POLITECNICO DI MILANO

Scuola di Ingegneria dei Sistemi

POLO TERRITORIALE DI COMO

Master of Science in

Management, Economics and Industrial Engineering

Security of Geographic Information System

Supervisor: **Prof. Mariagrazia Fugini**

Master Graduation Thesis by: **Wan Xiaogao**

Matricola Number: **786456**

Academic Year 2012/2013

Security of Geographic Information System

Abstract

With the development of information technology, the value and usability of Geographic Information Systems (GIS) are becoming highly crucial. GIS are more and more being applied not only to geography and information acquisition, but also to every field of society and *decision making*. Nowadays, people make analysis and decisions based on the GIS information, which is desirable, convenient and effective. However, the security problems of GIS are becoming increasingly prominent with the development of GIS and the enlargement of GIS users' community. Considering the characteristics and the volumes of available GIS data, these are likely to contain various attributes regarding individual information so needing protection of sensitivity and confidentiality in GIS. In this thesis, we summarize the GIS security research status. Then, we describe the concept of *context analysis* that can be performed by accessing spatial objects of a GIS for decision making e.g. in public administrations or at stakeholders repositories. This idea of context analysis is the basis for making our security considerations. Moreover, we are concerned with confidentiality only, while integrity is not tackled in our assumptions. We consider that GIS data are clustered in terms of their similar context attributes and that they are inspected (read) for analysis purposes. On these premises, we propose an *authorization model* allowing GIS users to gain specifically-required GIS information from large volumes of information for decision making. The authorization model useful for context analysis is given in terms of GIS data structures and of operations that can be performed for context analysis, such as zooming an object, observing some of its spatial attributes, selecting a detail of the object and analyzing it. The authorization model is based on role-based access control (RBAC), in which a role and permission should be distributed before users are allowed to access a specific object. It considers also hierarchical privileges in that objects in a GIS are considered here as organized at various vertical levels and can be inspected moving along a vertical dimension: privileges to access vertical dimensions are taken into account in our model by proposing inheritance of privileges along the vertical dimension. The model at work is specified using Unified Modeling Language (UML) and by proposing a security architecture of authorization components to be included in commercial GIS products.

Key Words: Security, GIS, RBAC, UML, Context Data, Decision Making Analysis, Authorization Control

Sommario

Il valore e l'usabilità dei Sistemi Informativi Geografici - Geographic Information Systems (GIS) stanno diventando di grande rilevanza. I GIS vengono sempre più utilizzati per il *decision making*. Contestualmente, stanno crescendo i problemi di sicurezza informatica nei GIS dovuti al volume di dati gestiti, alle varie informazioni sugli individui e ai requisiti di sensitività e confidenzialità.
Questa tesi analizza gli avanzamenti della sicurezza per i GIS; definisce il concetto di *context analysis* eseguita accedendo oggetti spaziali per il *decision making* per es. nelle Pubbliche Amministrazioni o nei vari repository degli stakeholder. Considerando solo la confidenzialità, si propongono cluster di dati relativi a un certo contesto di analisi e si propone un modello di autorizzazione per i GIS. Il modello definisce quali utenti possono accedere a quali dati spaziali, a quali attributi di contesto e come si può zoomare su questi dati. Il modello si basa sui concetti di Role-Based Access Control (RBAC), che controlla l'accesso utente in base al suo ruolo e su gerarchie di privilegi e di oggetti del GIS. Pertanto, il modello definisce autorizzazioni orizzontali (per i contesti) e verticali (per I diversi livelli di granularità degli oggetti GIS). I principali aspetti del modello di autorizzazione sono specificati in UML.

Parole Chiave: Sicurezza degli oggetti spaziali, geo-referenziazione, controllo di accesso, modello di autorizzazione basato su ruoli.

Content

List of Figures

Table

1. Introduction

GIS stands for Geographic Information Systems, often defined as a computerized database management system for capture, storage, retrieval, analysis, and display of spatial data. Any data that includes information about location—a street address, zip code, census tract, or longitude and latitude coordinates—can be considered spatial. Many different types of data can be integrated into GIS and represented as a map layer. When these layers are drawn on top of each other, spatial patterns and relationships often emerge. The most common GIS product is a map, but GIS can be used to generate answers to queries or as part of spatial statistical analysis (Cartographic Modeling Laboratory, 2004).

With GIS integrating hardware, software and data, information based on geographic reference can be captured, managed, analyzed and displayed. People can view, understand, question, interpret and visualize GIS data through the Internet in various ways that reflect relationships, patterns and trends in the form of maps, globes, reports and charts. All these information can be shared easily and quickly. And GIS technology can be used in many organization information systems, such as government, universities, enterprises, and so on. Different users can take the advantages of GIS in terms of their distinctive requirements. For example, some users want to view special objects with geographic attributes and context attributes, others can use GIS to analyze context objects and make decisions based on these context analysis, while governments and some organizations can utilize GIS to deploy emergency rescue and even to forecast and predict natural disasters.

GIS are currently widely used and change the way we see the world around us and overcome boundary barriers. Countries have been setting up their own Spatial Data Infrastructures (SDI) and have been sharing geospatial information globally [4]. Some information sharing standards have been established nationally and globally, which make GIS data information interoperable and compatible. This interoperability facilitates information sharing and helps improve users' experience. People nowadays get benefits from GIS, such as cost savings and increased efficiency by optimizing maintenance service of specific geo areas, decision making about location including in the realm of real estate sites, route selection, natural resource extraction and evacuation planning and emergency dealing where location is critical, improving communication among different areas, department, organizations and team, better recording information and managing geographically. For repository management, we assume that objects have geographic attributes and context attributes, for example, one object is household building, its geographic attributes are longitude and latitude reference(34° 54' north latitude, 118° 34' east longitude), its context attributes can be economic attributes because it can be used to analyze economic status by utilizing such data as household income and tax payment and so on, and it can also be education and science attributes because it can used to assist education analysis such as population and education expense. With geographic attributes, we can

define places where resources are and also record relevant quantities and densities. With context attributes, we can analyze related contexts and make favorable decisions. By viewing the information change over a period of time through GIS, we can find out pattern and trends of objects so that we can make better decisions.

The Spatial Objects (SObj-s) are defined as objects such as maps, streets, buildings, rivers, forestry and parks, analyzed in special locations, which are assigned geographic and context attributes. These attributes can be handled to analyze corresponding objects. When we define a spatial object, we should provide some corresponding attributes, such as geo reference, object owner, object extension, object context and levels in terms of granularity and so forth. GIS SObj-s are distributed in the network with different information provision resources in order to provide complete information service and facilitate better decision making, which can be beneficial because data required in GIS are tremendously large and specifically detailed and must be contributed by outsourcing and sharing [1]. Considering SObj-s information provision, we should take into consideration information providers and information transmission security. In this sense, we need to distribute a role and permission to those who can read, write, modify or delete information. For users, because data are sensitive and confidential, are also required to apply a role and permission which enables them to read, zoom in or out, write, modify, delete. As a result, they can get much more reliable information and make better decisions based on valuable information. In order to manage SObj-s and provide context analysis information, relevant data are clustered in repository in different context forms, such as economic contexts, quality contexts, utility contexts and government contexts and so on. Meanwhile, geographic and demographic data should be provided and can be retrieved in every context condition because they are basically-used widely.

However, with the development of GIS, security problems are becoming more and more imperative, especially in military, public security, electronic affairs, power, digital cities and privacy and so forth but also in Public Administration repositories or in applications for the so called Smart Cities [13]. Recently, security threats facing GIS from are mainly from eavesdropping and intercepting, unauthorized access, sniffing, masquerading, vicious attack and internal attack. To tackle these threats, three general measures are taken: spatial information access control, spatial information transmission security and spatial information repository security. There are many researches on these three measures, but there is no integrated security technology system to guarantee security of GIS and satisfy application requirements of GIS from an overall and systemic point of view.

In order to protect confidentiality and sensitivity of GIS SObj-s, users' right to access a specific SObj should be controlled with respect to user's identification(roles and permissions). In fact, users with different identifications can access different data in terms of granularity. In the vertical level, users are allowed to access SObj

information in a hierarchical way, such as region, municipality, city, and town. In the horizontal level, users can be limited to access SObj-s or only some attributes thereof because of SObj-s sensitivity and confidentiality. For example, in the same level, common users can only view a house building's geo reference, extensions, but building manager can read the names of the house owners while a government employees can see and modify people's tax data referred to that building. Based on roles and permissions, users can access SObj-s at different details so as to protect data and improve GIS security under selective access modes.

Many research has been done to discuss GIS security issues. In the thesis, we first review such research works. Then, we define users, roles and permission relationship based on which we propose a GIS security model. In the model, we assume that different users can access GIS SObj-s with different purposes, in general for decision making in business environments [15] to perform data analysis under different contexts. Operatively, access modes, such as read, zoom in/out, write, modify and delete, must be defined for users on GIS SObj-s. We also assume that authorization issuers have designed a role and permission database and will assign these roles and permissions to different users when requested. Under these roles and permissions, a user can operate on GIS SObj-s in the vertical hierarchy and in the horizontal granularity.

Unified Modeling Language insert ref is considered by the International Standard Organization as industry standard for modeling software-intensive systems. In the thesis, UML is used to specify security so to understand GIS security issues. We will use class diagrams to show components and structure within SObj-s. GIS use cases, the GIS UX model, and the GIS analysis diagram and sequence diagrams model the structures and procedures of the GIS systems under security requirements.GIS should provide all kinds of information resources requested by users securely and efficiently. This requires GIS to not only prohibit different attacks and intrusions but also to maintain and recover information security when attacked and intruded. Furthermore, GIS should provide secrecy of different components when users access information by giving a role and permission.

This thesis's aim is to provide a security model based on roles using the RBAC model. User access requirements and control are suggested after reviewing researches status and giving UML specifications for roles. We also sketch how to manage SObj-s repository with respect with context analysis. Moreover, in order to let users access more specifically required spatial objects information, we introduce a security access function by selecting a specific area and filtering a required context. Finally, we discuss the use of the authorization model and its specification in a secure GIS architecture.

This thesis is organized as follows. In Section 2, we review current security researches on GIS and mainly in how to control access secrecy based on RBAC and data

protection. In Section 3, we define spatial objects and their attributes. We provide how to manage data repository based on context analysis by clustering data with similar attributes creating a context. In Section 4, based on repository management and RBAC, we draw a class diagram for spatial objects and establish a security model. In Section 5, UML models secure GIS. In Section 6, we introduce security configuration in GIS to illustrate how to use the security model. In Section 7, we discuss the use of the security model in a GIS architecture.

2. Review of researches on security in GIS

GIS security is a global and imperative issue. Currently, GIS security researches mainly focus on spatial data security management, data sharing and transmission, user access control.

A role-based control access standard is discussed in the paper by [2]. They provided a unified model for RBAC as a standard model, which is intended to serve as a foundation for developing future standards, to solve uncertainty and confusion situation by unifying ideas from prior RBAC models, commercial products and research prototypes. Although RBAC is often considered a single access control and authorization model, RBAC is in fact composed of a number of models, each fit for a specific security management application. This model is organized into four levels of increasing functional capabilities called flat RBAC, hierarchical RBAC, constrained RBAC and systematic RBAC.

An authorization model is proposed in [3]. This model enables users to inspect spatial data securely in terms of contexts required and analyzed by users depending on users' roles and the data security classification model. Users gain vertical authorization in different layers and context authorization in the same layer to access specific authorized information. Based on context analysis, it is better to choose useful data information and make decisions.

A simplified GeoDRM model for SDI services is provided in [4]. Countries have been setting up their own Spatial Data Infrastructures (SDI) and have been sharing geospatial information globally. These advancements have recently raised many security, privacy, and safeguarding concerns. Digital Rights Management (DRM) technology attempts to control use of digital media by preventing access, copying or conversion to other formats by end users. Geospatial Digital Rights Management is similar paradigm that attempts to have a rights management system catering to specific issues with Geospatial entities. The paper describes details of the GeoDRM system for SDI services which can be independent of the participating components and yet be flexible enough to incorporate new and existing standards with same level of ease and also use open interoperable standards for rights management.

[5] analyzes the security solutions for Geographic Information Storage Systems (GISS)

within n-tier GIS architecture. The paper outlines the application of the main categories of database security for management spatial data. A file system within database(FSDB) with traditional and new encryption algorithms has been proposed to be used as a new GISS solution, which provides more safe and secure storage for spatial files and support centralized authentication and access control mechanism in legacy DSMS. Cryptography solutions as a topic of central importance to many aspects of network security are discussed in details. The paper also describes several traditional and new symmetric, fast and nonlinear encryption algorithms' implementation with fixed and flexible key size.

GEO-RBAC, an extension of the RBAC model to deal with spatial and location-based information, is presented in [6]. In GEO-RBAC, spatial entities are used to model objects, user positions, and geographically bounded roles. Roles are activated based on the position of the user. Besides a physical position, obtained from a given mobile terminal or a cellular phone, users are also assigned a logical and device independent position, representing the feature(the road, the town, the region) in which they are located. They introduced the concept of role schema, which specifies the name of the roles as well as the type of the role spatial boundary and the granularity of the logical position, to make the model more flexible and reusable. The GEO-RBAC is also extended to cope with hierarchies, modeling permission, users and activation inheritance.

