IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. II (May – Jun. 2015), PP 86-93
www.iosrjournals.org

Pervasive Computing Applications And Its Security Issues & Challenges

R.Uma, G.Archana, V.Komail.

Assistant Professors, Department Of Computer Applications, Dhanalakshmi Srinivasan College of Arts & Science for Women Perambalur.
Assistant Professors, Dept of MCA, Dhanalakshmi Srinivasan college of arts and science for women Perambalur,

Abstract: *This paper discusses the emerging field of pervasive computing applications and its security challenges, the word pervasive or ubiquitous mean "existing everywhere." It produces sevice to anyplace, anywhere, at any time service to small or portable and wearable devices. This technology create new opportunities and challenges for the Information Technology companies to place high-performance computers and sensors in virtually every device, appliance, and piece of equipment in buildings, home care,Intelligent transport system, workplaces, and factories, and even in clothing. Pervasive computing environment or PCE share most of the security issues of traditional networked applications. These include authentication of devices and users, privacy of data or information, defense against malicious code such as viruses, worms, Trojan horses etc, and access control mechanisms. Finally it describes about the future focus for the pervasive computing through the real time applications.*

Keywords: *Pervasive computing,Devices,Connectivity,Issues,Privacy,User Interfaces.*

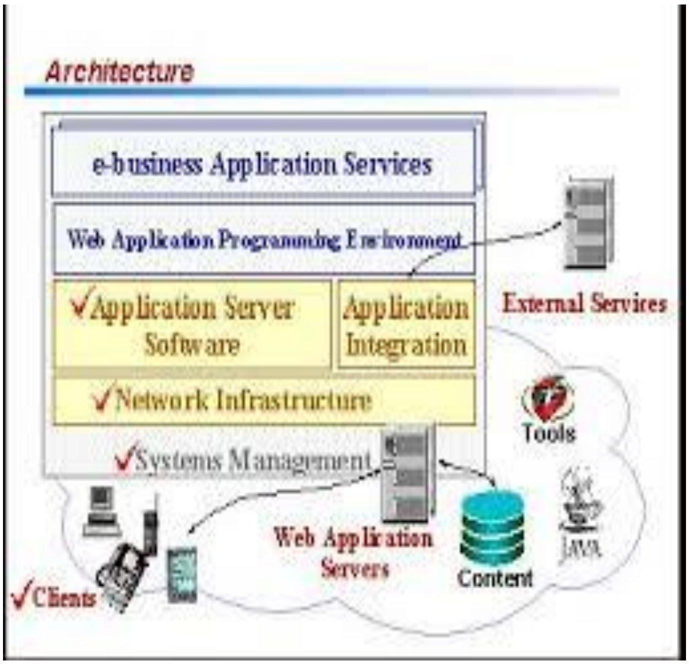
I. Introduction

The Pervasive computing encompasses three things all of the areas: 1. It concerns the way people view mobile computing devices, and use them within their environments to perform tasks. 2. It concerns the way applications are created and deployed to enable such tasks to be performed.3.It concerns the environment and how it is enhanced by the emergence and ubiquity of new information and functionality. The advantage of pervasive computing environments is to make life more comfortable by providing device mobility and a digital infrastructure that has the ability to provide useful services to people in the environment, when and where they need them. At the same time pervasive computing presents many risks and security related issues that were not previously encountered in more traditional computing environments. In particular, issues such as privacy, trust and identity become more challenging to the designers of such environments. Designing secure pervasive environments requires the system to reliably confidently identify the user who wishes to access the environment's resources. It is also

Important to appreciate the risks involved in establishing and verifying the identity of users insuch environments. Privacy is also important as users need to be confident that their personal information is not used in a way that they do not approve of. Privacy in such environments is particularly important as the syste needs to be protective of the users' data and perceived by the user to be that way.

