

PLEASE NOTE! THIS IS SELF-ARCHIVED VERSION OF THE ORIGINAL ARTICLE

To cite this Article: Rajamäki, J. & Rathod, P. (2013) Leveraging Benefits of Standardized Utility and Cloud Computing with Service-oriented Architecture in Public Protection and Disaster Relief . In Sergio Lopes (Editor) Recent Advances in Computer Science and Networking. 2nd International Conference on Information Technology and Computer Networks (ITCN '13), October 8-10, 2013, Antalya, Turkey, 74-80.

URL: <http://www.wseas.us/e-library/conferences/2013/Antalya/ITCN/ITCN-08.pdf>

Leveraging Benefits of Standardized Utility and Cloud Computing with Service-oriented Architecture in Public Protection and Disaster Relief

JYRI RAJAMÄKI and PARESH RATHOD

Laurea SID Leppavaara

Laurea University of Applied Sciences

Espoo

FINLAND

{jyri.rajamaki, paresh.rathod}@laurea.fi <http://www.laurea.fi/en>

Abstract: - The Public Protection and Disaster Relief (PPDR) organizations are using Information and Communication Technology (ICT) services in very heterogeneous and customized delivery methods. Majority organizations have tailored processes, contracts and technologies. In many cases, these are managed by internal and external suppliers. Currently, ICT field is going through many innovations as a process of evaluation in technologies. On the one hand, cloud computing, utility computing and service-oriented architecture (SOA) have shown promising potential. While on the other hand, these technologies are bringing various challenges. There is a gap in knowledge leveraging benefits of such technologies, especially in the fields of PPDR. This paper studies utility and cloud computing with service-oriented architecture in the context of ICT services. The study argues that all processes, technologies and contracts in utility computing should be standardized to leverage the full benefits of these innovative technologies in PPDR. Paper also discusses and describes the benefits of standardization as well as some potential issues due to lack of standardization.

Key-Words: *ICT Services, Cloud Computing, Service-Oriented Architecture (SOA), Utility Computing, Public Protection and Disaster Relief (PPDR)*

1 Introduction

Information and communication technology (ICT) services are undergoing an evolutionary phase. The traditional ICT services used to be built of hardware and software components. These are now offered as commodity services. Organizations have realized that the personalized service model where everyone used to build their own services may not be the most effective solution. The application of shared large scale utility services combined with Service Oriented Architecture (SOA) is more flexible both from the financial and service quality perspective. Multiple standardized utility services already exist, e.g., Customer relationship management (CRM), managed operating systems, e-mail, instant messaging and file sharing. Deployment can be quick, and service charge is based on actual consumption, time, transactions or other measurable units.

Deployment of utility services has been typically automated, making it a very effective way to duplicate the service to multiple clients. From the business perspective, this approach is warmly welcomed—time of project deployment reduced dramatically, and substantial investments are not required. For example, the ICT costs for the Finnish government in 2009 were 1.8% out of the entire Finnish government's costs [1]. Additionally, even

service pilots can be done in a very short time and with minimal investments.

The Public Protection and Disaster Relief (PPDR) actors have significant organizational and technical problems with interoperability, intercommunication and interconnection with each other. In the European Commission Framework Programme 7 security theme, this research activity is divided into four areas: information management, secure communications, interoperability and standardization [2]. An actual technical problem is that every participant organization has its own ICT solutions, and even if they have the same program, it is not shared. Every authority has its own installation of the same program, which means that they might have different versions of it.

This paper investigates leveraging benefits of utility, cloud and service-oriented computing, and also how processes, technologies and contracts surrounding ICT services could be standardized especially in the field of Public Protection and Disaster Relief. Further, advantages of standardizing and disadvantages of not standardizing are discussed. A novel conceptual method is presented for PPDR organization and how they can prepare for the benefits of utility and cloud computing with SOA presented. The paper is a descriptive paper resulting in practical recommendations in the field.

2 Service Standardization to Utility Model

Utility services are defined as a “collection of technologies and business practices that enables computing to be delivered seamlessly and reliably across multiple computers” and “capacity is available as needed and billed according to usage” [3]. In this model organizations are able to use resources when and according their consumption need.

