"A Research upon Various Issues and Challenges of Securing Pervasive Computing Applications"

Nandita Argal Shrivastava

Research Scholar, Mahatma Gandhi University, Meghalaya

Abstract – This paper describes about the recent research topic pervasive computing which focus on the characteristics, architecture, issues and challenges. The pervasive architecture relates how the end-user interacts with the pervasive network using the middleware support. Finally it describes about the future focus for the pervasive computing through the real time applications.

Pervasive computing technology has the potential to benefit applications in the military, financial, and health care domain. Although pervasive computing technology looks promising, one critical challenge needs to be addressed before it can be widely deployed – security. The problem is serious because pervasive computing applications involve interactions between a large number of entities that can span different organizational boundaries. Unlike traditional applications, these applications do not usually have well-defined security perimeters and are dynamic in nature. Moreover, these applications use knowledge of surrounding physical spaces. This requires security policies to use contextual information that, in turn, must be adequately protected from security breaches. Uncontrolled disclosure of information or unconstrained interactions among entities can lead to very serious consequences. Traditional access control policies and mechanisms rarely address these issues and are thus inadequate for securing pervasive computing applications.

----------♦----------

INTRODUCTION

Pervasive Computing is the latest computing technology which is available in all over the place where the communication taken place. In this pervasive environment any device from anywhere can access by the user. In here the user can interact with the system by using laptops, tablets, terminals, mobile phones and smart phones. The major technologies such as internet, advanced middleware, operating systems, sensors/actuators, microprocessors, and mobile protocols are used to give support for this pervasive computing.

Pervasive network presumes an altogether different vision. A device can be a portal into an application-data space, not a repository of custom software that a user must manage. An application is a means by which an end user can performs a task, not software written to exploit a device's capabilities. And a computing environment is information enhanced physical space, not a virtual environment that exists to store and run software.

Security and privacy are a major concern for such applications. Preventing data transmission to the monitoring service or sending false data may be fatal. Sending too many false alarms can cripple emergency services. Disclosing the patient's health data to prospective employers may cause financial hardship and disclosing the data to unapproved doctors causes breach of privacy. Comparing a patient's report to unauthentic reports of other patients may result in incorrect diagnosis. These severe consequences motivate the need to consider security issues when designing secure pervasive computing applications.

Security policies and mechanisms developed for traditional applications are inadequate for pervasive computing applications. Unlike traditional applications, pervasive computing applications have no definite security perimeters – the entities an application will interact with or the resources that will be accessed may not be known in advance. These applications are also dynamic in nature – the accessing entities may change, resources requiring protection may be created or modified, and an entity's access to resources may change during the course of the application. Protecting resources during application execution remains challenging.

Moreover, pervasive computing applications use the knowledge of surrounding physical spaces to provide

services which requires security policies to use contextual information. For instance, access to a resource may be contingent upon the location of the user and time of day. This contextual information can be used to infer the activities of the user and cause a privacy breach. Contextual information must, therefore, be protected by security and privacy policies.

Our requirements for the pervasive computing infrastructure are centered on a high-level conceptual model consisting of devices, users, software components and user interfaces. The distinction between software components and user interfaces is an important one. While software components are programming units that are dynamically composed to form complete applications, user interfaces are conceptual entities that are responsible for interaction with the user, and which may be distributed over multiple software components and devices.

The pervasive computing landscape will involve vast numbers of the four component types. A scalable supporting infrastructure will be required, in order to enable the dynamic discovery of software components and information; the dynamic interconnection of components; the sensing, interpretation and dissemination of context; the mobility and adaptation of components; and the rapid development and deployment of large numbers of software components and user interfaces.

The technological advance over the last few years has revolutionized the world of personal computing. Today, handheld devices exist that can function as a cellular phone, video camera and a PDA, all in one box. Also, wireless service providers have started offering numerous data services over their networks (e.g., NTT DoCoMo's I-Mode). With all these diverse technologies coming together, the vision of pervasive computing. Anywhere, anytime data access on any device is finally beginning to take shape1.

