LAUREA AMMATTIKORKEAKOULU Uuden edellä

Pelastustoiminnan parantaminen katvealueella sekä pilvipalveluiden hyödyntäminen pelastustoiminnassa: suunnittelututkimus

Lehto, Jouni

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Pelastustoiminnan parantaminen katvealueella sekä pilvipalveluiden hyödyntäminen pelastustoiminnassa: suunnittelututkimus

Jouni Lehto
Ylempi AMK
Tietojärjestelmäosaamisen koulutusohjelma
Lopputyö
Tammikuu 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojärjestelmäosaamisen koulutusohjelma, ylempi AMK

Jouni Lehto

Pelastustoiminnan parantaminen katvealueella sekä pilvipalveluiden hyödyntäminen pelastustoiminnassa: suunnittelututkimus.

Vuosi 2012 Sivumäärä 68

Pelastustoiminnassa Suomessa on yhtenä isona ongelmana viranomaisten välinen kommunikaatio. Ongelma on, että heillä ei ole yhteisiä järjestelmiä eikä muitakaan sähköisiä palveluita, joiden avulla he voisivat kommunikoida. Pilvipalvelut voisivat olla yksi ratkaisu tähän ongelmaan. Tutkimuksessa keskitytäänkin selvittämään millaisia pilvipalveluita on olemassa sekä mikä niistä sopisi parhaiten Suomen pelatustoiminnan tarpeisiin sekä miten palveluja voitaisiin tarjota nykyisestä VIRVE -verkosta. Lisäksi tutkitaan miten lait, säädökset ja ohjeet vaikuttavat Suomen pelastustoimintaan rakennettaviin sovelluksiin.

Toisena isona ongelmana ovat katvealueet, joissa ei saada yhteyttä viranomaisverkkoon (VIRVE). Kuitenkin olisi hyvä, että katvealueellakin ainakin tärkeimmät tietojärjestelmät toimisivat paikallisesti hälytysajoneuvossa. Tässä tutkimuksessa rakennetaankin kokonaisarkkitehtuuriratkaisua, jolla taklataan ainakin osa niistä ongelmista, jotka syntyvät, kun yritetään käyttää sellaisia ohjelmia paikallisesti, joita ei siihen tarkoitukseen ole rakennettu. Kokonaisarkkitehtuurissa otetaan myös kantaa siihen miten pilvipalveluita voitaisiin hyödyntää viranomaistoiminnassa.

Tämän tutkimuksen tuloksena syntyneessä kokonaisarkkitehtuurissa on lähdetty siitä, että VIRVE -runkoverkosta tarjottaisiin sen sisällä olevia julkisia pilvipalveluita SaaS -mallin mukaisesti eli jossa palveluiden käyttäjät hankkivat vain sovelluksen käyttöoikeutta ja ylläpitovastuu on pilvipalvelun tarjoajalla.

Kokonaisarkkitehtuurissa esitellään myös hajautusratkaisu, jossa voidaan ylläpitää saman sovelluksen tietoja ilman, että niillä on sama tietolähde. Tässä ratkaisussa hyödynnetään uudenlaista tietokantaratkaisua NoSQL, joka ei perustu relaatiotietokantaan, vaan NoSQL -toteutuksesta riippuen kantaan tallennetaan joko avain-arvopareja tai kokonaisia dokumentteja.

Asiasanat: Pilviteknologia, pilvipalvelu, tietoturva, NoSQL, VIRVE, pelastustoimi

Laurea-university of Applied Sciences **Abstract**
Laurea Leppävaara
Master Degree in Information Systems

Jouni Lehto

Improve the rescue work at the shadow region and how the cloud computing can be used to improve the rescue work: design research in information systems

Year 2012 Pages 68

The Rescue Service in Finland has a major problem with the communication with the other authorities who also participate in the rescue process. The problem is that they don't have shared programs or any other e-services which they can use to communicate with each other. The cloud computing might be the answer for this problem. In this research is figured out which cloud computing deployment model and cloud service model would be suitable. How these cloud services can be provided from VIRVE IP Network nowadays and in the future are presented in this research. How the laws, regulations and guidelines effects to the application building in Finnish rescue service area, is figured out in this research.

