ISSN: 2321-7782 (Online)

Volume 2, Issue 2, February 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Paper / Case Study

Available online at: www.ijarcsms.com

A Survey on Secure Access Control Mechanism of Geospatial Data

Kalpesh V. Chaudhari
Student of Master in Computer Science & Engineering
Gujarat Technological University
Ahmedabad - India

Abstract: Geospatial data is data about the geographic locations of earth surface features and boundaries on Earth. Nowadays spatial data is used in every field of society and due to the advancements in spatial data acquisition technologies, such as the advancements in the satellite sensor technologies, high precision digital cameras used in the capturing of photogrammetric images and high precision land surveys are producing mass high precision spatial data. Due to these issues nowadays sensitivity of spatial data has increased too many folds. To store such high precision data onto the database is a big challenge today. Spatial database is different from relational database as it contains data along with its location into the database, so security concerns of spatial database are also different from relational database. Due to the high sensitivity and space requirement, spatial database requires special security policies and implementation of these security policies. Major security concerns of the geospatial data are based on authorization, authentication, access control, integrity, security and secure transmission of spatial data over the network and transmission media. Secure access control mechanisms play an important role to provide more security of geospatial data. However, the existing data access control technologies are inadequate to meet the security requirement of spatial data, especially in fine-grained access control. In this paper, Access control mechanisms of geospatial data are discussed. Then, issue of security mechanism of authorization of different model is discussed in details. After analyzing the access control data models and access control policies, fine-grained access control mechanism of Fuguand Ma and Fuchun Xu (2010) resolved some issue compared with other access control mechanism of geospatial data. There are two authentication levels in fine-grained access control method that overcome some issues and increased security and privacy of geospatial data.

Keywords: GIS, Spatial data Security, Security mechanism, Access Control, Authorization model.

I. INTRODUCTION

A. *Geographical information system (gis) and geospatial data*

A geographic information system (GIS) integrates hardware, software, and data for capturing, managing, analyzing, and displaying the information related to the surface of the earth. In recent years, GIS has become a powerful technology because it has the potential to organize complex spatial setting with table relationships. The emphasis given is on developing digital spatial database, using the data sets derived from precise navigation and imaging satellites, aircrafts, and digitization of maps. In recent years, the use of GIS has been raised for effective data handling and also for analyzing and geographically transferring information around the world. According to Folger (2010) [1] the power of GIS is the ability to combine geospatial information in unique ways by layers or themes and extract something new.

Geospatial is used as a synonym for "geometric", "graphical", and "geographic", which means related to the earth, so in spatial data we store information related to the earth surface. Geospatial data is the data or information that identifies the geographic location of features and boundaries on Earth, such as natural or constructed features, oceans, and more [1]. Spatial data is often accessed, manipulated or analyzed through GIS. Geospatial data can be acquired using a variety of technologies such as land surveyors, using satellites, aerial photographers, police, and even average citizens with a GPS-enabled cell phone can collect geospatial data using GPS and this collected data can be entered into GIS. Spatial Data exists in many forms such as digital maps and printed maps, aerial photography, toposheets and digital satellite imagery. This data can be manipulated in desktop mapping or GIS programs such as ArcView, Mapinfo, or Intergraph.

B. Spatial Database and Security issue

Security issues for geospatial data are different and in many ways more complex than security issues for relational data. According to Ma et al. [2] nowadays due to developments in GIS and network technologies, the spatial data security is becoming more and more important, also the spatial data acquisition technologies are producing mass high precision data, which contains high resolution images, and requires large disk space, so it is seriously demanded to ensure the data security access restrictions and also to apply advanced security policies to spatial data.

Today the big challenge is to ensure secure access to spatial data on network as geographical data may contain sensitive information, so data cannot be freely disclosed. Users of spatial web services, such as public administration, planners, surveyors and professionals, due to their different roles and responsibilities, you must assign the appropriate rights to operate on the data. Thus, a controlled corporate and government data access is paramount to the development of Spatial Data Infrastructures.

Data providers need to protect the resources published on the Web. There are men in the middle attacks and password attacks during access between clients and servers. To resolve security problems of spatial database access and transmission, we should focus on identity management, authentication, access control and secret data transmission.

C. Security Concerns in Geospatial Data

According to Bertino [3] (2008) nowadays GIS systems are widely spreading in every field of society such as government organizations, municipalities, military affairs, disaster defense, public security emergency management, environmental monitoring and utilities. Core of GIS is spatial database; it is obvious that spatial database has a quite important function in GIS, thus it requires the definition and administration of user tailored security policies.