In order to migrate from a pervasive computing vision (or, hype?) into reality, fundamental issues in numerous areas. Networking, data management and security among others, have to be addressed. The need above all is that of .killer apps.. applications with mass appeal that are economically attractive. Vertical domain specific applications exist today (e.g., mobile inventory tracking used by UPS) but the growth of the field is limited unless applications move beyond niches. Today, handheld and mobile devices are abound; the leap will occur when these devices can be networked together into a creative, useful application with wide public appeal.

In this paper, we thus, take an application-centric view of the challenges, namely, what spaces are ripe for killer apps and the appropriate data management infrastructure needed to support them. While a brand new killer app is always a possibility, we focus on how existing applications might adapt and be effective in this environment. To do that, one needs to first understand the unique environmental constraints. From a data management perspective, the following three key issues need to be noted:

Resource Impedance Mismatch: Even though handheld and mobile devices have come a long way, they are still a generation away in terms of capabilities compared to desktop systems. This impedance mismatch is apparent on nearly all aspects. processing power, screen size, battery power etc. Additionally, bandwidth for wireless access is clearly lower compared to wire line networks even with the arrival of next generation wireless 3G networks. In fact, one may easily argue that pervasive systems will always be one order of magnitude or more inferior to that of traditional computing systems.

Scalability: The mobile, wireless environment is conducive for applications in the information-centric arena. Examples of such applications include wireless internet access and real-time traffic planning systems. Scalability for such applications is a serious issue on many fronts. number of users (e.g., a traffic information system can have 100,000+ users in rush hour), physical spread of the client base (e.g., continental USA) and variety of devices (PDAs, cell phones, laptops). Additionally, the application data is likely to have a real-time component requiring specific

Mobility: Mobility can arise in two forms in a pervasive network. Mobility of devices (such as driving with a cell phone) and mobility of users from device to device (with an expectation of their environment following them). For data management, mobility is a less of an issue if the underlying network layer hides it. In fact, mobility opens up a slew of new applications such as location-based services.

ISSUES IN PERVASIVE COMPUTING

Mobility Issues -

- How to integrate mobile communicators into complex information infrastructures?
- What effect will they have on work and leisure?
- Privacy
- How to develop and manage adaptable, context aware software systems?

- What support is needed within the network?
- Power supplies

Wireless Problems -

- Too many similar standards
- Shortage of spectrum
- Use low power + multiple base stations with intelligent antenna.
- Overlapping spectrum usage can cause interference eg Bluetooth and IEEE 802.11
- Unregulated bands lead to chaos
- Health risks?

Open Issues -

In the pervasive computing environment, we need a security policy that will simultaneously be an unobtrusive mechanism to the user as well as have the ability to discover the services available for the user in a transparent manner. The system needs a dynamic security policy which is flexible enough to update and modify on the fly.

Heterogeneity - Due to the distributed and ad hoc nature of the pervasive computing environment, this system is open to several unique vulnerabilities and suffers from quite a number of well-known problems whose reputed solutions are not applicable here.

Location Detection - In this surrounding and because the number of devices can be really vast, it is very hard to detect the physical device with which I am interacting. For this we need a secure communication channel along with device authentication. Again the request for establishing this trust channel is flowing through the shared, unreliable wireless channel.

Access Control - In case of access control, the system is based on user's role and identity. Again this freedom of accessing system resources and services is a variable which depends on the time, situation and other contextual information. Here the user needs to trust the pervasive computing environment including the resources and services available. At the same time the system needs to ensure the identity and access privileges of the user.

Trust - In order to overcome several constraints, mutual cooperation, interconnectedness and inter dependability have been exposed as the obvious uniqueness of pervasive computing environment. Along with these occurs the issue of trust. If data is shared with an unwarranted device, the probability of data security reduces automatically. .

CHALLENGES

The four component types that make up our conceptual model of pervasive computing each present challenges, which place requirements on both the supporting infrastructure and the manner in which software components and user interfaces are constructed. These challenges are characterized in this section.

Devices -

Two device-related challenges must be addressed by the pervasive computing infrastructure; these are the wide differences between heterogeneous device types and the problems caused by device mobility.

