View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UUM Repository

International Journal of Information Technology & Computer Science (www.ijitcs.com) Volume 15 Issue No 1, June 2014
ISSN (online) : 2091-1610

Anonymity Handling and Sensor Object Modeling for Pervasive Environments using VISA Processing

Dr.G.Radhamani
School of IT and Science, Dr.GRD College of Science, Coimbatore, India
radhamani@grd.edu.in

K.Vanitha
School of IT and Science, Dr.GRD College of Science, Coimbatore, India
vanitha.k@grd.edu.in

Angela Amphawan
Research Laboratory of Electronics
Electrical Engineering and Computer Science Department
Massachusetts Institute of Technology, 02139 Cambridge, USA
angelaa@mit.edu

Abstract*:*

Pervasive computing devices are configured for anywhere at any time services to adapt the changes in the dynamic environment with respect to the user mobility. The paper proposes a salient model for a log based anonymity handling in pervasive networks. The model defines a resource registry and sensor object modeling. Associability between the nodes are configured with an allied user interface in the environment. Resource registry refers to a record of information about the sensor nodes. A log book is maintained to keep track of the service discovery issues. New device enquiry, registration and adaption are major issues in such pervasive devices. These issues lead to unacknowledged communication that causes anonymity. This paper defines and discusses the presence of anonymity in pervasive environments due to aforementioned issues.

Keywords- : Pervasive Computing; Service Discovery; Anonymity; Middleware.

I. INTRODUCTION

Personal computing is expanded to pervasive computing when the user interaction increases to many devices or computers. Pervasive computing provides an attractive vision for accessing information anywhere and anytime. Such environments gracefully integrate networked computing devices from tiny sensors to extremely dynamic and powerful devices with people and their ambient environments. A room, for example, might be saturated with hundreds of devices that provide information to people without seeking their active attention. Pervasive computing is the idea that almost any type of device can be embedded with chips to connect the device to an infinite network of other devices to provide convenient access to relevant information when and where it is needed. With respect to the development of applications for pervasive environments, a middleware can be used to bridge the gap between the application and the underlying operating systems and networks. One of the basic purposes of any middleware is to satisfy application requirements as well as to support the challenges and issues in computing devices. Dynamic changes of the environment reflect in the mobility and location change of the user or the device, data transfer between sensor nodes and any state change information. Since the devices are mostly invisible across the users computing environment, there may be possibility of unknown devices or unknown user emerging in existing computing environment to access resources. This possibility renders the anonymity in pervasive environments. Handling anonymity using object-based registration and log-based reusability are the key contributions of the paper.

II. LITERATURE REVIEW

Several middleware are available for pervasive systems. Some of the most representative are described in this section. [1] focused on some important middleware categories and technologies suitable for today's mobile middleware and discussed about how the middleware is connected to the pervasive environment. [2] presented the concept and design of BASE, a flexible middleware supporting the additional requirements of pervasive computing environments, and how the design implementation of BASE middleware shields applications from the multitude of different communication technologies and interoperability protocols by separating the communication model of the application and the interoperability protocols used.[3] discussed a privacy-aware solution for service discovery in heterogeneous networks, based on the MUSDAC platform and privacy issues that arise during service discovery and mechanisms to control disclosure of private information contained in service related data. [4] described about the privacy threats identified in a pervasive environment and presented a set of principles for ensuring privacy.

Number of privacy protection mechanisms for pervasive systems were examined with the focus on the level of anonymity offered to the end user. Also Stelios Dritsas et al concluded by presenting a set of essential actions one should take into account, in order to ensure users anonymity in a pervasive computing environment. [5] Provides an object-based framework for supporting context-sensitive applications. [6] Presented the Sensor Enablement for the Average Programmer (SEAP) middleware, which lowers the barrier to entry for programming pervasive computing applications with existing languages. A Virtualized Secure Framework between mobile devices (clients) and Location Based Services (LBS) Server in Virtual Machine (VM) environment based on Direct Anonymous Attestation protocol is proposed. Trusted Platform Module (TPM) acts as the foundation for mobile security mechanisms and privacy of user's information.[13]. The privacy for internet of things technologies by focusing on the most "primitive" members, bare sensors and RFIDs is addressed. [14]. Classification of anonymity in pervasive environments is discussed and a handling model is suggested. [15].

