *Approach based on multiple credential types*

Use of standard credential can grant user the access to most of the data sources. However, the usage of standard credential does not completely remove the requirement of other types of credentials. In smaller organization, access control based on identity or role is the appropriate choice. Standard credentials are found more suitable in multi domain environment where open and immediate access is required. However, standard credentials have limitation where fine grained access control is required. In such situations, access control based on crisp values of various attributes is more appropriate. Access policy may also require the value of some attributes which are not part of any of the standard credential and thus attribute credentials can be used. Delegation of access rights can be done using authorization credential and thus user possessing the authorization credential can gain access to the data source. Thus we propose an access control system in which access control policies are defined in terms of multiple types of credentials. The usage of different credentials can grant access to different users on different data sources. Depending on the access requirements, the users submit different types of credentials at different times. It is up to the data source provider to decide that what credentials and from which CIAs it can accept the credential in order to provide access on the data source. A typical application having varied requirement is EHR in which the required access control methodology should be such as to enable immediate and open access to critical information by competent users in addition to providing fine grained access control to registered users. The doctor submitting the standard credential of 'doctor' can get access to limited data about every patient whereas a doctor by submitting the identity credential can access complete details of his patients.

IV. DESIGN CONSIDERATIONS

A. *Standard Credential*

In this paper, we have proposed a new credential type called as 'Standard credential'. These credentials are similar to paper credentials commonly in use like passport, club membership, etc. It is proposed to have various types of standard credentials and all credentials of same type contain similar attributes. Various types of standard credentials are identified and published by some apex authority. The attributes associated with each type of standard credentials are also identified and published. The information about these standard credentials is published so that the data or the resource providers can define their access policies in terms of these standard credentials. The information which is typically published about each of the Standard credential is the name of the credential and the list of associated attributes. Any university can issue the standard credential of 'student', but every 'student' credential will have different values for the attributes associated with 'Student' credential. Although different universities may consider different values of those attributes for issue of that credential. One type of credential can be issued by multiple CIAs. However, the issuing policy for same type of credential can be different for different CIAs.

1) *Format of Standard Credential*

ISSN : 0975-3397

The standard credential grants a status to the user which is defined in terms of various attributes. Thus every standard credential is associated with some fixed attributes. For example, the standard credential of a 'student' will have associated attributes like name of the course, duration of the course, year of admission, etc. As the standard credential contains the values of various attributes, the structure of standard credential as shown in Figure 1 is similar to that of attribute credential. In order to differentiate between various types of credential, every credential has a typeId which differentiates that credential from other types of credentials. In addition to name value pairs of the attributes and type identifier, the standard credential contains information like Serial number, Name of the issuer, Validity Period, etc and is digitally signed by the issuer.

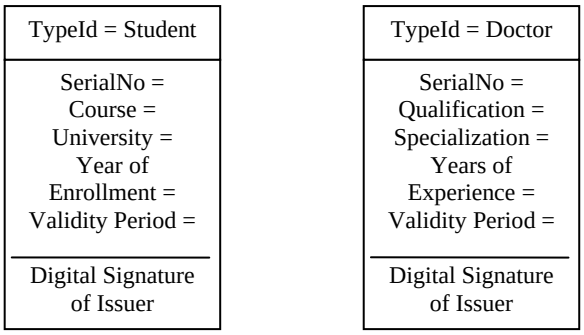

Figure 1. Sample Standard Credentials

2) CIA Hierarchy

Like any other digital certificate, standard credentials are issued by CIAs. Multiple CIAs are organized in the form of Certification Authority Hierarchy as shown in Figure 2. It is assumed that an apex authority identifies and publishes the list of standard credentials. This apex authority may empower some government agencies usually one per country to work as nodal controlling authority to authorize various CIAs for issue of different standard credentials. These nodal agencies identify certain organizations as the root issuers. There is usually one root issuer for one type of standard credential in one country. For delegation and distribution of work, these root issuers may have hierarchy of CIA to work under them.

