

Towards Secure Mediation

Joachim Biskup Ulrich Flegel Yücel Karabulut

Fachbereich Informatik, Universität Dortmund
August-Schmidt-Straße 12
D-44221 Dortmund, Germany
{biskup | flegel | karabulu}@ls6.cs.uni-dortmund.de

Abstract

A secure mediated information system should support scenarios where dynamically changing information sources advertise their information resources, and application specific mediators collect and assemble these resources into useful information in order to support the requests of their spontaneous clients. While doing this, the mediators should enforce security constraints in the application environments. In this paper, we compare mediated information systems with federated database systems with respect to design issues and security issues in order to clarify the different motivations of both systems. Furthermore, we present our secure mediated querying protocol using the concepts of credentials for authentic authorization. We also highlight some multimedia specific security requirements and mechanisms.

1 Introduction

Current advances in communication technologies led to increasingly interconnected systems. As the core technologies stabilize and performance allows for higher traffic volumes, extensive on-line information providing becomes feasible. Information suppliers apply a variety of heterogeneous systems. Convenient information retrieval and integration from several information sources represents one of the emerging and challenging demands of today's users. Information providers, particularly those with a commercial background, appreciate facilities to handle a dynamic legion of potential clients, or rather customers.

Diverse approaches to interoperable information systems have undergone substantial research. Nowadays these systems are categorized as federated database systems and mediated information systems. Both kinds constitute more or less independent intermediary components trying to satisfy broad client queries involving a multitude of information sources. The general design issues for those components are characterized in section 2.1.

While in this context most security related research results focus on resolving heterogeneity issues in federated database systems, work on security in mediated

information systems recently also becomes available. In section 2.2 you also find a discussion of the security requirements in both approaches.

As we focus on mediated information systems, in section 3 we give an overview about our proposed protocol for secure information acquisition via mediators. Such a protocol is not only required to deal with heterogeneity and autonomy of information providers, but also with various aspects of security, such as confidentiality, authenticity and integrity, as well as anonymity and others.

Modern information supply tends to comprise mixtures of multimedia parts. The different features of these media raise varying security issues, some of them being discussed in section 4.

We conclude with an overview of requirements met by our protocol and an outlook on future research in our mediator project.

2 Federated database systems versus mediated information systems

While both federated database systems and mediated information systems are used to integrate various autonomous information sources, several differences between both approaches may be identified. In the following subsections we will discuss the differences related to and affecting design issues and security issues of both approaches.

2.1 Differing design requirements

The differing motivations between both approaches influence strongly the design styles of them. In the following we discuss the design styles of both approaches and clarify the differences between federated databases and mediators.

2.1.1 Design issues in federated database systems

Federated database architectures [15, 31, 21] have been developed to provide interoperation among multiple heterogeneous databases. The main difference between the federated system concept and distributed system concept is that each information source of the federated system remains autonomous with respect to design, communication, execution, association and authorization [19]. Autonomy means that the local administrator of each information source maintains control over his/her system. There are two types of federated databases: the *tightly-coupled* and the *loosely-coupled*, where we only consider the former one. Federated database systems require the construction of a global schema integrating the information source schemas. Semantic heterogeneities among participating component databases are resolved at the global scheme level. The federation administrator is responsible for creating and

maintaining the federation. The common global schema captures the union of data available in the federation. After the global schema is specified, queries can be submitted against it and are transparently decomposed into subqueries for appropriate information sources. Using this kind of federation, one can realize the benefit of locally maintained data but globally executed queries. In order to provide the interoperability, a common canonical data model is used for the global schema. Building a global schema is a *bottom-up* procedure. Firstly, each local information system has to extend its schema to the uniform (canonical) data model of the federation. This makes the local information systems appear as if they were too from the same data model of the federation. Secondly, the global schema is specified on top of the extended schemas of local information sources. Finally, the federation administrator defines the application views to the global schema.

2.1.2 Design issues in mediated information systems

In contrast to federated database system concept, mediators [38] are developed in a *top-down* procedure. A mediator is a system that supports a mediated (integrated) view over multiple heterogeneous information sources. Mediators can be considered as specialized global views.

The behaviours of mediators tends to be different from federated database systems. While the latter are based on a static, bottom-up derived global schema, the former are intended to treat the heterogeneity problems more dynamically. Mediators work with a top-down designed application oriented schema which is dynamically augmented with wrappers at connection time of sources and which is prepared to resolve remaining mismatches during query processing.

Mediators provide via wrappers [36, 37] access to information sources and only integrate those parts of the underlying information sources that are crucial for the user's query. Wrappers can be realized using distributed object managers such as CORBA [25] or software agents [14, 1].

