Security Model for Federated Database Systems

Kavitha Juliet
Assistant Professor
Department of Computer Science & Engineering
RYMEC, Bellary

Abstract

One of the new emerging technologies for data management today is represented by federate systems. Security enforcement at the federation level must take into consideration the protection requirements and protection policies of each participating site. This task can be further complicated by the heterogeneity of the constituent systems, which may enforce protection policies either difficult to combine or inconsistent with each other. The need to share data in the federation on one side and to maintain site autonomy on the other side raises several protection requirements which traditional security models do not address. So this paper proposes the security model for federated database systems.

Keywords- Federated, access control, authorization

I. INTRODUCTION

A federated database management system(FDBS) integrates existing, possible heterogeneous databases while preserving their autonomy [1]. The need for federated database services has increased dramatically in recent years. Within enterprises, IT infrastructures are often decentralized as a result of mergers, acquisitions' and specialized corporate application resulting ion deployment of large federated databases. Perhaps more dramatically, the Internet has enabled new inter-enterprise ventures including Business-to-business Net Markets (or hubs) [2,3] whose business hinges on federating thousands of decentralized catalogs and other database. Broadly considered federated database technology [1] has been the subject of multiple research thrusts including schema integration [4,5], data transformation [6], federated query processing and optimization [7], transaction management [8]and security. Security and transaction management in FDBS have not been receiving, if not for few exceptions, much attention by the research [1]. However, many are the security issues that need investigation. The need to share data in the federation on one side and to maintain site autonomy on the other side raises several protection requirements which traditional security models [9, 10] do not address.

Security enforcement at the federation level must take into consideration the protection requirements and protection policies of each participating site. This task can be further complicated by the heterogeneity of the constituent systems, which may enforce protection policies either difficult to combine or inconsistent with each other. Moreover, local autonomy impacts the ability of the federation to acquire and replicate data or to make them available to others. A major problem in this context is also the establishment of administrative policies that determine the authority of the different federation participants for the specification of access authorization. As a matter of fact, while in a centralized or distributed system ownership or centralized administration may be satisfactory solutions. Federated systems call for more flexible approaches [11]. Enforcing complete strict ownership would put on the data owner the burden of specifying authorizations for federated users and therefore to maintain information on who can access the federation.

Applying a centralized administration approach at the federation level may imply a loss of control and therefore of autonomy, for the data owner. Moreover, even traditional problems such as authentication; require careful reconsideration in the federated context.

This paper proposes a security model for federated database systems. Section 2 discusses the related work. Section 3 describes the proposed model.

II. RELATED WORK

Some research has addressed the problem of protecting federated systems [12, 13, 14] and few federated systems like Mermaid [15], Orion-2[16], or the one proposed by Heimbigner or McLead[17] support some form of authorization specification and access control, several issues still remain to be investigated.

Security in federated database is very complex because a large set of users with extraordinary diverse security requirements expect to use a pool of component databases containing data of varying sensitivity. Therefore, we propose a federated security model that is necessary to express and enforce the security policies.

Some approaches have been developed for the federated access control. Goyal Singh's [18] approach uses access rules to check whether or not the user may access a view. Jonscher and Dittrich [19] use a DAC model to enforce federated security policy. A mapping of access rights to local components is provided and a user is granted global access rights unless local rights are not

available. In this approach, federated security policies have priority over local ones-the federation manager has been "given trust" to authenticate user. Pernul[20] proposes the AMAC model, which offers a supporting policy for automated security labelling because due to the large amount of data in FDBS, manual security labelling of subjects and objects is almost impossible. These approaches are useful in the context of distributed and heterogeneous environments. All these approaches have one major limitation that the federation managers lack of knowledge of local security requirements. Due to the autonomy of local databases, local security requirements have to be understood by a federated manager in order to control, optimize and delegate sub transactions to the local databases.

III. PROPOSED MODEL

The proposed security model for federated database system overcomes these difficulties by providing a uniform expression of heterogeneous security information which can be reliably used by the manager to invoke (or abort) federated transaction. In the proposed model agents are responsible for the enforcement of local and federated security policies. The different security agents enable understanding of local security policies. The proposed model also decides who is responsible to handle federated security policies and how these can be enforced. In a federated environment, the design of security procedures is very important as it can affect the usability of federated system. The proposed model as in figure 1 considers the following security issues:

A. Authentication and Access Control

A good user's authentication is a prerequisite for a correct access control. The identity of a user determines the groups to which the user belongs, the roles he can play (if applicable), and ultimately the privileges he is allowed to exercise. In federated systems, access to data can be seen at two different levels: at the federation level, where users explicitly require to access the federated data, and at the local level, where the local requests corresponding to the global requests must be processed. Access control may possibly be executed at both levels. Traditional approaches for authorization and access control in computer systems (i.e., discretionary [21], mandatory [21], and role-based access controls [21]) are not appropriate to address the requirements of federated systems, and that proper authorization and access control requires infrastructural support in one way or another. So, we propose an access control model for federated systems that integrates the best features of traditional models.

