Secured Policy based Resource Access and User Authentication in Ubiquitous Computing Environment

S.Pandikumar, S.Malathi, K.Sathiesh Kumar, M.Arun, R.Kalpana

Abstract: Policy-based resource access and data sharing are the most specific in context-aware computing. Granting authentication to the wireless and ad hoc users is usually difficult because the system has got to take into account several context factors whereas authoring access. During this epoch, the mobile phone plays a significant role in info access in a ubiquitous environment. Wireless technologies, significantly the GSM-SMS is efficient and efficient to access shared data around the world with fewer security issues. The shared resources like printers, scanners, databases, books, email, etc. are liable to the users once they try and access with proper authentication. The proposed system provides systematic access policy schemes and creates the access mechanism to remote users. These policies and mechanisms are entirely supported context info. The user should satisfy the defined context and defined the user level. This mechanism provides the facilities to users to request and access control through SMS.

Keywords: SBAC, Ubiquitous Computing, Policy based, Resource Access.

I. INTRODUCTION

Ubiquitous computing and pervasive computing are the emerging research area to achieve anything, anytime, at anywhere philosophy [1]. Even it's a predecessor of the Internet of Things. There is a need to connect all the devices without any obstacles and provide services to the users. Mobility is the goal of ubiquitous and it will be implemented through wireless technologies. The convergence of computing and wireless technology gives new exciting services and flexibility to the users to access shared resources [3]. Such places and organizations need to share some resources with their customers or user to access. For example, an equipped digital library provides mobile access of their e-books to maximum members and they want to protect the e-books from the intruders and non-members of the library. A company wants to share its resources, dataset or sensitive data to its trustworthy employees at a particular time but they want restrict the resources from access at particular period of time. Even they want to protect them from outsiders also. The intruders may enter into the system and attack all the resources. Even trustworthy employees may crash the sensible data or other data by accident and intentionally.

So the ubiquitous system to allow the users to enter into the secured communication and access rights at particular context [4-6].

That kind of situation in ubiquitous computing needs a context-based architecture and high-security policies to access and restricts resources and even it demands seamless, secured and efficient wireless technology also.

This paper introduces a novel, policy, and session based context aware, cost effective and seamless access control model to access the shared resources. The remote devices or resources can be accessed through GSM short message service with particular time context. The user can use any kind of GSM device like mobile phone, tablet, or any other GSM enabled computing device. The user access policies are created and allocated by administrator when the users want to be a member of this ubiquitous environment. The user can access the resources within the environment or without the environment because they use SMS service to create a logical connection between the user equipment and remote device. The temporary sessions are created to all users on the basis of user requests. The session time is defined by the administrator.

The session and trust policies are maintained and all the processing happens in the monitoring system.

The scope of this paper is

- A secured and policy-based access model is proposed to access the remote resources and sharing services within the ubiquitous environment.
- Seamless, low cost and error-free wireless technology that is GSM-SMS is used for communication purposes.
- The session and trust policies avoid and identify the malicious access

The paper further arranged by 8 sections. Section 2 explores various results from fruitful researches through a detailed literature review. Section 3 proposes architecture. The access policy model and its procedures are discussed in Section 4. Section 5 discusses how the GSM interface used for the authentication process. Section 6 focuses on authentication steps and procedures. It explains how the system recognizes user commands and how it will be parsed. Remote resource access is discussed with an architecture diagram in Section 7. Section 8 gives the conclusion and directions to future research.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author

Dr.S.Pandikumar*, Assistant Professor in Department of Computer Science, The American College, Madurai, India.

S. Malathi, Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India.

M.Arun., MCA, Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India.

K.Sathiesh Kumar, Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India.

R. Kalpana, Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India.

II. LITERATURE SURVEY

The survey focus to study between 2015 to 2019 papers and the papers were collected from IEEE Xplore, Scopus, and Semantic Scholar. Totally 40 papers are identified as relevant to the area but only 8 papers were chosen for review because those are result based works. The selected papers are related to the following; Role-based, Ontology, location, dynamic-context and trust-based [7]. Those papers are proposed navel methods to develop authentication and access models.

