PERVASIVE COMPUTING SERVICE DISCOVERY IN SECURE FRAMEWORK ENVIRONMENT

Mrs. Sweta Singh, Mr. Alok Katiyar, Mr. Amit kumar Singh

[1]Asst. Professor (M.Tech), Department of Computer Science, JIT Barabanki, Lucknow, UP, India, 225203
[2]Asst. Professor (M.Tech), Department of Computer Science, Inderprastha Engineering College, Ghaziabad, UP, India, 201010
[3]Asst. Professor (M.Tech), Department of Computer Science, BBDUniversity, Lucknow

---***---

Abstract - Pervasive systems must offer an open, extensible, and evolving portfolio of services which integrate sensor data from a diverse range of sources. The core challenge is to provide appropriate and consistent adaptive behaviors for these services in the face of huge volumes of sensor data exhibiting varying degrees of precision, accuracy and dynamism. Situation identification is an enabling technology that resolves noisy sensor data and abstracts it into higher-level concepts that are interesting to applications. We provide a comprehensive analysis of the nature and characteristics of situations, discuss the complexities of situation identification, and review the techniques that are most popularly used in modeling and inferring situations from sensor data. We compare and contrast these techniques, and conclude by identifying some of the open research opportunities in the area.

Introduction

Pervasive computing means the technology that is gracefully integrated in our everyday life. The user is no longer aware of this embedded technology. Pervasive computing uses web technology, portable devices, wireless communications and nomadic or ubiquitous computing systems. Other terms for pervasive computing are Ubiquitous Computing, Calm Technology, and Things That Think. It is about the ability to deliver any information to any device over any network. In short, it is about computers everywhere where computers are embedded into equipments, machines, furniture or people. The current technology has evolved into embedded, networked and wireless. Ubiquitous **A synonym of the word 'pervasive', meaning things that seems to be everywhere.** Pervasive computing devices are not personal computers, but very tiny – even invisible -devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods all communicating through interconnected networks.

Service discovery: Service discovery provides a mechanism which allows automatic detection of services offered by any node in the network. In other words, service discovery is the action of finding a service provider for a requested service. When the location of the demanded service is retrieved, the user may further access and use it.

Service Discovery: Objectives, Features, and Techniques:

According to the objective of a service discovery mechanism is to develop a highly dynamic infrastructure where users would be able to seek particular services of interest, and service providers offering those services would be able to announce and advertise their capabilities to the network. Furthermore, service discovery minimize human intervention and allows the network to be self-healing by automatic detection of services which have become unavailable. Once services have been discovered, devices in the network could remotely control each other by adhering to some standard of communication.

Service Description:

In order to facilitate the service discovery process, each protocol has a description language to define the vocabulary and syntax used to describe the service and its properties. The available methods for this task vary according to the degree of expressiveness: key/value, template-based and semantic description. In the key/value approach, services are characterized using a set of Attribute-value pairs. The template-based approach: uses the same technique as in the first approach, in addition it offers predefined set of common attributes which are frequently used. The semantic description relies on the use of ontology. It has richer expressive power than the first two approaches.

Service Discovery Architecture:

Architecture used by service discovery protocols can be classified as directory and non-directory based models, according to how the service descriptions are stored.

The directory based model has a dedicated directory which maintains the whole service descriptions. In this case, the directory takes care of registering service descriptions and processing user requests. The directory can be logically centralized but physically distributed over the network. Therefore, service descriptions are stored at different locations (directories).

The non-directory based model has no dedicated directory, every service provider maintains its service descriptions. When a query arrives, every service provider processes it and replies if it matches the query.

Service Announcement and Query

Service announcement and query are the two basic mechanisms for clients, service providers, and directories to exchange information about available services.

Service Announcement allows service providers to indicate to al l potential users that a set of new services is active and ready for use. This will be accomplished by registering the appropriate service descriptions with the directory if it exists, or multicast service advertisements.

Query approach allows users to discover services that satisfy their requirement. To do this, users initiates (a) unicast query to the directory, or (b) multicast query. The query is expressed using the description language, and specifies the details about service it is looking for. The directory or service provider that holds the matching service description replies to the query. When a directory exists, service providers and users will first discover the directory location before services can be registered and queried. In this case, the directory can be seen as any service in the network and makes advertisement to advertise its existence.

