A Location-based Secure Access Control Mechanism for Geospatial Data

Manali Singh Rajpoot
Maulana Azad National Institute of Technology
Bhopal, 462051(M.P), India

ABSTRACT

Nowadays due to the advancements in spatial data acquisition technologies, data acquisition technologies are producing mass high precision spatial data. 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, so security concerns of spatial database are also different from relational data. Thus spatial data requires special security policies and implementation of these security policies. In this work, a secure access control mechanism for geospatial data is developed. In this method, security is provided on two levels. In first level, authorization to every user is provided; thus a user can access only that part of spatial database, over which he has authority to access. In second level, access is controlled over an image; based on the location over which a user needs to access data and access is provided only to that part of an image.

Keywords

Geospatial data, partial access, geographical information system, location-based, raster file formats

1. INTRODUCTION

In today's scenario [1] geographical information system is widely spreading in every field of society like military affairs, disaster defense, environmental planning, electronic government affairs and emergency management etc. Core of a GIS system is spatial database; and [3, 4] nowadays 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, and with large coverage of area. Due to these issues sensitivity of spatial data has increased too many folds. To store such high precision data onto the database is a big challenge today, because spatial database is different from relational database as it contains data along with its location into the database. Thus security concerns of spatial database are also different from relational data. Spatial data requires special security policies and implementation of these security policies. Major security concerns of the geospatial data are based on authentication, integrity & security of data and secure transmission of spatial data over the network.

In this work, a secure access control mechanism is developed. In this method, security is provided on two levels. In first level, authorization to every user is provided so that a user can access only that part of spatial database, over which he has authority to access. In second level, access is controlled over an image; based on the location over which a user needs to access data and provide access to only that part of an image.

2. BACKGROUND

Various access control methods have been designed and implemented to secure geospatial data. According to the method proposed in [6] the relationship of roles and authorities is saved on a role control table which is maintained on the database server. For a client to access spatial database, firstly he has to register himself to spatial database server, and send his basic information including his name, ID, password, authorization code, role and ID. Once he submits his basic information, database server returns authorization code and based on his authorization code, he can register his certificate from database server by right of their login password. When users access the spatial database, they transmit their own certificates and roles to the database server, and then the server confirms the validity of their identities based on their certificates and lookups the role control table based on their roles in order to decide their authorities.

One another method is Fine Grained Security Access Control Method proposed in [8]. It is based on Role Based Access Control Method. In this method the authorization mechanism used is a double authorization, and it is refined gradually. The two authorization methods used restrict the user's access in two directions horizontal & vertical respectively. Similarly to RBAC, by the first authorization, in this authorization all users are provided with their appropriate roles and users get the appropriate permissions of the role. It is the authorization to layers, with a horizontal layer as a unit. The Secondary authorization judges whether the user has access to the data within a particular region based on the attribute information of the user stored. It is processed through layers in the vertical direction. In the implementation process, a user gets the layers about location through the horizontal authorization firstly. When the second authorization is further required, the vertical authorization will decide whether the user has access to the data within the specific regions.

In these two mechanisms discussed above a particular user is granted access over the whole image for which he is authorized to access, whether he needs to access whole image or not.

2.1 Need of the Method

The data stored in the spatial images contains information of earth surface features like land, ground, rocks, water, sea & ocean; some of these images contain information of very broad area. For example satellite images contains data of whole continent, aerial photographs contains area of whole of a state. But usually people working over projects of GIS do not need such broad area for their work. When these persons access that whole image while requiring only a small part of it; processing speed also gets slow & time consumption also increases. Due to these issues we need to implement a security policy in which we provide access only to that part of an image where a user is actually interested to work.

3. DATA MODEL OF THE METHOD

To access the database a user first register himself to the database server to gain the security credentials to access the database. Registration is done by the security manager. User provides his/her identity to the security manager, and according to user's identity his registration is done & database is maintained by database manager. Once registration is completed; one UserID is generated by the security manager. UserID is the security credential here; UserID is generated to each user according to his/her identity which defines his/her authorization to access database.