According to Li et al.[4] (2010) due to the advancements in sensor technologies, satellite imagery, and field surveys have made it possible to collect large amount of spatial data with high precision, with large coverage of area and with high resolution. Due to these issues nowadays sensitivity of spatial data advancements have recently raised many data security, privacy, and safeguarding concerns, not only by the public but also by federal, state, and local government organizations. To store such high precision data onto the database is a big challenge today.

Spatial database is different from relational database as it contains data along with its location into the database, so security concerns of spatial database are also different from relational data. Due to the high sensitivity and space requirement, spatial data requires special security policies and implementation of these security policies. Major security concerns of the geospatial data are based on user authorization, authentication, and data access control, integrity and security of data and secure transmission of spatial data over the network. For example, thematic and topographical maps in support of disaster and emergency management, homeland security, and environmental crises provide geospatial data for various features of locations and facilities at very fine-grained levels of detail. Also publicly available geospatial information can be exploited by attackers for corrupting critical infrastructures and compromising the security and privacy of people, property, and systems.

II. ACCESS CONTROL MECHANISM

Access control is divided into DAC (Discretionary Access Control), MAC (Mandatory Access Control) and RBAC (Role-Based Access Control).[6] Mandatory access control (MAC) developed in an atmosphere of military and national security setting; discretionary access control (DAC) has its roots in academic and commercial laboratories research; the RBAC model, since the seminal work has gained increasingly consensus in the scientific community as well as in industry to finally become a standard widely adopted by organizations.

A. Mandatory Access Control

Mandatory access control models control accesses on the basis of a predefined classification of subjects and objects in the system. Objects are the passive entities that store information as relationships in a DBMS. Subjects are active entities performing data accesses. The classification is based on a set of access classes, also called tags that are associated with each subject and object in the system. A subject is granted permission to access a given object, if and only if some relationship, according to the access mode is fulfilled between the classifications of the subject and the object. A class of general access consists of two components: a security level and a set of categories. The security level is an element of a hierarchically ordered set. A very well-known example of such a set is the one including the levels TopSecret (TS), Secret (S), Confidential (C), and Unclassified (U), where TS > S > C > U.[6] The set of categories is an unordered set (e.g. NATO, Nuclear, Army). Access classes are partially ordered as follows. An access class ci dominates ≥ an access class cj if the security level of ci is greater than or equal to that of cj and the categories of ci include those of cj [6]. The security level of the access class reflects the sensitivity of the information contained in the object. Categories are used to provide finer-grained security classifications of subjects and objects.

B. Discretionary Access Control

These models are discretionary in the sense that they allow users to grant other users permission to access the data. Specifically, DAC policies governing user access based on user identity and authorizations which specify, for each user (or user group) and each object in the system, the access modes (e.g. read, write, or execute) the user is allowed on property.[6] Each request of a user to access an object is checked against the authorizations provided. If there is a release indicating that the user can access the object in the specific embodiment, the access is granted otherwise denied. Because of this flexibility, discretionary policies are adopted in many applications. An important aspect of DAC associated with policy administration authorization. Authorization administration refers to the function of granting and revoking authorizations. It is the function by which authorizations are introduced (removed) to (from) the ACS. Common administration policies include the centralized administration policy, by which only some privileged users may grant and revoke authorizations, and the ownership-based administration, by which grant and revoke operations on a data objects are issued by the creator of the object. The ownership-based administration is often extended with features for administration delegation. Administration delegation allows the owner of an object to assign other users the right to grant and revoke authorizations, thus enabling decentralized authorization administration.

C. Role based Access Control

Role-based access control (RBAC) [5] is an emerging approach to access control that is attracting much attention from both the scientific community and industry. In RBAC, permissions are associated with roles, and users are granted membership in appropriate roles, thereby acquiring the roles' permissions. [5] In the context of an organization, roles are created for the various job functions and users are assigned and revoked role memberships based on their skills and qualifications. Roles add a level of indirection between users and permissions, thus simplifying the management of the many-to-many relationships between users and permissions. A role is a semantic construct job function within an organization. Specifically, the RBAC [6] standard consists of four basic groups of elements: users, roles, permissions, and sessions.

- User is as a human being or an autonomous agent.
- Role represents the function of a user within a community. The community can be a structured organization, for example, a company or a more informal community, for example the citizens of a city organization. A role gives a set of user permissions.
- Permission. Permission is an approval to perform an operation on one or more objects. An object is a resource that must be protected. An operation is an executable image of a program that performs a particular function invocation to

the user through an object. The types of operations and objects depend on the context in which application is deployed RBAC. For example, in a file system, operations might include read, write, and execute in a DBMS, operations might include insert, delete, add, and update.

