ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 3 (July - Sept. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Context-Aware Architecture for User Access Control

[I]P. Priya, [II]P. Joseph Charles, [III]Dr.S. Britto Ramesh Kumar
[I]M.Phil Scholar, [II]Assistant Professor, [III]Research Advisor
[I,III]Dept. of computer science, St.Joseph's college, Trichy, Tamilnadu, India.
[II]Dept. of Information Technology, St.Joseph's college, Trichy, Tamilnadu, India.

Abstract
Web Service has been widely used in the field of distributed application system. But the security issue of the Web Service has often been considered as a crucial barrier to its application in many fields that conducts sensitive information. The proposed system presents a context-aware architecture for user access control model (CAUAC). Unlike traditional systems, in this access control has been explored and access decisions may depend on the context in which requests are made. It is illustrated and explained how the well developed notion of roles can be used to capture security relevant context of the environment in which access requests are made. By introducing the environment roles, a novel access control framework that incorporates a context-based access control it creates. Moreover this architecture is presented to support security policies that make use of environment roles to control access to resources. Furthermore, it outlines the configuration mechanism need to apply the model to the Web services environment, and describes the implementation architecture for the system.

Keywords
Context-Aware Web Services, RBAC, Security Issues

I. Introduction

A web service is regarded as a software application designed mainly to provide support for an interoperable machine-to-machine communication through Internet using XML- based standards like Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and Universal Description Discovery and Integration (UDDI) which together provide a service description, discovery and messaging framework for Web Services applications. Web Services are self-contained, modular, distributed, dynamic applications that can be described, published, located, or invoked over the network to create products, processes, and supply chains. These applications can be local, distributed, or Web-based. Web services are built on top of open standards such as TCP/IP, HTTP, Java, HTML, and XML.

Context is defined as "any information which is used in characterizing the current condition of any object or entity". In a much broader perspective, a context is being termed as "some information which can be utilized to identify the present condition of any entity". A system is considered to be context-aware if it utilizes the context in an effort to provide the appropriate information or service to the user where appropriate and significant information depends upon the requirement and need of the user. In real time, Context referred as location, time, temperature, noise, band width of communication, connectivity of network etc.

Context can be characterized into two types. First is the Enumeration based context and other is Role based context. Enumeration based context is classified as computing context, user context, physical context and temporal context. Computing Context referred as network connectivity, communication cost and bandwidth, User Context referred as user profiles, location, Physical Context referred as lighting, noise level, temperature, Time Context referred as time of day, season of the year and month. Role based context consists of active context and passive context. Active Context means application uses contextual information to adapt its own functionalities (static context), Passive Context means application uses contextual information is not important but boost up the user to realize the situation (dynamic context).

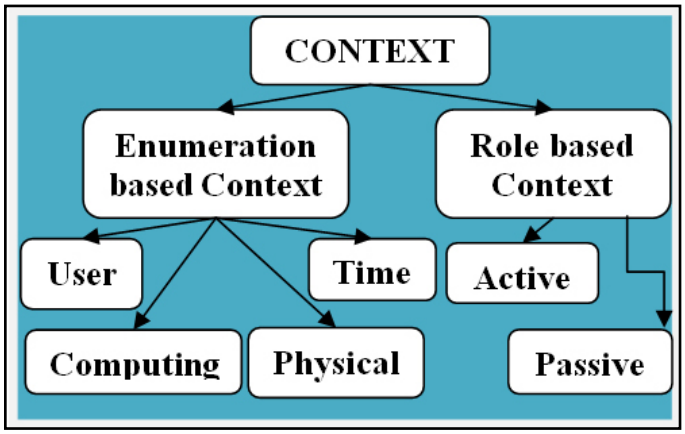

Fig. 1.1: Types of Context

Applications that uses context, whether on a desktop or in a mobile or ubiquitous computing environment are called context-aware. "Context-aware computing" as "software that examines and reacts to an individual's changing context". It means aware of its user's state and surroundings and help to adapt its behaviour. Context-Aware computing is need for essentially required context in Ubiquitous computing environment. Ubiquitous computing has given users the expectation that they can access whatever, whenever and wherever information and services they require. The computers being used in such a wide variety of situations, interesting new problems arise, and the need for context is clear: users are trying to obtain different information from the same services or systems in different situations.

A context aware system is recognized as "system which uses any context information previous to, or in the duration of, service stipulations", whereas the main goal of this system is to track and identify the users. Context aware systems are different from traditional systems as provide unique features such as heterogeneity, high complexity and artificial intelligence. Since the parameters that constitute a context aware system, such as location and time of the day are rapidly changing.

