IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Principles of Ubiquitous Computing Systems

Aasha S. A[*1], M. Sravanthy[2], Prof. T.Venkat Narayana Rao[3]

[*1,2] B.Tech, Final Year Students, Hyderabad Institution of Technology and Management, India

[3] Professor, Department of C.S.E, Guru Nanak Institutions Technical Campus Ibrahimpatnam, Hyderabad, A.P, India

tvnrbobby@yahoo.com

Abstract

This paper provides a concise summary of pervasive computing and also the challenges faced in computer systems research posed by the emerging field of pervasive computing. This papper probes the relationship of this new field to its predecessors distributed systems and mobile computing. First, the application data and the functionality need to be held apart, so that they can graciously evolve in a global computing infrastructure. Second, the applications must be able to acquire any resource they need at any time, so that they can continuously provide their services in a highly dynamic environment. Third, pervasive computing requires a common system platform, which allows the applications to run across the range of devices and to be automatically distributed and installed. This paper also discusses about the growing debate over privacy, safety and environmental implications. Finally the paper closes with a discussion of the research necessary to develop these capabilities.

Keywords: Ubicomp,services,sensors,networks,microprocessors,heterogeneous.

Review of the Literature

Ubiquitous computing (ubicomp) is an expeditiously developing area of information and communications technology (ICT). The term refers to the increasing integration of ICT into people's lives and environments, made possible by the growing availability of microprocessors with inbuilt communications facilities. Ubiquitous computing has many potential applications, from health and home care to environmental monitoring and intelligent transport systems[1] .

Usage control has considered as the next generation access control model with distinguishing properties of decision continuity. In this paper, we present a usage control model to protect services and devices in ubiquitous computing environments, which allows the access restrictions directly on services and object documents. The model not only supports complex constraints for pervasive computing, such as services, devices and data types but also provides a mechanism to build rich relationships between models and objects. Finally, comparisons with related works are analyzed. In his first ground-breaking 1991 paper "The Computer for the 21st century" , Mark Weiser termed pervasive or ubiquitous computing. His vision of pervasive computing is related to the creation of environments which involves computing and integrated communication with the end users. Environments in pervasive computing includes the interaction, coordination, and cooperation of numerous, casually accessible and invisible computing devices[3]. These devices are connected via wireless and wired links and are connected to the global networking infrastructure. This provides more of relevant information and integrated services. The existing approaches to build various distributed applications, which include client/server computing, which is ill suited to meet different challenges. They are all targeted at smaller and less dynamic computing environments that lack in sufficient facilities to manage changes in the network configurations. Network computing devices will proliferate in the landscape of the users which are embedded in objects ranging from home appliances to clothing. Applications would have greater awareness of context, and thus it enables more intelligent services that can reduce the burden of the users to direct and interact with the applications. Mobile computing and communication are one of the crucial parts of the ubiquitous computing system. The coordination between these devices is maintained through communication, which can be wireless or wired. Due to the advent of Bluetooth and Ad hoc networking technologies, the wireless communication has overtaken the wired counterpart. With the reduction in size and cost of processor chips it is possible to implement it in every field of life. Nowadays about 99% of the processors are manufactured for embedded devices compared to the PC applications.

The interface between Voice and Gesture recognition along with steer able would make the interactions and use of these devices more user friendly. Efficient security and privacy policies along with the power management, can enhance the performance of such systems. The predominant future of ubiquitous computing, is to design a user centric and application oriented computing environment. Such environments may vary from the traditional computing models as, the physical space within the environments which are supported by associated hardware and software will speed up the interactive information exchange between users and the space. Due to the availability of such cheap computing devices, the wireless networks are making such spaces possible. It's not necessary for a user to log into a single personal computer as in traditional computing environments, but communicates with a variety of computing devices in the space. Scalable configuration is a substantial aspect in such a created space as the same space is often used for various tasks at various times. Contextual information, such as the current users in the space, or the current activity in the space, is essential for the configuration. The widely use of advanced technology in field of computing, networking and sensor has expedited the development of ubiquitous computing, that would help in enabling various convenient applications. Different users, heterogeneous sensors, share resources and information in ubiquitous computing environments and so on[4]. Security issues play a vital role in the environments as the contextual information such as sensor locations and applications evolve into an integral part of the system authorization. On the other hand, the application and user interaction with the pervasive environment poses a new security challenge to the traditional user-password approach for security of the computer. The heterogeneous devices and mobile users makes the security management complicated in dynamic pervasive computing environments, especially the access the authorized users posses ,as it is a basic security requirement for guaranteeing user's privacy, information confidentiality, availability and integrity[2].

