Journal of Engineering and Applied Sciences 13 (2): 505-512, 2018
ISSN: 1816-949X

Access Control Techniques for Web Service Security

Jeong-Joon Kim, Teayoung Kim, Kwang-Jin Kwak and Jeong-Min Park
Department of Computer Engineering, Korea Polytechnic University,
Gyeonggi-do, 15073 Siheung-si, South Korea

Abstract: Recently, as the demand for high value-added spatial information contents increases, various technologies for spatial information security are increasingly needed. However, supplementary policies are managed independently in each system, There is a problem that the reliability is poor. Therefore, GeoXACML is proposed based on XACML in OGC for the control of spatial information access as the need for a common language for expressing security policies increases. GeoXACML extends spatial information types and functions for spatial access control. Therefore, this study develops GeoXACML based access control technology that can expand the grammar and semantics and provide integrated security policy for many platforms and programs.

Key words: Web security, XACML, GeoXACML, PEP, PDP, PAP

INTRODUCTION

With the recent convergence of spatial information and various multimedia, the demand for high value added spatial information contents has increased and the cases of damage due to insufficient security have increased rapidly. Therefore, the need for precise access control for the management of spatial information and information security has been emphasized in domestic and Foreign public institutions and corporations and as the need for a common language for expressing security policies has increased, OGC an international standardization organization, GeoXACML is proposed to extend the spatial information type and function in the proposed access control language, XACML (Anonymous, 2005, 2007).

Therefore, this study researches and develops access control system based on GeoXACML proposed by OGC an international standardization organization. The developed GeoXACML based access control system is composed of Geo PAP for creating policy or policy set for spatial information access control, Geo PAC for generating decision request for spatial information access control, PEP, Geo PDP for evaluating applicable policy for access request of spatial information and Geo PDP for determining whether or not to grant access to user's query based on spatial information access control decision, related system WMS (Web Map Service) or WFS (Web Feature Service) and a context handler that converts the request and response contexts (Yuan and Tong, 2005; Tao, 2005).

GeoXACML-based spatial information access control system has been extended based on open source XACML API under study by Sun to manage methods and attributes and related data to process XACML requests. By using GeoXACML, it is possible to support spatial operations, extend syntax and semantics and provide integrated security policies for many platforms and programs. This can induce distribution of reliable spatial information for various digital contents including spatial information and it is possible to utilize secure spatial information because security can be enhanced through access control to online spatial information. Finally, the effectiveness of the system was tested by setting and applying the virtual scenario requiring the access control system.

Literature review

Related technology trends: XACML (eXtensible Access Control Markup Language) is an XML-based access control policy language that allows OASIS and ITU-T to grant rights to authorized resource request entities and access resources (Lorch *et al*., 2003; Anonymous, 2005). XACML provides an XML schema that can specify the access control policy, the request context and the response context as XML, so that, the system can automatically make a policy decision when a user makes a request and respond as a result. XACML was adopted as 1.0 in 2003 and 2.0 in 2005 and is currently being standardized for 3.0.

The Platform for Privacy Preference (P3P) is a standards-related privacy protection technology

Corresponding Author: Jeong-Min Park, Department of Computer Engineering, Korea Polytechnic University,
237 Sangideahak-ro, Siheung-si, Gyeonggi-do, South Korea

developed by the W3C. It is a standard related to data processing and user's personal information on websites. P3P is expressed in XML format for automatic analysis of privacy policy between information communication service provider and service user. When a service user accesses a specific web site by using a web browser, the web site provides a policy regarding privacy protection to the user's web browser and the user compares the level according to a preset privacy policy and then processing it according to the result. However, P3P does not enforce mandatory enforcement to ensure that personal information was used correctly for the purpose of collecting it. P3P is a meaningful technology only on the assumption that the service user has infinite trust in the telecommunication service provider.

The Enterprise Privacy Authorization Language (EPAL) was licensed by W3C as a standard technology developed jointly by IBM and ZKS. EPAL is intended to establish and exchange policies on privacy information such as customer information in the enterprise and uses the concept of vocabularies to create a privacy policy. It defines a hierarchical list of user categories, data categories, objectives, behaviors, conditions and obligations and uses these vocabularies to create privacy policies . The EPAL policy is created by combining these vocabularies. EPAL defines the format of the request message requesting the use of information. The request message includes a user category an action, a data category and a purpose (Anonymous, 1999).