Traditionally ICT services have been insourced or outsourced, and the platform is fixed for the organization only. This means an organization using the ICT service has a dedicated environment for them. Organizations have the possibility to use their own technologies. In many cases they are partly legacy, their own support methods and processes and also custom contracts both internally and externally. In utility services, multiple customers using the service underneath shared platform. As the service is shared, the customers in a multi-tenancy environment have no or very little possibility of special tailoring for their service.

In shared service, all customers need to follow the service lifecycle and service conditions much more strictly than they are probably used to doing [4]. The common practice of non-standard customized technologies is informal processes and gentleman agreements. As a contrast, global utility computing service suppliers having thousands of customers from different background and cultures, have standard technologies, processes and contracts for their service catalogue.

2.1 ICT Architecture and Trends

Ross and Westerman [3] studied large ICT outsourcing arrangements in different circumstances. Their research provides clear recommendation on how organizations can achieve fruitful outsourcing agreements. They also predict that, in the future, organizations will continue their outsourcing as part of utility computing. Smaller organizations will more likely make a partnership with one supplier, whereas large organizations are more likely to use selective sourcing with their network of suppliers [3].

Increasingly organizations are moving their services to cloud computing as their utility service, because using resources when needed is strategically feasible and financially beneficial. In order to use cloud resources firm’s architecture should be standardized. A heterogeneous environment cannot get the benefits of utility computing and therefore a strong global standardization is required. Some

organizations seek partners to help them to standardize the environment to compensate their resource deficit and allow organizations to have a roadmap for utility services.

The demand for ICT services are increasing every day. Hence, standardized architecture would be more beneficial and needs to develop strong strategy of it. This allows organizations to have the cost effective outsourcing models and to move towards utility computing efficiently.

2.2 Computing Exchange and Contracting

Buyya et al. [4] have studied how cloud computing as utility is going to change the computing model. They have presented a model in which computing capacity is provided by the same model as electricity exchange. In current electricity exchange model, the market prices are changing based on demand and supply. A similar model could work in the ICT domain where large data-center and powerful computing capacity holders could sell their services on market price. And anyone requiring could buy for the best market price. Within this model, brokers buy and sell capacity (e.g, computing, storage), and enterprises purchase capacity where they can get it most economical and can customize according to their need [4]. The idea of computing exchange sounds an effective way of managing the demand and supply of computing capacity globally. However, the technology and standards that support the movement of ICT services between different suppliers’ data-centers on the fly do not exist yet.

Another very important aspect is the agreement in addition to the technical boundaries. In order to make computing exchange possible, all different types of contract terms for computing exchange should be standardized and preferably categorized to avoid possible risks. The risks would include: the supplier is selling more capacity than it actually holds, which might cause unavailability of service, performance issues or inability to transfer the service between the suppliers. Different type of Quality of Service (QoS) agreements must be in place together with penalties, aligned with service level agreements and key performance indicators. Several ways to measure performance exist.

2.3 Demand Management and Processes

One of most significant study of ICT management history from 1970 to 21st century carried out by Salle [5]. His studies reveals how the ICT domain started to work in a more structured way and how the same ICT service management practices have spread around the world. Thus, core ICT processes

look similar in most organizations. Salle also describes how the roles of ICT managers are changing from technical ICT experts to organizations' strategic business partners who manage the services based on the business' requirements.

In the early years of ICT, it was seen as a technology only and not as a service for business organization. Hence, there were no common processes or practices existed for ICT problem management. The IBM Information Systems Management Architecture (ISMA) was the first service management practice that was created to respond to this problem. ISMA was later extended and refined with, for example, Information Technology Infrastructure Library (ITIL), HP IT Service Management (ITSM) and Microsoft Operations Framework, which are taking a broader look into service management and defining core functions and processes in more precise and practical ways.

Organizations are increasingly aware that, in order for ICT to be managed efficiently, a standardized service management framework needs to be followed. When organizations consider changing a part of the business support into utility services, they need to validate their capability to operate with a supplier following ITSM principles. For the client organization, the challenge is not to manage the technology any longer but to master the demand from business, and work with the supplier accordingly.

2.4 Standardization of ICT Services

There are three pillars of ICT services and should be standardized on the journey to utility services: 1) technology, 2) contracts and 3) processes. These are presented in Table 1. We have briefly presented the benefits for both supplier and customer organizations when these pillars are standardized.