- Session. When the user logs in, a session is established, during which the user activates a subset of the functions that he or she is assigned. The permissions available to the user of the session, then, are the permissions assigned to the roles that are currently active in all user sessions.

In previous sets of elements, a number of relations are defined. The *user assignment* refers tousers f users to roles through a many-to-many relationship, a user can therefore be assigned multiple roles and the same role assigned to different users. The *permission-assignment* relation relates roles and permissions again through a many-to-many relationship; thus a role can be assigned multiple permissions and similarly each permission can be assigned to multiple roles. The function *SessionUser* maps each session into a user, whereas the *SessionRole* function maps a session onto a set of roles, namely the roles that are active in the session. The basic concepts are formally summarized as follows:

Definition: (Basic Concepts of RBAC). [6] *Let* U, R, PRMS, *and* SES *denote the set of users, roles, permissions, and sessions, respectively. We define:*

- $UA \subseteq U \times R$. *The user assignment relation that assigns users to roles.*
- $AssignedUser: R \rightarrow 2^{U}$. *The mapping from a role to a set of users.*
- $PA \subseteq R \times PRMS$. *The permission assignment relation that assigns permissions to roles.*
- $PrmsAssignment: R \rightarrow 2^{PRMS}$. *The mapping of a role into a set of permissions.*
- $SessionUser: S\,ES \rightarrow U$. *The mapping from a session to a user.*
- $SessionRole: S\,ES \rightarrow 2^{R}$. *The mapping from a session to a set of roles.*

D. Fine-grained Access Control Mechanism

All access control mechanisms are based on a certain authorization model, which define how a system can implement the access control. According to Fuguand Ma and Fuchun Xu [2], the design of control model of fined-grained access to geospatial data include two parts: the authorization part, which means how to authorize the user, and the authentication part to reflect the authorized result. This section discusses these two issues specifically, and presents a viable model for access control.

1. The Authorization Model

The authorization model decides how to authorize a user, the granularity and the principle of the authorization. Based on RBAC model, In paper of Fuguand Ma and Fuchun Xu uses multi-level authorization to achieve the fine-grained access control. The first authorization authorizes the role of users, like to the RBAC model. And the second authorization level that authorizes the specific user, based on the attribution of the user.

The role authorization uses the most common method, the classic triple tuple, whose structure is: [2]

<R, RS, M>,

Where, R is an authorized role, RS is the resources that the role has access to, and M is the access model, including the Read or Write.

According to the principles of the authorization default, the second authorization is to determine whether a user is entitled to access the specific region and then dynamically and then authorize the user based on the user attribute. The structure of authorization is shown as follows: [2]

<U, P, T>,

Where, P is the polygon information necessary to authorize specific region, U is the authorized user, and T is the type of authorization, which is the positive or negative.

2. The Authentication

Depending on the authorization model, it is necessary that there is an appropriate access control mechanism to make it happen. On the authorization model above, there are two methods of authorization, so that the needs of the different methods of access control to achieve it. For the role authorization, which is a common method, use the common access control method the Access Control List to achieve it. ACL is easy to implement, although it is a long time when resources are enormous.

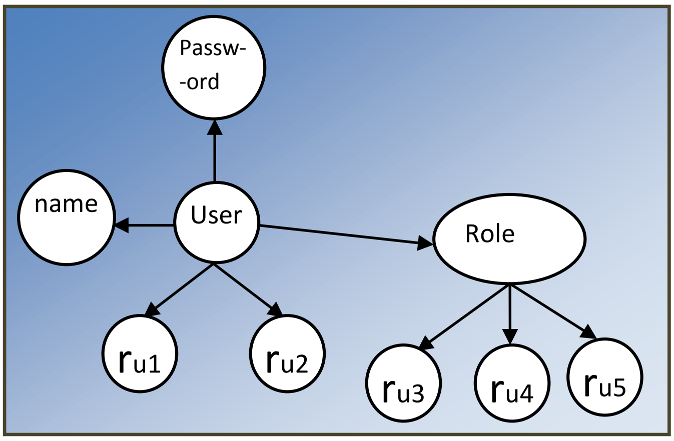

Fig. 1 Example of fine-grained access control system [11]

III. Analysis of Access Control Mechanism

Companies and businesses need a reliable and safe to manage and analyze their data system. Researchers have developed various types of security systems for data access. Role-based access control (RBAC) [9] is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies. Includes attracting increasing attention, particularly for commercial applications. The principal motivation behind RBAC is the need to specify and enforce security policies specific to the company in a way that maps naturally to the structure of an organization. In fact, a large number of commercial activities a user's identity is only relevant from the point of view of accountability. The conventional discretionary access controls, in the ownership of individual user data plays an important role, are not a good fit. Neither are the complete mandatory access controls, in which users have security clearances and objects have security classifications.

