Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 179 (2007) 97–109

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Secure Information Sharing in a Virtual Multi-Agency Team Environment [1]

Nabil Adam,[2] Ahmet Kozanoglu,[3]
Aabhas Paliwal[4] and Basit Shafiq[5]

CIMIC, Management Science & Information Systems
Rutgers University
NJ, USA

Abstract

This paper proposes a two tier RBAC approach for secure and selective information sharing among virtual multi-agency response team (VMART) and allows expansion of the VMART by admitting new collaborators (government agencies or NGOs) as need arise. A coordinator Web Service for each member agency is proposed.The coordinator Web Service is responsible for authentication, information dissemination, information acquisition, role creation and enforcement of predefined access control policies. Secure, selective and fine-grained information sharing is realized through the encryption of XML documents according to RBAC policies defined for the corresponding XML schema.

Keywords: XML, RBAC, Virtual Team, Access Control, Information Sharing, SOA, Web Services

1 Introduction

In the context of homeland security, one of the key challenges is achieving effective, timely and systematic collaboration and information sharing among various government agencies at the Federal, state, and local levels. Given the sensitive nature of the information, it is critical that information sharing be based on relevance and security. A majority of the agencies are using the Web as a means for sharing related information, that exists in different forms, and increasingly utilizing XML to represent this information. In case of a crisis, a virtual response team needs to be formed in an ad-hoc manner. Members of this virtual response team come from various government agencies and private organizations. Depending on several factors,

[1] This work is supported in part by the National Science Foundation under grant IIS-0306838

[2] Email:adam@cimic.rutgers.edu

[3] Email:ahmetk@cimic.rutgers.edu

[4] Email:aabhas@cimic.rutgers.edu

[5] Email:basit@cimic.rutgers.edu

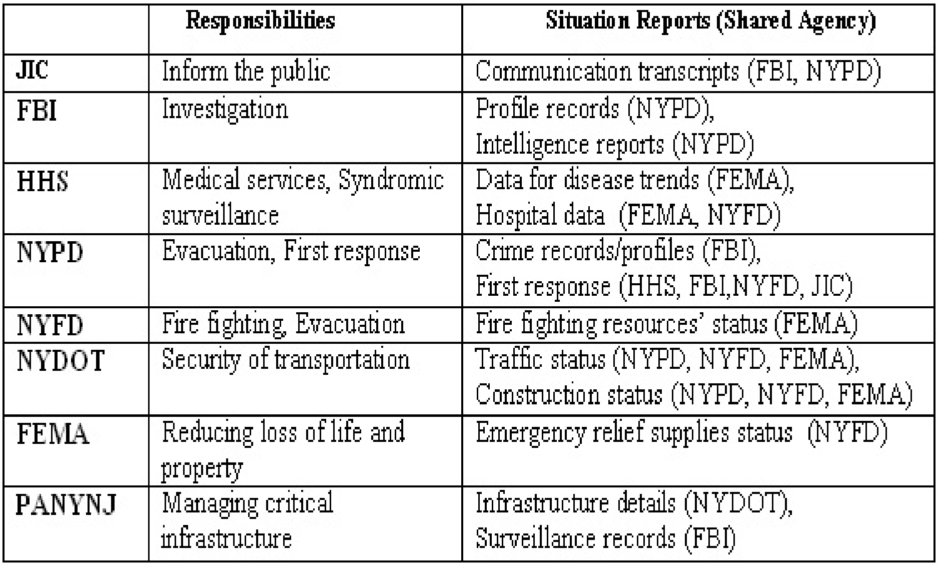
doi:10.1016/j.entcs.2006.08.034

including the location and nature of the crisis, the composition of this virtual multi-agency response team may change from one crisis to another. Furthermore, during the course of a given crisis the membership of this virtual multi-agency response team (VMART) may change dynamically to accommodate various needs (e.g., public health versus fire) and to conform to certain constraints, such as jurisdictions, e.g., the crisis extends, initially from New York to New Jersey.