II. Characteristics and Architecture of Pervasive Computing

Pervasive computing can be classified by a set ofattributes and capabilities that describe the extent of itsfunctionality. Mobility and ad-hoc networking capabilities are expected to emerge relatively soon, that is within the next one to two years. [1]Characteristics such as autonomy, context awareness and energy autarky are not expected until later, taking anywhere from five to ten years. Context awareness and embededt in day-to-day objects are viewed as pervasivecomputing's ultimate and determining characteristics. Pervasive computing is the result of computer technology advancing at exponential speeds -- a trend toward all man-made and some natural products having hardware and software. [2]Pervasive computing goes beyond the realm of personal computers: it is the idea that almost any device, from clothing to tools to appliances to cars to homes to the human body to your coffee mug, can be imbedded with chips to connect the device to aninfinite network of other devices. The goal of pervasive computing, which combines current network technologies with wireless computing, voice recognition, Internet capability and artificial intelligence, is to create an environment where the connectivity of devices is embedded in such a way that the connectivity is unobtrusive and always available.



III. Pervasive Computing Applications

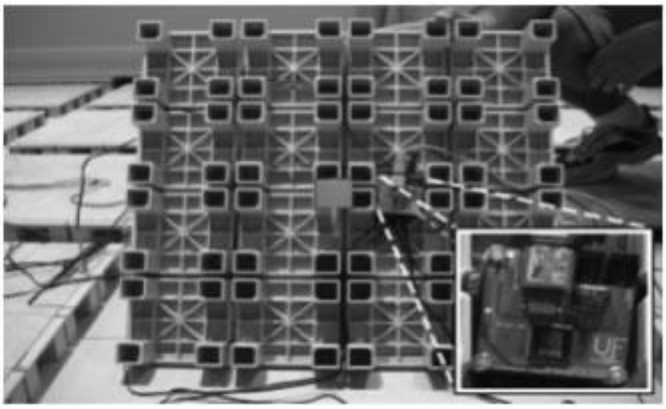
Pervasive computing could be exploited to achieve great societal, organizational and individual benefits. [3]The high-level goals of such applications mostly center on Quality of Life, Quality of Experience, Convenience, Return on Investment, Assistance, among others. The Mobile and Pervasive Computing laboratory is a pioneer and one of the world leading research centers in applying pervasive computing in support of Aging, Disabilities and Independence (ADI) addressing Quality of Life for the elderly and individuals with special needs. ADI research is highly multi-disciplinary and requires diversified research talents that cannot be attained without research collaborations (including international). The lab also addresses proactive health applications of pervasive computing with emphasize on persuasive tele-health systems, which is another multi-disciplinary research area.

Smart Greenhouse It is a natural air purifying system that utilises plants that havenaturally powerful air purifying qualities in a mini greenhouse in the house, which provides fresh air and a pleasant natural scent.

The greenhouse automatically controls the climate to adjust the plants purifying abilities in order to provide adequate freshness according to the contamination level of the house.

The Smart Floor

[4]The primary location tracking system used in the house is the Smart Floor, which is built into a residential-grade, raised tile system. Each tile is approximately one square foot with a pressure sensor fitted underneath. Unlike other tracking methods, the Smart Floor requires no attention from the residents, any device to wear, or cameras that invade the residents' privacy. To the user, the Smart Floor is very convenient as it is unencumbered and requires no user attention. To the Smart House, the Smart Floor is very powerful as it provides for rich sentience of location and activities, quietly and invisibly.



The Smart Floor is utilized as a collection of location and activity services (API) to other smart house applications. Applications may need location contexts in which case they invoke the location service. Some applications are entirely based on locations such as daily activity counter, in which the total steps taken by the resident are counted and reported to the cloud and other subscribers (e.g. care giver, or a relative). A phenomena cloud implementation of the location service is also available which provides for a higher level of reliability of the location service despite sensor failures and high levels of noise exhibited by the pressure sensors.

SMART PEN [4][[[:Smart pen offers a way of finding a definition for any unknown vocabulary when people have problems reading books .

This is especially useful for documents written in a foreign language. All you need to do is underline or write down the unknown word, press the translation key and then the pen automatically projects the translation onto the document in.