ZKS and IBM jointly developed an XML-based enterprise-standard privacy tool in 2001 and in February 2002 jointly developed and released the Enterprise Privacy Markup Language (EPML) 1.0 specification, a privacy-related standard. This specification has since become the basis of IBM's Enterprise Privacy Authorization Language (EPAL) 1.0.

IBM Security Solutions provides identity management and access control. Through its integrated identity management and access control solution, IBM provides policy-based services to efficiently manage authentication and access rights to existing Web services applications. It is also responsible for authentication issues in SSO through IBM Identity and Access Management Services.

HP openView select access is an integrated account management solution that allows you to centrally manage user's access to e-Commerce or internal resources. SAML-based single sign-on, user management and delegation, user authentication and access control, user registration and profile self-management, integrated account management and password management.

GeoXACML: GeoXACML is an extension of the spatial operation function to XACML, the access control standard for the development and integration of distributed geographic information (Anonymous, 1999, 2002, 2003, 2007). This was adopted by OGC in 2007 and has been updated to 1.0.1 through the 2011 revision. GeoXACML enables the implementation of an access control system that controls access through spatial operations and interoperability. It also restricts access based on spatial limits and conditions, so that, access to specific spatial information can be accessed only by specific objects. It is possible.

Since, GeoXACML is an extension of XACML, it follows the existing XACML policy language authorization model, information flow model and component concept such as PAP, PDP, PEP, PIP related to XML policy schema and policy. A policy is a set of rules for controlling access and a decision is made by a plurality of policy combining algorithms. PAP is a component that generates and manages rules for controlling access and PEP is a system element that performs access control by generating decision requests and enforcing authorization decisions. A PDP is a system element that evaluates applicable policies and makes authorization decisions. A PIP is a system element that accesses a spatial information service and obtains attributes necessary for judgment.

Extended spatial data types and spatial functions in GeoXACML are used to define additional spatial constraints for XACML-based policies. GeoXACML uses a spatial data model based on the simple geometry of OGC and defines a structured <AttributeValue> type to represent the simple geometry of GML 3.0 following the policy language of XACML. The newly added datatype is urn: ogc: def: dataType: geoxacml: 1.0: geometry which is a superclass of all geometric datatypes. This simplifies function declaration and avoids the complexity of introducing many datatypes. It is intended to facilitate implementation.

MATERIALS AND METHODS

System design

System introduction: The GeoXACML-based access control system structure is shown in Fig. 1. GeoXACML based access control systems are classified into Geo PAP, Geo PDP and Geo PEP manager. Geo PAP is a system element for creating a policy or policy set for spatial information access control. Geo PDP is a system element for evaluating policy for spatial information access control and determining authorization and Geo PEP is a system element for controlling spatial information access control

Is a system element for generating a decision request and performing access control on an authorization decision (Fig. 1).

Geo PAP manager: The GeoDRM agent is responsible for checking the authority to display on the GeoContents screen and controlling the authority to view the data from unauthorized users and the download agent is responsible for downloading GeoContents from a server external to GeoContents. And End-User refers to the user who inquires and updates GeoContents information.

GeoContents access control checks whether the user has access rights to GeoContents. Time access control controls the available time for access time when checking access rights to GeoContents.

Spatial unit access control controls the available time for available space (when GPS receiver attached to the terminal is used and not available when there is no GPS receiver) when checking access rights to GeoContents and information protection is performed in GeoREL based on the description, users who do not have access control the ability to access and view GeoContents.

Access control space operation access to GeoContents based on the contents described in GeoREL if some areas do not have access right within the area requested by the user it performs other spatial operations such as masking and cropping some areas that are not accessible.

Geo PDP manager: Geo PEP requests WSE and WMS queries from users and requests policy decision from Geo PDP. If Permit, it queries WFS and WMS again and returns the result. Geo PDP supports policy and attributes defined in Geo XACML specification It is a system that processes decision point, receives query from Geo PEP and returns the result of policy decision. The policy repository is where Geo XACML is stored which is the basis for judging policy decision of Geo PDP (Fig. 2).

