A Secured Framework for Geographical Information Applications on Web

Mennatallah H. Ibrahim, Hesham A. Hefny
Computer Science and Information
Institute of Statistical Studies and Research, Cairo University
Cairo, Egypt

Abstract— **Current geographical information applications increasingly require managing spatial data through the Web. Users of geographical information application need not only to display the spatial data but also to interactively modify them. As a result, the security risks that face geographical information applications are also increasing. In this paper, a secured framework is proposed. The proposed framework's goal is, providing a fine grained access control to web-based geographic information applications. A case study is finally applied to prove the proposed framework feasibility and effectiveness.**

Keywords— spatial data; geographic information systems; access control; authorization

I. INTRODUCTION

Geographic information applications on web strongly need to be secured for several factors: (1) most of the geographical data contain sensitive information, so data cannot be freely disclosed to or altered by illegitimate users, (2) geographical information application's users have different roles and expertise, so they need to be assigned different rights for operating on data, and (3) the power of geographical information applications comes from its ability to relate different types of data in a spatial context, in which these related data are supplied by different data providers such as governments, private companies, academic organizations, and so forth. Each data provider need to ensure the protection of its own data when published on the Web. However, security of geographic information applications on web is an issue that has not been much investigated by Geographic Information Systems (GIS) community.

Applying a controlled access to geographic information applications on web is one of the most important security aspects to such applications. Controlled access ensures the information confidentiality and integrity. Since the geographic information applications are in most cases critical and complex applications (e.g., health applications) contextual permissions are needed , such permissions give concrete rights to users for operating on data in specific situations (e.g., doctors may be given concrete permission to operate on patient's data in emergency situations).

In general, there are two main models used for digital spatial data: (1) vector data models that use discrete elements such as points that represent small objects, lines that represent linear objects and boundaries, and polygons that represent areas. These three elements used to represent the geometry of real world entities, (2) raster data models which identifies and represents grid cells for a given region of interest, raster cells are arrayed in a row/column pattern cell values represent type or quality of mapped variables used with values that may change continuously across a region: elevation, mean temperature, average rainfall [8].

Fine-grained access control and spatial or non-spatial access control are two important requirements for spatial data access control. Fine-grained access control is important where; the spatial data in database usually have different granularities, which are organized in hierarchical architecture. The hierarchy from top to down has two representations in which one is using terms of database, namely, tables, records and cells, while the other is using terms of geospatial domain, namely, map layer, geospatial objects, geometric or descriptive properties. Spatial or non-spatial access control is also very important where; restricting access to some spatial objects, whose descriptive properties meet some conditions, is frequently needed. For example, those spatial objects, whose type is military unit, cannot be accessed by ordinary users.

The aim of this paper is to propose a framework that provides access control to web-based geographic information applications depending on Organization Based Access Control (ORBAC) model [9]. The proposed framework supports new concepts that were not addressed before in order to provide more security to the geographic information applications on Web. These concepts are: (1) contextual permissions, and (2) supporting various security polices in a unique framework. The proposed model also has an important advantage which is achieving fine grained access control through views. Thus, users of the proposed framework are not allowed to access database tables, instead, they are only allowed to access views of these tables. The proposed framework deals with vector data models where, vector data models are more adequate for usage in current GIS applications and spatial database management systems, also vector data models are more adequate for dynamic applications that require data modifications.

II. RELATED WORK

The pioneer access control model for vector-based spatial data on web is proposed in [1, 2]. This pioneer model is based on Role-Based Access Control (RBAC). It extends the

classical discretionary access control model in which it adds a spatial dimension to the authorization rules by assigning a geographical scope in which this geographical scope defines the spatial region in which the authorization is valid. When an access request is issued for an object, the system checks if the requested object lies in the authorization space and if so, it grants the access. A similar architecture but differs in focusing on XML-based representation of spatial data, has been proposed in [3]. The main limitation in such models is represented in, not addressing the issue of multi granularity of spatial data. This limitation has been addressed in [4] where, a more complex spatial data model has been proposed in which, the specification of authorization rules to access complex structured spatial data stored in a DBMS is allowed and organized according to multiple spatial representation levels and at multiple granularities. The model proposed in [4], however, does not deal with geographically bounded roles.

