Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Policy for Context Aware Computing– A Survey

Madhusudanan. J *
Department of CSE, Associate Professor, SMVEC
Pondicherry University, Puducherry, India

Giri Sruthy
Department of CSE, PG Scholar, SMVEC
Pondicherry University, Puducherry, India

Abstract*— Portable devices have become a part of our everyday life, more people are unknowingly participating in a pervasive computing environment. People might engage in many computational devices simultaneously without even the awareness of their existence. The idea of pervasive computing is that almost every device we see today will be capable of communication and function in collaboration with one another in the near future. A security model for pervasive system is proposed that compose the required pervasive security functions to be smart.

Keywords*— Pervasive computing, pervasive security, smart security, security issues, portable devices.

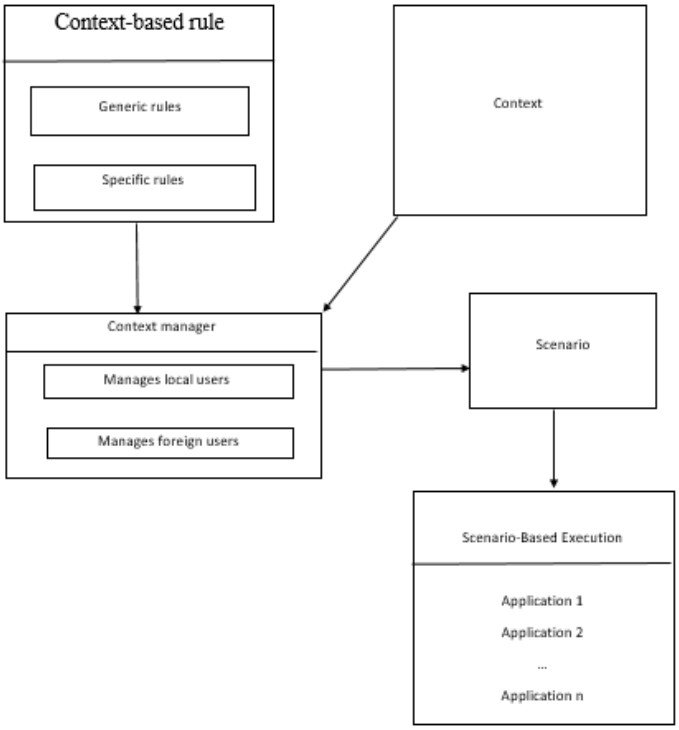
I. INTRODUCTION

Pervasive computing is becoming more popular in everyday life by just inserting chips to some sort of microprocessors in order for people to communicate with the electronic devices. Pervasive and ubiquitous means it is existing everywhere. These can be implemented in the fast growing technological world where computing devices are progressively becoming smaller. The main aim of pervasive computing is that it combines network technologies with wireless computing by embedding the chip in any kind of device where the connectivity is available at anytime and anywhere.

There are three main aspects of context:

1) where you are
2) who you are with
3) What resources are nearby?

Pervasive computing devices are completely connected and constantly available. The goal of researchers working in pervasive computing is to create *smart* products that communicate unobtrusively. The products are connected to the Internet and the data they generate is easily available. The pervasive computing is where a user interacts with a computer which can be of many different forms that includes laptop computers, tablets and also terminals in everyday objects such as washing machine or wrist watch too. The technology that supports this type of computing include internet, advanced middleware, operating system, sensors and microprocessors.



© 2016, IJARCSSE All Rights Reserved

Pervasive Computing Evolution

3 waves of computing

- *First wave* shows the mainframe where one computer and many people uses it.
- *Second wave* shows personal computer where one computer and one person use it.
- *Third wave* shows the ubiquitous computing where one person and many computers work for them.

a) Contribution

In this work, we present a survey of security policy for context aware computing. We start by discussing that security is very important in a context-aware computing, where the user will be provided with certain context aware rules. Later we develop an environment where one can access the devices by specifying the privileges for the users in order to access. The authorized users will be able to access only the devices based on the context rules. Each user will be given access by specifying the users with the access rights. When giving access rights, the unauthorized users will not be allowed to access the system. While building the environment, the users will are controlled and managed by the context managers. The context managers will make the users to access the system based on the pre-defined context rules.

b) Organization

The rest of this work is designed as follows. Section 2 describes the related work. Section 3 describes the vision. Section 4 describes the challenges. Section 5 presents possible directions for future research and section 6 concludes the paper.