[7] presents a secure access control in a Multi-user Geodatabase. An access control model is introduced in the spatial database, which enable different users to access predetermined views according to their access authorization. The paper proposes three different security architectures: single Multi-level database (multi-level relations), replicated Multi-level database and single multi-level database (Uni-level relations).

[8] demonstrates encryption technique in the database. In order to save time for encryption and decryption, data in the database are divided into sensitive data, non-sensitive data and user data. Non sensitive data can be stored and retrieved directly, but sensitive and user data should be stored and retrieved in symmetric encryption in terms of their role and permission.

[10] presents a signature scheme based on AES and ECC considering characteristics of spatial data's larger capacity, sensitivity and confidentiality. To grantee that identities of clients and servers are right and legal, the paper presents an identities authentication scheme based on ECC digital certificate, which not only implements unified management of certificate and private key to ensure the security of private keys, but also makes use of ECC certificate's smaller size and ECC arithmetic's advantages to improve the security and efficiency of the system. The paper also presents a RBAC scheme especially applied in GIS, its authorization is convenient and flexible, and meanwhile it satisfies requirements of cooperative work in spatial

application. Data are protected with AES symmetrical encryption to guarantee data confidentiality and integrality during transmission.

[17] presents integration and security of spatial information. A framework, a Spatial Decision Support System (SDSS), is built to demonstrate how spatial analysis resources can be interfaced within decision making environments, which includes authorization issues related to integrated data. Architectural and security aspects are considered based on Web-based technology and on services as integration scenario. A model of spatial decision support system is proposed to integrate local and Web-based information within GIS services available in the internet. And an architecture is established for the SDSS illustrating how this technology can be effectively deployed beginning with contexts and functionality which are available on the Web. This paper comprehensively explains the integration and security of spatial information, which supports decision making and context analysis.

[14] debates the smart infrastructure development framework and the surveying positional accuracy of locating the assets as a base of the smart city development architecture integrated with all the facilities and systems related to the smart city framework. The paper discusses also the main advantages of the proposed architecture including the quantifiable and non-quantifiable benefits. A smart city is generally meant as a city capable of joining “competitiveness” and “sustainability”, by integrating different dimensions of development and addressing infrastructural investments able to support economic growth as well as the quality of life of communities, a more careful management of natural resources, a greater transparency and participation to decision-making processes. The smart city infrastructure is the introductory step for establishing the overall smart city framework and architecture. The paper demonstrates how GIS can be used for decision-making and the smart city development.

[15] talks about that many Information Technology (IT) tools play a vital role in the business world due to their wider applicability. Extremely competitive retail environment necessitates retailers to choose new store locations strategically. GIS with its capability to manage, display and analyze business information spatially, is emerging as one of the powerful location intelligence IT tool. The purpose of this paper is to explore the possibility of strategic retail outlet location through online Decision Support System (DSS) in Hyderabad Metropolitan city, India. The procedure makes use of data, information and software from Web-based Geographical Information Systems (GIS) to generate online analysis, mapping and visualization systems. These procedures are integrated and synchronized with appropriate data layers (multi data layer system) to arrive at better decisions. This DSS combines different data layers through spatial methodological analysis to arrive at possible solution for ideal retail store location.

[16] discusses how to use geographic information systems for locating potential

customers of a small business. Entrepreneurs are advised to define a target market for their companies, they must know what unmet needs their company is designed to meet, and how to meet the needs of potential customers in the target market. Because of resource limitations, finding the location of customers in the target market can be very difficult. However, the convergence of several trends has made GIS accessible to small businesses. GIS has the potential to help entrepreneurs pinpoint the location of customers in a target market. The paper applies GIS to a start-up company's sales data to test whether GIS delivers on its promise. They propose that GIS is able to accurately identify the location of customers in the target market, and is able to predict there past sales have already occurred.

[18] discusses the traces of moving objects in a city, which depict lots of semantics concerning human mobility and city dynamics, are becoming increasingly important. In this article, they first give a brief introduction to trace data; then they present six research issues in trace analysis and mining, and survey the state-of-the-art methods; finally, five promising application domains in smart cities are discussed.

[19] shows that the recent changes in service environments have changed the preconditions of their production and consumption. These changes include unbundling services from production processes, growth of the information-rich economy and society, the search for creativity in service production and consumption and continuing growth of digital technologies. These contextual changes affect city governments because they provide a range of infrastructure and welfare services to citizens. Concepts such as 'smart city', 'intelligent city' and 'knowledge city' build new horizons for cities in undertaking their challenging service functions in an increasingly cost-conscious, competitive and environmentally oriented setting. What is essential in practically all of them is that they paint a picture of cities with smooth information processes, facilitation of creativity and innovativeness, and smart and sustainable solutions promoted through service platforms. This article discusses this topic, starting from the nature of services and the new service economy as the context of smart local public ser-vices. On this basis, an overall framework is built for understanding the basic forms and dimensions of smart public services. The focus is on conceptual systematization of the key dimensions of smart services and the conceptual modelling of smart service platforms through which digital technology is increasingly embedded in social creativity.

[20] presents many people living in villages are now migrating to the cities due to tremendous increase in population. It is predicted that very soon most of the human civilization will be concentrated in the cities. This increased population will consume more energy and need more space to live. Finally, they will leave behind a more prominent environmental footprint as the cities grow to metropolises. This has been occurring globally and has led to serious consequences. So, to restrain the burden on traditional cities, a paradigm of a new kind of cities has

come up, one called smart city. A smart city uses advanced technology to minimize the effect of human activities on the environment. With the increase in population, more and more people also learn and are taught to use computers/handhelds. This has resulted in having a large number of computers/handhelds in every city. In this paper they propose to develop smart software which is used to from a smart system to use optimal power and hardware resources to produce minimum carbon footprint and to make the city smart and green.

[21] demonstrates that the concept of Smart City is considered increasingly strategic for the solution to the questions related to the irreversible urban agglomeration growth. Created in the nineties in parallel to the liberalization process of telecommunications and the development of internet services, this expression risks remaining too generic and without a shared operational definition. This paper contribute to the existing literature in two ways: i) providing an overall survey of the definition and measurement problems; ii) deriving some methodological suggestions from the analysis, in order to proceed towards a robust and comparable Smart City measurement system. The latter results extremely relevant in the perspective of a dedicated monitoring system implementation.

[22] illustrates that information is one of the most important business success factors nowadays, as it provides an opportunity to respond to emerging changes and to take effective decisions. This information has to be precise and easily accessible. The aim of this research is to create a methodology for automatic real world adequate geo-simulation model preparation, based on Geographical Information Systems (GIS) models and statistical data collected. All structures of an urban environment interact, and the urban environment is a network that exists among different structures, links, flows and relationships. The spatial distribution and development direction of the territory, also business environment development is determined by a street network and transport communication network. Besides, city development plans require the newest information about transport traffic and pedestrian flows as well as information on the accessibility of local services, open territories, etc. This information is well formed in GIS models. Most of model objects also contain capacity information. As the GIS models are static, they cannot be used to determine any dynamics of the territory; however, the urban environment is nonlinear. A possible way to solve nonlinearity is to prepare geo-simulation models, as they are more informative for dynamic processes than GIS models. Geo-simulation models also allow making experiments and solving optimization tasks. The automatic creation of geo-simulation models does not require deep knowledge of simulation techniques for domain specialists further using them. From the economic aspect, it is characterized by lower expenses, quicker access to data and larger flexibility.

[23] discusses a model for, user oriented selection of bus rapid transit (BRT) corridor for Jaipur city in GIS environment. The objective of the model is to select the BRT corridor based on spatial distribution of transit trips in the city for horizon year. The model uses the demographic, transit trip and land use characteristics of the city to identify the high ridership oriented BRT corridor. The methodology comprises of two models, first model deals with BRT transit demand forecasting and second model is responsible for selection of the BRT corridor based on some pre-defined conditions. The model generates graphical GIS based maps as output for the better understanding of the transit demand pattern and policy making, for the urban planners. The methodology can be utilized for any similar size cities in Indian context for mass transit planning effectively.

[24] shows making a city "smart" is emerging as a strategy to mitigate the problems generated by the urban population growth and rapid urbanization. Yet little academic research has sparingly discussed the phenomenon. To close the gap in the literature about smart cities and in response to the increasing use of the concept, this paper proposes a framework to understand the concept of smart cities. Based on the exploration of a wide and extensive array of literature from various disciplinary areas. we identify eight critical factors of smart city initiatives: management and organization, technology, governance, policy context, people and communities, economy, built infrastructure, and natural environment. These factors form the basis of an integrative framework that can be used to examine how local governments are envisioning smart city initiatives. The framework suggests directions and agendas for smart city research and outlines practical implications for government professionals.

3. GIS Repository Management Based on Contexts

In order to define security of GIS, we put forward a model of the Objects contained in GIS repositories. First we give a simple explanation of the concepts, than we come to a model that is then enriched with authorization issues.

3.1 General Overview

Research on how to manage GIS repository has been suggested Section 2. Considering context analysis and decision making, we can cluster data of GIS objects in terms of attributes involved in the same domain of interest, which we call a context. Examples are the *economic* context, the *quality of life* context and the *environmental* contexts. Among different contexts, the attributes of SObj-s can be repeated (namely, attributes can belong to different contexts). We study and analyze how SObj-s are managed in order to assign security privileges to users accessing these objects. Management includes entering data, manipulating data, analyzing data, reviewing data, verifying data, making corrections and visualizing data.

Using the concept of *meta data* (data about data, which can help to cluster data in an effective way in which similar attribute data are collected together), we define a SObj repository as a set of SObj-s with attributes clustered according to predefined contexts. When users want to retrieve SObj-s, they will have to specify which context they want to analyze and hence the GIS repository will be partitioned into retrievable objects starting from the security requirements established for the various users, objects and contexts. Based on contexts, we define a GIS database snow flaking model as depicted in Figure 1.

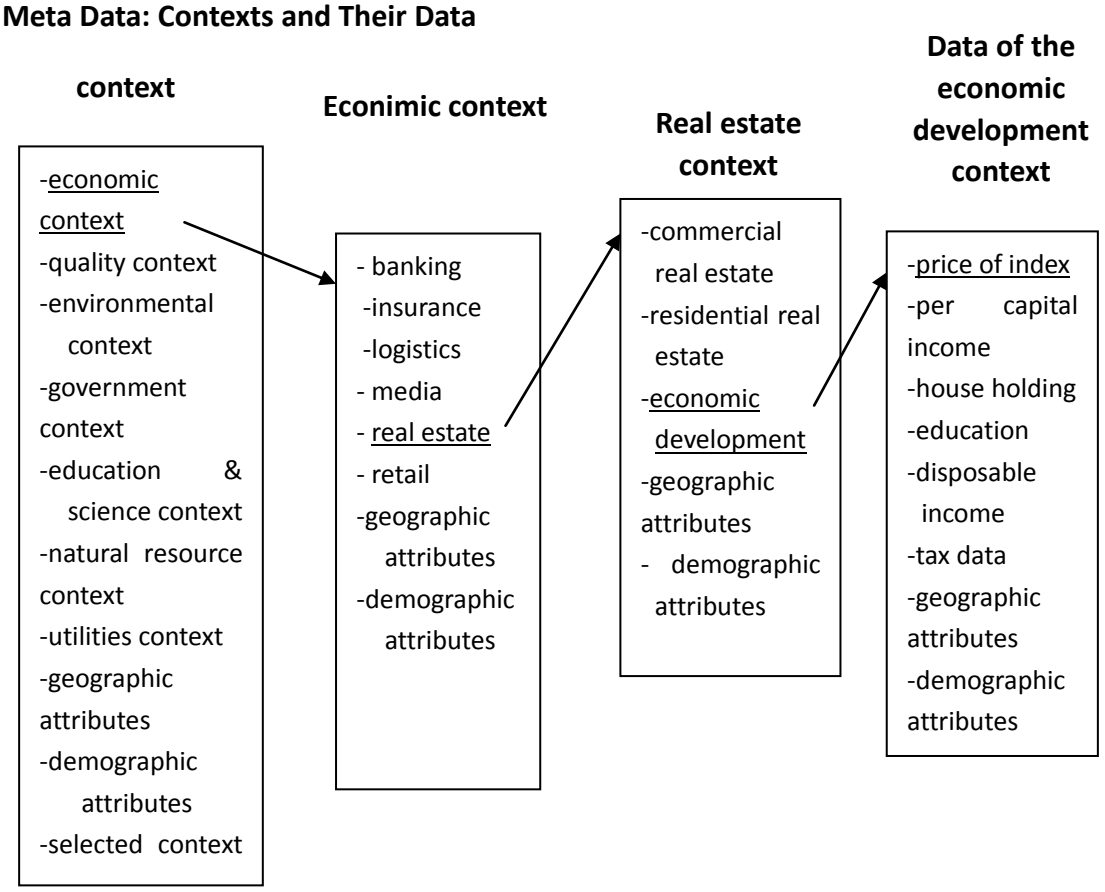

Figure 1: GIS database snow flaking modeling example

Figure 1 shows the GIS meta data used for clustering different SOb*j*-s in terms of their pertinence to context. Here we have the economic, quality, environmental, government, education and science, natural resources and utilities contexts. Geographic and demographic attributes are always present in all contexts. Contexts can be selected and navigated. For instance, by selecting the Economic Context (underlined in Figure 1) we can move to its details, which are also Contexts. Here we have the banking, insurance, logistics, media, real estate and retail contexts, and the default always present geographic and demographic attributes. Then, the navigation from the economic context can move to inspect the real estate context. The geographic and demographic attributes in the specific context will be showed because they are used widely and basically. Finally, the economic development context is reached; here its attributes are inspected (no more detailed contexts are

shown here beneath economic development) in order to get data, indexes, indicators by filtering information.