Device heterogeneity. We believe that heterogeneity in computing systems will not disappear in the future, but instead will increase as the range of computing devices widens. Devices in a pervasive computing environment will include sensors and actuators that mediate between physical and virtual environments; embedded devices in objects such as watches and shoes; home and office appliances such as videos, toasters and telephones; mobile devices, such as handheld organizers and notebooks; and traditional desktop machines.

Heterogeneous devices will be required to interact seamlessly, despite wide differences in hardware and software capabilities. This will require an infrastructure that maintains knowledge of device characteristics and manages the integration of devices into a coherent system that enables arbitrary device interactions (for example, between a mobile phone and a desktop workstation).

Device mobility. Mobility introduces problems such as the maintenance of connections as devices move between areas of differing network connectivity, and the handling of network disconnections. While protocols for wireless networking handle some of the problems of mobility, such as routing and handovers, some problems cannot be solved at the network level, as they require knowledge of application semantics. It should be the role of the computing infrastructure to cooperate with applications in order to perform tasks related to device mobility, such as management of replicated data in cases of disconnection.

Software components -

The responsibility of the pervasive computing infrastructure with respect to applications includes

supporting application requirements such as context awareness, adaptation, mobility, distribution and interoperability; facilitating the rapid development and deployment of software components; providing component discovery services; and providing scalability. This section addresses the challenges involved in meeting these requirements.

Users -

Users in pervasive computing environments can be mobile and have computing sessions distributed over a range of devices. The infrastructure's role with respect to users should be to maintain knowledge of their context and to manage tasks related to their mobility.

User interfaces -

Users in pervasive computing environments will demand ubiquitous access to their computing applications, which will create a requirement for universally available user interfaces. Device heterogeneity will introduce a further requirement for user interfaces that are highly adaptable. Finally, the diminishing amount of user interaction with applications (brought about in part by the increasing ratio of applications to people) and the changing nature of the interactions (brought about by computing becoming situated in mobile and other novel situations) will mandate the creation of new types of user interfaces.

CHALLENGES TO PRIVACY PROTECTION

Unobtrusiveness - The goal of pervasive computing is to be unobtrusive. For this purpose, technology is embedded into everyday objects that transmit and receive information. This "embedding" reduces the visibility of the pervasive computing environment surrounding the user and makes the technology more friendly and acceptable . Ironically, the same characteristic makes it possible to invade the privacy of the user without the user realizing it. This leaves the users with limited control over their own privacy and also adds the responsibility that they do not intrude on privacy of others. This invasion and responsibility cannot be managed or imposed through social and organizational controls .

There is a need to find a balance between usability and privacy. Traditional models requiring explicit user input have to be replaced with models that can sense information securely and automatically from the context and environment, and exchange it seamlessly with communicating devices and users . A single sign on feature to enable single-step authentication to multiple applications can be a solution. The extension of such models to truly pervasive environments still remains a challenge.

Location Dependency - Pervasive computing applications make use of location information to provide services including local information access (traffic reports, news, navigation maps) and nearest-neighbor services (locating nearby restaurants) . To utilize these location-based services, the users have to make their location known to the service provider. The access to location information about a user can provide opportunity for its misuse. Location is privacy-sensitive information that is available readily making its protection a challenge.

There is also the added requirement for the services to be flexible enough to support different location privacy policies based on situation. For example a user might want location privacy but change this need in case of an emergency to pinpoint and communicate the exact location .

Context Dependency - Pervasive computing applications also depend on context information. This information can include the type of wireless device used by the application, GPS coordinates, user profiles, user preferences, current time, etc. . The ability to use contextual information to enhance traditional user attributes is important for making privacy protection less intrusive . Providing sufficient protection for context information is difficult as context-aware systems deal with sets of information that might have different privacy requirements due to variance in sensitivity and user preference . However there is a lack of protocols and infrastructure for securely collecting, validating, and using contextual information.

Amount of Data Collection - Compared to current computing technology, pervasive computing implementation relies on an increased amount, quality, and accuracy of data generated and collected. This is also enhanced by increasing capabilities to process and analyze the data.