A fine-grained access control model based on RBAC for grid environment is proposed in [5]. The proposed model is based on Globus Security Infrastructure, in such model, every user is mapped to a given role, and every role is given a unique digital certificate to distinguish its identification, then every role had the given permission to access the resources. The main advantage of the model proposed in [5] is represented in, providing strong access control through digital certifications. In [6], also a fine-grained access control model based on RBAC to spatial data in grid environment is proposed. The proposed model adopts a double authorization mechanism: the first authorization authorizes the role, similarly to the RBAC model, and the second authorization authorizes the specific user based on the user's attribution. The limitations of such model are: (1) the role authorization is achieved through Access Control List which is a time consuming method when the resources are massive, (2) the fine-grained authorization method is complex, and (3) conflicts may occur between both the role and the fine-grained authorizations.

As mentioned before, the power of geographical information applications comes from its ability to relate different types of data in a spatial context, such related data are provided by different data providers, and as a result each data provider needs to apply its own security police to ensure its data security while sharing them over the web. Furthermore geographic information applications are complex and critical; such applications strongly need contextual permissions. All of the previously proposed models are based on RBAC model. RBAC models are not fully satisfactory for web-based geographic information applications, as they are not supporting the authorizations rules that specify contextual permissions, or the rules that are specific to particular organization. In another word, none of the previous access control models is able to model security policies that are not restricted to static permissions or to support various security polices in a unique framework.

III. ORGANIZATION BASED ACCESS CONTROL MODEL

ORBAC defines permissions that are applied within an organization to control the activities performed by roles on views under specific conditions. In ORBAC, the subject must be assigned to a given role, the object must be used in a given view and the action must partake in some activities. There are eight basic sets of entities in ORBAC which are: Org (a set of organization), S (a set of subjects), α (a set of actions), O (a set of objects), R (a set of roles), a (a set of activities), V (a set of views) and C (a set of contexts). The following are the basic entities of ORBAC model:

A. Organizations

The Organization is the most important entity in ORBAC model. An organization can be seen as an organized group of subjects who agreed to form an organization. Subject must plays specific roles in the organization according to their agreement.

B. Subjects and Roles

A subject is an active entity (e.g., a user). A role is used to create a link between subjects and organizations. If org is an organization, s is a subject and r is a role, then Employ (org; s; r) means that org employs subject s in role r.

C. Objects and Views

The entity Object covers inactive entities (e.g., database tables). As in relational databases, a view corresponds to a set of objects that satisfy a common property. If org is an organization, o is an object and v is a view, then Use (org; o; v) means that org uses object o in view v.

D. Actions and Activities

The entity Action represents computer actions such as read, write, send, and so forth. The entity Activity is used to abstract actions. If org is an organization, α is an action and a is an activity, then Consider (org; α; a) means that org considers that action α falls within the activity a.

E. Context

Context is used to specify the concrete circumstances where organizations grant roles permissions to perform activities on views. If org is an organization, s is a subject, o is an object, α is an action and c a context, then Define (org; s; o; α; c) means that within organization org, context c is true between subject s, object o and action α. The conditions required for a given context to be linked, within a given organization, to subjects, objects and actions is formally specified by logical rules.

In ORBAC Security Policy, the relationship "Permission" corresponds to a relation between organizations, roles, views, activities and contexts, also the relationships Prohibition, Obligation and Recommendation are defined similarly. If org is an organization, r is a role, v is a view, a is an activity and c a context then Permission (org; r; v; a; c) means that organization org grants role r permission to perform activity a on view v within context c.

IV. VIEWS AND FINE GRAINED ACCESS CONTROL

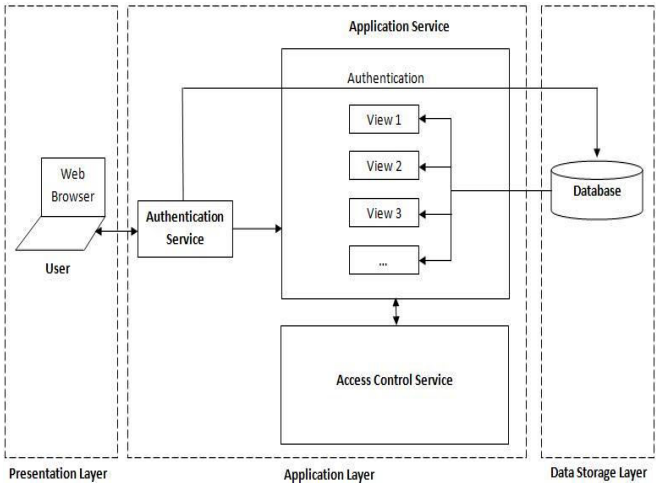
A view is a logical representation of database table(s). In essence, a view is a stored query with no physical storage. A view derives its data from database tables on which it is based; such tables are called base tables. All operations performed on a view affect the base tables. Views provide an additional level of table security by restricting access to a predetermined set of rows or columns of a table, it enable one to tailor the presentation of data to different types of users [7].