Author [8] proposed a technique to authenticate a user based on multi-factor authentication. The research introduced a brand new context-aware identification that is user-in-a-context that identifies the user's location, time and alternative biometric parameters to provide secure authentication to access the sensitive information on the particular premises (Fig 1). The research assigns totally different access policies to different users in a different context. The work used sensors for acquiring location context and uses biometric devices for physical context.

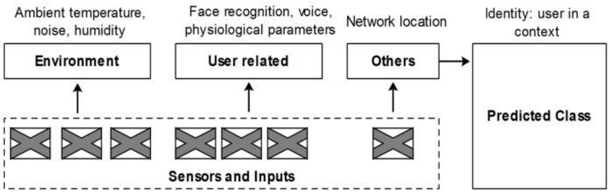
Ambient temperature, noise, humidity
Face recognition, voice, physiological parameters
Network location
Identity: user in a context
Environment
User related
Others
Predicted Class
Sensors and Inputs

Fig 1. Context dimensions used to identity a user in a context [8]

Vishal Rathod et al [9] proposed a new access model that's a semantically rich context-sensitive access control system for open-source resources in the cloud environment. The granting of access rights of the users is based on current context attributes like location, time, etc (Fig 2 and Fig 3). The system is implemented on the OpenStack cloud computing platform.

A. S. M. Kayes et al [10] introduced a new approach of context-aware access control by using ontology. This research proposed the OntCAAC framework to provide authentication of stakeholders to access software service and information depositories. The framework work based on dynamic context and entity and its relationships.

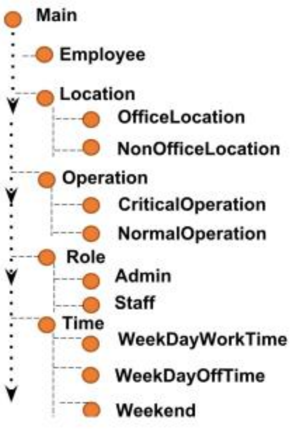

Fig 2. Some context Attributes used in the sample scenario [9]

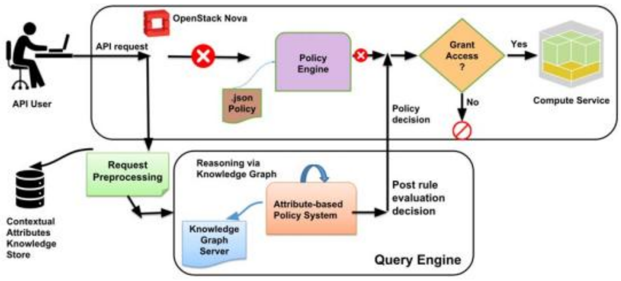

Fig 3. OpenStack Policy Engine Architecture [9]

Bilal Shebaro et al [11] describes the new access control model that is Context-based Access Control (CBAC) is used to define policies to access smartphone Apps in different context level. The architecture modifies the Android core and incorporates the policies into the operating system functions. It restricts some of the Applications from accessing the data at a particular location.

Research [12] proposed a context-aware dynamic permissions model (CAPM) for Android systems. This method assigns a different authentication profile to different android applications. These profiles have different access permissions and restrictions associated with their context and it will be activated automatically when the context is matched without user interference. The context information is acquired from mobile sensors and other sources. The permission of such applications like

- SMS_ SEND_RECEIVE
- VOICE_ CALL
- AUDIO_ RECORDING
- READ_ WRITE_CONTACTS
- ACCOUNTS_AUTHORIZATION

The permissions will be activated or deactivated based on the location or time.

The author [13] proposed a method to generate two kind of authentication password that is textual as well as graphical. The system generates a temporary session password to the user and it will generate authentication password for access the resources. The pair based authentication and hybrid authentication techniques were used to generate the passwords.