Members of the VMART are both information providers and consumers. As an information provider, an agency will send information, e.g., situation report, to the rest of the team as soon as it is created. As this information is ”pushed” to the various agencies, there is a need to be concerned about access to this sensitive information both at the agency level (inter-agency) as well as within a given agency (intra-agency).

At the inter-agency level, each agency that is member of the VMART fulfils a certain role and, accordingly, gains access to certain information that is necessary to discharge its duties and fulfill its responsibilities within the overall efforts. For example, the public health agency would need to have access only to information related to public health, whereas FBI may need access to other related information that is different from the information needed by the public health agency. Due to the dynamic nature of the environment, a situation may arise where there is a need to admit an agency, that was not a part of the overall predefined set of agencies, as a member of the VMART. For example, as a certain crisis evolves, the Department of Homeland Security (DHS) might find it necessary to include the State Department as a member of the current VMART. In this case, DHS should be able to assign the State Department an appropriate role together with matching permissions that enable the State Department to fulfill its function in the overall efforts. Clearly, in this case, the DHS can not grant permissions, to the State Department, that they themselves do not own. At the intra-agency level, each of the agencies, that make up the VMART, has its own complex security policy. In addition, within each of these agencies there are individuals who perform a certain role (e.g., chief, first responder), possess different credentials and have different levels of access permissions that match their duties and their roles within the agency. Adherence and enforcement of these distributed policies that determine, who can access what information and at what level of granularity?, (e.g., the entire situation report, or only the part of the report that pertains to public health) are essential in order to ensure effective inter-agency and inter-governmental response. Our problem can be stated as follows. Given the environment described above, there is a need to provide each member of the VMART with automated capability to distribute to other members of the VMART only those portions of the generated information that are deemed relevant. In this paper we will limit our focus to information represented as an XML document with an underlying schema.The paper is organized as follows; section 2 discusses a motivating scenario. Section 3 provides our approach. In section 4, we detail the system architecture. Section 5 discusses related work. Section 6 includes our conclusion and future work.

Table 1
Agencies, responsibilities and situation reports



	Responsibilities	Situation Reports (Shared Agency)
JIC	Inform the public	Communication transcripts (FBI, NYPD)
FBI	Investigation	Profile records (NYPD), Intelligence reports (NYPD)
HHS	Medical services, Syndromic surveillance	Data for disease trends (FEMA), Hospital data (FEMA, NYFD)
NYPD	Evacuation, First response	Crime records/profiles (FBI), First response (HHS, FBI,NYFD, JIC)
NYFD	Fire fighting, Evacuation	Fire fighting resources' status (FEMA)
NYDOT	Security of transportation	Traffic status (NYPD, NYFD, FEMA), Construction status (NYPD, NYFD, FEMA)
FEMA	Reducing loss of life and property	Emergency relief supplies status (NYFD)
PANYNJ	Managing critical infrastructure	Infrastructure details (NYDOT), Surveillance records (FBI)

2 Motivating Example

As a motivating example, consider a scenario where there several explosions in various parts of New York and assume that the following agencies constitute the initial VMART.

(1) JIC (Joint Information Center), (2) FBI (Federal Bureau of Investigation), (3) HHS (Health & Human Services), (4) NYPD (New York Police Department), (5) NYFD (New York Fire Department), (6) NYDOT (New York Department of Transportation), (7) FEMA (Federal Emergency Management Agency), and (8) PANYNJ (Port Authority of New York and New Jersey)

Based on its responsibilities, a given agency may generate a set of situation reports. Table 1 lists the different types of situation reports shared among different agencies. Once a situation report is generated by a given agency, certain portions of the report need to be shared with various members of the team. Based on its responsibilities, a given agency may generate a set of situation reports. Table 1 shows examples of such situation reports. Once a situation report is generated, certain portions of the report is shared with members of the team.