Background

The number of embedded microprocessors is expected to increase dramatically over the next decade making the devices ever more pervasive. These microprocessors will range from a few Millimeters in size (small sensors) to several meters (displays and surfaces). They may be interconnected via wireless and wired technologies which would be broader, with more capable and efficient networks. Ubiquitous computing systems (PCS) and services are a form of intelligence ,which may lead to a greater degree of user knowledge of control over, the surrounding environment, either at home, or in an office or in a car. For instance, if a 'smart' electrical appliance could detect its own impending failure and it can notify its owner as well as the maintenance company, to arrange a repair. Ubiquitous computing has been under development for almost 15 years and yet it is far from becoming a fully operational reality. Although the development of battery technologies and the user interfaces pose some particular challenges, some core technologies have emerged. It would take a span of 5-10 years for the complete PCS to be completely available and this scenario would depend upon the market forces, industry, public perceptions and the effects of any policy/regulatory frameworks. While world with digital information. This advent basically emphasizes the use of mobile technologies, geographical arrangement of systems and internet-linked databases to distribute information via personal digital companions. Such devices could come in several forms: children might have Ubiquitous computing systems will depend on the interlinking of independent electronic devices into broader networks. This can be acquired via both wired (such as Broadband (ADSL) or Ethernet) and wireless networking technologies (such as WiFi or Bluetooth), with the devices themselves being adept of assessing the most effective form of connectivity in any given scenario. The effective development of development is still at an early stage there have been numerous calls for more a widespread debate on the association of ubiquitous computing[10].

Ubiquitous Computing Technologies

Ubiquitous computing involves three different converging areas of ICT they are computing devices, communications in connectivity and user interfaces.

Devices

PCS devices are precise to assume many different forms and sizes, from different handheld units that are similar to mobile phones and to near-invisible devices that are set into 'everyday' objects . These allow to communicate with each other and act 'intelligently'. Such devices can be categorized into three[6].

1. Sensors input devices that detect environmental changes, user behaviors, human commands etc.
2. Processors electronic systems that interpret and analyze input-data.
3. Actuators Output devices that respond to processed information by altering the

environment via electronic or mechanical means.

There are various visions for the future development of PCS devices. Assorted research groups endeavor to produce networks of devices that could be as small as a grain of sand. The idea is that each one would function independently, with its own power supply, and could also communicate wirelessly with the others too. These could be disseminated throughout the environment so as to form a thick, but almost invisible, ubiquitous computing network, thus eliminating the necessity for overt devices. At the other extreme, the augmented reality would include overlaying the real them integrated into school bags, whereas adults might use devices more closely resembling the personal digital.

Connectivity

Ubiquitous computing systems rely on their degree of interoperability, as well as on the convergence of standards for wired and wireless technologies.

User interfaces

User interfaces represent the point of contact between ICT and the human users. For example with a personal computer, the mouse and keyboard are used to input information, while the monitor will provide the output[11]. With PCS, new user interfaces are being developed that will be capable of sensing and supplying more information about the users, and the broader environment, to the computer for processing. With future user interfaces the input might be visual information - for example recognizing a person's face, or responding to gestures. It may also be based on sound, scent or touch recognition, or other sensory information like temperature. The output might also as the technology develops. Three very different forms of human-computer interaction are postulated: active, passive and coercive[9].

Human-Computer Interactions (HCIs)

Active

Users can have overt control over ubiquitous computing technologies as well as the devices in the environment. The users are allowed to issue direct spoken or written commands through language-based interfaces. Digital companions such as smart phones and PDAs can act as personal and wireless control units in an intelligent environment[8].

Passive

Ubiquitous computing would disappear into the background if people would no longer realize that they are interacting with computers. The technology will sense and respond to human activity, behavior and demands intuitively and intelligently similar to lighting altering in reaction to users' location, mood and activity.

Coercive: Ubiquitous computing could control lives and environments either overtly or covertly. Decisions that are made by the developers such as programming a system in accordance with health and safety regulations, the development errors, unintended device interactions and malicious interference could all lead to loss of user control, and possibly have negative implications for users. The following tables1 to 5 illustrates the difference between Traditional Networking And Ubiquitous Computing on different criteria.

