CREDENTIAL BASED MEDIATOR ARCHITECTURE FOR ACCESS CONTROL AND DATA INTEGRATION IN MULTIPLE DATA SOURCES ENVIRONMENT

Dr. Nirmal Dagdee[1], Ruchi Vijaywargiya[2]

Department of Computer Science and Engineering,
S. D. Bansal College Of Technology, Indore, India
[1]nirmal_dagdee@rediffmail.com
[2]ruchivijaywargiya@yahoo.com

ABSTRACT

In multiple data sources environment where open access is to be provided to the users not known to the system, the credential based access control has emerged as a suitable approach for achieving security on shared data [22,23,28,29,31]. Mediation techniques have been developed for data integration that provide a single unified view of the multiple data sources to the user[1,2,3,4,5,6,7,18]. For enforcing common access policy across the available data sources and enabling controlled access on data at local levels, appropriate multilevel access control policy is also required. In this paper, we propose a credential based mediator architecture to achieve multilevel access control and data integration in open access environment. To realize the multilevel access policy a credential transfer protocol has been proposed to accomplish the transfer of credentials and extracting attribute values associated with them.

KEYWORDS

Credential, mediator, access control, data integration

1. INTRODUCTION

In multiple data source environment where heterogeneous data sources exist, data integration and controlled access to various data sources have been the basic issues to be handled. To support open access to user not known to the system, credential based access control (CBAC) is found to be a more suitable approach [22,23,28,29,31]. In CBAC systems, user submits a set of credentials for accessing the data source. The access decision depends on the properties the user possesses and can prove by submitting one or more credentials. For data integration, mediator architecture has been recognized as the most commonly used approach for integration of data from heterogeneous data sources [1,2,3,4,5,6,7]. The mediator presents a virtual integrated view of the data sources to the user by mapping the data models of the various sources onto the exchange model of the system. Various mediation systems like Medience, Tsimmis, Agora, Xyleme, Garlic and e-XMedia have been developed [4] for academic as well as commercial use.

The mediation system can be viewed as a three layer system: presentation layer, mediation layer and the source layer as shown in Figure 1. At the presentation layer, the user gets a single integrated view of the data sources generated using unified global schema and can pose query prepared using global schema. At the mediation layer, the Subquery Generator (*SubQGenerator*) divides the user's query represented using global schema into various subqueries represented using local schemas of the various data sources. The *Schema Mapper* resolves the differences between the global schema and the local schemas using mapping approaches like Global as View (GaV) and Local as View (LaV) [1,2,4,5]. This layer is also

DOI : 10.5121/ijnsa.2011.3304

responsible for integrating the results received from various data sources into a single resultset. The source layer is where the connection to the actual data sources is established. Each data source has a wrapper associated with it [4]. The subqueries are sent to the respective wrappers at the source layer. The Subquery Converter (*SubQConverter*) translates the query language of the subqueries into the native query language of each source. These subqueries are submitted to the respective data sources. The respective sources execute the queries, and return the results. The Result Converter (*ResConverter*) converts the data model of the received data to the exchange model of the system and sends it to the Result Integrator (*ResIntegrator*) where the results received from various data sources are integrated and sent back to the user.

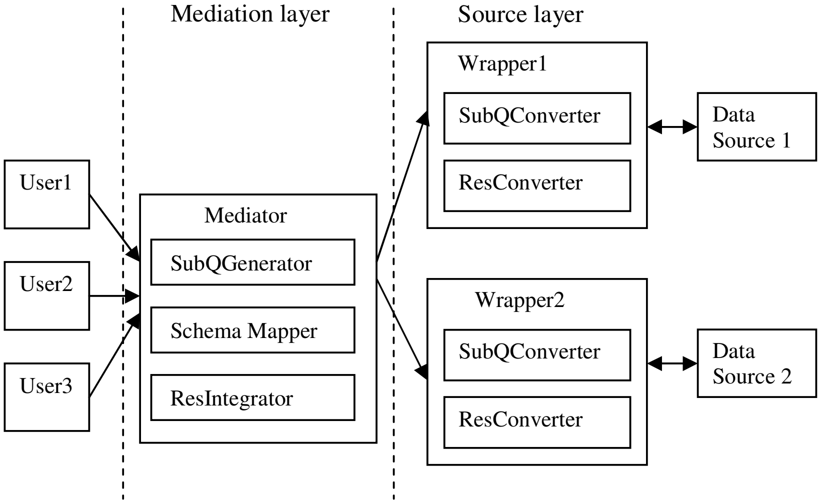

Figure 1. Typical Mediator based architecture

In this paper, we propose a credential based mediation system for access control and data integration to support open access on heterogeneous data sources along with the fine grained access control on data at local data sources.