Some current projects on mediation are TSIMMIS [35], HERMES [33], Information Manifold [20], SIMS [4], AURORA [40], DISCO [34], Squirrel [16], DIOM [22], Garlic [10], OBSERVER [24], InfoSleuth [5], and MMM [7, 8, 2]. There also appeared some contributions to security in mediated information systems [9, 39, 18].

The mediators may use different approaches to support the schema, e.g. materialized, virtual, and hybrid [8]. The *materialized* approach retains in the persistent store of the mediator all relevant and worthwhile information (results from the previous queries), such as attribute values of an object. If attribute values are subsequently needed for further queries they can be simply fetched, and thereby avoiding their possibly time and resource consuming recomputation. This is a very important feature, if the queries have to be answered from multiple multimedia information sources. In the *virtual* approach the attribute values must be determined from external items

by means of a communication each time they are accessed. The *hybrid* approach materializes only part of the relevant information. It means that some of the attribute values are available both by fetching the mediator's persistent storage and by querying the external items.

Some of the commonalities and the differences between federated database systems and mediated information systems are visualized in Figures 1 und 2.

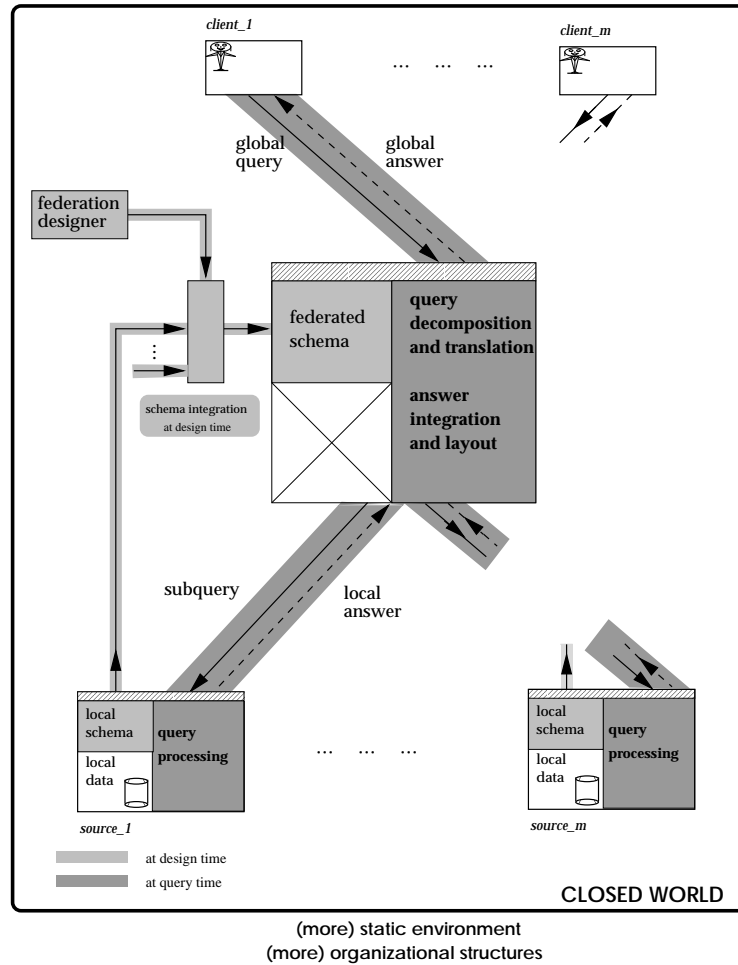


Figure 1: Design of federated database systems

2.2 Differing security requirements

Most interesting in the context of this paper are differences related to and affecting security issues of both approaches. We first observe that many of the differences result