3.2 GIS spatial objects model

We consider a spatial object SObj as defined in [5] namely, a "recognizable object" "located in a specific place marked as a unique longitude and latitude zone in the world". A spatial object SOb*j* with *j* = 1..N being N the total number of objects in the GIS, is for instance a map, an image of an area, a park map, a canal/river hydrological system, a city, or a building cadastral map.

An SOb*j* is stored in the GIS with its set of *attributes* {aj_i}, *i* = 1..M being M the total number of attributes of SOb*j* and at a given level *l* of the GIS, where *l* = 1..L being L the total number of detail levels defined in the GIS. Hence, L is a predefined property of the GIS.

The GIS is layered according to various levels corresponding to cartographic layers. Objects exist at a given layer *l* of the GIS, and are mapped into many objects (a 1-to-1 or 1-to-many relationship) at *l*+1 level. For example, an object "Lombardy Region" at level 1 of the GIS is mapped into 11 "Lombard Province" objects at level 2. Then, recursively each "Lombard Province" object (e.g. Milan Province) is mapped into 1 province capital of the Province (e.g. Milan City) and into the *s* main cities of the province (e.g. Magenta, Pioltello, Sesto, etc. of Milan Province).

At each layer, an object has a set of clustered attributes. Clustering occurs by contexts, namely domains of interest. Attributes are for instance the dimension, the location, the owner, and other geo specific attributes (latitude, coordinates, etc.) that characterize the object as a *geo referenced* one. Other attributes of SOb*j* define the features of the object from different viewpoints, namely from the viewpoint of *Contexts*.

Also attributes are mapped from one layer *l* into the *l*+I layer according to the levels existing for the pertaining object. Mapping of attributes along GIS levels is also 1-to-1 or 1-to-many. For example, the attribute *Number-of-Inhabitants* of Lombardy Region will become *Number-of-Inhabitants* of provinces and next of cities (1-to-1 mapping at the schema level). The instances of the attribute values along the mapping Region→ Provinces will be 11 (equal to the number of Lombard Provinces) and a rule will establish that the Sum of the *Number-of-Inhabitants* instance values will be equal to the *Number-of-Inhabitants* of the Region.

Contexts

Contexts are a mechanism to perform detailed, focused analysis and to improve manipulation capabilities to take decisions about GIS objects, e.g. about

management of an area. Hence, we assume we have a context-based repository of the GIS.

A *context* is defined as a cluster of attributes {aj_i}*k* where *k* denotes the *k-th* context, with k= 1..P being P the total number of contexts defined in the GIS. A context groups attributes which are relevant under a certain perspective of analysis, namely for a certain domain of discourse. A default context always existing for objects of the GIS is named *GeoContext* and groups geo reference attributes. One attribute aj_i can belong to more than one contexts. Sample contexts for an object like a map are economic, environment quality, green areas, traffic, taxes, mobility and health contexts.
Contexts can be navigated along by the user. More precisely, a context can be selected and then expanded to check its details, i.e. what objects are in the context and what sub-contexts are defined for that contexts. This means that contexts can be nested and can be inspected by using a recursive function. Navigationally, this appears as a hyperlinking of contexts until the needed context is reached and its data can then be inspected, as in Figure 1 occurs for Economic Development.

By clustering attributes in contexts, we can solve requests queries like Q1: "How large is the green coverage in this area?" or Q2: "How many people having one or more children live in a certain area?". By storing attributes grouped in contexts, an analysis can be performed by selecting an objects SOb*j* and one context *k* (e.g., "Green" context for Q1, and "Urban Quality Life" context for Q2).

Thanks to the containment properties of contexts, contexts can be analyzed at various zoom, or detail, levels. This means that spatial properties of an SOb*j* can be inspected at various zoom details by considering first the region map (a large area), then the map of provinces in the region, further, the maps of the cities in the various provinces and so on. Objects and their attributes clustered in contexts and stored at the different layers of the GIS can be retrieved at different granularity with respect to users' role and permission. For instance, the "Urban Quality Life" context can be inspected attributes at various levels of granularity: from macro attributes (e.g. number of green areas in a city) to more specific attributes (number of children-friendly sport places in a district).

Summarizing, we have the following definition:

SOb*j*={{geo-attributes}, {attributes}, {(context,level)}, level}

Where { geo-attributes} includes geo references, owners, {attributes} is the set of all attributes of SOb*j* , {(context, level)} is the list of pairs : context and its available levels of detail for which SOb*j* is of interest; Level is the number granularity levels existing for SOb*j* in the repository.

A relation {{aj_i}*k}* is then defined to represent the aj_i attributes of SOb*j* as clustered in

the *k*-th context (with *k* belonging to the list of contexts for SOb*j*}. Such relation is many to many.

Examples.

1. A Region Map can be defined as SOb*j* with Geo reference coordinates, attributes, contexts, and level as shown below.

Region Map={Geo reference coordinates, owner, extension}, {net income, population density, schools, rivers, monuments, average income, transportation means}, {(Economic, 3), (Environment Quality, Education}, 4}.

Here contexts for the region map are the Economic, Environment Quality, and Education. Level = 4 means that the Region Map can be displayed in the GIS at 4 levels of detail: province, city, district, area. The Economic context appears with 3 levels of detail as from Figure 1, where 3 levels are navigated to reach the data of the context.

A relation {{aj_i}*k}* is as follows: {aj$_i$} is a set of attributes, *k* denotes number of contexts. For each context *k*-th, there are one or many set of attributes for it and also this set of attributes can belong to different contexts. The relation is many to many.

2. A University can be an object in the GIS, which is located in a specific area in one city, has 3 contexts of analysis, has three levels of detail. This is formalized as follows.

University={Geo reference coordinates, extension}, {buildings, students, taxation level, facilities, number of faculties}, { (Education,2), (Research,2), (Spin-off, 3)}, 3}

If for instance we assume a prospective student (a user) wanting to analyze one university's the *research* context, he need to define the {{aj_i}*k}* link *to identify* the university's attributes belonging to this context. By entering the context name, e.g. Research, he is returned the attributes belonging to this context. Then, he can move vertically along the 2 levels of Research and access the "General Scientific Research" (first level), then a more detailed context "Scientific Research in Departments" (second level), where the indicators about the research performance in departments are available (impact factors of publications, number of awards, and so on). Based on this information, he can analyze and make decisions such as application to PhD, grants, scientific research areas of departments and so on.
Different users, like prospective students, current students, professors, managers and president, can access different information in terms of their roles distributed permissions. Based on retrieved information, users can analyze specific objects and make more reliable and effective decisions.

3.3 GIS repository architecture in SDSS

When managing repository, integration and security of spatial SObjs information should be considered. We explore how spatial analysis resources can be interfaced within decision making environments in a single framework, namely a Spatial Decision Support System (SDSS), which includes also authorization issues related to integrated data [11].

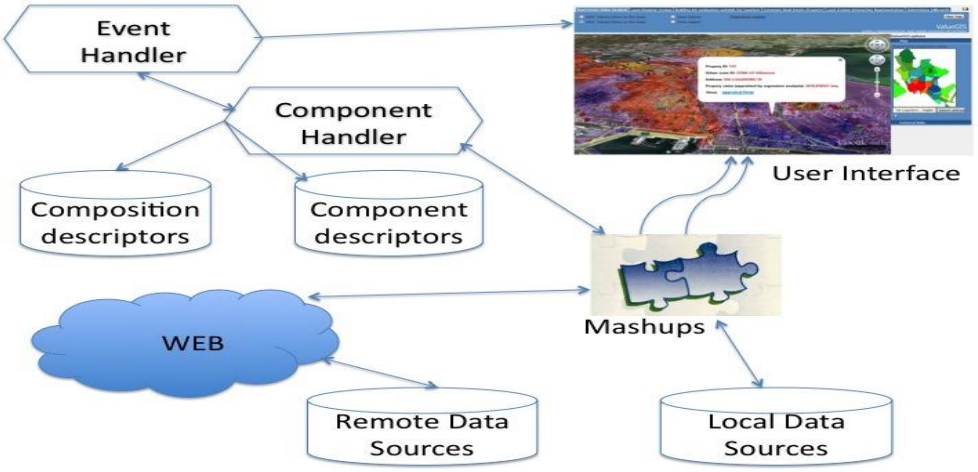

Figure 2: Functional architecture of the SDSS

As we can see from Figure 2, we rely on mashups as feasible solutions for interconnection, integration of different information sources that support the user during his decision-making processes. Specifically, a mashup is a process that integrates data/content from different resources on the Internet in order to provide the user with a flexible and easy-of-use way for service composition on the Web. Fig. 2 shows the proposed functional architecture of the SDSS. This is centered on the mashup framework [12]: events generated from the user interaction with one mashup component (i.e., the selection of the decisional context) are mapped onto operations of one or more components subscribed to such event (i.e., the spatial visualization of data).

Components operate independently or within a networked environment. This gives the opportunity of creating direct dynamic links between components and other applications, and allows distinguishing between the architectural aspects and the updating functionality on data available to the user. In more detail, the *User Interface* supports user interactions. Users can access the computational environment to carry out both simple and advanced spatial analysis on data and to browse maps. A Web Interface implements access. The visual composition has been specifically conceived to hide the complexity of technical details actually managing the execution of the mashup.

Components and composition descriptors are stored in dedicated repositories. Specifically, the component description repository stores the component descriptions plus wrappers through which the SDSS invokes service operations. The composition description repository stores the XML-based descriptions that provide a reference model for coordinating the mashup composition and execution.

The component handler manages the event composition and maintains the description of mashup instance status. As soon as the mashup is completed, it is executed and rendered through the user interface.

This allows the decision-maker to actively select and compose different decision contexts. The related spatial representation (i.e., a geo-referenced map, a thematic map, or a graphic) is immediately rendered so that the user can easily check whether the decision context choice satisfies his needs. In case of unsatisfactory results, he can modify the decisional context by adding further data, or by requiring a different integration modality.

4. GIS Security Model

In order to tackle GIS security issues, we introduce a security model based on RBAC. When users want to access GIS information, they must be distributed with roles and permissions with which users can access corresponding SOb*j-s*. Users are given permissions through their roles in which users are not directly connected with permissions but through roles.

We assume, as an example, we have mobile users endowed with a smart phone. Users move along spatial objects by physically entering spatial areas. Their movements are identified through the GPS so that a map corresponding to the area they are traversing is rendered by the GIS progressively as the user moves.

In this thesis, the security model extends the RBAC model proposed in [2] by introducing an *extent*, which defines the purposes of roles in analyzing contexts. For example, if the user is the mobile user (U)has an active GPS connection while moving around a zone (e.g. Polimi-Leonardo campus) with a green manager role (R), the *extent of U-R* will change according to the areas he enters or levels he moves. For example, U-R will receive the 'Building 20' extent when he enters the area of Building 20; when he leaves Building 20, he will lose this extent. In this thesis, we model users in roles with extents.

4.1 GIS Class Diagram

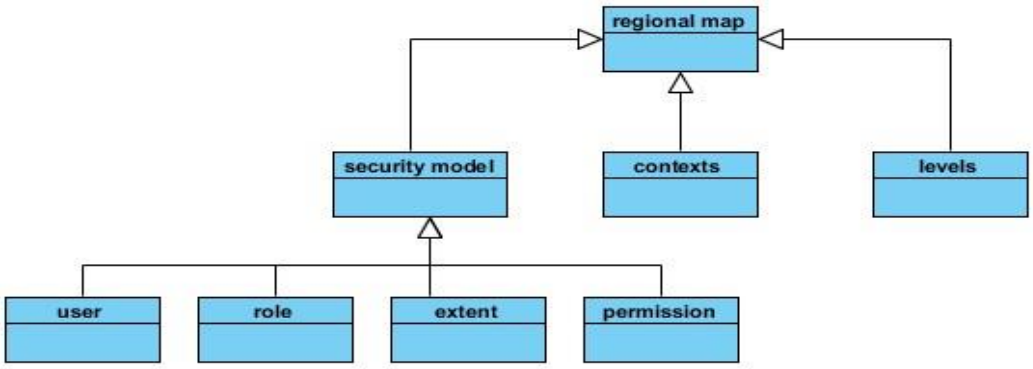

Figure 3: GIS class diagram for regional map object

Figure 3 shows the class diagram of the structure of a GIS “regional map" Object. As far as its security is concerned, it includes the security model, the contexts and the level. And for the security model, it considers user, role, extent and permission. The regional map is a spatial object located with attributes, and containing various attributes clustered in contexts. These attributes are stored in the GIS repository, which needs to be secured based on the security model established for confidentiality. In order to get more detailed information, users can access the object at different levels of detail: level denotes the level at which the object is stored. Users receive access privileges on the Object basing on their roles and permissions by filtering and selecting within authorized spatial objects with contexts to access more specially-selected context, by analyzing attributes aligned with this object, users can make an analysis and decisions. And extent indicates relevant activities a role can activate with the corresponding permission.

