A CONTEXT-AWARE BASED AUTHORIZATION SYSTEM FOR PERVASIVE GRID COMPUTING

MARILYN LIM CHIEN HUI

UNIVERSITI SAINS MALAYSIA
2015

A CONTEXT-AWARE BASED AUTHORIZATION SYSTEM FOR PERVASIVE GRID COMPUTING

by

MARILYN LIM CHIEN HUI

Thesis submitted in fulfillment of the requirements for the degree of Master of Science

February 2015

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation to my supervisor, Dr. Chan Huah Yong for his invaluable help. He provides supports, constructive criticisms and helpful suggestions during the research. Without his offering to accomplish this research, I would not be able to finish my study at USM. I’m thankful to Dr. Nabil Elmarzouqi for his help during my studies. He always gave a support for the in-depth discussion about the state-of-the-art of my research domain and various research problems. Instead he is the one inspiring me to conduct this study. I’m grateful to my lab mates, that always give me support and help me in better understanding of JAVA programming and Jade framework, and also all of my friends that always support and give full attention for me to solve my problems and being my personal proofreader and grammar coach. I would also like to thank my family for their fully encouragement and support. And I would like to express my gratitude to the School of Computer Sciences for making all this possible. I would also like to thank Universiti Sains Malaysia, USM for the financial support given through the USM Fellowship Scheme.

TABLE OF CONTENTS

CHAPTER 1 – INTRODUCTION

CHAPTER 2 – LITERATURE REVIEW

CHAPTER 3 – SIMULATION DESIGN AND IMPLEMENTATION

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACL	Agent Communication Language
ACM	Attribute Certificate Management
ADF	Access Decision Function
AEF	Access Control Enforcement Function
API	Application Programming Interface
CAS	Community Authorization Service
CoCoA	Context-Constrained Architecture
CMS	Context Management System
CN	Common Name
EALS	Enterprise Authorization and Licensing Service
JADE	Java Agent Development Framework
MAS	Multi-agent System
OGSA	Open Grid Services Architecture
PE	Policy Editor
PERMIS	Privilege and Role Management Infrastructure Standards Validation
PMS	Policy Management System
SAML	Security Assertion Markup Language
SSA	Session Service Authority
VO	Virtual Organization
VOMS	Virtual Organization Membership Service
XML	Extensible Markup Language
XACML	eXtensible Access Control Markup Language

SISTEM PENGESAHAN KUASA BERASASKAN KONTEKS UNTUK PENGKOMPUTERAN GRID PERVASIF

ABSTRAK

Tujuan kajian ini adalah untuk mengatasi had grid pervasif terutamanya dalam bidang pengesahan kuasa.Kemajuan dalam teknologi tanpa wayar telah mempercepatkan evolusi dari teknologi grid kepada grid pervasif. Ini telah membawa cabaran kepada mekanisme pengesahan kuasa, kerana pengesahan kuasa konvensional tidak menyokong konteks alam sekitar semasa proses pengesahan kuasa. Matlamat penyelidikan ini adalah untuk meningkatkan kebolehpercayaan yang lebih baik bagi rangka kerja pengesahan kuasa untuk berkerja dalam grid pervasif. Daripada kajian ini, mekanisme pengesahan kuasa yang sedia ada mempunyai keterbatasan di mana ia hanya mampu menyokong sifat-sifat statik (yang nilai tidak berubah sepanjang sesi pengesahan kuasa itu) dan juga tidak mempunyai mekanisme untuk mengesahkan semula dan mengenalpasti maklumat persekitaran pengguna. Ini telah menyebabkan penurunan dari segi tahap keselamatan grid, seperti darjah rintangan sistem grid terhadap pengguna yang tidak sah yang sengaja menyalahgunakan prasarana grid. Salah satu penyelesaian untuk mengatasi had ini adalah memperkenalkan kesedaran konteks kepada mekanisme pengesahan kuasa. Dalam tesis ini, satu rangka kerja pengesahan kuasa berasaskan kesedaran konteks telah dicadangkan untuk meningkatkan tahap keselamatan infrastruktur dan perkhidmatan grid pervasif bagi mengetatkan tahap kawalan capaian dengan maklumat konteks sebagai kriteria pengesahan tambahan. Walau bagaimanapun, pemerikssan tambahanakan memanjangkan masa pengesahan kuasa, dan juga meningkatkan toleransi kepada pengguna tak sah semasa perubahan persekitaran. Oleh itu, pengenalan token sesi akses telah dicadangkan untuk mempermudahkan proses dan meningkatkan kecekapan mekanisme pengesahan kuasa.Reka bentuk simulasi dan platform pelaksanaan telah dibincangkan untuk memahami pembangunan model simulasi bagi rangka kerja yang dicadangkan. Pelbagai senario dan eksperimen telah direka dan diuji dengan model simulasi untuk menilai prestasi rangka kerja yang dicadangkan. Keputusan eksperimen menunjukkan bahawa, dengan data kontekstual tambahan, model simulasi berjaya menghasilkan keputusan pengesahan kuasa yang diinginkan dengan berkesan, dengan masa pengambilan konteks 0.0014s untuk konteks persekitaran yang bersaiz kecil. Eksperimen juga menunjukkan bahawa, pelaksanaan token sesi akses telah meningkatkan kecekapan keseluruhan proses pengesahan sebanyak 90% bagi kes ujian dengan permintaan semula pengesahan kuasa. Penemuan penting dari keputusan ini menunjukkan bahawa mekanisme kebenaran itu dapat memutuskan sambungan pengguna yang tidak dibenarkan daripada perkhidmatan itu dengan lebih tepat pada masanya untuk melindungi keselamatan grid. Analisis berskala menunjukkan bahawa rangka kerja dapat menyokong sehingga saiz maksimum sebanyak 423 pengguna aktif dan beroperasi tanpa overhed berlaku. Dapatan kajian dalam tesis ini telah membuktikan bahawa penyelesaian yang dicadangkan itu telah mengatasi had sistem pengesahan kuasa yang sedia ada dengan peningkatan kecekapan dan skala. Kita boleh membuat kesimpulan bahawa rangka kerja yang dicadangkan dapat meningkatkan tahap kebolehparcayaan pengesahan kuasa dalam grid pervasif.