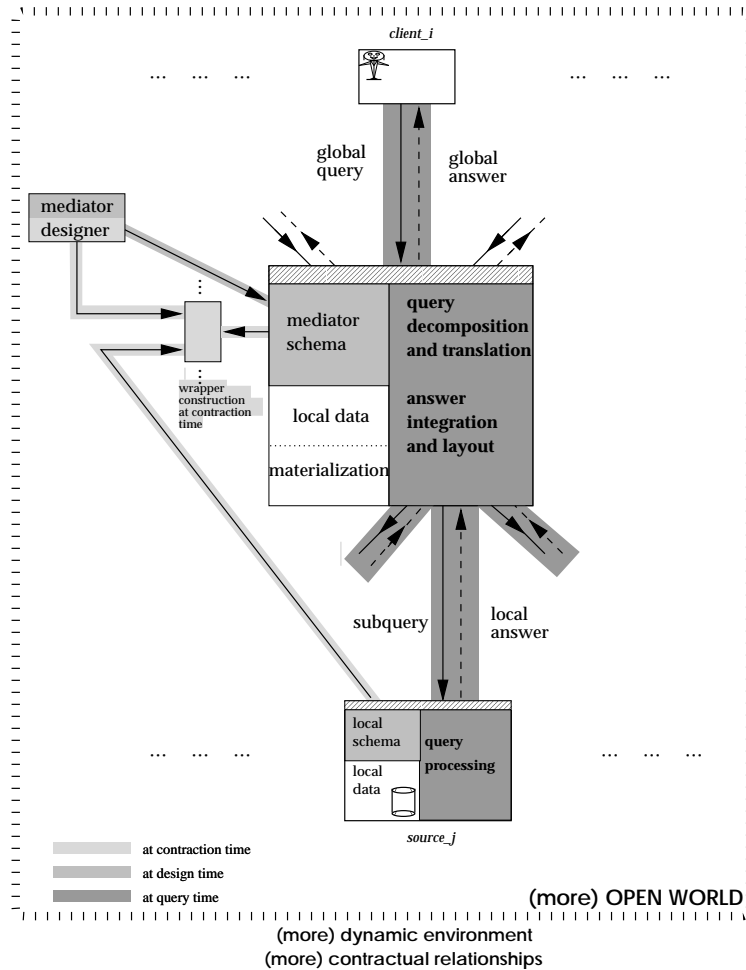


Figure 2: Design of mediated information systems

from differing motivations of participants of federated and mediated environments, respectively.

2.2.1 Security issues in federated database systems

In a federated system the federation establishment is stimulated by the members of the information source organization in order to support a closed group of client users. In many cases the client group is part of the organization which supports its interactions by means of the federation. Furthermore there exist dependencies between clients and information sources due to their identical organizational origin. The information sources of a federation act in a common interest anchored in the organization they belong to. This network of dependencies probably has had significant impact

on specific security architectures as often found in federated database systems.

As mentioned above, the information sources directly belong to a holding organization and therefore are trusted. Most federated database systems do not authenticate information sources in a client-verifiable way. The methods used to integrate information sources at the federation layer often involve administrative interaction, which takes place before client queries can be accepted. This suggests, that the set of information source layer members is rather static than dynamic. Under the assumption of a closed world the static nature of this approach leads to temporary loss of service when one or more information sources, which hold information relevant to a client's query, are unavailable.

Opposed to information sources the federation clients are not trusted and require proper authentication and authorization. Because clients normally are members of the federation's organization, there is a closed group of registered users. New users are assigned predefined roles but some systems also support anonymous client accesses.

2.2.2 Security issues in mediated information systems

The motivation to integrate information sources using mediators is quite different. Clients demand systems enabling them to effectively work with heterogeneous information sources. This demand stimulates information sources to supply their information on an ad-hoc basis, in particular for purchase. Information sources are likely to meet the client's requirements and to cooperate with mediators. Like in a marketplace of demand and supply there exist different motivations for cooperation in each layer. Generally clients, information sources and mediators are independent of each other. Information sources exist in competitive and non-competitive relationships with other information sources. Obviously there is no base for mutual trust between arbitrary participants of a mediated information system.

While information sources probably will have cooperation contracts with mediators, it can be assumed that spontaneous clients are unknown beforehand. Clients thus cannot be registered in a static way with specific sources or mediators before their queries can be accepted. Even the group of information sources probably will not be as stable as found in federated database systems due to the lack of organizational associations in mediated information systems. Though one or more information sources may be temporarily unavailable a client query can be satisfied. There apparently is no useful assumption of a closed world in mediated information systems due to their dynamics.

2.2.3 A case for mediated information systems

Table 1 summarizes some of those key differences between federated and mediated approaches, which also affect security considerations. Obviously both approaches are

	<i>federated approach</i>	<i>mediated approach</i>
interoperability stimulated	by members	by spontaneous clients
relationship between participants	organizational	contractual
trust between participants	high	low
design	bottom-up	top-down
information sources	static	dynamic
union of source data	= all relevant data (closed world)	\subseteq all relevant data (open world)
data at the integration layer	virtual	hybrid
clients	static	spontaneous & dynamic

Table 1: Federated vs. mediated approach

destined for quite different fields of employment. We believe that mediated information systems are more suitable to model dynamics and low trust of interacting parties. A mediator’s top-down design paradigm allows for a stable presentation schema of integrated information at varying degrees of source fluctuation, whereas a bottom-up approach requires a redesign of the global integration schema each time a local schema changes or is added. Mediators strive for tolerance with respect to information provider failures and offer service to ad-hoc clients which have not registered with the supplier beforehand. The latter forbids deployment of merely identity based identification approaches as traditionally used in federated database systems.