With respect to security, we usually want to let specific users access some columns and rows of base tables while hiding other sensitive ones. In our proposed framework, views provide a solution for realizing fine-grained access control for spatial database. By creating views, table level (map layer level), record level (feature level), field level (property level) or even spatial context access control can be easily implemented.

V. PROPOSED FRAMEWORK

The proposed framework aims to: provide fine-grained access control to geographic information applications on web. The proposed framework based on ORBAC model which provides mean to specify different security policies within a unique framework, so that each organization providing data to build the geographic application will be able to define its own security policy, furthermore organizations will be able to specify contextual permissions.

Fig.1. "Proposed Framework"



As shown in Fig.1, the proposed framework depends on the well known three-tier architecture which consists of three layers: (1) Presentation layer; it resides on the users side and consists of either html pages or specialized programs, such as Java code, and plugs in. Users interact with the web-based geographic application through the presentation layer by sending requests and receiving responses, (2) Application layer consists of three services which are: (a) Access Control Service that exposes and implements the operations for both authorization rules checking and administration, (b) Application Service that exposes and implements the application logic and access the application data, and (c) Authentication Service. (3) The data Storage layer consists of database servers.

The proposed framework consists of the following components:

1) User accounts with usernames and passwords;
2) Organizations that users belonging to;
3) Roles that users plays in their organizations;
4) Actions that is assigned to users according to their roles;
5) Views which includes spatial objects that have common properties;
6) Contexts in which the roles permitted to perform actions
7) Database tables that contain spatial and non-spatial data about the spatial objects.

In our proposed framework, the views are created from the base tables in the spatial database according to different access control requirements: either spatial, non-spatial or their combination. These created views are granted to different roles with corresponding authorized actions. The views are granted to users according to their roles and organizations. The proposed framework will support the fine grained access control through these created views.

The typical interaction between the user and the system is as follows: (1) the user will connect to the system through the Authentication Service, (2) an organization and a role will be assigned to the authenticated user, (3) The user will be allowed to issue request(s) to the system through the presentation layer. Each request from the user is then mapped onto one or more operations of the Application Service. The application service in turn interacts with the Access Control Service to verify whether the operation can be performed or not, and (4) the response is sent back to the user from the application service through the presentation layer.

VI. CASE STUDY

A case study has been carried in order to prove the feasibility and effectiveness of the framework proposed in this paper. This case study is represented in creating a web-based geographic information application for two business organizations dealing with each others. These two organizations need to collaborate together in order to enhance their performance level and such enhancement will be achieved by creating a web-based geographic information application. The first organization owns a number of warehouses for electronic products, while the second organization owns a number of stores that sell the products of the first organization. The goal of the application is to maintain the warehouses, the stores and their products over the Web. Data in such application can be queried, inserted and modified using a Web browser.

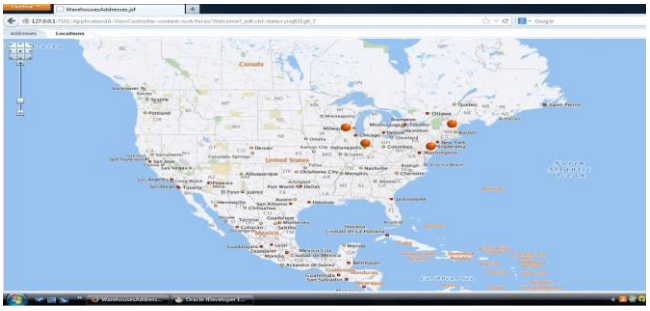


Fig.2. "AllWarehouses" View on map that retrieves all warehouses

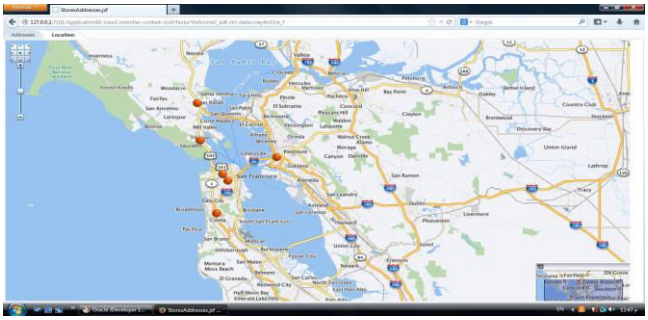


Fig.3. "AllStores" View on map that retrieves all stores.

