A Design of Authentication and Access Control Model for Remote Access using GSM Technologies

S.Pandikumar
Department of Computer Science,
Thiagarajar College, India.

S.Ambethkar
Department of Computer Science,
Madurai Kamaraj University College, India.

ABSTRACT

The GSM technologies plays vital role in pervasive computing environments. The open and dynamic nature of the pervasive computing environment allows entities to join and leave frequently. This causes a large number of autonomous entities to interact in an ad-hoc manner, raising concerns as to the trustworthiness of the service providers. Thus service providers are not willing to share their resources to the anonymous users for fear of a potential security violation. To handle the issue of anonymous resource access, a policy based trust management system must grant user access of resources and information based on trustworthiness rather than the conventional technique map access rights authorization. In this paper, we have developed a new model of GSM-SMS based user authentication and policy based resource access, which will guarantee that service providers can securely share an unlimited number of resources to remote access. This framework provides mechanism to administrator to create policy and grant session based access permission to trusted users. The users can access information and resources based on the access policies and session policies through their mobile phone by sending SMS. This is a low cost and high performance model for preserving access control and resource access in pervasive computing environment.

Keywords: GSM, SMS, Access Control, Remote Access, Remote Authentication, Resource Sharing, AT Commands, Pervasive Computing, Wireless.

1. INTRODUCTION

Pervasive computing aims to simplify day-to-day life by providing mobile users with the means to carry out personal and business tasks via portable and embedded devices [7]. These tasks range from the simple–switching on the lights in a conference room, checking e-mail, and organizing meetings– to the more complex–booking airline tickets, buying and selling stock, or managing bank accounts [7]. Pervasive computing applications need the knowledge of surrounding physical spaces to provide services which require security policies to use contextual information. For instance, access to a resource may be contingent upon trust of the user and time of day. This contextual information can be used to infer the activities of the user and cause a privacy breach. Contextual information must, therefore, be protected by security and privacy policies [7].

Several researchers have focused on develop dynamic access control policies, and more specifically on event and location context [8, 9, 10, 11]. My research is satisfy all the existence and propose a generic, high secured and location free access model using GSM technologies.

Wireless technologies are the backbone of pervasive computing environment, among wireless technologies; GSM is a cost effective, generic, wide covered and efficient technology.

This paper proposes a novel access control model uses GSM-SMS technology to interact among smart devices like mobile phones, PDA and computers. The users can share and access remote resources through SMS in pervasive computing environment. The user need not be physically present in the computing environment; they can access data and devices from anywhere in the world. This model does not require internet connection; instead it uses normal short message service to communicate data between devices. This kind of SMS is called special SMS. It has different message structure which is special SMS start or end that with special characters such that '#' or '%' and uses different syntaxes [2].

This paper provides session based remote access. This access control model specifies the access policies and session policies of the users and admin. The user can share and access the resources based on trust policies. These policies are maintained in the local system and the admin can edit or update these policies through or SMS and in person. This proposed model supports only single tier architecture.

The scope of this paper is

- ✓ The major contribution to secured service sharing solution for the open and dynamic pervasive environment [1].
- ✓ The user can use GSM-SMS to access computing devices from anywhere in the world
- ✓ The trust based access model attempts to identify malicious users and weeds out using trust measures [1].

2. ARCHITECTURE

The trusted users can access computing devices through GSM technologies from anywhere in the world. In this model the user cannot operate the devices directly, instead they have to send commands through structured SMS to the remote computer and the remote computer will respond to the commands. The remote computer connects with dedicated GSM module for receiving user/admin commands. This GSM module is logically connected and monitored by control software. The control software creates interface between user/admin, GSM module, local resources and peripherals (see Figure 1). When the user/admin sends SMS (commands) to GSM module (which is connected with remote computer) the interface software reads the new incoming SMS and performs some validation to check whether its special SMS or ordinary SMS. If it's a valid SMS then this SMS will be parsed and will execute a user/admin commands in the computing environment and reply acknowledgement.

