ACCESS MODEL IN COOPERATIVE INFORMATION SYSTEMS

Preserving local autonomy with a global integration process

Eric Disson, Danielle Boulanger
MODEME Team, FRE CNRS 5055, Université Jean Moulin Lyon 3, 15, quai Claude Bernard 69007 Lyon, France

Keywords: Information Systems Security, Access Policies Heterogeneity, Access Model, Information Systems Federation, Cooperation.

Abstract: This research focuses on access security in cooperating information systems. The offered modeling has to treat the interoperation of open and evolutive information systems and, moreover, has to guarantee the respect of various local security policies. The coexistence of heterogeneous information sources within an information systems framework involves homogenization problems between local security policies. We distinguish two types of heterogeneity: heterogeneity of the local access policies and semantic heterogeneity between object or subject instances of the local access schemas. To solve this twofold difficulty, we propose an original role model allowing a unified representation of local access schemas. This model preserves the flow control properties in the three main access policies (discretionary, role-based model and multilevel models). The described access schemas are enriched to establish intra-system access authorizations.

1 INTRODUCTION

This research focuses on access security in cooperating information systems. The offered modelling has to treat the interoperation of open and evolutive information systems and, moreover, has to guarantee the respect of various local security policies.

Two main assumptions are taken in federated databases: autonomy and heterogeneity (Shet et al. 90). The first refers to the ability of the local database system to retain a most large degree of control over the aspects of the systems. Heterogeneity means that databases built on different schema designs and different data access models must be interconnected. The highest heterogeneity level is the semantic heterogeneity between local entities of the federation. An other heterogeneity problem is the difference between local organizational security methods (different schemas of user types and objects). Federated security systems must support both open and / or closed security axioms and logical access modes.

2 RELATED WORKS

Several approaches are used to define federated security models:

- using views and granting authorizations on the views to allow or prevent a global user to access information within a federation. In the Goyal's (Goyal 91) approach, access rules are used to authorize or deny the access to a global view.
- extending an existing access control model (such as DAC or MAC) to deal with the problems of autonomy and heterogeneity.

The CHASSIS (Configurable, Heterogeneous, And Safe, Secure Information Systems) project (Jonscher et al. 94) is a tight coupled system with discretionary access control and a right granting system. In tightly coupled systems, a federation authority exists and the federated database system has its proper access model. In case of conflicts, prohibitions override permissions. Access rights can be granted to individual users and to roles. Multiple role activation is controlled by an activation conflict relation. Several rules exist to infer implicit rights according to the data model. In this approach the global schema has more importance than local ones. Some other propositions (Olivier 94) use a multi-level access control but in a relatively compatible and homogeneous database system. In (Oliva 02) authors propose an other MAC model with the same

Disson E. and Boulanger D. (2004).
ACCESS MODEL IN COOPERATIVE INFORMATION SYSTEMS - Preserving local autonomy with a global integration process.
In *Proceedings of the Sixth International Conference on Enterprise Information Systems*, pages 259-266
DOI: 10.5220/0002610702590266

objective. But we think this access model is too constrained for the local systems to be use in an cooperative process. Several propositions (Sandhu 96) and (Sandhu 98) use a role-based access control model for DAC and MAC simulation in non federated systems but their approaches of access model heterogeneity are relevant for database federation security. The AMAC model uses both MAC and DAC models at the federated level (Pernul 93). It supports an automated labeling object system to compute large data queries in a federated system. These approaches have two limitations: the federated manager has a bad local security visibility and the sub-transaction (part of the global query) to a local system could be aborted later affecting the performance of the federated system; the lack of logical secured architecture do not permit how the federated security can be enforced.

One of the issues in the Distributed Object Kernel (DOK) (Tari et al. 97) is the development of a federated access control and a secured logical architecture. It allows the DOK system to enforce federated security policies in the context of autonomous, distributed and heterogeneous databases. The authors consider DAC and MAC access control. The federated level of the DOK system supports a bottom-up approach for access control: the Global Access Control (GAC) is derived from all the local security policies and ensures that no violation or overriding of local policies is possible. The DOK system is an open system: the federated access list for an aggregate is explicited as a union of the different security information defined in the local databases. If only one database allows the reading of the aggregate, according to global policies, the user has 'read access' to the required information.