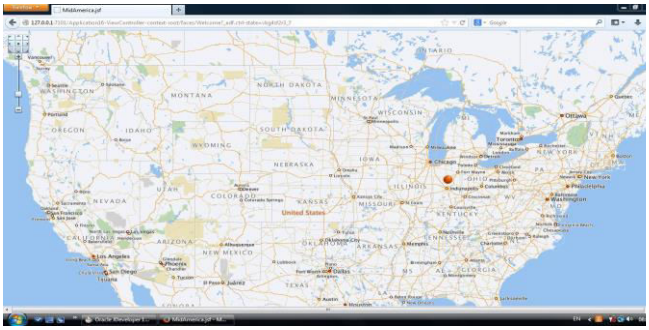


Fig.4. "MidAmericaWarehouse" View on map that retrieves only Mid America Warehouse.

The oversimplified information which defines the access control policy is assuming that there are two roles which are Manager and Coordinator. These roles belong to two organizations which are, Organization1 and Organization2. The features to be secured are the warehouses and the stores. The privileges are RetrieveData, InsertData, UpdateData and DeleteData. The contexts in which privileges will be granted to roles are normal and emergency.

Three views are created: (1) "AllWarehouses" view which is created from three base tables. Such view contains data about all warehouses owned by Organization2, (2) "AllStores" view which is also created from three base tables and contains data about all stores owned by Organization1, and (3) "MidAmericaWarehouse" view which is a subset of "AllWarehouses" view that contains data about only one warehouse called Mid America warehouse.

Let O be the set of organizations, R be the set of roles, V be the set of views, A be the set of actions and C be the set of contexts:
O= {Organization1, Organization2}
R= {Manager, Coordinator}
V= {AllWarehouses, AllStores, MidAmericaWarehouse}
A= {RetrieveData, InsertData, UpdateData, DeleteData}
C= {Normal, Emergency}
Note: The keyword ALL stands for all possible values for the field.

The authorization rules are defined as follows:
r1= <Organization1, Manager, AllStores, ALL, ALL >
r2= < Organization2, Manager, AllWarehouses, ALL, ALL>
r3= < Organization2, Coordinator, MidAmericaWarehouse, ALL, ALL>
r4= < Organization2, Coordinator, AllWarehouses, RetrieveData, Emergency >

Rule r1: states that the role "Manager" in "Organization 1" is authorized to retrieve, insert, update and delete data in the "AllStores" view in all contexts.
Rule r2: states that the role "Manager" in "Organization 2" is authorized to retrieve, insert, update and delete data in the "AllWarehouses" view in all contexts.
Rule r3: states that role "Coordinator" in "Organization 2" is authorized to retrieve, insert, update and delete data in the view "MidAmericaWarehouse" in all contexts.
Rule r4: states that the role "Coordinator" in "Organization 2" is authorized **only** to retrieve data in the "AllWarehouses" view and this is **only** in Emergency context.

From the previous rules, it is clear that by using views fine granularity and is achieved. Fine granularity is clearly shown in the "role Coordinator" in "Organization1" which is operating on data of a certain warehouse (i.e., Mid America Warehouse), but not operating on data of all other warehouses. The previous rules also show that using the entity context enable us to control when to allow a specific role (i.e., Coordinator) to perform a specific privilege (i.e., RetrieveData) on specific view (i.e., AllWarehouses) in specific context (i.e., Emergency) In normal cases such role is allowed only to deal with "MidAmericaWarehouse" view.

The effect of authorization rules and views on different user's interactions are illustrated through a number of screen shots. "Fig. 2" shows the "AllWarehouses" view which is displayed to the role "Manager" in "Organization2" as this role is allowed to retrieve all warehouses. "Fig. 3" shows the "AllStores" view which is displayed to the role "Manager" in "Organization 1" as this role is allowed to retrieve all stores. While "Fig. 4" shows the "MidAmericaWarehouse" view which is displayed to the role "Coordinator" as this role is allowed to retrieve only Mid America Warehouse except in Emergency context in which such role will be allowed to retrieve all warehouses.

