Educational Aspects of Service Orientation: Smart Home Design issues and Technologies

Arshad Muhammad [1], Dinesh Kumar Saini [1], Kashif Zia [1], Mabruk Ali. Fekihal [1]

[1] *Sohar University, Faculty of Computing and Information Technology, Sohar, Sultanate of Oman*

Abstract **- In this paper efforts are made to review the state of art of service oriented technologies in smart home design. Services oriented software architecture for data exchanges and unit's integration with reusability is studied in this paper. The standards used in unit design for a smart home like "The Open Gateway Services Initiative" (OSGi) and "Universal Plug n Play" (UPnP) are reviewed in the paper. Secure web service messaging, discovery and eventing on resource-constraint devices are reviewed in the paper. In this paper efforts are made to address the issue of seamless integration between devices in the home using networking and service orientation.**

Keywords: **Web Services, Architecture, Smart Home, Standards, Security**

1. Introduction

With recent advancements in technology, home networking is gaining more popularity. Home networking enables users to share services within the home. As the number of companies involved in making network devices increases, prices become affordable. Small business and home networks equipped with dialup Internet access using modem and with little investment may require high bandwidth broadband such as Digital Subscriber Line (DSL) such as AOL, BT or cable. Most providers give initial installation free of cost or with little charge. Most of these devices are very user friendly and with very little technical knowledge a user can easily manage it. Many home networks are setup to share an Internet connection and networking devices usually equipped with firewall/security features or can be using operating system features. In the following section we discuss a number of ways to connect computers in a small office or home network internally and then connect them to the Internet. In this paper we provide an overview of the work carried out in the research area of gateways relevant to research area. We also discuss Service Oriented Architecture which is software architecture, to allow applications to exchange data with each other and separate functions into units which can be accessible over network and can be joined together and reused.

DOI: 10.18421/TEM62-09
https://dx.doi.org/10.18421/TEM62-09

Corresponding author: Arshad Muhammad,
Faculty of Computing and Information Technology, Sohar, Sultanate of Oman
Email: amuhammad@soharuni.edu.om

2. Service-Oriented Architecture (SOA)

OASIS (Organization for the Advancement of Structured Information Standards) [2] defines SOA as "*A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations*." Figure 1. shows the evolution of SOA gateways, other types are discussed later in this paper.

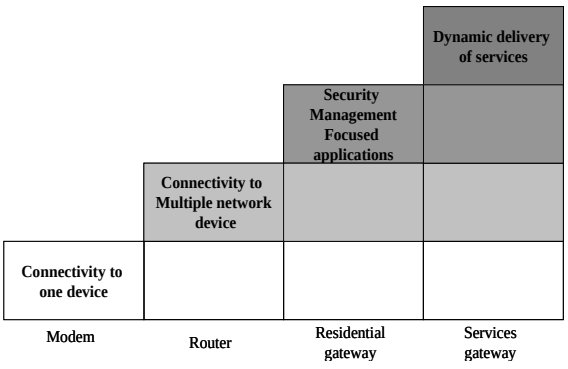

Figure 1.: Gateway Evolution. Sources: BT Exact Technologies [2]

SOA is also defined as a group of services that can communicate with each other. Communication either involves simple data communication or could be two or more services performing some activity. SOA is used in many online applications; for example, a CD

player which can play any CD. In this scenario the CD player is offering a CD playing service. The CD player does not bind with a particular CD, so the same player can be used to play any CD. Similarly, in the case of software services they can be reused or amended as the user demands. This kind of technology is ideal for implementing a flexible gateway service. A majority of services a home user might want to access such as CD player service. are naturally described and implemented in terms of services. To explain in more details, take an example of an ecommerce website where users can shop online. The same interface is used by a number of websites or may be with some minor changes. Web Services (WS) are used to implement a SOA [21], the goal of WS is to make these services reachable over the standard Internet protocols, independent of any platform and programming languages. There are three main building blocks in SOA:

- *Service Provider* creates a web service, publishes it and provides information to a service registry. It is up to the provider to decide how to publish the service, what category it should be listed, its security and cost.
- *Service Broker* known as service registry, used for making WS interfaces available for potential service requestor. Universal Description Discovery and Integration (UDDI) [17; 21] specification is used to publish and discover information regarding WS, other service broker technologies include Electronic Business using eXtensible Markup Language (ebXML) [23].
- *Service Requester* or web service client locate entries in broker service registry to bind to the service in order to invoke or use one of its web services.