A CONTEXT-AWARE BASED AUTHORIZATION SYSTEM FOR PERVASIVE GRID COMPUTING

ABSTRACT

The purpose of this study was to address the limitation of pervasive grid particularly on the area of authorization. The advance in wireless technologies had accelerated the evolution from grid technologies to pervasive grid. This brings challenges to the authorization mechanism, as the conventional authorization does not support the environment context during the authorizing process. The aim of this research is to enhance the authorization framework for better trustworthiness in order to work in pervasive grid. From the review, the existing authorization mechanisms have limitations of only supporting static attributes (which value is unchanged throughout the authorization session), and also lack of mechanism to re-verify and confirming on user's environment information. This resulted in decrease of grid security level, such as the degrees of the grid system resistance to unauthorized user whom purposely misuse the grid infrastructure. One of the solutions to address this limitation is introducing context-awareness into the authorization mechanism. In this thesis, a context-awareness authorization framework was proposed to improve the security level of pervasive grid infrastructure and services by tightening the access control level with context information as additional authorization criterion. However additional checking will prolong the authorization time, which will also prolong the toleration of unauthorized user during change in environment. Thus the introduction of session access token was also proposed to simplify the process and improve the efficiency of authorization mechanism. Simulation design and implementation platform were discussed to understand the development of simulation model for proposed authorization framework. Various scenarios and experiments were designed and tested with the simulation model to evaluate the performance of proposed framework. The experimental results show that, with additional contextual data, the simulation model was able to produce desired authorization decision result effectively, with the context acquisition time of 0.0014s for small size environment context. The experiment also demonstrated that, implementation of session access token has improved the overall efficiency of authorization process by 90% for test case with re-authorization request. The significance of these results shows that the authorization mechanism was able to disconnect the unauthorized user from the service in timely manner to protect the security of grid. The scalability analysis shows that the framework was able to support maximum size of 423 active users to operate without overhead occurrence. The research findings in this thesis have proved that the proposed solution had overcome the limitation of existing authorization system with improvement in efficiency and scalability. We can conclude that the proposed framework was able to improve the trustworthiness level of authorization in pervasive grid.

CHAPTER 1

INTRODUCTION

1.1 Overview

Grid Computing uses a collective group of geographically distributed computer resources that have connected together to achieve a common goal. In recent years, the advancement of wireless technologies and embedded technologies has accelerated the evolution of grid technologies from conventional grid to pervasive grid computing (also known as ubiquitous computing). Pervasive grid computing enables users to access the grid infrastructure at anytime, anywhere, with any type of devices. As the outcome of the evolution of the grid, authorization security issues had been raised as one of the concerns in access management.

In grid computing, authorization can be defined as the process of determining user access levels in a Virtual Organization (VO). The authorization issues in pervasive grid are mostly referring to the limitation of existing authorization mechanism in handling environmental contexts. The goal of this research is to enhance the authorization mechanism in order to overcome the limitation and enhance the performance of existing solutions. There are some research works that have been done to address the authorization issues in pervasive grid computing. One of the approaches was to adopt context-awareness into the existing authorization mechanism.

Context-awareness refers to the idea where the computer can detect their physical environment and react accordingly. The term “context-awareness” was introduced by (Schilit et al., 1994). It turns out to be an important aspect of pervasive computing, allowing the system to perform tasks based on environmental context. Adopting context-awareness into the authorization process in pervasive grid computing allow the system to make an authorization decision not only based on the user's identity but also the environmental context of the user. This increases the trustworthy value of pervasive grid computing.

However, integrating context-awareness into an existing authorization system has its own challenges due to its inherent heterogeneity and dynamism. This thesis is written to study and find a solution to address the challenges of adopting context-awareness into the authorization process in pervasive grid computing by proposing a context-aware authorization framework for pervasive grid environment. A prototype implementation of proposed authorization framework is presented and the performance of the framework is evaluated.