Service Usage (Service invocation):

After retrieving the desired services information, the next step is to access. However, apart from performing service discovery, most protocols offer methods for using the services. An example is Simple Object Access Protocol (SOAP) used in Universal Plug and Play (UPnP).

Configuration Update (management dynamicity)

Service discovery protocol must preserve a consistent view of the network and deliver valid information about available services while network is dynamic. Therefore, the management of such dynamicity is required. Configuration update allows users to monitor the services, their availability and changes in their attributes. There are two sub functions in Configuration Update:

Configuration Purge Allows detection of disconnected entities through (a) leasing and (b) advertisement time-to-live (TTL). In leasing, the service provider requests and maintains a lease with the directory, and refreshes it periodically. The directory assumes that the service provider who fails to refresh its lease has left the system, and purges its information. With TTL, the user monitors the TTL on the advertisement of discovered services and assumes that the service has left the system if the service provider fails to re-advertise before its TTL expires.

Previous Definitions of Context-Aware

The first definition of context-aware applications given by Schilit and Theimer (Schilit and Theimer 1994) restricted the definition from applications that are simply informed about context to applications that adapt themselves to context. Context-aware has become somewhat synonymous with other terms: adaptive (Brown 1996a), reactive (Cooperstock, Tanikoshiet al. 1995), responsive (Elrod, Hall et al. 1993), situated(Hull, Neaveset al. 1997), context-sensitive (Rekimoto, Ayatsukaet al. 1998) and environment-directed(Fickas, Kortuemet al. 1997). Previous definitions of context-aware computing fall into two categories:

using context and adapting to context.

Consistency Maintenance: Allows users to be aware when services change their characteristics. Updates can be propagated using (a) push-based update notification, where users and directories receive notifications from the service provider, or (b) pull-based polling for updates by the user to the directory or service provider for a fresher service description

Various Service Discovery Approaches Adopted by Industry

Over the past years, many organizations and major software vendors have designed and developed a large number of service discovery protocols. This section provides a comprehensive survey for leading technologies in this area and examines functional issue defined in the previous section for each protocol.

SLP:

Service location Protocol (SLP) is an open, simple, extensible, and scalable standard for

service discovery developed by the IETF (Internet Engineering Task Force). It was intended to function within IP network. SLP addresses only service discovery and leaves service invocation unspecified.

- There are many service discovery protocols, including:
- Bluetooth Service Discovery Protocol (SDP)
- DNS Service Discovery (DNS-SD), a component of Zero Configuration Networking
- Dynamic Host Configuration Protocol (DHCP)
- Internet Storage Name Service (iSNS)
- Jini for Java objects.
- Service Location Protocol (SLP)
- Session Announcement Protocol (SAP) used to discover RTP sessions
- Simple Service Discovery Protocol (SSDP) a component of Universal Plug and Play(UPnP)
- Universal Description Discovery and Integration (UDDI) for web services
- Web Proxy Auto discovery Protocol (WPAD)
- WS-Discovery (Web Services Dynamic Discovery)
- XMPP Service Discovery (XEP-0030)
- XRDS(eXtensible Resource Descriptor Sequence) used by XRI, OpenID, OAuth, etc.

The SLP architecture consists of three main components:

- **User Agent (UA):** software entity that sends service discovery request on a user application's behalf.
- **Service Agent (SA):** advertises the location and characteristics of services on behalf of services.
- **Directory Agent (DA):** a central directory collects service descriptions received from SAs in its database and process discovery queries from UAs.

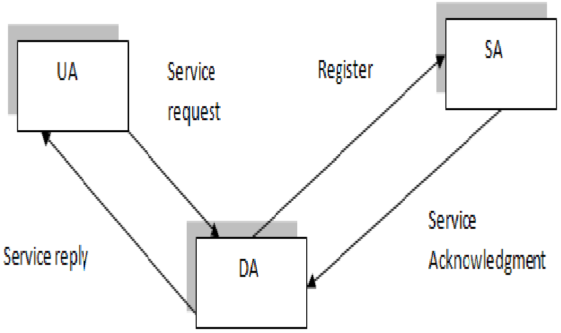


Figure -2- SLP agents and their transactions for service discovery and registration.