In the GeoXACML request and policy processing for a specific service, the Geo PEP analyzes the request and selects a different repository according to getmap, get feature and transaction to perform policy decision. In the phase function processing when the Geo PEP uses the phase function in the condition of the policy suitable for

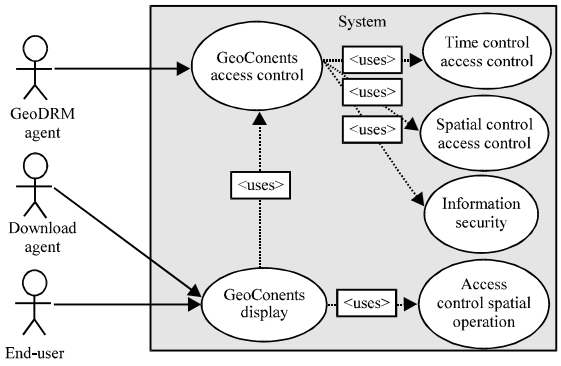

Fig. 1: Features of Geo PAP manager

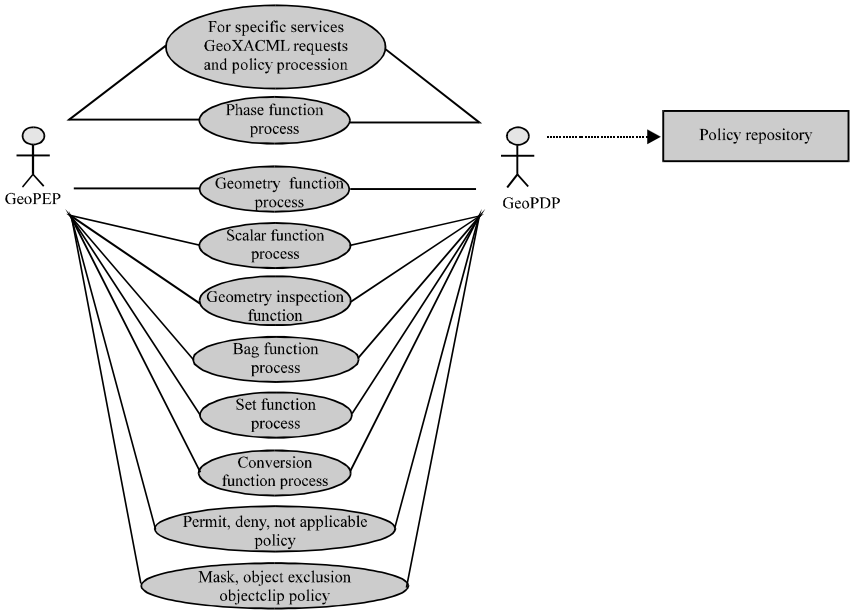

Fig. 2: Features of Geo PDP manager

the inquired query, the operation of the corresponding phase function is processed and the result is returned.

In the geometric function processing, Geo PEP uses the geometric function for the condition of the policy suitable for the inquired query, processes the operation of the corresponding phase function and returns the result. In scalar function processing, if a Geo PEP uses a scalar function in a policy condition that is suitable for a query that is queried, it processes the operation of the scalar function and returns the result.

In geometric prediction function processing, if Geo PEP uses a geometric check function in the condition of a policy that is appropriate to the request that is queried it returns the result by processing the operation of the geometry check function. In the case of the Bag function processing if you use the bag function on the condition of the policy, the operation of the corresponding bag function is processed and the result is returned.

In the aggregate function processing when the bag function is used for the condition of the policy suitable for the request which is inquired by the Geo PEP, the operation of the set function is processed and the result is returned. Transform function processing when a Geo PEP uses a transform function in the condition of a policy that is suitable for a query it processes the transform function and returns the result.

Allowed, unacceptable, unapplicable in making a policy decision, the result of a policy that is appropriate for a request that is queried by Geo PEP is set to one of the allowed, denied or not applicable values. And in Mask, ObjectExclusion and ObjectClip policy decision, the result of the policy suitable for the request that the Geo PEP inquired is determined as one of Mask, ObjectExclusion, ObjectClip.

Geo PEP manager: The Geo Rights Issuer makes a packaging request to the Geo Content Packager and the Geo Content Packager packages the geographical information.

In general packaging, geographic information data is packaged in packaging group packaging and geographic information is packaged in one group key (Table 1).