In particular, Fine-Grained Access Control (FGAC) system and Role-Based Access Control (RBAC) are widely used secure systems [10]. The FGAC system determines access control rights based on individual data. The access rights of every user allowed to access the data are stored inside the data itself [11]. In RBAC, access rights are defined based on the position or role of the user [12]. There may be multiple users with the same role. These multiple users may have access to the group or collection of data.

In FGAC, the access rights of a user are stored in the data itself. [11] Hence, if multiple users have access to the same data, the data must be replicated multiple times. This results in a complex system, which can't be scaled well. [13] The RBAC system has a simpler environment. Since all the users are grouped based on categories, the access right to data is based on the user's category. The problem with the RBAC system is the absence of identity of the user. Since all the users are recognized by their categories, the real identity of the user is lost. All activities of the user in the system are based on their categories, and the user's real identity is therefore unknown. Therefore, a RBAC system results in a less secure system.

Fuguand Ma and Fuchun Xu [2] describe the fine-grained access control for geospatial data that included two level authentications that can solve the problem of complexity and lack of security. The main objective of this fine grained access control mechanism is to inject the user's identity into the RBAC system while reducing the amount of data replication involved. In this system, all the users in the system are categorized into several groups, and at the same time, the users still retain their identity.

When the user accesses the data, the access permission is based on the user's category. All activities of the users are based on the users' identity and category. This system is much simpler because data is not replicated.

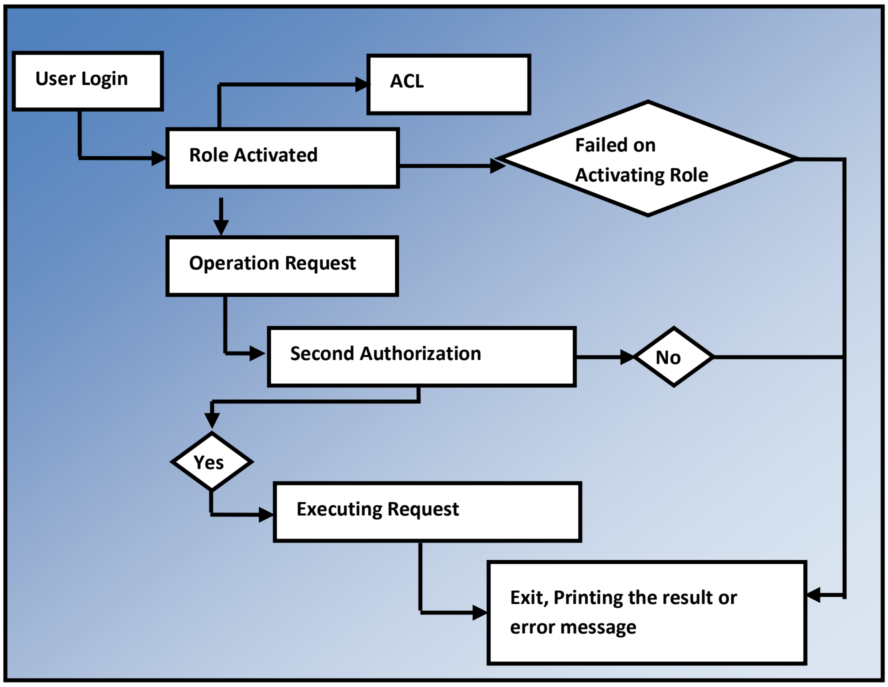

Fig. 2 The Framework of the fine-grained access control model [2]

IV. CONCLUSION

The data security access control has become the focus of GIS. Based on the survey paper, I conclude that on the basis of the RBAC, in this paper, a fine grained security access control model for spatial data is a big step to improve the access control system. The problem with the RBAC system is the absence of identity of the user. Since all the users are recognized by their categories, the real identity of the user is lost. One of the advantages of this system is the reduced information load required by the user and the data in the system compared to the pure FGAC system. The data is required to keep the role of the user who is allowed to access the data. When the user requests access to the data, the user's roles are matched to the data's rule to permit or deny access to the data. The other advantage of this system relates to the security issue. This fine-grained access system provides a more secure system compared to the RBAC system. In this system, the user ID is kept inside the data to backtrack when there is a security breach. In the RBAC system, this method is not provided. When a security breach occurs in an RBAC system, it is impossible to backtrack a use since the data does not keep the user's identification. However, the model ignores the real complexity, such as the principle of empowering; handle specific objects and so on. In the future, I will research for the principle of the authentication mechanism with improve model.

