Conceptualised View on Can Cloud Computing Improve the Rescue Services in Finland?

Jouni Lehto[1], Jyri Rajamäki[1] and Paresh Rathod[1]
[1]Laurea University of Applied Sciences, Vanha maantie 9, 02650 ESPOO, FINLAND
{jouni.lehto, jyri.rajamaki, paresh.rathod} @laurea.fi http://www.laurea.fi/en/

Abstract: The Rescue Services in Finland have a significant problem of communication with other authorities who also participate in the rescue process. The greatest challenge is a lack of shared programs, applications or any other e-services which they can use to communicate with each other. The cloud computing might be the answer for this problem. There are several solutions and guidelines available. This paper explores which cloud computing deployment model and cloud service model could be suitable to address the problem. Further study also conducted on cloud services provided by The Public Authority Network (VIRVE) in Finland. The paper also presents current and future VIRVE cloud services status.

Keyword(s): Cloud computing, Cloud security, Cloud services, Rescue service, Secure cloud, Public authority network, Public safety communications, VIRVE

1 Introduction

The Finnish law defines rescue authorities are responsible for safety in any kind of day to day incident, unlikely event of catastrophe or war [1]. The rescue services are further classified in three categories: accident prevention, rescue activities and civil defense. The functional responsibilities divided between State and Regional rescue service. The authorities taking part in rescue services are the Emergency Response Centre Administration, Finnish Police, Border Guard, Finnish Defense Forces, Ministry of Social Affairs and Health, National Public Health Institute, National Agency for Medicines, National Product Control Agency for Welfare and Health, Radiation and Nuclear Safety Authority, National Authority for Medicolegal Affairs, Finnish Institute of Occupational Health, Ministry of Agriculture and Forestry, state enterprise for forestry Metsähallitus, Ministry of Transport and Communication, Civil Aviation Administration, Finnish Meteorological Institute, Finnish Maritime Administration, Finnish Rail Administration, Finnish Communication Regulatory Authority, Regional State Administrative Agencies, and offices and agencies in charge of the various branches of municipalities [2].

The range of authorities who have a duty to take part of the rescue work is quite extensive as you can draw a conclusion from above. The Government took a decision to divide Finland into 22 smaller rescue service regions [3]. The functions of regional rescue services are performed in cooperation between the municipalities of the region, as lay down by law [2].

Fig. 1 shows a usual rescue service process. In such scenario, process begins with the citizen observing the situation and calling the Emergency Response Centre Administration. The operator in the Emergency Response Centre Administration will try to find out all the information which is necessary, and after that the Operator will alert the right rescue units to the destination according to response guideline. In a fire situation, the fire department will get the task from the Emergency Response Centre Administration, and the firemen are alarmed to start proceeding toward the fire station. Before departing, they have to check the actual address of the destination manually. Some times to locate the address might take a while if the address is unfamiliar or unknown.

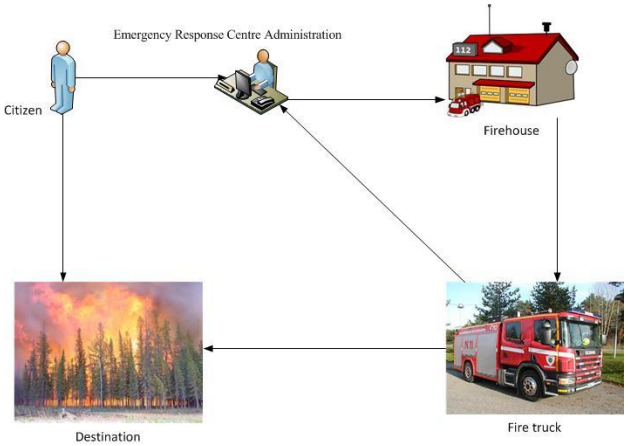

Fig. 1 Usual rescue scenario and process

ISBN: 978-1-61804-084-8

On the way to the destination the rescue unit will try to get all possible information for rescue service beforehand. This will happen with various mean, especially by phones and computers. After the rescue unit has arrived at the destination, they start to brief the Emergency Response Centre Administration and the other rescue units which are still on the way.

1.1 VIRVE Network

VIRVE (– a Finnish acronym for Common Network for Authorities) is nationwide radio network, and mainly used by Finnish authorities who have a duty to take part in rescue operations. VIRVE Radio Network is based on the Terrestrial Trunked Radio (TETRA) standard. TETRA standard has been implemented and developed by the European Telecommunication Standard Institute (ETSI).

