A Location based Secure Access Control Method for Geospatial Data using Fine Grained Security Access Method

Ms. Jalpa K. Goswami[1] Prof. Chetan Chauhan[2]
[1] P. G. Student [2]Professor
[1, 2]Department of Computer Engineering
[1, 2]Noble Group of Institution-Junagadh, Gujarat, India

Abstract—Geospatial data is data about the geographic location 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 photogram metric 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. 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. In this paper the major security concerns of geospatial data are analyzed. Spatial data and access control methods developed to provide secure access over the spatial database are analyzed and studied. The data models and access control some issues to be resolved for spatial data security are found. In this paper a secure access control method is developed. In this method security over geospatial data on two levels is provided. In first level we provide authorization to every user so that a user can access only that part of spatial database, over which he/she has authority to access. In second level we control access over an image; based on the location over which a user wants to access data and provide access to only that part of an image, so that a significant amount of access time can be saved and quick access to the data can be provided.

Keywords: Geographical Information System - (GIS), GIS data models, spatial data, spatial database, Role Based Access Control - (RBAC) Registration Authority - (RA), Access Control List - (ACL), Certificate authority service - (CAS), spatial Database Enterprise - (SDE), Spatial Database Management System - (SDBMS)

I. Introduction to Geographical Information System (GIS)

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. According to Folger the power of GIS is the ability to combine geospatial information in unique ways by layers or themes and extract something new [1].

II. Geospatial Data

Geospatial is used as a synonym for "geometric", "graphical" and "geographic" who means related to the earth, so in spatial data we store information related to the earth surface.

III. GIS Data Models

GIS Data Models are sets of mathematical construct for representing and describing the geographical features of earth surface. Two commonly used GIS data models are Raster Data Model and Vector Data Model.

A. Raster Data Model

This data model represents continuous data over space. Raster data is divided into rows and columns; it forms a regular grid structure. This grid structure contains individual elements commonly called cells or pixels.

B. Vector Data Model

It is used to represent geographic features of earth surface. Points represent geographic features too small to be depicted as lines or areas; Lines represent geographic features too narrow to depict as area; and areas represent homogeneous geographic features. A Cartesian coordinate system references real world locations. In a vector data model, each location is recorded as a single x, y coordinate. Points are recorded as a single coordinate. Lines are recorded as a series of ordered x, y coordinates. Areas are recorded as a series of Cartesian coordinates defining line segments that enclose an area.

IV. Spatial Database

Spatial database is different from a relational database, as it includes geographical and attribute data. It is used to effectively store and query data related to objects in space, including points, lines and polygon items.

Advances in relational database management technology giving users the option of storing their GIS data in a spatial database rather than using file based storage.

A. Access Control Methods for Geospatial Data

Two important access control methods reviewed are as follows:

1) Role Based Access Control Method:

According to the method proposed by Zeng et al. the relationship of roles and authorities is saved on a role control table which is maintained on the database server [7]. For a client to access spatial database, firstly she has to register herself to spatial database server, and send her basic information including her name, ID, password, authorization code, role and ID.

Once she submits her basic information, database server returns authorization code and based on her authorization code, she can register her 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.

Certificates of the server agent, clients and Registration authority (RA), are generated and maintained by the Certificate authority service (CAS), its main task is to generate and manage certificates.

Registration of all clients and distribution of roles to them is maintained by the Registration Authority (RA).

The server agent is an agency between spatial database enterprise (SDE) and spatial database, with which clients submit their access requests to Spatial Database Management System (SDBMS) and SDE To clients.

2) Fine Grained Security Access Control

One another method is Fine Grained Security Access Control method is based on Role Based Access Control Method [5].

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 judge 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.

On the authorization model above, there are two authorization methods, so we need different access control methods to achieve it.

We use Access Control List method to apply access control and to authorize the end users with their roles. ACL is easy to implement, though it is time consuming when the resources are massive.

The second authorization is the fine-grained authorization. The fine-grained authorization requires the pre-processing of the polygon information, then according to the type of authorization, overlay the polygon and obtain the authorized region.

Now detection of conflict of role authorization is performed to detect if any conflict is there. If any conflict found then resolve it and return to the region that the user can access.

V. Mechanism of Authorization

To access the GIS data, users from all areas register themselves on the database with some specific attributes necessary to registration. All the users will be having one identity attribute according to which every user will get authorization on the database. This identity attribute will be unique to every end user who will use the database without this attribute a user can not register him/her on the database.