3 Proposed Approach

Our approach builds on SOA that facilitates effective assimilation, and sharing of information that is vital for homeland security wherein it is important for agencies to communicate in a decentralized environment. The identification of proper tasks and agencies that can accomplish the tasks is followed by the dynamic discovery of resources and applications needed for achieving these tasks utilizing the

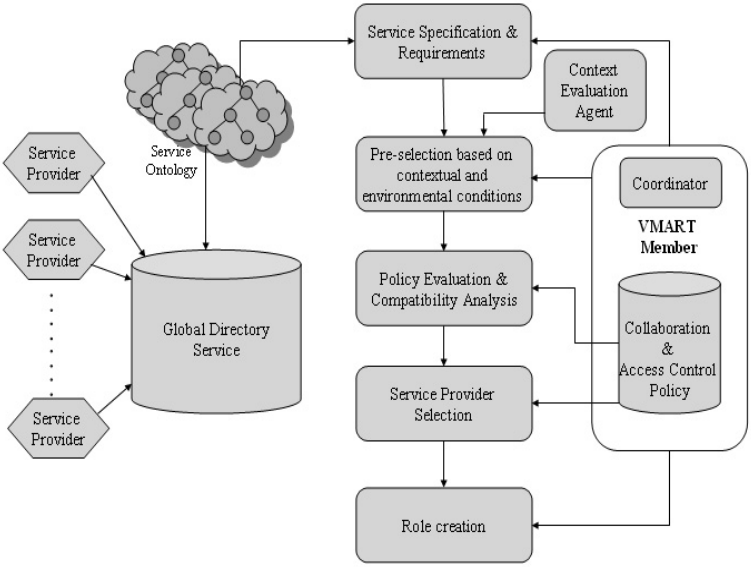

Service Specification & Requirements
Context Evaluation Agent
Service Ontology
Service Provider
Service Provider
Service Provider
Pre-selection based on contextual and environmental conditions
Coordinator
VMART Member
Global Directory Service
Policy Evaluation & Compatibility Analysis
Collaboration & Access Control Policy
Service Provider Selection
Role creation

Fig. 1. Proposed service oriented framework in the VMART environment

SOA. Putting the information and tasks together manually jeopardizes the timely response to a crisis. SOA provides an automated way to identify and compose tasks and to disseminate relevant information to be executed by different team members. Our approach proposes sharing information and data in the VMART environment using push or pull mechanisms. In the following sections, we explain the proposed solution for secure dissemination of information contents using the push mechanism. We begin detailing our approach with a discussion on SOA in section 3.1. For secure and selective dissemination of information, we assume that the information can be represented as XML document for which fine-grain access control can be specified. The authorizations for the XML documents are specified using the role based access control (RBAC) model. Due to the autonomous nature of the collaborating agencies and their diverse organizational structure, we consider two levels of information sharing: 1) at the inter-agency level - to members of the VMART, by the site coordinator Web service of the owner agency; 2) at the intra-agency level - to authorized users within a given agency, by the site coordinator Web service of the receiving agency. The site coordinator Web service is described in section 3.2. This information sharing takes place according to the predefined policies already in place and is enforced by the agency's coordinator Web service. Each role at inter-agency level or intra-agency level has different authorizations over the information contents organized as XML document. Each role is assigned a separate key which is used to decrypt the portion of XML documents for which the role has valid authorization. The details of role permission assignment and XML document encryption are described in sections 3.5 and 3.6, respectively.