3. Gateways

According to the Oxford dictionary, a gateway is defined as a passage that is or may be closed by a gate; an opening through a fence or wall. The term gateway is also used by webmasters as a webpage designed to attract visitors. Gateway also defines a link between two computers that acts as a portal between two programs to enable them to share information and translate protocols. In terms of networking, gateways interconnect different networks with distant and incompatible communication protocols. In networking, a gateway is commonly used to transfer data between different networks or one network and the Internet. The computers that are used to control traffic flow within local network or Internet Service Provider (ISP) are gateways. In networking gateway is usually associated with router or switch, which knows where and how to direct packets in the network. Gateway also enables connection from a LAN to WAN; connecting LAN via local server and then to the Internet. The traditional gateway is used to interconnect devices within a LAN, for example, home or office, all the information about the devices held in central register [16], [15]. When the device is connected to the network for the first time, it registers which can be used to locate the device within the network. This central register is queried, upon which a search is conducted for the device. The gateway is responsible for protocol translation security, naming & addressing and Quality of Service[4; 16]. In order to connect to the gateway, the device must first obtain a unique name and address, to be used in the future for the communication. Gateway can maintain a high level of security by authorizing username/password and encrypt/decrypt the data accordingly. Some of these gateways are designed in such a way that devices from different manufacturers can communicate through it. On the other hand, if the gateway fails, the whole network may fail or become partitioned.

The network gateway can be implemented in hardware, software or as a combination of both[4]. Within the network, one computer is designated as a Gateway, which is used to make communication possible between devices. The major task of the networking gateway is protocol translation; it receives the data from one machine, does the relevant translation and sends data packets to the destination devices as shown in Figure 2. The gateway may also be responsible for NAT (Network Address Translation) to translate IP addresses between a private and the public Internet.

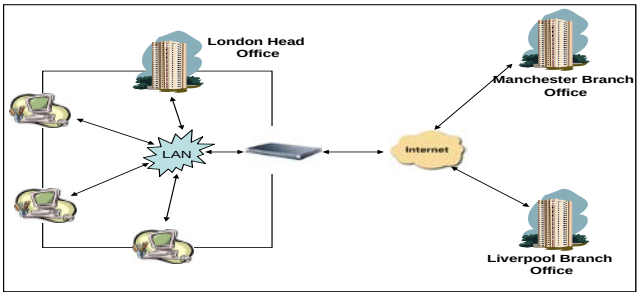

Figure 2.: Gateway in Network

Home networks are connected to internet via home or residential gateways which are shown in the figure. In the beginning there were single service providers providing services to homes via single access route, this kind of architecture is good for security but it has bottleneck for performance and fault tolerance, the centralized architecture is not good architecture. In today's scenario the architecture is moving towards distributed or towards cloud services.

The residential gateway uses NAT to provide network access to all computers in a home network to share one IP address and Internet connection. The residential gateway acts as a bridge and interacts between DSL or cable modem and the internal network. Residential Gateways (RG's) [2], are an intelligent network device to provide way to remotely access devices across the Internet. Usually RG's are used to interconnect different devices within the home/office environment. Home gateway provides functions such as bridging, protocol and address translation [6; 12; 14]. It allows the user to use their home networks and control devices based on e.g. OSGi or UPnP. Usually these gateways are located in the network or external to the consumer premises. In the following subsections we discuss some examples of residential gateways.