The Smartwave: Meal Preparation Assistant

The SmartWave is a consists of a microwave oven and other devices and services that provide assistance in meal preparation. An RFID reader mounted under a counter surface below the microwave allows appropriately tagged frozen meals to be recognized by the SmartWave. The resident is provided via a monitor above the microwave with the necessary instructions to ready the meal for cooking (remove film, stir ingredients, etc.). The SmartWave can handle multiple cooking cycles (e.g. thaw, low-power followed by high power) automatically. It sets power levels and cooking times automatically. Once the meal is ready, a notification is sent to the resident, wherever he or she is in the house. This technology assists a variety of residents, such as those with visual impairments who are unable to read the fine print on the frozen meals. It also assists residents with hand dexterity problems or with mild dementia.

Cognitive Assistant

The main goal of the Cognitive Assistant (CA) project is to assist older adults with mild dementia overcome difficulties in carrying out basic daily activities by means of reminders, orientation, and context-sensitive triggering. Indoor, the cognitive assistant provides: (1) Attention Capture and (2) anywhere multimedia cueing capabilities. The assistant itself is a general service decoupled from the specific contents and events of interests. It can be utilized by any number of applications in the Smart House requiring any type of reminders, training, or cueing. The CA has been used proactively as a reminder for critical tasks (to take medications, to eat at meal times, to go see the doctor, to call son on his birthday, or to feed the pet). It has also been used as a training tool to perform step-by-step tasks (specifically in re-training on hygiene tasks). Another purpose for training is behavior alteration, which we demonstrated in preparing a meal using the SmartWave and ensuring hydration. CA has also been used as a monitoring tool to record the activities performed by the elder.

Smart Plug

An intelligent environment should be able to sense and recognize the devices and services it has available, interpret their status, and if needed interact with these devices to influence them. For example, in the Gator Tech Smart House, self-sensing is a service that provides a real-time model that reflects the status of all the appliances in the space. The SmartPlug is a prerequisite service that enables self-sensing. The Smart Plug is a standard power outlet invisibly fitted with a low-cost RFID reader housed inside the wall behind the plug hardware. Each electrical device, such as a lamp or a fan, is given an RFID tag that contains information about the device. Currently, the RFID tags are embedded in pass through plugs (the white cubical below). Once an appliance is plugged (through the pass through cube), its RFID tag is read and its location id identified. The house gets to know this dynamic information instantaneously. By attaching a sensor node to the plug, actuation becomes possible. Actuations are limited to on/off switching of the appliance

Smart Bed

It can be difficult in this modern age for busy working people to feel good and peaceful when they must get up early in the morning, but with smart bed, you can turn a stressful morning into an enjoyable one.

Smart Pillow

A pillow that could look after your bed time needs.

Smart pillow can read any books of your choice to you at bedtime and can play your favourite music to drift off to when you start to get sleepy.

Cyber-Analytic Tele-Health

Researchers in the social and life sciences, as well as medical researchers and practitioners, have long sought the ability to continuously and automaticallymonitor research subjects or patients for a variety of conditions or disorders. Additionally, the use of monitoring data to influence treatment dosage or regimen within real-time constraints is an important objective of behavior modification practice for psychological and medical therapies. The Mobile and Pervasive Computing lab has formed a multi-disciplinary team to research tele-health systems in the domain of obesity and diabetes. We have analyzed the traditional model for tele-health and developed key advances to the model that we believe will invigorate tele-health as an effective delivery mode for health care. Our work so far addressed the need to extend tele-health systems with two powerful capabilities: (1) behavior recognition, which is powerful sentience over and above vital signs and activity sensing, and (2) persuasion and adaptive persuasion loops, which is powerful (human) actuation. We believe that both additions (sentience and actuation) will have significant impact on the effectiveness and efficacy of tele-health systems. We are currently working on behavior recognition, Action Behavior Models for persuasion and participatory tele-health. We are also planning for a major validation and quantification of our hypotheses.