III. ANONYMITY IN PERVASIVE COMPUTING

Anonymity can be defined as a subject who is not identifiable or unacknowledged among the set of subjects. In pervasive computing, anonymity plays a key role in user, device and data components, as illustrated in Fig. 1. It can be of any device or user which is unidentifiable by other devices among them. Information can also be anonymous in pervasive environments.

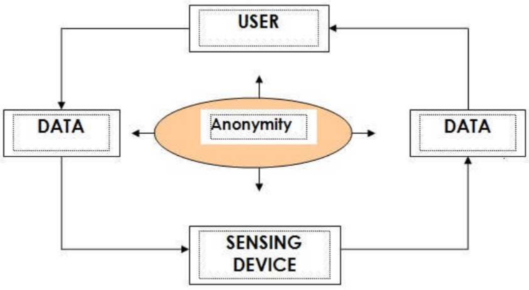


Fig.1. Anonymity in Pervasive Environment

A. Device or User Anonymity

Each device in pervasive computing environment performs their role for a user to satisfy their requirements and makes adaptable to the changes in the physical world. An anonymous user is a user who unknowingly enters into its computing world. An unacknowledged user may provide some malicious access to the other devices to destroy in it. The anonymous user may steal the personal information such as user personal data (trusted entity in the pervasive environment) device identity, location etc among other user in the pervasive systems. Ubiquitous and pervasive devices are becoming very popular and less expensive these days with which different devices like mobiles, smart phones and PDA etc has been dynamically adding into the computing environment to interact and coordinate easily with other existing devices in the pervasive environment .due to this dynamism any device entering into the existing pervasive environment may be a malicious one to abuse the service or resources available there or anonymously interact with all the devices in the computing environment to access the resources. Since pervasive computing permeates, dynamism in addition and removal of devices leads to misidentification or anonymity in Pervasive computing.

B. Data Anonymity

The pervasive applications may need the user's static or dynamic data to provide access to services. Static data may include age, group, education level, etc. Dynamic data refers to contextual information such a location, activity state, etc. The static profile and contextual information are exchanged often among devices in the dynamic environment. The owner of the information desires control of what goes out of the system. On the other hand, the service provider requires a certain level of quality of the information disclosed in order to provide the service. The greater the amount of information disclosed, the higher the chance of re –identification of the user even if the identity of the user is not disclosed. The balance hinges between the user's desire to control the anonymity level of the information disclosed and the provider's requirement of meeting a quality level of that information.

IV. MODELING SENSOR SERVICES IN PERVASIVE COMPUTING

Service discovery is an increasingly important issue as we move towards realizing pervasive systems. How does the user identify and access a particular service from the plethora of services that may potentially be available around him at any moment? Having discovered a service, a second important issue is how the user interacts with it. Pervasive computing systems are not like the common desktop PC network, but are composed of smallembedded devices, communicating in a wireless network independent of any global management. This is where the field of service discovery fits in. For a device to be truly mobile, it must be able to interface and co-ordinate with its surroundings without the user's intervention. For this to happen, the service discovery protocol must be able to discover local resources and form an ad-hoc network. Thus, ubiquitous service discovery is the ability to discover and form an ad-hoc network without explicit user direction. A typical service discovery protocol has ten main components. They are service and attribute naming, initial communication method, discovery and registration, service discovery infrastructure, service information state, discovery scope, service selection, service invocation, service usage and service status inquiry. Pervasive computing in sensor networks is different from regular networks. The reason is the sources of data are tiny sensors that are attached to a Sink node.

A. Transforming Sensor Data as an Object

From a computing perspective, a user interface would interact with sensing signals so as to transform them to an understandable format. Every sensed data is to be converted as an Object and deployed in the registry. Object creation is a process of memory allocation, acquiring state information and recording. Thus an object will have life span and expiry time. Fig.2 illustrates a Sensor Object to be stored in the registry.