4. Open Service Gateway Initiative (OSGi)

Open Gateway Services Initiative (OSGi) [18] project goals to build a framework which enables the use of services over WAN to LAN. OSGi is the leading standard for the Internet services to homes, cars, mobile phone etc., it delivers an open, common architecture for the service providers, software vendors, gateway operators to develop, deploy and manage services. According to OSGi "these components can be installed, updated or removed at any time and dynamically discovered using Java interface"[4]. "The service register itself with the Service Registry allows clients to find the service or check the availability/non-availability of the service. In the case of failure, the service registry cannot be accessed; therefore services cannot be registered or discovered". According to OSGi "to support the deployment of service applications well-known as bundles, OSGi uses a Java framework which supports automatic detection of attached hardware and can automatically download and start device drivers". Device plugs and unplugs at any time and it can respond to it immediately. It provides support to given devices as well as dynamic discovery and downloading of device drivers. There are three main components: Drivers used to do registration of the services, Device Manager coordinates the relationship between certain devices so that they can present multiple representations of the same device, and initiates the process of downloading new drivers and Driver Locator where vendor specific knowledge about the location of drivers is located. Device manager uses this service to identify and download new drivers when they are needed.

Applications within OSGi are called bundles, according to OSGi "Devices can download bundles on demand and can remove them anytime, when a bundle is installed, it can register a number of services to be shared with other bundles under the framework". "Bundles can register news services, receive notifications regarding the state of services, or look up existing services to adapt to the current capabilities of the device. New bundles can be installed for added features or existing bundles can be modified and updated without requiring the system to be restarted". These bundles can be remotely installed, started, stopped, updated and uninstalled without requiring a reboot. Figure 3. shows the OSGi system design. In the OSGi Service Platform, bundles are the only entities that allow deployment of Java-based applications. "A bundle is comprised of Java classes and other resources which together can provide functions to end users and components called services to other bundles. A bundle is deployed as a Java-Archive (JAR) file". Configuring an OSGi framework is human centric but in most cases managed and controlled via centralised controller by service providers. Service discovery and composition is based on proprietary communication and middleware protocols, which are somewhat restrictive as distributed computing and service models are becoming more pervasive. As devices and services are more heterogeneous, this makes management of such framework more complex. As technologies become more sophisticated, control placed on devices and service integration becomes more difficult. Due to this device and service, providers will use different communication standards, therefore, interoperability is a problem and requires a more efficient solution. New architectures need to be developed to overcome these restrictions on current OSGi standard.

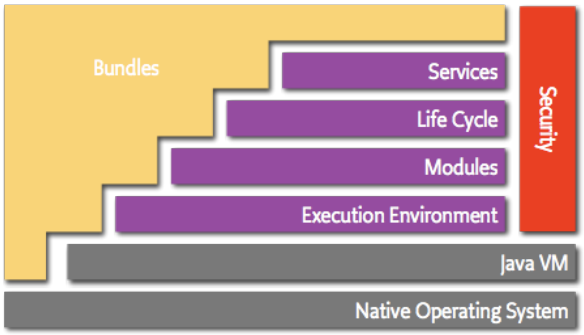

Figure 3: OSGi System Diagram[19]

5. Universal Plug n Play (UPnP)

For the past two decades, the idea of 'plug and play' has gained popularity. Operating system automatically detects the devices which instantly start working. UPnP [22], a set of protocols which allow devices such as PC, printers, mobiles, Wi-Fi access points to discover each other and establish connection using TCP/IP and HTTP to automatically discover, configure and control services. Protocols are used by devices to publish their services over the

network, allowing other devices to discover them. UPnP allows P2P networking of PC's, Networked Appliances (NA) [7] and wireless devices. UPnP supports zero-configuration networking; any vendor device can dynamically join the network, obtain an IP address, and broadcast its capabilities. Devices not only broadcast their services but also discover other devices. There are no restrictions on the devices so devices can leave a network at any time. The main limitation of UPnP is that one cannot access service outside a local area network. All the communication in UPnP happens over Internet Protocol (IP), a target must obtain an IP address before it can join a UPnP network and by using IP addresses, a control point can contact other UPnP devices within same subnet, the messages within UPnP are sent using SOAP [1].