Some propositions focus on security object similarity evaluation like (Castano et al. 97); the authors propose similarity criteria and associated metrics to compare security specifications of different applications. They consider security specifications according to a role-based model providing powerful authorization mechanisms suitable for similarity analysis. They use a set of basic criteria called affinity criteria (like synonymy, genericity…), some dictionaries of terms and roles, and a global similarity coefficient to compute the authorization affinity between two roles. They deal with the highest level of data semantic heterogeneity and not with the access model heterogeneity level.

Security in federated information systems is a critical issue. When a high security level is defined it often implies a tight coupling among local databases. Similarly, a loose coupling leads to local information sources autonomy and consequently to a poor global security level.

3 OUR APPROACH

To solve this twofold difficulty, we propose a three steps process to integrate a local system in the federation (see figure 1). At first, the local administrators define the exported schemas. An original "extended role model" allows a unified representation of local access schemas. This model preserves the flow control properties in the three main access policies (discretionary (Lampson 71), role based model and multilevel models (Bell et al. 76)). At the third phase of the integration process, the described access schemas are enriched to establish intra-system access authorizations.

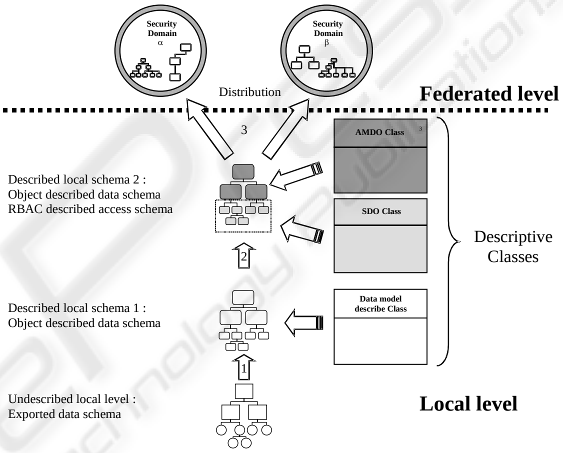
Security Domain α
Security Domain β
Distribution
Federated level
3
AMDO Class
3
Described local schema 2 :
Object described data schema
RBAC described access schema
SDO Class
2
Descriptive Classes
Described local schema 1 :
Object described data schema
Data model describe Class
1
Undescribed local level :
Exported data schema
Local level

Figure 1: The overall security incorporation process.

We propose a global framework dedicated to autonomous preexisting data sources cooperation provided with an acceptable security level based on a rich descriptive object oriented layer.

To constitute the descriptive layer we define metadata insuring an homogeneous representation of each local available information source (Boulanger et al. 98), (Boulanger et al. 00). The layer supports global queries treatment through Data Descriptive Objects (DDO) and Semantic Links (SemL). DDO and SemL are dedicated to the abstract description of the local data entities structure and the semantic links among them. For a given data model (relational, object, rule-based…) a set of DDO classes is defined to allow a description of the model as precise as required at the federated level. Thus for each local data entity a DDO is instantiated in the descriptive layer. To improve the expressiveness of the description, a set of SemL classes is also created (SemL are data model independent) to express semantic links among the data. It allows to implement inner links at the local level as well as inter-database links: semantic links like synonymy, hypernymy and hyponymy describe syntactic and conceptual equivalencies among the data entities. The obtained semantic network constitutes a knowledge base used for global imprecise queries processing.

We use a Role-Based Access Model (Disson et al. 01) to describe each local system at the global cooperation level. This model is enriched by specific metadata describing the data manipulation rights. We do not use the data definition rights and rights administration concepts in the global system with the loosely cooperation hypothesis. Such access rights are administrated only by the local data owners or “security officers”. RBAC models are efficient for simulating other access policies (Nyamchama et al. 96), (Sandhu et al. 96) and respect the loosely coupled cooperation hypothesis.