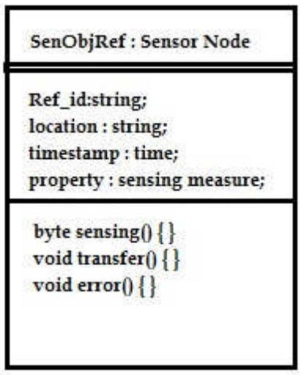


Fig.2 A Sensor Object

B. Object Registration

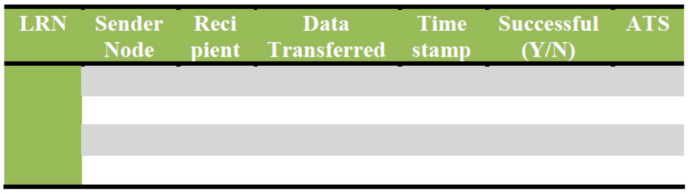
Every deployed sensor is accounted in the Object Registry in the Pervasive Environments. Object Registry is a directory maintained in Pervasive Server. The Server is operated as a dynamic or stationary node based on the application domain. The proposed model describes with sensor networks in an agriculture farm. The farm is said to Pervasive since the nodes are minimum visible, autonomous and cognitive. The end users of the Pervasive farm are to be plants and moving cattle. Obviously, the network is mandatorily self-sustained. Initial registration of sensor objects is probably started manually by human interaction. Over the period of time, the network receives registered and unregistered entities within the boundary. The network is responsible to account the unknown signals.

V. LOG BASED HANDLING

A. Design of the Log

The log records the transactions between the sensor nodes and the user every time. The log is designed with a Log Run Number (LRN) that is generated automatically. Creation of the Log is made when the sub-net of the sensors nodes are deployed. Anonymity handler is a software component in Pervasive Server Application that checks for the registered entries. The Log is classified into (a) Transaction Log and (b) Guest Registry. The Transaction Log (TL) is a record of routine signal passing between the nodes or to the base station vice versa. The Table 1 illustrates the transaction log template that maintains the data transfer between nodes and user. A special field Attest (ATS) is created for checking the authentication of the registered user.

Table 1. Transaction Log Template



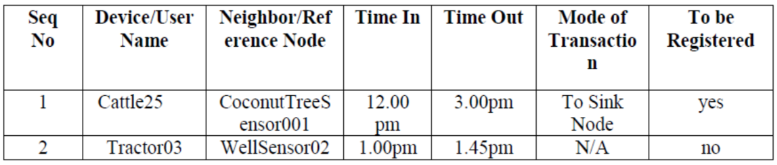
LRN	Sender Node	Recipient	Data Transferred	Time stamp	Successful (Y/N)	ATS

ATS is valued by Pervasive Server attached to the Network. If the value recorded as ‘1’, the data transfer is valid. Otherwise the value is set as ‘0’ for anonymous entry.

B. Guest Registry (GR)

The Transaction Log pours out the data to Guest Registry if the value of ATS IS ‘0’. i.e. the book considers the anonymous entry as a guest objects. The Guest Registry (GR) is responsible to keep track of unregistered entries passed from TL. All anonymous entries are not malicious ones. Since, Pervasive Networks avail the proactive identification some nearby cluster sensors are possible. So many times the need for including a guest as an authenticated Sensor Object happens. Table 2 refers the Guest Registry Log in a farm region scenario.

Table 2. GUEST REGISTRY IN FARMING SCENARIO



Seq No	Device/User Name	Neighbor/Reference Node	Time In	Time Out	Mode of Transaction	To be Registered
1	Cattle25	CoconutTreeSensor001	12.00 pm	3.00pm	To Sink Node	yes
2	Tractor03	WellSensor02	1.00pm	1.45pm	N/A	no

C. The Data log

The nodes are sending signals to the sink nodes synchronously, wherein the time interval is fixed. And the signals are the similar to the prior in most of the cases. The replicated signals are to be filtered in the sink end, called data filtering. The data log is maintained at the sink end for accounting the data for further classification and decision making. The refined data log is generated with registered sensors. If any unknown signals are identified in the network, the Sink node and base station would enquire the Pervasive Server for the verification. The Pervasive Server replies to the base station with guest acceptance or for rejection of new service.

