Contextual View-based Access Control Model for Spatial Data on Web

Mennatallah H. Ibrahim
Institute of Statistical Studies and Research
5 Dr.Ahmed Zwel Street, Orman, Giza, Egypt

Hesham A. Hefny
Institute of Statistical Studies and Research
5 Dr.Ahmed Zwel Street, Orman, Giza, Egypt

Nermin Hamza
Institute of Statistical Studies and Research
5 Dr.Ahmed Zwel Street, Orman, Giza, Egypt

ABSTRACT
The proliferation of geographical information services on the Web is creating unprecedented opportunities for the shared use of spatial data. As a result, the spatial data may be subjected to various security risks where, it may be displayed to or modified by illegitimate users. Therefore, there is an increasing need to control access to spatial data on the Web. Geographic information services almost deal with critical applications such as health applications in which many critical situations need to be handled by unusual decisions, so the controlled access to spatial data must be tolerant to handle any critical situations. In this paper, a contextual access control model is proposed. The goal is, providing a fine grained access control to spatial data on the Web and granting contextual permissions to authorized users to handle any critical situation that they may face. An architectural framework for enclosing the proposed model is developed. Finally, a case study is applied to prove the proposed model feasibility and effectiveness.

General Terms
Geographic Information Systems

Keywords
Geographic Information Systems, Spatial Data, Access Control, Authorization

1. INTRODUCTION
Current applications increasingly require that spatial data to be managed through the Web. As a result, spatial data is increasingly exposed to various security risks. Indeed, there is a strong need for securing spatial data on Web motivated by several factors: firstly, geographical data may contain sensitive information, so data cannot be freely disclosed to or modified by illegitimate users; secondly, the users of Spatial Web services have different roles and expertise, so they need to be assigned different rights for operating on data; thirdly, the power of Geographic Information System (GIS) applications comes from its ability to relate different types of data in a spatial context, these related data are supplied by various data providers such as governments, private companies, academic organizations, and so forth. Each data providers need to protect the data it publishes on the Web.

However, an issue that has not been much investigated by GIS community is that how to ensure secure access to spatial data on Web, in order to ensure the information confidentiality and integrity. Ensuring confidentiality means preventing improper disclosure of information to users that are not authorized to access it., while ensuring integrity means to protect data from unauthorized modifications [1].

Generally, there are two main models used for digital spatial data: first, vector data models that use discrete elements such as points, lines, and polygons to represent the geometry of real world entities where, points represent small objects, lines represent linear objects and boundaries and areas represented by closed, connected set of lines; second, 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 [2]. The model proposed in this paper adopts the vector models as such models are adequate for usage in current GIS and spatial database management system and also adequate for dynamic applications requiring data modifications.

2. RELATED WORK
As mentioned before, security of spatial data on Web is an issue that has not been much investigated by GIS community. The pioneer access control model for vector-based spatial data on web is proposed in [1, 3]. This pioneer model is a Role-Based Access Control (RBAC) based on extending the classical discretionary access control model where, its idea is to add a spatial dimension to the authorization rules by assigning a geographical scope; 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. The main limitation in such model is represented in, not addressing the multi-granularity of spatial data. A similar architecture, but focused on XML-based representation of spatial data, has been proposed in [4]. The main limitation of [1, 3] has been addressed in [5] 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 proposed model, however, does not deal with geographically bounded roles.

In [6], a fine-grained RBAC control model in grid environment was proposed based on Globus Security Infrastructure. In such model, every user is mapped to a given role, and every role has a unique digital certificate to distinguish its identification, then every role had the given permission to access the resources. In [7], also a fine-grained RBAC model 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, the role authorization is achieved through Access Control List which is a time consuming method when the resources are massive; also the fine-grained authorization method is complex; furthermore

conflicts may occur between the role and the fine-grained authorizations.

The model proposed in this paper addressed to new concepts that were not addressed in the previous models which are preventing authorized users from accessing base tables and allowing contextual permission. More clearly the proposed model differs from the previous models in the following:

1. The proposed model uses views to allow fine granularity access to spatial data on the Web. Views are an effective way to reach fine granularity with higher protection where, all the authorized users will not be able to access the base tables and this is providing more security to base tables as only the authorized rows and columns will be displayed to the authorized users.

