ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Ultimate Disguised Computing Its Variability and Challenges.

Edvina Crasto[1], Chithra[2], Rama Moorthy H [3]

Department of CSE, SMVITM-Bantakal, Karnataka, India[1,2]

Assistant Professor, CSE, SMVITM-Bantakal, Karnataka, India[3]

Abstract: The main goal of Ubiquitous computing is that it enhances computer use by making many computers available throughout the physical environment, as well as making them effectively invisible to the user. Mobile computing and pervasive computing briefs the major evolutionary steps in the field of research during the mid-1970s. Through the interconnected devices and services, pervasive computing promises seamless integration of digital infrastructure into our day to day lives. Now the focus of current research is on how to connect new devices and build useful applications to enhance functionality, the security and privacy issues in these environments have not been explored in any depth. While traditional distributed computing research tries to abstract away physical location of resources and users, pervasive computing applications often exploit physical location as well as other context information of users and resources to enrich the user experience. In this paper we have discussed about the challenges in computer systems research posed by the emerging field of pervasive computing. Initially it compares the relationship of this new field to its predecessors: distributed systems and mobile computing.

Keywords: Ubicomp, Teleporting, UNL.

I. INTRODUCTION

The benefit of that idea was the creation of environments saturated with communication capability and computing, but also gracefully integrated with human users. [1].

The concept in computer science and software engineering where computing is made to appear everywhere and anywhere is called Ubiquitous computing (ubicomp). Compared to desktop computing, ubiquitous computing can occur in any location, using any device, and in any format. A user interacts with various forms of the computer, including laptop computers, tablets and terminals in objects used in day to day life such as a pair of glasses and fridge.

The basic technologies to support ubiquitous computing include Internet, networks, operating system, advanced middleware, mobile code, microprocessors, sensors, new I/O and user interfaces mobile protocols, location and positioning and new materials.

This new technology is also called as pervasive computing, ambient intelligence, [2] ambient media [3] or 'every ware'. [4] Each term describes slightly different ideas.

Ubiquitous computing contains a broad range of research topics, mobile networking, and mobile computing, including distributed computing, context-aware computing, location computing, sensor networks, human-computer interaction, and artificial intelligence. Pervasive computing will provide users with a comfortable and convenient information environment that blends physical and computational infrastructures into an integrated habitat. This habitat will show a proliferation of hundreds or thousands of computing devices and sensors which will provide specialized services, and offers new functionality, and increases productivity and interaction. The realization of this paradigm in computing is not far-fetched. A common man today already has a vast numbers of electronic gadgets consumer devices, and gizmos that already have microcontrollers, processors, and memory chips embedded into them, like TVs, VCRs, washers and dryers.

II. BACKGROUND STUDY

Mark Weiser framed the term "ubiquitous computing" during 1988, while his tenure as Chief Technologist of the Xerox Palo Alto Research Center (PARC). Along with PARC Director and Chief Scientist John Seely Brown, Weiser wrote few of the earliest papers on the topic, largely describing it and sketching out its main concerns.

Realizing that the expansion of processing power into day to day scenarios would necessitate understandings of cultural, social and psychological phenomena beyond its proper ambit, Weiser had influenced by various fields besides computer science, along with "philosophy, phenomenology, psychology, anthropology, post-Modernism, sociology of science and feminist criticism". He was specialized about "the humanistic origins of the 'invisible ideal in post-modernist thought'", [8] indicating as well the ironically dystopian Philip K. Dick novel Ubik.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Andy Hopper from Cambridge University UK initiated and displayed the concept of "Teleporting" - where applications is present with the user anywhere he/she moves.
Andy Hopper at Cambridge University, experimented on the "Active Badge System", that is an advanced location computing system in which personal mobility which is merged with computing. Bill Schilit (presently at Google) even did little past work on this field, and involved in the early Mobile Computing workshop held in Santa Cruz during 1996. Dr. Ken Sakamura of the University Of Tokyo, Japan heads the Ubiquitous Networking Laboratory (UNL), Tokyo together with as the T-Engine Forum. The joint aim of Sakamura's Ubiquitous Networking specification and the T-Engine forum, is to make able any day to day device to broadcast and retrieve information.