As shown in figure 2, when a new service connects to the network, the SA contacts the DA to advertise its existence (Service Registration). Registration message contains: service lifetime, URL for the service, and set of descriptive attributes for the service. Both URL schemas and Attributes are defined. Registration should be refreshed periodically by the SA to indicate its continuous existence. The same when the user needs a certain service, the UA sends request message to the DA which in turn responds with message containing URLs for all services matched against the UA needs. The client can access one of the services pointed to by the returned URL. The protocol used between the client and the service is outside the scope of the SLP specification. To perform their respective roles UA and SA have first to discover DA location. SLP provides three methods for DA discovery: static, active, and passive. In static approach: SLP agents obtain the address of the DA using DHCP; the necessary DHCP options for SLP are defined. With active approach: SLP agent (UA/SA) sends service request to the SLP multicast group address, a DA listening on this address will respond via unicast to the requesting agent. In passive approach: DA multicasts advertisements periodically, UAs and SAs learn the DA address from the received advertisements.

It is important to note that the DA is not mandatory; it is used especially in large networks to enhance scalability. In smaller network (e.g. home network, office network) there may be no real need for DA, SLP is deployed without DA. In this case, UAs send their service requests to the SLP multicast address. The SAs announcing the service will send a unicast response to the UA. Moreover, SAs[1] announce their presence via multicast SLP provides a powerful filter that allows UAs to select the most appropriate service from among services on the network. The UA can formulate expressive queries using operators such as AND, OR, comparators (<, =,>, <=,>=) and substring SLP is an open source; it does not depend on any programming language and scales well in large networks. The scalability is supported by various features such as scope concept, and multiple DAs.

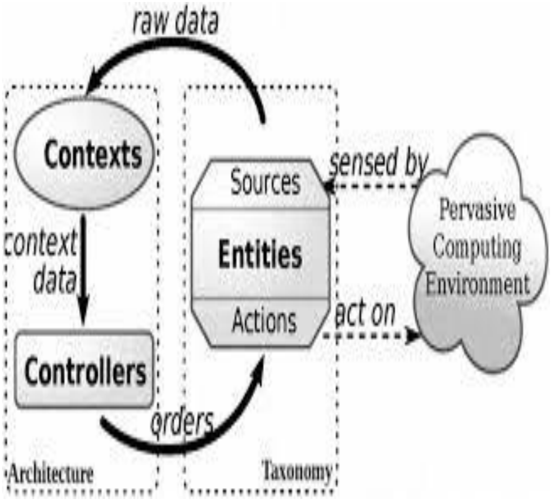
Client: requests Lookup Service for available service.

Service provider: registers its services and their descriptions with Lookup Service.

Lookup Service (LS): Directory which collects service descriptions and process match queries in manner analogous to DA in SLP. Unlike SLP, where DA is optional, Jini operates only as a directory based service discovery and requires the presence of one or more Lookup Services in the network. The heart of Jini is a trio protocols called: discovery, join, and lookup. Discovery occurs when a service provider or client is looking for Lookup Service. Join occurs when a service provider has located a LS and wishes to join it. Lookup occurs when the client needs to locate and invoke a service.

Design the taxonomy for Setup Environment

A design-driven methodology: We introduce DiaSpec, a design language dedicated to describing both a taxonomy of area-specific entities and pervasive computing application architectures. This design language provides a conceptual framework to support the development of a pervasive computing application. The design is used to provide a dedicated programming support to the developer for the subsequent stages of the development cycle, namely the implementation and testing stages. This methodology has two main characteristics; it is (1) design-driven and (2) tool-based. Our methodology relies on the Sense-Compute-Control (SCC) paradigm.



Security and Privacy: We consider user authentication, service authorization, confidentiality, integrity, non-repudiation, availability, and user privacy in service discovery protocols. Although there is much research related to service discovery, few protocols have full security and privacy functionality built-in.

User Authentication and Service Authorization: Protecting services from unauthorized use is necessary. For example, we do not want a storage service to be accessible by anyone. Furthermore, users of a storage service should not be allowed to access other's files arbitrarily. The problem is that it is not realistic for each service to maintain its users and an access control list. User passwords may be different on different services. Small devices may be overburdened to handle authentication and authorization. In many network infrastructures, servers are available to store user information and distribute cryptographic keys. With these servers, providing authentication and authorization is not difficult. While it is more difficult to obtain these servers in adhoc environments, it is even worse for some devices with very limited processing and communication capability to do authentication and authorization.