4.2 Users Roles-Permissions Relation Based on RBAC

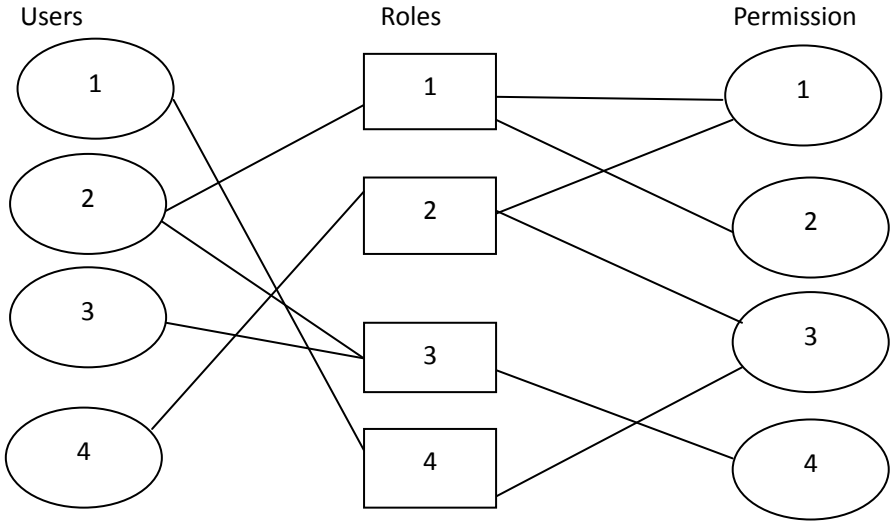

Figure 4: Users-Roles-Permission relation (taken from [2])

In Figure 4, we can see that roles are set of access permissions. Users are given different roles holding relevant access rights. A user can have many roles and a role can be authorized to different users. A role can include many permissions and one permission can be included by many roles. Users gain permission by being distributed roles and does not connect with permission directly. To illustrate this point, let's assume that a green manager in one area wants to make an analysis about the green coverage in this area and to take a decision about how much should be invested by increasing green coverage of 15%. The green manager will be assigned roles and permission to search information and to make a context (green coverage) analysis. With roles, he can have permissions to view, zoom in, zoom out, select and filter information. Based on his role and permission, he gains GIS SOb*j-s* information with which he can make analysis and decisions. This definition of roles is compliant with what proposed in [2].

4.3 GIS Security Model

In order to improve GIS security and protect the confidentiality and sensitivity of SOb*j-s* information, users should be authorized for roles and permission to control access. According to the role-based access control, users are given permissions in terms of their roles and then GIS services (operation of GIS Sob*j-s*, such as view/read, zoom in/out, write, modify, delete) are rendered. Roles and permission are stored in a role and permission database, they are extracted from this database and are assigned to users by role and permission issuers when GIS SOb*j-s* are accessed by users.

Table 1

Role	Extent	Permission
Public user	Information search	View
Green manager	Context analysis	Zoom in/out
		View
Object owner	Data management	Modify/update
		Write
		Zoom in/out
		View
Governor	Decision making	Modify/update
		Write
		Zoom in/out
		View
System manager	System maintenance	Create/delete
		Modify/update
		Write
		Zoom in/out
		View

Table 1: GIS security model

In
Table 1, the GIS security model is established to secure SOb*j-s* based on RBAC. Roles are combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles (in
Table 1, roles increase from the first to the last row).

Roles are predetermined with permissions and distributed when accessed by different users. Roles are unique within one session of interaction with the system.
Public users can just view SOb*j-s* information. For green managers, they are distributed two roles: information search and context analysis. We assume that they need a specific password for each role. When they want to retrieve SOb*j-s* for context analysis, by entering a password, not only can they view information, but also they can zoom in or zoom out to attain more information and make analysis according the retrieved information. In the same way, when a user is recognized as system manager, he can enter the system under three roles, each with the corresponding permissions. Different passwords allow him to connect to the system under one role. For example, a system manager can just view information with information search role. But if he wants to maintain the GIS system, he needs to employ the system maintenance role and utilize permissions such as delete, modify/update, write, zoom in or out, view/read.

Green Manager has two possible roles: Information Search and Context Analysis. A given role implies the same set of permissions. E.g., Context Analysis gives the Zoom in/out and view/read permissions. The System manager user the System maintenance roles that give him a large set of permissions for system maintenance: view, zoom in/out, write, modification and create/delete SOb*j-s*. The Object owner user has no permission to create/delete objects. Users can get the same permission considering their roles, such as Object owner and Governor: in
Table 1 they have the same permission even with different purposes. For example, Object owner and Governor are both given permissions to view, zoom in/out for Sob*j-s* for their own context analysis purposes.

Figure 5 shows GIS security model in a hierarchical way, from the figure, we can understand the hierarchy in different roles with different permissions. The public users have the lowest permission, which means that they can only access and view the specific information assigned to them, and as for green managers, they have all permissions assigned to the public as well as the permission of zoom in/out which the public users are not allowed to access. In the same reasoning with this hierarchy, the system managers with the role of system maintenance have the highest permissions to view, zoom in/out, write, modify/update and create/delete data in the system. With this hierarchy, security of GIS information is assured because access to information is strictly controlled by distributing corresponding roles and permissions. This hierarchical security model is shown as follows:

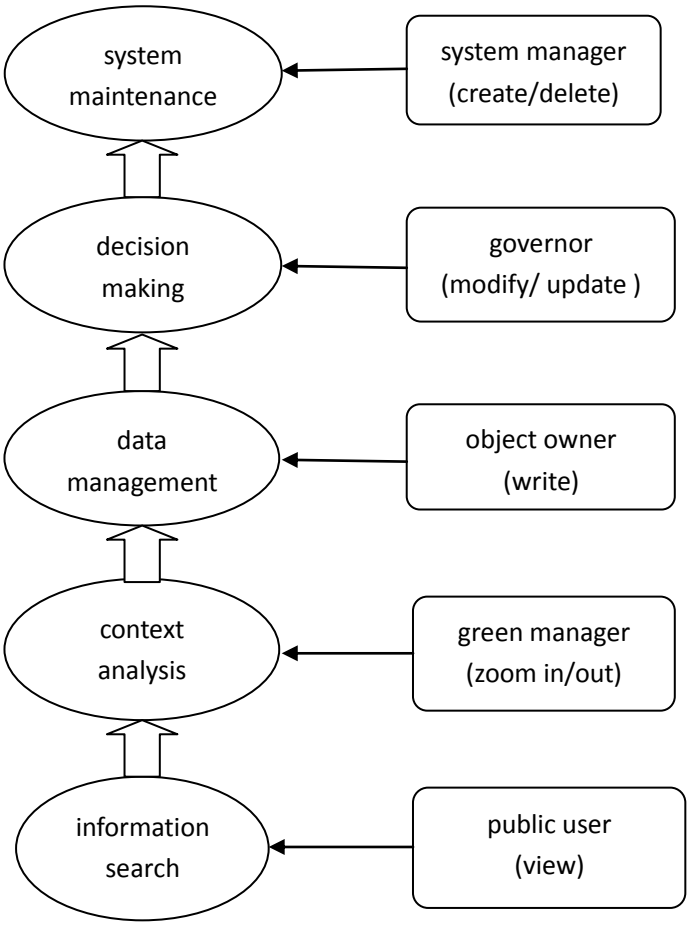

Figure 5: GIS security model with hierarchy of roles

5. Security Architecture of Data in the SDSS

Data sharing brings about security issues. Decisions makers and stakeholders need to share decisional data provided both internally by their organizations and provided by services of other administrations, and sometimes, it is necessary to outsource data collection contributed by different data providers, which can trigger security issues.

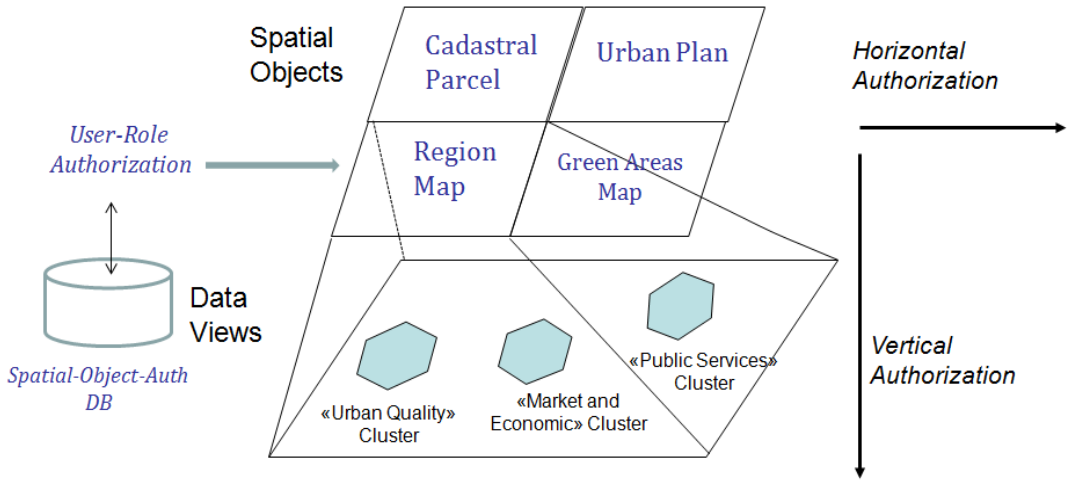

Figure 6: Security architecture of data in the SDSS.

In Figure 6, security architecture of data authorization model presented here aims at dynamic data protection based on the decisional context of the user accessing the data. Granting access to information that can be disclosed or modified depending on the various steps of a decisional process requires the specification for decision makers of data views over the different data sources. The model considers that the SDSS Data space is a geo-coded database containing both *geo-referenced objects* (i.e. complex types that are composed of multiple pieces of information and of attributes) and *spatial objects*, such as geographic maps.

According to this data organization, we have two orthogonal authorizations: horizontal and vertical authorizations as depicted in Figure 6. Horizontal authorizations are associated to User-Roles and their permissions to access spatial objects (i.e., geographic maps) while vertical authorizations specify User-Role permissions to access data views on geo-referenced objects on the basis of protection needs.

Data views are defined by clustering object attributes in layers, which model the decisional context. The first layer contains spatial objects, such as region maps or cadastral parcels. The second layer refines spatial objects according to contexts, that is, vertical layers cluster data about different decisional facets, such as urban quality, market and economic indicators or public services (see Figure 6).

The Horizontal Authorization step consists in granting User-Roles access to selected spatial objects (e.g., a Region Map) and the visualization of the related geo-referenced objects (e.g., buildings and parks in the Region Map). Then, based on a set of User-Role related attributes, the Vertical Authorization grants access to data views on attributes of geo-referenced objects.