This sheer amount of data collection and processing leads to users frequently ignoring or being deprived from the decision of release of personal data. In addition, pervasive computing environments have a majority of wireless devices. These devices have limitations for processing power, bandwidth, throughput, memory etc . These factors put a resource limitation on elaborate models and protocols for privacy protection that might depend on extensive use of these resources.

Role of Service Provider - The role of the service provider as maintainer and preserver of the privacy sensitive data is critical. There are numerous opportunities for misuse of data passing through the devices of the

service provider. The Platform for Privacy Preferences (P3P) of the World Wide Web Consortium (W3C) provides a specification that can be used to ensure that each data request by the service providers also specifies purpose, retention, and recipients of the data . In the real-world ensuring that all service providers follow the rules is difficult.

Lack of ownership - Resources in a traditional computing system have ownership and access control. On the other hand pervasive computing environments "permit looser and more dynamic couplings between people and resources, thereby invalidating the usual approaches to ownership and control of resources" . For example a user has no control over a camera recording activities in a room where the user is. It is difficult to implement privacy control when ownership cannot be easily determined.

SOLUTIONS FOR PERVASIVE COMPUTING CHALLENGES

Security plays an important role in field of Pervasive Computing environment. There are some security solutions to face pervasive systems are proposed.

Role Based Access Control-Role Based Access Control (RBAC) is in view of different roles on an individual happening as a component of an association. Role based access control is achieved the user role and their privileges. In this technique, every role is assigned to a set of authorization to hold a place as an order among different entities. It incorporates two sorts of mappings, which are user role assignment (URA) and role permission assignment (RPA). These are upgraded independently .

Single Sing on (SSO)-User frequently needs to get to different administration services getting included with various verification and different devices, services and networks. So it is obliged to execute a single sign-on solution which changes the initiation for entries to validate once in all system domains to incorporate reliable leaving and joining of perva sive systems without disturbances .

Digital Right Management (DRM)-While huge ability of conveying numerous administrations by Pervasive Computing to users is perceived, affirmation of being secure for providers in computerized environment is ensured utilizing a Digital Right Management (DRM) framework to implement in pervasive devices .

Ubiquitous Device Management UDM-In dynamic environment, outgoing access effect the networks entirely, so UDM is concerned to provide the act against modification of environment to preserve availability .

Radio Frequency Identification (RFID)-The suggested methodology receives a useful acknowledgment of a protected detached (battery-less) RFID label and integrates the ultra-low power Advanced Encryption Standard (AES) design together with a novel random number generator. The test results demonstrate that the suggested comprehensive methodology can give a solid security ensure with low power, low number of cycles, and low range for accomplishing to obliged execution inside the strict imperatives forced by submissive RFIDs. RFID has traceability facility to read, transform validity and match RFID-tag to the database server for authentication .

Trust Based Security Solution-This proposal increase a security policy and assigning identification to entities. The solution has thought on extending out of SPKI and RBAC for accessibility of smart devices associated together i.e. utilizing Bluetooth. Trust base security authenticates to new user and take feedback from trusted entities is connected .

Service-Oriented and User-Centric Intrusion Detection System (SUIDS)-Intrusion detection system (IDS), have weaknesses prompting to tough deployment because of absence of consideration about heterogeneity, adaptability and resource limitation of Pervasive Computing system networks. To make sense of this issue service-oriented and user-centric intrusion detection system (SUIDS) is recommended which record events and logs to infer protection techniques on different systems devices against intrusions. It joins the exceptional needs of pervasive system by selecting the restricted resource limit of administration nodes and high portability of user nodes into record. SUIDS attains to better execution regarding energy efficiency whereas having high detection efficiency. The normal lifetime of node is expanded 23.9% and the lifetime of network is expanded 17.8% .

Biometrics-Biometric system is basic to first examine the information and consolidate this understanding inside the recognition system and making evaluation of biometric quality an imperative part of biometrics. Biometric system experience variability in information that impact capture, treatment, and usage of a biometric example. It offers consistent and computerized systems to deciding and affirming identity. Finger print, face and iris recognition techniques are rapidly incoming as a secure source of passwords by reading image feature techniques.