Such results cannot be achieved with the previously proposed models as such models don't allow any organization as a data provider to specify its own security policy as a result all users who assigned the role "Manager" will be able to access same views regardless the organizations that these users belong to. Also in the previous models, contextual permissions are not allowed as a result the role "Coordinator" will be allowed either to retrieve all warehouses data or not without considering any contexts. Furthermore, the previously proposed models allow all authenticated users to access base tables of database while in our proposed framework all users are prevented from accessing those tables.

By comparing the proposed framework and the previously proposed ones, it is clear that, the proposed framework supports two new important concepts that were not supported previously, although these new concepts are very important to the web-based geographic information applications. The first concept presented in, the ability of the proposed framework to provide a mean to specify different security policies within a unique framework. So each data provider that collaborated in building the application can define its security policy to protect its own data. The second concept presented in, the ability to specify contextual permissions. Furthermore, the proposed framework supports the fine-grained access control through views. Furthermore, an important difference between the proposed model in this paper and the previously proposed models is that the model proposed in this paper prevents authenticated users from accessing base tables, as users are allowed only to access specific views according to their roles and organizations. TABLE I summarizes the differences between the model proposed in this paper and the previously proposed ones.

TABLE I. Proposed Model and Previous Models Comparison

Criteria	**Frameworks**	
	Previous Models	*Proposed Model*
Allowing each data provider to define its security policy to protect its own data	–	✓
Preventing access to base tables	–	✓
Allowing Contextual Permissions	–	✓

The proposed framework advantages:

1) The framework depends on ORBAC model which provides means to specify different security policies within a unique framework.
2) The framework supports fine granularity access control to data through views.
3) The framework provides authorization rules that specify contextual permissions.

The proposed framework limitations:

1) *Concurrent control:* The multi views mode to a single base table may cause the concurrent control problem and this happens when many users access those views that based on the same base table concurrently. Fortunately, this problem has been solved to some extent by the database internal mechanism.
2) *Redundancy and information leakage:* The abusive usage of views can result in redundancy of the access control predicates, and the potential of information leakage through exceptions and errors that are caused by user-defined functions.

I. CONCLUSION

Security is very important and critical for web-based geographic information applications. Access control is required to keep data confidentiality and integrity. In this paper, we proposed a framework for secured web-based geographic information applications based on ORBAC model. The goal of this framework is to ensure the security of data in such applications.

REFERENCES

[1] E. Bertino & M. L. Damiani. *"A controlled access to spatial data on Web"*. 7th AGILE Conference on Geographic Information Science, Heraklion, Greece. 29 April-1May 2004. Pages 369-377.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] E. Bertino, M.L. Damiani, & D. Momini. *"An Access Control System for a Web Map Management Service"*. In Proc. of the 14th International Workshop on Research Issues in Data Engineering (RIDE-WS-ECEG), Boston, USA. March 2004. Pages 33–39.

[3] B. Purevjii, T. Amagasa, S. Imai & Y. Kanamori. *"An access control model for geographic data in an XML-based framework"*. In Proc of the 2nd International Workshop on Information Systems Security (WOSIS). 2004. Pages 251-260.

[4] A. Belussi, E. Bertin, B. Catania, M.L. Damiani & A. Nucita. *"An authorization model for geographical maps"*. Proceedings of the 12th annual ACM international workshop on Geographic information systems, New York, NY, USA. 2004. Pages 82-91.

[5] M. Yan, Y. Gao, L. Wu, P.Wu, & Y. Zhao. *"Spatial data access control in grid environment"*. Geoinformatics, 17th International Conference. August 2009. Pages 1-6

[6] F. Ma, Y. Gao, M. Yan, F. Xu & D. Liu. "The fine-grained security access control *of spatial data"*. Geoinformatics 18th International Conference. June 2010. Pages 1-4.

[7] http://docs.oracle.com/cd/E18283_01/server.112/e16508.pdf

[8] P. Bolstad. April 2012.*"GIS fundamentals: A firat text on geographic information systems"*.4th Edition.U.S. *State of* of Minnesota: Eider Press.

[9] A. Abou El Kalam, S. Benferhat, R. El Baida, A. Miege & et al. "*Organization based* access control". Proceeding of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks. 2003. Page 120.