6. UML Analysis for GIS security

In order to show GIS applications, we carry out UML analysis, including use cases, UX model, analysis diagram and a sequence diagram. With this UML analysis, we can better understand and illustrate GIS security problems that could happen and then propose a model to solve those security issues in an overall and systematic way

6.1 Use Case

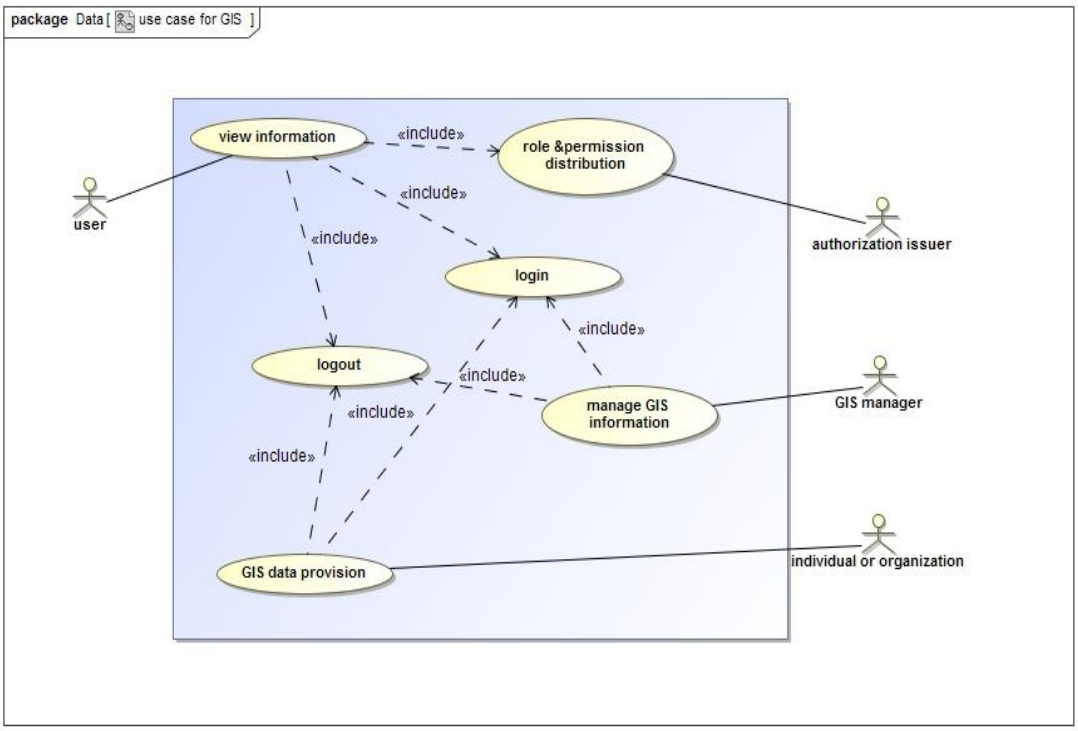

Figure 7: A use case for GIS

Figure 7 shows a use case for GIS security. There are four actors:
-users, who use information from GIS and use them to solve operational problems and improve processes;
-authorization issuers, who issue the role and permission to one special user and can be a third party in the system;
-GIS manager, who plans, maintains and controls the GIS information and database;
-individuals such as stakeholders and **organizations** such as the chamber of economy, who provide GIS information and can be a part of GIS managers.
In order to get the required GIS SOb*j-s*, users should login and be distributed specific role and specific permission to access a specific GIS object. Users, individuals or organizations, GIS managers can read, write, modify and delete information in terms of role and permission distributed by authorization issuers.

6.2 UX Model for GIS

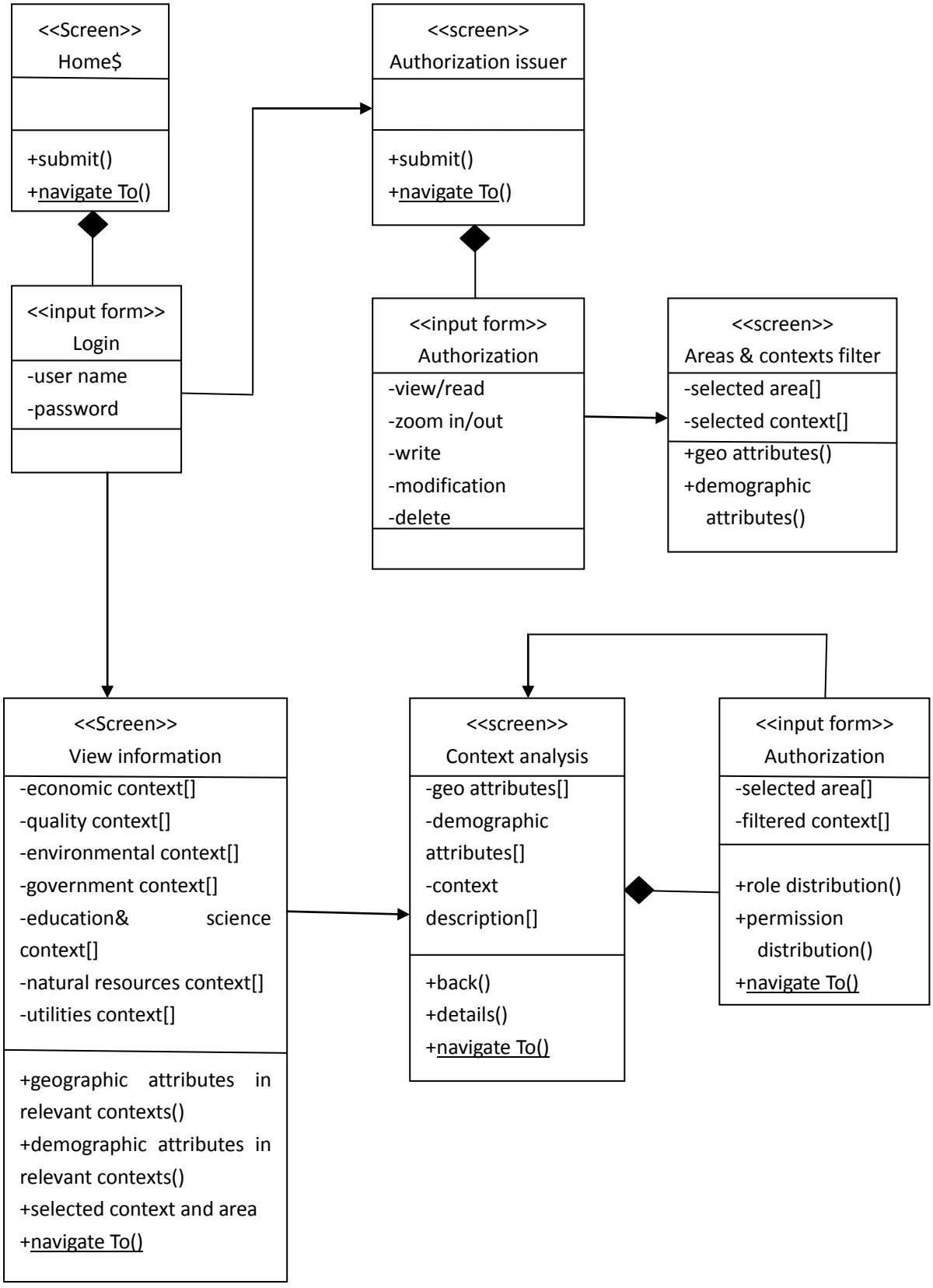

Figure 8: UX model for GIS

In figure 8, the UX model for GIS is shown. Users want to access SOb*j-s* and we cluster SOb*j-s* with respect to contexts, such as geographic and demographic attributes, economic, quality, environmental, government, education and science, natural resources and utilities contexts. A specific context is associated with a user-role authorization which results in the authorization to access data sources associated into clusters, which the users can select and configure depending on the analysis needs [2].

Specifically, economic contexts data include, per capital income, banking, retail, logistics, purchasing power and disposable expenses and so on. Quality contexts include quality property of pollution, public green zones and urban planned expected changes. Environment contexts include such information as water, ocean, land, wildlife and vegetation. Government contexts include national and local government, homeland security and military defense, fire, emergency medical services, disaster, law enforcement, health and transportation information. Education and science information context refers to research, libraries and museums, K-12 education and higher education etc.. Natural resources contexts let us access information such as agriculture, forestry, mining, petroleum and pipeline. Utilities contexts include data information on power management, electricity, gas, telecommunication and water and wastewater etc. users can access all this information according to their roles and permission.

Noticeably, for each context in selected areas, we all provide geographic and demographic GIS data which should be considered as basics of GIS.

6.3 Analysis Diagram for GIS

In Figure 9, the GIS analysis diagram for users shows how a user accesses the required GIS information. Generally, a user login and get permission, the role and permission distribution can be controlled by authorization issuers. After getting the role and permission, a user can access all available information. And then a user may use filtered function to gain more specific data for a specific object in a specific area.
In the same reasoning, we can draw the GIS analysis diagram for authorization issuers, individuals or organizations, and GIS managers respectively.

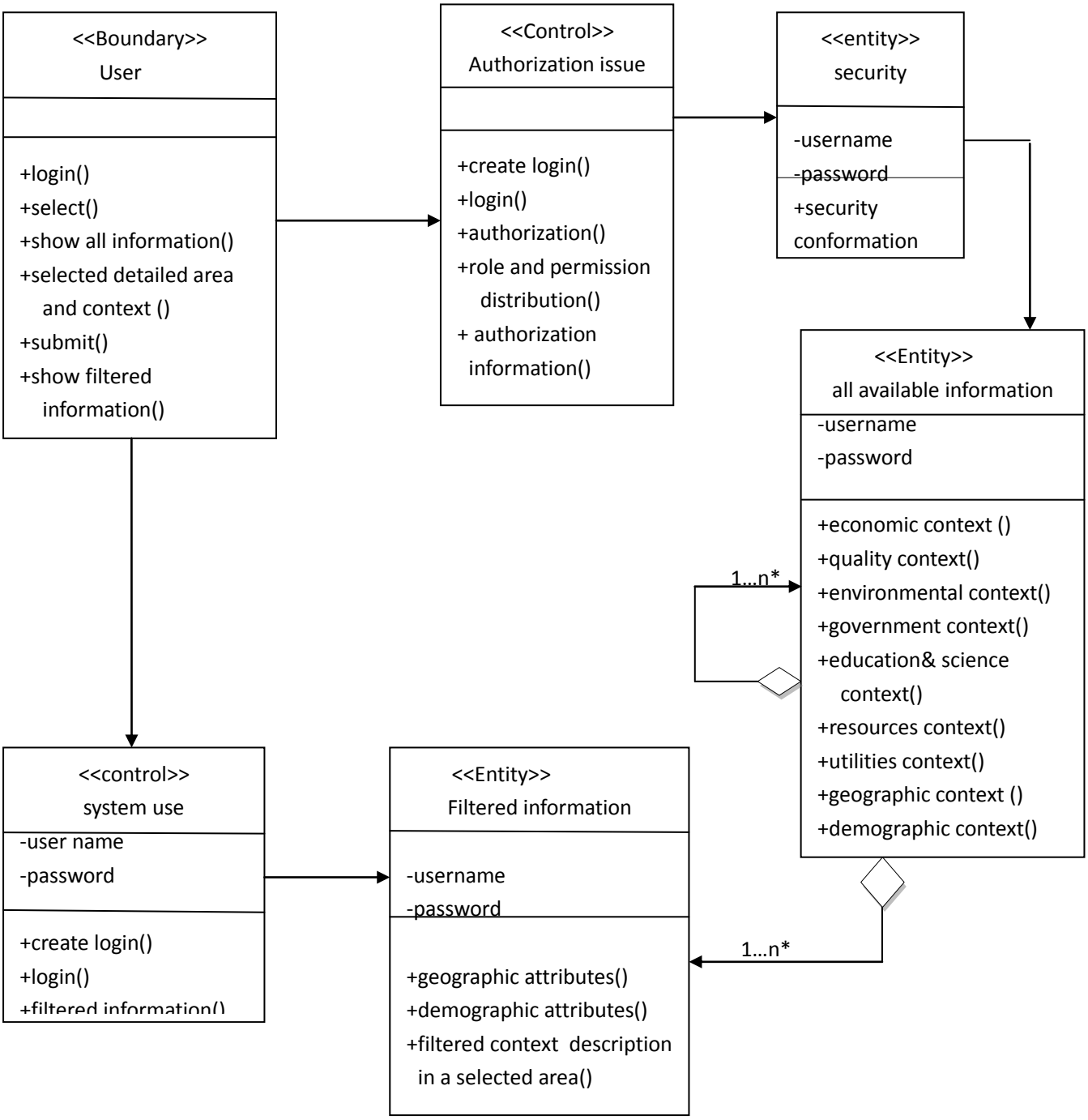

Figure 9: The GIS analysis diagram for users [Boundary-Control-Entity Model]

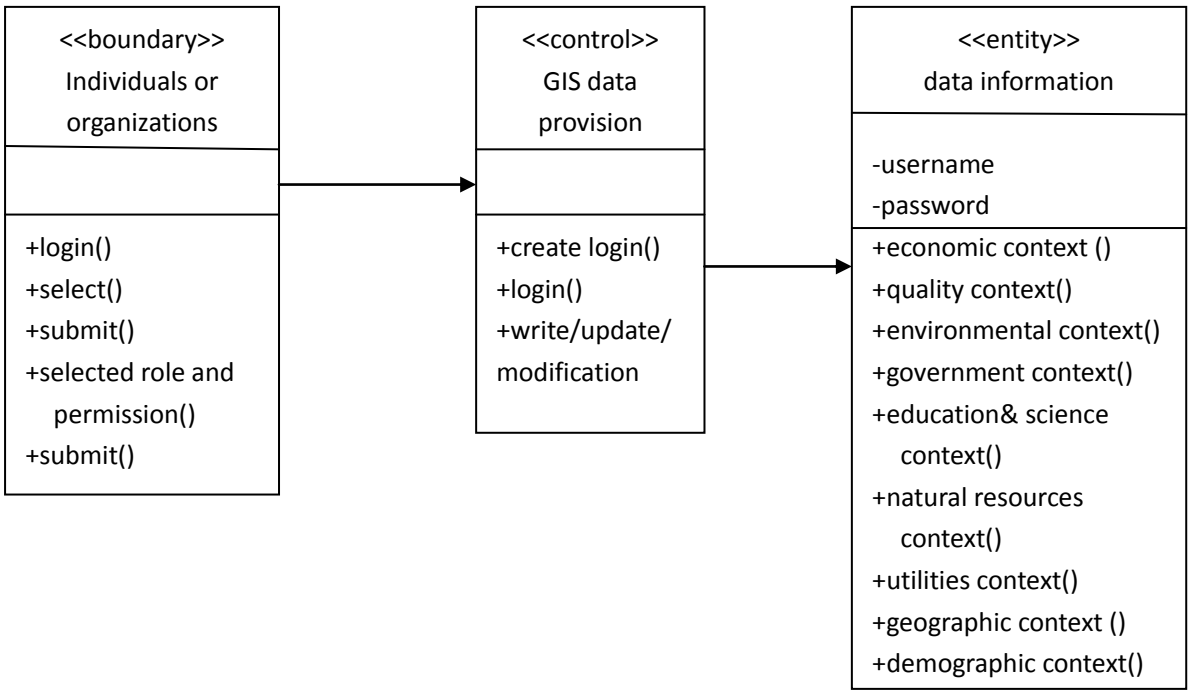

Figure 10: The GIS analysis diagram for data providers as individuals and organizations [Boundary-Control-Entity Model]