The first standardization aspect is the applied technology and architecture. For example, a client is looking for the most efficient hosting solutions for their web application developed with PHP. PHP is a popular web application development language. We can find hundreds of hosting services which provide a managed hosted server where clients can install their own PHP applications. Clients are not required to have their own teams around the clock to maintain the availability of servers; this is done by the supplier. These types of utility services are typically cost effective as the same platform can be shared among tens of clients with no customization or manual work. However, if the web application needs to run some customised scripts on the host

operating system then service offering disrupted. It is very rare to find such suppliers where customers have options to access data files at an operating system level and run scripts in supplier portfolio. This would make the management complex if users had customized access. It would also cause security concerns if the users had access to each other's data. In such cases, the client would be required to have a non-standard and dedicated service for them which is considerably more expensive. Applications which are not built to run on standard technology and based on best-practices can be very expensive in the long run.

TABLE 1. SERVICE STANDARDIZATION

	Standardized	Non-Standardized
Technology and Architecture	<ul style="list-style-type: none"> -Operations can be automated. -Commodity cost effective to run, transferable from supplier to another. -No specific knowledge required. 	<ul style="list-style-type: none"> -Tailored and heterogeneous. -No automation, a lot of manual work. Hence, it can be costly. -Client specific knowledge needed.
Contracts	<ul style="list-style-type: none"> -Predefined service levels and penalties, formal papers and agreements. 	<ul style="list-style-type: none"> -Based on gentleman agreements, no official warranties or penalties.
Process	<ul style="list-style-type: none"> -Ability to operate with practically any supplier. -Capability to manage changes and problems between the companies not just between people. 	<ul style="list-style-type: none"> -Based on people relationships, no roles. -Does not scale up to support broad business models.

The next standardized aspects are contracts. They would describe the service performance, availability, support hours, and other aspects. They are commonly referred as different Service Level Agreements (SLAs). If the contract between the supplier and the client does not have any warranties about performance or service hours, later on the client (or the supplier) could be in trouble. Clients should confirm that their suppliers are capable of delivering services based on their contractual requirements, such as 24/7 support or four hour response time for the contact centre. If contracts are standardized and they describe the sufficient service detail, it is possible to compare service between

different suppliers. Hence, over all standardised contract helping both clients and suppliers.

The final aspect is process standardization. Within all leading ITSM frameworks, some processes are very similar. Common ITSM processes include the change management, problem management and incident management. All of these processes have certain roles from both suppliers' and clients' perspectives. Communication and collaboration are very complex if no common understanding exists about what is an incident or what are the responsibilities of the change manager. A typical issue would be clients who are unfamiliar with ITSM practices. The requests cannot be managed by a single person in varying situations. Organizations which are used to working with gentleman agreements will need to revise their requirements. Standardized processes are beneficial for both the client and the supplier.

3 Cloud Computing and SOA Approach

The organizations in private and public sectors are interested in knowing what cloud computing is and what it can bring to them? There are four different cloud computing deployment models: Public cloud, Private cloud, Community cloud and Hybrid cloud. Fig. 1 depicts these four deployment models.

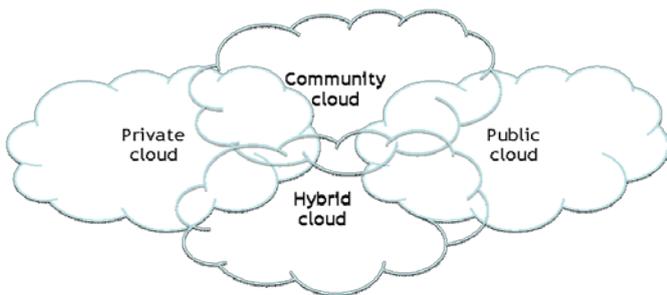


Fig. 1 Cloud computing deployment models

3.1 Cloud Computing Categories and Models

In the Public cloud deployment model, the cloud infrastructure is provided for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or combination of them. It exists on the premises of the cloud provider [6]. In the Private cloud deployment model, the cloud infrastructure is provided exclusive use for single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by

one or more organization, a third party, or combination of them, and it may exist on or off the premises. [6].

In the Community cloud deployment model, the cloud infrastructure is provided for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off the premises [6].

While in Hybrid cloud deployment, the cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but which are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [6].