The local security items are modeled with two concepts. The security object (passive data entity) and security subject (active entity like user) are described with Security Descriptive Object (SDO) which are instantiated from SDO classes (Data, User…). The Application SDO class describes the general security strategy of the local system.

The local security authorization units like groups (DAC policies), roles (RBAC policies) or MAC “containers” (result of cartesian product between MAC category and MAC classification hierarchy of the local model) are described by Access Policy Descriptive Object (APDO).

The main objective of the flow control policy at the global level is to respect the local users’ profiles : a local user can read or modify federated information only if it is equivalent to local information on which he has such authorizations.

In each local information system the security manager must define the flow control policies adapted to the exchanges between the system and the federation. The import policy (input flow of the local system) is defined to be strict. It is a common feature that each local system must respect. The export policy (output flow of the local system) is either strict or liberal.

- Strict import policy: in our proposal, all the local systems adopt the same import access policy. At any time the following security axiom has to be valid: “for a given local user, the access to a global data must be equivalent to the access to a local data belonging to the local user’s profile”. A user profile is defined as a set of access rights to local objects. In our proposal the set of access rights is stored in the (one or more) roles which reference the proper User at the descriptive layer of the framework.
- Strict or liberal export policy: the export policy in a local system defines the way local data can be read from the federated level. In the case of a liberal export policy, the access requests from the federated level are automatically performed on local Security Objects. Access equivalencies defined among the DDO referenced in the User and the actual local data are used to verify the rights the user has on the concerned data. Access rules on the Security Objects related to the federated user predominate access rules defined at the local level.

  In the case of a strict export policy a first mapping allows to detect which Role of the local system corresponds to Roles related to the global user. Then a second mapping is performed to verify the correspondence of access rights related to the Security Objects referenced in the Role.

At last, we define a global trusted session respecting the import and export data policies between the federation and its various members. A solution to implement our object model of secured cooperation is also proposed.

4 THE DESCRIPTIVE CANONICAL MODEL

The figure 2 highlights our data and security canonical model. Successively we specify local access policy descriptive classes, local access schema descriptive classes and link classes.

Our objectives are:

- to represent local access schemas respecting different access policies (DAC, MAC, RBAC).
- to establish access equivalence between described schemas.
- to control the federated information flow with:
  - the respect of local user profiles.
  - the respect of local exportation policies (information flow from a local system to the federation).

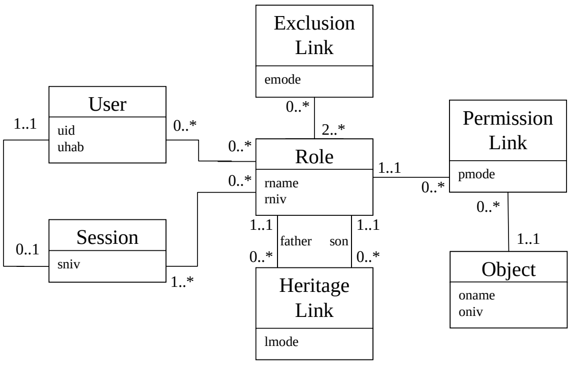

Figure 2: The canonical model (reduced version).

An Access Policy Descriptive Object is defined by the tuple < FID; LD; LAP; LAMT; LMT; {role} >. FID is the Federated Identifier of the local system; LD is the Local Designation. LAP is the Local Access Policy which can be chosen in the set { DAC; RBAC; MACS; MACL } with DAC for Discretionary Access Control (Lampson 71), RBAC for Role-Based Access Control, MACS and MACL for respectively mandatory model with strict I-property and mandatory model with liberal I-property (Bell 76). LAMT is the Local Access Mode Table and defines the correspondences between the local access modes and the federated access modes. The Local Mandatory Table (LMT) defines the correspondences between the local secrecy hierarchy level of a mandatory system and the federated secrecy level hierarchy. LMT attribute is null-valued in case of DAC or RBAC system description. {role} is a set of Roles which describe discretionary user group, role and mandatory category.