II. RELATED WORK

It is especially important when controlling the access of different users. OSGi[1] platform supports the role based access control. In home network environments, OSGi platform plays a major role as the service gateway to access into home appliances. It is important to provide appropriate services as well as security mechanisms to protect confidential or sensitive information and devices. Authentication and authorization is especially important when controlling the access of different users. User authentication is performed using the id/password, user certificate and biometric information such as finger prints. To authorize users, there are several kinds of access control model such as mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC).The main advantage is that designed and implemented an access control method, using delegation model on the OSGi platform. The disadvantage is authorization cannot perform the appropriate access control mechanism for the new service.

UbiCOSM[2] dynamically determines the contexts of mobile proxies by taking into account different types of metadata (user profiles and authorization policies), expressed at a high level of abstraction and cleanly separated from the service logic. the recent proliferation of heterogeneous portable devices and of different technologies for wireless connectivity in home/office environments suggests not only to extend to mobile users/devices the access to traditional Internet services, designed and implemented for the fixed network infrastructure, but also to develop new classes of services that can provide results that depend on the relative position of clients and on the consequent resource visibility (context-aware services).The main advantage is that effective service provisioning over the wireless Internet requires the full visibility and the flexible management of context information. The disadvantage is Runtime conflicts among policies to be enforced, and prototyping solutions based on policy prioritization.

The current work in the area and the trends and challenges to be addressed when designing and developing SOA middleware solutions for different application domains. Some researchers view SOA[3] as a replacement for middleware since application development will not rely on detailed implementation, but will mainly integrate with available components based on SOA. However, even the SOA architecture itself has grown drastically that it resembles very large scale applications and require careful and well planned design and development. As a result, middleware approaches are used to facilitate the design and development of services within SOA. Middleware helps to abstract the distribution and heterogeneity of the underlying computing environment and services available. It also supports the addition of non-functional values such as interoperability, load balancing, scalability, reliability, availability, usability, extensibility, manageability, reusability, services discovery, Quality of Service (QoS) stability, efficiency, automaticity and security. The main advantage is that SOM solutions need to support efficient handling of the heterogeneous resources and functionalities of the distributed applications. The disadvantage is to further enhance the approach, we must have dynamic, adaptive and auto-configurable SOM architectures for effective integration and reuse.

Java object-passing interface (JOPI)[4] class library. It is portable and allows executing programs in parallel across multiple heterogeneous platforms. With the middleware infrastructure, users need not deal with the mechanisms of deploying and loading user classes on heterogeneous system. Requirements such as remote loading and execution, resource management and scheduling, naming, security, group management and communications, and synchronization mechanisms were identified. Furthermore, the middleware infrastructure is designed to satisfy these requirements in a multilayered modular manner, which separates the programming model's specific functionalities from the general runtime support required by any parallel or distributed programming model. The layered approach also allows for easy modifications and updates of the different functions and services at the different layers and provides flexible component-based plug-ins. The main advantage is that the middleware allows the distributed/parallel application developers to build, deploy, monitor, and control their applications, which can be written using the middleware directly. The disadvantage is Additional functions can also be integrated to the infrastructure such as fault tolerance and dynamic load balancing.

© 2016, IJARCSSE All Rights Reserved

In recent years, privacy in ambient systems has become a major issue. Users will have to control their data more and more in the future. Current security systems don't support a strong constraint: policy writers are non-technical users and not security experts. This research area provides techniques to inform and assist non-technical users to write their own authorization policies following the paradigm of Attribute Based Access Control. Ambient intelligence defines the world as flooded by electronic devices and computer. These devices are interconnected, context aware and have a certain degree of intelligence, in order to make our daily environment easier. Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data. People will have to control the access to their information in a complex and moving environment. Thus, they will have to write complex authorization policies themselves. There exist authorization systems that provide both a very expressive policy language and adaptable enforcement architecture like XACML. Decision Support Systems (DSS)[5] is a research area that focuses on informing the decision maker and giving him tools and methods to model and understand the decision and give then point of solution. New trends in DSS design aim at taking into account the context of the user and the decision.

Due to the rapid advancement of communication technologies, the ability to support access control to resources in open and dynamic environments is crucial. Conventional Role-based Access Control (CRBAC)[6] systems evaluate access permissions depending on the identity/role of the users who are requesting access to resources. An access control model with both dynamic associations of user-role and role-permission capabilities is needed. For context-aware access control (CAAC) applications that extends the RBAC model with dynamic attributes defined in an ontology. Our policy framework uses the relevant context information in order to enable user-role assignment, while using purpose-oriented situation information to enable role-permission assignment. Access control is one of the fundamental security mechanisms needed to protect computer resource, verifying whether a user is allowed to carry out a specific action on that resource.