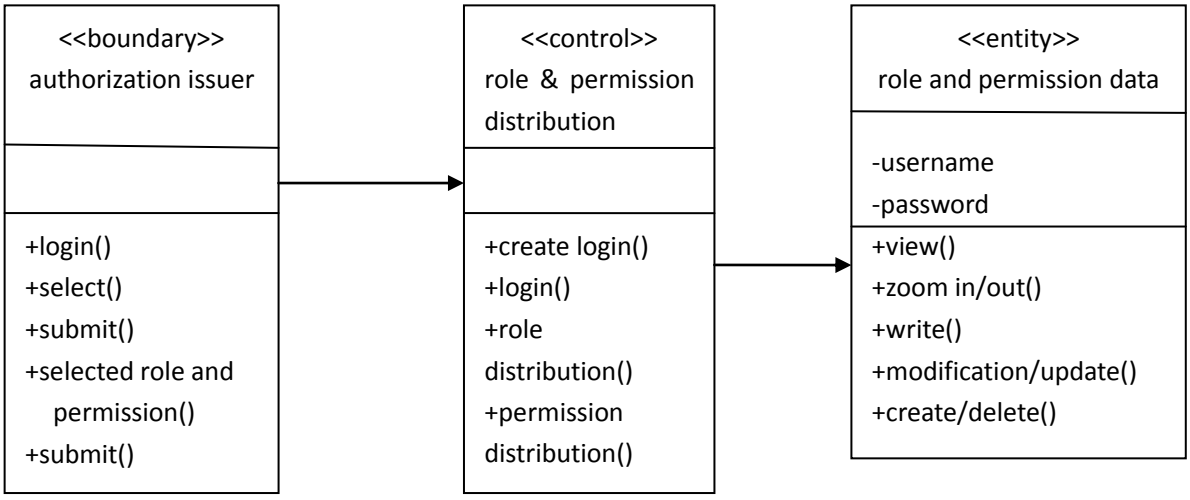

Figure 11: The GIS analysis diagram for authorization issuer [Boundary-Control-Entity Model]

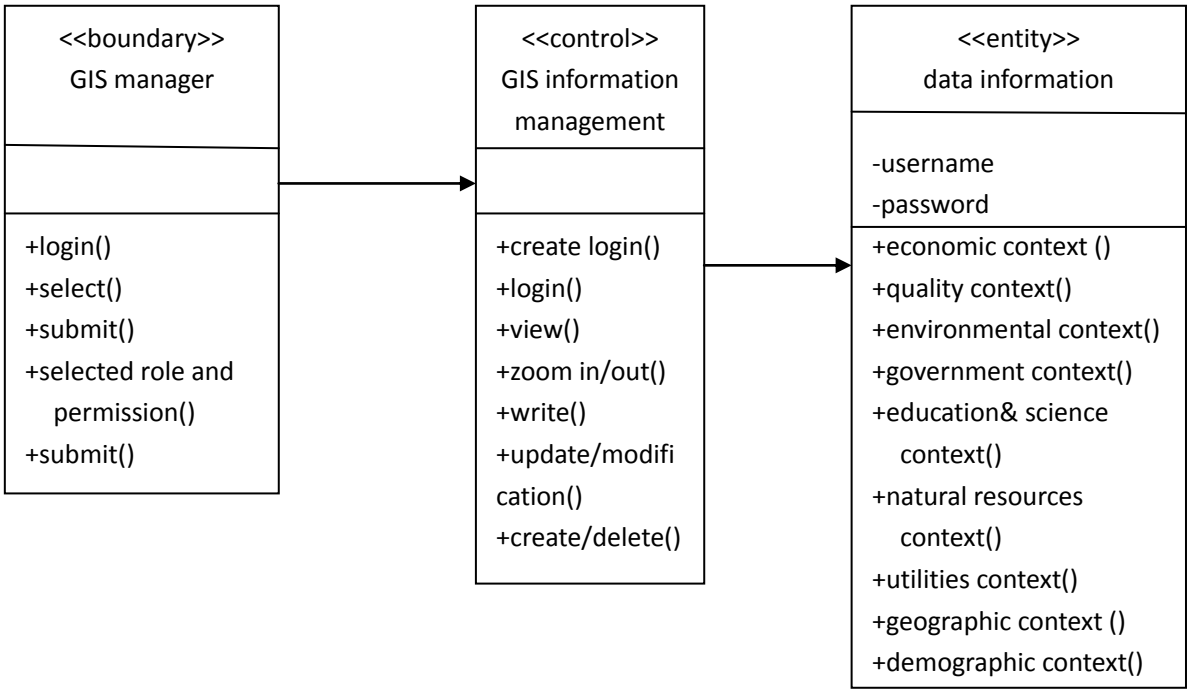

Figure 12: The GIS analysis diagram for GIS manager [Boundary-Control-Entity Model]

6. 4 Sequence Diagram of GIS

In this session, GIS sequence diagrams are drawn to show the information retrieving and storing in the GIS system, specifically for GIS users, GIS data providers(individuals or organizations), authorization issuers and GIS managers, which can embody the security issue in the GIS and possible security threat problems facing GIS.

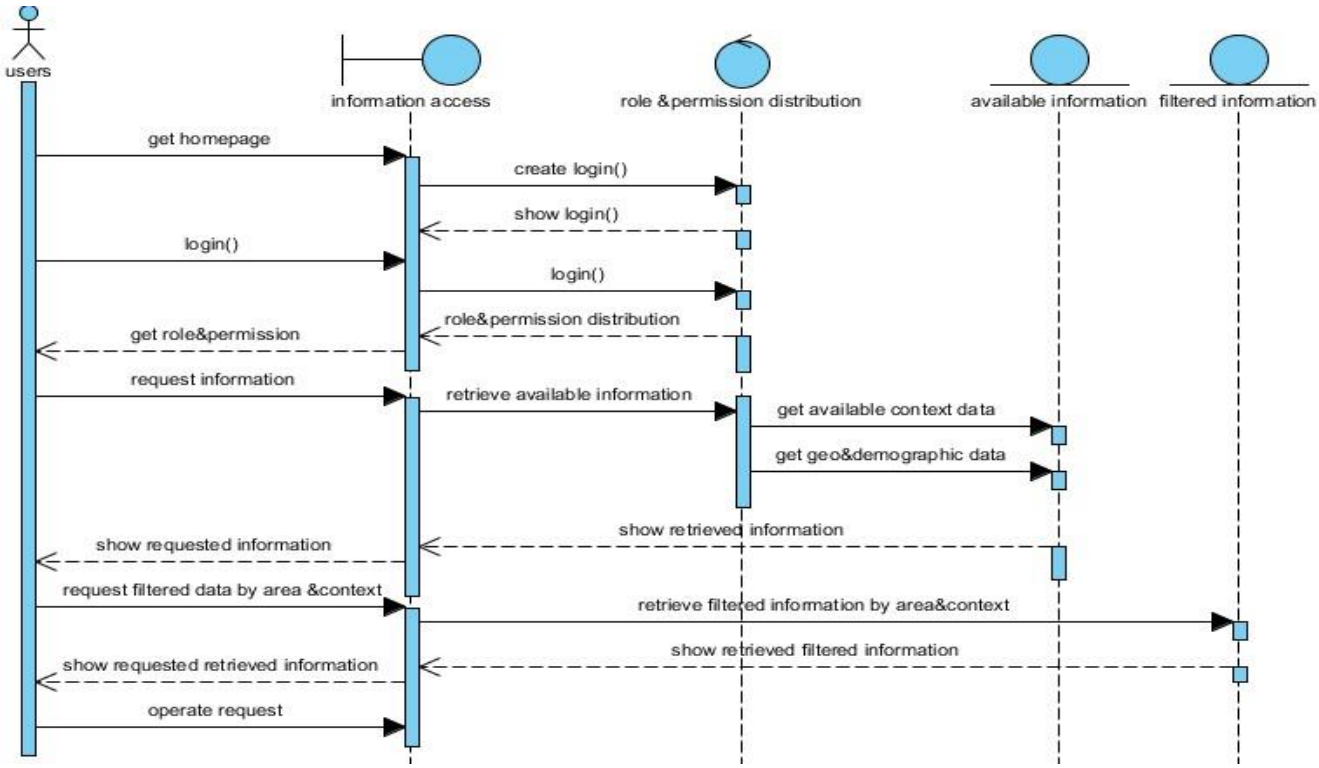

Figure 13: A sequence diagram for GIS users

As the above-shown sequence diagram (figure 13), a user can access the required information by following procedures described as the graph display. All these activities should be done in time sequence, such as login, getting role and permission, gaining all available information, select more detailed context, get relevant context analysis description.

It should be mentioned that a priority should be given if there is a contradictory occurrence between role and permission.