At the federated level we use five logical access modes: read-only (r), execute (x), append (a), upgrade (u) and delete (d) with r ^ x ^ a ^ u ^ d. Each local access mode is described by a federated access mode combination. For example, in Unix system the “write” access mode is described by the federated access mode combination a + u + d. All the local access mode descriptions are defined in the Local Access Mode Table.

The Local Access Mode Table contains the federated access mode combinations which is equivalent to each local access mode (mainly read-only and write-only local access modes). Then the Local Mandatory Table is created to translate the local secrecy level hierarchy.The dominate level is always the first. For example, a local system with the hierarchy of sensibility Non-Classified < Classified < Secret < Top Secret is described by the LMT {(Non-Classified; 1); (Classified; 2); (Secret; 3); (Top Secret; 4)}.

A Security Object represents a secured entity of the local access schema. A SO is defined by the tuple < FID; LD; ML; DDO >. FID is the Federated Identifier of the local resource. LD is the Local Designation. FSL is the Federated Sensibility Level. This attribute is null in case of DAC or RBAC model description. DDO is a referenced Data Descriptive Object. Each local secured data is described by one to n Security Objects and one Data Descriptive Object (see section 5).

A User Object describes a physical user of the local access schema. A User is defined by the tuple < FID; LD; FSL >. FID is the Federated Identifier of the local user. LD is the Local Designation and FSL, the Federated Sensibility Level. This attribute is null in DAC or RBAC model description.

A Permission defines the access mode combination the Subjects Descriptive Object of a given role is allowed to execute on one Security Object.

An Access Rule is defined by the tuple < so; m > with so, a SO reference and m, a federated access mode combination.

Our access model is a closed security system: all non-authorized accesses are forbidden.

A Role is used in two cases: to represent a local discretionary user group, or to extract each sensibility level of a local mandatory category.

A Role is described by the tuple < FID; LD; FSL; {Permission}; {User}; {AHL} {CLO}; {AELO} >. FID is the Federated Identifier of the described element. LD is the Local Designation of the described element. FSL is the Federated Sensibility Level. This attribute is null in case of DAC or RBAC model description. {Permission} is the set of Permissions which defines access modes to Security Object allowed for the Subject Descriptive Object. {AHL} is the set of Access Heritage Links. {CLO} is the set of Constraint Link Objects, and {AELO}, the set of Access Equivalent Link Objects (see the section 6).

An Access Heritage Link defines an access mode combination from a “father” role to a “son” role with the tuple < “father”; “son”; Mode > where “father” is the “father” role reference, “son” is the “son” role reference and Mode is a federated access mode combination that Subject Descriptive Objects of the “father” role are allowed to execute on all the Security Objects of the “son” role. A null Mode means that all SDO of the “father” role may execute Access Rules of the “son” role (complete access).

Two types of Constraints are used in our system:

An Exclusion Constraint Link Object (ECLO) references two or more roles. A User can be referenced in only one role in a set of roles which references the same ECLO (static constraint).

An Activation Constraint Link Object (ACLO) references two or more roles. For a given user session, the user actives only one role, in a set of roles which references the same ACLO (dynamic constraint).

5 A EXAMPLE OF MAC POLICY SCHEMATA DESCRIPTION

Mandatory security models govern the access to information by classifying the subjects and objects in the system (Bell et al. 76). Objects are passive entities storing information. Subjects are active entities accessing the objects. Generally, a subject is considered to be an active process operating on user's behalf. Mandatory access classes are associated with every object and subject in the system. A secrecy level hierarchy (with the relation "dominate") is used to qualify each object and subject (mandatory clearance).

Two axioms define access rules of a subject to an object (referenced in the same category):

- Read axiom: A subject with a mandatory clearance c can read all the objects with a secrecy level dominated by c.
- Write or I-property: A subject with a mandatory clearance c can write on all objects with a secrecy level strictly equal to c (strict I-property) on all objects with a secrecy level dominating c (liberal I-property).