Database stores all the spatial data. Data in the database can be uploaded only by the administrator of the database. If administrator uploads any image file to the database, firstly it will be sent to the security manager. Security manager finds the location of the image & then database manager decides as to which database it should be stored. Database server maintains the file storage, access of the various users onto the database, web requests; converts the requests of various users to the security manager. Once their request is accepted by the security manager, it gives response to them.

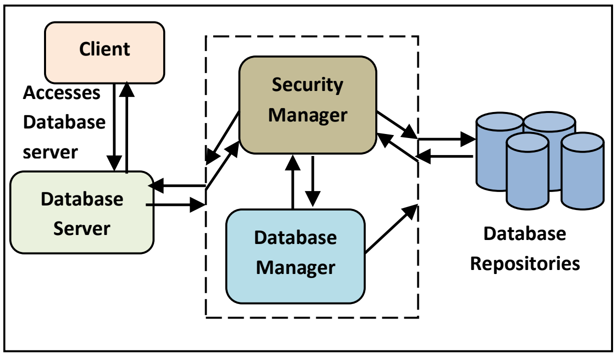

Fig 1: Data Model of the Method

4. MECHANISM OF AUTHORIZATION

To access GIS data users from all areas register themselves on the database with some specific attributes. All the users will be having one identity attribute according to which every user will get authorization on the database. During registration user will enter certain important information regarding him like firstname, lastname, location, EmailID and identity attribute. Once they entered this information, they will get one UserID based on the identity attribute, it decides their authorization. The authorization mechanism used in this method is double authorization. We authorize each user at two levels. In the first authorization all the users are categorized into three different classes according to the identity attribute. According to this authorization users can access parts of databases based on their authority.

During the time of registration users have entered one attribute *location*. This attribute is the location which he/she wants to use in his work. This attribute will define the location he wants to access from the image. So whenever a user will access any image from the database, this attribute will get activated & he will be able to access that part of the image, and rest part of image will be omitted. It defines second level of authorization.

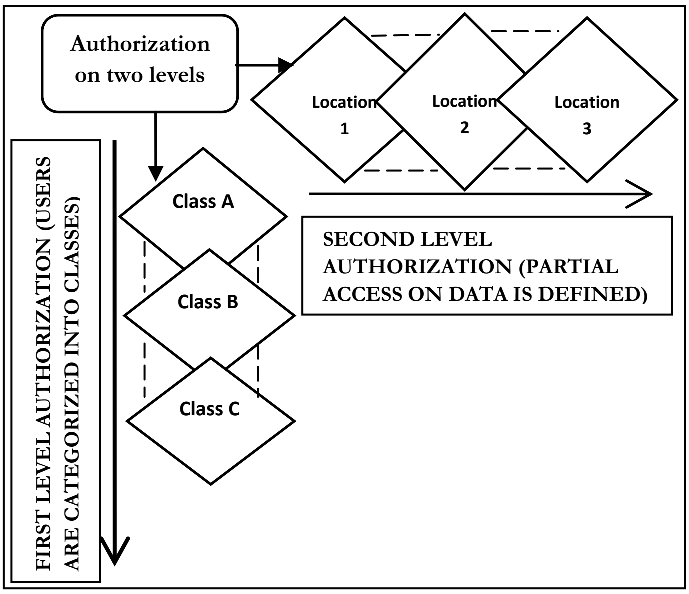
Authorization on two levels
Location 1
Location 2
Location 3
Class A
Class B
Class C
SECOND LEVEL AUTHORIZATION (PARTIAL ACCESS ON DATA IS DEFINED)
FIRST LEVEL AUTHORIZATION (USERS ARE CATEGORIZED INTO CLASSES)

Fig 2: Mechanism of Authorization

Images can only be uploaded onto the database by the administrator of the database. Spatial images are stored in the database ordered according to the locations they contain.