MIT has also provided significant research in this area, notably Things That Think consortium (directed by Hiroshi Ishii, Joseph A. Paradiso and Rosalind Picard) at the Media Laband the CSAIL effort known as Project Oxygen and few main contributors including Cornell University's People Aware Computing Lab, , Intel Research and Equator,Ajou University UCRi& CUS, University of Washington's Ubicomp Lab (directed by Shwetak Patel), , NYU's Interactive Telecommunications Program, Georgia Tech's College of Computing, UC Irvine's Department of Informatics, Microsoft Research.
Indus Valley civilization: initially known permanent and predominantly urban settlement that grew from 3500 BC to 1800 BC boasted of an advanced and thriving economic system. Its citizens practiced agriculture, domesticated animals, made sharp tools and weapons from copper, bronze and tin and traded with other cities.[6] Evidence of well laid streets, layouts, drainage system and water supply in the valley's major cities, Harappa, Lothal, Mohenjo-daro and Rakhi garhi reveals their knowledge of urban planning.

III. RELATED FIELDS

Pervasive computing indicates a major evolutionary step in a line of work during the mid-1970. Two unique steps in this evolution are mobile computing and distributed systems. Some of the technical problems in pervasive computing relates to problems previously identified and researched earlier during the evolution. While in some of those cases, solutions that existed were applied directly; in some other cases, the requirements of pervasive computing are quite different that new solutions have to be sought.

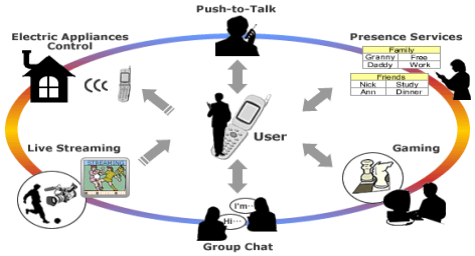

Figure 1: Showing the varied fields of ubiquitous computing.

A. Mobile Computing:

The availability of laptop computers and wireless LANs in the early 1990s led researchers to face the issues that arise in composing a distributed system with mobile clients. The field of mobile computing thus emerged. The four main key constraints of mobility led to the development of specialized techniques. These constraints are: lowered trust and robustness of mobile elements, and concern for battery power consumption, unpredictable variation in network quality, and limitations on local resources imposed by weight and size constraints. Mobile computing is the most active and evolving area of research. The results obtained so far can be grouped into the following broad areas:

- Mobile networking, ad hoc protocols, including Mobile IP, and techniques for improving TCP performance in wireless networks.
- Mobile information access, which includes disconnected operation, selective control of data consistency and bandwidth-adaptive file access.
- Support for adaptive applications, as well as transcoding by proxies and adaptive resource management.
- System-level energy saving techniques, such as variable-speed processor scheduling, energy aware adaptation, and energy-sensitive memory management .
- Location sensitivity, as well as location-aware system behavior and location sensing and Pervasive Computing:
- Pervasive computing is a surrounding saturated with computing and communication capability, but also gracefully integrated with users that it becomes a ‘‘technology that disappears.’’ Since motion is an important part of day to day life, this kind of technology must support mobility; else, a user will be aware of the technology by its absence when he moves. Hence, the research of pervasive computing also includes features of mobile computing, but goes much further. Refer Fig1.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

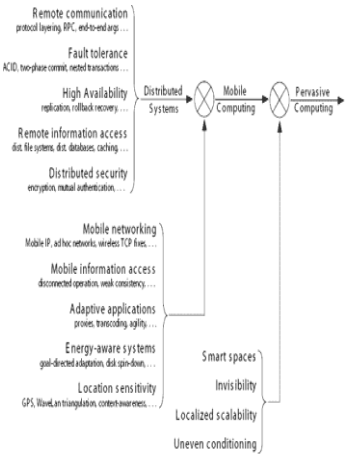

Figure 2: Evolution of Mobile and Pervasive Computing from Distributed Systems.

As Figure 2 shows, pervasive computing shares various research themes which is common to mobile computing. [6] As well as, it addresses four key issues:

- Smart Spaces: fusing computing infrastructure in building infrastructure brings together two environments that have been separate until now. The combination of these environments enables mutual sensing and control of these environments.