Security has become the key issue in the field of context-aware web services technology. As a result, web service security needs to have more concern for the major security issues such as

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

authentication means process of verifying authenticity (human user's id and password) of the user to access a system. The result of authentication is a set of credentials, which describes the attributes (identity, role, group and clearance) that may be associated with the authenticated principal, authorization means process of ensuring that only the authorized user accesses the system, access control means process of giving permission or access to authenticate and real users to utilize the system facilities. The Role-Based Access Control (RBAC) models permit the grouping of a set of permissions related to a position in an organization, rather than the person assigned to the permission., integrity means process of ensuring that the data received is the same as the data sent and non-repudiation means process of ensuring that the sender/ recipient of a message cannot later deny after having sent/received the message.

This system provided a simple and effective formalization of novel concepts that have to be supported for enforcing the new access control paradigm needed in context based web services. This concept applies the CAUAC in Institution Service System. In this system variety of services are available to the user (student, staff). This secure architecture for context-aware is intended to provide services using web-enabled devices and itself establishes a communication between the web user and the service provider using SOAP messages. This architecture not only deals with the secure transmission of data but also permits only the authorized users to make use of the academic-related web services.

II. Related works

George et al. [1] mentioned the growth in the number of users and geographic coverage, enforcing of access control policy to context-aware enabled wireless networks which maintaining the security and Quality of Service (QoS). This research work compares the existing frameworks confab, Uniform Access Control (UAC), General Role Based Access Control (GRBAC), Cerberus and Kerberos. It intended a new framework named SECCON (Security Context) and discuss context graph to implement the role based access control services to context-aware facilitated wireless networks. It will increase the cleverness in handling the wireless device. This research work is to provide better security control mechanism to access data from business organizations database using context graph. This context graph is not found in existing frameworks and it achieves crucial security features like authentication, access control, privacy and authorization. In this the context modeling with wireless sensor devices is not strengthened.

Shade et al. [2] describes web service security issues in distributed environment. Web Service control the ubiquity of the internet to link applications, systems and resources within and among enterprises to enable stimulating, new business processes and relationship with clients, partners and providers around the world. It allows access to data that has been prior to protect within corporate networks and accessible only via specialized software. This work discusses a security tendency of web service and a typical web service security implementation. It demonstrates the new and existing security mechanism for securing web services at different security tiers and it presents general security framework of web service such as Authentication, Access Control, Authorization and Confidentially, Availability, Integrity of data.

Liu Hong-yue et al. [3] investigates the impact and functions of context factors in access control policy decision and proposes a context-aware fine-grained access control policy and method. The context factors in access control is analyzed, classified and formalized from four characteristic such as platform security context, user trust context, space context and time context. The traditional RBAC is a user-centred, static resource access control and does not take into context factors. So it may be not suitable for distributed computing applications. To achieve dynamic fine-grained resource access control, the entities and relations in RBAC model are redefined and formalized using context constraints. This research works consider only some of the context constraints to grant the permission for dynamic access in context-aware systems.

Zhao et al. [4] propose trust management architecture for web services. This architecture provides basis for dependency and consistency analysis for trust management tasks such as locating, evaluating, and consuming of trust relationships. Since the primary focus of this architecture is to provide trust management solution for web services, the other security issues such as message confidentiality and data integrity have not been addressed and it limits the wide scope of the research.

Sangkeum Lee et al. [5] studied the history of context-aware systems and existing systems related to this work. Technical issues are derived by realizing context-aware services and proposed seven context-aware service scenarios and their related issues. Context-aware system is responsible for several tasks: context data representation, collecting and managing context data, service matching and so on.

Additionally, It requires examining what the architecture style of each system is (e.g., Peer-to-Peer or Centralized Server). In context-aware system, context information can be represented in any one of the models such as Simple data model (e.g., attribute-value tuple), Complex hierarchical (e.g., object-oriented model or graph model) or Ontological data model). Earlier systems are usually domain-specific application systems that can support various kinds of context such as location but later systems use specific types of context are usually general purpose context-aware system. The research areas in context-aware systems are architectural style, performance and scalability, historical context data and user behaviour and privacy protection of data. In this research work, the concept has not been focused in-depth in the system.

Shang et al. [6] intended a context based dynamic role based access control model (CDACM) for web service. Web service is a new service-oriented computing concepts which creates the unique security challenges because it's inherent heterogeneity and highly dynamic in environment. In traditional RBAC model cannot meet the dynamic and context sensitivity features. This research model grants and adapts permissions to users based on a set of contextual information collected from environment of the system and users. The features of CDACM are independence and expansibility, suitable for web service security requirement, support for security control principles having least privilege and separation of duty principle. It enhances the adaptability of web service access control mechanism by using Context constraints and improves the efficiency of security strategy implementation by defining permission hierarchies. Using two-level access control mechanism consisting of service level access control and service attribute level, the access control granularity will be suitable to application features of web service. This research work focused only two access control mechanism which is the drawback and there are many other mechanism can also used in the application.