5. FRAMEWORK OF THE ACCESS CONTROL METHOD

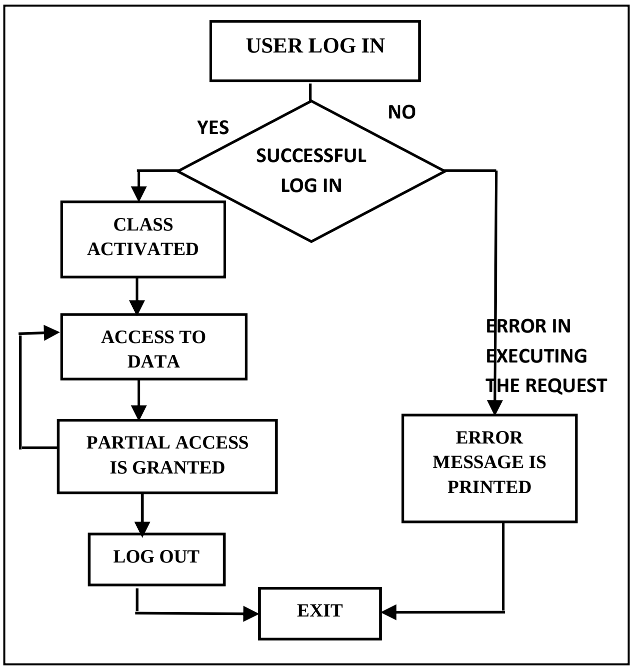

Fig 3: Framework of Access Control Method

As the user successfully enters the UserID & password on the server his class will get activated & access is granted to him on the database. If the user gets failed to log on to server then an error message will be printed on the screen specifying the error which has occurred while processing the request.

Now the user is granted with the data that he can access on the server; as he accesses to a particular image file, the location attribute will start working & he will be granted access only to that part of the image which is defined by the location attribute & rest part is omitted. Here the image is cropped to generate the image which a user wants to access from the original image saved on the server. After this as soon as the user has accessed the generated image, this generated image will automatically be destroyed & original image will be sustained on the database server.

6. REALIZATION OF SECURITY MODEL

This security model is implemented in PHP with ImageMagick extension and MySQL server. Image resolution of an image is obtained by the ImageMagick command and image is cropped with PHP command. According to my work users with class A membership can access all the images from the database, class B user can access images with resolution 100 dots per inch (dpi) or less and class C user can access images with resolution 72 dpi or less.

6.1 Realization of security model on first level of authorization

Here three images of Bhopal Lake (India) are taken with image resolutions of 120, 96 and 71 dpi. There are three users user1, user2 and user3 having membership of class A, class B and class C respectively. So user1 can access all the three images, user2 can access two images with resolution of 96 and 72 dpi, and user3 can access image with resolution 72 dpi only. Locations taken are 5 parts of India, North, South, Mid, East and West.

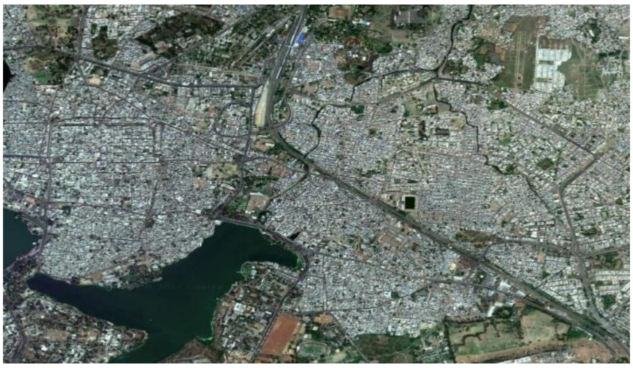

Fig 4: Image with Resolution 120 dpi (Class A User)

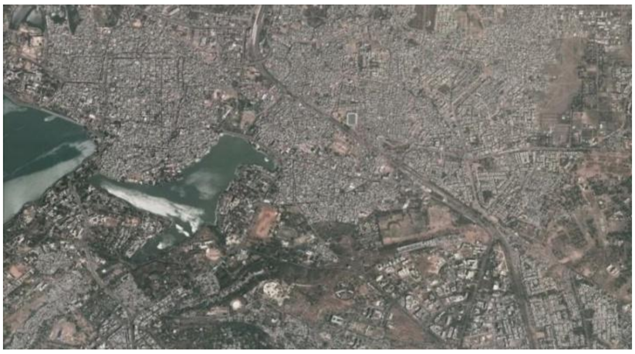

Fig 5: Image with Resolution 96 dpi (Class B User)