Neetesh Saxena et al [14] proposed a user authentication and authorization scheme based on the smart grid for accessing the sensible devices in the ambient. Each user (operators, auditors, administrator, user, etc) should have attributes based authentication policies which is using hash function. A paired secret key is generated to share data between user and device at periodic interval.

The author [15] introduced a new access scheme called trust-role based access control model to granting the authentication dynamically. Once the user wants to access the sharable resource or information the system analyse the user trust level through calculating the user behaviour and context aware info of platform environment and build the trust relationship of the user. If the user satisfies the trust level then only they authorized otherwise the denied.

III. PROPOSED ARCHITECTURE

The architecture policy-based access control system through SMS is two-tier architecture which is a user and monitoring system (or control system). The detailed role of administrator is discussed in the forthcoming section but the overall responsibilities of admin are creating/ deleting the user and define their access right policies.

Trustworthy users are can have the rights to access sharable devices and data through SMS in ubiquitous or anyplace in the world (Fig. 4). In this architecture, the admin is playing a key and powerful role (In this text, the administrator, admin and superuser are the same and use interchangeably). The system is designed based on granting the rights of admin. The detailed access policies are discussed in the following sections.

The users give a request to the administrator to include or join the access system through SMS. The syntax of the special SMS is defined by the system. The admin creates a User ID and assigns the user level. The user levels are standard, special and administrator. The admin creates the detailed access policies of users and resources. The entire authentication process will be executed based on these policies only. Based on these levels and policies the user can access the resource from a remote place. This process of creating policies for the user occurred once in the lifetime of the users. After receiving user id, the one can send a request to get access token. Once, the monitoring system allocates the token to the user then only the user can have an active session to access the remote resources. During the process of allocating token, the system is verified the user level and their accountability. The session is nothing but the access time of every user. Every user receives a different session ID. Once the session is allocated, the user can until the session is ended. If the user wants to extend the session, then again the requesting procedure should be followed.

The whole process is executed only through SMS. The GSM module is attached in the monitoring system and it controlled by the system (Fig. 4). Each and every incoming SMS is read and parsed. If received SMS is special SMS, then it will be executed.

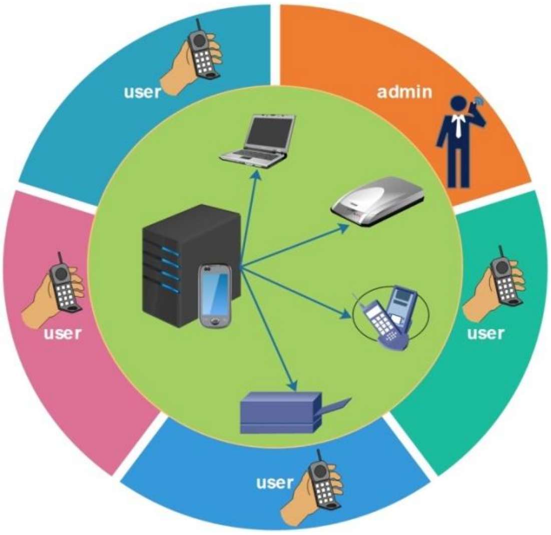

Fig 4. Prposed Architecture

The computing algorithms like load balancing, scheduling, and parallel processing are used to receive SMS and session management.

IV. ACCESS POLICY MODEL

Every user comes under access control schemes. Those schemes are grouped into three. That is Administrators, Special_Users, and Standard_Users. Anyone of those levels should be assigned to the user during user creation.

The administrator user can be a default user and can be a superuser. This level user has maximum access rights on the resources and monitoring system. This control can be auto or manual mode. When the admin can be auto mode, the system takes over all the processes of creating users and policies. If the control is manual, the person will take over the user managements.

The role of admin is follows

- The superuser has maximum rights on users and resources. This level user can Create/Delete/Edit users and Share/unshared resources through SMS.
- The superuser contributes to generate user access token and session and grant the access permission to the users.
- Sharing database and internet.
- The admin has to ensure the certification itself from the monitoring system by transfer pass-code by SMS before the process started.