There are three service models of cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In SaaS, a client only pays for the use of the software. The user has extremely limited rights to the software. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user specific application configuration settings. In PaaS service model, the client maintains the software used by them and the cloud provider maintains the hardware and the virtualization. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application hosting environment [6]. While in IaaS service model, the cloud provider maintains only the hardware, and the client takes care of the rest. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls)[6]. Fig. 2 depicts how these responsibilities work in different service models.

Security is one of the biggest concern and reason behind cloud services not been implemented widely as would be expected, especially in the public sector and authority work, where the security is playing a crucial role in everyday function. Almost all information they are dealing with is confidential and

sensitive in nature. The Public cloud has the biggest problems with security because it is unrestricted in use, so everyone can buy the services and put their own software to the same cloud. That brings security challenges due to exploitation of vulnerabilities. In comparison to the Public cloud, the Private cloud deployment model has the least security problems.

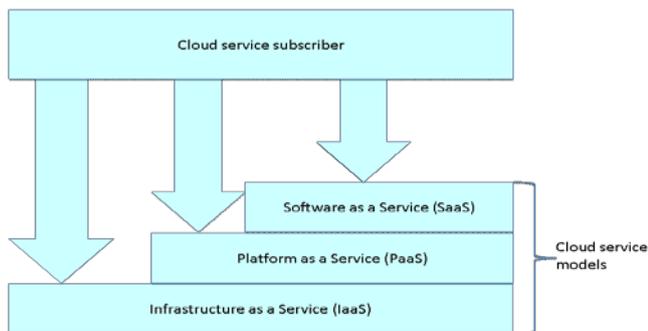


Fig. 2 Cloud service models

3.2 Service-Oriented Architecture (SOA)

SOA is an architectural paradigm, the main characteristics of which are to promote loose coupling, reusability and interoperability during the designing and implementation of a software system [9]. SOA is all about fixing existing systems' architecture, addressing them as services and abstracting those services into a single domain and solution.

As shown in Fig. 3, there are three key components which are essential to building SOA services. The service provider can build a SOA service, but if the service is not published anywhere then no-one can use it because of the invisibility of those services. That is why the service provider has to publish it in a Discovery Agency. The service requester will find compulsory service descriptions at the Discovery Agency. With this description, the client can make the connection to the right service provider by adhering to the communication agreement and is able to use the SOA service [8].

4 ICT Systems for Public Protection and Disaster Relief

In recent years, the capabilities of PPDR responders across Europe have been considerably improved with the deployment of new technologies including dedicated Terrestrial Trunked Radio (TETRA) networks. However, there are challenges in public safety communications especially 1) lack of broadband connectivity and 2) lack of

interoperability. Our previous researches have addressed this problem by introducing new model [15][18]. We are further expanding our conceptual model by leveraging benefits of standardised utility computing and cloud computing with service-oriented architecture (SOA) as discussed in previous sections. Fig.4 on next page depicts proposed standardized ICT Service model for PPDR organizations. The model is outcome of leveraging benefits of cutting-edge technologies.

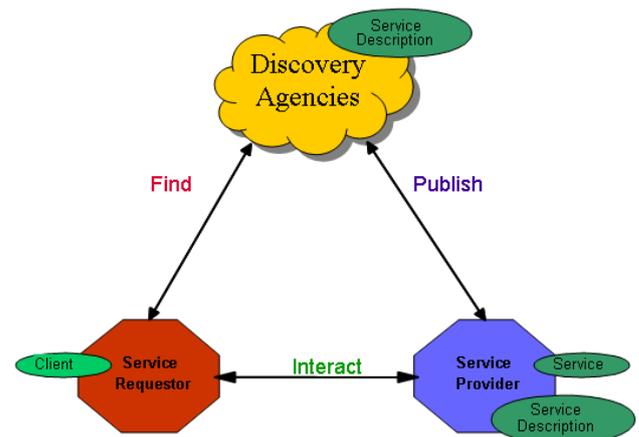


Fig. 3 SOA Architecture [9]

On the journey to utility computing, ICT services should be standardized, as neither clients nor suppliers can utilize the benefits of utility computing unless this is done. Benefits of standardized technologies, processes and contracts are obvious. A client is able to change its supplier more flexibly if the service is transferable from one supplier to another. The technology must be commodity compliant, so clients are able to so move their services. Also, the suppliers will have more providers of commodity services. The price of standard utility services is decreasing and in order clients to be able to take advantage of this trend, they need to be compliant with standard service platforms, contracts and processes.