2. The proposed model allows contextual permissions to help users to handle any critical situations. The concept of contextual permissions is very important to GIS as it almost deal with critical applications as health applications.

3. SPATIAL DATA ACCESS CONTROL REQUIREMENTS

Access control systems ensure data protection within a data management system. Basically, data access is controlled through access control policies that contain a set of authorization rules, these rules states who can access which resource for doing what. An authorization rule, in its basic form, consists of : <subject, object, privilege>. The subject refers to who can access the data, the object is the data itself, and finally, the privilege is the kind of action that can be performed by the subject on the data. Authorization rules are granted in accordance to an administration policy. We adopt a discretionary access control policy; it means that subjects with proper administration authorizations can grant or revoke authorizations to other users at their discretion.

Fine-grained access control, spatial or non-spatial access control and contextual permissions are important requirements for spatial data access control.

- **Fine-grained access control:** The spatial data in database usually have different granularities, which are organized in hierarchical architecture. The hierarchy from top to down has two representations. One is using terms of database, namely tables, records and cells. The other is using terms of geospatial domain, namely map layer, geospatial objects, geometric or descriptive properties.
- **Spatial or non-spatial access control:** Restrict 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.
- **Contextual permissions:** Contextual permissions help users to handle critical situations. The concept of contextual permissions is very important to GIS applications as such applications almost deal with critical applications as health applications.

4. VIEWS AND FINE GRAINED ACCESS CONTROL

A view is a single table that is derived from other tables. These other tables can be base tables or previously defined view. A view does not necessarily exist in physical form; it is considered a virtual table, in contrast to base tables, whose tuples are actually stored in the database. [8]

In the model proposed in this paper, 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. With respect to security, we usually want to let specific users access some columns and rows of base tables while hiding other sensitive ones. We can reach this objective by creating a view which only contains fields accessible to those users.

5. THE PROPOSED ACCESS CONTROL MODEL

The proposed model is a contextual view-based model where, users can only access views of the base tables not the base tables themselves, and contextual permissions are granted to various roles. Contexts will be used to specify the concrete circumstances where roles will be granted specific privileges on views. The proposed access control model accounts for both the spatial dimension and the Web service context. It is based on the classical discretionary models defined for data management systems.

The authorization rule in the proposed model is a relation between the following:
<Role, View, Privilege, Context, Grantor, Grant Option>

- **Role:** specifies the "who" of the rule. A role is a set of users who interact with the system and share the same rights on spatial objects.
- **View:** specifies the "what" of the rule, the resource that needs to be protected.
- **Privilege:** it specifies the "how" of the rule, the operation that is to be performed on the view.
- **Context:** it specifies the concrete circumstances where roles will be granted privilege
- **Grantor:** the grantor is the role that granted the authorization.
- **Grant Option:** it either true or false, if true the role is authorized to grant/revoke the rule to some other roles.

Administration policy for the authorization rules indicates how authorizations are granted and revoked. In the proposed model, the administrative operations are performed by system-defined role "administrator". The administrator is given the whole set of privileges for the whole set of views and he is able to create/delete users, create/delete roles, create/delete views, create/delete contexts and grant/revoke privileges. Moreover, according to classical discretionary models, the administrator can delegate someone else to perform the administrative functions so the administration policy is decentralized. Privileges dependencies is taken in consideration when granting and revoking privileges.

By comparing the proposed model and the previously proposed ones, it is clear that the proposed model provides more security to spatial data on web than the previously proposed models as it uses views to provide fine grained access to spatial data on web, as a result authorized users will not be allowed to access the base tables instead, only the authorized rows and columns will be displayed to the

authorized users. The proposed model also addressed an important concept that was not addressed before in any of the previously proposed models which is contextual permissions. Contextual permissions help users to handle any critical situations. The concept of contextual permissions is very important to GIS applications as such applications almost deal with critical applications as health applications that deal with critical situations. Table 1 below shows the main differences between the proposed model and the previous models.