Table 1: Main processing flow chart of Geo PDP manager

Main processings	Flows
GeoXACML requests and policy processing for specific services	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the service type in XACML (GetMap, GetFeature, Transaction) and selects the appropriate policy repository for the service
	Analyze the results of the XACML policy decision requested by GeoPEP in the selected repository
	Communicate the policy decision to GeoPEP
Policy processing with topological functions	GeoPAP creates a policy containing the topological function and records it in the policy repository
	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the request and generates the result of the policy by applying the topological function created by GeoPAP in the policy repository
	Pass the policy decision to GeoPEP
Policy processing with geometry functions	GeoPAP creates a policy containing geometry functions and writes them to the policy repository
	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the request and generates the result of the policy by applying the geometry function created by GeoPAP in the policy repository
	Pass the policy decision to GeoPEP
Policy processing with scalar functions	GeoPAP creates a policy containing a scalar function and writes it to the policy repository
	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the request and generates the result of the policy by applying the scalar function created by GeoPAP in the policy repository
	Pass the policy decision to GeoPEP
Policy processing with geometry checking functions	GeoPAP creates a policy containing the geometry check function and records it in the policy repository
	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the request and applies the geometry check function created by GeoPAP in the policy repository to generate the result of the policy
	Pass the policy decision to GeoPEP
Policy processing with the Bag function	GeoPAP creates a policy containing the geometry check function and records it in the policy repository
	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the request and applies the geometry check function created by GeoPAP in the policy repository to generate the result of the policy
	Pass the policy decision to GeoPEP
Policy processing with set functions	GeoPAP creates a policy containing the set function and records it in the policy repository
	GeoPEP sends an XACML request containing a geometry object
	GeoPDP analyzes the request and generates the result of the policy by applying the set function created by GeoPAP in the policy repository
	Pass the policy decision to GeoPEP
Policy processing with transform functions	GeoPAP creates the policy containing the conversion function and records it in the policy repository
	GeoPEP sends an XACML request containing a geometry object

Table 1: Continue

Main processings	Flows
	GeoPDP analyzes the request and generates the result of the policy by applying the conversion function created by GeoPAP in the policy repository
	Pass the policy decision to GeoPEP
Determining Permit Policy	GeoPAP creates a policy whose result of policy decision is permit on the access of a geometry object contained in a specific area and records it in the policy repository
	GeoPEP sends an XACML request to access the geometry objects contained in the area
	GeoPDP analyzes the request and applies the policies of the policy repository to generate a permit result
	Pass Permit results to GeoPEP
Deny policy decision	GeoPAP creates a policy whose result of policy decision is deny for accessing a geometry object contained in a specific area and records it in the policy repository
	GeoPEP sends an XACML request to access the geometry objects contained in the area.
	GeoPDP analyzes the request and applies the policies of the policy repository to generate deny results
	Pass deny results to GeoPEP
Non applicable policy decision	GeoPAP creates a policy whose result of policy decision is permit or deny for accessing a geometry object contained in a specific area and records it in the policy repository
	GeoPEP sends an XACML request to access a geometry object that is not included in the area
	GeoPDP analyzes the request and applies the policies of the policy repository to generate Non Applicable results
	Pass non applicable results to GeoPEP
Mask policy decision	GeoPAP uses the geometry-deny operator to create a policy whose result is a mask and write it to the policy repository
	GeoPEP sends an XACML request to access the geometry objects contained in or over the area defined by the geometry-deny operator
	GeoPDP determines the overlap of the area defined by the geometry object of the request and the geometry-deny operator as the masking area and generates the Mask result
	Pass the mask result to GeoPEP with masking field
Objective Exclusion Policy Decisions	GeoPAP uses the geometry-deny operator to create a policy whose result is object exclusion and write it to the policy repository
	GeoPEP sends an XACML request to access the geometry objects contained in or over the area defined by the geometry-deny operator
	GeoPDP extracts the objects except the objects that span the area defined by the geometry object of the request and the geometry-deny operator, and generates the result as a featurecollection of wfs
	Pass the result of ObjectExclusion of type featurecollection to GeoPEP
Determining the ObjectClip policy	GeoPAP uses the geometry-deny operator to create a policy whose result is an ObjectClip and write it to the policy repository
	GeoPEP sends an XACML request to access the geometry objects contained in or over the area defined by the geometry-deny operator
	GeoPDP creates the geometry object in the form of a FeatureCollection of WFS by creating Geometry that overlaps the outer region of the deny region with respect to the objects that span the region defined by the geometry object of the request and the geometry-deny operator
	Pass the result of ObjectClip of FeatureCollection type to GeoPEP