The second biggest problem which they have is shadow regions where the rescue authorities can't get the connection to the VIRVE network. It would be better if these important programs could work locally in emergency vehicle. Enterprise Architecture which will be the result of this research, will reduce some of the problems which will come when installing the programs locally when they are not intend to work that way. How the cloud computing can be used in Finnish rescue services, is also covered in the enterprise architecture.

The Enterprise Architecture which will be the result of this research is based on the knowledge that the cloud services will be provided from VIRVE IP Network with SaaS service model. In SaaS service model the cloud subscribers only pays from the rights to use the application and the provider has the maintain responsibility.

The decentralized solution is also presented in the enterprise architecture. With this decentralized solution it is possible to maintain the same information from different application without they have the same database. In this solution is utilized the new database solution called NoSQL. NoSQL is not relational database, but depend on the used implementation; it will save key-value pairs or whole documents to the database.

Key-words: Cloud computing, Cloud service, Cloud security, NoSQL, VIRVE, Rescue services

Sisällysluettelo

1 Johdatus aihealueeseen

Tutkimus on osa Tekesin rahoittamaa MOBI-hanketta, jonka tavoite on uudentyyppinen viranomaisajoneuvon sovellus- ja tietoliikennearkkitehtuuri, joka perustuu standardoituihin rajapintamäärittelyihin. Tutkimuksessa on selvitetty miten pelastustoiminnassa voitaisiin hyödyntää pilvipalveluja sekä mitä pilvipalvelujen käyttöönotossa tulisi huomioida niin tietoturvan osalta kuin palvelukeskeisen arkkitehturin (SOA) kannalta. Tukimuksen lopputuloksena esitellyssä kokonaisarkkitehtuurissa otetaan myös huomioon pelastustoiminnassa ongelmana olevat katvealueet, jolloin järjestelmät eivät toimi. Kokonaisarkikitehtuurissa esitellään hajautusratkaisu, jonka avulla eri hälytysajoneuvot jakavat tietoja keskenään sekä yleisiin pilvipalveluihin. Viranomaistoimintaa rajataan, valvotaan sekä ohjataan useiden lakien, säädösten ja ohjeiden avulla, joten tutkimuksessa selvitetään mitkä kaikki lait, asetukset sekä ohjeet tulee huomioida esitettyssä kokonaisarkkitehtuurissa. Kokonaisarkkitehtuurin tarkoituksena on parantaa viranomaisten toimintaa sekä helpottaa heidän välistä tietojen välittämistä.

1.1 MOBI

Poliisin, tullin, rajavartiolaitoksen ja pelastuslaitosten keskeisimpiä työtehtäviä on erilaisten hälytysluontoisten tehtävien hoitaminen maalla, vesillä ja ilmassa. Heidän käyttämiensä ajoneuvojen ja niihin asennettujen laitteiden tulee sopeutua hyvin vaativiin ja erilaisiin olosuhteisiin. Myös vuodenaikojen vaihtelu lisää vaatimuksia. (Rajamäki, 2010.)

Viranomaisten ajoneuvoihin on vuosikymmenten kuluessa lisätty teknistä laitteistoa, jolloin ajoneuvon käyttäjien käyttöliittymien määrä on noussut kymmenillä ajoneuvon hallinnan käyttöliittymien lisääntymisen myötä. Tämä on johtanut ajoittaisiin toiminnallisuusongelmiin (esimerkiksi turvatyynyn toimintatilan supistuminen) ja teknisiin ongelmiin sähkönsaannissa ja kaapeloinneissa. Lisäksi sovellettujen ratkaisujen dokumentointi on ollut vaihtelevaa eikä kaivattua standardoitumista alalla ole tapahtunut laitetoimittajien moninaisuudestakin johtuen. (Rajamäki, 2010.)