The special users have full access rights except for the change of some SYS_CORE_ACCESS. This kind of user may be higher officials.

The Role of Special Users:

- The special users have equal access rights of admin users in FILE_SYSTEM_ACCESS and PERI_DEV_ACCESS, except for some restrictions in SYS_CORE_ACCESS and PRIVATE access.
- These users are restricted to access confidential data, resources, and operations. Mostly, this policy is granted by an admin.
- These users are not allowed to Terminate Process/services and edit user management and their authentications and control of monitoring system management.

The standard users are normal users; they have restricted and limited access rights that are designed by the admin.

The Role of Standard Users:

- The restricted/standard users can grant to access user services and resources.

Usually, these kinds of users have minimal access rights but if needed the administrator can provide maximum.

4.1 Custom Access Policy Design

The access scheme or model is divided into four categories. That is SYS_CORE_ACCESS, FILE_SYSTEM_ACCESS, PERI_DEV_ACCESS, and PRIVATE. System core access category allows the user to access operating system related operations and user management operations and it includes internet and database related manipulations too. The File system access category allows users to access file system-oriented manipulations. The peripheral device access categories allow accessing all kinds of I/O devices such as scanners, printers, etc. through GSM-SMS. The private category is the same as a confidential category. This kind of policy and data are maintained and accessed by administrators only.

The detailed security policies of the four categories are given below.

Table 1. Access Resources and Functions

Categories	Access resources and functions
SYS_CORE_ACCESS	User management, user installed software and system management, system services, database management, internet options and security, I/O management, Memory optimization and status, Network management.
FILE_ ACCESS	Disk Usage Size, Disk Drive Partitions Details, Directory List, Directory size, File List, all file operations and manipulations.
PERI_DEV_ACCESS	I/O manipulations and Network features enable/disable.
PRIVATE	Assign security policies of user, List policies of user, I/O

The monitoring software maintains all the modules and user details which is normally run on the special equipped server computer. This module and system can be authorized by admin-level users only. All internal database of security policy is maintained in the same system. All the resources and operations are clearly identified by its unique identifier like

- ✓ A1- List Installed Software's,
- ✓ A2-Running Apps,
- ✓ Q1-Disk Size and
- ✓ P1-Access Printer likewise.

During the registration of the user, the admin defines the access policy list and resources. This model contains what are the rights the user have and how the user will access the resource and which time the user can execute those rights. These policies are assigning based on the record of employee and the requisition. Every user must know their access policies after registration through the structured SMS command "#ACL" to the server and receive an access list. The superuser creates the user database like table 2.

Table 2. User Access Policy Database

UID	ACCESS LEVEL	ACCESS CONTROL
UID1	Users_Std	A1,A2,A3,A5,A8,Q1,Q2,Q9,D2
UID2	Users_Spl	Full Control
UID3	Admin	Full Control
UID4	Users_Std	A1,A2,A3,P1,P2

The user UID1 granted access only A1, A2, A3, A5, A8, Q1, Q2, Q9, and D2 operations. If the user UID1 tries to access other services or resources the monitoring system responds error message. The UID3 and UID2 have full access rights that they have in the policy list. Only the registered user can access resources through SMS.

4.2 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:

- ➢ SES_SHORT,
- ➢ SES_NORMAL,
- ➢ SES_MAXIMUM

These session slots provide an active connection to the user to access the requested resource up to 30, 60, and 120 minutes time duration respectively. If the active user wants more time, the one can send the "#EXTEND" command SMS to the monitoring station. The users token verified and renew the session time.

V. GSM INTERFACE

GSM interface is the core component of this architecture. It is the gateways of the monitoring station and it fixed in the monitoring server. It always ready to send/receive SMS from the user and send an acknowledgement to the user. This module is entirely controlled by a monitoring station and indirectly by the admin.