Every CIA can have their own policy for issuing the credentials. However, it is mandatory for every CIA to publish its credential issuing policy. These policies will facilitate the resource providers in developing trust on issuers. It depends on the provider to trust various issuers and accept the credentials issued by them. This infrastructure would be similar to that of Internet addressing by which globally unique IP addresses and domain names are issued to various organizations.

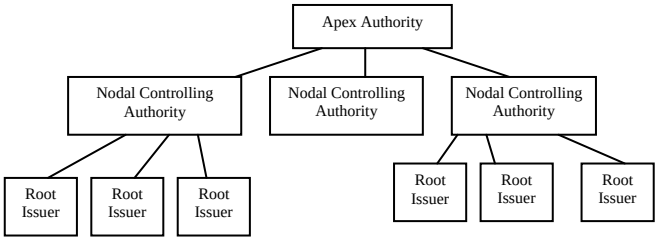

Figure 2. CIA Hierarchy for standard credentials

3) Issue of standard credential

Standard credentials are issued by specific CIA. The process of issue of standard credential is similar to that of any other credential in which the user is required to register with the certification authority. The registration process requires the user to submit the values of various attributes which are associated with the requested type of credential. After verification of the attribute values, the certification authority issues the certificate. Many a times, user may not wish to disclose these values to the providers to whom the credential will be submitted. Therefore, user may also specify that out of all submitted attributes, which attribute and its corresponding value can be part of the credential and which cannot be. If any attribute becomes part of the credential, its value will be disclosed to the provider to whom the credential is submitted for data access. However, for values of all the other attributes, the provider may refer to the credential issuing policy of the issuer which specifies the range of values of an attribute for a specific type of credential.

4) Verification of standard credential

In order to access the data, the user submits one or more standard credentials to the data source provider. The data provider verifies the credential. As the issuing policy of the standard credential is known, the verification process of standard credential is usually simpler than that of any other credential. Generally it only verifies that the user who is submitting the credential is also the owner of the credential. Verification is done by the method of credential chaining. Using cross certification methodology, certificates issued by different CIAs can also be trusted. Validation of credential involves matching the type of standard credential with the required credential type.

B. Access Control Policy Specification

Access control policy is a mapping between the data items and the credentials required to access those data items. In the proposed system, access control policy is defined using various types of credentials. Identity credentials can grant the access to the registered or known users. Whereas in open access, most of the access can be achieved using standard credentials. Each standard credential has its own associated attributes. But the access policy may be defined using attributes which may be or may not be part of any standard credential. In such cases, submission of attribute certificates by the user can grant him

ISSN : 0975-3397

the access. Granularity of access control is enhanced by specifying the data elements which the user can access on submission of desired credentials. These elements can be specified directly or by defining some conditions on the data source.

Access policy also maintains the list of issuers for various types of credentials which it trusts and can accept. Identity credential is usually issued by the data provider whereas the standard credentials can be issued only by the registered authorities whom usually everyone trusts. Any one can issue the attribute certificate and it is up to the data provider to decide whether it can accept the attribute certificate from specific CIA.

An access control policy is defined in terms of

- Access control rule
- Access control condition, and
- Credential attributes value tuple

An access control policy is a set of access control rules where each rule contains one or more access control condition corresponding to each of the data items of the data source. An access control condition is a logical combination of credential attribute value tuples which defines the specific values of attributes of a credential.

In this paper, we are considering Northwind database, sample database with MSAccess as case study. Northwind is a relational database having tables like Employees, Customers, Orders, Products, Shippers, and Suppliers etc.

1) Credentials

As the various kinds of credentials are used to define the access policy, we propose to have unique Group Id for each of the credentials and each of the standard credential will have unique type id which differentiates one standard credential from other. For NorthWind datasource, we propose following standard credentials: Std_Shipper, Std_User, Std_Student, Std_Inspector, Std_Employee. Employees of the organization possess the Identity Credential as well. Customs department has issued an authorization certificate Auth_Inspector to one of its inspector.