1.2 Background

Grid computing is introduced with the aim to integrate the distributed resources as a group for solving scientific and industrial complex computational problems (Foster, Kesselman, and Tuecke 2001). It emerged from supercomputer and distributed system technologies, but it is more loosely coupled, heterogeneous, and geographically dispersed compare to the conventional high performance computing system. When a group of users or stakeholders sharing the same computing resources to achieve a collaborative goal, it forms a VO, where a set of rules will be established and follow by the VO to determine who are allowed to share, and the conditions for a valid share of the resources (Foster, Kesselman, and Tuecke 2001).

Due to the nature of sharing resources by wide range of users within a transparent environment, and also the confidentiality of some shared data, security management will become challenging. Protecting the data and privacy of the user and stakeholder require a strong security service. Hence, researcher distinguished a security mechanism to assure only authorized users are permitted to access the grid resources or services, known as authorization mechanisms. Failure in providing secure authorization to the VO will lead to an exposure of user's privacy and confidentiality on the pervasive grid system as a whole. Besides that, the uncontrolled resource access and usage will lead to unfair sharing environment for the VO. The risk of the grid resources misused by unauthorized or even authorized user can be reduced by utilizing authentication and authorization system for access controlling. Hence the authorization process should be seen as an important topic in grid computing and need huge attention from researchers.

The advance of technologies in recent years had led to the evolution from the traditional grid to pervasive grid due to the introduction of wireless devices such as: mobile devices, robots, sensors and context-aware applications as part of the grid resources. In the ubiquitous computing, remote accesses to grid resources via a variety of computing devices are required. Thus, managing and controlling the resource access in these environments had become more challenging. The uncontrolled resource access creates an insecure sharing environment. Upon the introduction of robots, mobile devices, sensors, and context-aware applications as part of the resources in a pervasive grid environment, authorization in the pervasive grid environment is not limited to human user authorization, but also to authorize the heterogeneous infrastructure; ensuring the security and privacy of user’s resources with environmental information awareness. As a result of the increase of requirement on authorization system, the authorization process for pervasive grid computing becomes more challenging in the ubiquitous environment. A number of researches and studies have been conducted in order to enhance the authorization system to be more applicable for the dynamic mobile computing environment. One of the approaches is bringing up the context-awareness in authorization system. This requires an authorization solution that is able to handle the environmental info of the grid.

1.3 Research Problem

Conventional authorization systems are only be able to work with static attributes, for example: roles, group memberships. They are not designed to work with context attributes, such as: location, time, temperature, time or other environmental information. However, this information is not sufficient to make an authorization decision in pervasive grid computing. As the environmental context in pervasive environment may change rapidly, the security status of a user may change from safe to unsafe after the environment changes. In order to maintain the security, context attributes need to be revised from time to time to evaluate the security level of user’s circumference. Thus the context attributes are needed to be considered in an authorization process as the second layer of access management criteria for better security control.

In addition, conventional authorization systems lack of facility for capturing and handling environment context, hence unable to respond towards the changes of environment context. This will result in conventional authorization system to lose their performance in pervasive environment that requires frequent monitoring and spontaneous update on authorization decision, such as decrease of authorization result correctness and decrease of overall trustworthiness of the authorization system. Hence an enhancement on the authorization mechanism is needed to improve the trustworthiness level of the authorization system in the pervasive grid environment.

1.4 Objectives

The main goal of this research is to improve the trustworthiness level of authorization system in pervasive environments. The objectives of the research are:

- To enhance the security process of authorization framework for the pervasive grid environment
- To improve the scalability of authorization framework in pervasive grid computing
- To improve the efficiency of authorization framework in pervasive grid computing

1.5 Importance and Significance of this Research

The proposed framework in this research is beneficial for VO participant who need to work with pervasive grid computing and ubiquitous environment. It allows the VO to utilize wireless technologies and embedded technologies into their grid environment with better security access control. By integrating the context-awareness into the authorization process, the authorization system can make a better decision to control the user access not only based on their identity but also the safety of their environment. These have increased the trustworthiness level of authorization mechanism and ensure the overall security level for pervasive grid infrastructures.

1.6 Scope of the Research

The scope of this research included:

- A study on how to adapt environment context data into the existing authorization mechanism.
- Introducing a method to improve the efficiency of the authorization process
- Develop a simulation model to evaluate the performance of the proposed framework

1.7 Contribution

This research work improved the trustworthiness level of authorization mechanism. The main research contributions included an authorization framework design with enhanced context-awareness so that the proposed authorization framework is more ready for the pervasive environment. A method of using more simple authorization credential, namely “simple session access token” were introduced to simplify the user attribute identification and verification method and in conjunction increase the efficiency of the overall authorization process. This research work also contributed a study on the limitation of the centralized authorization architecture.