Issues : There are engineering problems to be solved before the envisaged applications of PCS can become a reality. Moreover, the operation of PCS raises for a genuine purpose only. However, the opportunities for activities like 'data mining' could be vastly increased with PCS. Data mining activities involves processing large quantities of data to spot patterns and trends. In terms of consumer data, this lead be in any of these formats[12]. The technology could 'know' the user (for example through expressed preferences, attitudes, and behaviors) and tailor the physical environment to meet some specific needs and demands. However, designing systems that can adapt to unforeseen situations presents considerable engineering challenges. There is debate over the degree of control the users will have over future ubiquitous computing user interfaces plenty of questions over privacy, security, safety and environmental impact. Many of these issues occur already with ICT, such as the Internet or mobile phones. However, the potential ubiquity and integration of PCS into the environment poses some additional challenges.

Engineering issues: The UK Computer Research Centre (UKCRC), highlights specific issues including the current lack of low cost technologies to locate devices and the lack of suitable power sources. Also the complexity of PCS systems which means that their communications, software and hardware are likely to suffer from faults. These might be accidental or the result of deliberate attempts to damage the system. The National Consumer Council (NCC) suggests that there may be questions over liability – for example, if systems are interconnected it will be harder to establish who is responsible if something goes wrong. The NCC also points out those faulty systems may be harder to repair because of the degree of interconnection.

Privacy: The opportunities for data interception, theft and 'ubiquitous surveillance' (official and unofficial) will be heightened with personal information being collected, transmitted and stored in greater volume. In places considered private, such as the home, PCS

could be embedded. With the risk of breaches of privacy, data on many aspects of personal life could be recorded and stored. Data that can be collected without a person's knowledge or consent may mean the advent of ubiquitous computing. Some argue that this could violate the existing data protection law. This law also requires that the personal data should be collect to more effective targeted marketing. However, some argue that there is the potential to violate existing legislation because data mining activities can detect unknown relationships in data. There is debate over how privacy can be defended while still realizing the benefits of pervasive computing, and whether a new legislation will be required.

Safety and security: Ubiquitous computing often rise to debate over safety. Breaches of security exposes vulnerable individuals to malicious acts within their own homes – for example the withholding or over-prescribing of medications[7].

Technological measures: At the design level of PCS if appropriate procedures and protocols are integrated rather Data that require transmission, should be encrypted and sent anonymously (without reference to the owner Security should be treated as an ongoing and integral part of PCS.

These principles are accepted by many PCS research and development centers. However, consumer groups such as the NCC say that developers need to pay more consideration to the privacy issues. The NNC argues that in the case of RFID, privacy issues were considered only late in development and have still not been fully addressed.

Environment

Through the miniaturization of PCS devices the consumption of natural resources might be reduced, any gains are likely to be offset by technological proliferation. This may be compounded by the troubles of cvcvctreating microelectronic waste embedded in ther objects and has implications for recycling due to the possibility of such waste contaminating recycling channels.

Taxonomy

Pervasive computing constitutes a major evolutionary step in a line of work dating back to the mid-1970 as shown in figure 1.. Distributed systems and mobile computing are the two distinct earlier steps in this evolution. Some of the technical problems faced in pervasive computing correspond to the problems already identified and studied earlier in the evolution. In some cases, existing solutions apply directly and in other cases, the demands of pervasive computing are sufficiently different that new solutions have to be sought. There are also few new problems introduced by pervasive computing that have no obvious mapping to problems studied earlier. In the rest of this section, we try to sort out this complex intellectual relationship and to develop taxonomy of issues characterizing each phase of the evolution[5].

Difference Between A Traditional Networking And A Ubiquitous Computing.

Than implemented retrospectively, it is argued that privacy, safety and security can be protected in a better way. Three measures frequently plays a vital role in establishing robust security measures. The volume of transmitted data should be kept to a minimum.

Non-ionizing radiation is a by-product of the wireless signals that are apt to be used to connect ubiquitous computing devices into broader networks. As these devices may carry close to the body (more so than current ICT) and remain constantly activated, there may be an increased risk from exposure of body tissues to the potentially damaging effects of such radiation.