During registration user will enter certain important information regarding him/her like first name, last name, password (he/she wants to use), location (they want data to use), Email ID and identity attribute. Once they entered this information they will get authorization according to identity attribute.

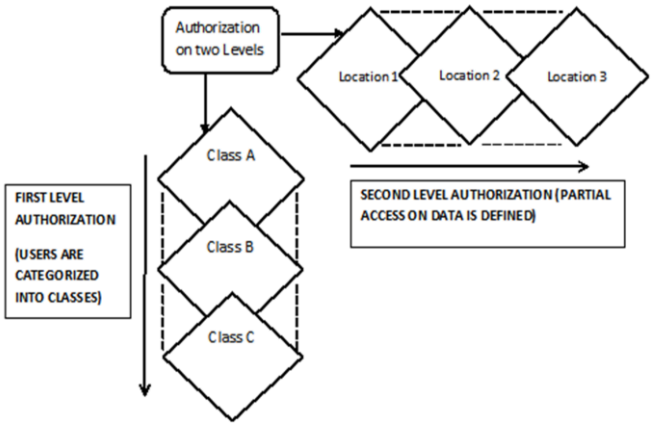

Fig. 1: Mechanism of Authorization [5]

As a user has entered all the information during the registration process a user ID will be generated it will define the authorization of user. So whenever user wants to access the database this user ID will be entered by him/her it will authorize him/her to access the database. The access control method used in this work is Mandatory access control.

All the privileges which will be defined to every user are predefined by the administrator of the database and cannot be redefined by any user. The authorization mechanism used in this method is double authorization. Every user is a authorized at two levels; each level is discussed as following bellow.

A. First level of Authorization:

Firstly all users will be categorized with their class according to the identity attribute. This attribute defines the authority of each user it defines a user belongs to which class. According to identity attribute a user with high authority will be provided with high class and a user with less priority will be categorized into less authority class and like this every user will be categorized into different classes.

This categorization is predefined by the administrator of database & cannot be changed by any end user. This method categorizes all the users into three different classes like Class A users, Class B users and Class C users; every class is discussed in brief.

Class A users can access almost all images except private spatial data which is not accessible to end users due to privacy policies and is put private and is non-accessible. Class A users can access almost all images with any resolution and are provided with maximum authority than any other class users.

Class B users are provided with second level of authority. Class B users can access images with resolution 100 dots per inch (dpi) or less. These users can access moderate resolution images and cannot access images with more than 100 dpi resolution. This policy is predefined by the administrator.

Class C users can access images with resolution 75 dpi or less from GIS database. They are authorized with the least level authority according to their identity. They can access only a small part of the database from the database.

B. Second level of Authorization:

In this level of authorization every user is provided Partial Access to the GIS images and a user can access only a part of the image according to the location entered by him during registration. It will define second level of authorization in the authorization method.

During the time of registration users have entered one attribute location. This attribute is the location where 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 and a user will be able to access that part of the image which he/she is supposed to access and rest part of the image will be inaccessible to him/her.

So due to this attribute a user can access only that part of the image which is of his/her relevant use rest part of the image will be hidden from him/her.

VI. IMPLEMENTATION

The work is implemented over the images of India and locations to be chosen are five regions of India, so users can choose their location as region of India on which region want to access. Regions are five parts North India, South India, Mid India, West India and East India.

We are using PHP language and MYSQL database with Java script because it offers a wide and flexible range of capabilities for the data.

This is the First level of Authorization. Users are categorized into Classes like class A, class B and class C. When user selects class A they access the following data as per categories of the classes. This is the First Level of Authorization of Class A user.

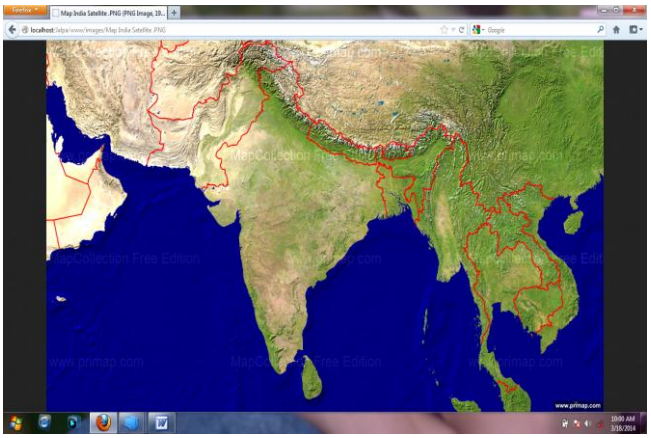

Fig. 2: First level of Authorization of Class A user

This is the Second level of Authorization. Users have to access data within a Location. Locations are like North India, South India, Mid India, East India and West India. When user selects Location South India then user can access the following South India as per selected location.