1.8 Organization of Thesis

The remainder of this thesis is organized as follows: Chapter 2 presents the literature reviews that were relevant to understand the background of authorization mechanism, authorization in pervasive grid computing, and context-awareness. An introduction of the pervasive grid computing, a study on authorization system including: definition of authorization, models of authorization system and characteristic of the existing authorization system, and the limitation of the grid authorization system and mechanism in pervasive grid were conducted for addressing the research gap in this topic. Also reviews of related work are discussed. Chapter 3 presents the simulation design and implementation work on the proposed framework. The architecture of simulation work, simulation model design, and details of other entity used in the simulation work such as X.509 certificate, proposed session access token, and also the fundamental operation flow of the simulation model are discussed. Chapter 4 presents the simulation scenarios, test cases and results. Analysis and discussions are made based on the simulation result. Chapter 5 concludes the overall research work with a summary and presents the limitation and future work of this research work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents the literatures that are relevant to understand the background and research movement in research work. The first part of this literature study introduces on pervasive grid computing and highlights the authorization concerns in this field towards authorization issues. The following part presents the overview of authorization including the definition, models, and characteristic of authorization system. It explains the term authorization, presentations on the authorization models and mechanisms, and discusses on characteristics of existent authorization systems for better understanding on the authorization. All of these studies contributed to the design of a quality pervasive authorization framework. The next part of the literature study covers the limitation of existing authorization infrastructure. Through the analysis on limitation of the existing system, a set of major requirement for pervasive authorization mechanism were established. Subsequently, an introduction of context-awareness was presented. Finally, the last part of this literature study summarise the related work done by recent researcher on solving the authorization issue in pervasive grid.

2.2 Pervasive Grid Computing

Pervasive grid computing is an evolved version of grid computing, where the grid resources involved new technologies such as embedded devices and ad-hoc short-range wireless networking (Parashar and Pierson, 2010) that forms a continuous interaction between individuals (Vipul and at el., 2003), in other words: mobility of user. Thus, pervasive grid computing has more advantageous in handling the projects that involve seamless human-computer interaction. With the wireless networking, pervasive grid users can access the Virtual Organization (VO) anytime anywhere with various types of devices (Chin et al. 2007). Thus, this sets the pervasive grid apart from conventional grid computing as pervasive grid environment is large, heterogeneous and dynamic, globally combined large numbers of independent computing and communication resources, data storages, and embedded devices.

In Parashar and Pierson (2010) research work, they have mentioned that this advancement had also introduced new challenges to the nature of pervasive grid which cause uncertainty in the system, information and application. They had also drawn out the basic requirements for pervasive grid application, unlike in traditional grid infrastructure, pervasive infrastructure should have the ability to detect and dynamically respond to the changes either to the execution environments, state and requirements, or the overall context of the application, during execution time.

In pervasive grid environment, users are allowed to access the shared data from anytime and anywhere. When a user moves from a location to another new location, it is considered as context changes. This phenomenon happens very rapidly and frequently. The security requirements of a smart space may vary according to the context of the space where some operation or data access might require greater security to be take place. Thus, it is a challenge for the system to consider on how to ensure only user with secure context are authorized to access the resources in such a volatile environment. Pierson (2008) have presented an overview of research effort on pervasive grid particularly on data management side, by reviewing existing solutions and their limitation.

This challenge has been further discussed in Parashar and Pierson (2010) research work, where they state that the challenge of the authorization mechanism in pervasive grid computing was not only to authorize human user, but also to authorize the heterogeneous infrastructure. In this research work, we will focus on how to address this challenge in the authorization process in pervasive grid computing environment.

2.3 Authorization

The term authorization is very common in VO management and has many meanings. In information security and computer security field, authorization is referred as the function of specifying access rights to resources. Chakrabarti (2007, pp. 67-104) define authorization as the process of providing and inspecting the authority of the subject to a specific set of resources. However, the word authorization, authentication, and access control are sometimes mixed up. Some research work has been done to clarify the scope of these terms. According to (Authentication vs. Authorization 2010), authentication is the mechanism to identify users’ identity, whereas authorization is the mechanism to determine the access level of a user. In other words, authentication is in charge of verifying users and provides credentials to users, and authorization is in charge of storing user information, such as: access levels, roles, or permissions and inspecting the authority of a user on particular sets of resource (Chakrabarti, 2007). On the other hand, Tanenbaum and Steen (2002) referred authorization as granting access rights, whereas access control is referred as verifying access rights. In other words, an access control system is also part of an authorization system, where it executes the security restriction issued by policy model in an authorization system.

Authorization system is responsible to filter the user of VO from gaining excessive access that beyond what they deserved to the resources by inspecting their roles and group permission to reduces the risk of misusing grid resources by non VO user or even the internal VO user. Authorization involves three basic entities: (1) Subject: can be a user that able to request access to certain resource or service, or can be a process that acts on behalf of a user who delegated the access rights to it, (2) Resource: a component of the system that provides services or data storage, (3) Authority: an administrative entity that able to issue, validate and revoke the electronic means of proof (Lorch et al, 2004). The main purpose of authorization process is to ensure only authorized user is allowed to access the resource or service in a shared environment. Generally a good authorization infrastructure should have the following ability: (1) limit the access to outsider, (2) a good access control mechanism, and (3) provide resource control to the authenticated and authorized user (Chakrabarti 2007).

2.3.1 Type of Authorization Model

There are two types of authorization mechanisms: (1) push-based mechanisms and (2) pull-based mechanisms. In push-based model, user obtains valid attributes certificates from the certificate generator in advance and push together with service request to the resource for authority checks. (Chakrabarti, 2007). Figure 2.1 illustrates the push based authorization model. Push model have better scalability, because the certificate generator are designed in the way that loosely coupling to the resource access controller. Hence, the assignment of certificates process happens separately from the accession controlling process for the reason of preventing traffic conjunction at resource site.