Digital divide

For those who do not use the technology (whether it be through choice, lack of income or skills) there is a risk of technological and social isolation. For instance, banking, retail services and education are likely to be delivered through PCS embedded within smart homes and this could lead to some consumers being deprived of access and freedom of choice. Ubiquitous computing can also improve the lives of those with illnesses and disabilities, and the elderly. However, it's extensively agreed that in order for these groups to benefit from PCS, their needs and capabilities should be considered from an early stage in the design of the system [9].

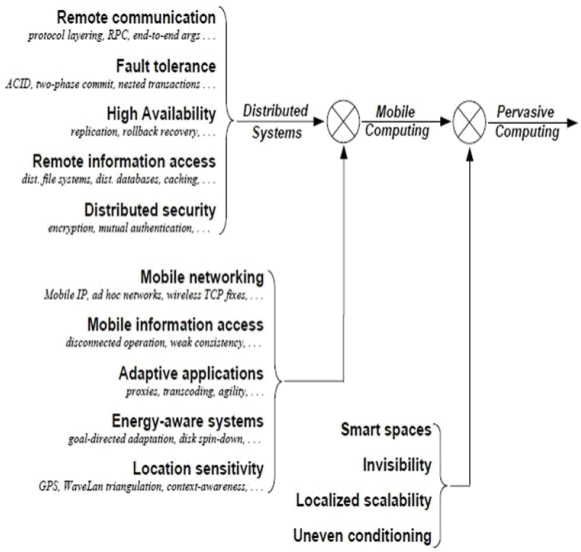

Figure 1 : Taxanomy of Prevasive computing.

Distributed Systems

At the intersection of personal computers and local area networks the field of distributed systems arose. The research followed from the mid-1970's through the early 1990's created a conceptual framework and algorithmic base that has proven to be of enduring value in all work which involves two or more computers connected by a network that can be mobile or static, wired or wireless, sparse or pervasive. This body of knowledge spans in many areas that are foundational to pervasive computing.
Remote communication, includes protocol layering, the use of timeouts, remote procedure call and the use of end- to-end arguments in placement of functionality[6] .

Fault tolerance, that includes nested transactions, distributed and atomic transactions, and two-phase commit.

High availability, that includes optimistic and pessimistic replica control, mirrored execution, and optimistic recovery. Remote information access, that includes caching, distributed databases, function shipping and distributed file systems, Security, includes encryption-based mutual authentication and privacy.

Mobile Computing

In the early 1990s the appearance of full-function laptop computers and wireless LANs led researchers to confront the problems that arise in building a distributed system with mobile clients. Thus the field of mobile computing was born. Four key constraints of mobility forced the development of specialized techniques although many basic principles of distributed system design continued to apply. These constraints are: unpredictable variation in lowered trust, network quality and robustness of mobile elements, limitations on local resources imposed by weight and size constraints, and concern for battery power consumption. Mobile computing is still a very active and evolving in the field research, whose body of knowledge awaits codification in textbooks. So far the results achieved can be grouped into the following broad areas:

Mobile networking, includes Mobile IP , ad hoc protocols, and techniques for improving TCP performance in wireless networks .

Mobile information access, includes disconnected operation, bandwidth-adaptive file access, and selective control of data consistency.

Support for adaptative applications, includes trans coding by proxies and adaptive resource management.

System-level energy saving techniques, such as energy aware adaptation, energy-sensitive memory management, and variable-speed processor scheduling

• Location sensitivity, includes location sensing and location-aware system behavior.

Challenges for Implementation

With most of the new advanced technologies, obstacles are encountered and they must overcome them to succeed. The Tabs, Pads, and Boards that are developed at XEROX PARC are no different. Mark Weiser has stated that Ubiquitous computing is a very difficult task. The name alone implies computers everywhere but they must dissolve into the background in order to achieve success. To do this, ubiquitous computing devices must overcome six problems as stated below:

1. The "Accidentally" Smart Environment
2. Impromptu Interoperability
3. No Systems Administrator
4. Social Implications of Aware Technologies
5. Reliability
6. Inference in the Presence of Ambiguity

Applications

Ubiquitous computing could have a wide range of applications, many of which may not yet have been identified. Applications includes healthcare, home care, transport and environmental monitoring are most frequently cited, as discussed below. Research is taking place in industry and academia, often collaboratively, and some government activities are underway

Government Initiatives

The Next Wave Technologies and Markets Programme was launched in 2001, which was a government initiative. This was established as a virtual interdisciplinary research collaboration, dedicated for the development of ubiquitous computing technologies and establishing potential markets. Through this initiative which includes PCS applications in health care, domiciliary care, 'integrated home environments', cities/buildings and environmental sensing, which are expected to report towards the end of 2006, seven projects have been funded.