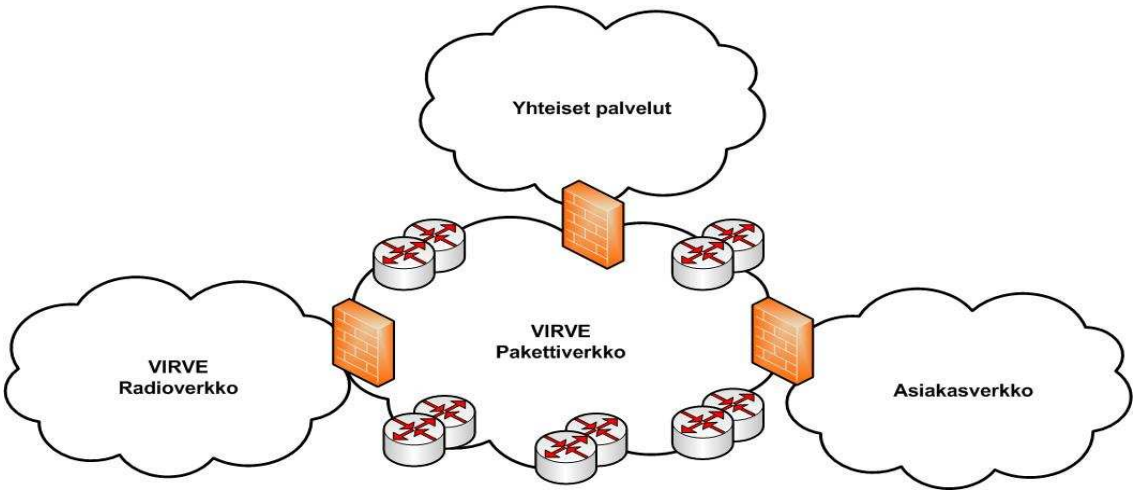
1.2 Pelastustoimi

Pelastustoimi kuuluu sisäasiainministeriön alaisuuteen. Ministeriön tehtävänä on valvoa pelastustoimen palveluiden saatavuutta ja tasoa. Sen tehtävänä on myös huolehtia pelastustoimen valtakunnallisista valmisteluista ja järjestelyistä sekä yhteensovittaa eri ministeriöiden toimintaa pelastustoimessa. Lääninhallituksen tehtävänä on vastata omalla alueellaan käytännön tehtävistä. Pelastustoimen suunnittelua, kehittämistä ja seurantaa varten sisäasiainministeriön apuna on pelastustoimen neuvottelukunta (Pelastuslaki, 2003). Pelastuslain (2003) 2 luvun 6§ mainitaan, että Pelastusviranomaisten ohella velvollisia

osallistumaan pelastustoimintaan ja väestönsuojeluun siten kuin niiden tehtävistä kunkin toimialan säädöksissä tai muussa lainsäädännössä säädetään ovat: 1) Hätäkeskuslaitos; 2) poliisi; 3) rajavartiolaitos; 4) puolustusvoimat; 5) sosiaali- ja terveysministeriö, Kansanterveyslaitos, Lääkelaitos, Sosiaali- ja terveydenhuollon tuotevalvontakeskus, Säteilyturvakeskus, Terveydenhuollon oikeusturvakeskus, Työterveyslaitos; 6) ympäristöministeriö, Suomen ympäristökeskus, alueelliset ympäristökeskukset; 7) maa- ja metsätalousministeriö, Metsähallitus; 8) liikenne-ja viestintäministeriö, Ilmailulaitos, Ilmatieteen laitos, Merenkulkulaitos, Ratahallintokeskus, Viestintävirasto; 9) lääninhallitus; sekä 10) kunnan eri toimialoista vastaavat virastot ja laitokset. Tästä syystä pelastustoiminnassa yhdeksi hyvin tärkeäksi osaksi syntyy tiedon liikkuminen eri viranomaisten välillä. Samaisen pelastuslain (2003) 9 luvun 43§ kerrotaan pelastuslain mukainen kuvaus pelastustoiminnan sisällölle. Pelastustoimintaan kuuluu hätäilmoitusten vastaanotto, pelastusyksiköiden ja muun avun hälyttäminen, väestön varoittaminen, uhkaavan onnettomuuden torjuminen, vaarassa olevien ihmisten, ympäristön ja omaisuuden suojaaminen ja pelastaminen, tulipalojen sammuttaminen ja muiden vahinkojen torjuminen ja rajoittaminen, jälkiraivaus ja -vartiointi sekä näihin liittyvät johtamis-, tiedotus-, huolto- ja muut tukitoiminnat (Pelastuslaki, 2003).

1.3 Suomen Erillisverkot Oy

Suomen Erillisverkot Oy ylläpitää tällä hetkellä viranomaisverkkoa (VIRVE). Eri viranomaiset ovat yhteydessä VIRVE -runkoverkkoon ja kaikki liikenne eri viranomasverkkojen välillä kulkee tämän runkoverkon kautta kuten kuvasta 1 nähdään.