Table 1. Main differences between proposed model and the previous models

Models / Criteria	Previous Models	Proposed Model
Preventing access to base tables	–	✓
Allowing Contextual Permissions	–	✓

6. FRAMEWORK

An architectural framework for a web service including the proposed access control model is considered. This framework is based on the well-known three-tier architecture which is consisting of presentation, application and data storage layers.

The presentation layer, which displays the output of the application layer to the user and also user's requests are posted to the application layer through the presentation layer. The application layer consists of two main services which are the access control service and the application service. The first service exposes and implements the operations for authorization rules checking and administration. The second service exposes and implements the application logic and access the application data. When an operation is invoked by the user, the application service interacts with the access control service to checks whether the operation is authorized or not and if it is authorized, the operation is performed. The application layer also includes an authentication service that can be based on username/password, or provide more complex service. The data storage layer is responsible for the storage and the provision of data to the application layer.

The proposed framework typically has the following components: user's accounts (username and password), roles, privileges, views, contexts, and base tables. The views are created from the base tables in spatial database according to different access control requirements, either spatial, non-spatial or combination of them. These created views are then granted to different roles. After the user is authenticated to the system, his role(s) is assigned to him then he gains the privileges to his role's specified views.

The typical interaction between the user and the system is as follows: the user connects to the system through the authentication service. Next, if the user is authenticated, his roles will be assigned to him. 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.

7. CASE STUDY

In order to prove the concept we proposed in this paper a case study has been developed consisting of a spatial Web service for a business organization that owns number of warehouses in different countries. The goal of such application is to maintain the organization's warehouses over the web. Organization's warehouses can be queried, created and modified using a web browser.

The oversimplified information which defines the access control policy is that two roles are assumed which are Administrator and Mid-AmericaBranchesManager. The features to be secured are the warehouses owned by the organization. The privileges are GetView, InsertView, UpdateView and DeleteView.

Two views are created from a base table in the database. The base table is called "Warehouses"; this table contains data about all the warehouses owned by the organization (i.e. id, name, address, manager id, manager assistant id). The first view is, "AllWarehouses", it includes all records of warehouses table. The second view is, "Mid-AmericaWarehouse" view that includes only records of a warehouse named "Mid-America".

Let R be the set of roles, V be the set of views, P be the set of privileges and C be the set of Contexts:

R= {Administrator, Mid-AmericaBranchManager}
V= {AllWarehouses, Mid-AmericaWarehouse}
P= {GetView, InsertView, UpdateView, DeleteView}
C= {Normal, Emergency}

The authorization rules are defined as follows:

r1= <Administrator, ALL, ALL, ALL, _, true>
r2= < Mid-AmericaBranchManager, Mid-AmericaWarehouse, GetView, Normal, Administrator, false>
r3= < Mid-AmericaBranchManager, Mid-AmericaWarehouse, UpdateView, Emergency, Administrator, false>

Rule r1 is the default rule stating that the administrator has full privileges on all views in all contexts. The keyword ALL stands for all possible values for the field.
Rule r2 states that the role Mid-AmericaBranchManager is authorized only to retrieve Mid-AmericaWarehouse view when system is in the normal context.
Rule r3 states that the role Mid-AmericaBranchManager is authorized to update Mid-AmericaWarehouse view when system is in emergency context.

From the previous rules, it is clear that by using context it easy to control when to allow a specific role (i.e.: Mid-AmericaBranchManager) to perform a specific privilege (i.e. update) on specific view (i.e. Mid-AmericaWarehouse). In normal cases the role AmericaBranchManager is allowed only to retrieve the view but in emergency cases the role is allowed to update it as well.

We illustrate, through a number of screen shots, the effect of authorization rules and views on user interaction. The screens in Fig 1 and Fig 2 show the AllWarehouses view which is displayed to administrator role as this role is allowed to retrieve all warehouses. While Fig 3 shows the Mid-AmericaWarehouses view which is displayed to Mid-AmericaBranchManager as this role is allowed to retrieve only Mid America branch.