Mandatory models can belong to three categories relatively to the security object granularity. In single-level mandatory models, the components of Security Objects (i.e. attributes in an object class or in a relational table) have the same secrecy level (Jajodia et al. 90), (Millen et al. 92). In our proposition, each mandatory object is described by one single SO (security description) referencing one DDO (data description). An attribute must have the same Mandatory Level as its class level. In multi-level mandatory models, attributes in an object class or in a relational table are mandatory objects. Their levels of sensibility can dominate or be equal to the level of sensibility of their classes / relational tables (Keefe et al. 90), (Lunt 90). Each mandatory object is also described by one single SO but in this case, Mandatory Levels of Attribute and classes / relational tables are not necessarily equal. In poly-instantiated multi-level mandatory models, instance attribute can be multi-valued. The attribute value captures the secrecy level equal to subject's clearance level (Denning 87). Each attribute is described by one DDO and n SO (SO have different Mandatory Levels); n is the secrecy level number in the local mandatory hierarchy of sensibility.

A local mandatory access system is proposed in six steps:

- A Local Model Descriptive Object describes the local access security policy. First the Local Access Mode Table is created and contains the federated access mode combinations which is equivalent to each local access mode (mainly read-only and write-only local access modes). Then the Local Mandatory Table is created to translate the local secrecy level hierarchy.
- For each local subject with a given clearance level cl, is created a User with secrecy levels. Ex: Mr. Smith has a clearance level "Secret" in a mandatory system with the LMT {(Non-Classified,1); (Classified;2);(Secret;3); (Top Secret;4)}. Mr. Smith subject is described by one User with the Mandatory Clearance 3.
- Security objects describing the local mandatory objects:
  Single level objects with a given secrecy level sl: is created one SO with a Mandatory Level equals to sl. The SO points to its related DDO.
  Poly-instantiated objects in a lattice-based access model: are created as much SO as there is secrecy levels in the local sensibility hierarchy. Each SO has a different Mandatory Level. All the SO reference a single DDO.
- For each local mandatory category is created as much roles as there is secrecy levels in the local sensibility hierarchy. The User (subject of the local mandatory category) having a Mandatory Clearance n is referenced in the role with a Mandatory Level n.
- Mandatory security axioms:
  Read axiom and strict I-property:
  For each role with a Mandatory Level n are created two permissions (with mode = a+u+d ≈ write and with mode = r for read) per SO referenced in the role.
  In a described local mandatory category, Access Heritage Links (with mode = r) bind each role of a given level n (dominant) with the role of the level n-1 (dominated) providing a descending read access heritage.
  Read axiom and liberal I-property:
  For each role with a Mandatory Level n is created two permissions (with mode = a+u+d ≈ write and with mode = r for read) per SO referenced in the role.

In a described local mandatory category, Access Heritage Links (with mode = r) bind each role of a given level n (dominant) with the role of the level n-1 (dominated) providing a descending read-only access heritage.

In a described local mandatory category, Access Heritage Links (with mode = a+u+d) bind each ROLE of a given level n (dominated) with the ROLE of the level n+1 (dominant) providing an ascending write-only access heritage.

The Figure 3 illustrates such a local mandatory model description. The local mandatory model is composed of:

- A local single-level mandatory policy with a liberal I-property (EX2 IS:APDO).
  The following Local Access Mode Table: Read (r) and Write (a+u+d).
  The local hierarchy of sensibility is Non-Classified (NC), Classified (C), Secret (S) and Top Secret (TP) with the dominate relation ">": TS > S > C > NC. The Local Mandatory Table is: 1. Non-Classified, 2. Classified, 3. Secret and 4. Top Secret.
- A mandatory category: Finance.

- The following Objects of the category Finance: Sales Result (NC), Salary (C), Account 105 (S), Financial Plan (TS)
  The subject Smith with “Secret” clearance level belonging to the category Finance.