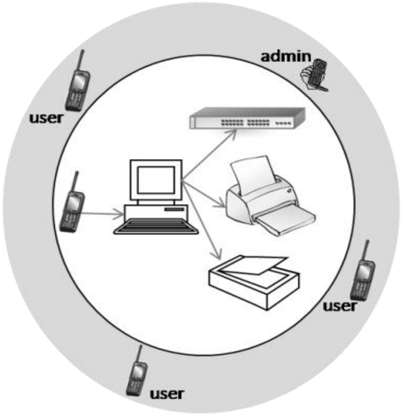

Fig 1: System Architecture

The load balancing and job scheduling algorithms are used for user management and session management.

3. ACCESS POLICY MODEL

The access control policy model designed based on user's levels. This model has three user levels they are Administrators, Special_Users, and Standard_Users. The administrators has full access rights. The special users have maximum access rights except change of some SYS_FUNC_ACCESS. The standard user access rights are defined by the administrator. The role of each user is given below.

The Role of Administrator:

- The administrator has full rights to ADD/EDIT/DELETE users through SMS.
- The administrator can create the session and grant the access permission to the users.
- The administrator can have full access rights of local and remote resources.
- The administrator has to ensure the authentication itself from the server by sending pass-code from the registered mobile phone before the proceedings.

The Role of Special Users:

- The special users have equal access rights of administrator user in FILE_SYSTEM_ACCESS and PERIPHERALS_ACCESS, but there is some restriction in SYS_FUNC_ACCESS and CONFIDENTIAL access.
- These users are not allowed to access confidential category data and operations and some operations of other category operations.
- These users are not allowed to Terminate Running Process, Add/Edit/Delete Users and Shutdown/Restart/Logoff Computer.

The Role of Standard Users:

- The standard user's access rights are designed by administrator.
- These kinds of users have limited access rights but the administrator can provide maximum access rights if required.

3.1 Custom Access Policy Design

In this proposed access model the administrator divides computing resources into four categories. That is SYS_FUNC_ACCESS, FILE_SYSTEM_ACCESS, PERIPHERALS_ACCESS and CONFIDENTIAL. System function access categories allow operating system oriented operations and user management operations. The File system access list allows file and directory oriented operations. The peripherals access list allows to access printers and scanners through GSM-SMS. The confidential category data is maintained and accessed by administrators only. Here the most required access resources and functions are given below; these resource lists can be updatable and editable.

Table 1. Access Resources and Functions

Categories	Access resources and functions
SYS_FUNC_ACCESS	List Installed Software's, Running Apps, Terminate Running Process, Memory Usage, List Installed/Running Services, Change Virtual Memory Size, Add/Edit/Delete Users, List Users, Shutdown/Restart/Logoff Computer.
FILE_ SYSTEM_ACCESS	Disk Size, Disk Partitions Details, DIR List, DIR size, DIR File List, File Size, Create/Delete/Copy Files, File Attributes, Read/Write Files.
PERIPHERALS_ACCESS	Access Printer, Access Scanner, Disable N/W Connections
CONFIDENTIAL	Read/Write/Copy Dir, Read/Write/Copy Files and Delete Dir and Files

All the settings, policies and session information's are stored and monitored by the software module which is run in the remote computer and all the actions and operations are done in that computer only. Every resource and function has unique ID like S1- List Installed Software's, S2-Running Apps, F1-Disk Size and P1-Access Printer likewise. In the process of building access policy model, the administrator creates a list of access resources and functionalities to users. The users can access the resources and executes commands based on the access policies that are set by the administrator. The users are not allowed to access the functions without the access list, every user can ensure the access rights and resources by sending SMS like "#ACL" to server and receive an access control list. The administrator create the user database like

Table 2. User Database

UID	ACCESS LEVEL	ACCESS CONTROL
AB001	Std_Users	S1,S2,S3,S5,S8,F1,F2,F9,C2
AB002	Spl_Users	Full Control
AB003	Admin	Full Control
AB004	Std_Users	S1,S2,S3,P1,P2

The user AB001 has permission to access only S1, S2, S3, S5, S8, F1, F2, F9 and C2 operations. If the user AB001 tries to access apart from the access list the system respond error message. The AB003 and AB002 have full access rights what they have in policy list. Only the registered user can access resources through SMS.