Confidentiality and Integrity: Confidentiality and integrity in service discovery are primarily communication security. Communication between service discovery components should be safe. Malicious users may listen to communication channels or even actively attack systems. We do not want service information exposed to malicious users or changed during communication. These requirements are translated to use of message encryption and message authentication code.

vailability, User Privacy, and Non-repudiation: Services and directories may be targets of attackers. Making services and directories available against attack is similar to other network applications. User privacy is always a concern. We want to use services easily but keep our information private. In the mean time, service usage should be tracked. A digital signature is usually used to achieve non-repudiation of the service usage. Deploying security in service discovery protocols means more administrative overhead. Proper permissions need to be set for services and users. With thousands of services and hundreds of users in an enterprise, groups or roles need to be created and privileges need to be assigned. In dynamic environments, daily administrative tasks may be overwhelming. Bluetooth has its built-in challenge-response authentication, authorization, and also an encrypted mode of communication.

Security Technology

A central feature and one that will most likely be a determining factor to the success of pervasive

computing is the concept of security. For a pervasive system, like a smart home, to function properly all smart objects contained within the environment must exchange information. Add to this the fact that the communications technology to be used within the system would contain wireless elements. Knowing that radio communications can be manipulated more easily than wired networks, only emphasizes the need to ensure the security of the information exchanged. Additionally, since a smart home intervenes in all aspects of a user's life, even without them realizing that sensitive information is being passed, safety mechanisms must be put into place to ensure that no damage can occur from system failures or operator error. Further concerns revolve around the aspect of data protection as safeguarding an individual's data and privacy are of paramount importance. From the rationale provided above security, with regards to a smart home, is made up of three basic areas: security from malicious actions; safety; and privacy protection.

Security from Malicious Actions

The concept of security within the smart home deals with intentional attacks on the system from an outside source. Security objectives can be further broken down into the following areas of authenticity, data integrity, confidentiality, and non-repudiation. The concept of **authenticity** refers to both persons and objects (as objects within a smart home environment must interact with one another). Authenticity itself ensures that all individuals and objects that are accessing the system are genuinely identifiable through proper and verifiable credentials. Many different technologies can be used in authentication. For individuals, these mechanisms include passwords, Personal Identification Numbers (PINs), and biometric methods such as fingerprints. For objects without biometric characteristics, RFID can be used in automatic identification processes for authentication.

Data integrity is the mechanism that is in place to ensure that manipulation of system data cannot be achieved without notice. In order to guarantee that system data has not been tampered with a checksum is usually calculated from the data. Any manipulation can be determined by comparing the checksum to a reference value. Checksums are usually generated through a hash value from an encryption algorithm such as SHA1 and MD5, which then transforms any length of data into a unique value of a fixed length (the reference value).

Confidentiality of data is ensured through data encryption. Currently there are two basic encryption methods used in industry, which are symmetric and asymmetric encryption .In symmetric encryption a secret key, which can be a number, word, or string of random letters, is applied to the data to be secured and changes it in some form based on the encryption algorithm utilized. This key is shared between both the originator of the encryption and the individual or device attempting to decrypt the information. The most widely used standard for this method is the Advanced Encryption Standard or AES. In asymmetric encryption there are two related keys known as a key pair, unlike symmetric encryption where there is a single shared private key. Within the key pair there is a public key which would be known by all individuals and devices within the smart home. A second, private key is then kept secret. All data is secured with the private key and can then only be decrypted by using the matching public key.

Non-repudiation, within the concept of digital security refers to applying cryptology in order to ensure that the individuals and devices accessing the system are who they say they are. This is currently achieved through the use of digital signatures, and asymmetric encryption methods. In this type of system a Public Key Infrastructure (PKI) is used in the administration of available public keys, which then allows a key's ownership and validity to be confirmed through a trusted authority. PKI systems are a central component in trust management systems that are relevant in the use of pervasive systems using the Trusted Platform Module (TPM). With TPM, the industry organization Trusted Computing Group (TCG) has defined a hardware based solution to support key management, which applies directly to a system and not an individual user.

Safety The term safety, in a digital environment, is often referred to as reliability or fault tolerance .Reliability simply means that the system functions according to its specifications. Within the smart home many widespread systems, such as door locks, heating systems, security systems will be completely interconnected resulting in people becoming very dependent on them. It is then essential for the system to function reliably.

Due to the highly interconnected aspect of a smart home, providing safety mechanisms are currently very hard to develop, especially considering the relative infancy of the concept as well as there being a lack of overall standardization. This is an area where further research is required and will play a key role in determining whether smart home technology is viable.