The rest of this paper is organized as follows. Section 2 provides an overview of the work being done in the field of credential based access control and security enforcement in mediator architecture. In section 3, we have discussed about the proposed credential based mediator architecture. In section 4, implementation details have been briefed. In section 5, we have concluded by summarizing the salient advantages of the proposed work.

2. RELATED WORK

Considerable research is in progress in the field of credential based access control. CBAC has emerged as a prominent access control methodology in open access environment. Research efforts are being made to enforce appropriate security to shared and integrated data in mediator architecture.

CREDENTIAL BASED ACCESS CONTROL

Various access control approaches have been developed for enforcing security in multiple data source environment. Traditional access control methods like identity based or role based access control are found inadequate to reflect the dynamic mediator environment and the flexible access control requirements [3,5,12,14,21] of multiple data sources. Also, they are more suitable in closed administrative domain where data is accessed by users already known to the system.

In open access environment, the system is usually accessed by unknown users and the access decision depends on the properties the user possesses and can prove by submitting one or more credentials [22,23,24]. In Credential based access control [22,23,24], the access policy is defined in terms of various types of credentials like identity credentials [23,24], attribute credentials [23,24,25,26,27], etc. The data provider matches the credentials submitted by the user against the credentials required as per the access control policy and accordingly grants or denies access. Recent research has resulted into another type of credential called as Standard credential [15,28] that grants a status to the user. Standard credentials are similar to paper credentials like driving license, membership certificate etc. These credentials have standard verification procedure and are issued by specific agencies which usually everyone trusts. Each standard credential contains a fixed set of attributes and has a predefined type associated with it. Standard credential being versatile can grant access to multiple data sources. A similar credential comprising of specific credential type and a fixed set attributes has also been proposed in [30, 32].

Credential based access control policy is defined in terms of various credentials like identity credential, attribute credential, standard credentials etc. Credential based access control policy is a collection of access control rules where one or more rule is defined for each data item on which access control is required. Typically an access control rule consists of two parts: the credential part and the attribute condition part. The credential part specifies one or more credentials which the user has to submit in order to gain access on the data. The attribute condition part specifies the various conditions that have attributes associated with the credentials, the data sources or the environment as operands. A comprehensive architecture for credential based access control has been discussed in [29].

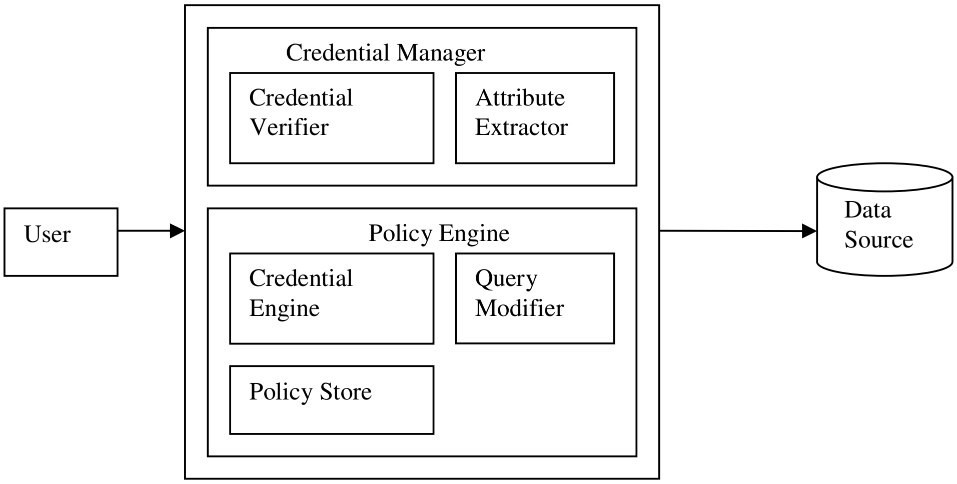

Figure 2. Credential based access control system

The credential based access control system has been presented in [28]. The system intercepts every query from the user to the data source. User submits the set of credentials along with the data access query. The two main components of the system are the Credential Manager (CM) and the Policy Engine (PE) as shown in figure 2. The role of Credential Manager is to store and verify the credentials submitted by the user. The CM also extracts the values of various attributes of the credentials as and when required by the PE. The access control policy is defined and stored in the Policy Store. Input to the PE is the set of data items requested by the user. Credential Engine applies the access control policy defined for those data items. The query modifier modifies the query so as to grant access on only that data for which user has proved his authorization by submitting desired set of credentials.

SECURITY IN MEDIATOR ARCHITECTURE

The mediation system not only enables the sharing and integration of data stored across multiple data sources but also ensures its security against unauthorized access [1,2,3,5,12]. Considerable research efforts have been made to handle the issues related to access control in a mediated environment[3,4,6,7,11,12,17]. A traditional approach to enforce security in an integrated system is to have centralized access control in the form of Security Mediators [3,6,12,17] where the administrator or the security officer focuses on the global behaviour of the system and writes access policies.