Gate Reminder (DESK)

Forgetting an important item at home that you need for your day is something that happens to the best of us.But now, this innovative Gate reminder will remind you what you need before you leave the house, so you will never need to forget anything again.

Smart Dressing Table

The smart dressing table is the perfect accessory for women who are fed up with having to put their makeupon in the morning in a bad and dark environment. This dressing table has several innovative functions that work with the user to create a perfect and convenient atmosphere for putting up makeup on quickly and effectively.

Digi Flower

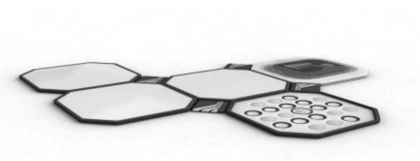
It is a cordless communication system that indicates whether or not any member of the family is approaching the home.As well as improving communication and general relationships within the family, it also provides general convenienc eand can also act as a safety device. It is composed of a portable transmiter and a receiver.This device indicates by bursting into bloom when a family member approaches the house.This innovation can act as a new communication interface for the people both inside and outside the house.

Electronic Paper And Smart Wall

The days of paper books and newspapers what they are going to be replaced with, according to someentrepreneurs, is “**epaper”.**It is basically a computer monitor that is so thin that you could roll it up and stick it in your pocket. One of the problems when changing a display is the size.How can we utilise the size of a display effectively when it is constantly getting bigger.

Smart Mat

A mat at the entrance of home, provides a vital connection between inside and outside the house.By sensing the body weight and footprint of the user, the smart mat immediately recognises which user isstepping on the mat.



Pervasive Computing in Healthcare

Pervasive computing is often mentioned in the context of improving healthcare.Usually, these examples involve consumer monitoring devices such as bloodpressure cuffs and glucose meters that can upload data to a personal computer for collection and dissemination to professional caregivers.By collecting patient data in settings more varied than doctors’offices, healthcare provider shope to better understand themany facets of patients’ daily gives and then modify the rapies to the individual.Another important context is emergency care to accelerate access to medical records at the emergency site or to bring experts to the scene virtually. By giving medical professionals appropriate,complete information,we expect to deliver better care that’s tuned not only to the situation but also to the patient’s history.The surgical field also receives much attention,as surgeons and nurses must monitor and controlvarious vital functions under intensely stressful conditions. Technologists are developing systemsto collect and process an ever-increasing range of telemetry from instruments used in an operating room and to augment human ability to detect patterns of concern that could require immediate action.