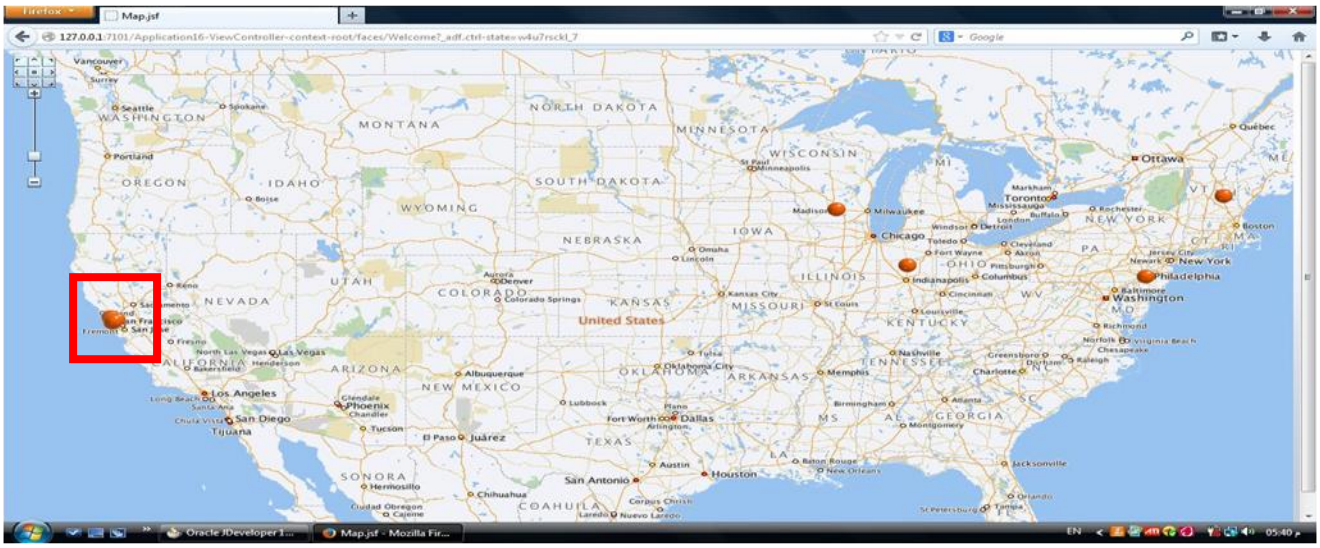

Fig 1: AllWarehouses View that retrieves all warehouses

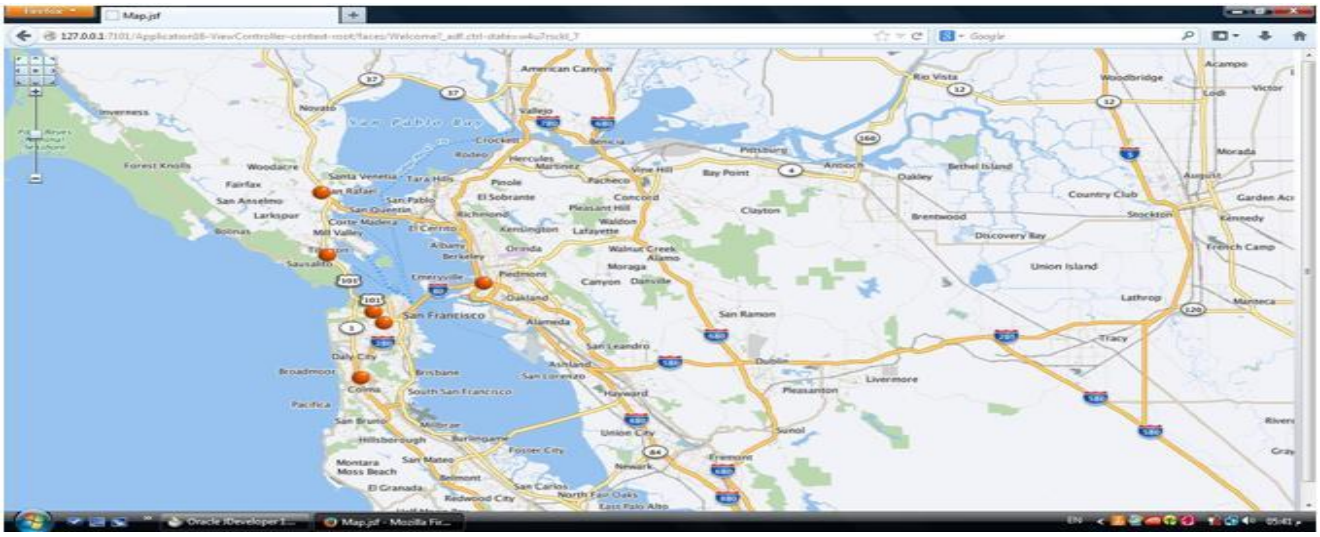

Figure 2: Part of AllWarehouses View (After zooming the squared part in Figure 1)