2) Credential attributes value tuple

The credential attributes value tuple is defined as a credential with specific values or range of values for its attributes. Different values of attributes of a credential may be required to access different data items. Thus, there could be multiple tuples corresponding to one credential.

TupleId	Credential_Id	Attribute1	opr	Value 1	Attribute2	opr	Value 2
T1	Std_Shipper						
T2	Id_Employee	Employee Id	=	Employee Name			
T3	Std_User	Country	=	USA			
T4	Std_Student	Course	=	Business Management			
T5	Auth_Inspector						
T6	Std_Inspector						
T7	Std_Employee						

3) Access Control Condition

An access policy on a data source may require multiple credentials with specific attribute values. This is specified using access control condition where each access control condition is a logical combination of various credential attribute value tuple. This way, field level access control is provided on the data source. However, record level filtering is done by defining one or more data conditions as part of the access control conditions.

ACC Id	ACC Description	Tuple Id	operator	Tuple Id	Condition
ACC1	A user having standard credential of shipper can see all details of Shippers table	T1			
ACC2	A user having standard credential of shipper can see only 'ship via' field of Orders	T1			
ACC3	An Employee can see order details of his orders only	T2			EmployeeId = Orders.Employee
ACC4	Any user can access product details except units_in_stock and units_in_order	T3			
ACC5	An inspector carrying the authorization can access all details of products	T5	AND	T6	

ISSN : 0975-3397

ACC6	A student can access all details of the orders already executed	T4			Date of shipping is before the current date
ACC7	An Employee can see all details of only those Employees who reports to him	T2	AND	T7	ReportsTo = EmployeeName

4) Access Control Rule

Access Control Rule is a mapping between the data items and the various access control conditions. In order to grant the access to the user on the data item, one of the corresponding access control conditions has to be true. If multiple data items have same access control policy, then all those data items can be part of the same access control rule. However, one data item will be part of one access control rule. Asterisk(*) in the fieldname indicates all fields of the table.

Table Name	Field Name	Field Name	Field Name	ACC Id	OR	ACC Id
Shipper	*			ACC1		
Orders	Ship via			ACC2		
Products	Product Name	Product Category	Unit Price	ACC4		
Orders	*			ACC3	OR	ACC6
Employee	*			ACC7		

5) Trusted Issuer List

The access policy also maintains the list of trusted credential issuers from whom it can accept the credentials. The list of issuers has more relevance in case of attribute credentials as standard credentials are usually issued by registered authorities and the identity certificate is usually issued by the data source provider.

V. SYSTEM ARCHITECTURE AND IMPLEMENTATION

The proposed System comprises of mainly three modules: Data Source Provider, Request Handler, Policy Engine and the Policy Store as depicted in Figure 3. Request sent by the user is received by Data source provider which provides a standard data access interface to the user application. Access authorization is determined by the Policy Engine, and accordingly data source provider forwards the user request to the data source.

A. Data Source Provider

Data source provider provides a standard data access interface to the user application. In this system, user request is intercepted at the data source provider and access control is applied. DS Provider forwards the user request to the Request handler for extraction of access authorizations. In absence of access control system, data source provider directly forwards the user's data access request to the data source.

B. Request Handler

Request handler comprises of three modules: *Credential Separator (CS)*, *Data Item Separator (DS) and Request Modifier(RM)*. In general, the request from the user contains the data access request and a set of credentials. The *credential separator* separates the credentials from the user request. *Data item separator* of the system extracts the data items from the data access request and creates a list of data items. The list of credential identifiers and the list of data items are sent to Policy Engine for verification.