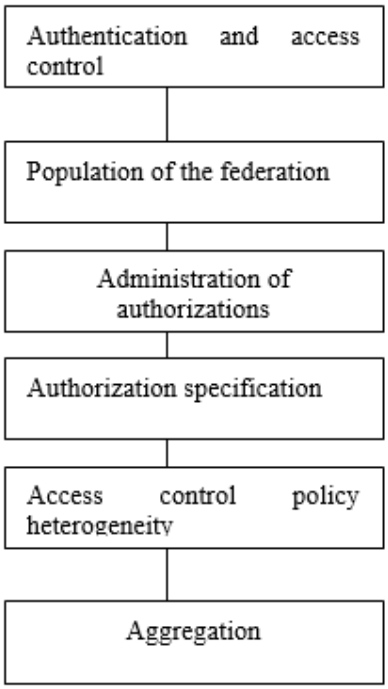

Fig. 1: Proposed security model for federated database systems

B. Population of the Federation

Populating the federation means defining the objects that are part of the federated schema. Population of the federation can be done in two ways: by directly creating objects in the federated database, or by importing objects from the local sites taking part into the federation. Direct creation of objects in the federated database can be executed by either the federation administrator or any user explicitly authorized for that. Import of objects from local sites is instead more complex, since it requires agreement between the local administrators of the objects and the federation administrator. The local administrator of an object must be willing to share the object with the federated users. The federation administrator must be willing to include the object among the federated data. This negotiation process can be required only at the time a site enters in a federation. In this case, users can then be allowed to

directly insert their objects and federation administrators directly allowed to import the objects. Alternatively, the negotiation process can be carried out through different steps as follows. First, local users declare the objects they wish to share with the federation, thus defining a sort of export schema from which the federation administrator can get data. This operation allows simply declaring data which are available to the federation but it does not include them in the federated schema and does not have any effect on it. Second, the federation administrator imports objects into the federation by getting them from the export schemas. This approach has the advantage that negotiation can be enforced at the granularity of each single object, and even for each specific access mode. It therefore allows users to selectively share their objects and federation administrators to selectively import objects in the federation. The fact that both the object's and the federation's administrator must agree in order for an object to be inserted in the federation also represents a guarantee to both of them with respect to the protection of the information they manage. The proposed security model implements these approaches.

C. Administration of Authorizations

A major issue that arises after the federation has been populated is who should administer access on the federated objects, i.e., who should specify authorizations to exercise privileges on them. As for objects directly created in the federation, classical administrative policies applied in centralized systems can be considered. For instance, the administration can rest with the federation administrator (centralized administration) or with the user who created the object (ownership). The proposed model discusses some of the methods to choose the best one.

D. Authorization Specification

In federated database systems authorizations can be specified at two different levels: at the federation level (on the federated data) and at the local level (on the objects exported to the federation). The proposed model gives an approach for the specification and coexistence of global and local authorizations.

E. Access Control Policy Heterogeneity

Besides the different forms of heterogeneity at the system or at the data model level, which may impact enforcement of security measures, a further kind of heterogeneity may need to be consider: access control policy heterogeneity. With this expression we refer to the case where the different local sites enforce different access control policies. Beside heterogeneity in the specific elements of the authorization model, heterogeneity can also concern the regulation policies governing access to the data at the different sites. "Meta policies" may then need to be defined that coordinate the enforcement of the different security policies [22].

F. Aggregation

Aggregation which is not easy to control in centralized environment, become even more difficult in federated systems, where data from different, autonomous systems are collected together to form the federated data. The. The situation can therefore be where users who are authorized to access each single component should not. be given access (or should be given only partial access) to the federated data. The increased sensitivity of the federated data may be due to global policies which are unknown to the single components. For example, federal laws exist that control the computer matching of data among the different federal agencies [23]. Although users can access separately the databases at the different federal agencies, they must not, be allowed to match data among them. The federated system must therefore enforce this global policy if local sites may not even be informed about it. The proposed architecture gives an approach to this aggregation problem.