3.1 SOA

Our approach adopts Web Services to achieve complex tasks to automate the discovery of the necessary information services (tasks) and compose these services for a particular incident in a crisis situation in accordance with the national, regional or local agency protocols (policies). Specifically each agency has its own set of localized Web services. These localized services provide agency specific functionalities. Each agency site coordinator Web service selects and composes a set of services based on the functionality required for responding to a particular incident in a crisis. These services provide the agency specific output required as part of the response. The outputs from the set of services are then summarized in an XML document as information forming the situation report. The agency site coordinator Web service then selectively disseminates this information to all the members of the VMART based on their roles,e.g., the NYDOT invokes its trafficStatus Web service to gather the traffic reports for the affected area. The output of this Web service is the situation report as reported by NYDOT. The NYDOT Web service then disseminates this situation report to other members of the VMART. Figure 1, shows the proposed framework based on SOA and details the steps involved in the selection of the relevant Web service and the creation of the situation report. In this framework, the different agencies and organizations that participate in the VMART activities, specify the services they offer, policy statement that govern their use, and the information/data they need from the VMART members to perform the designated task. This specification is stored in a service directory that is localized to individual VMART member. The framework utilizes service ontologies for semantic classification of services offered by the service providers. Depending on the crisis situation and the current contextual conditions such as the proximity of the service provider to the affected area, the service delivery time, infrastructure availability at the service provider site, the coordinator service selects the potential services from the available pool of service providers. After short listing of candidate service providers, the policies of all the collaborating agencies and candidate service providers are analyzed for satisfaction of authorization and policy constraints.

3.2 Site Coordinator Web Service

A key component of the proposed framework of Figure 2 is the site coordinator Web service. In the following, we discuss the responsibilities of the site coordinator Web service in the context of VMART expansion

A site coordinator Web service is installed at each VMART member site as shown in Figure 2. The coordinator Web service performs three major tasks: 1) discovery and selection of service providers, 2) secure sharing of information to all collaborating agencies, and 3) role creation for dynamic formation of VMART. These tasks are achieved using a set of authentication service, information dissemination service, information acquisition service and a role creation service. The service specifications and collaboration requirements are specified by the VMART agency that needs to access the services of other agencies to perform the designated tasks. The site co-

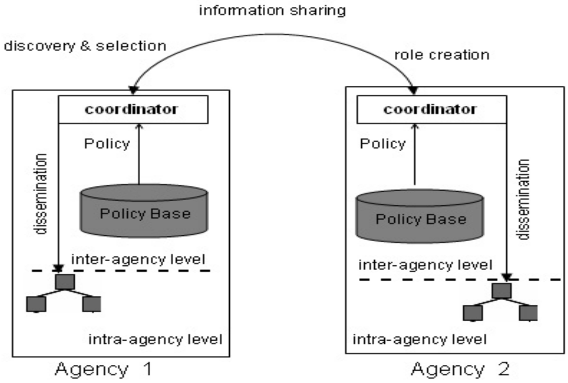


Fig. 2. Responsibilities of coordinator

ordinator Web service has access to the service directory (UDDI), which stores the specifications and usage policies of services offered by various collaborating service providers and organizations willing to participate in the VMART activities. Based on the current contextual conditions, the service policies, and collaboration requirements, the site coordinator Web service utilizes the coordinating service to select appropriate service providers and control the information flow among them. The second major responsibility of the site coordinator Web service is secure sharing of information contents to relevant agencies in a timely manner.

Information sharing takes two different forms: information distribution and information acquisition. At the inter-agency level, information distribution is the process of pushing relevant portions of the information. The information push takes place at two levels: 1) at the inter-agency level - to members of the VMART, by the site coordinator Web service of the owner agency; 2) at the intra-agency level - to authorized users within a given agency, by the site coordinator Web service of the receiving agency. This information push takes place according to the predefined policies already in place and is enforced by an agency's coordinator Web service

Information acquisition is the process of "pulling" needed information from other agencies. Initially, an agency's coordinator Web service authenticates itself to other agencies' coordinators. Once the authentication process is successful, a secure session is established where the requester (agency) sends the details of its request. The coordinator Web service of the owner agency decides whether the requester agency can pull the information according to predefined access control policies and SLA. In contrast with information dissemination, information acquisition takes place at only at inter agency level.