GSM module can have a physical or logical connection. The physical connection is made by the USB port and the logical connection made by any wireless devices like Bluetooth, wi-fi [2]. The monitoring station use AT (Attention) commands to create and manage connections and do all operations. All commands and acknowledgement SMS are sent or receive through this AT commands technically. These commands are instructions to the GSM modem.

Table 3. Example of AT commands

AT Commands	Description
AT+CSMS	Select message service
AT+CPMS	Preferred message storage
AT+CMGF	Message format
AT+CSCA	Service Centre Address
AT+CMGL	List messages
AT+CMGR	Read message
AT+CMGS	Send message
AT+CMGD	Delete message

For example, AT Commands are "AT+CMGL" List messages, "AT+CMGR" Read message, "AT+CMGS" Send message [2] (Table 3). All those commands are composed and executed by the monitoring system.

VI. AUTHENTICATION PROCESS

The authentication processes are the core process of this system because it ensures the user to register itself and access remote resources through SMS within the session. These processes occur among three entities, the user, admin and remote interface software (server).

The one who wants to join the access system, who must register itself with the system through sending request SMS with essential details to the admin. The admin verifies the one identification with local database and provides user ID to them. This process is started through send "#REQ_ID" SMS to admin system which monitoring station obviously. The server reads the special SMS (special SMS or commands are usually starts with '#' symbol) and parses that SMS then it allocates UID, user level, and access list. Once the above process is over, the server sends user ID to one with an acknowledgement (Fig 5). The user-level and access list of that user is recommended by admin only.

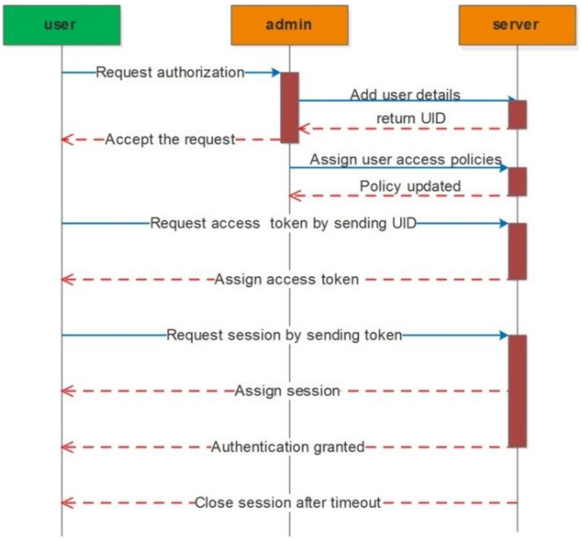

Fig 5. Authentication Process

After the registration process, the user can send SMS “#REQ_Token <UID>” to request access token to the server to create a session. The token numbers are five-digit random and unique numbers. The monitoring station verifies and accepts the request and sends the session details to the user. The token number generation process verifies the authentication of the user. The session is providing access permission to the resources otherwise return an error message. The active session manager is like

Table 4. Session Manager Database

UID	Token	Mobile No	Session	Status
UID1	AX005	0123456789	SES_SHORT	Active
UID4	BB006	9876543210	SES_NORMAL	Active
UID2	BC007	1122334455	SES_MAXIMUM	InAct

Sometimes the user wants more access permission to access the resource, that time the one can request access to admin. The admin can edit ACL and resume session time through “#EDT_ACL <UID> <access_list>” and “#SES <UID> EXTEND”. If the active session is a timeout, the connection is disconnected and the session status of the user is put into Inactive. Some of communication SMS commands are given below

Table 5. SMS Commands

Command	User	Description
#AccessList <UID>	All	Get user Access Control List
#REQ_Token <UID>	Std_Users	Request for Connection
#Authenticate <pass-code>	Super_user	Authenticate Admin itself
#Allot <UID> <MobileNo> <SID>	Super_user	Request Allotment for user
#EDT_ AccessList <UID> <access list>	Super_user	Edit user ACL
#SESION <UID> EXTEND	Super_user	Extend user session duration
#CLOSE <UID>	Super_user	Force Close Connection
#DELETE <UID>	Super_user	Delete user
#CH_UserLevel <UID> <NewLevel>	Super_user	Change User Level

VII. REMOTE RESOURCE ACCESS

The monitoring station allows the user to access shared resources through SMS during the session time. When the user has access time with authentication to control devices like printers, scanners, or other peripherals, etc. The user sends a valid SMS command to control devices. These access policies are defined by the admin during the user registration.