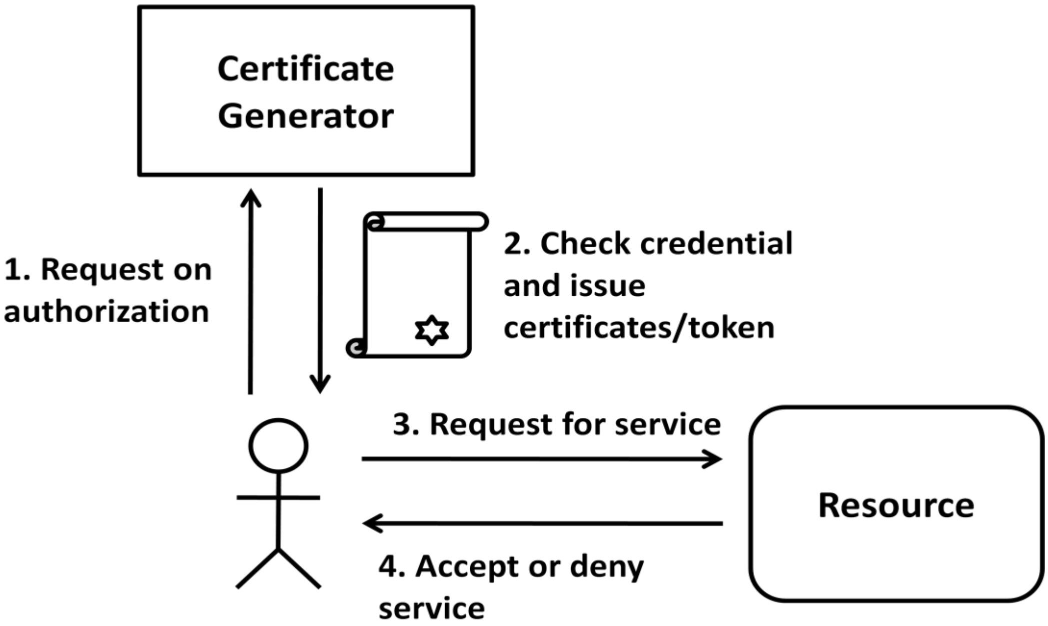
Certificate Generator
1. Request on authorization
2. Check credential and issue certificates/token
3. Request for service
Resource
4. Accept or deny service

Figure 2.1: The Push-Based Authorization Model

In the pull-based model, requests of service are directly send to the resource with minimum credential (Chakrabarti, 2007). The access controller at resources site pulls the user identity from predefined credential entry in a database. Figure 2.2 illustrates the pull based authorization model. Pull-based model have more advantages in user friendliness over push model, because it is designed in such a way that the user does not need to predefine certificates.

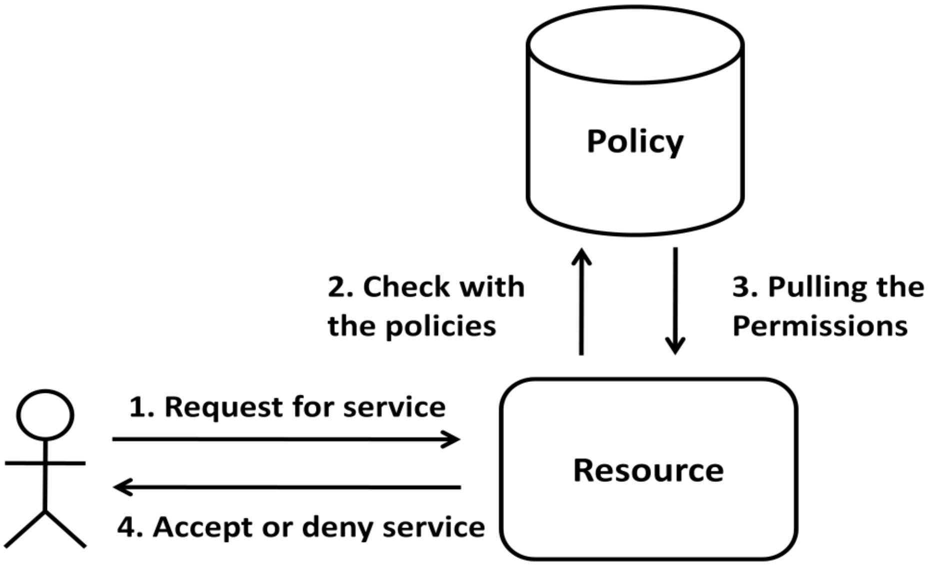
Policy
2. Check with the policies
3. Pulling the Permissions
1. Request for service
Resource
4. Accept or deny service

Figure 2.2: The Pull-Based Authorization Model

2.3.2 Characteristic of Authorization System

In order for the authorization system to support context-aware access control in a pervasive grid, the issues of interoperability, scalability, security precaution, and revocation mechanism, in addition to context-awareness, should be considered. Therefore, review works of several well known conventional authorization system's characteristic are compared and discussed to identify the essential characteristic from existing authorization framework that should be inherited in the design of the proposed authorization framework. In the review work done by Jie and et. al. (2011), they have discussed several typical grid authorization technologies on their authorization model, scalability, security issue, delegation, flexibility and others.