3.2 Session Management

The users can access the resources within the session time. The authentication processes include session allocation. This model has three kinds of session durations: 1.SHORT, 2.NORMAL, 3.MAXIMUM and these session slots provide 30, 60, and 120 minutes time duration for active connection respectively. If the users want to extend the session, they request administrator and the admin can extend the session duration through EXTEND command.

4. GSM INTERFACE

The GSM receiving module acts as a gateway in this model. This receiving module can be a GSM/GPRS modem, mobile phone or any SMS send/receiving device. This device connects with computer through USB cable [2]. The AT commands are used to managing connections and send/receive the SMS. Sample AT Commands are “AT+CMGL” List messages, “AT+CMGR” Read message, “AT+CMGS” Send message [2]. The interface module communicates with GSM device and reads the SMS and checks whether it’s a command SMS or ordinary SMS. If it’s a command SMS, this commands are executed by the local computer.

5. AUTHENTICATION PROCESS

The authentication processes ensure the user to access remote resources through SMS within the session. These processes occur among the user, admin and remote interface software. The users request access token from admin by sending UID. The admin ensure the UID is registered user and allot the session and access control list.

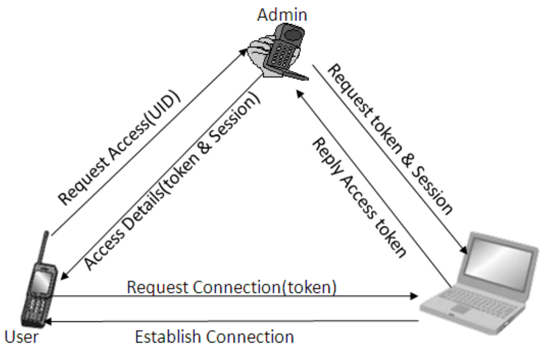

Fig 2 : Authentication Process

The registered user can request access token by sending “#REQ <UID>” SMS to admin. The admin forwards the user request with UID, user mobile no and SID to gateway mobile phone. The admin request SMS like “#ALT <UID> <MobileNo> <SID>”. The interface software reads and parses the incoming SMS and checks the SMS. If it is command then check for registered user, if it so then generates five digit alpha numeric random numbers every time and it will includes in active session manager. The active session manager is like

Table 3. Session Manager Database

UID	Token	Mobile No	Session	Status
AB001	TX001	9898012345	SHORT	1
AB004	AN002	9942654321	NORMAL	1
AB002	BS003	8965324222	MAXIMUM	0

The interface software replies with connection details or error SMS. The admin forward the acceptance SMS to the user. Then the user ensures the connection by sending token number to the server computer. The server checks and send acknowledgement to the user, after that the user start resource access through mobile SMS. The admin can edit ACL and resume session time through “#EDT ACL <UID> <access list>” and “#SES <UID> EXTEND”. The user can request admin to grant permission to access some resources apart from the list and terminates the connection before session is over. If the session is over or the user terminates the connection, the control software put the status value as ‘0’ to status of the user. List of admin SMS commands are

Table 4. SMS Commands

Command	User	Description
#ACL <UID>	All	Get user Access Control List
#REQ <UID>	Users	Request for Connection
#ATN <pass-code>	Admin	Authenticate Admin itself
#ALT <UID> <MobileNo> <SID>	Admin	Request Allotment for user
#EDT ACL <UID> <access list>	Admin	Edit user ACL
#SES <UID> EXTEND	Admin	Extend user session duration
#CLS <UID>	Admin	Force Close Connection
#DLT <UID>	Admin	Delete user
#CUL <UID> <Level>	Admin	Change User Level

6. REMOTE RESOURCE ACCESS

The user can access any resources in remote computer through SMS by sending valid commands. This model allow the user to access operating system functions, file systems, I/O functions, peripherals, network devices and whatever the functionality include in the policy list. Once the commands are reads and validated by the control software then it processed in local computer. The control software take the responsible to executes commands in local computer through OS API and codlings.