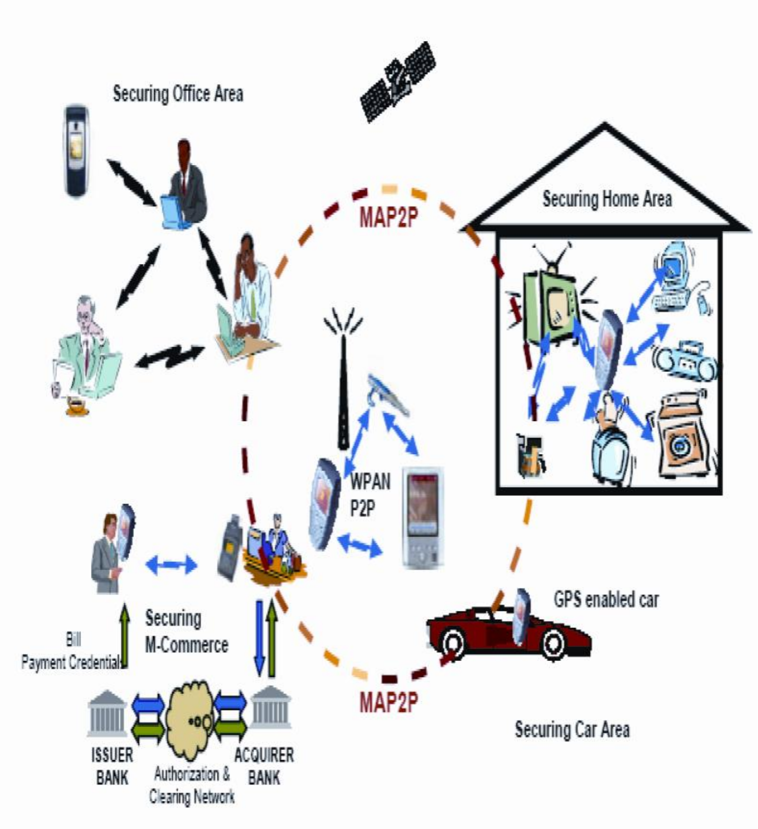
A promising future

Many of these applications have appeared in the popular press and are actually starting to be deployed.At one end of the spectrum, consumer devices easily network with home PCs to let users gather data from sensors in the home that their physicians can access online. At the other end, telesurgery is becoming a practical reality, with remote physicians able to consult on a patient’s conditionas well as take part in a surgical procedure.This special issue seeks to go beyond these“expected” applications and bring the reader an even wider range of applicability for pervasivecomputing technologies in the highly variedhealthcare domain.Proponents tout pervasive computing as benefiting healthcare in at least three ways:

1. Lowering costs by getting appropriate care tothe people who need it much faster than previously possible;
2. Making expert care accessible to more people, there by increasing the scale at which first-rate healthcare is applied;
3. Making healthcare more personalized, prompting individuals to take more responsibility for maintaining their health.

IV. Security Challenges In Pervasive Computing Environment

Pervasive computing environment or PCE share most of the security issues of traditional networked applications. These include authentication of devices and users, privacy of data or information, defense against malicious code such as viruses, worms, Trojan horses etc, and access control mechanisms. However, the pervasive computing environment adds some unique issues to the already complex security arena. Physical security is important as the devices can be easily misplaced or stolen. Information that is usually confined behind a corporate firewall is now winging its way through the air, possibly spending some time on hosted servers or wireless gateways.



V. Security issues

Many attempts have been made to apply traditional security concepts and solutions to pervasive platforms. However, in most cases, a lot of modifications are needed inorder for the security infrastructure to fit within the pervasive framework leading to a high level of risk of introducing new breaches. A generic security framework is needed [5]. One way to minimise the security issues with pervasive computing frameworks is to identify them in the early stages of their development. These issues include:

5.1 Reliability

Pervasive systems expose a larger attack surface with many points of failure in comparison to traditional computing environments [2]. If people depend upon pervasive systems to mediate day-to-day activities, such systems will quickly become missioncritical.They need to be robust, dependable, and always available. This is a very difficult problem for a pervasive computing framework to address. Due to the wide variety of computing technologies that entities will use, the risk of introducing security issues that may threaten the reliability of services will increase.

5.2 Trust

The infrastructure that supports a pervasive computing system introduces new security challenges not addressed in existing security models, including in the domain of trust management [6, 7]. The issue of trust will arise when anentity, such as a PDA, mobile phone or laptop computer that is unknown to otherentities offers services. Entities offering services may have an established connection history and are trusted. An entity connecting to a pervasive environment for the first time will have no historical records on which to base a measure of trust. Such an entity may act maliciously and try to disrupt services being offered or it may be genuinely trying to avail of a specific service. The question of trust arises and whether existing members of the environment trust the intentions of this new entity. For example, two new entities (A and B) that are connected to the pervasive environment may wish exchange data. Do they trust each other? to traditional computing environments [2]. If people depend upon pervasive systems to mediate day-to-day activities, such systems will quickly become mission critical.They need to be robust, dependable, and always available. This is a very difficult problem for a pervasive computing framework to address. Due to the wide variety of computing technologies that entities will use, the risk of introducing security issues that may threaten the reliability of services will increase.