3 Secure mediated querying protocol

A secure mediation environment is based on a public-key infrastructure and digital credentials [11, 28, 17]. In this environment clients have to provide evidence that they are eligible for requested information, and sources have to maintain mechanisms to inspect such evidence and to decide whether and which information is delivered.

We assume that there are trusted third parties (TTPs), trusted by all participants of a transaction, that signs a *credential* of the rough form

$$\langle \text{attribute, public (encryption) key, public (verification) key} \rangle,$$

thereby assuring the *attribute* specified by the first component is enjoyed by the owner of the matching secret keys for decryption and signing.

Given this basic informational environment, we can specify our basic secure mediation protocol as introduced in [6]. We distinguish a preparatory phase and a query phase.

In the *preparatory phase*, clients and sources do not yet interact. A client, wishing to request information later on, assembles *credentials* with his attributes supposed to provide evidence of his eligibility.

And a source, entitled to answer queries later on, defines a *security policy* with respect to confidentiality which relates sets of attributes to the amounts of information allowed for delivery. As input, the source security policy accepts an arbitrary set of credentials belonging to a unique owner. For instance, this is the case if all occurring public encryption keys are the same. It is important to observe that it is not necessary for the source to know the identity of that owner. Only based on the set of attributes included in the credentials, the policy states which kind of information is allowed to be delivered to the owner.

The protocol for the *query phase* is illustrated in Figure 3 and outlined as follows.

Protocol for secure mediated query answering: In the query phase we distinguish a request phase and delivery phase:

Request phase:

- a) A client sends a request including a global query and a set of credentials to a mediator.
- b) The mediator decomposes the global query into a set of subqueries, where each subquery is supposed to be appropriate for a certain source.
- c) The mediator sends the subquery and the received set of credentials (or an appropriate subset of it) to each corresponding source.

Delivery phase:

- d) Each relevant source verifies each credential, checks whether the set of credentials is acceptable, i.e. belong to a unique owner.
- f) Each relevant source determines the associated set of attributes.
- g) Each relevant source evaluates its subquery under the restriction that only such information is generated that, on the basis of the associated set of attributes, is allowed to be delivered.
- h) The result of the restricted query evaluation is considered as plaintext and encrypted with (some of) the public key(s) occurring in the shown credentials.
- i) Each relevant source sends its encrypted local answer back to the mediator.