Role creation becomes necessary when an agency joins a VMART through an existing agency. For example, NYFD may create a new role New Jersey Fire department (NJFD) in case the NYFD needs the help of NJFD and wants to append it to the current VMART. This new role is created according to the role creation policies which are discussed in detail in section 3.5.

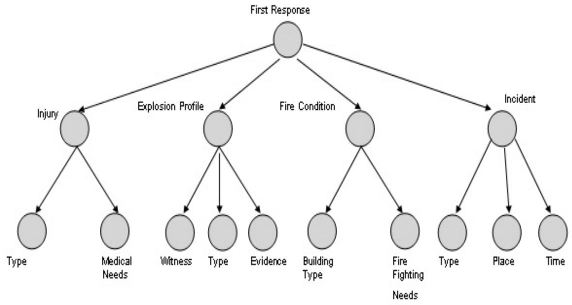
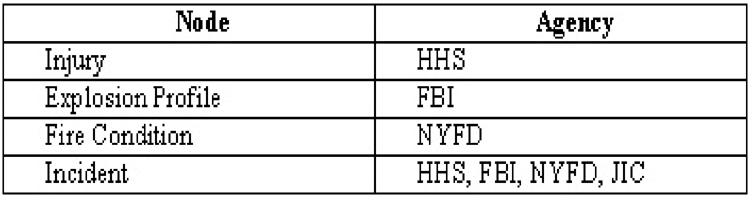


Fig. 3. Agencies, responsibilities and situation reports

Table 2
Nodes of the XML document and agencies that can access these nodes



Node	Agency
Injury	HHS
Explosion Profile	FBI
Fire Condition	NYFD
Incident	HHS, FBI, NYFD, JIC

3.3 XML Document

To support fine-grained access to information in a collaborative environment, we assume that shared information can be represented as an XML document for which access control policies can be specified at the element level(e.g [6,9]). As an example, Figure 3 depicts a fragment of a first response situation report (generated by NYPD - see Table 1) as an XML tree.

Another important aspect of proposed framework is that due to the sensitivity and relevance of information with respect to an agencys role, different portions of the XML document are accessible by different agencies. Table 2 shows the nodes of the XML document of first response situation report and the corresponding agencies that can access these nodes.

For example, Injury part of the XML document is accessible by HHS, whereas Explosion Profile part is accessible by FBI. To achieve having different agencies gain access to different portion of an XML document we discuss a document encryption and key generation scheme in Section 3.6.

3.4 Two-Tier RBAC

The role based access control model (RBAC) [4] seems to be well suited for our environment. In RBAC, permissions are associated with roles and users are assigned to roles based on their respective functions and responsibilities. RBAC, which simplifies management of permissions, is policy-neutral and directly supports important security principles, e.g., separation of duties, least privilege, and data abstraction.

We propose two tier RBAC: inter-agency level (VMART members); and intra-agency level. At the inter-agency level, each member of the VMART fulfills a given role, e.g., NYPD (New York City Police Department), NYFD (New York Fire

Department), etc. On the other hand, at the intra-agency level, we assume that roles exist for various functions and users within a given agency are assigned to the roles based on their qualifications and responsibilities.

In order to support dynamic collaboration among agencies and allow expansion of the VMART, by admitting new collaborators (government agencies or NGOs) as needs arise, we modified RBAC so that a coordinator Web service can create other roles. This modified RBAC model is similar to the self-evolving RBXAC model[6]. At the inter-agency level, an agency coordinator Web service enforces both the role permission assignment and the role creation for the other collaborating agencies. On the other hand, at the intra-agency level, an agency coordinator Web service enforces only role permission assignment for the roles within the agency. For role permission assignment, Read is the access mode through which roles can access objects. For role creation, Create is the access mode through which an agency coordinator Web service can create other roles. Below is the detailed discussion on the specification of role creation and permission assignment privileges.