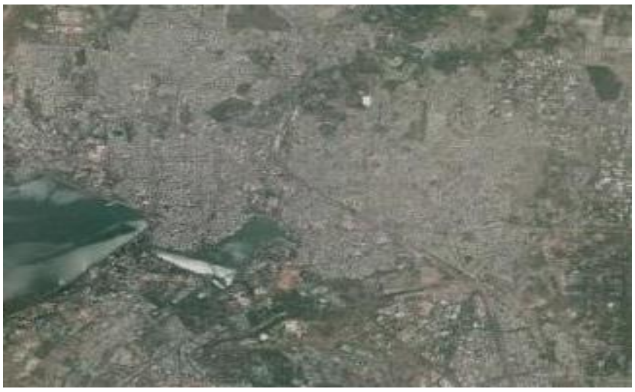

Fig 6: Image with Resolution 72 dpi (Class C User)

6.2 Realization of security model on second level of authorization

Here is an image of India stored in the database having resolution of 72 dpi, so this image can be accessed by users of all the classes. Three users' user1, user2 and user3 with locations Mid India, North India and South India respectively access this image.

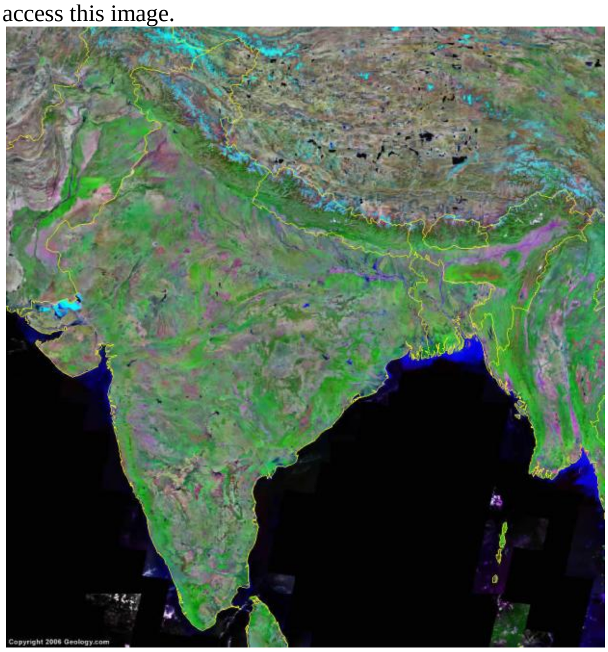

Fig 7(a): An Image Stored in the Database

Images generated for users user1, user2 and user3 are the cropped images of the original image.

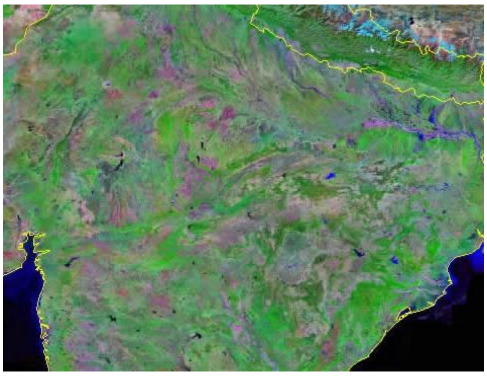

Fig 7(b): User1 Image

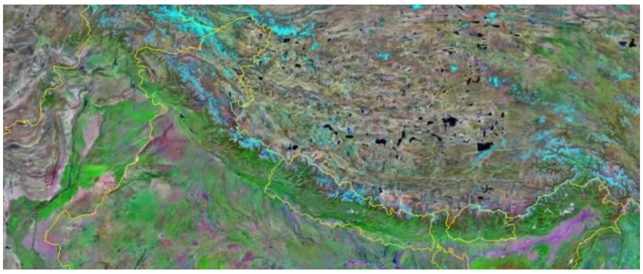

Fig 7 (c): User2 Image

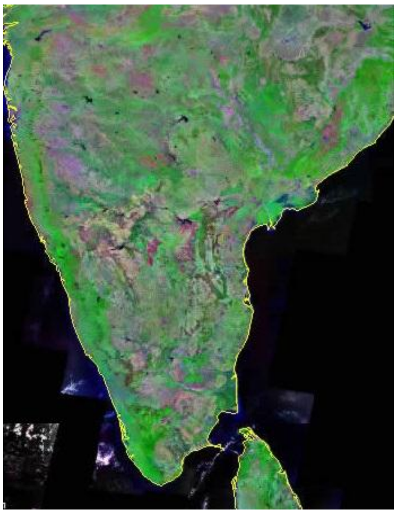

Fig 7 (d): User3 Image

7. RESULTS AND DISCUSSION

In the example given above, we analyzed that in each case size of the cropped images on the disk is reduced by a high factor than the original image.