Kuva 1 VIRVE -runkoverkko tilanne vuonna 2011 (Kuva saatu Suomen Erillisverkot Oy:ltä)

Runkoverkossa on palomuurein rajattavissa mistä verkosta päästään mihinkäkin verkkoon. Tällä hetkellä VIRVE -runkoverkossa ei Antti Koposen Suomen Erillisverkko Oy:stä mukaan ole kaikki viranomaiset, mutta tämän tutkimuksen kannalta siellä on mukana kuitenkin

pelastustoimi sekä hätäkeskus. Suomen Erillisverkot Oy on valtion 100% omistama voittoa tavoittelematon osakeyhtiö. Yhtiön tehtävä on tuottaa myös poikkeusoloissa turvallisia, häiriöttömiä ja toimintavarmoja verkkopalveluita (Suomen Erillisverkot Oy, 2011).

1.4 Pilvipalvelut

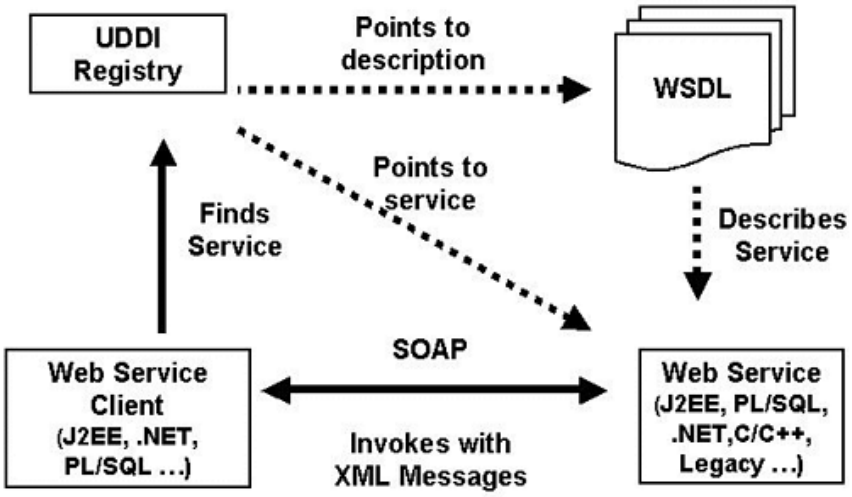
Tänä päivänä kaikki puhuvat pilvipalveluista, mutta kuinka moni oikeasti tietää mitä pilvipalveluita oikeasti on ja mitä yleensä pilvipalveluilla tarkoitetaan. Tutkimuksessa avataan käsitettä pilvipalvelu sekä käsitellään tarkemmin mitä riskejä tulee ja kannattaa ottaa huomioon suunniteltaessa siirtymistä julkiseen pilvipalveluun tietoturvanäkökulmasta. Julkinen pilvipalvelu tämän tutkimuksen kontekstissa tarkoitta yleistä pilvipalvelua VIRVE -runkoverkossa. Tämä palvelu ei näy julkiseen Internettiin, vaan julkisen siitä tekee se, että eri viranomaiset pääsevät samoihin palveluihin.

Pilvipalveluilla yleensä haetaan kustannustehokkuutta, joustavaa kapasiteettipalvelua sekä helpompaa hallittavuutta. Pilvipalveluiden yhtenä suurena etuna ovatkin halvat aloituskustannukset, jotka tulevat siitä, että ei tarvitse hankkia laitekapasiteettia tai kalliita sovelluslisenssejä itselleen, jolloin ei myöskään tule niiden pystytys kustannuksia. Pilvipalveluina tarjotaan yleensä laitekapasiteettia, sovelluspalvelinkapasiteettia sekä sovelluskapasiteettia. Tässä tutkimuksessa selvitetäänkin miten Suomen Erillisverkot Oy voisi tarjota pilvipalveluita Suomen viranomaisille ja miten vastuukysymykset sekä tietoturva tässä tapuksessa menisi.