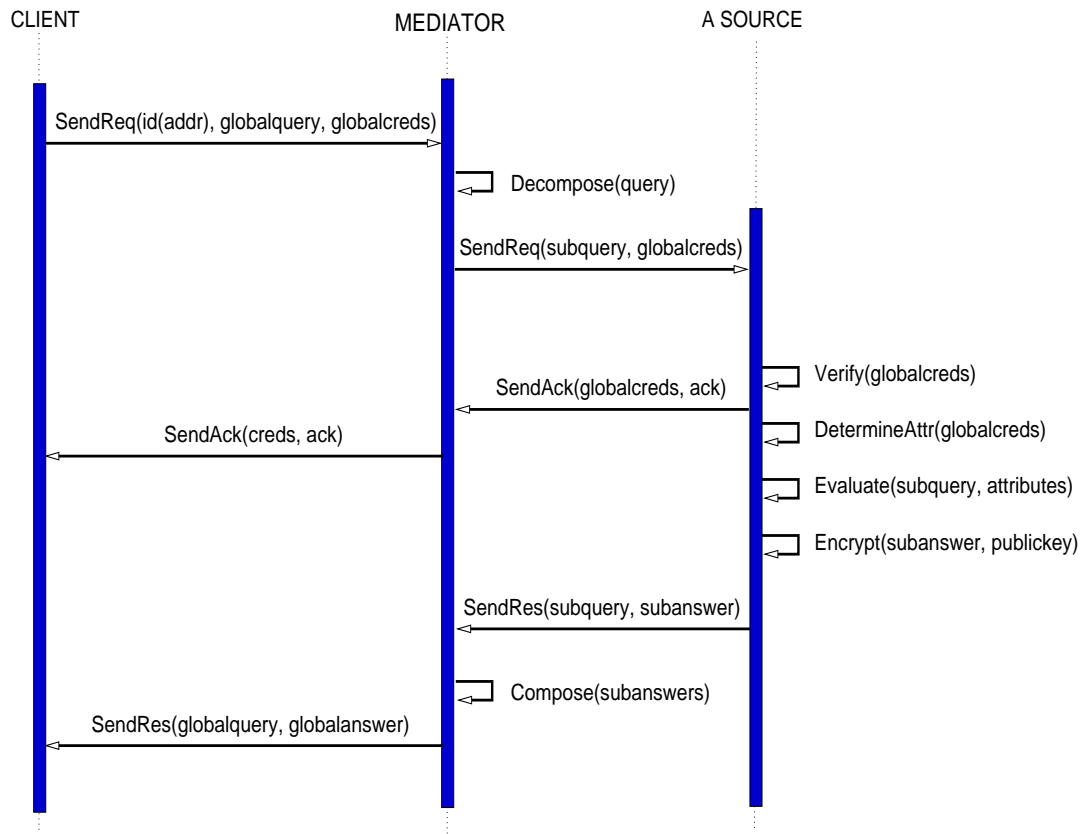


Figure 3: Protocol for secure mediated querying

- j) The mediator integrates the received local answers into a global answer and delivers it to the client.

The secure mediation protocol satisfies the following security properties:

- Clients, sources and mediator exclusively have to trust the TTPs that signed credentials.
- Sources are supposed to have an interest in checking eligibility which is supposed to be definable in terms of attributes. Thus, for instance, data subjects, the data of which is stored in a source, have to trust the source with respect to checking eligibility appropriately.

- A client can stay anonymous with respect to a source, since in general there is no need for a direct connection between the client and a source.
- Even in an untrusted network, only the unique owner of the verified credentials can recover the plaintext and thus gains the requested information.
- We observe some minor restrictions in the secure mediation protocol. The mediator acquires knowledge about the client's credentials and thus could give raise to false blames about the sender of a request. In a dispute about the sender of the request nobody can exhibit any essential evidence pro or contra the blame. If there is an interest in documenting the sender of a request, the protocol must be extended by appropriately signing the request.
- Further concerns about authenticity or requirements on integrity could be dealt with by additional actions that are based on appropriate signing.
- In particular, if a source is concerned about a client redistributing received data without the source's approval, the source can fingerprint [26] the delivered copies of the data.
- There are no specific provisions or additional obstacles to availability.

However, there are important observations dealt with in an advanced secure mediation protocol presented in [6]:

- The mediator has to integrate and possibly materialize the local answers, sent back to the mediator by the sources to be finally delivered to the client. The functional requirements on the mediator may be seriously affected, because the mediator possibly can not perform the expected operations on the ciphertexts for integrating local answers. In [6] we propose some pessimistic and optimistic solutions to this problem.
- In the secure mediation protocol presented above the mediator just forwards the received set of credentials to each of the relevant sources. A client may wish to present a minimal set of credentials to each source and thereby specify a desired level of quality with respect to the global answer. So, the mediator may assist a client in the management of credentials. Other aspects with respect to credential management are presented in [6].

Another important aspect is related to the secure query evaluation by the mediator. For this goal we intend to use a unified model of query evaluation and role based security enforcement [29, 30]. This issue is also explained in [6] in some detail.

4 Further topics for multimedia extensions

The acceptance of new multimedia communication services depends on whether suitable techniques for the protection of the multimedia providers' interests are available. In the following we would like to mention some multimedia specific security requirements and mechanisms.

Encryption of multimedia data: Multimedia applications need fast encryption mechanisms, handling up to tens and even hundreds of Mbit/s. Symmetric stream ciphers seem to be the most suitable option, and nowadays still hardware implementations are necessary [13].

Normally, data compression must be performed before encryption, which itself must be performed before channel coding. This is not true in some applications for digital TV broadcasting [23]. Macq and Quisquater show in [23] the interest in developing new approaches, in which the secure coding is developed as combination of channel coding and cryptographic coding. [27] and [23] have shown that the encryption of images and videos differs from the encryption of text files due to various reasons.

It should also be possible to encrypt arbitrary areas of images. Different keys for different encrypted image parts may be used. This could be useful in the cases where different users are not allowed to see some parts of an image [32].