Privacy Protection

Another very important aspect to the overall security of a system revolves around the protection of an individual's personal information and thus maintaining their privacy. This is largely achieved through data protection. Consider within the smart home that there are a large number of smart objects. Their ability to create ad hoc networks and share information help to provide areas within the system that can be exploited.

Research status in India

Establishment of National Ubiquitous Computing Research Centre's

Under National Ubiquitous Computing Research Initiative by C-DAC Centre's (Hyderabad, Chennai & Bangalore), the objective is to create a R&D base in the multi-disciplinary areas of Ubiquitous Computing (UbiComp). Some of the development areas include Intelligent Home technologies for Illumination control, HVAC and augmenting artifacts used at home such as Interactive Mirror, Smart Bed, Automated Kitchen, as well as Body Area Networks for connecting health care sensors in order to provide always-on (ubiquitous) healthcare.

Pollution Monitoring and Evaluation system

A project on Pollution Monitoring and Evaluation system using Sensor based Wireless Mesh Network for the protection of Public spaces" was initiated at IIM Kolkata. The objective of the project is development of a Wireless Sensor Network for pollution monitoring by identifying the primary source of emission, (detecting Benzene, Toluene, Xylene, CO & CO2 et al, developing a mechanism for data filtering and aggregation, power management and finally commercialization of the product/ system. The field trials have been successfully completed in Kolkata Metropolitan area and the project is to be launched soon.

Design and Development of Ubiquitous Computing Test Bed and UC Applications

A Project on “Design and Development of Ubiquitous Computing Test Bed and UC Applications" is at IISc Bangalore. The project aims to develop efficient test-bed architecture for ubiquitous applications and a framework for testing UC applications having standard configurations. Currently many of the systems have already been developed.

Wireless Sensor Network for Real-Time Landslide Monitoring

A project on Wireless Sensor Network for Real-Time Landslide monitoring is on at Amrita University, Kollam, in Kerala. The project aims at development of a Wireless Sensor Network for Real-Time Landslide Monitoring with pore water pressure, tilt meter and rain gauge sensors, along with a wireless sensor network for the deployment site. With this technology in operation, the risk of landslide will be assessed and remote command and control interface will be provided for different purposes. The on-site sensors are to be installed very soon.

Development of Multimodal User Interface

A project on development of multimodal user interface for Internet access to common people in India is going on at IIT-Kharagpur. This project aims to providing support for Internet access to backward communities in India in their own languages like Hindi and Bengali and providing multimodal interaction facilities.

National Centre for Medium Range Weather Forecasting Centre (NCMRWF)

A project on National Centre for Medium Range Weather Forecasting Centre (NCMRWF), Noida is being implemented by C-DAC, Pune. This project jointly funded by DST and DIT is for setting up PARAM system. The project aims to port several weather forecasting models for Medium Range Weather Forecasting on PARAM Computers. Currently the system is under benchmarking and porting of forecasting software models will be continued for regular operational data.

Research status in Global

Canada

- Topological Media Lab, Concordia University, Canada

Finland

- Community Imaging Group, University of Oulu, Finland

Germany

- Telecooperation Office (TecO), Karlsruhe Institute of Technology, Germany

India

- Ubiquitous Computing Research Resource Centre (UCRC), Centre for Development of Advanced Computing

Sweden

- Mobile Life Centre, Stockholm University

United Kingdom

- Mixed Reality Lab, University of Nottingham

The Technology of a Smart Home

Building on the pervasive paradigm and establishing that a smart home is a large pervasive space, it must be stated that pervasive computing is not an independent technology. Pervasive technology describes how various computing technologies can work in conjunction with one another in a seamless manner that is invisible to those using the technology. The following summarizes the basic principles of the technology required to achieve truly pervasive environments and by extension the smart home.

Microelectronics

Microelectronics deals with the miniaturization, development, manufacture and application of integrated circuits (IC). This is already an essential component in a vast number of technological devices and equipment that are used in everyday life. The most common industries where microelectronics can be found are in consumer electronics, automotive and medical technology. Currently, the field of microelectronics works with structures smaller than 90 nanometers. At the present rate of development this size will be reduced by 50% by 2010. This significant increase in the circuit density will allow for significant gains in functional capacity for a given IC size. However, there are physical limits that are starting to be reached that are becoming very expensive to overcome.