5.3 Malicious attacks

A common form of malicious attack is a Denial of Service (DoS) attack. A DoS is anattack with the purpose of preventing legitimate users from using a specfied network resource such as a website, web service, or computer system [9]. A Distributed Denialof Service (DDoS) attack is a coordinated attack on the availability of services ofa given target system or network that is launched indirectly through many compromised computing systems [10]. The threat of a deliberate attack by an entity connectedto a pervasive computing framework will exist. Any entity can act maliciouslyand may deliberately try to access a service provided by another entity that it is not permitted. A DoS attack can not only cause the innocent entity to malfunction but may also introduce other problems such as severe network latency, scalability problems when other entities try to connect to the framework and service unavailability.

5.4 Information propagation

When data is transmitted between entities, it is possible that it may be altered or corrupted accidentally or maliciously. It is important that the integrity of the data in apervasive environment is maintained. If the data is altered, the entities may not have any mechanism to detect this.

5.5 Recourse

Ranganathan states that because pervasive systems will mediate everyday physicalactivity, technical mechanisms to facilitate recourse must be built-in from the start[2]. When one entity provides a service to another, the problem exists when one of the entities reneges before a successful termination. A pervasive computing frameworkshould have mechanisms to deal with this.In the next section we introduce an example of a pervasive computing framework called ConStruct. We use this to motivate discussion ofhow security issues impact services that are supported in a pervasive environment.

5.6 Data Communication

Privacy of the data encompasses two aspects. First, it hasto ensure that data being shared or communicated is not being hacked by any active or passive attackers. As aninitial thought, we consider several encryption and decryption techniques. But at the same time we need to think about the other side of the coin which reminds us about the memory, battery power and other limitations.Along with that, the users in pervasive computing environment have much more elasticity and sovereignty in mobility. This includes a large variety of domains ranging from well protected environments to totally open unprotected situations which makes the data protect its issue worse. Secondly, how can it be guaranteed that theuser data which is being collected almost obviously willnot be used maliciously? Or how we can ensure with certainty that the complicated data is not being processedby any unauthorized user

5.7 Trust

In order to overcome several constraints, mutualcooperation, interconnectedness and inter dependabilityhave been exposed as the obvious uniqueness of pervasivecomputing environment. Along with these occurs theissue of trust. If data is shared with an unwarranted device, the probability of data security reduces automatically. [8].

VI. Conclusions

In this Paper we have gathered the information about the pervasive computing technologies, architecture, applications, issues and challenges we have seen, today the pervasive/ubiquitous computing is a fertile source of challenging problems in computer systems. In future we focus our research for creating applications such as smart home or office or university etc.without any technical challenges by using the advanced embedded systems or by efficient soft computing techniques.devices need to be perceived as portals into the application/data space supported by the environment, rather than repositories of custom software. Applications need to be seen as tasks performed on behalf of a user, not as programs written to exploit the resources of a specific computer. The goal of a pervasive computing framework is to support services offered by entities in a heterogeneous environment. It is highly probable that most entities havelittle or no knowledge of other entities and the services they offer. This introduces important security issues especially when a new entity makes available a new servicefor the first time.As a result of this 'unknown' factor introduced in this environment, there is astrong expectation for a pervasive computing framework to provide adequate security to all entities. The framework is transparent to these entities and as such they appear to communicate peer-to-peer. Unless entities are aware of appropriate security mechanisms, there may be reluctance for these to connect to the framework and avail of services in offer.

References

[1]. http://en.wikipedia.org/wiki/Pervasive_Computing

[2]. Lathies Bhasker T "Pervasive Computing Issues, Challenges andApplications"International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 2 Issue 12, Dec.2013.

[3]. **"Security Issues with Pervasive Computing Frameworks"** Michael CollinsSystems Research Group, School of Computer Science and Informatics,UCD Dublin, Ireand.

[4]. "Issues and challenges in ubiqutious computing" Protocol Engineering & Technology (PET) Lab. Indian Institute of Science,Bangalore.

[5]. https://www.google.co.in/search?q=pervasive+compuing+characteristics&biw.

[6]. A Survey on Pervasive Computing Er. Manita Gorai, Er. Kamna Agarwal , International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012

[7]. M. Satyanarayanan: Pervasive Computing: Vision and Challenges. IEEE Personel Communications, 2001