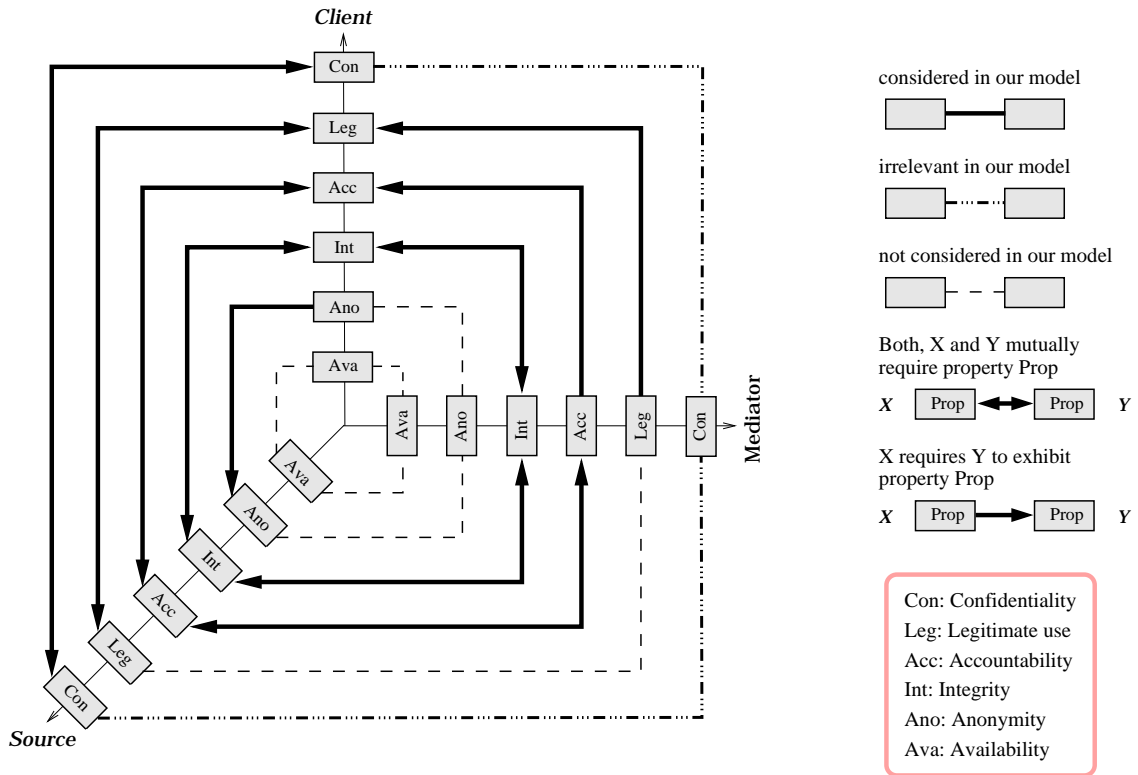
Image compression and encryption: An image compression algorithm can be modified such that its output can be decomposed into several parts [12]. The encryption process classifies each part into two types: the crucial parts and the remaining parts. The crucial parts contain the significant information about the original image. The remaining parts yield negligible information if the crucial parts are unknown. Only the crucial parts need to be encrypted. The remaining parts are left unencrypted and can be sent on demand. The concepts discussed in [12] can also be adopted to mediated information system environments.

Claim of origin: A limiting factor in using multimedia communication services is that providers of multimedia data are reluctant to allow the distribution of their documents in a networked environment because of electronic piracy.

Robust digital watermarking [3] and fingerprinting [26] represent sufficient deterrents, since they enable identification of source, owner, distributor or authorized consumer of digitized images, audio and video recordings. A digital watermark or a fingerprint is an identification code, permanently and imperceptibly embedded into digital data, carrying information pertaining to copyright protection and data authentication. A copyright protection code can contain a copyright notification, a unique serial number, a creator identifier, a distributor identifier, as well as other data attributes.

5 Conclusion

This paper has presented the flavour of a secure mediation environment. We addressed the different design styles and security requirements stemming from different motivations of participants in both federated and mediated environments. Within the secure mediation environment outlined in our work, clients seeking information and autonomous sources holding data can communicate with each other via mediators while complying with their security requirements. We mainly have focussed on the security requirements concerning confidentiality and authenticity. Our approach makes a specific contribution towards secure interoperation by combining the credential based authentic authorization with some kind of anonymity and of asymmetric encryption for confidentiality. Additionally, we have highlighted some multimedia specific security requirements and mechanisms.



Many security requirements such as accountability imply a requirement for authenticity.

Figure 4: Mutual security requirements of the participants in a mediated information system environment

Figure 4 illustrates which mutual security requirements of participants are covered by our concepts represented in [6]. We distinguish between two groups of security

requirements. In the first group two participants mutually require a security property. For example, the requirement with respect to integrity must be fulfilled by both the mediator and the client. So, both of them wish digitally signed messages from each other. In the another group only one participant wishes a property to be fulfilled by other participant. For example, the mediator wants a client to show her credentials to check whether she is a legitimate user or not.