- Invisibility: this idea initiated by Weiser is complete disappearance of pervasive computing technology from a user's consciousness. In efficient use, a reasonable approximation to this idea is lesser user distraction. If a pervasive computing world continuously meets user expectations and hardly gives him surprises, it lets him to interact at max at a subconscious level.

- Localized Scalability: as smart areas emerge in sophistication, the level of interactions between a user's personal computing area and its environment increases. This has severe energy, bandwidth and distraction implications for a wireless mobile user. Scalability, in the highest meaning, is hence a major issue in pervasive computing.

  Like the inverse square laws of nature, good system design needs to achieve scalability by severely reducing interactions between various items. This directly contradicts the present ethos of the Internet, which many assume heralds the "death of distance."

- Masking Uneven Conditioning: Uniform penetration of pervasive computing technology into the infrastructure is a number of years away. During then, there will be present many variations in the "smartness" of various environments. This huge dynamic variations of "smartness" can be jarring to a user, setting aback from the aim of making pervasive computing technology invisible.

  A way to lessen the amount of differentiations seen by a user is to have his personal computing area compensate for "dumb" environments. As a simple example, a system that is capable of disconnected operation is able to mask the absence of wireless coverage in its area.

Overlap with Other Research:
Figure 2 above shows a focused perspective on the research ancestor of mobile and pervasive computing.

Looking ahead, Figure 3 below shows a wider perspective of the research issues we face in this environment. As the figure shows, mobile and pervasive computing have in common many research topics with some areas discussed.

Figure 3: How Mobile and Pervasive Computing Relate to Other Areas

IV. SECURITY CHALLENGES AND REQUIREMENTS

Under this topic, we analyze the major challenges and needs for securing pervasive computing environments.

1. Challenges as briefed before, the various features and the extended functionality that pervasive computing provides make it prone to more vulnerabilities and exposures. Now, we describe these features that add extra load to the security subsystem. [5]

1.1. The Extended Computing Boundary: Traditional computing belongs to the virtual computing world wherein data and programs reside. Current distributed computing research happens to abstract away physical locations of users and resources.

Pervasive computing applications often exploit physical location and other context data of users and resources to enrich the user experience. In such environments,

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

information and physical security becomes interdependent. As a result, such areas become more prone to severe security threats that can threaten users and devices in the physical world as much as they can threaten their data and programs in the virtual world. Therefore, traditional mechanisms that aim hardly on digital security become inefficient.

1.2. Privacy Issues: The physical outreach of pervasive computing makes preserving users' privacy a much more difficult task. Through many sensors and combined devices, active spaces can easily be tailored to users' choices and can abstract and utilize context information fully. Unfortunately, this very feature could threaten the privacy of users a lot. For example, this capability can be exploited by malicious insiders, intruders, or even curious system administrators to track or electronically stalk particular users. The entire system hence becomes a distributed surveillance system that can abstract too much data about users. In some environments, like homes and clinics, there is usually an overflow of sensitive and personal information that must be secured. In addition, there are few situations when people do not want to be tracked.

1.3. User Interaction Issues: One of the main features of pervasive applications is a richer user-interface for interaction between users and the space. A variety of multimedia mechanisms are used for input and output, and to control the physical features of the space. At any point of time, the bunch of users in the space affects the security properties of the space. Due to the effects of these interactions, users in the space cannot easily be prevented from seeing and hearing things happening in it, so this has to be considered while designing access control mechanisms.

1.4. Security Policies: It is important in pervasive computing to have a flexible and convenient method for defining and managing security policies in a dynamic and flexible fashion. The policy management software have an exhaustive database of corresponding device and resource interfaces. As many policy management tools deal with these low-level interfaces, administrators may not have a clear idea of the ramifications of their policy management actions. Dependencies among objects can lead to unexpected side effects and undesirable behavior. Henceforth, the disclosure of security policies may be a breach of security. For instance, knowing whether the system is on the lookout for an intruder could actually be a secret. Thus, unauthorized personnel must not be able to know what the security policy might become under a certain circumstance.