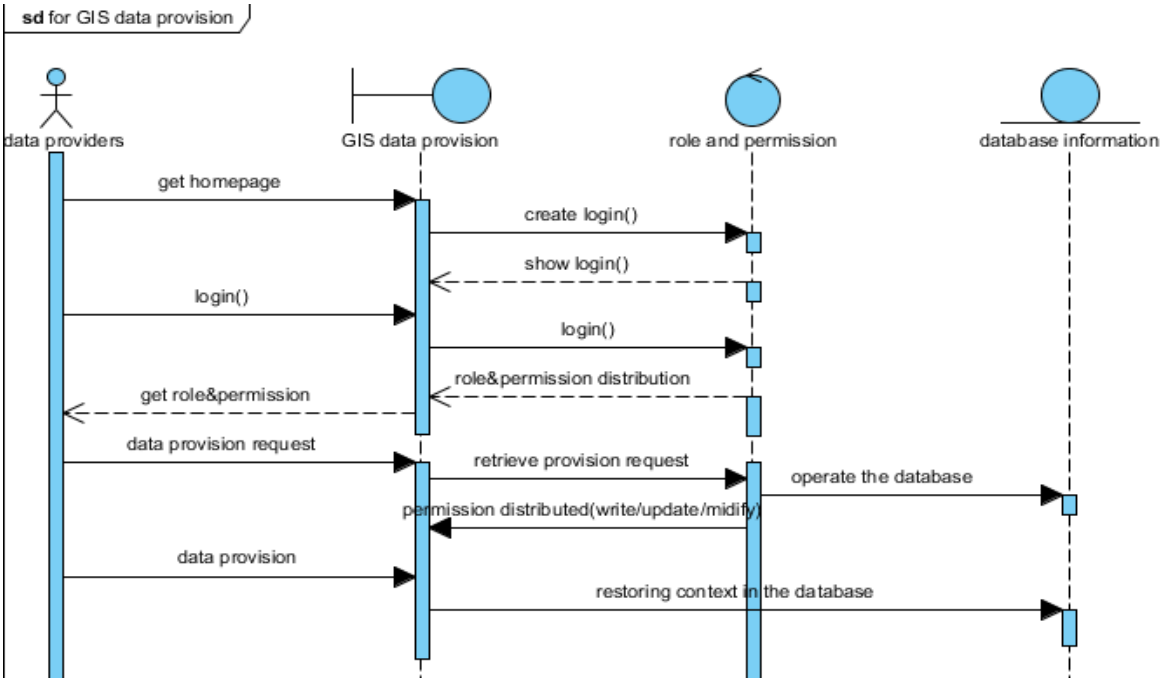

Figure 14: A sequence diagram for GIS data providers

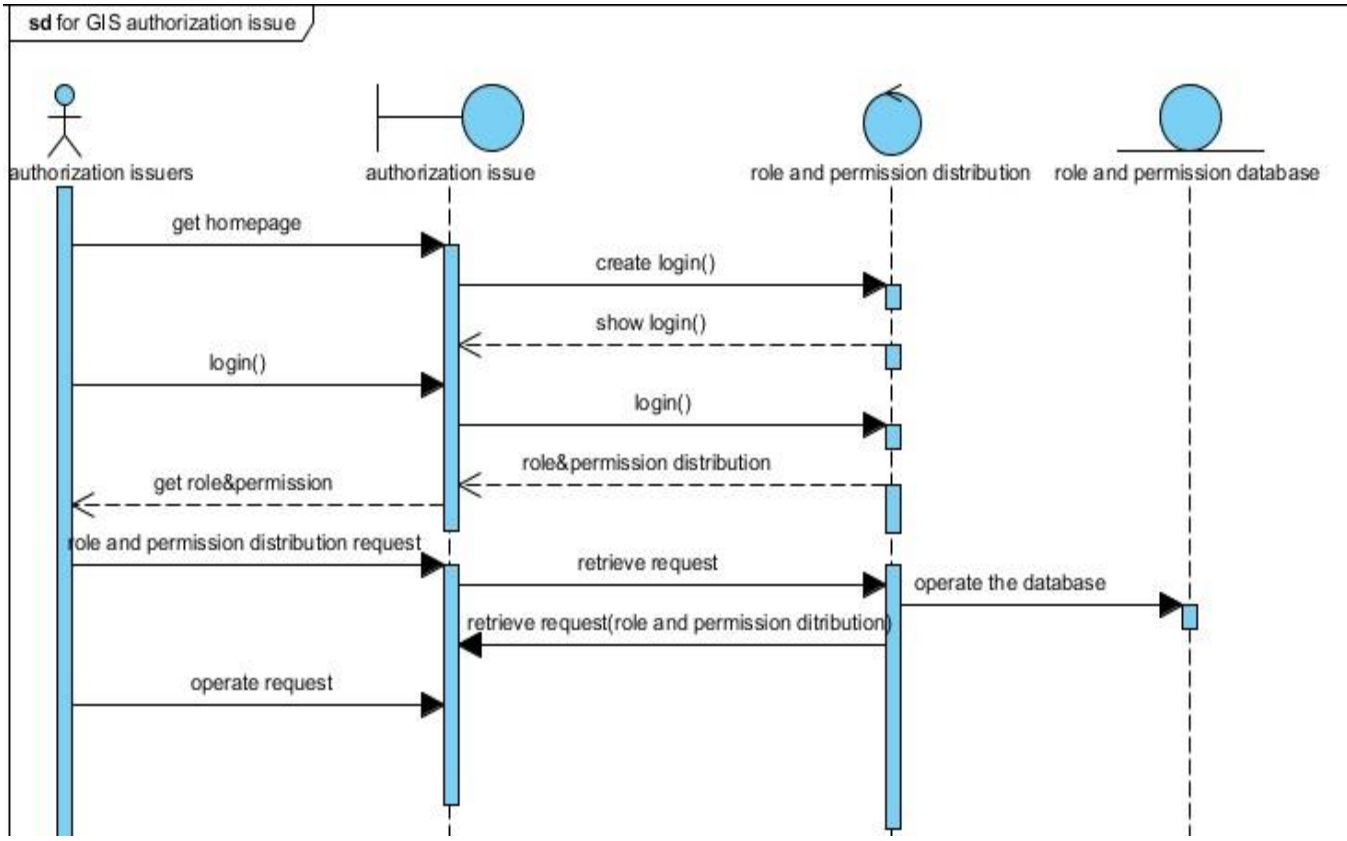

Figure 15: A sequence diagram for GIS authorization issuers

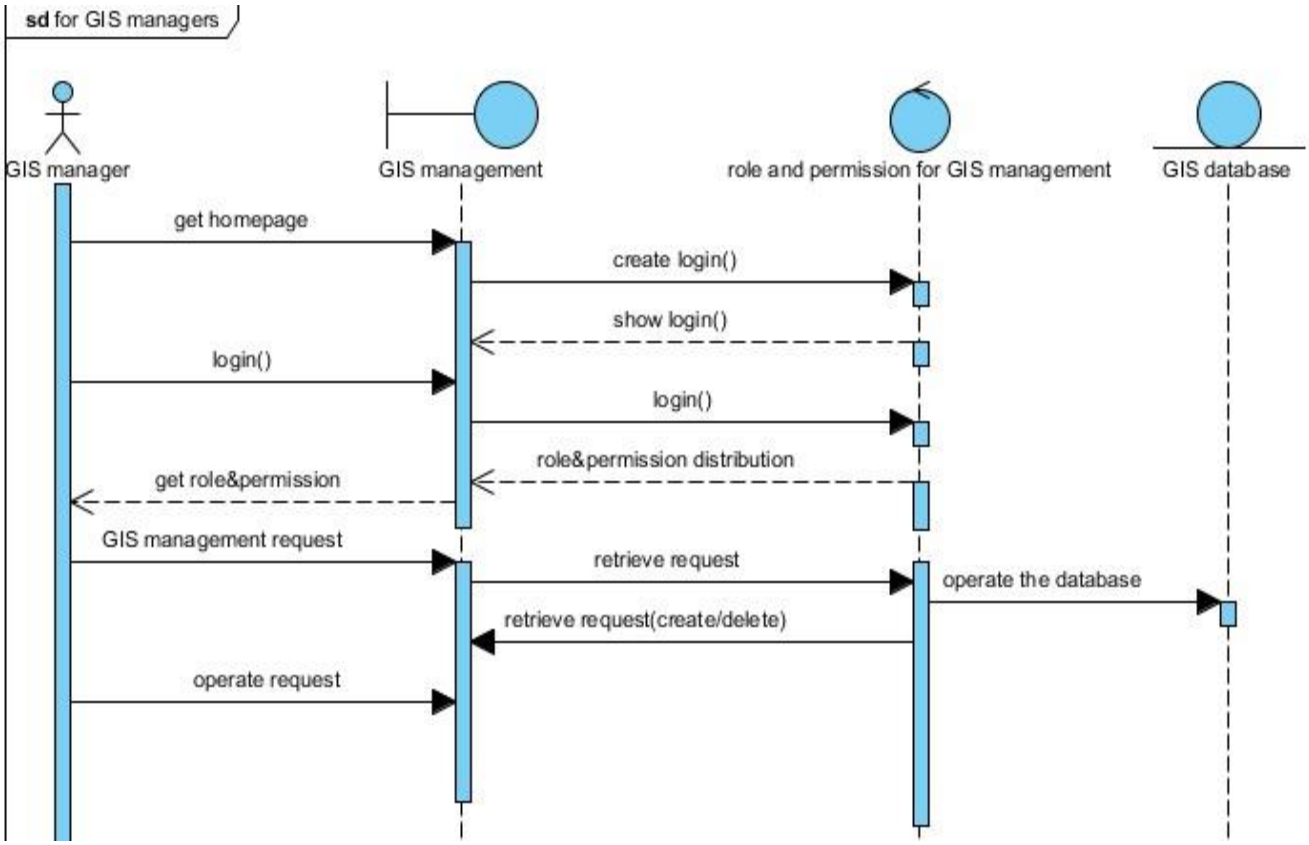

Figure 16: A sequence diagram for GIS managers

7. Access Control

7.1. GIS Security Configuration

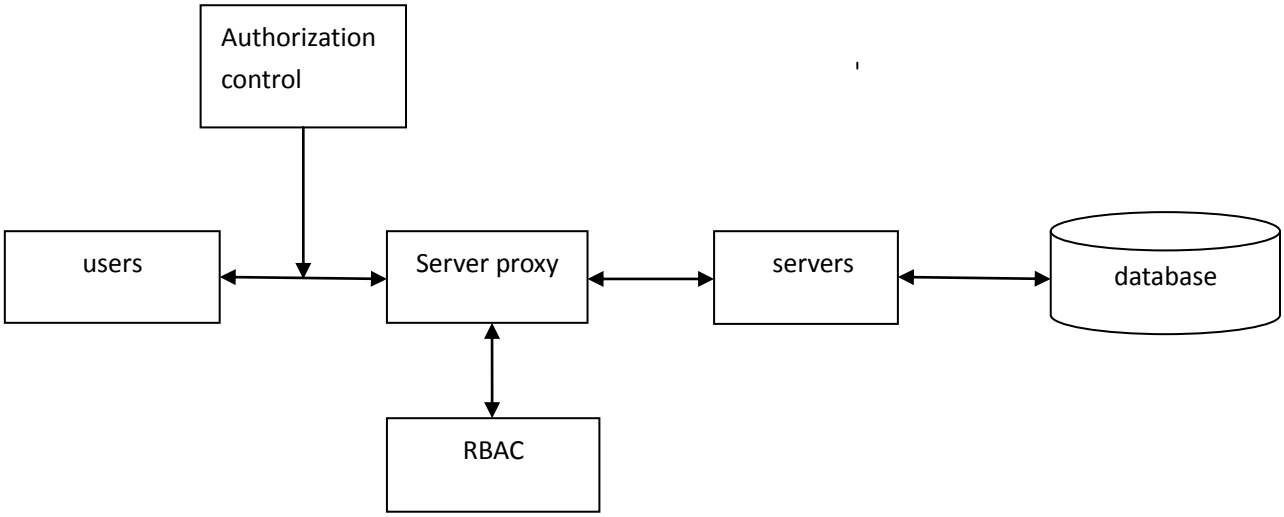

Figure 17: GIS security configuration

As shown in Figure 17, this configuration consists of users, server proxy, authorization control objects. Authorization control is mainly responsible for the role and permission distribution to users. In this way, when users request information, they will be given a special role allowing users to access specific objects information. Service proxy is communication connection between users and servers, users request and servers feedback can only be realized through server proxy. What's more, server proxy can control visit access from users in terms of their roles and give permission (context to be accessed) to users and cipher or decipher the data transmitted between users and servers.

Generally, users gain role and permission distribution, the server proxy can implement role-based access control (RBAC) and cipher or decipher transmitted data information, which assure and enhance security in GIS.

7.2 Role-Based Access Control Modeling

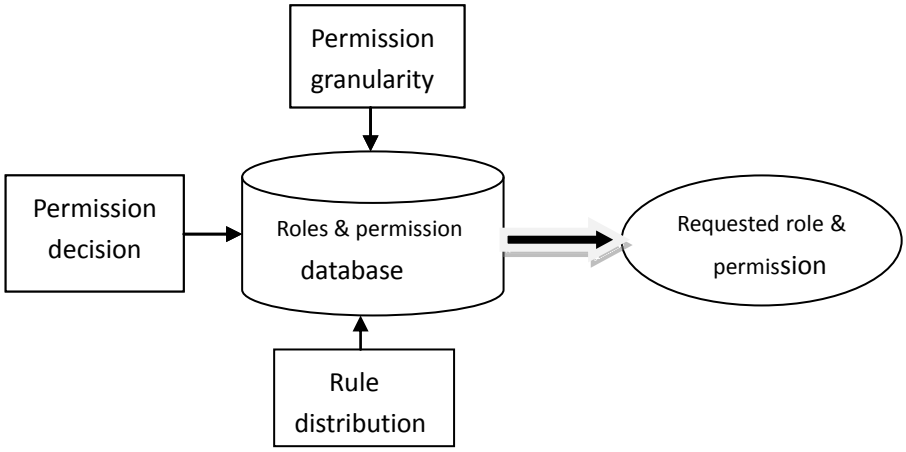

Figure 18: RBAC control modeling

As depicted figure 18 in the modeling, the RBAC can consist of roles and permission database, permission role, permission decision, permission granularity. Spatial data include special references and attribute data, which should be authorized concurrently in order to avoid authorization disagreement. In this sense, only managers can have the right to grant and cancel permissions. As for the role based access control, we define[r, o, m], r represents roles, o represents objects at specific layers and m means methods (Read, Write, Zoom-in/out, modification, delete etc.)
Granularity determines the vertical authorization permission users can access. According to the following authorization structure, as described in [2].
$<U_R, O_L, T>$
U_R is the user in a given Role, O_L is the special object at level L for which access is to be authorized. And T is a tuple, an ordered list of elements, specifying a chain of authorizations for O_L across the various spatial data layers.

Users may want to access to check a tuple in a specific level, but, sometimes they just want to gain more detailed data information instead of all information available in a tuple. For example, users want to know the information about Como schools, and when users get the role and permission to access this information, they can also know other information in this layer, such as hospitals, stadium, and shopping places, etc.. At this situation, we can define users as Role01, and give Role01 an object ID as 11, and the relevant permission is 'read'. We can define as [Role01, 11, Read]. Given this role, not only users can access Como schools requested by users specifically, but also they can access other such information as hospitals, stadium, and shopping places in this area.

However, if users just want to Como schools information and want to exclude other information unhelpful to them. We can define [Role01, All schools in Como, Read], in this way users can only access the schools in this area instead of all information in this area. Here 'All schools in Como' is spatial request clause.