This essentially makes the process too expensive to create very low-priced smart objects, such as RFID tags for consumer goods and their packaging, which cannot cost more than a few cents. Breakthroughs in the field of polymer electronics, which uses carbon based compounds in place of silicon as a semiconductor, appear highly promising for these types of applications. Unlike silicon ICs, polymer ICs can be produced through the use of an inexpensive printing based process, though at a cost of effectiveness as the switching speeds and robustness of these devices tend to be less than that of their silicone based counterparts. However, polymer electronics offer very distinct advantages specifically when the application requires flat, flexible and cheap ICs where performance standards are lower.

Overall, microelectronics is regarded as a mature field and a widely available technology that will not hinder the development of pervasive environments. The field is moving forward with many breakthrough and extensive research in nanotechnology and polymer electronics, thus allowing for cost reductions and feasibility for smart home based technology.

Future Scope

Pervasive computing will be able to sense our situations and anticipate our needs and proactively act in our best interests, much like a very good human friend or our parents. Prof. Dr. Daniel Siewiorek, Carnegie Mellon University, United States. Today, pervasive computing is still mostly a vision of technology, much like the World Wide Web 10 years ago. Extensive development work will be necessary to realize nearly all of its characteristics, such as autarkic power supply, machine-machine communication, the human-machine interface and security technologies. Apart from RFID-based logistics and security systems, there are very few pervasive computing applications currently in existence.

References :

1. Weiser Mark ,1991 ." The founder of ubiquitous computing: The computer for the 21st century".

2. Allan Jinsuo ,Helal Sumi,2005,"UbiNet : A Generic & ubiquitous service provider framework".

3. Edwards W. Keith, Grinter E. Rebecca,2001," At home with ubiquitous computing : Seven Challenges " .

4. BruneauJulien ,Cassou Damien,2012," Developing & Testing Pervasive Computing Application: Towards A tool based development methodology ".

5. KindbergTim ,Fox Armando,2002," System Software for Ubiquitous Computing " .

6. Cook J. Diane , Michael Young blood , Heierman O. Edwin , "Mav Home :An Agent based smart home ".

7. Broens Tom, PokraevStanislav ,SinderenVan Marten ,"Context –aware, ontology based service discovery ".

8. TokmakoffAndrew , Pravin Pawar," Ontology – based context aware service discovery for pervasive environments".

9. Karim Bendaoud,Talal&Merzougui Rachid,2013,"Service Discovery – A servey& comparison ".

10. Bettstetter Christian & Renner Christoph,2012,"A Comparison of service discovery protocols and implementation of the service location protocol " .

11. NajarSalma ,Pinheiro Kirsch Manuele , Sauveyet Carine ,2014,"A new approach for service discovery and prediction on Pervasive Information System".

12. Zhu Feng, MutkaMatt , Ni Lionel ,2011,"Classification of service discovery in pervasive computing environments " .

13. Nieuwdorp, E. (2007). "The pervasive discourse". Computers in Entertainment **5** (2): 13.doi:10.1145/1279540.1279553.

14. Hansmann, Uwe (2003). Pervasive Computing: The Mobile World. Springer. ISBN 3-540-00218-9.

15. Lugmayr, Artur; Risse, Thomas; Stockleben, Bjoern; Laurila, Kari; Kaario, Juha (September 2009). "Semantic ambient media—an introduction". Multimedia Tools and Applications 44 (3): 337–359. doi:10.1007/s11042-009-0282-z.

16. Greenfield, Adam (2006). Everyware: the dawning age of ubiquitous computing. New Riders. pp. 11–12. ISBN 0-321-38401-6.

17. "World Haptics Conferences". Haptics Technical Committee. Retrieved 2007-10-13.

18. Poslad, Stefan (2009). Ubiquitous Computing Smart Devices, Smart Environments and Smart Interaction. Wiley. ISBN 978-0-470-03560-3.

19. Weiser, Mark (1991). "The Computer for the 21st Century". Retrieved 2012-12-19.

20. Weiser; Gold; Brown (1999-05-11). "Ubiquitous computing". Retrieved 2008-05-07.

21. Weiser, Mark (1996-03-17). "Ubiquitous computing". Retrieved 2007-11-03.

22. "IEEE Xplore Abstract - T-Engine: Japan's ubiquitous computing architecture is ready for prime time". Ieeexplore.ieee.org. doi:10.1109/MPRV.2005.40. Retrieved 2015