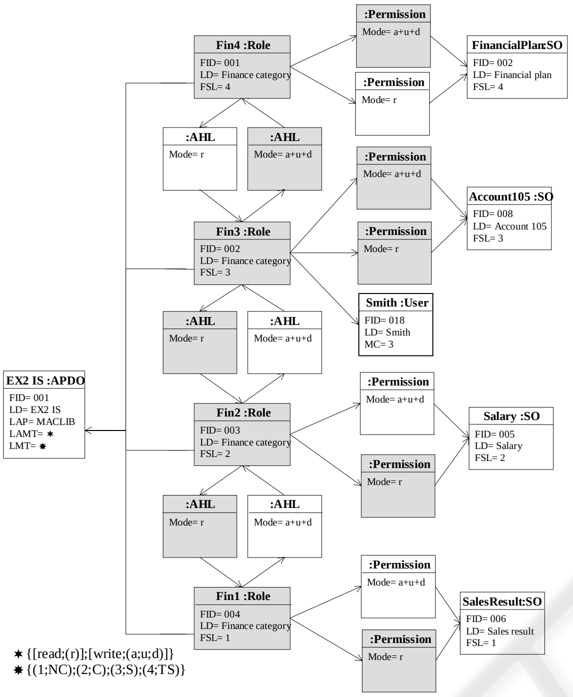

Figure 3 : An example of mandatory model description with liberal I-property.

The User 018 is created with Mandatory Clearance 3. The User is referenced in the right role.

- The “read” axiom is implemented by a descending access heritage (AHL with Mode = r). The liberal I-property is implemented by an ascending access heritage (AHL with mode = a +u +d). This heritage does not exist in a mandatory model with strict I-property.
- An Activation Constraint Link Object is referenced by the fourth role and forbids the simultaneous activation of the User "Smith".

This MAC schema description respects the MAC information flow acyclicity (see the grayed sensibility hierarchy of Mr. Smith’s session).

6 THE FEDERATED ARCHITECTURE

The global descriptive layer is composed of data description objects with access links and implements a flow control policy.

6.1 Access Bridge definition

For each data source involved in the federated information system a descriptive process is performed in order to create a semantic description of data at the federate level. All the knowledge intensive processes dedicated to global queries treatment and overall security setup use the data Descriptive Objects (DDO) composing the descriptive layer as the main resource for local data access.

Semantic links describe not only structural relationships among entities but also semantic links useful at the global level. With such links it is possible to enrich the data descriptive level allowing a higher level for reasoning processes about local information.

In our proposal the semantic descriptive layer is used by semantic evaluation functions. The semantic distance between two objects is given by the following formulae borrowed from the terminological description research field : SD = S(Nbi x Wi), with Nbi = Number of semantic links of type i linking the two objects in the global descriptive semantic net, and Wi = Weight of the link of type i. It is useful to give a weight to semantic links since a SemL type may be more or less important in a semantic evaluation. Semantic distance is mainly used when global security access equivalencies have to be defined in order to allow secured local data access by global user queries.

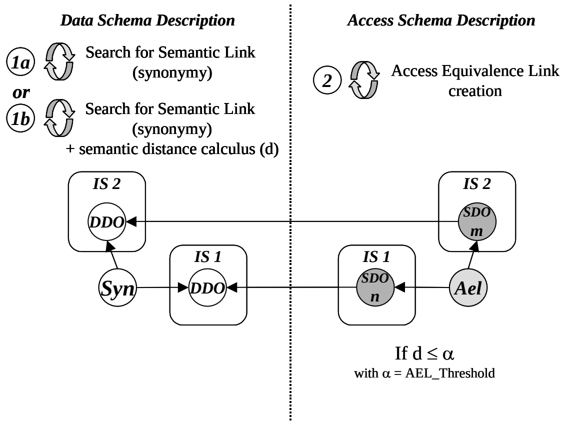
Data Schema Description
Access Schema Description
1a
Search for Semantic Link (synonymy)
or
1b
Search for Semantic Link (synonymy) + semantic distance calculus (d)
2
Access Equivalence Link creation
IS 2
DDO
IS 2
SDO m
IS 1
DDO
IS 1
SDO n
Syn
Ael
If d ≤ α
with α = AEL_Threshold

Figure 4: the AEL Creation Process.

The rules to define access equivalencies between SO and between ROLE belonging to different local systems are (see figure 4):

1- when a synonymy link exists between two DDO, an Access Equivalence Link (AEL) is instantiated and references the related SO.

2- we use a Semantic Distance (SD) to evaluate similarity between DDO belonging to a ROLE. The SD threshold (T) is given by the federated security officer. If SD>=T, an AEL is instantiated and references the two ROLE.