The introduction of the VIRVE Radio Network in Finland has enabled a high level of multi-authority co-operation at the (incident) scene. All authority actors have the same basic needs for the system and data communication, but also have their own distinct requirements. An intention exists for finding mutual solutions and operation models, facilitating system integration and enabling coherent system design. Improved activities, cost savings, and better multi- authority co-operation are desirable at the scene [4].

VIRVE IP Network is operated by the State Security Networks Ltd., which is limited non-profit company owned by the Finnish Government [5]. Fig. 2 gives the rough picture of the current situation of the VIRVE IP Network.

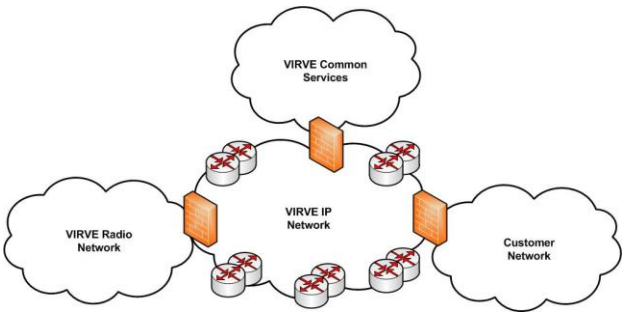

Fig. 2 High-level current VIRVE IP Network

As shown in Fig. 2 the VIRVE IP Network is a backbone for the whole authority network. All the customers which in this case are the Finnish authorities have their own networks. These customer networks are connected to the VIRVE IP Network and all communication between them goes through the VIRVE IP Network. But all customer networks are also accessible outside of the VIRVE IP Network. Inside of the VIRVE IP Network it is possible to limit the access between the customer networks with firewalls. At the moment VIRVE Common Services provide common services to all its clients. These common services include the short message service inside of the VIRVE IP Network. These common services are provided from the demilitarized zone (DMZ) of the VIRVE IP Network [12].

As mentioned before, the VIRVE Radio Network is based on TETRA standard. At the moment, the VIRVE Radio Network is used to transfer conversations and data. The main common services are group calls and short data messaging. The VIRVE Radio Network implements the TETRA Release 1 standard at the moment. TETRA Release 1 has extremely limited data transfer rate; around 2-4 kbit/s. There are also plans to use TETRA Enhanced Data Service (TEDS). TEDS is a wideband data solution which enhances TETRA with much higher capacity and throughput for data. TEDS maximum data transfer rate is about 100 kbit/s [13].

1.2 Cloud Computing

Currently cloud computing is a growing business, and in the headlines all the time. The companies in private and public sectors are interested to figure out what the cloud computing is and what it can bring to them. Often companies are interested in cloud computing because it would offer cost efficiency, flexible infrastructure, easy maintain and perhaps more security. One of the biggest advantages of cloud computing is low starting expense, which is possible when the customer does not have to buy for themselves frightfully expensive hardware or software. This also means that the expenses from building and maintaining the environment will not come to the customer directly. The only cost to the cloud service user is the monthly or annually access right costs. The users pay only for the resources which they use.

Cloud computing is the main category and there are four different cloud computing deployment models: Public cloud, Private cloud, Community cloud and Hybrid cloud. Fig. 3 depicts these four deployment models.

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

ISBN: 978-1-61804-084-8

(e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. [6].

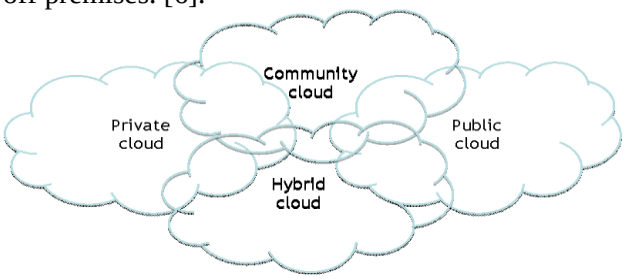

Fig. 3 Cloud computing deployment models

In the Community cloud deployment model, the cloud infrastructure is provisioned 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 premises. [6]

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

With rough partitioning, the services of the cloud computing can be divided in three service models which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In the service model SaaS, a client only pays from the use of the software. 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 actual used software by them self and the cloud provider maintain 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]. 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. 4 depicts how these responsibilities go in different service models.