3.5 RBAC Specification for Role Creation and Permission Assignment

In our model, there are two types of privileges that can be exercised by a coordinator Web service of each agency. These privileges are role permission assignment and role creation. *Role permission assignment* specification is a tuple *(role, permission set) (rpac)* where *role* is the role to which that permission set is assigned, *permission* set is the set of objects that the role can *Read*, and *rpac* is the role permission assignment constraint. Object can be a node, a set of nodes or the entire XML Schema. Role permission assignment constraints are as follows:

- If a node is added to the permission set of a role and access to that node requires access to the ancestor of that node, then this ancestor node should also be added to the permission set.
- If a node is eliminated from the permission set of a role, any child nodes of this node should also be eliminated from the permission set of that role.

For example,

$$(NYPD,\ Read\ (FirstResponse(Location)))$$

allows NYPD to read the "Location" node of "First Response" report. *Role creation policy* is a tuple *((role, access mode) (rcc))* where *role* is the role that is created by the coordinator Web service and *access mode* is *Create* and *rcc* is the role creation constraint. Role creation constraints are as follows:

- The created role can not have more privilege than the creating role.
- If an object is owned by an agency other than the agency which created the role, then the role permission assignment for the created role should be specified by the coordinator Web service of the agency to which the object belongs.

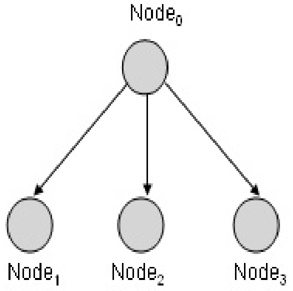


Fig. 4. XML schema nodes

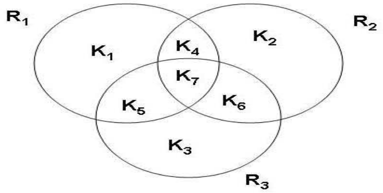


Fig. 5. Venn diagram of keys for three roles

3.6 Secure Selective Sharing of Fine-grained Information

Portions of an XML Document are selectively shared (push or pull) at both inter-agency and intra-agency level according to the predefined policies whose definitions are based on a corresponding XML schema. In [2], a solution was proposed where portions of the document to which the same policies (role in our case) apply are encrypted with the same key. This solution should result in a limited number of generated keys for a given document only if there are no overlaps i.e., more than one role has access to a give element of the XML document. To elaborate, consider a fragment of an XML schema as depicted in Figure 4,

where a role, R_1, may have access right to $Node_1$ and $Node_2$.At the same time another role, R_2, may have access right to $Node_2$ and $Node_3$. If $Node_1$ and $Node_2$ are encrypted with key, K_1, and $Node_2$ and $Node_3$ are encrypted with another key, K_2, then $Node_2$ will be encrypted with two different keys. If only one of the keys is delivered to R_1 and R_2, neither will be able to access $Node_2$. On the other hand, if, K_1 andK_2 are delivered then R_1 will gain access to $Node_3$ and R_2 will gain access to the $Node_1$ a violation of the access policy in place. To alleviate this problem, the overlapping node: $Node_2$ in this case, can be encrypted with a third key, K_3. Afterwards,K_3, K_1 can be distributed to R_1 and K_3, K_2 can be distributed to R_2. Although, this solution seems reasonable, it worst case performance would result in number of generated and distributed keys to be Minimum(2^R-1, N) where R is the number of roles and N is the number of nodes of the XML document. Figure 5 illustrates the possible overlaps and the number of keys necessary for encryption when number of roles is equal to three.

