International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Security Issues in Context-Aware System

[I]W.M.Vinitha Rajakumari,[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 Services platform provides the functionality to build and interact with distributed application by sending eXtensible Markup Language (XML) message.But security management is a difficult work of balancing security and usability. This paper present a context-aware system for user access model. Context-aware computing system successfully undertaking by sensor data. The main objective of the context aware system is to find and identify the client. To distributing personal information between different devices need privacy support. By introducing new access control model for accessing resource is needed. This paper proposes an overview of the context-aware access control.*

Keywords: Context-aware,Security,Access Control

1. Introduction

Web Services framework is an Xml based distributed service component system, Such as SOAP, WSDL and UDDI. It supports machine-to-machine interaction over the Network. Webservices has three major operations. Publishing: Making a web service available, Finding: Locating web services, Binding: Accessing web service. It allowed different applications from different sources to interact with each other without time consuming and custom coding.Web Service security adds important transparency to SOAP processing. Depending upon increasing size of the message via wire it plays significant role in web security. Due to its open access, HTTP,SOAP implemented by Webservices add a new set of requirements. That are Authentication,Authorization(Access Control) Privacy,Integrity. This paper focuses on access control in context-aware. The outward aspect of context is measured by hardware sensors such as Location, light, movement,touch, air pressure, sound.

Then internal context is identify by the user. It represent by displaying user interactions such as user's expectation,business process and user psychological state.Compare to internal attributes external attributes are easy to measure the sensors.Three entities can be differentiated in context-aware system they are places,people and things. Access Control is nothing but giving authorization to user when accessing information from distributed applications. The term Context refers as Some information which can be utilized to identify the present condition of any entity.[1]

A system is context-aware of it can discover and utilize context to adapt its behaviour based on the current situation. Context may provide variety of resources.It brings various security services. ie)Authentication-This is a primary process of checking the identity of existing unit.Each and every node in a system having authentication technique to access the network, simply, it checks whether the user are eligible and trustworthy to access the each and every node in context-aware system.This authentication will support only the valid user can access the system. Meantime there is no need to connect the user with application identify for a long time.Privacy-Privacy refers preventing the identity and the location of the node from being disclosed to any other entities.

Nodes consists of location information and data. Confidentiality refers keeping the privacy of data from unwanted users. All the nodes in the system must secure the information while interacting. Access Control: The name itself refers "Access Control" is giving permission to genuine users to utilise the system. If there is no valid authentic, it must reject the user from accessing the system. And also it provides some restriction from each other accessing their private information. There are many techniques that can be used for access control such as Discretionary Access Control (DAC),Mandatory AccessControl (MAC) and Role based Accessed control (RBAC). Data Integrity: During transaction, data should be consistent between users in context

aware system.Data should not be loss or changed by unauthorized person. This will be helpful in military, banking and aircraft control system. Corrupted or modified data would be damaged. Main aim of this data integrity is giving assurance about the data and it does not accessed or modify an invalid user. Insimply, users resources is not allocated or handover to the unauthorised user.
This paper proposes fully access control security while accessing distributed applications.

2. Review of Literature

Alexander smirnov et al.[1]describes a model of context-aware access controlfor smart system based on smart space technology."Smart space" is nothing but integrating of devices that can distribute its resources. It is easy to granting permission to access information from smart space in earlier classical access control model such as DAC,MAC, RBAC.Discretionary access control, Mandatory Access control, Role-based Access control. So that they illustrated virtualization mechanism which is virtual private smart space used by two participants these should be authenticated.After interaction of authenticated participants the space is automatically destroyed. Information exchange in the smart space is implemented via HTTP using a uniform Resource identifier.[7]So that they developed a new access control model which is a combination of role based and attribute based access control(ABAC)model. Then smart space will give authorization to to user to access the information by generating public and private key(RSA algorithm) Generally smart spaces don't have any restrictions while information sharing. But it should protected when information are private. Advantage of this model is human readable rules are used and computation resources used by (ACB)This research work focus only some of the context constraints to grant the permission for smart space in context-aware system.

Priya et al.[2]describes a context-aware architecture for user control access model.This research work fully based on security relevant context,which access request are made. It illustrated context-aware user access control in Institution service Management. This architecture provides various services to staff and students using web enabled devices and interacting between users and service provider by a SOAP message. It not only concerned with security but also it provides information to only the authorized users. In this paper CAUAC architecture consisting of security manager, context Data capture, context analyser and security policy enforcement modules are explained clearly. It gives solution for using dynamic context services in context aware environment. Though its extended by RBAC. This mechanism is used to capture security related context of the environment by using request to the server. In this research work, it would be better if it explains in-depth in alone user access control in context aware environment.

A.S.M.Kayes et al.[3]illustrated a new purpose oriented situation-aware access control(PO-SAAC)software services. This model specifies purpose oriented situations and its related to situation-specific access control policies. It initiate a primary idea of the situation and guiding principle for situation access control,and also this paper describes ontology-based development platform,with new technologies OWL & SWRL. It identifies the simple information from environment to know about the situation. Using PO-SAAC framework user can have different access permission to information resources and software services depending upon the purpose-oriented situation [ref] compared with old context-aware access control experimental results gives good performance. Main advantage of this model is mapping between user and role is many-to-many relationship. This project is fail to explain assigning user-role and it management problem.