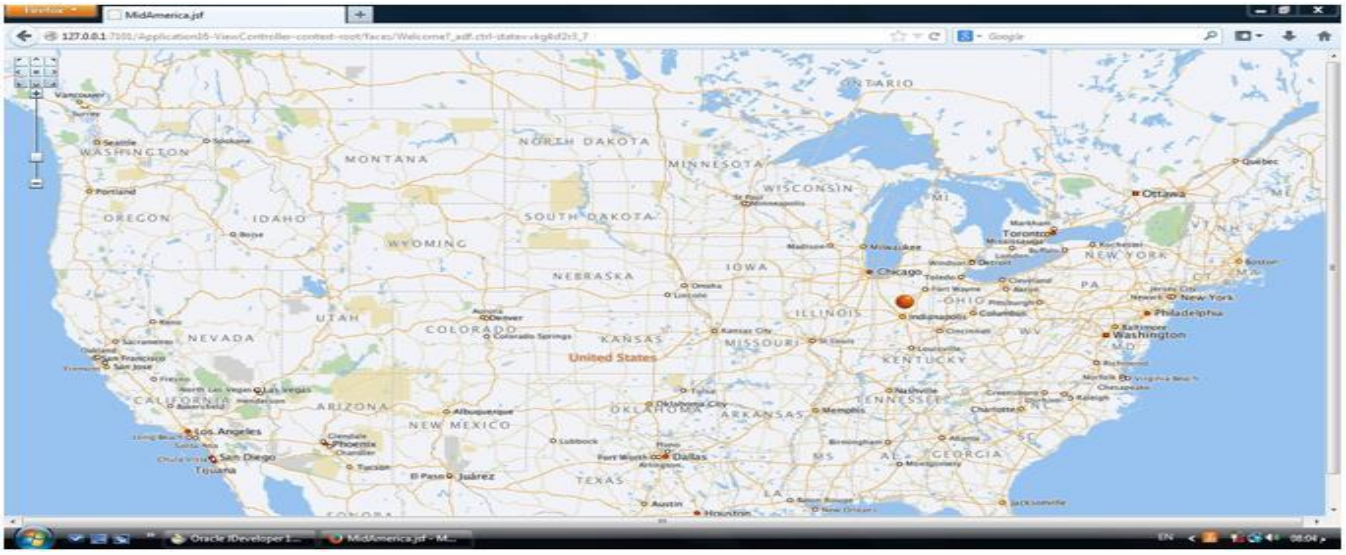

Figure 3: Mid-AmericaWarehouses View that retrieves only Mid America Warehouse

8. PROPOSED MODEL LIMITATIONS

The limitations of the proposed model are:

1. **Concurrent control**: Though the mode of multi views to a single base table may cause the problem of concurrent control when many users access those views based on the same base table concurrently. Fortunately, this problem has, to some extent, been solved 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

9. CONCLUSION

The main aim of this paper is to protect spatial data on the Web by applying controlled access to it. A contextual view-based access control model has been proposed. The proposed model is a RBAC model that uses views to achieve fine granularity access to spatial data. A possible framework to implement the proposed model has been discussed. Finally a case study has been carried out to prove the feasibility of the proposed model.

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.

[2] P. Bolstad. April 2012. *"GIS Fundamentals: A First Text on Geographic Information Systems"*. 4th Edition. U.S. state of Minnesota: Eider Press.

[3] 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.

[4] 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.

[5] 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.

[6] 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

[7] 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.

[8] R. Elmasri. March 2006. "*Fundamentals of database systems*". 5th Edition. Boston: Addison Wesley.