These discussions had derived a list of good design requirement that would be adopted when designing our proposed authorization framework. The pros and cons of the design of model, architecture and mechanism, and their impact of scalability, security, and revocation, and inter-operability were discussed in the following paragraph. Chakrabarti (2007) had also discussed a few of the characteristics of grid authorization system in his chapter of book, which are scalability, security issue, revocation method and interoperability. In this thesis, scalability, security issue, and revocation method and interoperability were discussed, as they have influences on the trustworthiness level of the authorization framework design.

In this thesis, scalability is referring to the maximum size of users or the resources the authorization system can handle without too much of overhead. Since the pervasive grid involved additional types of remote devices such as sensors, tablet and embedded devices, each of them are considered as a resource. Thus, it is expected that the size of resources to be handled by the authorization system will increase, in other words the scalability of the authorization needs to be improved. The type of security precaution techniques and revocation process also play an important role in determining the trustworthiness level of an authorization system design. In this thesis, security precaution is referring to the level of defence of the grid resource towards different malicious attack. When further access of the user might harm the system, revocation mechanism responsible to terminate that user access from the resources to reduce the chances of the system from malfunction, therefore make the system more trustworthy. Interoperability is also important as it determines the easiness of the framework design to allow adaption with different type of authorization system in future.

Therefore, in this thesis, these characteristics are discussed and compared among few popular grid authorization system: *Community Authorization Service (CAS), Virtual Organization Membership Service (VOMS), Enterprise Authorization and Licensing Service (EALS), Akenti, Privilege and Role Management Infrastructure Standards Validation (PERMIS) Project*, and *Gridmap.*

The model and architecture design of an authorization system were one of the factor in influencing scalability (Chakrabarti, 2007). In the existing authorization system such as CAS (Pearlman, Welch and et al, 2002) and VOMS (Alfieri, Cecchini and et al., 2003) where push based model is implemented, they distribute the authorization credential to the users to reduce the trust relationships between the user and the resource providers (Parashar and Pierson 2010). EALS, Akenti (Chadwick and Otenko, 2003) and Gridmap (Foster and Kesselman,1999) implemented pull-based model where the access controller take full responsibility of granting access to the user without requiring pre-defined certificates. PERMIS (Chadwick and Otenko, 2003) can be customized to both pull-based and push-based model. According to Chakrabarti (2007), the separation of the certificate generator from the access controller makes it possible for both operations to happen in parallel. This would avoid traffic conjunction, and thus becomes more scalable than the pull based mechanism alone in terms of user support scalability. However, pull based model are more user friendly than push based model. Therefore, push model is adopted in the proposed authorization framework for pervasive grid that enable to support the expected increment of number of users and resources in the pervasive environment and take advantage of its performance scalability.

CAS, VOMS, and EALS adopted centralized policy database, thus the administrator of these models is only required to update only one place when there are changes of policy, therefore these models have better administrative scalability but are having more risk of single point failure (Chakrabarti 2007). For PERMIS user, only users that are using the centralized main domain are required to get a pre-defined credential before sending access request to the resources. Akenti is customized to work in high performance distributed network environment by adopting a distributed policy database (Liu 2009). When there is the need of policy adjustment in Gridmap, each of the distributed policy need to be updated individually. Thus Gridmap has the highest administrative overhead. Therefore, we can deduce that centralized policy method with the extended feature to scheduling replication of policies is more efficient for the VO environment where policies are not often modified, whereas distributed policy database are recommended for the VO environment with frequently changes of policies.

There are various types of security precaution techniques implemented by different conventional authorization system. In VOMS system, it supports multiple stakeholders, even if one of the database storing a particular stakeholder's certificates us under Denial of Service (DoS) attack, the other resources would be unaffected (Chakrabarti 2007). Akenti and EALS hand out the traffic to several servers to prevent the server from getting suspended during DoS (Chadwick and Otenko, 2003). Gridmap system implemented distributed policies and certificate generator, thus the impact of DoS attack in Gridmap can be neglectable, unless the adversary is attacking a large amount of grid resources simultaneously. Others techniques such as resource level checking and access filtering are also introduced to limit the DoS attacks (Chakrabarti 2007). In order words, it can be deduce that push based model was more prone to DoS attack, whereas pull based model can distribute the request to multiple servers in case in DoS attacks. Thus, security prevention method have to be considered when designing the authorization framework, so that the framework is able to tailor to suits in pervasive environment that might have more malicious attack due to ubiquitous devices and users.

CAS and VOMS have no explicit revocation mechanisms, thus it is possible for the adversary to access the entire resource base on the granted credential. EALS, Akenti and PERMIS have inherited revocation mechanisms to suspend the attacker access by modifying the policies manually. Although Gridmap have inherent revocation but the administrator still need to renew each of the policy in every resource individually (Chakrabarti 2007). Thus, an explicit revocation mechanism is needed in order to suspend the attacker access when malicious attack is detected.