CONCLUSION

As we have seen, today the pervasive/ubiquitous computing is a fertile source of challenging problems in computer systems. In this Paper we have gathered the information about the pervasive computing technologies,

architecture, applications, issues and challenges. 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.

Pervasive computing is on a cusp of a revolution. The combination of powerful, mobile devices and universal network connectivity is close to critical mass. The next step is the availability of killer apps that can exploit the environment to provide useful services. The key area of research focus should be on infrastructure and hooks for application designers so that these killer apps may be built and deployed.

Technology is rapidly finding its method and changing states faster than speed into every aspect of our lives as a basic need of time. The way of the pervasive environment permits communication between devices whenever and everywhere, so the systems become more pervasive in modern world. Pervasive Computing will be a ripe resource of challenging research issues in computer systems for a long time to come. We will need to address study and explore the challenges in areas outside computer systems.

Pervasive Computing gives an appealing vision to the future of computing systems. Security, trust and privacy design methods are getting importance in HCI with the advancement of flexibility, nontraditional computing applications that have a solid effect on the personal, natural and instructive privacy of users. To develop security models we recommend to elegant designers by helping they see better work that goes into everyday security, trust and privacy. Hence, research in this field should build familiarity with the impacts of applying specific methods, and should help selecting whatever design methodology is most proper for the configuration of current workload. To accomplish this objective; we propose to develop the security methodologies. A number of the challenges we showing are sensible, applicable and within reach, making them prime challengers for rich future advancements.

REFERENCES

Banavar, G. et al., (2000). “Challenges: An Application Model for Pervasive Computing”, Proceedings 6th Annual Intl. Conference on Mobile Computing and Networking (MobiCom 2000).

Chandini, N., Reddy, N.C.S. and Bashwanth, N. (2014). Pervasive Computing Goals and Its Challenges for New Epoch. International Journal of Advanced Research in Computer and Communication Engineering, 3, pp. 6437-6439.

Debashis Saha and Amitava Mukherjee (2003). “pervasive computing: A Paradigm for 21st century” Published by the IEEE Computer Society,, pp. 0018- 9162.

E. Bertino, E. Ferrari, and A. C. Squicciarini (2004). “Privacy Preserving Trust Negotiations. In Proceedings of the 4th International Workshop on Privacy Enhancing Technologies, Toronto, Canada.

Esler, M. et al., (1999). “Next Century Challenges: Data-Centric Networking for Invisible Computing”, Proceedings 5th Annual Intl. Conference on Mobile Computing and Networking (MobiCom’99).

J. Xiaodong, J. A. Landay, (2002). “Modeling privacy control in context-aware systems”, Pervasive Computing, IEEE, Volume 1, Issue 3, pp. 59-63

L. Kagal, T. Finin, and A. Joshi (2001). “Trust Based Security in a Pervasive Computing Environment. IEEE Computer.

M. Haque, S. I. Ahamed, (2006) “Security in Pervasive Computing: Current Status and Open Issues”, International Journal of Network Security, Volume 3, pp. 203-214.

Munirul Haque and Sheikh Iqbal Ahamed (2006). “Security in Pervasive Computing: Current Status and Open Issues”, International Journal of Network Security, Vol.3, No.3, PP.203–214.

R. Beresford, F. Stajano, “Location Privacy in Pervasive Computing”, Pervasive Computing, IEEE, Volume 2, Issue 1, Jan-Mar 2003, pp. 46-55

R. Jacobs, G. D. Abowd, (2003). “A Framework for comparing perspectives on privacy and pervasive technologies”, Pervasive Computing, IEEE, Volume 2, Issue 4, pp. 78-84

Sandhu, R. (2013). “Shifting Paradigm from Mobile Computing to Ubiquitous/Pervasive Computing. Indexing Journal Indexing: Our Journal Has Recently Joined International Database for Indexing with DOAJ, Index Copernicus, Open J Gate, CAS, Google Scholar.

Sharifi, A. and Abdulahshah, M.K. (2013). Security Attacks and Solutions on Ubiquitous Computing Network. International Journal of Engineering and Innovative Technology (IJEIT), 3, pp. 40-45.