There are a number of promising areas for future work. First, there is a need for the mechanisms presented to be actually applied to emerging applications and to evaluate whether the mechanisms cover the specific requirements of those applications. Such research could reveal new kinds of security problems. For this reason we began to realise some of our concepts in a software prototype which is to be implemented in a student project.

Another area for further research is to investigate the tradeoff between efficiency and security in the context of materialization. This also is a promising research area for data warehousing applications. Typically, warehouses contain static collections of materialized views of multiple data sources with differing security policies.

Since our Multimedia Mediator (MMM) [7, 8] bases on CORBA [25], there is a need to explore the applicability of our approaches in the CORBA communication environment.

A final area of research would be to refine and formalize the model of role based query evaluation.

References

- [1] Knoblock C. A. and J. L. Ambite. Agents for information gathering. In J. M. Bradshaw, editor, *Software Agents*. MIT Press, Cambridge, 1997. <http://www.isi.edu/sims/knoblock/info-agents.html>.
- [2] C. Altenschmidt, J. Biskup, J. Freitag, and B. Sprick. Weakly constraining multimedia types based on a type embedding ordering. In *Proc. 4th Int. Workshop on Multimedia Information Systems*, pages 121–129, Istanbul, Turkey, September 1998.
- [3] R. Anderson, editor. *1st International Workshop on Information Hiding*, LNCS, Cambridge, England, April 1996. Springer-Verlag.
- [4] Y. Arens, C. A. Knoblock, and W. Shen. Query reformulation for dynamic information integration. *Journal of Intelligent Information Systems*, 6(2-3), 1996.

- [5] R. J. Bayardo et al. InfoSleuth: Agent-based semantic integration of information in open and dynamic environments. In *SIGMOD'97*, pages 195–206, Tucson, AZ, USA, May 1997.
- [6] J. Biskup, U. Flegel, and Y. Karabulut. Secure Mediation: Requirements and Design. In *12th Annual IFIP WG 11.3 Working Conference on Database Security*, Chalkidiki, Greece, July 1998.
- [7] J. Biskup, J. Freitag, Y. Karabulut, and B. Sprick. A mediator for multimedia systems. In *Proc. 3rd Int. Workshop on Multimedia Information Systems*, pages 145–153, Como, Italia, September 1997.
- [8] J. Biskup, J. Freitag, Y. Karabulut, and B. Sprick. Query evaluation in an object-oriented multimedia mediator. In *Proc. 4th Int. Conf. on Object-Oriented Information Systems*, pages 31–43, Brisbane, Australia, November 1997. Springer Verlag.
- [9] K. S. Candan, Sushil Jajodia, and V. S. Subrahmanian. Secure mediated databases. In Stanley Y. W. Su, editor, *12th International Conference on Data Eng.*, pages 28–37, New Orleans, Louisiana, USA, February, March 1996. IEEE, IEEE Computer Society Press.
- [10] M. J. Carey et al. Towards heterogeneous multimedia information systems: The Garlic approach. In *Proceedings of the Fifth International Workshop on Research Issues in Data Engineering(RIDE): Distributed Object Management*, pages 123–130, L. A., California, 1995.
- [11] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985.
- [12] H. Cheng and X. Li. On the application of image decomposition to image compression and encryption. In Patrick Horster, editor, *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, pages 116–127, Essen, Germany, September 1996. Chapman & Hall.
- [13] E. Crusselles et al. Secure communications in broadband networks. In *Proceedings of the 3rd International Conference on Telecommunication Systems*, pages 114–122, Nashville, Tennessee, USA, March 1995.
- [14] M. Genesereth and S. Ketchpel. Software agents. *Communications of the ACM*, 37(7):48–53, July 1994.