1.5. Info Ops: There is a great deal of concern over new types of threats, namely, Information Operations (info ops) and cyber-terrorism, which are obvious outcomes of the increasing importance of electronic information and the heavy dependency on digital communication networks in most civilian and military activities. Info ops, which can be described as "actions taken that affect adversary information and information systems while defending one's own information and information systems," is a important concern in today's networks. Pervasive computing provides max leverage and adds much more capabilities to the arsenal of info warriors, making info ops a much more severe threat.

2. Security Requirements: To deal with the new vulnerabilities introduced by pervasive computing, security and privacy ensures in pervasive computing environments must be specified and drafted early into the design process rather than being assumed as add-ons or afterthoughts. The Internet and Wi-Fi are two such example, both which still suffer from inadequate security. In this section, we describe the important requirements needed for a security subsystem for pervasive computing environments.

2.1. Transparency and unobtrusiveness: The focal point of pervasive computing is to transform users into first class entities, who no longer need to imply much of their attention to computing machinery. Hence, even the security subsystem should be transparent to some level, fusing into the background without distracting users too much.

2.2. Multilevel: When it comes to security, one size does not fit all. Hence, the security architecture chosen should be able to ensure different levels of security services based on system policy, temporal circumstances, available resources, context information, environmental situations, etc. In some situations, this may go against the previous point.

2.3. Context-Awareness: Often, traditional security is somewhat static and context insensitive. Pervasive computing integrates context and situational information, transforming the computing environment into a sentient space. Security services should make extensive use of context information available. For instance, access control decisions may depend on time or special circumstances. Context data can give valuable information for intrusion detection mechanisms. However, viewing what the security policy might become in a particular time or under a particular situation should not be possible. In addition, there is a need to verify the authenticity and integrity of the context information acquired. This is sometimes necessary in order to thwart false context information obtained from rogue or malfunctioning sensors.

2.4. Flexibility and customizability: The security subsystem should be flexible, adaptable, and customizable. It must be able to adapt to environments with extreme

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

conditions and scarce resources, yet, it is able to evolve and provide additional functionality when more resources become available. Tools for defining and managing policies should be as dynamic as the environment itself.

2.5. Interoperability: With many different security technologies surfacing and being deployed, the assumption that a particular security mechanism will eventually prevail is flawed. For that reason, it is necessary to support multiple security mechanisms and negotiate security requirements.

2.6. Extended boundaries: While traditional security was restricted to the virtual world, security now should incorporate some aspects of the physical world, e.g. preventing intruders from accessing physical spaces. In essence, virtual and physical security become interdependent.

2.7. Scalability: Pervasive computing environments can host hundreds or thousands of diverse devices. The security services should be able to scale to the "dust" of mobile and embedded devices available at some particular instance of time. In addition, the security services need to be able to support huge numbers of users with different roles and privileges, under different situational information.

V. CONCLUSION

Pervasive computing will be a productive promising source of challenging research developments in computer systems for several years ahead. Solving these issues will need of us to broaden our ideas on some fields, and to reanalyze long-standing design assumptions in others. It is also required to have to address research challenges in fields besides computer systems. These areas include software agents (with specific relevance to high-level proactive behavior), human-computer interaction (especially multi-modal interactions and human-centric hardware designs), and expert systems and artificial intelligence (particularly in the areas of decision making and planning). Ideas from these fields are required to be embedded with the kinds of computer systems capabilities described in this paper. Pervasive computing will hence be the crucible in which many various areas of research are merged.

REFERENCES

[1]. www.cs.cmu.edu/~aura/docdir/pcs01.pdf
[2]. Hansmann, Uwe (2003). Pervasive Computing: The Mobile World. Springer. ISBN 3-540-00218-9.
[3]. Jump up^ Lugmayr, Thomas; Risse; Stockleben, Bjoern; Laurila, Kari; Kaario, Juha (September 2009). Multimedia Tools and Applications 44 (3): 337–359.
[4]. Jump up^ Greenfield, Adam (2006). Everyware: the dawning age of ubiquitous computing. New Riders. pp. 11–12. ISBN 0-321-38401-6.
[5]. http://gaia.cs.illinois.edu/papers/towards-percomp-security.pdf
[6]. http://www.csd.cs.cmu.edu/research/areas/mopercomp/.