In UPnP, in discovery step, upon joining the network, UPnP discovery protocol allows the device to advertise its service to a control point in the network. Discovery messages contain information about devices such as name, services offered etc. UPnP uses Simple Service Discovery Protocol (SSDP) for this task. The next step is description to enable the control point to know about the device and its services. The control point can retrieve this information via a URL in the discovery message provided by the device during the discovery stage. This device description is expressed in XML and includes vendor name, serial number etc. The next step is Control, after the control point retrieves the description of the device it then sends actions to the device services. Control point uses the control URL for the service provided in the description step to send suitable control messages. These control messages are also expressed in XML using Simple Object Access Protocol (SOAP). Next is Event notification, UPnP description includes a list of actions, the services respond to and the state of variables that models the state of the service at runtime. The service publishes updates by sending event messages whenever these variables change. These messages are also expressed in XML and formatted using General Event Notification Architecture (GENA). Control point may subscribe to receive these messages and events are designed to keep the control point updated about the effects of any actions. The final step is Presentation, which allows the control point to retrieve a page into a web browser, if the device has a URL for presentation. This allows the user to control the device and view its status. The main limitation in UPnP is that it is human centric and so does not provide any mechanism for automatic discovery and composition of services without any human intervention. Attribute-value pair matching is used for discovery which is very restrictive.

6. Devices Profile for Web Services (DPWS)

Devices Profile for Web Services is another notable research that defines set of implementation constraints to enable secure web service messaging, discovery and eventing on resource-constraint devices [8]. DPWS was developed by Microsoft and printer manufactures allowing to send secure messages to and from web services, dynamic discovery, describing, subscribing to and receiving events from a web service. DPWS is a type of SOA targeting device-to-device communication such as OSGi, Home Audio/Video Interoperability (HAVi)[9] and UPnP. DPWS's objectives are similar as UPnP but DWPS is fully aligned with Web Services technology to allow seamless integration of device provided services. Its specification was first published in 2004 and defines an architecture in which devices run two types of services: *hosting services* associated directly to a device and *hosted services* are mostly functional and depend on the hosting device for discovery. The DPWS focuses on IP-capable devices, many of these are still resource-constrained by desktop and server standards but are ready to contribute to general web services' scenarios involving services already deployed in the home, office network [13].

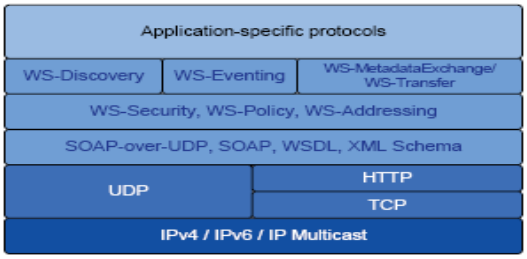

Figure 4.: DPWS as Protocol Stack [5]

According to DPWS "In addition to hosted services, DPWS also specifies a set of built-in services: *Discovery service* used by the device connected to a network to advertise its services and discover other services, *Metadata exchange services* provides access to the device hosted services and their metadata and *Published eventing services* allows other devices to subscribe to event messages by a given service". The DPWS protocol stack is shown in Figure 4. DPWS builds on core Web Services standards such as WSDL 1.1, XML schema, SOAP 1.2, WS-Addressing. DPWS gained attention from manufactures recently after successful demonstration of automation system in Consumer Electronic Show [3]. In DWPS discovery is usually done by sending probe messages over UDP multicast, indicating a client is looking for a particular service i.e. print service defined in WS-Discovery as part of a multicast discovery protocol [24]. The client device listens to the probe messages,

e.g. print service, and responds with a Probe Match message defined in WS-Discovery directly to the client. A Probe Match includes three pieces of information; the address for the device, transports where the device may be reached and security requirements. If a client requires security, the next message is to setup a secure channel between client and device. This channel protects the confidentiality and integrity of all messages between client and device. Each device uses a device certificate as authentication; a device may use self-signed certificates that require the user to enter a device-specific PIN into the client. If a client wants to find out more about a device it may send *GetMetaData* messages directly to the device, in response the device returns information such as manufacturer, serial number etc. Client can send a control message to start using the service i.e. to start a print job. The service sends an event to the client i.e., about the print job such as print job, number of pages printed etc. One of the successful projects is SIRENA, based on DPWS, which intends to create a service-oriented framework for specifying developing distributed applications in diverse real-time embedded computing environment.