Several standards had been established to define the policy for the ease of inter-operable between different authorization systems. CAS, VOMS and PERMIS uses Security Assertion Markup Language (SAML) Standard as the mark-up language (Chakrabarti 2007). CAS is more compatible than VOMS because it able to work with Web service and Open Grid Services Architecture (OGSA) tools (Chadwick 2003). Akenti implemented Extensible Markup Language (XML) standards in the policy management. EALS are introduced for enterprise usage, thus it has an adapter for most industry products. It implemented eXtensible Access Control Markup Language (XACML) standards for policies management and using SAML standard to exchange authorization credentials (Chakrabarti 2007).

2.3.3 Limitation of Existing Authorization System

The manual interactions such as manual logins, logouts, and file permissions methods that are required in the traditional access control were not satisfying the vision of non-intrusive ubiquitous computing anymore, as the security requirements of a smart space may vary according to the context of the space where some operation might require greater security to be take place, whereas some are not. Thus, the environment contexts of the space need to be taken as part of the security concern (Al-Muhtadi, Ranganathan et al., 2003). Therefore, as a pervasive grid application, one must fulfill the requirements: capable to detect and dynamically response to changes of state and overall context of the grid system during execution environment (Parashar and Pierson, 2010).

However, according to Naqvi and Riguidel (2005), conventional authorization process only focuses on static scenarios involving only the identity of the subject. Another research work done by Zhang and Parashar (2004) points out that, in conventional strategies whereby managing the access permission through only checking of membership listed in an access control list but without considering the context information, is inadequate for pervasive application. In the research work done by Demchenk, Mulmo and at el. (2007), the authors claimed that the existing access control implementations for grid resources are missing of two additional features: authorization session revocation and a configuration management interface which needed to configure multiple trust domains for interactive services. According to Chin et al. (2007), the existing authorization system were not capturing and utilizing environment context attributes, such as location, temperature, time, history, and other context attributes that will change their value from time to time. Those conventional authorization mechanisms are only focused on the entities that verifying the user's identity moreover access request is granted provided that the credential provided by the subject is valid (Chin et al. 2007). From the reviewing of these literature review done by previous researcher, it can be summarized that, conventional grid did not consider the context environment during the authorization process

From the review above, we can deduce that conventional authorization systems were insufficient to authorize the user in a pervasive grid computing environment, mainly because the absence of dynamic attributes during authorization decision, and also lack of re-authorization mechanism to handle the changes of dynamic context. These limitations were due to the lack of capability to capture environment context and also insufficient facility to handling context changes in authorization process. Therefore, these limitations have made the conventional authorization process become insufficient to support in pervasive grid computing. Hence, a number of researches have been done in order to improve the context-awareness of grid authorization infrastructure.

2.4 Context-Awareness

Schilit and Theimer (1994), used the term "context-aware" to illustrate the computing model where the interaction between the user and various mobile and immobile computers are permitted. They classify context-aware systems as a system that able to understand, manage, and react to the surroundings of its physical environment that may interact with it. In this thesis, “context” refers to environment or physical information of the system, such as location of user, time, access history, level of confidence, level of communication channel secrecy and others. This information can be used as input parameter for the authorization system to check the user condition and system environment during authorization decision. It can be used to enhance and tighten the security of access control. ”Context-awareness” refers to the ability of the system to understand, capture, and manage the context information. In ubiquitous computing, context-awareness responsible to handle surrounding environment changes of computer systems. Context-aware system improves user experience by achieving collaboration and integration for ubiquitous devices.

2.4.1 Context-Aware Authorization Mechanism in Pervasive Grid

In pervasive grid, authorization system not only receive static attribute from user certificates, but also received contextual attributes from sensors and robots which are changing dynamically. The introduction of context-aware authorization mechanism enables the authorization decision being made not only base on the user identity but also considering the safety of their environment, which become additional layer of access control checking and improves the overall security level. As the context attributes may dynamically changed, a mechanism to monitor the changes of the environment factor is needed to notify the decision making function for re-authorise the user upon the environment changed (Chin et al. 2007). Since pervasive world is composed of heterogeneous infrastructure, thus the pervasive authorization system must be able to adapt into different situation or scenario and various devices.

Therefore, in order to adapt into Pervasive Grid environment the pervasive authorization system are required to have the mechanism to handle both types of information: user identity and contextual data either parallel or sequentially, and also the mechanism to detect and respond to the changes of context information. These can be done by introducing a Context-Aware Infrastructure that implementing the mechanisms. Figure 2.3 illustrates the overview and relationship between each security infrastructure in a pervasive grid computing.