V. ACKNOWLEDGMENT

With the cooperation of my guide, I am highly indebted to Asst. Prof. Manali S. Rajput, for her valuable guidance and supervision regarding my topic as well as for providing necessary information regarding review paper. I am very much thankful to Asst. Prof. Dinesh Vaghela for helping me in text preparation.

References

1. Folger P., "Geospatial Information and Geographic Information Systems (GIS): Current Issues and Future Challenges", *Congressional Research Service*, Vol., pp.1-24, January 23, 2010.
2. Ma F., Gao Y., and Yan M., "The Fine-Grained Security Access Control of Spatial Data", the National Hi-Tech Research and Development Program of China, the National Natural Science Foundation of China, National key Technologies R&D Program of China, Vol., pp., 2010.
3. Bertino E., and Damiani M. L., "A Controlled Access to Spatial Data on Web", Conference on Geographic Information Science, *AGILE* Conference, Heraklion, Greece, Vol., pp., April 29-May 1, 2004.
4. Li G., Li C., Yu W., and Xie J., "Security Accessing Model for Web Service based Geo-spatial Data Sharing Application" Digital Earth Summit, *ISDE*, Nessebar, Bulgaria Vol., pp., June 12-14, 2010.

5. Cristina Nita-Rotaru and Ninghui Li, “A Framework for Role-Based Access Control in Group Communication Systems”
6. Maria Luisa Damiani and Elisa Bertino, “Access Control System for Geospatial Data and Application”
7. Hongi Chandra Tjan, “A Combined Fine-Grained and Role-Based Access Control Mechanism” May 2006.
8. Pierangela Samarati and Sabrina de Capitani di Vimercati, “Access Control: Policies, Models, and Mechanisms”, R. Focardi and R. Gorrieri (Eds.): FOSAD 2000, LNCS 2171, pp. 137–196, 2001.
9. Ravi S. Sandhu, Edward J. Cope, Hal L. Feinstein and Charles E. Youman, “Role-Based Access Control: A Multi-Dimensional View”, 1063-9527/94, 1994 IEEE
10. Andrei S.L., “Information retrieval in current research information system”, http://arxiv.org/ftp/cs/papers/0110/ 0110026.pdf , April 5, 2005].
11. Damiani E., Vimercati S. C., Paraboschi S., and Samarati P., “A finegrained access control system for XML documents.”, Fifth ACM Workshop on Information and System Security, Vol.5, No.2, 2002
12. Zhang L., Ahn G. J.,”A rule-based framework for role-based delegation and revocation.”, Sixth ACM Workshop on Information and System Security, Vol.6, No.3, 2003
13. Ahn G.J., Sandhu R., Kang M., “Injecting RBAC to secure a web-based workflow system”, Fifth ACM Workshop on Role-Based Access Control, Vol. 5, No.1, 2000.
14. “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”, National Spatial Data Infrastructure, Federal Geographic Data Committee, Reston Virginia, Vol., pp., June 2005.
15. Hansen F., and Oleshchuk V., “Spatial Role-Based Access Control Model for Wireless Networks”, IEEE International, Vol., pp., 2003
16. Kang T. C., “Introduction to Geographic Information Systems”, Tata Mcgraw Hill, Vol., pp. 1-40, April 2007.
17. Keating G. N., Rich P. M., and Witkowski M. S., “Challenges for Enterprise GIS”, URISA Journal, Vol. 15, pp. 2, 2003.
18. Mclnerney D., “Introduction to Spatial Data Types”, UII Summer School, Vol., pp., June 16, 2009.
19. “Procedure for Distributing Maps and GIS Data that are Security Sensitive”, PSC, Vol., pp.1-3, Nov. 12, 2008.
20. Zeng Y. H., Wei Z. K., and Yin Q., “Research on Spatial Database: A Secure Access Mechanism,” Machine Learning & Cybernetics, IEEE International Conference, Hong-Kong, Vol. 6, No., pp. 1-4, 19-22 August 2007.

AUTHOR(S) PROFILE

Kalpesh Chaudhari, received the Bachelor of Engineering degree in Computer Engineering from Government Engineering College Modasa under North Gujarat University in 2011, pursuing Master of Engineering degree in Computer Science and Engineering from Parul Institute of Technology under Gujarat Technological University, Ahmedabad.