In DWPS discovery takes place in few steps, clients usually first discover a service and then in later steps obtain service description. In some cases, after obtaining service description, a device might not contain services desired by client. Device discovery defined in DPWS may cause interoperability problems, may lead client unable to locate all the services requested. Length restrictions for message fields defined in the message section may lead to interoperability issues as the client side considers restrictions sending messages while the device side might reject the messages that exceed the restrictions. There is no mechanism in DPWS to rediscover alternative services as service configurations are manually created. Composition remains operational as long as all services within a composition remain operational, any fault need to be corrected manually.

7. Digital Living Network Alliance (DLNA)

Digital Living Network Alliance (DLNA) [20] also known as Digital Home Working Group (DHWG) is a coalition of leading enterprises in mobile and Personal Computing (PC) and Consumer Electronics (CE), DLNA aims to have industry standards, which will allow products from different companies to be compatible with each other. DLNA framework enables interoperability between devices within or out of three domains such as CE, mobile and PC. In order to give the user facility to interconnect devices seamlessly within three domains, they must address some challenges as follows:

- Products designed for the home should be easy to install;
- Must be affordable;
- These products must interoperate with all other devices;
- Current open industry standards are often too flexible leading to different vendor's products failing to interoperate so they need to design better industry standards to achieve better interoperability.

Another objective of DLNA is "to create wired and wireless interoperable network of mobile and PC and Consumer Electronics (CE), which enable devices to seamlessly connect to each other for sharing information". To deliver interoperability DLNA emphasises three key elements namely "industrial collaboration, standards-based interoperability and compelling product". Different manufacturers are trying to address the interoperability issue within their products and to develop standards that solve interoperability issues. A number of leading companies joined this alliance such as Motorola, Philips, Samsung, Nokia, Microsoft, HP, Sony and Intel. Different vendors are trying to manufacture devices that enforce standards of DLNA. It will enable different vendor devices to be interoperable. Due to rapid advancement in these domains, these standards keep changing to address new devices interoperability.

DLNA published some requirements in order to deliver interoperability within the home, which allow different vendors to participate. These requirements are mainly based on interoperability between networked entertainment and media devices. In future they are going to broaden these requirements in order to accommodate new technologies. These requirements concern media formats, device discovery, control and media management, media transport, network stack and network connectivity.

In the case of device connectivity, whether wired or wireless, it uses Ethernet, IEEE 802.11a/b/g and Bluetooth. Currently this is based on IPv4 for networking but future specifications will include IPv6. UPnP is used to achieve device discovery and control. HTTP is used for media transport and supports a number of media formats, categorised as required or optional. Required formats are JPEG, LPCM, and MPEG2 while optional formats are PNG, GIF, TIFF, MP3, WMA9, AC-3, AAC, ATRAC3plus, MPEG1, MPEG4 and WMV9. Future implementations will include MPEG 4 and JPEG2K. Interoperability guidelines include that technology

should be based on standard bodies, SIGs (Special Interest Groups), and industry forums. It also includes that in case of multiple DLNA-approved technologies are specified, they should bridge or translate as required between any of the two technologies. DLNA uses IPv4 for connectivity as IP allows applications running over different media to communicate easily. Device and service discovery enables devices to automatically discover other devices and their capabilities through which devices can share different services offered by these devices. DLNA uses UPnP™ Device Control Protocol Framework (DCP Framework), which addresses all these needs to discover, control and share services among devices. DLNA incorporates OSGi and inherits the limitation with OSGi as discussed above.

8. Home Audio/Video Interoperability (HAVi)

HAVi [9] is another approach that provides interoperability between audio/video devices within home networks. A/V devices inside the home network can interact with each other and allow devices to interact via another device. Devices from different manufacturers can interact in HAVi regardless of network configuration. HAVi is open, platform independent and language neutral; CE can free manufacturers to develop interoperable devices. These can be connected using HAVi, can share their resources and can build more applications such as having two VCRs connected to two tuners with either VCR able to record the signal from either tuner. Within HAVi there is no single device master controller, any device can control other devices. Controlling and controlled devices might be located anywhere within the network. Any device within HAVi can act as controlling and controlled at the same time. Currently HAVi uses digital IEEE-1394 network. IEEE-1394 provides bandwidth up to 800Mb/s which enables isochronous communication and simultaneously handles multiple real-time digital AV streams. The software elements comprising HAVi are 1394 Communication Media Manager, Registry, Event Manager, Messaging System, Resource Manager, Stream Manager, Device Control Module, Functional Component Module, Device Control Module Manager and Application.