Bing liu et al.[4] Illustrated a relationship based federated access control model for EPC Discovery service. This paper mainly focuses on interdependent security threat under EPCDS network context. The purpose of EPCDS is

- Distributing information
- Retrieving the data
- Security and privacy of data

Their framework and experiments are supposed to solve a interdependent.Security problem via relationship based access control. Interdependent security refers that data are retrieving from each independent data repository. And also combined with EPC Discovery services it eliminates redundancy.In addition to that it provides safe mode and gives solution under context Environment.
This paper provides

- Mutual authentication
- Decision Making
- Security rules

- Protecting its own data

And another main advantage of this paper (FAC) is to solve aggregation rules based decision aggregation model to evaluate all the independent decisions. In this federated access control model scalability should be improved.

Bilal shebaro et al.[5]illustrated context based Access control system for mobile devices. This paper describes about personalized report of Android OS using Context-based access control policies. Based on the user context limitations, it will define accessing particular data(or) resource. By using a new context-aware mechanism. This paper discriminate linking sub areas with same location by using GPS,Celltowers,Wi-Fi.CBAC mechanism for Android system that allows smart phones user to set configuration policies over their application usage of device resources and services at diff context[ref] They introduced new policy restriction that are connected with context and it is configured by device user.One of the most advantage of this paper is user can define context according to Location and time. Location is defined by Wi-Fi access points and its corresponding signal strength is used to differentiate nearby sub-area within same work space. Similarly it will be followed when a mobile device connects to their network, network administrator of organisation investigate application permission listed at installation time. This approach prevents malicious application access to resource of their network.

SimsonGansel et al.[6]illustrated a context-aware access control model for safety criticalautomative HMI system. A context can be derived from vehicle sensor or specific state of application ie) Speed,location,time,selected menu. This paper proposes that access control model provides access control to display areas where access decision depends upon the application and changes of context. Depends upon current context it permits to access display areas to application.Due to context of car and application restriction are there to access the display.Access is granted only by context specified in the constrained-permission matches with context of car ad application. This concept is used to prevent intended or unintended presentation of driver-distracting when vehicle is in motion. Proof and implementation of this paper shows automotive safeties while accessing the car. This research work considers only some of the context constraints to grant the permission for dynamic access in context-aware system.

3.Disscussion about Security Issues

Author(s)	*Title of the paper*	*Advantages*	*Future Work*
Alexander smirnov et al.	Context-aware access control model for privacy support in Mobile-Based Assisted Living	Provides authorization and privacy in mobile-based assisted living using smart space technology	Nil
Priya et al.	Context-Aware architecture for User Access Control	CAUAC in Institution Service System	It will focus on mobile environment and built a security to prevent malware attacks while accessing academic-related application
A.S.M. Kayeset al.	An ontological framework for situation-aware access control of software services	By using PO-SAAC framework & situation aware access control application to accessing health care domain	To investigate context-aware user-role assignment and its related management issues. Focus on scalability in mobile computing and Plan to apply PO-SAAC framework to real world.
Bing Liu et al.	Relationship-based federated access control model for EPC Discovery Service	Solving interdependent security Issues while accessing information by Federated access control mechanism	To develop the Scalability in EPC Discovery Service
Bilal shebaro et al.	Context based Acccess control systems for Mobile Devices	Access policy in modified version of android OS	Plan to enhance modified version of OS to give network administrators of organisation when a mobile device connects to network
SimsonGansel et al.	Context-Aware Access Control in Novel Automative HMI Systems	Access control mode for safety-critical automotive HMI Systems.	Using automotive HMI system will optimise the graphics forwarding between virtual machines and to add a Virtualized Android VM in future.

4. Conclusion

So far, from this research paper one of the major issues in context aware web service is Access Control. Accessing the information by authorized user only leads to safe and privacy communication. This paper describes various techniques used in Context-aware access control. Usage of context makes the model more flexible and appropriate for systems. Some information in real applications can be private and should be shared in a secure way.For this purpose, a context based access control model has been developed.

References

[1] Alexander smirnov and Alexey kashevnik , "2010 Mathememtatic subject classificataion " J. Intell. Syst.2015.pp 333-342.

[2]Priya.P and Joseph Charles.P, "Context-Aware Architecture for User Access Control", International Journal of Advanced Research in Computer Science & Technology 2014, Vol.02.

[3] Kayes A.S.M. and Jun Han, " An ontological framework for situation-aware access control of software services" Journal information systems2015 pp:253-277

[4] Bing Liu and chao-Hsienchu "Relationship-based federated access control model for EPC Discovery Service" Journal Computers and security 2015 pp:251-270

[5] Bilal Shebaro and UyindamolaOluwatimi "Context based Access Control Systems for Mobile Devices" IEEE Transactions on Dependable & Secure Computing 2013

[6] SimsonGansel and Stephen Schnitzer," Context-Aware Acccess control in Novel Automative HMI Systems", Springer International publishing Switzerland 2015,pp:118-138

[7] T.Berners-Lee R.Fielding and L.Masinter,RFC 3986-Uniform Resource Identifier(URI) 2014.