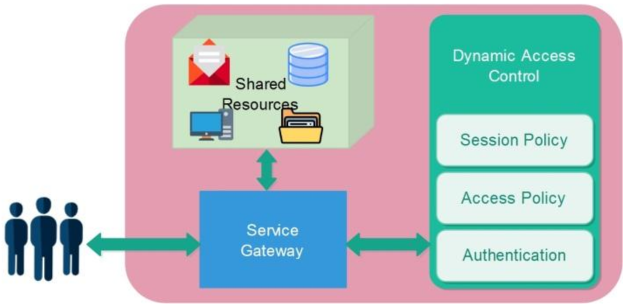

Fig 6: Resource Access Process Model

VIII. RESULT AND PERFORMANCE ANALYSIS

8.1 Measurement of SMS Arrival Rate

In Global System for Mobile Communication (GSM) architecture all the communications are made by set of logical channels. These channels are bot uplink and downlink. The SMS messages are carried on either SD-CCH or SACCH [16] depending on the use of the traffic channel. Traffic Channel (TCH) is responsible for carry the voice and data and the SMS is carried on the SDCCH (stand-alone dedicated control channel).

In this architecture, the GSM module does not commit TCH but it’s dedicate to Sending SMS only so it’s always use SDCCH to send SMS. The throughput of the SMS is depends on the network traffic and location [16, 17]. So that the delivery of user request and responses is entirely depends on the above parameters.

Let λsms, $\lambda\iota$ and λv be the arrival rates for received SMS, updation of the location and voice call setup respectively. The arrival rate of this aggregate traffic that uses SDCCH channels is given by

$$\lambda c = \lambda sms + \lambda\iota + \lambda\nu.$$

Let the mean service time (i.e. channel holding time) of a single SMS message like μ_{sms}^{-1}, and that updation of the location and voice call setup message be μ_l^{-1} and μ_v^{-1} for respectively. The unconditional expected service time of an arriving message is then given by

$$\mu_c^{-1} = \frac{\lambda_{sms}}{\lambda_c} \times \mu^{-1} + \frac{\lambda_l}{\lambda_c} \times \mu_l^{-1} + \frac{\lambda_v}{\lambda_c} \times \mu_v^{-1}$$

Figure 7 displays the differences of SMS delivery time between 8AM to 10PM. Here the lowest delivery time of special SMS is 1 sec at 2:10PM and the maximum delivery time is 6 sec at 7:50PM. The average delivery time of this architecture is 3.5 seconds and zero data lose.

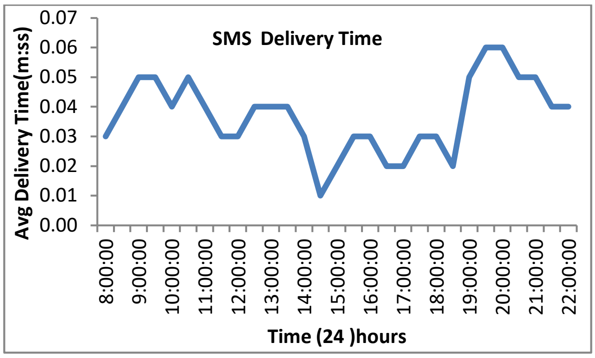

Fig: 7. SMS Delivery Delay Time

IX. CONCLUSION

This paper presents a novel, cost-effective policy-based access control architecture using SMS to access remote resources. Ubiquitous computing provides freedom to access resources from anywhere, anytime. This model allows the user to access sharable data and devices from remote places. It's very useful in an equipped digital library, share trading, modern offices, etc.