HAVi provides inter-relationship between other networking standards in respect to audio/video prospective. The main benefit of such inter-relationship is to build bridges with other networking standards as it provides additional benefits to consumer. Irrespective of underlying hardware or implementation details using HAVi the software API and the HAVi bridges, CE manufacturers can allow audio/video devices to interoperate within and across different network. This specification is designed to address interoperability for audio and video systems, which does not address wider interoperability issues.

9. Smart Home to Smart City

Smart homes provide promising concept of smart city and due to its services it makes it available for the smart citizens. Smart home services like smart grid, vehicles, mobile social networks, wireless communication are some of the fundamental services needed for smart city. Security and privacy are the two major issues which are very much needed from the smart home to the smart city.

Smart homes are the fundamental unit in smart cities, all the services described for smart home are used for building the smart city. All the devices used to build smart home must be secure and easy to use by the citizens. The services discussed in the paper for smart homes are used to build the smart city. Figure 5. explain how the security architecture is interacting.

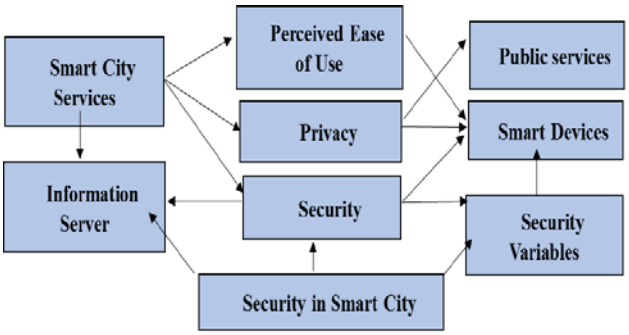

Figure 5: Security Architecture for Smart City

10. Conclusion and Future Research Work

The paper is providing educational aspect of the service orientation now which is in very advanced stage of implementation in smart home design, which is fundamental unit for the smart city. The solutions described in this paper do not offer any mechanism for discovery and composition of devices and services. Some solutions require separate hardware adaptors for conversion of appliances into networked appliances, which is somewhat restrictive as distributed computing and service models are becoming more pervasive. As such devices and services are more heterogeneous, this makes management of such framework more complex. As technologies become more sophisticated, control placed on devices and service integration becomes more difficult.

DHT-based P2P implementations adopted a more distributed model [11]. Pure P2P models unlike Napster are difficult to control due to the absence of a central server. It is expensive to maintain DHT-based solutions because more time is spent updating indices. DHT-based solutions provide efficient data access but exponential cost as the number of peers joining and leaving the network increases. If a DHT approach is not used, then computational costs are reduced, however it required an exhaustive traversal of the network which causes network flooding. These solutions work well in structured networks where control can be placed on network topology as opposed to unstructured networks such as global P2P network where devices continually come and go. Using distributed computing model such as P2P and service-oriented architecture needs a new approach to be used to enable ad hoc services to be shared and discovered within global network without or with less human intervention. The new approach provides services such as service discovery, service registration, service sharing and provides gateway services to make communication possible not only in the same network but also with other remote networks [10].

References

[1] Behnaz Nahvi and Habibi, J., "Improving Service-Oriented Architecture Processes in Process of Automatic Services Composition Using Memory and QF, QWV Factor", International Journal of Advanced Computer Science and Applications(IJACSA).vol. 7, no. 6, (2016),pp. 189-197.

[2] Bull, P.M., Benyon, P.R., and Limb, P.R., "Residential gateways", BT Technology Journal.vol. 20, no. 2, (2002),pp. 73-81.

[3] CES,"Consumer Electronic Show",http://www.cesweb.org/, (accessed 01 December 2016).

[4] Cheng, S.-T., Wang, C.-H., and Horng, G.-J., "OSGi-based smart home architecture for heterogeneous network", Expert Systems with Applications.vol. 39, no. 16, (2012),pp. 12418-12429.