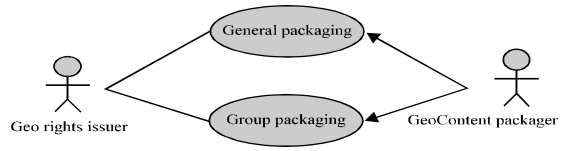

Fig. 3: Features of Geo PEP manager

System demo: Geo PAP is a system element for creating a policy or policy set for spatial information access control. It creates a policy for access control by using the spatial information types and functions defined in the spatial information access control markup language (GeoXACML). And provides a UI that can provide user convenience when creating an access control policy (Fig. 3). The created spatial information access control policy stores the policy in the access control policy storage that can store the policy and provides the spatial information access control policy statement of the corresponding control object when the access control policy of the other GeoXACML node is inquired. In addition, the third-party system inquires the policy through the Spatial Information Access Control Policy Generation Node (Geo PAP).

The Geo PDP is a system element that evaluates the applicable policy for spatial information access control and makes authorization decisions. The Geo PDP is an access control standard request (spatial information Access Control Markup Language (GeoXACML) format) and access control policy is retrieved from the Spatial Information Access Control Policy Generation Node (GeoPAP) or access control policy repository. It determines access control based on access control request and access control policy (Fig. 4 and 5).

Table 2: Main processing flow chart of Geo PEP manager

Main processings	Flows
General packaging	Receive a packaging interface message from Geo RI
	Paste the packaging interface to extract the required parameters configure the DCF header
	Load the original file from the Geo repository
	Package the original file and save it with the Hader in the georepository
	Generate packaging results with XML interface
	Output the result XML
Group packaging	Receive a packaging interface message from Geo RI
	Paste the packaging interface to extract the required parameters
	Enter the packaging parameters
	Configure the DCF header
	Load the original file from the Geo repository
	Package the original file with the group key and store it with the Hader in the Geo repository
	Generate packaging results with XML interface
	Print the resulting XML

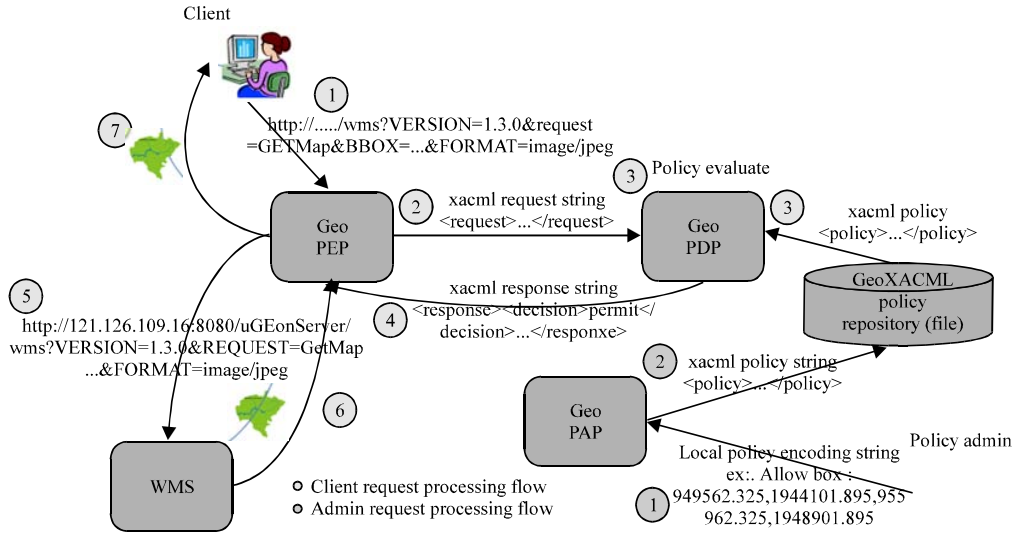

Fig. 4: Flow of query processing

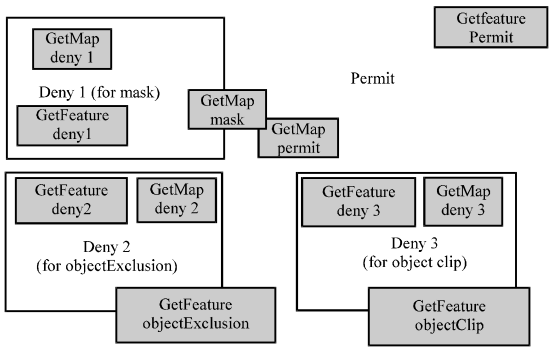

Fig. 5: Query example

The Geo PEP generates a request for spatial information access control and receives the service access request from the access requestor and transmits the access control service response information to the system element which performs the access control by performing the authorization decision (Table 2). In order to determine the access control for the received service request, a request is made to the Spatial Information Access Control Decision Node (Geo PDP) and the access control is received. Figure 4 shows the query processing flow chart.