Request handler comprises of two modules: *Credential Separator* and *Data Item Separator*. Request handler fetches the user request from the data source provider. Request from user contains data access request and the set of credentials. The *credential separator* separates the set of credentials from the user request and creates a list of credentials. *Data item separator* of the system extracts the data items from the data access request and creates a list of data items. The list of credential type identifiers and the list of data items are sent to Policy Engine for verification and validation. If the data access request from the user contains only the data access request than the list of data items present in the access request are sent to *Policy Engine.*

C. Policy Store

In Policy Store, access control rules are stored. The Policy Store maintains a mapping between the data items and the corresponding credentials required to access those items.

D. Policy Engine

The role of *Policy Engine (PE)* is to verify the submitted credentials using access control rules stored in Policy Store. List of Credential identifiers and the list of data items are sent to the *PE* by the *Request Handler*. Based on the elements present in the list of data items, *PE* extracts the list of credentials required to access those items from the *Policy Store*. If the elements in the list of Credential identifiers match with the elements existing in the list of required credentials, then the credentials are verified otherwise an access denied message is sent back to the user. Acceptance of the credentials also depends on their validity period. After successful verification, *RM* modifies the data access requests according to the access control rules applicable. DS Provider sends the data access request to the data source fetches the result from the database and sends it back to the user.

E. Implementation

In the proposed system, credentials are realized as digital certificates. X.509 [9] is popularly used for Identity

ISSN : 0975-3397

Credentials. Java APIs have been used for implementing X.509 digital certificates. Standard credentials are realized by using extension fields of X.509 certificates to store various attributes and their values. Credentials are verified by checking the issuer CIA's signature on the credential. In the prototype developed, we have used four categories of credentials: Standard Credential, Identity Credential, Attribute credential and Authorization credential. We have implemented the proposed system for a single data source (SQL Server) being accessed by multiple clients. The system is implemented as a socket server which accepts the data access request in the form of SQL query. Policy Engine is a component of the server and it stores the mapping between database items and required credentials in a separate database called as Policy database. MySQL is used for Policy Database. In the current implementation, access control is provided on viewing the database and thus only *select* queries are handled. A console application called *Policy Rule Console Editor* is being developed in order to feed policy rules into the policy store.

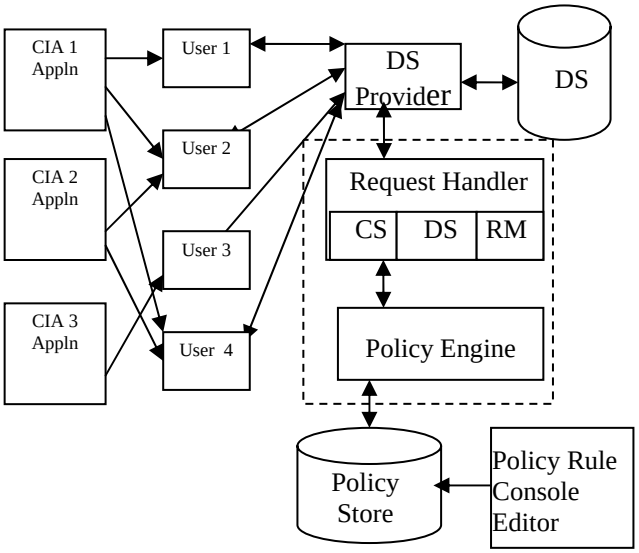

Figure 3. System Architecture

VI. CONCLUSION

The main motivation for the work described in this paper was to develop an approach for access control of shared data resources in an environment where open as well as closed domain access control is required. The main advantage of the proposed system is its capability to define access control rules using combination of Standard, Identity, Attribute and Authorization credentials simplifying the specification of access control policy. Standard Credentials are quite versatile and a single credential can grant access to variety of data sources across multiple domains and eases the access control management on the shared resources. Use of standard credentials provides easy access to large number of users possessing same type of standard credential. Use of associated attributes in the standard credentials considerably helps in achieving the required fine grained access control. Standardization of credential types and format simplifies the process of credential management and verification. As the standard credentials directly reflect the status of the user, its verification is quite simpler and therefore the proposed methodology provides easy and faster access to the authorized users on shared data. Use of different types of credentials enables the data source provider to have more granular access control policy. The proposed methodology is suitable for developing systems to incorporate open and closed access on shared data resources. Our future work incorporates design of appropriate infrastructure for issue and management of standard credentials.