Equivalence links between ODS complete this procedure to control information flow (with the respect of local profiles) at the federation level.

The figure 5 (at the end of the paper) offers an example: at the federated level the global schema is designed by two schemas, a role based model describing an hospital organization and a DAC model describing a private clinic. The ODS are shadowed.

6.2 The federated flow control policy

In each local information system the security manager must define the flow control policies adapted to the exchanges between the system and the federation. The import policy (input flow of the local system) is defined to be strict. Each local system must respect it. The export policy (output flow of the local system) is either strict or liberal (see the figure 6).

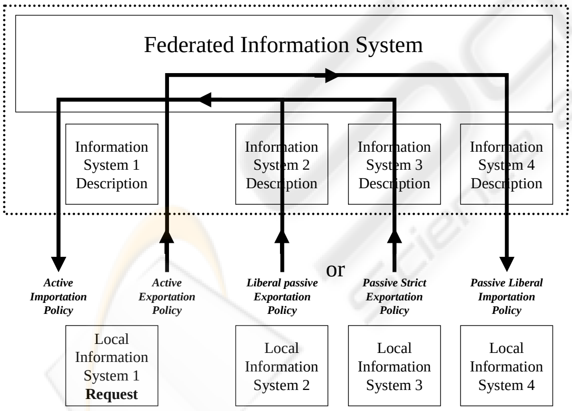
Federated Information System
Information System 1 Description
Information System 2 Description
Information System 3 Description
Information System 4 Description
Active Importation Policy
Active Exportation Policy
Liberal passive Exportation Policy
or
Passive Strict Exportation Policy
Passive Liberal Importation Policy
Local Information System 1 Request
Local Information System 2
Local Information System 3
Local Information System 4

Figure 6: The federated security policy.

Strict import policy: in our proposal, all the local systems adopt the same import access policy. At any time the following security axiom has to be valid: "for a given local user, the access to a global data must be equivalent to the access to a local data belonging to the user's local profile. A user profile is defined as a set of access rights to local objects. In our proposal the set of access rights is stored in the (one or more) Roles which reference the proper User at the descriptive layer of the framework.

Strict or liberal export policy: the export policy in a local system defines the way local data can be "son" from the federated level. In the case of a liberal export policy, the access requests from the federated level are automatically performed on local Security Objects. Access equivalencies defined among the DDO referenced in the User and the actual local data are used to verify the user's rights on the concerned data. Access rules on the Security Objects related to the federated user predominate access rules defined at the local level.

In the case of a strict export policy, a first mapping allows to detect which Role of the local system corresponds to Roles related to the global user. Then a second mapping is performed to verify the correspondence of access rights related to the Security Objects referenced in the Role.

7 CONCLUSION

It is obvious that security problems in federated loose coupled systems is a difficult issue when local autonomy data sources is respected, due to the dynamic evolution of local systems and the complex mappings required to yield various security models and policy interoperability. We have exhibited a proposal providing a secured framework for information systems cooperation. This proposal tries to give an appropriate answer to such complex problems by combining a dynamic description of local information sources and a global security policy derived from the local ones.

The originality is in the mix of (i) a federated architecture based on a rich descriptive layer composed of object oriented metadata and (ii) a role-based object model homogeneizing the local data access security schemas (discretionary and non-discretionary models).

Many questions are still in research phase: in particular further work is required to evaluate the impact of nested transactions during the query resolution process to the security framework. A validation phase for our description model is also necessary to be sure it can cover almost any local security policy at the local level.

REFERENCES

Bell D.E., LaPadula L.J., *Secure Computer System: Unified Exposition and Multics Interpretation*, Technical Report MTR-2997, MITRE Corp., Bedford, Mass, 1976.

Boulanger D., Disson E., Dubois G., *Object-Oriented Metadata for Secured Cooperation of Legacy Information Systems*, International Workshop on Model engineering IWME’00, Sophia-Antipolis and Cannes, France, 12-16th June 2000.

Boulanger D., Dubois G., *An Object Approach for Information System Cooperation*, Information Systems vol. 23, n°6, 1998.