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

REFERENCE

1. J. L. V. Barbosa, "Ubiquitous computing: Applications and research opportunities," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1-8.
2. S.Pandikumar, "A Model for GSM Based Intelligence PC Monitoring System", International Journal of Advanced Computer Science and Technology, 2012.
3. V. J. Silva, M. A. S. Rodrigues, R. Barreto and V. Ferreira de Lucena, "UbMed: A ubiquitous system for monitoring medication adherence," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-4.
4. 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.
5. 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.
6. Kui Ren and Wenjing Lou: "Privacy Enhanced Access Control in Pervasive Computing Environments"
7. Ran Yang, "Trust Based Access Control in Infrastructure-Centric Environment", IEEE International Conference on Communications (ICC), 2011.
8. A. Basu, R. Xu, M. S. Rahman and S. Kiyomto, "User-in-a-context: A blueprint for context-aware identification," 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 329-334.
9. V. Rathod, S. Narayanan, S. Mittal and A. Joshi, "Semantically Rich, Context Aware Access Control for Openstack," 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, 2018, pp. 460-465.
10. A. S. M. Kayes, J. Han and A. Colman, "OntCAAC: An Ontology-Based Approach to Context-Aware Access Control for Software Services," in the Computer Journal, vol. 58, no. 11, pp. 3000-3034, Nov. 2015.
11. B. Shebaro, O. Oluwatimi and E. Bertino, "Context-Based Access Control Systems for Mobile Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 2, pp. 150-163, 1 March-April 2015.
12. S. Kumar, R. Shanker and S. Verma, "Context Aware Dynamic Permission Model: A Retrospect of Privacy and Security in Android System," 2018 International Conference on Intelligent Circuits and Systems (ICICS), Phagwara, 2018, pp. 324-329.
13. Sanket Prabhu, Vaibhav Shah "Authentication Using Session Based Passwords" in proc. International Conference on Advanced Computing Technologies and Applications, Volume 45, pp. 461-464, 2015.
14. N. Saxena, B. J. Choi and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 907-921, May 2016.
15. R. Bhatti, E. Bertino and A. Ghafoor, "A trust-based context-aware access control model for Web-services," Proceedings. IEEE International Conference on Web Services, 2004., San Diego, CA, USA, 2004, pp. 184-191.
16. Pandikumar, & Vetrivel, R. (2014). Internet of Things Based Architecture of Weband Smart Home Interface Using GSM.
17. Fabian van den Broek, "Catching and UnderstandingGSM-Signals". Master thesis, Radboud University Nijmegen, March 22, 2010.
18. Agarwal, N., Chandran-Wadia, L., & Apte, V. "Capacity Analysis of the GSM Short Message Service".

AUTHORS PROFILE

Dr.S.Pandikumar., MCA., M.Phil., Ph.D. is working as an Assistant Professor in Department of Computer Science, The American College, Madurai, India. He has 11 years of teaching experience and successfully published 12 books in various topics. He published 27 research papers in various international journals and presented 48 papers in various international and national conferences. He received best teacher award twice in his service. His area of research is Cellular Networks, Green Computing, IoT.

S. Malathi., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. Her area of interest includes Data Structures and Data Mining. She has attended many National Conferences, Workshops and Seminars. She has presented 10 Research Papers in National Conferences and published 6 Research Papers in International Journals.

M.Arun., MCA., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. He has 9 years of teaching experience and published 6 papers and attended more than 6 international conferences. His research area is IoT, Mobile Computing.

K.Sathiesh Kumar., MCA., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. He has 11 years of teaching experience and published 6 papers and attended more than 6 international conferences. His research area is IoT, Data Mining.

R. Kalpana., MCA..M.Phil., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. He has 4 years of teaching experience and published various research papers in peer reviewed journals. Her research area is Data Mining and Spatial Data Mining.