Having studied on existing models, architectures and frameworks,

there are some limitations and security breaches were identified. There is a demand for designing a new architecture in order to solve the above mentioned limitation and drawbacks.

III. Proposed Architecture

This chapter presents and discusses the security architecture for context-aware web services based on user access control developed for the credentials authentication, authorizations, access control, integrity, Non-Repudiation between the Context Consumer and Context Owner.

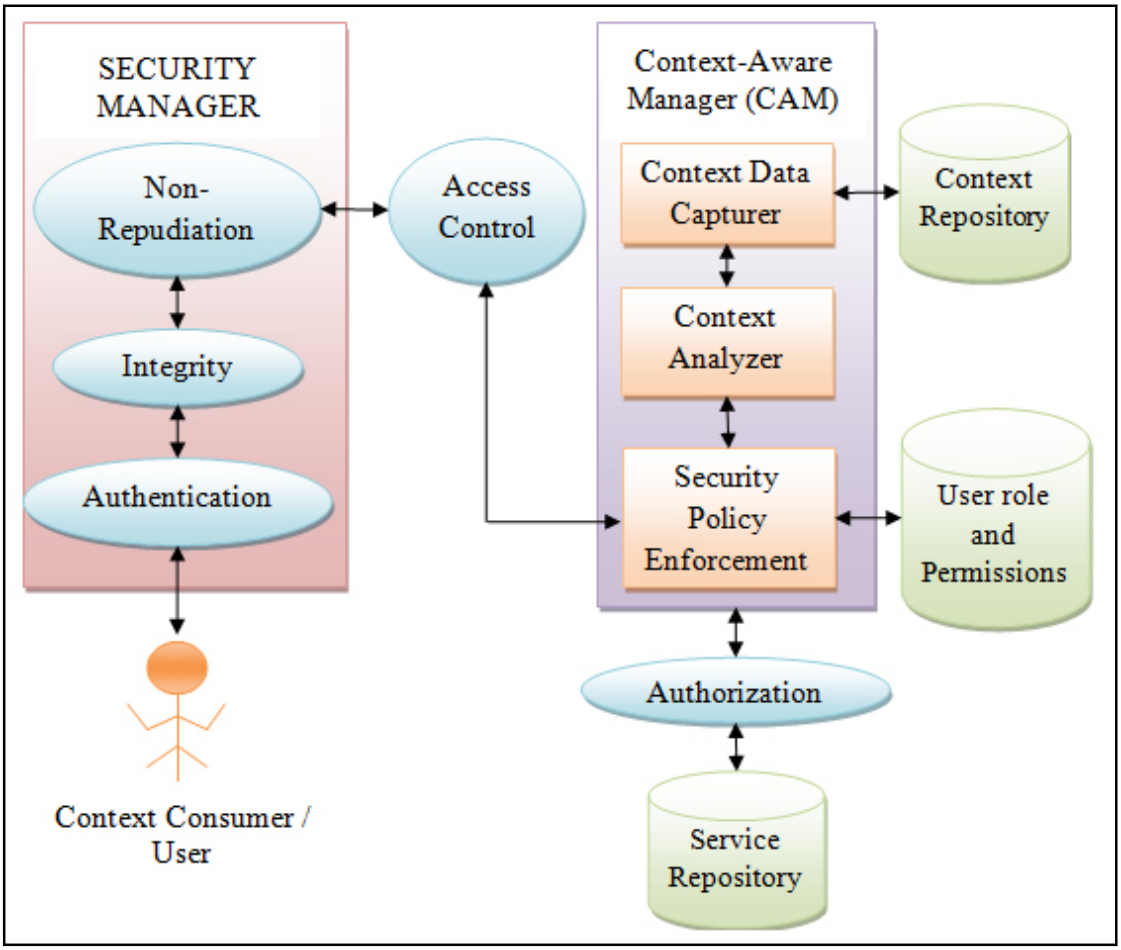

Fig. 3.1: CAUAC – Context Aware Architecture for User Access Control

It explains the secure transmission of the context information between the requestor (client) and the provider (server) with the security entities (attributes) and user role which is given by the user in the registration process. Security is a key area to be addressed for delivering integrated, interoperable solutions under context-aware web services architecture. There have been many technologies that focus on building blocks and specific aspects of a broad range of security issues. In the proposed system mainly focus on effective access control and trust-based models for context-aware web services environment. The proposed architecture has the following modules as, Security Manager, Context Data Capturer, Context Analyzer and Security Policy Enforcement. Context consumer (User) should register to the Context broker (Registry) to have a context view of the services available or not and adapt to the data flow, services and the interfaces of the user devices. Context consumer provides a mechanism for user to interact with application deployed in the web server and if acquire and validate data entered by the user. The Context Consumers describes what data should be captured. Security Manager Component drive security processes to provide secure user interface for authentication, authorization, Integrity, non-repudiation, etc. and offer access control to Security Policy Enforcement component.