Castano S., Martella G. and Samarati P., Analysis, comparison and design of role-based security specifications, Data & Knowledge Engineering 21, 1997.

Denning D.E., *Secure Distributed Data Views: the Sea View formal security model*, Technical Report A003 SRI International, 1987.

Disson E, Boulanger D., Dubois G., *A Role-Based Model for Access Control in Database Federations*, 3rd International Conference on Information and Communications Security, ICICS’01, Xian, China, 13-16 November 2001, LNCS 2229 Springer Verlag.

Goyal M.L., Singh G.V., *Access Control In Heterogeneous Database Management Systems*, Computers and Security, 10(7), North-Holland, 1991.

Jajodia S., Kogan B., *Integrating an object-oriented data model with multi-level security*, IEE Symposium on Security and Privacy, 1990.

Jonscher D., Dittrich K.R., *An Approach for Building Secure Database Federations*, Int.’l Conf. On Very Large Databases, Santiago, 1994.

Keefe T., Tsai W., *Prototyping the SODA Security Model*, Database Security III: Status and Prospects, North-Holland, 1990.

Lampson B.W., *Protection*, Princeton Symposium of Information Science and Systems. 1971.

Lunt T.F., *Multilevel Security for Object-Oriented Database Systems*, Database Security III: Status and Prospects, North-Holland, 1990.

Millen J.K., Lunt T.F., *Security for Object-Oriented Database Systems*, IEEE Symposium on Research in Security and Privacy, 1992.

Nyanchama M., Osborn S., *Modelling mandatory access control in role-based security systems*, Database Security VIII: Status and Prospects. Chapman-Hall, 1996.

Olivia M., Saltor F., Maintaining the Confidentiality of Interoperable Databases with a Multilevel Federated Security System in M. S. Olivier and D. L. Spooner (Eds). Database abd Application Security XV. Kluwer Academic Publishers, 2002.

Olivier M.S., *A Multilevel Secure Federated Database*, Database Security VII, North-Holland, 1994.

Pernul G., *Canonical Security Modelling for Federated Databases*, Interoperable Database Systems, North-Holland, 1993.

Sandhu R. S., Munawer Q., *How to do Discretionary Access Control Using Roles*, ACM Role-Based Access Control Workshop, 1998.

Sandhu R. S., *Role Hierarchies and Constraints for Lattice-based Access Controls*, Fourth European Symposium on Research in Computer Security, Rome, Italy, 1996.

Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E., *Role-Based Access Control Model*, IEEE Computer, Vol 29, n°2, 1996.

Shet A.P., Larson J.A., *Federated Database Systems for Managing Distributed Heterogeneous and Autonomous Databases*, ACM Computing Surveys vol.22 n°3, 1990.

Tari Z., Fernandez G., *Security Enforcement in the DOK Federated Database System*, Database Security X, 1997.

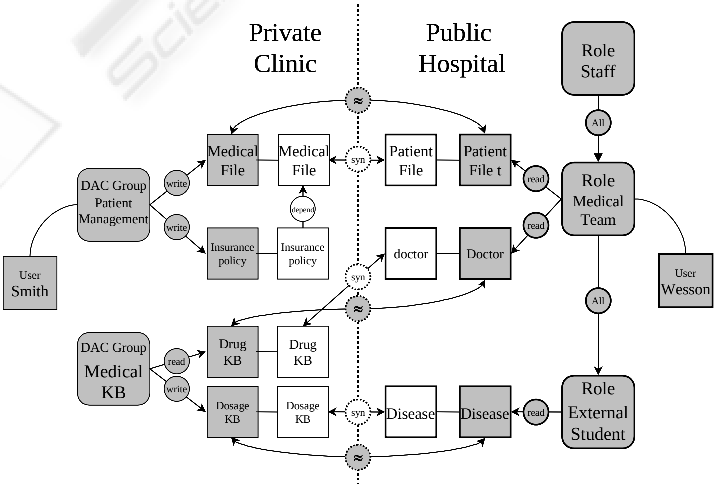

Figure 5: An example of Global Schema