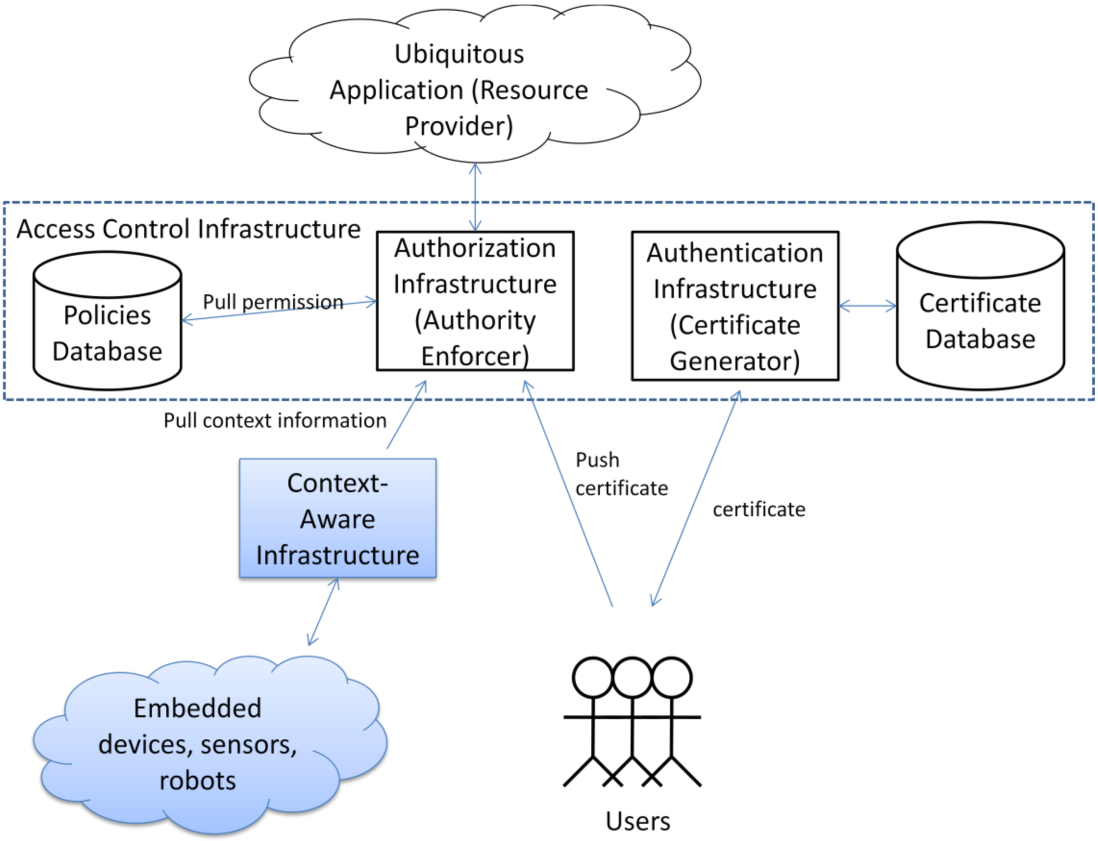
Ubiquitous Application (Resource Provider)
Access Control Infrastructure
Policies Database
Pull permission
Authorization Infrastructure (Authority Enforcer)
Authentication Infrastructure (Certificate Generator)
Certificate Database
Pull context information
Context-Aware Infrastructure
Push certificate
certificate
Embedded devices, sensors, robots
Users

Figure 2.3 Overview of Security Infrastructure in Pervasive Grid Computing

2.5 Related Works

Through the studying of the existing authorization model and the research work being done by previous researchers, the research effort can be categories into two main directions. The first direction of research effort focuses on the enhancing the characteristic such as scalability, security, revocation and interoperability for the authorization system. In the research work done by Pearlman, Welch and et al. (2002), the CAS authorization system are designed to address the scalability, flexibility and expressibility and the need for policy hierarchies in grid authorization system. PERMIS (Chadwick and Otenko, 2003) and VOMS (Alfieri, Cecchini and et al., 2003) focused on the research for information storing, PERMIS kept the Attribute Certificates (AC) in a single AC repository, whereas VOMS distributes the AC's to the users for greater flexibility so that user can customize the level of information about themself to present to resource provider. In the authorization system named Akenti (Chadwick and Otenko, 2003), the system's architecture is designed to provide scalable security services in highly distributed network environments. It provides a way to express and to enforce an access control policy without requiring a central enforcer and administrative authority to have greater scalability. Gridmap (Foster and Kesselman, 1999) emphasizes on the simplicity of the architecture. Although it lacks of scalability, the architecture allows the system to be implemented and adopted into grid infrastructure as simple as possible.

Another effort was more focused on adopting context-awareness into authorization system for supporting pervasive computing. In the research work done by Al-Muhtadi, Ranganathan and et al. (2003), the authors apply the context awareness and automated reasoning into the identification, authentication and access control process of their proposed framework, a context-aware security service named Cerberus. They enhance the security of ubiquitous application by improving the authorization algorithm through introducing confidence value into the policies. However, the interaction between their context infrastructure and authorization infrastructure is not clearly explained. This research work was more focused on enhancing the confidence level without much concern on the timely performance.

Wullems, Looi, and Clark (2004) had proposed an extended RBAC model to provide more flexible activation mechanism for roles, as well as providing role-centric context constraints that allows for simple access control policy instead of complex policy definitions that attempt to bind context data to credentials. The authorization architecture supports GSSAPI-based applications through the use of Kerberos. It supports context-aware authorization using both local and remote security contexts. The impact of size of context on the authorization system performance was not discussed in their research work.

In the research work done by Weili, Junjing, and Xiaobo (2005), they have proposed a formal and extendible context model, which formulate the access control decision based on subject, object, action, context condition and context mask. They claimed that context mask can speed up the access control decision since the decision module was not required to verify the entire context. In their context infrastructure, context information was directly provided instead of getting the context information through the context sensors in the system. If further context information is needed, system will invoke the context sensor adaptor to gather context information.