REFERENCES

[1] Wei Zhou, Christoph Meinel, "Implement Role based access control with attribute certificates", The 6th IEEE International Conference on Advanced Communication Technology, page(s): 536- 540, 2004

[2] Alan H. Karp, "Authorization Based Access Control for the Services oriented Architecture", Proc. Fourth International Conference on Creating, Connecting and Collaborating through Computing,(C5), 26-27 January 2006, Berkeley, CA, USA, IEEE Computer Society, p160-167, 2006

[3] Sudhir Agarwal, Barbara Sprick, Sandra Wortmann, "Credential Based Access Control for Semantic Web Services", American Association for Artificial Intelligence, 2004

[4] Mary R. Thompson, Abdellilah Essiari, Srilekha Madumbai, "Certificate-based Authorization policy in a PKI Environment", ACM Transactions on Information and System Security (TISSEC), Volume 6, Issue 4, pages: 566 - 588, November 2003

[5] William Johnston, Srilekha Mudumbai and Mary Thompson, "Authorization and Attribute Certificates for widely Distributed Access Control", IEEE WETICE, 1998

[6] Frikken K, Atallah M, Jiangtao Li, "Attribute-Based Access Control with Hidden Policies and Hidden Credentials", IEEE Transactions on Computers, Volume 55, Issue 10, Page(s): 1259 – 1270, Oct. 2006

[7] Mary Thompson, William Johnston, Srilekha Mudumbai, Gary Hoo, Keith Jackson, Abdelilah Essiari, "Certificate-Based Access Control For Widely Distributed Resources", ACM, Proceedings of the 8th conference on USENIX Security Symposium, Volume 8, Pages: 17 - 17 , 1999

[8] Shen Hai Bo, Hong Fan, "An attribute based access control model for web services", proceeding of the seventh international conference on Parallel and Distributed Computing, Applications and Technologies, IEEE 2006

[9] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", September 1998

[10] Sabrina De Capitanidi Vimercati, Pierangela Samarati, " New Directions in Access control", www.spdp.dti.unimi.it/papers/nato.pdf, 2002

[11] Ioannis Mavridis,Christos Georgiadis, George Pangalos, marie Khair, "Access Control based on Attribute certificates for Medical Internet applications", Journal of medical Internet Research, Vol 3, 2001

[12] Nirmal Dagdee, Ruchi Vijaywargiya, "Credential based hybrid access control methodology for shared Electronic Health Records", IEEE International Conference on Information Management and Engineering, Kuala Lumpur, Malaysia, 2009

[13] David Chadwick, "The X.509 Privilege Management Infrastructure", http://sec.cs.kent.ac.uk/download/X509pmiNATO.pdf, 2002

[14] David W. Chadwick, "Authorization using Attributes from Multiple Authorities", www.cs.kent.ac.uk/pubs/2006/2412/content.pdf, 2006

[15] Jun Li and Alan H. Karp, "Access Control for the Services Oriented Architecture", ACM 2007

ISSN : 0975-3397

AUTHORS PROFILE

Dr. Nirmal Dagdee is a professor of computer science and has about 25 years of teaching experience in various enginnering colleges. His areas of active research are data security, SOA and soft computing. He has authored several research papers that are published in reputed journals and conference proceedings. Currently, he is director of S. D. Bansal College Of Technology, Indore, India

Ruchi Vijaywargiya, a faculty of computer science in S.D. Bansal College Of technology has around 18 years of experience in teaching and software industry. She is pursuing her doctoral research under the guidance of Dr. Dagdee in the field of data security and access Control. Her areas of interest are data security, computer networks and object oriented technology.

ISSN : 0975-3397