Healthcare

Ubiquitous computing offers opportunities for future healthcare provision, which includes both for treating and managing disease, and for patient administration. For instance, remote sensors and monitoring technology will allow the continuous capture and analysis of patients' physiological data. To any detected irregularities medical staff could immediately be alerted. Data collection provides more accurate pattern/trend analysis of long-term conditions such as heart disease, diabetes and epilepsy. Wearable sensors might offer greater patient mobility and freedom within hospitals that would save both time and money by decreasing the

need for repeated and intrusive testing. Hospital administration could also be transformed. The patients might be tagged with wristbands containing digital photographs and medical notes. These wristbands would help patients to be traced more efficiently through hospital administration systems which reduce the risk of misidentification and treatment errors.

Domiciliary Care

There will be a rise in the proportion of people over 65 years old in most developed countries, over the next 20 years. These people may increasingly require care from a diminishing working population. PCS may help to address the consequences of this imbalance. Improved methods for monitoring health and wellbeing could allow people to live longer in their own homes. For example, sensors embedded in items of clothing, might allow constant monitoring of heart rates, body-mass index, blood pressure and other physiological variables. Further, sensors embedded throughout the home could detect movement and fluctuations within the ambient environment (such as temperature change) to alert care-workers to any irregularities. Visual displays or voice messages also helps people to remind take medications, while video telephones could provide personal contact with friends, family and careers.

Environmental monitoring

The methods to monitor the environment can be improved with the help of Ubiquitous computing. It will allow for the continuous real-time data collection and analysis via remote, wireless devices. However, for PCS developers, this poses certain significant challenges. Devices may be required to resist harsh environmental conditions (such as heat, cold and humidity). Due to this there may be a risk of the device being too costly or impractical to recover once deployed; thus they will have to be cheap and, where possible, environmentally sensitive. As a systems will need to operate over long periods of time, which requires high levels of energy efficiency and robust energy supplies i.e. Power is also a challenge.

Intelligent transport systems

In the development of intelligent transport systems to try to relieve these costs, Ubiquitous computing technologies are being employed. Such systems bring together information and telecommunications technologies in a collaborative scheme to improve the efficiency, safety and productivity of transport networks. Electronic devices could directly be integrated into the transport infrastructure, and into vehicles themselves, for better monitoring and managing the movement of vehicles within road, rail, air and sea transport systems. Computers are already incorporated into modern cars via integrated mobile phone systems, parking complex engine management systems and sensors. Intelligent transport systems take this process further by introducing 'intelligent' elements into vehicles. Vehicles tend to become capable of receiving and exchanging information ‘on the move’ via wireless technologies and will also be able to communicate with devices integrated into transport infrastructure, alerting drivers to traffic congestion, accident hotspots, and road closures. Making use of alternative routes could be relayed to in-car computers, speeding up journey times and reducing road congestion. This would help in adding coordination to the road transport system.It also enabling people and products to travel more securely and efficiently. Greater communication and coordination between different transports sectors (road, rail, air, etc.) may help in accomplishing integrated transport policies.

Future Scope

The table I, II ,III and IV discussed in the section below states a clear distinction between traditional and pervasive computing environments based on parameters like trust, privacy and and Identity .

Invisible : "Smart" environments would be embedded with computing technologies that would be mostly out- of-sight. Architecture will gain many more capabilities – but with less visual clutter.

Socialization : Interactions with architecture will be more social in nature as "Smart" buildings will illicit a more social response from different occupants as computers user interfaces which would embed themselves within the architecture.

Decision-Making: Smart environments would help the occupants to make better choices as they go about their everyday lives. At various key moments within many architectural experiences, a good architectural design would make "smart" environments really helpful. Such an architecture will be more proactive than passive.

Emergent-Behavior: Buildings are now becoming more and more kinetic in both form and function. Their movements and constructed designs come together dynamically to yield different behaviors which would make them more adaptive. Buildings will learn how to learn - in order to run efficiently and aesthetically.