Due to the nature of utility services, the standardization should be driven by a group of suppliers rather than, e.g., legal requirements. The standards should be voluntary and defined by consortia of organizations. This type of *de facto* standards, typically created by individual firms, groups of companies or in industrial associations, could be flexible and easily adopted by the community of service suppliers and clients. Ownership of standard development should be similar to the ITSM processes, where consortia of organizations are maintaining the industry practices [16], [17].

The cloud computing deployment can enhance the communication between PPDR organizations. It could also be the answer to reducing the ICT costs of governments. Selecting the right cloud model also provides secure data communication and flexibilities.

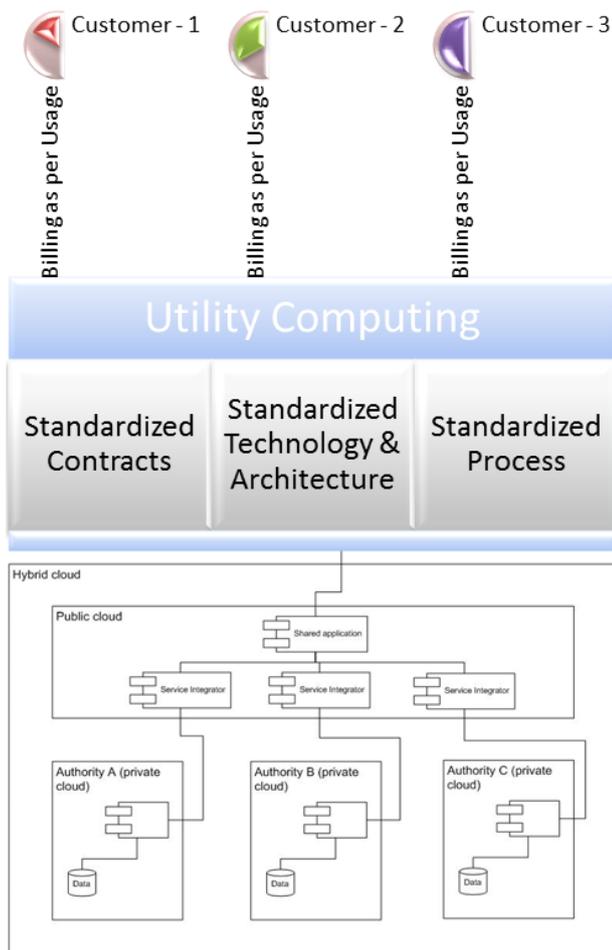


Fig. 4 Standardized ICT Services for PPDR

The Hybrid cloud is a cloud deployment model that can be provided via a secure virtual private network. This deployment model offers a flexible and secure model to implement cloud services. Flexibility means that PPDR organizations can start with the Public cloud services and, when they are ready with available service oriented type of services, they can switch to the Private cloud smoothly. Ultimately, they will be ready to expand the Public cloud to the Hybrid cloud. These integrations are done safely if the components could implement the 'SecureCloud' security model [14]. A suitable cloud service model would be the SaaS model, mainly because it helps better communication between PPDR organizations.

If authorities implement cloud services, it would reduce the ICT costs of PPDR organizations, mainly

because of service centralization, which would mean that all software and maintenance costs are centralized. Ultimately, the needs of software licenses, middleware licenses and maintenance would be reduced. Another advantage of service centralization is reducing complexity to the application life cycle. In order to merge existing applications together, a lot of time and resources are needed, especially in solving all the challenges of the integration. The same concept can mean different things for different organizations. These differences come from individual use of the applications by the authorities over the years. This concept problem can be solved using a SOA. In that case, every PPDR organization can have its own service inventory and services can be composed as required; that also helps avoid actual data conversion. The conversion take place at the integration level and reduces further complexities and problems.

5 Discussion and Conclusion

The current state of all PPDR organizations is heterogeneous. They have their own customized technologies, processes and contracts. for each supplier. In order for clients and suppliers to get the best benefits out of their ICT services, they should focus on *de facto* standardization of ICT services:

- Organizations should focus on how to standardize their technology and architecture to be technically compliant with utility services. All tailored nonstrategic solutions should be planned for retirement or migration.
- Organizations need to ensure that they are up-to-date with global ITSM methodologies. The ITIL framework is a good industry standard to follow. To work effectively with ICT suppliers, ITIL processes should be followed.
- Organizations should validate their development with contracts. Gentleman agreements must be changed to standard contracts. Terms of SLAs and QoS must be agreed with the supplier in order to ensure service quality and make services transferable.