It is desirable in many situations that the owner of each data source should have local autonomy of defining and modifying the access policies dynamically and transparently [7, 11]. It has also been observed that as the source data and security policy specifications are usually tightly coupled, when source data gets updated, especially when their data structure changes, the related security policies may need to be modified accordingly [7,12]. In such situations, the traditional centralized access control mechanisms do not provide the necessary functionality and flexibility [11]. Moreover it is not acceptable to any data source that is going to be integrated by a mediation system to replace its own pre existing security model and policies. Thus, the mediation system security architecture should be such as to integrate with existing security architectures and models across various data sources environment [4]. Typically the enterprise security policies are specified in terms of the primitive rules predefined for the mediation system. It is difficult to design a unified security mediator that can effective enforce a broad range of security needs of heterogeneous information systems [7,12]. Further the need of a central authority is not always acceptable by the data owners sharing their sources [7,11]. Centralized systems are unable to provide means to guarantee that originators retain control over their information.

Several research efforts are in progress to enforce security at the data source provider rather than through a central authority [12,14,19]. Systems have been proposed where multiple policies collaborate in making the access control decisions [10,20]. Efforts have also been made to automatically decompose global level policy to generate low level data source specific policies [8,9,13]. Uniformity and coordination among multiple policies across several data sources are achieved by global integrated policy at mediator level [3,8,16]. In multiple data source environment, secured access on integrated data can be gained by satisfying the access policy at global integrated level as well as various access policies at local data sources level [1,2,3,7,8,12,14,19]. In this paper, we propose a credential based mediator architecture for multilevel access control in heterogeneous data source environment.

3. PROPOSED CREDENTIAL BASED MEDIATOR ARCHITECTURE

3.1. System Architecture

In this section, we present the architecture of the proposed credential based mediator for data integration and multilevel access control. Various components of the proposed system have been depicted in figure3. The multilevel access control is realized by integrating the credential based access control system with mediator and various wrappers. Global access control is enforced at mediator level by defining *Global Credential Manager (GCM)* and *Global Policy Engine (GPE)* whereas the local access control is enforced by defining *Local Credential Manager(LCM)* and *Local Policy Engine(LPE)* at the various wrappers. The user submits the data access query along with the set of credentials. The global access control policy at mediator is applied on the query. If the credentials submitted by the user satisfy the policy, then the query is forwarded to the various wrappers where the local access control policies are applied. If the user's credentials also satisfy the local access control policy, then the data is fetched, integrated and then sent to the user.

The system has three layers similar to a typical mediator architecture having presentation layer, mediation layer and source layer. The global policy is defined at the mediator layer and the local policies are defined at wrappers at the source layer. A common integrated global view over a set of local sources is generated using GaV or LaV[4] approach. At the presentation layer, user gets a single integrated global view of the data sources and sends the query prepared using global schema along with the set of credentials. The set of credentials may consists of one or more standard or attribute credentials and also the identity credentials as issued by global system or the various local data source providers.

At the mediation layer, the set of credentials submitted by the user are stored with *Global Credential Manager (GCM).* The *GCM* verifies the credentials submitted by the user. The user query is sent to the *Global Policy Engine (GPE*). At GPE, the global policy is applied and the query is modified so as to grant access on only that data for which user is authorized. The modified query is sent to the *SubQGenerator* where various subqueries represented using local schemas are generated using *Schema Mapper*. The various subqueries are then sent to respective wrappers.