The query provided by the system developed in this study is divided into three types: GetMap, GetFeature and Transaction. GetMap is an interface for accessing GIS data based on WMS. It is a service using map image (format) through the web. That is, it is a service for visualizing a layer stored in a data server or vector and raster data generated through analysis. GetFeature and Transaction are interfaces for providing GIS data in vector form via. WFS based on WFS. It is used to import and manage (add, modify, delete) vector layers in data server using space and attribute conditions service. Figure 5 shows an example three queries.

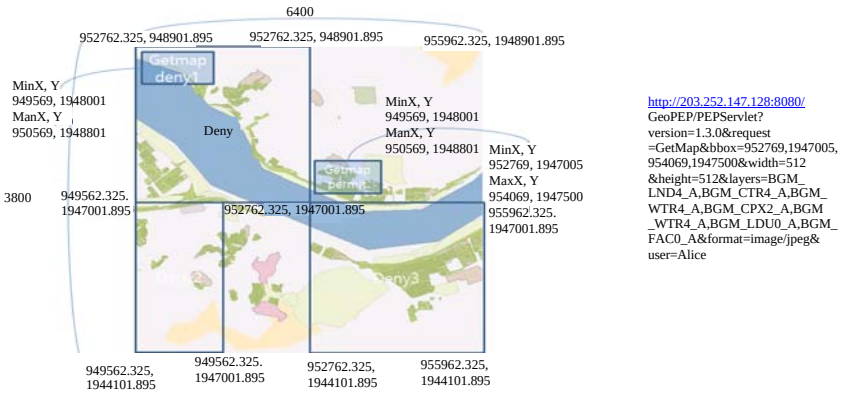

Fig. 6: GetMap query

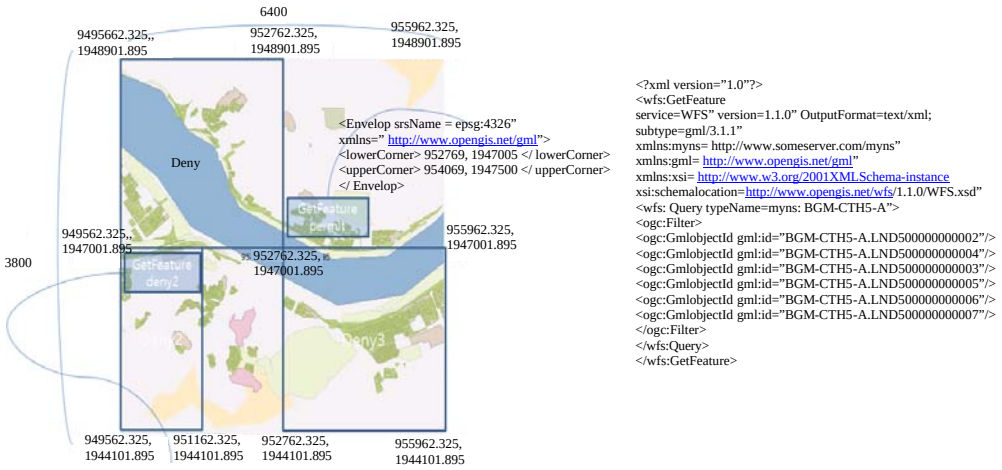

Fig. 7: GetFeature query

GetMap: The query is a query that requests a map image in a specific area with an Alice account in a GetMap query. At this time, the is returned only when the privilege defined in the policy is allowed (Fig. 6 and 7).

GetFeature: The above query is a query that requests, adds, deletes or changes information of a stored vector layer matching a specific space and attribute condition with an Alice account in a GetFeature query. At this time, the result is returned only when the privilege defined in the policy is allowed.