First, the User in the system is authenticated and then the proper access control is determined by transferring the control into the Context Management component. After implementing the necessary security policies, the user is authorized to access the Service Repository. User roles and permissions Repository, services repository and Context Repository are the three data stores used in this architecture. The user roles and permissions data store is used for the Security Policy Enforcement component and Context Data repository data store is used for Context Data Capturer component.

Context Data Repository contains all the data about the user and the security properties. When the user requests a service the web server refers Context Data Repository to check, whether the user is registered or not. Context Data Capturer, it filters the user data from the Context Policy Repository based on the role. To reduce the searching time it filters the data according to the request.

The Context Analyzer gets the request from the service requestor and matches the request information with the data in the Context Data Capturer. It aggregates the data and request information and sends the services to the Security Policy Enforcement. It has

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

rights to make decision whether the services can provide to the Service Requestor or not. If the service can provide, it will confirm the access rights to the service then it provides to the Service Requestor. Finally Service Repository is the data store which contains all the authorized services. From the Service Repository the service is forward to the user.

During the registration process all the data about the user are collected and stored in the user role and permission repository. It maintain the user roles and the right permissions to validate the user, who send the request for the web services and it confirm whether the user have the rights to use the services or not and it check the access rights. For implementing authorization and access control, this framework uses the initial of RBAC. This project aimed at a user preferences based on role, the access control language for context-aware web service environments.

IV. Conclusion

This proposed context aware access control architecture for secure web service has extended traditional role-based access control to include the concept of an environment role. It focuses on solving the problem of accessing dynamic context services and using environment roles for user-aware web in a context aware environment. This proposed architecture is mainly focus on the security requirements in context-aware service on the web. Using this some access control mechanisms are created on the basis of the services available and that mechanisms are taken in account during the services requestor login. It validates the user preferences based on the user role and it's the part of key to the actual data. The research shows how the well developed concept of a role can be used to capture security relevant context of the environment in which access requests are made. The resulting access control is highly versatile, yet the underlying constructs (roles) remain consistent with traditional RBAC. This work can be used to provide authorization and role-based access control policies to context-aware web services. Presently, the technological world is rapidly developing towards Context-Aware web services for easy and free access to information while the users are looking for academic related vital information and valuable data.

V. Future Enhancement

As a future scope it will provide mathematical and computational analysis to improve the security mechanisms. It also enforces in the mobile environment and access control mechanism develops to maintain the trust. Another important future scope is to develop a strong platform security environment against Web services malware attacks while deploying most sensitive academic-related applications. Most issues have reported that today's platform security does not prevent security issues related to the third-party applications.

References

[1] *Dr. D. I. George Amalarethinam and V. Jude Nirmal, "SECCON: A Framework for Applying Access Control Policies in Context-Aware Wireless Network", World Congress on Computing and Communication Technologies, 2014.*

[2] *Kuyoro Shade O, Ibikunle Frank, Awodele O and Okolie Samuel O, "Security Issues in Web Services", IJCSNS International Journal of Computer Science and Network Security, Vol .12 No.1, January 2012.*

[3] *Liu Hong-yue, Deng Miao-lei and Yang Wei-dong, "A Context-Aware Fine-Grained Access Control Model", International Conference on Computer Science and Service System, 2012.*

[4] *Weiliang Zhao and Vijay Varadharajan, "Trust Management for Web Services", Department of Computing Macquarie University, NSW 2109, Australia, IEEE 2008.*

[5] *Sangkeun Lee, Sungchan Park and Sang-goo Lee, "A Study on Issues in Context-Aware Systems Based on a Survey and Service Scenarios", Ministry of Knowledge Economy, Korea, under the Information Technology Research Center by Institute of Information Technology Advancement, 2008.*

[6] *Chaowang Shang, Zongkai Yang, Qingtang Liu and Chengling Zhao, "A Context Based Dynamic Access Control Model for Web Service", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008.*

[7] *Chun-Dong Wang, Ting Li and Li-Chun Feng, "Context-aware Environment Role Based Access Control Model for Web Services", School of Computer Science and Technology, Tianjin University of Technology, Tianjin, IEEE 2008.*

[8] *Kenya Nishiki and Erika Tanaka, "Authentication and Access Control Agent Framework for Context-Aware Services", Symposium on Applications and the Internet Workshops (SAINT-W), IEEE 2005.*

[9] *Saad Almutairi, Hamza Aldabbas and Ala-Samaha, "Review on the Security Related Issues in Context Aware Systems", International Journal of Wireless & Mobile Networks (IJWMN) Vol.4, No. 3, June-2012.*