VI. THE PROPOSED MODEL

Middleware is a software layer which sits below the applications and above the operating system to provide the common programming abstraction across all the distributed systems. Context-awareness, dynamism and heterogeneity are some of the properties that differentiate pervasive computing from traditional distributed systems. Most traditional distributed systems are unaware of context, are static, and are composed of homogeneous devices. Furthermore, different devices might be connected to different networks, with different latency and bandwidth. As a result, the middleware must provide mechanisms for handling disconnections, addressing fault tolerance, and adapting to a number of issues related to diversity including heterogeneous device resources. Many of the existing middleware's addresses the pervasive computing environment issues such as mobility, disconnection, dynamic introduction, removal of devices and merging of the physical environment with the computational infrastructure etc to provide a convenient interaction among the application and the pervasive devices. Even though middleware's which provides service such as privacy they can only protect the personal details. Due to the anonymity issues in pervasive systems may get into the risks such as personal information healing, memory destruction, routing failure can be occurred. Fig. 3 is the proposed middleware architecture which tackles the anonymity issues in pervasive systems.

The middleware architecture for handling anonymity deals with three components such as anonymity handler, Resource registry and device registry. Device registry contains the details about trusted devices (managing by the provider) and also it updates the device which is new to its computing environment. Resource Registry holds the details about the resources available for the devices in its local region. Anonymity handler is used to validate the equipments in pervasive systems to identify whether it can be acknowledgeable one or unknown one. It allows the registry to update the record if it is a valid device otherwise it will eliminate. Since services are on the opposite end from the client, it is difficult for a service to force itself upon the client.

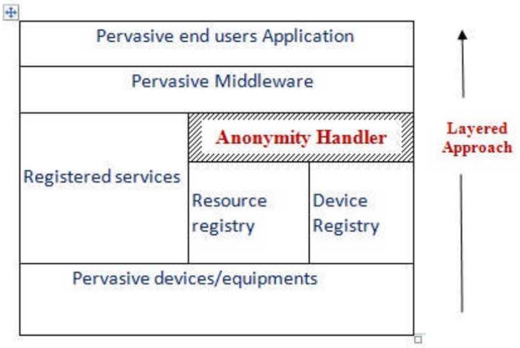


Fig.3 Anonymity Handler inMiddleware

None of the reviewed solutions employ this type of selection. This type is included to cover all possible decision making points in the service discovery process. Decisions by the Client Application A majority of the solutions select services on the client-end. After receiving a list of feasible services, the client application chooses a service based on service information and additional information provided by the user, operating system, and other bodies. Using this type of decision making process, though, the client must receive a full or partial list of available services. The Fig.4 illustrates the connectivity between the components such as Pervasive Server, Anonymity handler with a Base Station and a cluster of Sensor Nodes. A set of sensor nodes deployed in an environment attached to a base station. During the sensing time, the signals are verified for the registered owners by reaching the base station. If any exceptions carry for the unknown entry, the process of anonymity finding begins. The Pervasive server will be asked for the unknown entry to be added or rejected.

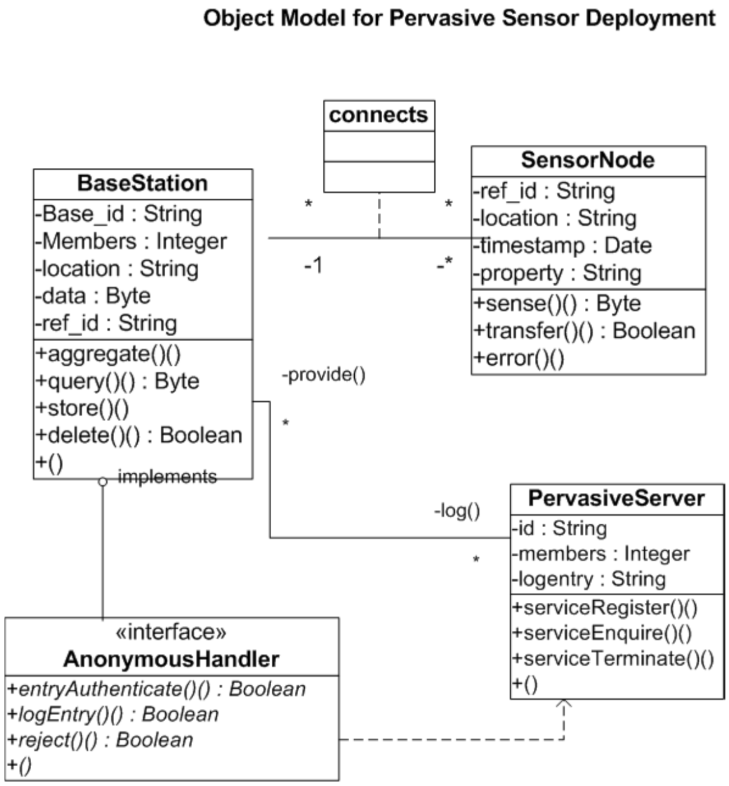


Fig.4 The Class diagram with relationships

Based on the decision making process with guest log based interpretation, the Pervasive Server reports to the base station either for allow or for reject.