The above query is an ObjectExclusion query of the GetFeature and an ObjectClip query. The ObjectExclusion query is to extract the objects excluding the objects that span a specific area. The ObjectClip query is a method for extracting the parts overlapping the outer area of the deny area To geometry to generate the result in the form of FeatureCollection of WFS (Fig. 8 and 9).

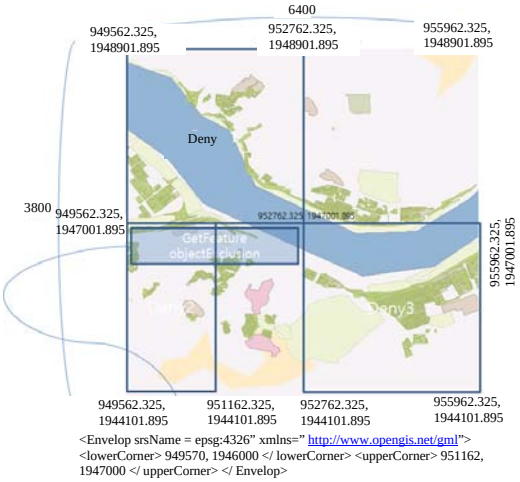

Fig. 8: GetFeature query (ObjectExclusion)

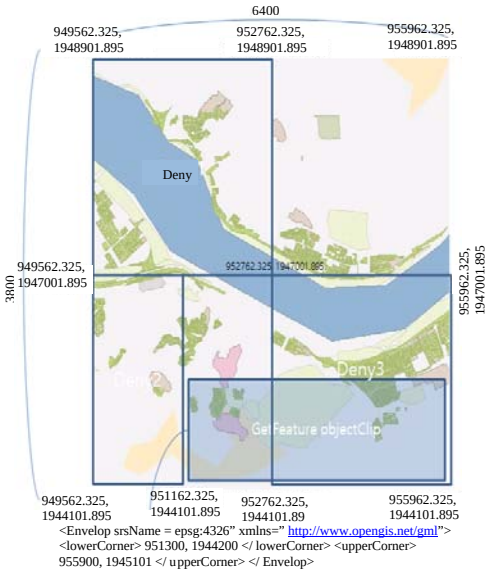

Fig. 9: GetFeature query (ObjectClip)

CONCLUSION

Recently, the necessity of various technologies for spatial information security has been increased and at the same time it has become a big issue to fix and integrate the policies used in the security service which are costly and unreliable.

Therefore, in this study, we designed and implemented GeoXACML based access control system which controls access through spatial operation and has interoperability. GeoXACML-based access control system is easy to extend syntax and semantics and supports object-based access control. In particular, it is possible to restrict access based on the spatial range and conditions that allow access to the spatial information only in a specific area. Finally, we verified the effectiveness of this system by applying a hypothetical scenario to the geographical information access control system based on GeoXACML developed in this study.

ACKNOWLEDGEMENTS

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2017R1A2B4011243).

REFERENCES

Anonymous, 1999. OpenGIS simple features specification for SQL. Open Geospatial Consortium, UK.

Anonymous, 2002. OpenGIS® Geography Markup Language (GML) implementation specifica-tion, version 2.1.2. Open Geospatial Consortium, UK.

Anonymous, 2003. Java topology suite version 1.4. The Vivid Solutions SEO Services, Web Designing & Web Development Company, Lahore, Pakistan.

Anonymous, 2005. eXtensible access control markup language (XACML) version 2.0. The Oasis Golf & Aqua Resort (Regional Office), Lahore, Pakistan. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

Anonymous, 2007. OpenGIS® GeoXACML implementation specification, version 1.0. Open Geospatial Consortium, UK.

Lorch, M., S. Proctor, R. Lepro, D. Kafura and S. Shah, 2003. First experiences using XACML for access control in distributed systems. Proceedings of the 2003 ACM International Workshop on XML Security, October 31, 2003, ACM, New York, USA., pp: 25-37.

Tao, H., 2005. A XACML-based access control model for web service. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing Vol. 2, September 26-26, 2005, IEEE, Wuhan, China, pp: 1140-1144.

Yuan, E. and J. Tong, 2005. Attributed based access control (ABAC) for web services. Proceedings of the 2005 IEEE International Conference on Web Services ICWS, July 11-15, 2005, IEEE, Orlando, Florida, USA., pp: 561-569.