Information: Processing: Since architecture will be gaining a type of "nervous system", the information processing will be gaining a whole new meaning. Architecture would change from crunching data to making sense of data; thus, eliminating our need to constantly input adjustments.

Enhancing Experience: As computers ubiquitously embed themselves in our environments, the sensors and actuators will create "smart" environments where architectural space will be goal-oriented. Therefore, more occupant needs would be met.

Convergence: Much of our environment will be supplemented with various interconnected digital technologies. With such interconnectivity, a new type of "sharing" will serve to eliminate many mundane task and fewer errors might, occur as systems pull data from shared digital locations.

In addition to the issue of security, the hurdles that ubiquitous computing companies face must overcome include reducing the cost of the microchips themselves. Implanting microchips on everything would require the production of a variety of different types of microchips to meet the needs of various objectives and we will need to produce hundreds of millions of such chips. The development of affordable and safe microchips would require great leaps in the production technology, for which much research and development has yet to be done.

Just to give you an idea of where we are now, it should be possible to supply hundreds of millions of microchips that offer a simple number reading capability at five cents per chip within a span of two or three years . At that point the chips containing microprocessors or sensors will still cost several cents. But it will likely be 10 years or so before the distributors will be ready to replace their bar-code systems with the new microchips.

Taking the consideration of cost into account, I foresee that the initial application will likely be in the area of traceability for products such as medicines and food where safety is a concern and very expensive products for which the merit of traceability exceeds cost considerations. The fields of application for ubiquitous computing would expand in a gradual process as the various challenges, which include cost considerations and production techniques, are overcome. I would not be surprised if it takes 10 years before ubiquitous computing begins to take shape in the way that we visualize it now. In fact, I feel it is important to take the time to do things right ,especially with a regard to achieve the necessary social consensus on privacy and security issues.

On Going Research

- Project Oxygen,being pursued By MIT.
- Project Endeavour, University of California
- Berkeley university
- Project Aura, Carnegie MellonUniversity

Conclusion

Pervasive Computing is an extremely powerful device for creating various new environments. It is defined as the trend towards increasingly ubiquitous, connected computing devices in the environment, a trend being brought about by a convergence of advanced electronic - and particularly, wireless - technologies and the Internet. Pervasive computing will be a fertile source of challenging research problems in computer systems for many years to come. Solving these problems will require us to broaden our discourse on some topics, and to revisit long-standing design assumptions in others. We will also have to address research challenges in areas outside computer systems. These areas include human-computer interaction (especially multi-modal interactions and human-centric hardware designs), software agents (with specific relevance to high-level proactive behavior), and expert systems and artificial intelligence (particularly in the areas of decision making and planning). Capabilities from these areas will need to be integrated with the kinds of computer systems capabilities discussed in this paper. Pervasive computing will thus be the crucible in which many disjoint areas of research are fused. When describing his vision, Weiser was fully aware that attaining it would require tremendous creativity and effort by many people, sustained over many years. Pervasive computing provides an attractive vision for the future of computing. Well, we no longer will be sitting down in front of a PC to get access to information. In this wireless world we will have instant access to the information and services that we will want to access with devices, such as Smartphones, PDAs, set-top boxes, embedded intelligence in your automobile and others, all linked to the network, allowing us to connect anytime, anywhere seamlessly, and very importantly, transparently.

References

[1] J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. State of the Practice of Intrusion Detection Technologies. Technical Report CMU/SEI-99TR-028, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA, 2000.

[2] Dong, M., Zheng, L., Ota, K., Guo, S., Guo, M., Li, L.: Improved Resource Allocation Algorithms for Practical Image Encoding in a Ubiquitous Computing Environment. Journal of Computers 4(9), 873–880 (2009)

[3] Dey, A.K., Abowd, G.D., and Salber, D., A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. Human-Computer Interaction Journal, Special Issue on Context-Aware Computing, 16, 1, 2001.