To overcome the overlap problem, we encrypt each node of the XML document with a different key. Keys of nodes to which the same role have access rights are collected in an envelope. Each of the envelopes is encrypted with the public

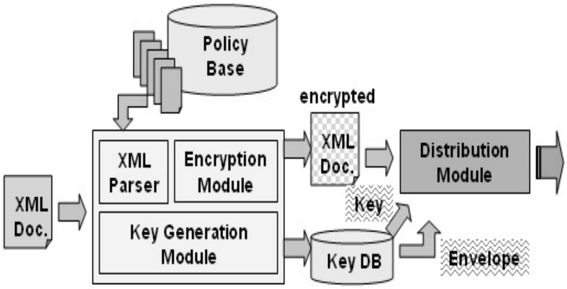


Fig. 6. System architecture

key for the corresponding role. Finally, encrypted XML document together with the corresponding roles envelopes and envelope keys are distributed to all roles simultaneously. This alternative requires distributing envelope keys as many as the number of roles. Algorithm 1 shows the detailed steps of the corresponding algorithm.

```
Algorithm 1 Step 1: Require:Role Permission Assignment Policy, P=($P_1$, $P_2$,...$P_y$)
Where Each $P_y$= ($Role_y$,$PermissionSet_y$)
Where Each $PermissionSet_y$ = ($AccessMode(Object)_1$,... $AccessMode(Object)_y$)
Where AccessMode =[Read]
Step 2: Require:XML Schema
Step 3: For Each Node= 1,2 ...m
Step 4:        $k_m \leftarrow$ Generate Key
Step 5:        $e_m \leftarrow$ Encrypt $node_m$ with $k_m$
Step 6:        $keytable_1 \leftarrow$($node_m$, $k_m$)
Step 7: End For
Step 8: For Each Role= 1, 2 ...y
Step 9:        For Each $node_m$ in $PermissionSet_y$
Step 10:           $envelope_y \leftarrow k_m$
Step 11:        End For
Step 12:       $k_y \leftarrow$ Generate Key
Step 13:       $e_y \leftarrow$ Encrypt $envelope_y$ with $k_y$
Step 14:       $keytable_2 \leftarrow$ ($envelope_y$, $k_y$)
Step 15:       Distribute (Encrypted XML Document, $envelope_y$, $k_y$)
Step 16: End For
```

4 System Architecture

As illustrated in Figure 6, the framework of our system for secure and selective sharing of XML documents consists of the following main modules: XML Parser, Encryption Module, Key Generation Module and Distribution Module. Initially, XML document is parsed into the nodes. Later, each node is encrypted in the Encryption Module with a different key coming from the key generation module. These generated keys are collected in an envelope for each role according to the policies coming from the Policy Base, and then these envelops are encrypted in Encryption Module by the keys coming from the Key Generation Module. Finally, encrypted XML document, envelope and corresponding key are disseminated to corresponding role.

5 Related Work

In [3], Damiani et al. present an access control model for XML documents.In addition, they present a language for the specification of access restrictions together with a description of system architecture for access control enforcement. However, their access control model is generic. In [5], Gabillon et al. define a security model for regulating access to XML documents. In their model, the authorization rules related to a specific XML document are first defined on a separate Authorization sheet. This Authorization sheet is then translated into an XSLT sheet. If a user requests access to the XML document then the XSLT processor uses the XSLT sheet to provide the user with a view of the XML document which is compatible with his rights. Again, their access control model is of generic nature. In [2], Bertino et al. propose a credential based access control model for XML documents where a solution was proposed where portions of the document to which the same policies apply are encrypted with the same key. However, their approach does not take into consideration the case where there are overlaps i.e., more than one credential has access to a given element of the XML document. In [6],He et al. proposed arithmetic so that access control policies can be specified at the element level. In addition, they propose self evolving RBXAC model which we make use of in our approach for the role creation process which is necessary for dynamic composition of VMART. In [7], Kudo et al. present an XML access control language (XACL) which is based on provisional authorization which tells the user that his request will be authorized if he takes certain security actions such as signing his statement prior to authorization of his request. However this approach does not fit into our environment where the initiative of sharing information resides with the information owner.In [9], Zhang et al. proposes RBAC policies should be defined in XML documents before being mapped to the XML documents of interest.