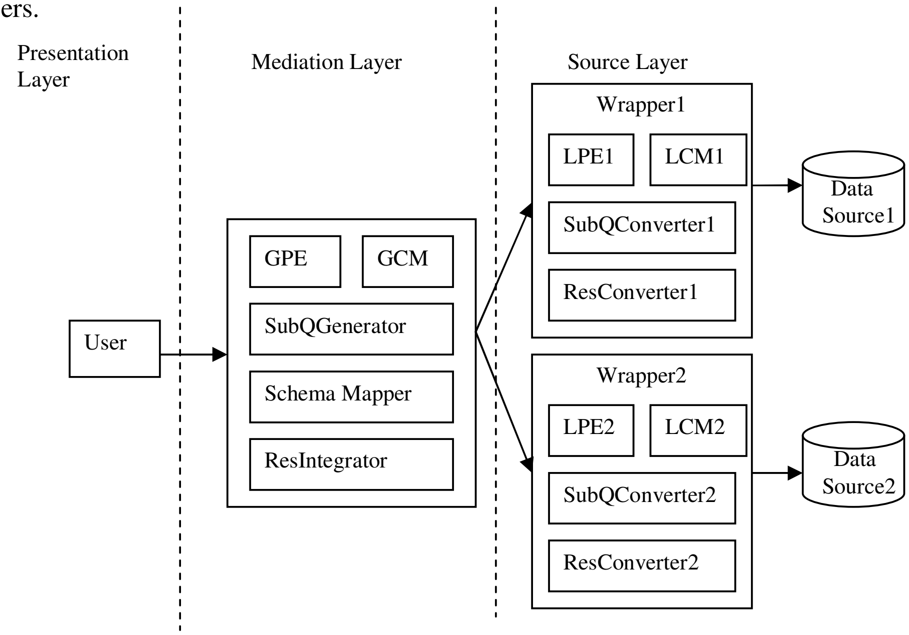

Figure 3. Credential based Mediator Architecture

At the source layer, the subquery is received by Local *Policy Engine (LPE).* The local policy is applied. The local access control policy requires some credentials or value of attributes of some credentials from user. The desired credentials and the attribute values are acquired using Credential Transfer Protocol which is discussed in section 4.2.3. The standard credentials are verified at mediator whereas the identity and the attribute credentials are verified by LCM. The local policy is applied and the query is modified. The modified subquery is sent to the *SubQConverter* that translates the sub queries into the query language supported by the data source. The subqueries are submitted to the respective data sources. The respective sources execute the queries and return the results to *ResConverter* that converts the data format to the exchange model. The Results from various wrappers are sent to the *ResIntegrator* where they are integrated into one resultset. The integrated resultset is then sent to the user.

3.2 Access Control

3.2.1 Multilevel policy specifications

In the proposed system, credential based access control policies are defined at multiple levels. Global access control policy defined at the mediator layer enforces uniform access control across all data sources. The global policy is defined by the administrator who focuses on the global behaviour of the system and writes access policies. The global policy enables centralized access control and provides consistency and coordination across all data sources. However, the security specification autonomy to data sources is provided by defining local policies at various data sources. The local policies provide fine grained access control on individual data sources.

A single integrated view of the data sources is presented to the user and the user submits the data access query prepared using global schema along with the set of credentials. Global as well as the local policies are applied on the user's query. When multiple policies are applied on the query, policy decision conflicts may occur. For example, for a data item the global policy may deny access whereas the local policy may permit access on the same data item or vice versa. Such decision conflicts are resolved by defining multilevel policy combination algorithms like global override, local override, allow override, deny override, both allow, both deny etc.

3.2.2 Access control policy architecture

Policy decision algorithm resolves the decision conflicts that may occur when multiple policies are applied on the data request. Depending on the nature of the item, an administrator may like to define policy combination algorithm for each data item on which access is controlled. Provision is required in access control architecture for specifying and executing the policy combination algorithm. Policy architecture suitable for credential based access control has been proposed in [29]. In this architecture, access policies are defined as a set of access control rule where each rule consists of two parts: credential part and attribute part. The credential part specifies one or more credentials which the user has to submit in order to gain access on the data. The attribute condition part specifies the various conditions that must be satisfied to gain access. These conditions have attributes associated with the credentials, the data sources or the environment as operands. The access policy is realized as a set of six relational database tables namely ARS(Access RuleSet), ACR(Access Control Rule), CrPartA, CrPartB, DsPart and EnvPart. In ARS, ACR is specified for each data item on which controlled access is required. ACR is a logical combination of the credential part and the attribute part. Logical combination of various credentials and the attribute conditions are realized as various tables as shown in Figure 4 below.

ARS

TId	*FId*	*ACRId*

ACR

ACRId	*SACRId*	*CrPartA*	*CrPartB*	*DsPart*	*EnvPart*

CrPartA

CPAId	*SCPAId*	*CrCatId*	*CrTypeId*	*Opd1*	*ROp*	*Opd2*

CrPartB

CPBId	*SCPBId*	*CrCatId*	*CrTypeId*	*Opd1*	*ROp*	*Opd2*

DsPart

DsId	*SDsId*	*Opd1*	*ROp*	*Opd2*

EnvPart

EnvId	*SEnvId*	*Opd1*	*ROp*	*Opd2*

Figure 4. Credential based access control policy architecture

For multilevel access control, we propose a modification in the policy architecture discussed in [29]. A new field called as Policy Combination Algorithm Identifier (PCAId) has been added to the Access Ruleset (ARS) as shown in Figure 5 in which the administrator can specify which policy combination algorithm will be applicable for corresponding data item.