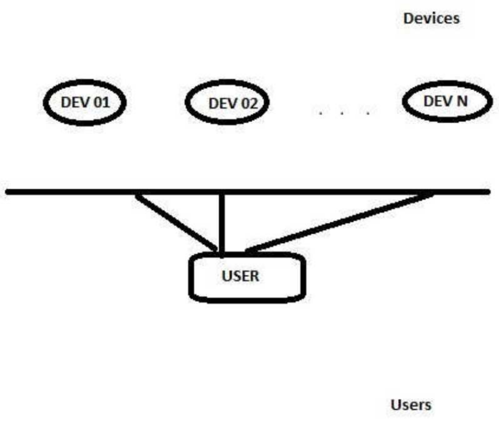


Fig.5 The cardinality between users and nodes

The user can communicate to one or more devices during the real time sensing. In negation, a device can communicate to multiple users. This paradigm is a mandatory process in Pervasive Environments. Many devices could interact with an individual user or many users can interact with a device vice versa. The Cardinality relationship between the devices and users are illustrated in Fig.5 above. The Service entry and dissemination could be carried in Many-to-One aspect for the sensors.

A. VISA Processing Techniques for a Pervasive Space

VISA is a document provided to one for the entry/exit to a region for being some amount of time. Visa provider must be the authority of the Region of Interest (ROI). The Person who receives Visa can be a visitor/guest to the region. Based on the Guest Registry log management in this context of anonymity handling, a Pervasive Server is responsible to issue the visa for a new arrival device or a user. Visa is classified multitude categories in many countries. A Pervasive Space is assumed as a country to be visited and the device/user requires to get a visa from the Server. Short-stay or visitor visa is the commonly required one. The Server identifies a new arrival once the boundary region is touched. On-arrival visa is issued with a time stamp.

Entry Visa Processing Algorithm

Algorithm 1: Entry-Visa Processor

(entry permit and verification in a Pervasive Space)

```
Begin
          Let (variables)
          PR → Pervasive Region
          B(i) → set of boundaries for a PR
           X → an anonymous device
          PS → Pervasive Server
          GR → Guest Log Registry

          If (X is in PS) then
          {
                    declare 'X' as a registered device
                    }
          Else (X is in GR)
          {
                    declare 'X' as a guest device
                    determine a finite time 'T'
                    }
End
```

b. Exit Processing Algorithm for a Pervasive Space

Algorithm 2 : Exit-Visa Processor
(exit processing from a Pervasive Space)

```
Begin
Let (variables are assumed from Algorithm 1)

          If (X expires) then
          {
          deactivate the services provided to 'X'
          mark in 'X' as removed in GR
          }
          Else (X volunteers to quit)
          {
                    cross-verify the GR for 'X'
                    mark in 'X as removed in GR
                    }

End
```

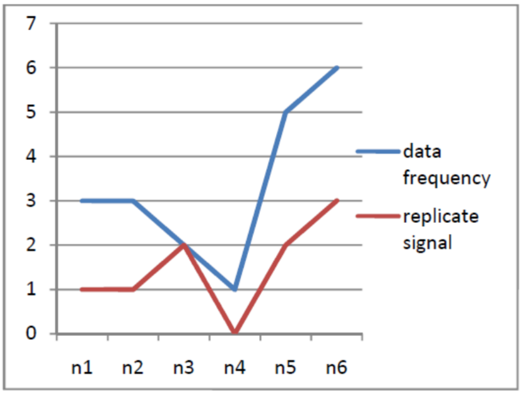


Fig.6. replicated signals over a Sensor Network

In the above Fig.6., the routine data frequency is measured in y-axis, whereas the number of sensors nodes are in x-axis. The signals far outnumbers from the replicate signals. The filtering of the replicate data is accounted. The node 'n4' has no replicated signals out which it transmitted only once. Whereas node 'n6' has three times replicated out of six times transmitted. The frequency of replication is a random measure based on the environmental changes.