6 Conclusion & Future Work

In this paper we proposed a two tier RBAC approach for secure and selective information sharing in a virtual environment which has two levels: 1) Inter-agency; 2) Intra-agency. In such an environment, we assumed that a coordinator Web service of each agency is responsible for authentication, information dissemination, information acquisition, role creation and enforcement of predefined access control policies. As part of this work we developed information sharing framework which is based on the encryption of XML documents according to RBAC policies defined for XML schema. In [8], B. Shafiq et al. proposed a policy integration framework for merging heterogeneous RBAC policies of multiple domains into a global access control policy. A key challenge in the composition of their policy is the resolution of conflicts that might arise among the RBAC policies of individual domains. As part of our future work we intend to extend their approach by merging the access control policies of collaborating agencies into a global access control policy. This approach will enable us to directly distribute XML documents to the roles within agency utilizing this merged global access control policy. Our extended work will also relax the dissemination responsibility of the coordinator Web services.

Given the dynamic nature of policy specification and the related changes, the evolution of these policies is a challenging issue that forms part of our future work. Another related issue deals with the description of policies in terms of rights, obligations, dispensations, and prohibitions. We intend to develop a semantic interface for describing policies in semantic languages that will enhance the associated interoperability and extensibility. The semantic description facilitates interpretation and reasoning over policies, conflict resolution and assists security and privacy governance by means of policy enforcement. A major hurdle in sharing resources between organizations is heterogeneity on account of semantic differences. Semantic differences occur due to differences in the organizational structure of agencies and the document generated are another major issue to be addressed. As part of our future work we are researching ontology mapping and linking techniques and we intend to explore applying to alleviate these semantic differences.

Our future work also includes selective distribution of sensitive multimedia information as our existing approach deals specifically with XML documents. However emergency management information is increasingly including multimedia information, e.g., audio, video, satellite images, topographic city maps and streaming media. In [1], W. J. Adams proposed a decentralized trust-based access control system for a dynamic collaborative environment by building a privilege management infrastructure (PMI) based on trust. His PMI system used past behavior as an indication of future performance, no a priori user or resource configuration was required. We plan to explore applying this work to overcome some of the limitation of the PKI infrastructure.

References

[1] Adams, W.J. "Decentralized Trust-Based Access Control for Dynamic Collaborative Environments", Ph.D. Thesis, Virginia Polytechnic Institute and State University, 2006.

[2] Bertino, E., and E. Ferrari, *Secure and Selective Dissemination of XML Documents*, ACM Transactions on Information and System Security, **5**(2002), pp. 290-331.

[3] Damiani, E., S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, *A Fine-grained Access Control for XML Documents*, ACM Transactions Information and System Security, **5**(2002), pp. 169-202.

[4] Ferraiolo, D.F., R.S. Sandhu, S. Gavrila, D.R. Kuhn, and R. Chandramouli, *Proposed NIST standard for role-based access control*, ACM Transactions on Information and Systems Security, **4**(2001), pp. 224-274.

[5] Gabillon, A., and E. Bruno, *Regulating Access to XML Documents*, 15^{th} *IFIP WG 11.3 Working Conference on Database Security*, 2001.

[6] He, H., and R.K. Wong, *A Role-Based Access Control Model For XML Repositories*, Proceedings of the First International Conference on Web Information Systems Engineering, **1**(2000), 138.

[7] Kudo, M., and S. Hada, *XML Document Security based on Provisional Authorization*, in: *Proc. of ACM Computer and Communications Security Conference*, 2000.

[8] Shafiq, B., J. Joshi, E. Bertino, and A. Ghafoor, *Secure Interoperation in Multi-Domain Environment Employing RBAC Policies*, IEEE TKDE, **17**(2005), 1557-1577.

[9] Zhang, X., J. Park, and R. Sandhu,*Schema based XML security: RBAC approach*, in: 17^{th} *IFIP 11.3 Working Conference on Data and Application Security*, 2003.