Modified ARS

TId	*FId*	*ACRId*	*PCAId*

Figure 5. Proposed modification in credential based access control policy architecture

3.2.3 Credential Transfer Protocol

In the proposed system, the global policy is defined at the mediator level whereas the local policies are defined at wrappers at the local data sources level. The user submits a data access query along with a set of credentials. The set of credentials are stored and verified at the mediator and the global policy is applied on the user's query. Then the user's query is forwarded to the data source layer where the local policy is applied on it. The local policy may require one or more credentials or the values of attributes of those credentials. The wrapper requests the mediator to send the desired credentials. The desired credentials are transferred from mediator to the wrapper using Credential Transfer Protocol. The protocol is based on the request-response format is shown in Figure 6. The wrapper sends the request for the credential or the attribute and the mediator sends the response.

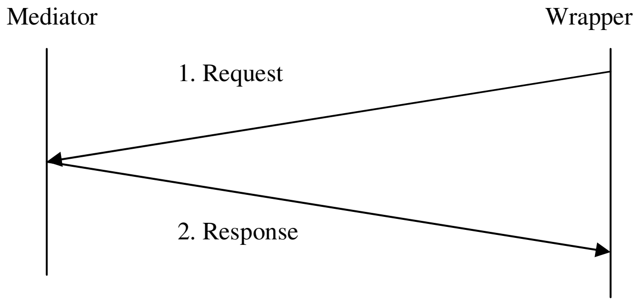

Figure 6. Credential Transfer Protocol

The credentials required by local policy could be Identity credential, Attribute credential or Standard credential. These credentials have a unique credential category identifier *CrCatId* [29]. *CrCatId* differentiates a credential belonging to one category from another. Similarly every standard credentials has a unique type identifier *SCTypeId*. The request sent by wrapper contains three parameters. First two parameters are *CrCatId* and *SCTypeId* respectively. The third parameter is different in different types of requests. The format of response depends on the type of request.

Following are the types of request response conversation between the mediator and the wrapper:

1. Standard Credential Request (SCRequest): The local access control policy expects the user to submit a standard credential. The wrapper sends a request for standard credential. The standard credentials have standard verification procedures and are verified by the mediator. The mediator layer sends the message indicating that the user has submitted the requested credential and is successfully verified at mediator as response to the wrapper rather than sending the standard credential itself.

   In SCRequest, the first parameter is the CrCatId which is SC for standard credential, second parameter is the type of standard credential SCTypeId and the third parameter is NULL. The response from mediator is a boolean value. The SCResponse is *True* if the user has submitted the desired standard credential and is successfully verified at mediator layer else the response is *False*.

   SCRequest: <SC, SCTypeId, NULL>
   SCResponse: True or *False*

2. Identity Credential Request (ICRequest): The local access policy expects the user to submit the Identity credential. As the identity credentials are usually issued by data source providers, the name by which it is registered as CIA or the name of CIA from whom it accepts the identity credential must be communicated to the mediator in the request. In response to ICRequest, the mediator sends the Identity Credential issued by specified CIA as ICResponse. If the user has not submitted the desired identity credential, then NULL value is sent as response.

   In the ICRequest, the first parameter is IC, the category Identifier for Identity credential, the second parameter is NULL and the name of CIA is the third parameter. The ICResponse contains either the Identity Credential or NULL.

   ICRequest: <IC, NULL, NameOfCIA>
   ICResponse: <Identity Credential> or *NULL*

3. Attribute Credential Request (ACRequest): The policy may require the value of some attribute. The attribute name is sent as the Attribute Credential Request. The mediator sends the attribute credential containing the desired attribute to the wrapper as Attribute Credential Response. If the user has not submitted any attribute credential containing the desired attribute, then NULL is sent as response. The ACRequest contains AC as first parameter, NULL as second parameter and the attribute name as third parameter. ACResponse consists of either the attribute credential or the NULL value.

   ACRequest: <AC, NULL, AttributeName>
   ACResponse : <Attribute Credential> or *NULL*

4. Standard Attribute Request (SARequest): The local policy requires a value of some attribute of some standard credential. The type of standard credential and the attribute name is sent as Standard Attribute Request. The mediator layer sends the value of desired attribute as Standard Attribute Response if the user has submitted the desired standard credential and is successfully verified else NULL.

The SARequest consists of SC as the first parameter, type identifier of standard credential SCTypeId as second parameter and the attribute name as third parameter. The SAResponse contains the value of desired attribute or NULL value.

SARequest = < SC, SCTypeId, AttributeName>
SAResponse =<AttributeValue> or *NULL*

3.3 Data Integration

Data integration provides an abstraction of the various data sources by mapping every data model. A unified global schema is generated and a common integrated global view of the data sources is presented to the user. Mapping between the local and the global schema is generated using GaV or LaV approach [4]. The main functionalities of data integration system are as follows:

- Connection Pooling

In the initialization or preparation phase every data source that wishes to join the system registers itself with the mediation system. The registration process involves sending the connectivity information [1,2] to the mediator. This information is used while sending the data access query received from user to various data sources.