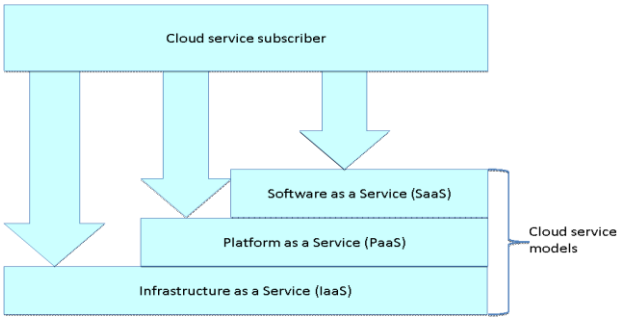

Fig. 4 Cloud service models

Security is one of the biggest questions and reasons why the cloud services have not been implemented yet as much as would be expected. Especially, in the public sector and authority work where the security is playing mighty crucial role in every day live. Almost all information they are dealing with is confidential and sensitive in nature. Public cloud has the biggest problems with security, because it is in public use, so everyone could buy the services and put their own software to the same cloud. Even if, you are sure that your program is safe, does not mean that your data is safe. In the same cloud might be some other programs, which may not be as safe as your program and this makes the whole cloud unsafe. On the contrary to public cloud, the private cloud deployment model has the least security problems. Cloud Security Alliance (CSA) has rated the top 7 usual threats to cloud computing. The purpose of that document, "Top Threats to Cloud Computing", is to provide needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies [7]. The Open Web Application Security Project (OWASP) has rated the top 10 most critical web application security risks and worth to notice when maintaining or building a new web application [8]. With these two threats and risks listing, it is possible to reduce the data security threats. That ultimately reduces cloud security vulnerabilities and strengthens delivery of secure cloud services.

2 Problem Formulation

The Rescue Service in Finland has a significant problem of communication with the other

ISBN: 978-1-61804-084-8

authorities who also participate in the rescue process. The actual problem is that every authority has its own IT -solutions and even if they have the same program, it is not shared. Every authority has its own installation of the same program and it means that they even might have different versions of it.

The ICT cost is one problem where the authorities have to pay attention. The ICT costs for the Finnish government in 2009 were 1.8% out of entire Finnish government's costs [9].

The VIRVE Radio Network does not work in some shadow regions. So, sometimes the rescue workers cannot have the information they need on-site and they do not have a way to brief the other authorities. Even if the VIRVE Radio Network is available, the strength of a signal might be weak and the network unusable. Even though the VIRVE Radio Network does not have a strong signal that does not mean there is no network available at all. Still there might be some networks to use, but how they can choose the right one with the best signal strength? The selection of the right network is not sufficient; the connection must be safe and secure. In reality, this is not the whole problem; there might be an area where the signal strength varies between other networks. And that is why there might be a need to change the connected network on the fly without losing connection or broken signals during such operation. Overall, these are three main rescue service problems faced by authorities.

3 Problem Solution

The cloud computing within the VIRVE IP Network might be the answer to above mentioned challenges. This research work is focused to figure out how cloud computing could be used to help the Finnish authorities on their daily rescue operations. Fig. 5 shows one suitable solution of how cloud computing could be used inside the VIRVE IP Network. The cloud services can be offered from the VIRVE IP Network as a common service. As earlier explained, all the client networks have access to the network of common services. Hence all the network connections are already available which are necessary for utilizing the cloud services from the client networks. Within the VIRVE IP Network, it is possible to limit access to the different services with firewalls if necessary. This means that all communication inside the VIRVE IP Network can be monitored. Monitoring and limitation means that there is a way to reduce the misuse and the possible security attacks.

When cloud services are provided inside a private network having only authority users, the security risks are extremely limited. The possible security threats are, for example, misuse of the software and unsafe software interfaces. Misuse in this context means that some official accesses someone's personal information without permission. Unsafe interfaces will cause security problems if there were integrations outside the private network, but also when there might be unreliable workers who can have access to the network. They can utilize these security flaws and gain information which they are not allowed to. But as mentioned earlier, with proper monitoring and controlling such security problems and risks can be handled. There are also ways to catch such misusers.