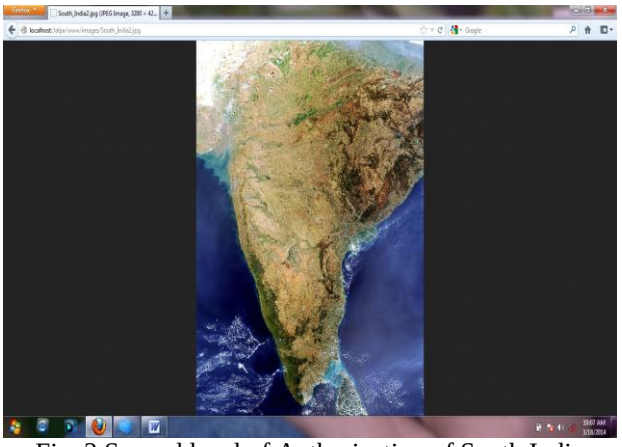

Fig. 3.Second level of Authorization of South India Location

VII. RESULTS AND DISCUSSION

These images are stored in database with different image resolutions.

Fig. 4.Image with Resolution 120 dpi

This image has resolution of 120 dpi, so only class A user can access this image class B, and class C users cannot access this image.

Fig. 5.Image with Resolution 96 dpi

This image has resolution of 96 dpi, so only class A and class B user can access this image; class C users cannot access this image.

Fig. 6.Image with Resolution 72 dpi

This image has resolution of 72 dpi so this image can be accessed by users of all the classes; so users of class A, class B as well as class C can access this image.

Access Time of Image is reduced

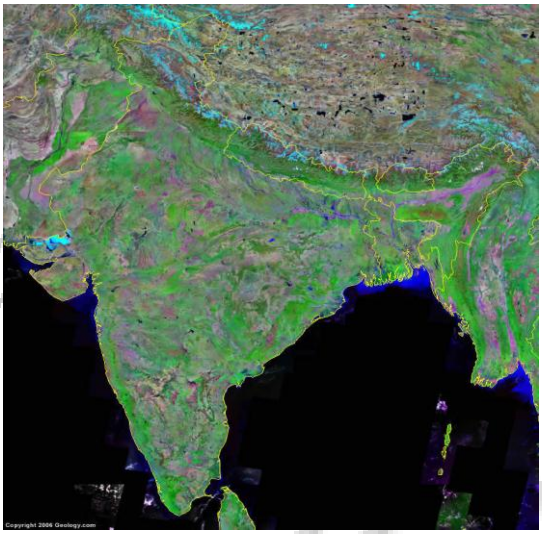

Fig. 7: Original Image

When users access this image from the database the image generated is the cropped image of this image, so the access time of cropped images is less than original image in each case. This image dimensions are 879×911 pixels. Size of this image on the disk is 800KB.So time required to access this image file in a 100Mbps network is 800*8/100000= 64ms.

(1) User1 with Mid India location accessing this image file, image generated is:

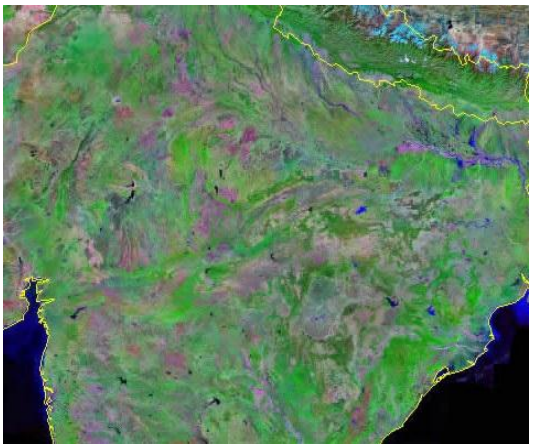

Fig. 8: User1 Image

This image dimensions are 477×362pixels. Its size on disk is 172K. So its access time over the network is: 172*8/100000 = 13.8ms

(2) When user2 with North India Location accessing this image file, image generated is:

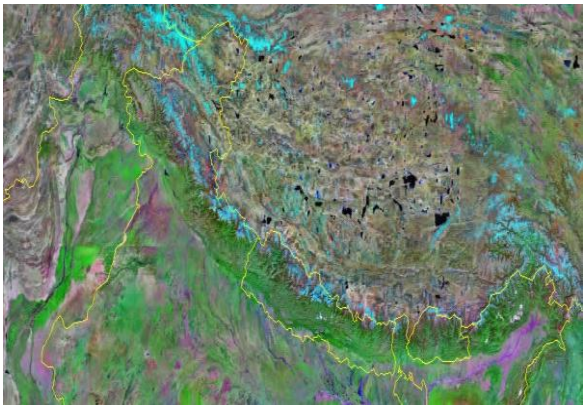

Fig. 9: User2 Image

This image dimensions are 878×364 pixels. Size on disk is 320KB And Access time: 320*8/100000 = 25.5ms

(3) User3 with South India Location accessing this image file, image generated is:

Fig. 10: User3 Image

This image dimensions are 346×440 pixels. Size on disk is 152KB. Access Time: 152*8/100000 = 12.17ms

So we can see that access times of cropped images are very less than the access time of original image.

VIII. Conclusion

Nowadays advancements in sensor technologies, satellite imagery and field surveys have made it possible to collect large amount of geospatial data with high precision with large coverage of area and with high resolution.
This advancement in the technology has raised many security and privacy concerns for people, property and system.

Main security issues for spatial data are access control, secure transmission of data, integrity of data, secure interoperable operations on GIS system and there is a need to develop strong security policies to handle the security issues on the spatial data and also the implementation of these security policies.

In our work, we have implemented an access control method 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.

A high authority user can access high resolution images and a less authority user can access only less resolution images.

During registration users are asked with location as to where they want to work, so in second level when a user accesses the spatial images he/she can only access only that location of an image which he specified during registration.

In conventional methods users are provided with access to whole image whether they want to access to whole area or not so in that case access time is very high but if we provide with access only to a part of image then access time to access the image will be less so that a significant amount of time will be saved if many users are accessing the database at the same time.

Also this method we provide access control to the database so that high precision image files can only be accessed by the users who have authority to access them.

REFERENCES

[1] Peter Folger, "Geospatial Information and Geographic Information Systems (GIS): Current Issues and Future Challenges", Congressional Research Service, January 23, 2010.
[2] Prof. Qiming Zhou, "GIS Data Modeling", 2006
[3] Elisa Bertino, Michael Gertz, Bhavani Thuraisingham, Maria Luisa Damiani, "Security and Privacy for Geospatial Data: Concepts and Research Directions", Inaugural Paper for SPRINGL Workshop, SPRINGL, Irvine USA, 2008.
[4] Guoqing Li, Chenhui Li, Wenyang Yu and Jibo Xie, "Security Accessing Model for Web Service based Geo-spatial Data Sharing Application" 3rd ISDE DIGITAL EARTH SUMMIT 12-14 June, 2010.
[5] Fuguang Ma*, Yong Gao, Menglong Yan., "The Fine-Grained Security Access Control of Spatial Data" National Hi-Tech Research and Development Program of China, the National Natural Science Foundation of China, National Key Technologies R&D Program of Chinaand Major National S&T Program of China, 2009.
[6] Orlandl Eugdo, "Integrity and Security in AM/FM-GIS", IEEE International, Roma, Italy, IEEE 1993.
[7] Yi-Hong Zeng, Zu-Kuan Wei, Qian Yin, "Research on Spatial Database: A Secure Access Mechanism," Machine Learning & Cybernetics, IEEE International Conference, Hong-Kong, 19-22 August 2007.
[8] Yanqun Zhang, Qianping Wang, "Security Model for Distributed GIS Spatial Data", Symposium on Information Science and Engineering, IEEE International, 2008.
[9] Xing Han-fa, Cui Bing-liang, Xu Li-lin, "An Mixed Access control method Based on Trust and Role", Second IITA International Conference on Geoscience and Remote Sensing, IEEE 2010.
[10] Guoliang Tang, Feng Yang, Zhiyong Zhang, Jiexin Pu, "A Extended Role-based Access Controls Model", Temporal,Spatial,Workflowed and Attributed Role-based Access Controls Model Fourth International Conference on Genetic and Evolutionary Computing, IEEE 2010.
[11] Ms. Jalpa K. Goswami, Prof. Chetan Chauhan, "Introduction to Geographical Information System, GIS data models, spatial data, spatial database, A Location based Secure Access Control Method for Geospatial Data" IJSRD - International Journal for Scientific Research & Development, Vol. 1, Issue 9, 2013 | ISSN (online): 2321-0613