- Schema Mapping

During the process of registration of data sources, the various data sources send their local schemas to the mediator. A unified global schema is generated from the various local schemas and a common integrated global view of the data sources is presented to the user. Mapping is generated between the local and the global schema. *Schema mapper* maintains a mapping table that contains information required to map global schema to local schema or viseversa. A user query is formulated in terms of the global schema. The *SubQGenerator* uses mapping table to translate the user query into multiple subqueries expressed in terms of the local schemas of the data sources.

A sample mapping table for NorthWind database would look like the one that follows:

Global schema	Local schema of Data Source1	Local schema of Data Source
Orders	*Orders*	*Order*
Orders.Employee	*Orders.Emp*	*Order.Empl*
Orders.Requireddate	*Orders.Reqdate*	*Order.Reqdt*

Table 1. Mapping table

For example the query received from GPE is like:
Select Orders.Employee, Orders.Requireddate from Orders;
The schema mapper uses the mapping table to modify the user query in the following manner:
For DS1: *Select Orders.Emp, Orders.Reqdate from Orders;*
For DS2: *Select Order.Empl, Order.Reqdt from Order;*

- Heterogeneity Handling

The various data sources could be heterogeneous in terms of query language they support for accessing the data. The query language heterogeneity is handled at wrapper level by maintaining the syntax tree of typical queries for different data sources. The *SubQConverter* converts the user query into the native language supported by each data source and the *ResConverter* converts the data model of the resultset to the exchange model of the system.

- Result Integration

Various wrappers send the resultsets received from data sources to the mediator. *ResIntegrator* uses *Schema mapper* to remap the local schema of various resultsets onto the global schema and integrates them into a single result set. The mediator sends the integrated result set to the user.

4. IMPLEMENTATION

A prototype system has been implemented for medical domain where the patient's data is distributed between two data sources. The data sources are heterogeneous in terms of the data model, the schema and the query language. One data source is realized as MySQL database and the other as XML repository. System is based on MVC architecture and is implemented using Java servlets. A single integrated view of the data sources is presented to the user and the user can submit the data access request prepared using global schema along with the set of credentials. In the current implementation it is assumed that the user is aware of the access control policy and thus can submit the desired credentials along with the data access request.

The credential based access control policies are defined at global level as well as at the two data sources. Access policy specification is in terms of various types of credentials like the identity credential, the attribute credential and the standard credential. The credentials are realized as X.509 v3 certificates. Java APIs have been used for implementing X.509 certificates. The access policies are stored in policy stores implemented as MS Access database. In the current implementation, access control is applied on viewing the data only. The multiple access control policies are applied on the same request and therefore when the outcome of global policy and the local policy conflicts, then the deny override approach has been used to calculate the final outcome.

Certificate Formats

The access control policies are defined in terms of various types of credentials and their attributes. These credentials are realized as X.509 v3 certificates. The format of the identity certificate is as shown in Figure 7 and is implemented as standard X.509 PKI certificate. In order to realize the attribute certificates, the extension field of X.509 certificate is used to store the various attributes associated with the subject. Attributes are name value pairs such as “Name = Alice”, “Company = IBM”, “Role = Manager”, etc. The format of the standard certificate is same as that of attribute certificate except that in addition to other attributes, it has one attribute called as Standard Certificate Type SCType.