[5] DPWS,"Devices Profile for Web Services ",http://www.ws4d.org/, (accessed 15 December 2016).

[6] Hartog, D., Balm, M., De Jong, and Kwaaitaal, J.J.B., "Convergence of residential gateway technology", IEEE Communications Magazine.vol. 42, no. 5, (2004),pp. 138-143.

[7] Kaneko, M., Arima, K., Usami, M., Sugimura, H., Isshiki, M., and Koh, K., "Development of information living integrated by home appliances and web services", Proceedings of the IEEE 4th Global Conference on Consumer Electronics (GCCE),(2015), 27-30 Oct. 2015.

[8] Lee, G., "DPWSim: A Devices Profile for Web Services (DPWS) Simulator", IEEE Internet of Things Journal.vol. 2, no. 3, (2015),pp. 2327-4662.

[9] Lee, M., Kim, Y., and Lee, Y., "A home cloud-based home network auto-configuration using SDN", Proceedings of the IEEE 12th International Conference on Networking, Sensing and Control,(2015), 9-11 April.

[10] Liu, G., Shen, H., and Ward, L., "An Efficient and Trustworthy P2P and Social Network Integrated File Sharing System", IEEE Transactions on Computers.vol. 64, no. 1, (2015),pp. 54-70.

[11] Ma, H., Tan, S., and He, Z., "The research of P2P recognition technology", Proceedings of the IEEE 5th International Conference on Software Engineering and Service Science,(2014), 27-29 June 2014.

[12] Madjid Merabti, Paul Fergus, and Abuelma'atti, O., "Internetworking the Home - Networked Appliances and Home Networking" in "Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications", IGI Global, (2010), pp. 171-180

[13] Microsoft,"A Technical Introduction to the Devices Profile for Web Services - MSDN",http://msdn.microsoft.com, (accessed 25 Decemeber 2016).

[14] Muhammad, A., Fergus, P., Merabti, M., and Askwith, B., "Peer-to-Peer Overlay Gateway Services for Home Automation and Management", Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA),(2010), 20-23 April.

[15] Muhammad, A., Merabti, M., and Askwith, B., "E-System: Package Delivery Framework", Proceedings of the Second International Conference on Developments in eSystems Engineering (DESE),(2009), 14-16 December

[16] Muhammad, A., Merabti, M., Askwith, B., and Fergus, P., "Ad Hoc Gateway Service for Automatic Package Delivery using Networked Appliances", Proceedings of the IEEE Wireless Communications and Networking Conference,Kowloon, China, (2007), 11-15 March.

[17] OASIS,"OASIS: Organization for the Advancement of Structured Information Standards",http://www.oasis-open.org/home/index.php, (accessed 15 November 2016).

[18] OSGi,"OSGi and the Enterprise",http://www.osgi.org/wiki/uploads/Links/OSGiAndTheEnterpriseBusinessWhitepaper.pdf, (accessed 01 December 2016).

[19] OSGi, 2014. *OSGi Service Platform Core Specification*

[20] Park, Y.S., Park, S.H., Lee, K.T., and Yoon, M.H., "DLNA protocol analysis tool for smart device interoperability test", Proceedings of the International Conference on Information Networking (ICOIN),(2015), 12-14 January.

[21] Thomas Erl, Clive Gee, Berthold Maier, Hajo Normann, Pethuru Raj, Leo Shuster, Clemens Utschig-Utschig, and Wik, P., "Next Generation SOA: A Concise Introduction to Service Technology & Service-Orientation ",Prentice Hall (2014).

[22] Toschi, G.M., Campos, L.B., and Cugnasca, C.E., "An UPnP architecture for interoperability in Home Area Network", Proceedings of the IEEE International Symposium on Consumer Electronics (ISCE),(2016), 28-30 September

[23] W3C,"ebXML - Enabling A Global Electronic Market",http://www.ebxml.org/, (accessed 20 November 2016).

[24] Zeeb, E., Bobek, A., Bonn, H., and Golatowski, F., "Lessons learned from implementing the devices profile for Web services", Proceedings of the Inaugural IEEE International Conference on Digital Ecosystems and Technologies,Cairns, Australia, (2007), 21-23 February.