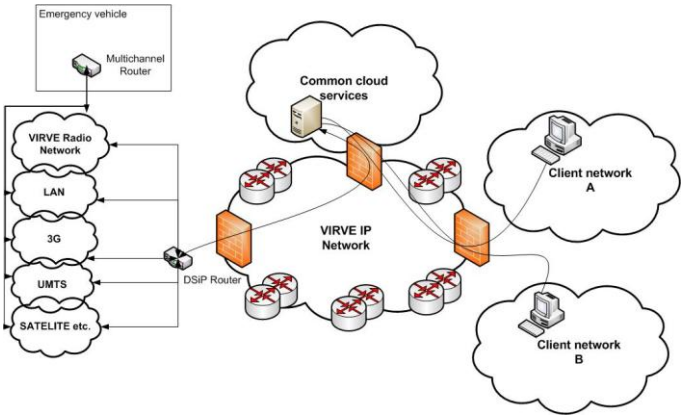

Fig. 5 Cloud computing inside VIRVE IP Network

Inside the VIRVE IP Network it is possible to provide many different versions of programs, applications, services and solutions from cloud deployment models. The Private cloud deployment model would mean, in the VIRVE IP Network every authority organizations have their own cloud services and no-one else have access to its services. This model can reduce the ICT costs and will make maintaining easier, but it would not make the communication between authorities any easier than before.

The Community cloud deployment model could be possible but in this context, it would mean that someone or some authorities have to provide a cloud services from their own client network. And in this research it is not considered as a possible way to proceed, because in this model maintenance of the cloud services would not be centralized. Centralization of maintenance is one of the main ways of saving the ICT costs.

The Hybrid cloud deployment model might be the best model to provide the cloud services from the VIRVE IP Network. In this model, all authority

ISBN: 978-1-61804-084-8

organizations have a possibility of own private cloud; which is also provided from common cloud services from the VIRVE IP Network, and not from their own client network. Further all organizations have access to service from public cloud model. With this private cloud, they can protect their private information from other authorities and they can provide the necessary information from public cloud as a public service. With service oriented approach, it is possible to build new applications that provide services to all authorities, at the same time it is possible to limit access to the sensitive data and enhance security. All parts of the Hybrid cloud deployment model could be provided as the centralized services. So this model will give the best and possibly most suitable way to build common cloud services to the Finnish authorities. Fig. 6 presents this model combination.

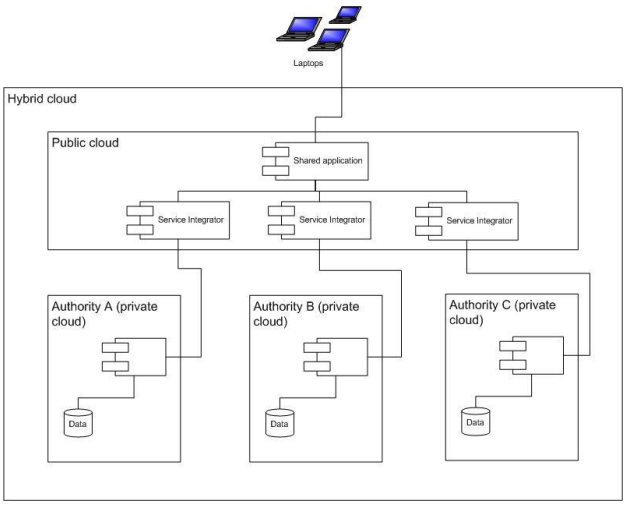

Fig. 6 The Hybrid cloud model with service oriented approach

SecureCloud [10] is a security model for cloud computing with the idea to integrate many different cloud services together in a secure way. This security model introduces the component called Service Integrator. This component's work is to take care of all security issues which are needed for secure integration between different applications.

The Public cloud deployment model itself would be enough for making the communication between the authorities better. However, it will not give the same protection to sensitive data as the private deployment model inside the hybrid model. In this context, the Public cloud deployment model means that data is visible and accessible to all Finnish authorities but not publically available for the whole world via the Internet. At the moment, the Public cloud deployment model could be the right one to start with because the authorities do not have service oriented way built services which could be provided from the Private cloud. As mentioned earlier, the range of software is wide; even if different organizations use same applications, they might have a different version of them. So, the first step should be that all the authorities have to get to use the same application and the same version of it. This can be done with the Public cloud model and software as a service (SaaS) model. In order to have such solution, actually it means extremely sturdy and complicated conversions. Conversions are unavoidable, because every authority has its own concepts and in order that existing application can be put together as one perfect solution, these concepts must be merged first.

In the future when authorities have built their own service oriented services, the Public cloud deployment model could be changed to the Hybrid model. This, however, means that there must be someone who provides the Hybrid cloud and takes care of maintenance. This provider must also check all the services which will become a part of the service portfolio of the Public cloud. Naturally in Finland, the State Security Networks Ltd., who already operates the VIRVE IP Network, might be the right one acting as a cloud provider.