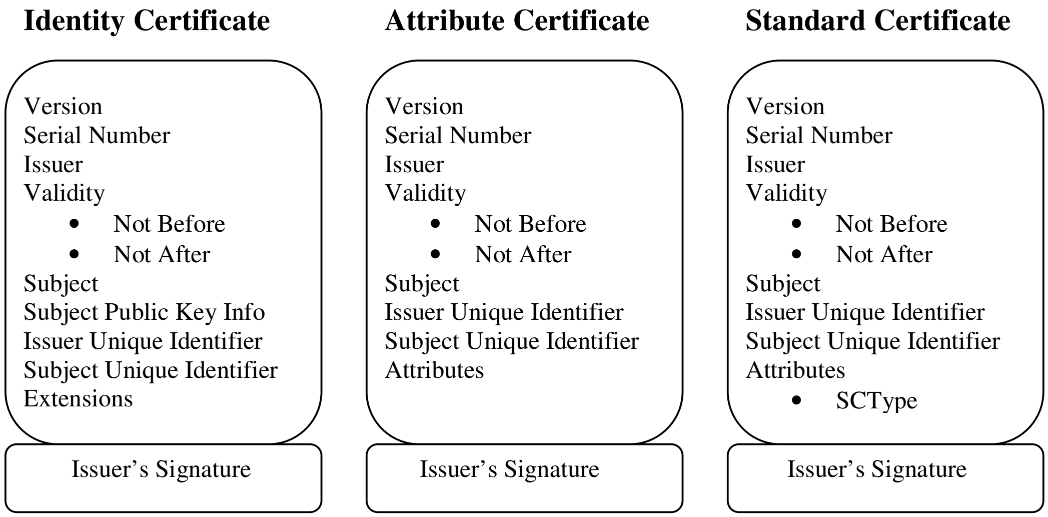

Figure 7: Certificate Formats

Schema mapping

Relational data model has been used as the data exchange model. Data query sent by user is converted to SQL at mediation layer and the SQL is converted into XQuery by the respective wrapper at XML data source. The GaV approach has been used to provide a common integrated global view over a set of local sources. Mappings are established between elements in the local sources and a similar element representing them in the global view. This mapping information is used to rewrite queries originating in the global view to queries that can be issued to the local sources.

Global view	*DS1 View*	*DS2 View*
Diagnosis	Case	Diagnosis
Test	Test	Investigation

Table 2 : Mapping between global view and various local views

4.2 Access Control Policy Specification

The global access control policy is defined at mediation layer whereas the local access control policies are defined by each data source at the source layer.

- Global access control policy(GACP):

GACP states that the *Diagnosis* and *Test* field can be accessed only by a registered Doctor.

Diagnosis, Test: Allowed by SC_Doctor

ARS

TId	*FId*	*ACRId*
Patient	Diagnosis	ACR1
Patient	Test	ACR1

ACR

ACRId	*SACRId*	*CrPartA*	*CrPartB*	*DsPart*	*EnvPart*
ACR1	SACR1	CPA1			

CrPartA

CPAId	*SCPAId*	*CrCatId*	*CrTypeId*	*Opd1*	*ROp*	*Opd2*
CPA1	SCPA1	SC	Doctor			

- Local Access Control Policy at DS2(LACP1):

LACP1 does not allow open access. Users carrying the identity credential issued by DS1 can access the *case* and *test* fields of their own patients only. This means only those records are accessible in which the UserId in the identity credential matches with the DoctorId field in the data source DS1.

Case, Test: Allowed by IC_{DS1} *where* IC_{DS1}*(UserId) = DS1(DoctorId)*

ARS

TId	*FId*	*ACRId*
Patient	case	ACR1
Patient	Test	ACR1

ACR

ACRId	*SACRId*	*CrPartA*	*CrPartB*	*DsPart*	*EnvPart*
ACR1	SACR1		CPB1		

CrPartB

CPBId	*SCPBId*	*CrCatId*	*CrTypeId*	*Opd1*	*ROp*	*Opd2*
CPB1	SCPB1	IC	NIL	UserId	=	DoctorId

- Local Access Control Policy at DS2(LACP2):

LACP2 states that a doctor having more than five years of experience of practicing medical profession can access the *Diagnosis* and *Investigation* fields. The attribute certificate containing the attribute *experience* has to be issued by Registered Medical Association (RMA).

Diagnosis, Investigation: Allowed by SC_Doctor and AC_{RMA}*(experience >= 5 years)*

ARS

TId	*FId*	*ACRId*
Patient	Diagnosis	ACR1
Patient	Investigation	ACR1

ACR

ACRId	*SACRId*	*CrPartA*	*CrPartB*	*DsPart*	*EnvPart*
ACR1	SACR1	CPA1			

CrPartA

CPAId	*SCPAId*	*CrCatId*	*CrTypeId*	*Opd1*	*ROp*	*Opd2*
CPA1	SCPA1	SC	Doctor			
CPA1	SCPA1	AC		experience	>=	5 years

5. CONCLUSION

Credential based mediation system for access control and data integration in multiple data sources environment has been presented in this paper. Mediation architecture has been enhanced to support credential based access control. The system is viewed as a single data source and the user gets a single integrated view of the data sources. Credential based access control is enforced at integrated level as well as at the local data source level. Multilevel access policy provides uniform access control across all data sources and also enables local data providers to have fine grained controlled access on their data sources. Access control policy defined in terms of various types of credentials enables open and immediate access to data integrated from heterogeneous data sources along with desired access on domain confined data. Access control conditions based on attributes associated with the credentials, data sources and the environment provides fine grained access control. A simple request-response based credential transfer protocol facilitates the transfer of credentials and various attribute values associated with them.