The distributed computing applications represent comprehensive dynamics and the user requirements in them are significant difference, they require dynamic differentiated fine-grained resource access control policies taking context factors into consideration before making access control decisions. The context factors in access control is analyzed classified and formalized from four aspects including platform security context, user trust context, space context and time context. As a static access control strategy, conventional RBAC[7] mechanism is absence of ability of representing dynamics in information system and of ability of associating context states for resources access control. For satisfying requirements of distributed computing systems in access control techniques, it is necessary to enhance the ability of RBAC model to support dynamic resources access control and make it suitable to influence of the changes of resources access context states to system access control policies.

III. VISION

Nowadays, in each and every home the security has become an important issue and it is mainly used for protecting the system from unauthorized users. The system can be made more secure by providing security policies for the users who are trying to access the system. A security policy is a technique used to provide policies set by a manager who is in charge of managing all the access rights of the users. Thus a security policy is used to The main problem arises when more no of users tries to access the system at the same time and this problem can be overcome when the users are being separated based on authorization and authentication policies.

IV. CHALLENGES

From the literature overview, Pervasive computing has to be given more security features as well as security policies in order to maintain the system from being accessed by unauthorized users. The main challenge occur when the users are getting increased by time. The system is where unauthorized users cannot access the system without access rights being set to them. The users are controlled and administered by a context manager who has a database table to manage the users who are trying to access the context aware pervasive system.

V. CONCLUSIONS

Thus the security policy has been explained in my paper and conclude that in the existing work, the security policy is not explained or implemented. The unauthorised users cannot access the system unless they are given access rights to access a particular device in that system This feature enables secured policies that can be used by everyone who is using the devices in the pervasive computing environment.

REFERENCES

[1] Intae Kim, Daesung Lee, Kuinam J. Kim, Junghyun Lee: "Flexible authorization in home network environments", *Journal on Cluster Computing*,vol.15, no.1,2012.

[2] Montanari.R, tibaldi.D, toninelli.A , "A context centric security middleware for service provisioning in pervasive computing", *in proceedings of the 2005 symposium on applications and the internet*, pp.421-429,2005..

[3] Al-jaroodi, j., N. Mohamed, and J. Aziz, "Service oriented middleware: trends and challenges," *in proc. 7th international conference on information technology: new generations (ITNG)*,2010.

[4] Jameela al-jaroodi, nader mohamed, hong jiang and david swanson, "Middleware infrastructure for parallel and distributed programming models in heterogeneous systems", *IEEE transactions on parallel and distributed systems*, vol. 14, no. 11,2003.

© 2016, IJARCSSE All Rights Reserved

[5] Arnaud Oglaza, Romain Laborde, Pascale Zarat´, "Authorization policies: Using Decision Support System for context-aware protection of user's private data", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[6] A. S. M. Kayes, Jun Han and Alan Colman, "A Semantic Policy Framework for Context-Aware Access Control Applications", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications,2013.

[7] Achilleas Achilleos, Kun Yang, Nektarios Georgalas: "Context Modelling and a Context-aware Framework for Pervasive Service Creation: A model-driven approach", *Journal on Pervasive and Mobile Computing*, vol.6, pp.281-296, 2010.

[8] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac: "Internet of Things: Vision, applications and research challenges", *Journal on Ad Hoc Networks*, Elsevier,vol.10,no.7,pp.1497-1516,2012.

[9] Jiehan Zhou, Ekaterina Gilman, Juha Palola,Jukka Riekki, Mika Ylianttila, Junzhao Sun: " Context-aware pervasive service composition and its implementation", *Journal on Personal and Ubiquitous Computing*, *Elsevier,v*ol.15, 2011.

[10] Wei-Wei Ni er, Jin-Wang Zheng, and Zhi-Hong Chong: "HilAnchor: Location Privacy Protection in the Presence of Users' Preferences", *Journal Of Computer Science And Technology*,vol.27,pp.413-427,2012.

[11] Sheng-Tzong Cheng, Chi-Hsuan Wang: "An Adaptive Scenario-Based Reasoning System Across Smart Houses", *Journal on Wireless Personal Communications*,vol.64,2010.

© 2016, IJARCSSE All Rights Reserved