Table 1: Comparison of access time of Original Image with access times of Cropped Images

Case	Access time of images (ms)	Access time of cropped image (ms)	Reduction Factor
a)	64	13.8	¼
b)	64	25.5	1/(2.5)
c)	64	12.17	1/5

All these three images are accessed in a 100Mbps network. So we can see that access times of cropped images are reduced by a high factor than the access time of original image in each case.

8. CONCLUSIONS

Main security issues for spatial data are access control, secure transmission of data, integrity of data, secure interoperable operations on GIS system.

In this work, an access control method is implemented in which access to the spatial data is controlled at two levels. At first level users will be categorized into various classes depending on their authority. Users will access parts of database on the basis of their authority. Accesses on images are controlled on the basis of their resolution. Every class of user has a fixed resolution as up to which image resolution of images they can access. During registration users are asked with location as to where they want to work. So in the second level of authorization; when a user accesses the spatial images, he can access only that location of an image which he has specified during registration. Due to this access time of the image on the network will be less and a significant amount of time will be saved.

In this project database used is MySQL so image files with limited disk size can be stored into the database, and MySQL does not support all the raster image file formats, so they are converted them into appropriate format. I recommend you to use spatial databases like Oracle spatial, PostgreSQL or Microsoft SQL server to store large size images files as they support image files with large disk sizes on the server and also these databases support all spatial image file formats, which are used in a GIS, so work can be performed with more accuracy and precision.

9. ACKNOWLEDGMENTS

This work would not have been possible without the guidance and help of my supervisors Dr. S K Katiyar and Dr. Deepak Singh Tomar, who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study. I am also grateful to my parents and my family members for their love, support and prayers. Last but not the least, I sincerely express my gratitude to almighty for his heavenly blessings.

10. REFERENCES

[1] Bertino E., Thuraisingham B., Gertz M., and Damiani M. L., “Security and Privacy for Geospatial Data: Concepts and Research Directions”, Inaugural Paper for SPRINGL Workshop, SPRINGL, Irvine USA, Vol., pp., 2008.

[2] 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.

[3] Folger P., “Geospatial Information and Geographic Information Systems (GIS): Current Issues and Future Challenges”, Congressional Research Service, Vol., pp.1-24, January 23, 2010.

[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] Orlandl E., “Integrity and Security in AM/FM-GIS”, IEEE International, Roma, Italy, Vol., pp. 26-00151, 1993.

[6] 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.

[7] Kiefer R. W., Lillesand T. M., and Chipman J. W., “Remote Sensing and Image Interpretation,” John Willey and Sons, V edition, University of Wisconsin, Madison, pp. 1-25, 2009.

[8] Ma F., Gao Y., and Yan M., “The Fine-Grained Security Access Control of Spatial Data”, the National Hi-Tech Research and Development Program 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., 2007.

[9] Li G., "Research of Key Technologies on Encrypting Vector Spatial Data in Oracle Spatial", IEEE International, Vol., pp., 2010.

[10] Keating G. N., Rich P. M., and Witkowski M. S., "Challenges for Enterprise GIS", URISA Journal, Vol. 15, pp. 2, 2003.

[11] Wu C., Li C., Lv. X., and Li J., "Geological Data Access Security Mechanism Based on Grid GIS", Grid GIS Soft and Important Application, Grid GIS Business System Research, IEEE International, Vol., pp., 2011.

[12] Sayed E., and Stoltzfus E., "Spatial Databases GIS Case Studies", UC Berkeley, IEOR, Vol., pp., Dec 4, 2002.

[13] Zhang Y., and Wang Q., "Security Model for Distributed GIS Spatial Data", Symposium on Information Science and Engineering, IEEE International, Vol., pp., 2008.