VII. CONCLUSION AND FUTURE SCOPE

The proposed model defines anonymity for pervasive computing at the middleware level and classifies the presence of anonymity in unknown scenarios so as to open up the avenues of handling a new user as a guest not a un-trusted entry. The log-based model for anonymous entries is also accounted. Visa processing algorithms for entry and exit provides a virtual fencing to pervasive space. The key research issue is to handle unknown and unauthorized entities into the pervasive networks. Even for the first time enquiry or missing registrations are to be focused for future avenues. The guest registry and log for replicate signals are archived. Future work will be focused on the implementation of the anonymity handler and to evaluate the performance at the application level.

REFERENCES

[1] Vesa Kautto (2001), "Middleware for Pervasive Computing " HUT, Telecommunications Software and Multimedia Laboratory.

[2] Christian Becker, Gregor Schiele, Holger Gubbels, and Kurt Rothermel "BASE -A Micro broker- Based Middleware for Pervasive Computing " University of Stuttgart Institute of Parallel and Distributed Systems (IPVS), Breitwiesenstr. 20-22, 70565 Stuttgart, Germany

[3] Roberto Speicys Cardoso, Pierre-Guillaume Raverdy, and Valeŕie Issarny, "A Privacy-Aware Service Discovery Middleware for Pervasive Environments" , Inria Rocquencourt 78153 Le Chesnay, France.

[4] Cardoso R.S., Raverdy, P.-G and Issarny, V., 2007, in IFIP International federation for Information Processing, Volume 238, Trust Management, eds, Etalle, S., Marsh S.,(Boston:Springer) pp 59-74

[5] Stelios Dritsas, Dimitris Gritzalis a, Costas Lambrinoudakis "Protecting privacy and anonymity in pervasive computing: trends and perspectives", Volume 23 Issue 3, August 2006. pp 196-210

[6] Stephen S. Yau, Fariaz Karim, YuWang, Bin Wang, and Sandeep K.S. Gupta (July 2002), "Reconfigurable Context Sensitive Middleware for Pervasive Computing", Arizona State Arizona State Volume 1 Issue 3, pp 33-40 .

[7] Seth Holloway, Drew Stovall, Jorge Lara-Garduno, and Christine Julien, "Opening Pervasive Computing to the Masses Using the SEAP Middleware " Mobile and Pervasive Computing Group , The University of Texas at Austin , March 2009.

[8] R. Jason Weiss, and J. Philip Craiger (2002), "Ubiquitous Computing ", University of Nebraska–Omaha, Volume 39, Number 4, pp. 44 - 52.

[9] Wassim Masri, Zoubir Mammeri (September 2007), "Middleware for Wireless Sensor Networks: A Comparative Analysis," IFIP International Conference on Network and Parallel Computing Workshops. Pp 349-356

[10] Stephen S.Yau et al., (September 2002) Reconfigurable Context Sensitive Middleware for Pervasive Computing“, IEEE Pervasive Computing,. pp 33-40

[11] Tinghuai Ma et al., (2011) “Privacy Preserving in Ubiquitous Computing: Classification and Hierarchy”, COMSIS Journal, Vol 8, No. 4,. pp 1185-1206.

[12] Miyuki Imada, Masakatsu Ohta, Masayasu Yamaguchi, Sun Yong Kim, (2008) "LooM: An anonymity quantification method in pervasive computing environments", International Journal of Pervasive Computing and Communications, Vol. 4 Iss: 1, pp.110 – 123

[13] Chi Lin; Guowei Wu; Lin Yao; Zuosong Liu, "A Combined Clustering Scheme for Protecting Location Privacy and Query Privacy in Pervasive Environments," *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* , vol., no., pp.943,948, 25-27 June 2012 doi: 10.1109/TrustCom.2012.19

[14] Trcek, D.; Brodnik, A., "Hard and soft security provisioning for computationally weak pervasive computing systems in E-health," *Wireless Communications, IEEE* , vol.20, no.4, pp.22,29, August 2013.doi: 10.1109/MWC.2013.6590047

[15] G.Radhamani, K.Vanitha and D.Rajeswari. “Classification and Handling of Anonymity in Pervasive Middleware”. *International Journal of Computer Applications* , Vol. 17, No.6, pp. 28-31, March 2011. Published by Foundation of Computer Science.