7.3 Access Control Process with RBAC in GIS

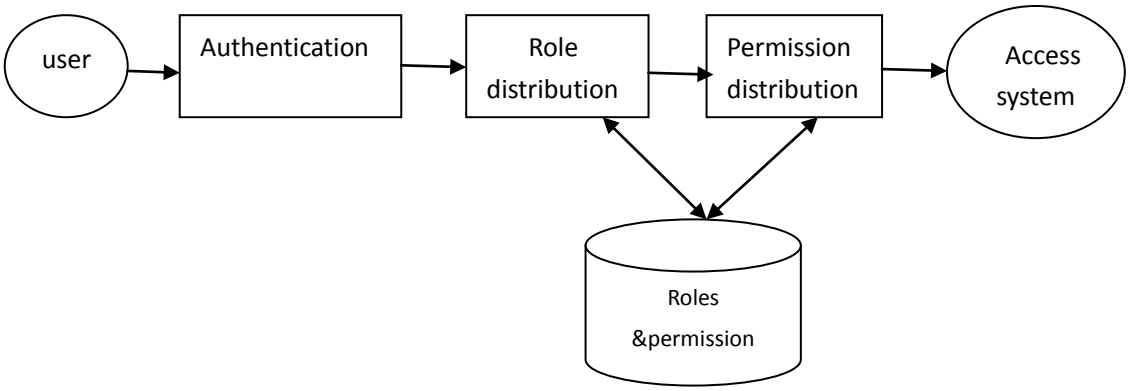

Figure 19: Access control process with RBAC in GIS

From Figure 19, we can know that in every service, a user should be authenticated and send request to servers for accessing information. At the same time, users will be given permission for specific objects in the specific layers based on their roles. When users have role and permission, they can be authorized to read, write, zoom, modification or delete information provided by servers.

7.4 Use of Authorization Model for Context Analysis

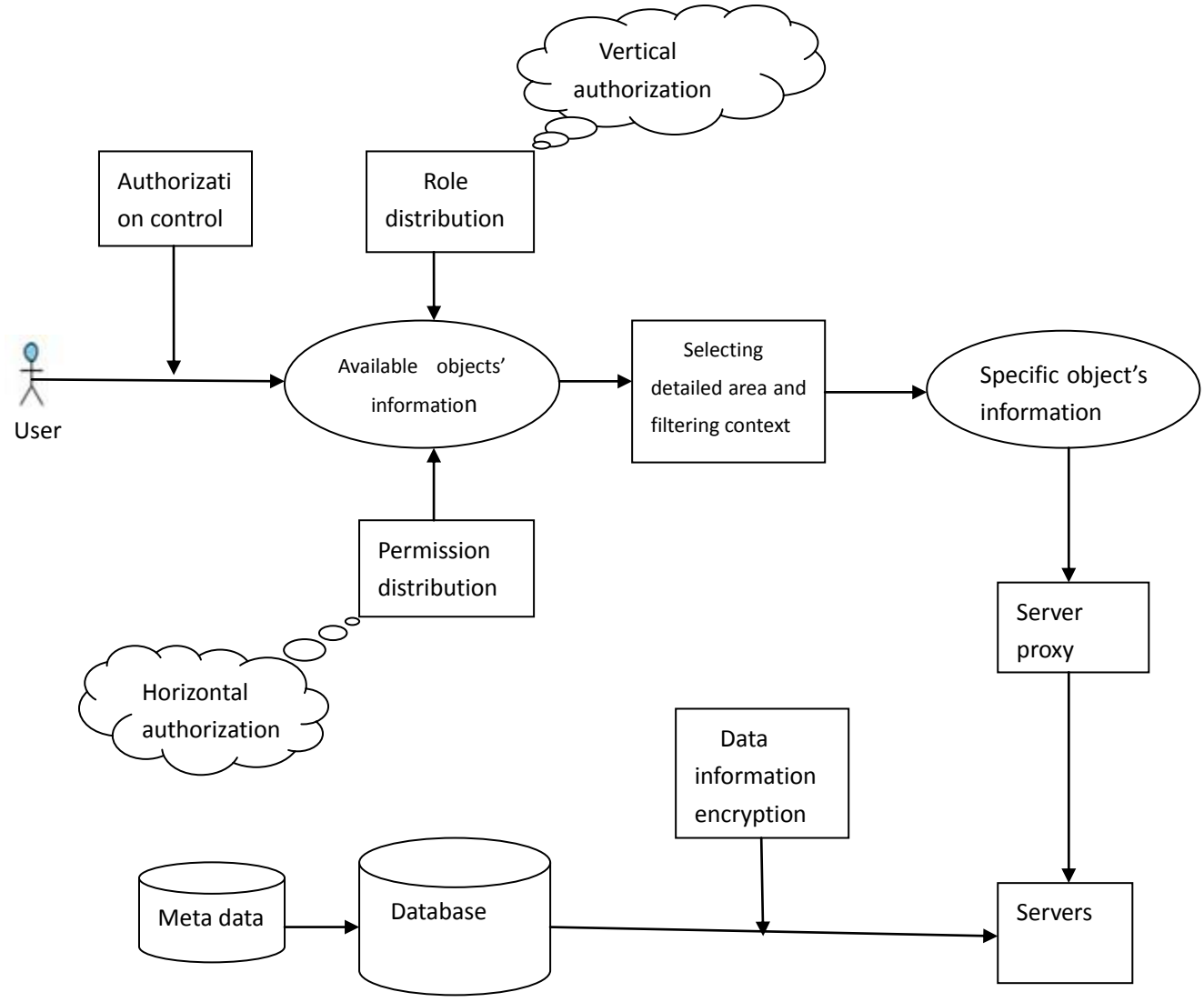

Figure 20: Authorization model based on context analysis in GIS

This section presents the above authorization model (figure 20) to demonstrate process of GIS information retrieval and security issues that could happen as well as how to solve these security problems.

From the figure, we can see that users want to gain information stored in the database in the form of context clustering. Firstly, users should be authorized to access information all available in terms of users' role and permission distributed by authorization entity in which users' ID must be checked and validated. However, information displayed may not be what the users what and may be cumbersome. For example, a green manager wants to decide how much should be invested to improve the green coverage by 30%. In this situation, he may just want to understand all green information about this area, including streets with trees, mountains, forestry,

park and change of green condition over a period of time. But when he first enters the information interface, he gets all available information in terms of his role and permission. Including economic situation, wells, governments, etc., this is burdensome because some information is not useful for him to make decisions but must be dealt by him, which is not efficient and effective. In this sense, we provide a model in which users can select a specific area or filtering context information further, in this way, users can hide that unhelpful information to access specific green information in a chosen specific area, which help better analyze and make decisions. After the selected areas and filtered contexts, users will access the information interface to get the more specific information, based on this interface and information, users can zoom in, zoom out vertically and horizontally with different granularity and continue to select and filter if necessary. As shown in the figure, request from users can be transmitted through server proxy to information servers which retrieve related data from database, in which data are encrypted to secure information.

In order to access information, users must get a role and permission. Role distribution enables users to get information granularity in terms of vertical authorization in the different hierarchical layers, permission distribution allows users to access information details in terms of context authorization in the same layer.

8. Conclusion

This thesis has proposed a security model for security issues in GIS. Based on context analysis purposes, this model enables users to access specific spatial objects in terms of their roles and permissions and helps users to make decisions based on context analysis. This is critically important for the application of GIS because users just seek useful data for context analysis and decision making. In this way, users can save time and enhance effectiveness.

There are two important problems which should be noticed in this model. Firstly, we need to cluster data in terms of their contexts with similar context attributes, we should establish Meta data to better manage database system. Meanwhile, geographic and demographic attributes in a selected area should always be provided in each of the context levels because Geo and Demographic attributes are basic and widely used information. Secondly, role and permission distribution should be controlled in a balanced way. Role distribution deals with vertical authorization in a hierarchical way and permission distribution copes with context or horizontal authorization in the same level.

We proposed model to assure security in GIS in terms of RBAC, data transmission and sharing. For further study, applicability of this model can be done to solve problems,

such as items connected to smart cities, real estates and e-government and so on, and also a much more overall and systematic GIS security model is badly needed in order to meet users' requirement and technology development, such as mobile users.

9. Acknowledgements

This paper is supervised by Professor Mariagrazia Fugini. I am very grateful to her for her patience and kindness. Nothing could be done without Professor Fugini's help and suggestions.

10. References

[1] Zhong-ren Peng and Ming-Hsiang Tsou. INTERNET GIS Distributed Geographic Information Services for the Internet and Wireless Networks. Published by John Wiley & Sons, Inc., Hoboken, New Jersey. 2003.

[2] Ravi Sandhu, David Ferraiolo, Richard Kuhn. The NIST Model for Role-Based Access Control: Towards A Unified Standard. 2000.

[3] Mariagrazia Fugini. Spatial Data Security: Analysis Contexts and Authorization Model. Department of Electronic, Information and Bioengineering, Politecnico di Milano.

[4] Murti K C S, Venkat R Tadimeti. A Simplified GeoDRM Model for SDI Services. Bilra Institute of Technology Pilani, India. Proceeding ICCCS'11 Proceedings of the 2011 International Conference on Communication, Computing and Security. 545-548.

[5] Michael Govorov, Youry Khmelevsky, Vasiliy Ustimenko, etal. Security for GIS N-tier Architecture. Developments in Spatial Data Handling, Leicester: Springer Berlin Heidelberg. Peter F. Fisher, 2005. 71-83.

[6] Elisa Bertino, Barbara Catania, Maria Luisa Damiani, et al. GEO-RBAC: a spatially aware RBAC. In Proc, 10th ACM Symposium on Access Control, 2005,29~37.

[7] Sahadeb De, Caroline M.Eastman, Csilla Farkas. Secure Access Control in a Multi-userGeodatabase. http://gis.esri.com/library/userconf/proc02/pap0355/p0355.htm .

[8] Samba Sesay, Zongkai Yang, Jingwen Chen and Du Xu. A secure Database Encryption Scheme. Consumer Communications and Networking Conference, 2005. 49~53.

[9] Elisa Bertino, Barbara Catania, Maria Luisa Damiani. GEO-RBAC: A Spatially Aware RBAC. Proceedings of the tenth ACM symposium on Access Control Models and Technologies. 29-37.

[10] Li Juan. Secure GIS research and application. Zhong Nan University. 2008.

[11] Mariagraza Fugini. Architectural and Security Aspects in Spatial Decision Support Systems. ITAis Workshop, Milan, Dec 19,2013.

[12] Yu,J., Benatallah, B., Casati, F., Daniel, F., 2008. Understanding mashup development, IEEE INTERNET COMPUTING Volume: 12 Issue: 5, Pages:44-52.

[13] Papa, Rocco and Gargiulo, Carmela and Galderisi, Adriana (2013) Towards an urban planners' perspective on Smart City. TeMA Journal of Land Use, Mobility and Environment, 6 (01). pp. 5-17. ISSN 1970-9870.
[14] Mahmoud AL-HADER, Ahmad RODZI. The smart city infrastructure development and monitoring. Theoretical and Empirical Researches in Urban Management. Number2(11)/May 2009.
[15] Sreekanth PD, Kumar KV, Soam SK, Rao NH and Bhaskar Kannoju. GIS-based Decision Support System(DSS) for Recommending Retail Outlet Locations. Information and Knowledge Management Vol.3, No.4, 2013.
[16] George H.(Jody) Tompson, S.Wright Kennedy. Where Exactly is the Target Market? Using Geographic Information Systems for Locating Potential Customers of a Small Business. Entrepreneurial Practice Review, VOL 2, NO 4(2013).
[17] Michele Argiolas, Nicoletta Dessì, Barbara Pes A Web-Based Application Supporting Real Estate Decision Making, Internal Report University of Cagliari, May 2013.
[18] Gang Pan, Guande Qi, Wangsheng Zhang, Shijian Li, and Zhaohui Wu, Zhejiang University Laurence Tianruo Yang, Huazhong University of Science and Technology and St. Francis Xavier University. Trace Analysis and Mining for Smart Cities: Issues, Methods, and Applications. IEEE Communications Magazine , June 2013. Pages:120-126.
[19] Ari-Veikko Anttiroiko, Pekka Valkama, Stephen J. Bailey. Smart cities in the new service economy: building platforms for smart services. Springer-Verlag London 2013.
[20] Mourjo Sen, Anuvabh Dutt, Jennifer Shah, Shalabh Agarwal, Asoke Nath. Department of Computer Science St. Xavier‟s College (Autonomous), Kolkata, WB, India. Smart Software and Smart Cities: A study on Green Software and Green Technology to develop a smart urbanized world. International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-2 Number-4 Issue-6 December-2012.
[21] R. De Santis, A. Fasano, N. Mignolli, A. Villa. Smart cities: theoretical framework and measurement experiences. MPRA Paper No. 50207, posted 26. September 2013.
[22] Kaspars Cabs, Arnis Lektauers, Yuri Merkuryev. A methodology for automated geosimulation model generation. International Conference on Applied Information and Communication Technologies (AICT2013), 25.-26. April, 2013, Jelgava, Latvia.
[23] Vimal Gahlot, B.L. Swami, M. Parida, Pawan Kalla. User oriented planning of bus rapid transit corridor in GIS environment. International Journal of Sustainable Built Environment (2012) 1, 102–109.
[24] Hafedh Chourabi ,Taewoo Nam,Shawn Walker. Understanding Smart Cities: An Integrative Framework. 2012 45th Hawaii International Conference on System Sciences.