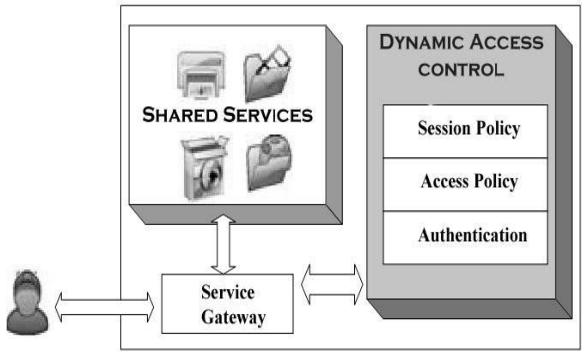

Fig 3: Resource Access Process Model

7. CONCLUSION

In this paper we present next generation trust based access model using GSM-SMS in pervasive computing environment. Nowadays the SMS is generic feature which use all kind of people so SMS based resource access will be the easiest access model. This model is very efficient and useful for digital library, office environments, trading environments etc. to access resource and data from remote place at particular time duration.

As a continuous addendum to the features, this model will extend to virtualization using video streaming and GSM-MMS services in pervasive environment. By this feature, the users are enabling to get computer screen in their smart device and operate computers virtually. This will be another version of virtual system.

8. REFERENCES

[1] Sheikh Iqbal Ahamed, Munirul M. Haque and Nilothpal Talukder, “Service Sharing with Trust in Pervasive Environment: Now it’s Time to Break the Jinx”, 2008.

[2] S.Pandikumar, “A Model for GSM Based Intelligence PC Monitoring System”, International Journal of Advanced Computer Science and Technology, 2012.

[3] Rainer Steffen, Rudi Knorr, “A Trust Based Delegation System for Managing Access Control”, In Advances in Pervasive Computing: Adjunct Proc. Pervasive 2005.

[4] Sudip Chakraborty and Indrajit Ray, “TrustBAC - Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems”, SACMAT, June 7–9, 2006.

[5] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli, “Role-Based Access Control”, Artech House, Inc., Norwood, MA, USA, 2003.

[6] Alessandra Toninelli, Rebecca Montanari, Lalana Kagal, and Ora Lassila: “A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments”, 5th International Semantic Web Conference, 2006.

[7] Manachai Toahchoodee, “Access Control Models For Pervasive Computing Environments”, Ph.D Dissertation, Colorado State University, 2010.

[8] Alessandra Toninelli, Rebecca Montanari, Lalana Kagal, and Ora Lassila: “A Semantic Context-Aware Access Control Framework for Secure Collaborations in ervasive Computing Environments”, 5th International Semantic Web Conference, 2006.

[9] M. Anisetti, C.A. Ardagna, V. Bellandi, E. Damiani, S. De Capitani di Vimercati, P. Samarati , “OpenAmbient: a Pervasive Access Control Architecture”, Co-located with the International Conference on Emerging Trends in Information and Communication Security (ETRICS’06), Freiburg, Germany, June 6-9, 2006.

[10] Kui Ren and Wenjing Lou: “Privacy Enhanced Access Control in Pervasive Computing Environments”

[11] Ran Yang, “Trust Based Access Control in Infrastructure-Centric Environment”, IEEE International Conference on Communications (ICC), 2011.

[12] Michel Kamel, Romain Laborde, Francois Barrere and Abdelmalek Benzekri, “A trust-based virtual collaborative environment”, journal of Digital Information Management, 2008.

[13] Deok Gyu Lee, Jong-Wook Han, Doo Soon Park and Im Yeong Lee, “Intelligent Pervasive Network Authentication: S/Key Based Device Authentication”, Consumer Communications and Networking Conference, 2009.

[14] Long Zhao Hua, “Research on Pervasive Computing Security”, International Conference on Ubiquitous Intelligence & Computing, 2010.

[15] Tsaur, M.J, Wei-Chi Ku and Hao-Rung Chung, “An Improved Password-Based Authenticated Key Agreement Scheme for Pervasive Applications”, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008.