[4] M. Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems," presented at ACM UbiComp 2001, Atlanta, GA, 2001.
[5] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," presented at 4th International Conference on Ubiquitous Computing, 2002.
[6] F. Stajano, Security for Ubiquitous Computing: Halsted Press, 2002.
[7] L. Kagal, T. Finin, and A. Joshi, "Trust-Based Security in Pevasive Computing Environments," IEEE Computer, 2001.
[8] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 1996.
[9] C. English et al. Dynamic Trust Models for Ubiquitous Computing Environments. In Proceedings of the 4th International Conference on Ubiquitous Computing, Goteberg, Sweden, September 2002.
[10] B. Shand, N. Dimmock, and J. Bacon. Trust for Ubiquitous, Transparent Collaboration. In Proceedings of the 1st IEEE International Conference on Pervas ive Computing and Communications, Dallas – Ft.Worth, TX, March 2003.
[11] R. Grimm, System Support for Pervasive Applications, doctoral dissertation, Dept. of Computer Science and Eng., Univ. of Washington, 2002.
[12] L. Arnstein et al., “Systems Support for Ubiquitous Computing: A Case Study of Two Implementations of Labscape,” Proc. Int’l Conf. Pervasive Computing, LNCS 2414, Springer-Verlag, 2002, pp. 30–44.
[13] C. Becker and K. Geihs. Generic QoS-support for CORBA.In Proceedings of 5th IEEE Symposium on Computers and Communications (ISCC’2000), 2000.
[14] C. Becker, G. Schiele, H. Gubbels, and K. Rothermel. Base- a micro-broker-based middleware for pervasive computing. In Proceedings of the IEEE international conference on Pervasive Computing and Communications (PerCom), Mar.2003.
[15] L. Bergmans and M. Aksit. Composing crosscutting concerns using composition filters. Communications of the ACM, 44(10), Oct. 2001.

Criterion	Traditional Computer Networks	Pervasive Computing Environments
User Interaction	The user's intervention is considered necessary to initiating the connection to a specific device to network.	The devices connect automatically to a network without the users' participation.
	The standard authentication are used for controlling access to network resources.	Standard authentication protocols cannot be readily used in pervasive system environments, because they cannot provide the required mobili and scalability needed I such environments.
	The computing model is based on localized desktop devices, where there is one–to–one relationship between the machin and user.	Computing is highly distributed into the surroundings and onto the user's personal digital devices. There is a many–to-one relationship between the machine and user.
	The user is conscious about the interaction with the desktop devices, where all information supplied by the user is under full control of the user at all times.	The user is unconscious about the interaction with many devices and The connection between these devices will be unknown. The user is unaware of what information is sent to what device at any particular point in time

Table 1: Comparison between Traditional and Pervasive Computing Environments with respect to User Interaction

Criterion	Traditional Computer Networks	Pervasive Computing Environments
Trust	In traditional networks, trust relationships are established based on identity, recommendation from third trusted party (TTP) or reputation and it also means a lot for it controls access to various resources	In pervasive computing, trust relationships are established using the identity of a user and their context And, trust also portrays how accurate the information is.
	Trust relationships in traditional systems are static in nature. Once the relationship is formed between the trustier and trustee, it remains valid until it is broken explicitly by the trustier. Here traditional systems are quite simple.	In pervasive systems, the relationship is more dynamic and based on historical information and risk assessment. Every ime a device requires access to a resource, the trust relationship is re-assessed according to the device's current and previous status. relationship is rather complex.

Table II.Comprision between Traditional and Pervasive Computing Environments with respect to trust

Criterion	Traditional Computer Networks	Pervasive Computing Environments
Privacy	In traditional networks, privacy is less problematic as despite people are concerned about holding and storing their persona information, they know where this information is stored and used.	In pervasive computing environments, privacy is more significant, for people are less willing to exchange their personal information with the environment. This is because they are unaware or unsure where their information being held and used.
	There is a lower risk in storing personal information on traditional networks, as they can only be accessed by authorize users.	There is a higher risk involved in storing personal information on pervasive and mobile systems, as they may be accessed anywhere an by anyone.

Table III. Comparison between Traditional and Pervasive Computing Environments with respect to privacy

Criterio	Traditional Computer Networks	Pervasive Computing Environments
Identity	In traditional systems, the user identity is established and verified by using the common authentication methods, su as checking a password, swiping a smartcard, or other means of provi that the user is who they claim to be.	In pervasive computing environments, more subtle ways are required establish the user identity, because common authentication protocols may not be adequate
	The risk of identity theft is mainly linked to stealing a password or credentials which an attacker will use to impersonate someone else.	The risk of identity theft is higher in pervasive computing because th is a higher risk of losing the user's device; such as PDA or a mobile phone, where identity is normally stored.

Table IV. Comparison between Traditional and Pervasive Computing Environments with respect to identity