REFERENCES

[1] Li Yang, Mediation Security Specification and Enforcement for Heterogeneous Databases, Proceedings of the ACM symposium on Applied computing, 2005

[2] Li Yang, Security Enforced Mediation Systems for Data Integration, http://www.dcc.ufla.br/infocomp/artigos/v5.1/art01.pdf

[3] Li Yang, A Role-Based Access Control Model for Information Mediation, Proceedings of the IEEE International Conference on Information Reuse and Integration, 2004

[4] Mostafa Ezziyani, An Advanced XML Mediator for Heterogeneous Information Systems Based on Application Domain Specification, International journal of computer science and applications, vol 3, No. 2, June 2006

[5] Li Yang, Enhancing Mediation Security by Aspect-Oriented Approach, The 16th International Conference on Software Engineering & Knowledge Engineering, 2004

[6] S. Dawson, Secure Access Wrapper: Mediating Security between Heterogeneous Databases, Proceedings of DARPA Information Survivability Conference and Exposition, 2002

[7] Lillian Røstad, Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges, Proceedings of second international conference on Availability, Reliability and Security, 2007

[8] Ben Mbarka Moez, Control access policies for distributed resources, http://www.fisoft1.com/sources/master_report.pdf, 2007

[9] Linying Su, Automated Decomposition of Access Control Policies, Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks, 2005

[10] Vincent C. Hu, Access Control Policy Combinations for the Grid Using the Policy Machine, Proceedings of the Seventh IEEE International Symposium on Cluster Computing and the Grid, 2007

[11] Zahir Tari, Security Enforcement in the DOK Federated Database System, ACM digital library, 1997

[12] David Liu, CHAOS: An Active Security Mediation System, www.springerlink.com/index/qxeeyydyvy53xv2d.pdf, 2000

[13] Dan Lin, Policy Decomposition for Collaborative Access Control, Proceedings of the 13th ACM symposium on Access control models and technologies, 2008

[14] Sarbjeet Singh, Design and Evaluation of Policy Based Authorization Model for large scale Distributed Systems, http://paper.ijcsns.org/07_book/200911/20091107.pdf, 2009

[15] Nirmal Dagdee, Credential Based System for realizing Open and Domain confined accesses on Shared Data Source, International Conference on Data Management, Institute of management Technology Ghajiabad, India, Nanyang Technological University Singapore and University of Saskatchewan Canada, Feb 10-11, 2009

[16] Javier López, XML-based Distributed Access Control System, Proceedings of the Third International Conference on E-Commerce and Web Technologies, 2002

[17] Prasenjit Mitra, Privacy-preserving Semantic Interoperation and Access Control of Heterogeneous Databases, Proceedings of the 2006 ACM Symposium on Information, computer and communications security,2006

[18] M. Álvarez, FINDER: A Mediator System for Structured and Semi-Structured Data Integration, IEEE Computer Society Digital Library, 2002

[19] Awad M. Awadelkarim, An effective security interoperability archetype for secure multilevel databases, Asian Journal of Information Technology, Volume: 5, Issue: 4, Page No.: 418-428, 2006

[20] Isabel F. Cruz, An Interoperation Framework for Secure Collaboration among Organizations, Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, 2010

[21] D. Jonscher, Argos - A configurable access control system for interoperable environments, in Database Security, IX: Status and Prospects (eds. Spooner, D. et al.), Chapman-Hall, London, 43-60, 1995

[22] Sudhir Agarwal, Credential Based Access Control for Semantic Web Services, American Association for Artificial Intelligence, 2004

[23] Mary R. Thompson, Certificate-based Authorization policy in a PKI Environment, ACM Transactions on Information and System Security, Volume 6, Issue 4, pages: 566 - 588, 2003

[24] Mary Thompson, Certificate-Based Access Control For Widely Distributed Resources, ACM, Proceedings of the 8th conference on USENIX Security Symposium, Volume 8, 1999

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

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

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

[28] Dr. Nirmal Dagdee, Access control methodology for sharing of open and domain confined data using Standard Credentials, International Journal on Computer Science and Engineering Vol.1(3), 148-155, 2009

[29] Dr. Nirmal Dagdee, Policy architecture for credential based access control in open access environment, International Journal on Information Assurance and Security, 2010

[30] Jan Camenisch, Credential-Based Access Control Extensions to XACML, www.w3.org/2009/policy-ws/papers/Neven.pdf, 2009

[31] Ernesto Damiani, New Paradigms for Access Control in Open Environments, Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, Dec 2005

[32] Jan Camenisch, A Card Requirements Language Enabling Privacy-Preserving Access Control, ACM 2010

Authors

Dr. Nirmal Dagdee has earned his BE, ME and PhD degrees in Computer Engineering from Shri G.S. Institute of Technology and Science, Indore, India. His major research interests are in the fields of Service oriented computing, Data security and Soft Computing. He has authored several research papers that are published in reputed journals and conference proceedings. Presently, 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, Indore, India has around 19 years of experience in academics and software industry. She has done BE and ME in Computer Engineering and is pursuing Phd under the supervision 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.