IV. CONCLUSION

Federated systems represent one of the new emerging technologies for distributed database management and organization. These systems are characterized by the fact that while the component systems cooperate and share their resources they also must maintain their autonomy and a good degree of control over their data and resources. Moreover, component systems can be heterogeneous with respect to different aspects of the system. These characteristics raise several interesting issues regarding the specification and management of authorizations and the enforcement of access control. In this research we propose a model for security that comprise authorization, access control, administration and aggregation. The different security agents enable understanding of local security policies. The proposed model also decides who is responsible to handle federated security policies and how these can be enforced. In a federated environment, the design of security procedures is very important as it can affect the usability of federated system. In the future the proposed model will be implemented with service oriented architectures (SOA).

REFERENCES

[1] A. Sheth and J. Larson. Federated database systems for managing distributed, heterogeneous, and autonomous databases. ACM Computing Surveys, 1990.
[2] Net market makers inc. http://www.netmarketmakers.com, 1999
[3] L. Knight. "the e-market maker revolution", dataquest inc. http://www.netmarketmakers.com/documents/perspective1.pdf, 1999.
[4] C. Batini, M. Lenzerini, and S. B. Navathe. A comparative analysis of methodologies for database schema integration. ACM Computing Surveys, 1986.
[5] R. J. Miller, L. M. Haas, and M. A. Hern´andez. Schema mapping as query discovery. In VLDB, 2000.
[6] S. Abiteboul, S. Cluet, T. Milo, P. Mogilevsky, J. Sim´eon, and S. Zohar. Tools for data translation and integration. IEEE Data Engineering Bulletin, 1999.
[7] Amol Deshpande Joseph M. Hellerstein Decoupled Query Optimization for Federated Database Systems, IEEE Data Engineering Bulletin 2002

[8] Yuri Breitbartt, Hector Garcia-Moli, Avi Silberschatz Overview of Multidatabase Transaction Management The VLDB Journal, 1992
[9] R S Sandhu and P Samarati access control: principles and practice.IEEE communication pages2-10 September 1994.
[10] S Castano, M G Fugini, G Martella and P Samarati Database Security-Addison Wesley,1995.
[11] P Samarati E bertino and S jajodia An authorization model for a distributed hypertext system. IEEE transaction on knowledge and data engineering, 555-562, August 1996.
[12] T Holrigl, F schell, S suelmann, H harten stein, Towards Systematic Engineering of Service –Oriented Access control in Federated Environments
[13] Sabrina, P samarati, access control in federated systems,ACM 1997.
[14] Matthew Morgenstern, Teresa F. Lunt, Bhavani Thuraisingham, and David L. Spooner. Security Issues in Federated Database Systems: Panel Contributions. In C. E. Landwehr and S. Jajodia, editors, Database Security, V: Status and Prospects, IFIP, pages 131-148, 1992
[15] M. Templeton, E. Lund, and P. Ward. Pragmatics of Access Control in Mermaid. In IEEE-CS TC Data Engineering, pages 33-38, September 1987.
[16] Worn Kim, Nat Ballou, Jorge F. Garza, and Darrel Woelk. A Distributed Object-Oriented Database System Supporting Shared and Private Databases. ACM Transactions on Ofice Information Systems, 9(1):31-51, January 1991.
[17] D. Heimbigner and D. McJ,eod. A Federated architecture for Information Management. A CM Transactions on. Ofice /71fo7mr~ti071 Systems. 3(3):253-278. 1985
[18] M.L. Goyal and G.V. Singh, ªAccess Control in Heterogeneous Database Management Systems, º Computers and Security, vol. 10, no. 7, pp. 661-669, 1991.
[19] D. Jonscher and K.R. Dittrich, ªAn Approach for Building Secure Database Federations, º Proc. Int'l Conf. Very Large Database (VLDB), pp. 24-35, 1994.
[20] G. Pernul, ªCanonical Security Modelling for Federated Database, Interoperable Database Systems, D.K. Hsiao, E.J. Neuhold, and R. Sacks-Davis, eds., pp. 207-222, 1993.
[21] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. IEEE Computer 1996;29(2):38e47
[22] IIilary H. Hosmcr Mullipolicy Paradigm Il. In Procfrifings oj the Sew Securil,q Paradigm.s Workslrop, Lit,t.le compton, R.I., Sept,enlber 1992.
[23] T.F. Lunt, ªAggregation and Inference: Fact and Fallacies, º Proc. IEEE Symp. Research in Security and Privacy, 1989.