Because of capacity limits at the moment, applying cloud services from an emergency vehicle could be difficult. The limited data transfer rate of the VIRVE Radio Network has to be taken into account when planning to use it for cloud services. TEDS might bring some relief, but it would not be enough for using cloud services nationwide. Distributed Systems intercommunication Protocol® (DSiP) [11] could be applied to cover this problem. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using the wide range of physical media, including IP and non-IP communication. It dramatically increases the reliability, security and controllability of communication systems being totally independent of operators [4]. With DSiP, the access to the VIRVE cloud services can be extended safely from the VIRVE Radio Network, e.g., to the 2/3/4G, WLAN and Satellite network. The DSiP will hide the selection of the network from the software level. This will mean that the software does not know which network is used. To this extend the cloud services are usable from the emergency vehicle. In order to have the DSiP work from emergency vehicle will mean that every emergency vehicle has to have a multichannel DSiP node inside it.

ISBN: 978-1-61804-084-8

4 Conclusion

The cloud computing can be used to help the Finnish authorities to communicate better between each other. The cloud computing could be the answer to reduce the ICT costs of the Finnish government.

The right cloud deployment model, which could be provided from the VIRVE IP Network, is Hybrid cloud deployment model. This deployment model offers the most flexible and most secure model to implement cloud services by the VIRVE IP Network. Flexibility means that the authorities can start with the Public cloud services and when they have more service oriented type of services available could convert to the Private cloud; ultimately they are ready to expand the Public cloud to the Hybrid cloud. These integrations are done safely if the components will implement the 'SecureCloud' security model. The suitable cloud service model would be the SaaS model, mainly because it will improve the communication between the Finnish authorities.

The VIRVE Radio Network is not ready yet to be used for data transfer from cloud services. Before cloud computing can be used for emergency vehicles, the capacity of the VIRVE Radio Network has to be increased or some other transfer channel has to be used. At the moment, the VIRVE IP Network allows authorities access from their client network to the VIRVE Common Services Network. This makes possible the provision of cloud service even today. If authorities applied cloud services, it would reduce the ICT costs of the Finnish government, because of service centralization. The centralization would mean that all software and maintenance costs are centralized. Ultimately, the necessary needs of middleware licenses, software licenses and maintenance would be reduced. Another advantage of service centralization is that it will also reduce complexity to the application life cycle.

In order to merge existing application together, a lot of time and resources are needed for solving all the problems, which will arise when combining all the concepts. The same concept may mean different things for different organizations. These differences have arisen just because of individual use of the applications by the authorities over the years. One solution for this concept problem is the service oriented architecture (SOA) where every authority can have its own service inventory and compose required services as needed; this way they can avoid the actual data conversion. The conversion would be done in the integration level, so it might reduce the further problems and complexities.

References:

[1] *Rescue services in Finland*, Ministry of the Interior, Department for Rescue Services, Finland 2010, http://www.pelastustoimi.fi/en/responsibility

[2] *Finnish Rescue Act 468/2003*, Chapter 2, 6§.

[3] *Rescue services in Finland*, Ministry of the Interior, Department for Rescue Services, Printed by Aldus Oy, 2010

[4] J. Holmström, J. Rajamäki and T. Hult, The future solution and technologies of public safety communications – DSiP traffic engineering solution for secure multichannel communication, *International Journal of Communication*, Iss 3,Vol.5, 2011, pp.155-122.

[5] State Security Networks Ltd. - Front page, http://www.erillisverkot.fi/?lang=en

[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] *Top Threats to Cloud Computing V1.0*, Cloud Security Alliance, 2010, https://cloudsecurity alliance.org/topthreats/csathreats.v1.0.pdf

[8] OWASP, The Open Web Application Security Project, 2010, https://www.owasp.org/index. php/Category:OWASP_Top_Ten_Project

[9] Y. Benson, Valtion ICT 2010-2013, Valtiovarainministeriö, 2010, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakir jat/03_muut_asiakirjat/20100503JulkIT/04_Be nson_ValtIT_R024.pdf

[10] 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), 2010 IEEE 34th Annual*, pp. 393-398.

[11] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, "A TCP/IP communication architecture for distribution network operation and control", *Proc. of the 17th Internal Conference on Electricity Distribution Barcelona, Spain*, 2003.

[12] G. Adams, G. Ben-Ari, *Transforming European militaries: coalition operations and the technology gap*, Routledge, 2006.

[13] TETRA Interoperability and Certification explained, TETRA Association, 2011, http://www.tetramou.com/Library/Documents/ TETRA_Resources/Library/Reports/TETRA% 20Interoperability%20and%20Certification%2 0explained_Issue4.pdf