This paper deals with ITSM from the strategy perspective, looking at its overall picture. However, the methodologies in multi-supplier management in ITIL core processes have not been studied yet. Each PPDR organization has its own requirements for ICT services. When external suppliers are providing ICT services, standard services might be inflexible for the multi-tenant service base. Suppliers' standard

services might not respond to all client requirements. It is vital to understand and study the ways organizations can manage the gaps between the suppliers' standard services and clients' requirements. Our approach is not looking at the dependencies between the different ICT services for a multi-supplier service base but only from a single ICT service perspective. In the future, synergies and/or conflicts between different SOA based ICT services should be studied within a multi-supplier service base. Additionally, the differences between traditional outsourcing and cloud sourcing governance methodologies should be investigated.

References:

- [1] Y. Benson., "Valtion ICT 2010-2013," Valtiovarainministeriö, 2010. Available: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20100503JulkIT/04_Benson_ValtIT_R024.pdf
- [2] European Commission C. 4536, 2010. Available: <http://ec.europa.eu/research/participants/portal/download?docId=32768>
- [3] J. W. Ross, G. Westerman. "Preparing for utility computing: The role of IT architecture and relationship management," IBM Systems J., vol 43, no. 1, 2004.
- [4] R. Buyya, C. Yeo and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," 10th IEEE Int. Conf. on High Performance Computing and Communications, 2008.
- [5] M. Salle, "IT service management and IT governance: Review, comparative analysis and their impact on utility computing," HP Laboratories, HPL-2004-98, June 2, 2004
- [6] P. Mell and T. Grance, "The NIST definition of cloud computing," Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, 2011.
- [7] Cloud Security Alliance. "Top threats to cloud computing V1.0", 2010. Available: <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
- [8] OWASP. The Open Web Application Security Project, 2010.
- [9] M. Champion, C. Ferris, E. Newcomer, et al. "Web service architecture," W3C Working Draft. 2002. Available: <http://www.w3.org/TR/2002/WD-ws-arch-20021114/>
- [10] G. Baldini. "Interoperable communications for safety and security," presented at the workshop organized by DG ENTR and DG JRC with the support of EUROPOL and FRONTEX, Ispra, Italy, June 2010. Luxembourg: Publications Office of the European Union, 2010.
- [11] M. Rantama, "Mapping the future for Finland's rescue services," TetraToday, issue 3, pp. 32-35, 2011.
- [12] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, "A TCP/IP communication architecture for distribution network operation and control", Proc. 17th Int. Conf. on Electricity Distribution, Barcelona, Spain, 2003.
- [13] J. Holmström, J. Rajamäki. and T. Hult, "The future solution and technologies of public safety communications – DSiP traffic engineering solution for secure multichannel communication," Int. J. of Comm., issue 3, vol.5, pp.155-122, 2011.
- [14] H. Takabi, J. B. D. Joshi and G.-J. Ahn, , "Securecloud: Towards a comprehensive security framework for cloud computing environments," Computer Software and Applications Conference Workshops (COMPSACW), presented at the IEEE 34th Annual, pp. 393-398, 2010.
- [15] J. Lehto, J. Rajamäki, and P. Rathod., "Conceptualized view on can cloud computing improve the rescue services in Finland?", In *Proceedings of the 11th WSEAS international conference on Applied Computer and Applied Computational Science(ACACOS'12)*, World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, USA, 2012. pp65-70.
- [16] A. Kivimäki, Wireless telecommunication standardization processes, University of Oulu, Department of Information Processing Science, 2007.
- [17] S. Wardley , "Cloud Computing - why IT matters," Open Source Conv.. San Jose, CA, July 20-24, 2009.
- [18] J. Rajamäki and P. Rathod., "Service Standardization with Utility Computing and SOA as a Tool for PPDR", In *Proceedings of the 2013 European Intelligence and Security Informatics Conference (EISIC '13)*. IEEE Computer Society, USA, 2013 (in print)