- [15] D. Heimbigner and D. McLeod. A federated architecture for information management. *ACM Transactions on Office Information Systems*, 3(3):253–278, July 1985.
- [16] R. Hull and G. Zhou. A framework for supporting data integration using the materialized and virtual approaches. In *ACM SIGMOD'96*, pages 481–492. ACM, Montreal, Canada, June 1996.
- [17] IETF SPKI Working Group. SPKI certificate documentation. <http://www.clark.net/pub/cme/html/spki.html>, 1998.
- [18] Sushil Jajodia, Pierangela Samarati, V.S. Subrahmanian, and Elisa Bertino. A unified framework for enforcing multiple access control policies. In *SIGMOD'97*, pages 474–485, Tucson, AZ, USA, May 1997.
- [19] Dirk Jonscher and Klaus R. Dittrich. An approach for building secure database federations. In *Proceedings of the 20th international conference on very large databases*, pages 24–35, 1994.
- [20] A. Y. Levy, A. Rajaraman, and J. J. Ordille. Querying heterogeneous information sources using source descriptions. In *Proceedings of 22nd International Conference on Very Large Data Bases VLDB'96*, pages 251–262, Mumbai (Bombay), India, September 1996. Morgan Kaufmann.
- [21] Witold Litwin, Leo Mark, and Nick Roussopoulos. Interoperability of multiple autonomous databases. *ACM Computing Surveys*, 22(3):267–293, September 1990.
- [22] L. Liu and C. Pu. Distributed interoperable object model and its application to large-scale interoperable database systems. In *Proceedings of ACM International Conference on Information and Knowledge Management (CIKM'95)*, 1995.
- [23] B. Macq and J.-J. Quisquater. Cryptology for digital TV broadcasting. *Proceedings of the IEEE*, 83(6):944–957, June 1995.
- [24] E. Mena, V. Kashyap, A. Sheth, and A. Illarramendi. Observer: an approach for query processing in global information systems based on interoperation across pre-existing ontologies. In *First IFCS International Conference on Cooperative Information Systems (CoopIS'96)*, Brussels, Belgium, June 1996.
- [25] Object Management Group. The common object request broker, architecture and specification, revision 2.0. <http://www.omg.org/corba/corbiop.htm>, July 1995.

- [26] Birgit Pfitzmann and Michael Waidner. Anonymous fingerprinting. In *Euro-Crypt'97*, LNCS, Berlin, 1997. Springer-Verlag.
- [27] RACE Concertation. *Conditional Access Workshop, 44th RACE Concertation Meeting*, Brussel, November 1994.
- [28] R. L. Rivest and B. Lampson. A simple distributed security infrastructure (SDSI). <http://theory.lcs.mit.edu/cis/sdsi.html>, 1998.
- [29] Ravi Sandhu. Role hierarchies and constraints for lattice-based access controls. In Elisa Bertino, Helmut Kurth, Giancarlo Martella, and Emilio Montolivo, editors, *ESORICS '96*, pages 65–79, Rome, Italy, September 1996. Springer-Verlag.
- [30] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. Role-based access control models. *IEEE Computer*, 2:38–47, 1996.
- [31] Amit P. Sheth and James A. Larson. Federated database systems for managing distributed, heterogeneous, and autonomous databases. *ACM Computing Surveys*, 22(3):183–236, September 1990.
- [32] D. Storck and E. Koch. Controlable user access on multimedia data in world wide web. In *Proceedings of the International Conference on Image Science, Systems, and technology (CISST'97)*, pages 270–278, Las Vegas, Nevada USA, June-July 1997.
- [33] V. S. Subrahmanian, S. Adali, A. Brink, R. Emery, et al. HERMES: Heterogeneous reasoning and mediator system. Submitted for publication. <http://www.cs.umd.edu/projects/hermes/>.
- [34] Anthony Tomasic, Louiqa Raschid, and Patrick Valduriez. Scaling heterogeneous databases and the design of DISCO. In *Proceedings of the International Conference on Distributed Computer Systems*, Hong Kong, 1995.
- [35] Jeffrey D. Ullman. Information integration using logical views. In *Proceedings of the 6th International Conference on Database Theory, ICDT'97*, LNCS, pages 19–40, Delphi, Greece, 1997. Springer-Verlag, Berlin.
- [36] D. Wells. Wrappers: Survey. http://www.isse.gmu.edu/I3_Arch/index.html, 1996.
- [37] G. Wiederhold. I3 (intelligent integration of information) glossary. <http://www-db.stanford.edu/pub/gio/1994/vocabulary.html#value>, 1995.
- [38] G. Wiederhold and M. Genesereth. The conceptual basis for mediation. *IEEE Expert, Intelligent Systems and their Applications*, 12(5):38–47, Sept.-Oct. 1997.

- [39] Gio Wiederhold, Michel Bilello, and Chris Donahue. Web implementation of a security mediator for medical databases. In T. Y. Lin and Shelly Qian, editors, *Database Security XI: Status and Prospects, Proceedings of the 11th Annual IFIP WG11 Working Conference on Database Security*, pages 60–72, Lake Tahoe, California, 1997. IFIP, Chapman & Hall.
- [40] L. L. Yang, T. Özsu, and L. Liu. Accessing heterogeneous data through homogenization and integration mediators. In *Second IFCIS Conference on Cooperative Information Systems (CoopIS-97)*, Charleston, South Carolina, June 1997.