1.5 Määritykset – Sanasto – Lyhenteet

Lyhenne	Selite
Pelastustoiminta	Pelastustoimintaan kuuluu hätäilmoitusten vastaanotto, pelastusyksiköiden ja muun avun hälyttäminen, väestön varoittaminen, uhkaavan onnettomuuden torjuminen, vaarassa olevien ihmisten, ympäristön ja omaisuuden suojaaminen ja pelastaminen, tulipalojen sammuttaminen ja muiden vahinkojen torjuminen ja rajoittaminen, jälkiraivaus ja -vartiointi sekä näihin liittyvät johtamis-, tiedotus-, huolto- ja muut tukitoiminnat (Pelastuslaki, 2003).
SOA	Service Oriented Architecture, palvelukeskeinen arkkitehtuuri.
SLA	Service Level Agreement. Tietojärjestelmien palvelusopimuksien palvelutasot sekä laatukriteerit sovitaan tällä sopimuksella.
VIRVE	VIRVE on olennainen osa pelastus- ja turvallisuusviranomaisten johtamisjärjestelmää. Se tarjoaa mahdollisuuden kommunikoida

	tietoturvallisesti yli viranomaisrajojen. Järjestelmään määritellyt puheryhmät tukevat tehokkaasti operatiivista johtamista. Tilannekuvan tiedot ja ohjeet saadaan perille yhdellä kertaa kaikille operaatioon osallistuville. (Sisäasiainministeriö, 2009). VIRVEä operoi ja sen palveluista vastaa sisäasianministeriön ohjauksessa Suomen Erillisverkot Oy. VIRVEn käyttäjäkunta muodostuu kuitenkin useiden ministeriöiden sekä eri pelastus- ja turvallisuusviranomaisten käyttäjistä. Käyttäjiä on yhteensä noin 31.000. (Sisäasiainministeriö, 2009). VIRVE rakennettiin korvaamaan yli 50 aiemmin eri viranomaisia palvellutta tietoliikenne- ja radioverkkoa. VIRVE -verkko on maan kattava. Verkko perustuu TETRA -teknologialle ja on suunniteltu viranomaistarpeita varten. (Sisäasiainministeriö, 2009). VIRVEn toiminta-ajatuksena on tuottaa laadukkaita, toimintavarmoja ja kustannustehokkaita operaatiokriittisiä tietoliikenne- ja järjestelmäpalveluja turvallisuusviranomaisten viestintä-, johtamis- ja yhteistoimintatarpeisiin. (Sisäasiainministeriö, 2009). Kansainvälisissä vastaavien turvallisuusverkkojen vertailuissa VIRVE on todettu suhteessa pinta-alaan ja tukiasemamäärään kustannustehokkaaksi. Myös verkon käyttäjämäärä ja käyttöaste ovat asukaslukuun suhteutettuna korkeita. (Sisäasiainministeriö, 2009). Turvallisuusviranomaisten toiminta edellyttää tehokasta ja turvattua radioviestintää, joka ei saa olla ulkopuolisten kuunneltavissa eikä kaupallisten palveluiden tukkeutuminen saa estää viranomaisviestintää. VIRVEn tärkein käyttömuoto on ryhmäpuhelu, mutta sen ohella erityisesti dataliikenne on voimakkaassa kasvussa. (Sisäasiainministeriö, 2009).
Web Service	Web Service on itsenäinen, itsensä kuvaava komponentti, joka voidaan julkaista, löytää sekä herättää verkon kautta. (Panda, 2005).



Kuva 2 Kuinka Web Service toimii (Panda, 2005)

Kuvan 2 mukaan Web Service käyttäjä (kuvassa Web Service Client) etsii tarvitsemaansa palvelua UDDI -rekisteristä. UDDI tulee sanoista Universal Description Discovery and Integration. UDDI on avoin palvelurekisteristandardi. UDDI rekisteri sisältää Web Service palvelusta WSDL -kuvauksen, joka kuvaa itse palvelurajapinnan. WSDL tulee sanoista Web Service Definition Language. UDDI rekisterissä palvelukuvauksen (WSDL) lisäksi on tieto siitä missä itse palvelu sijaitsee. Kun Web Service käyttäjä saa palvelukuvauksen sekä palvelun osoitteen UDDI reksiteristä, niin se luo SOAP -kuoressa XML -viestin Web Servive -palveluun, josta palvelu vastaa XML (eXtensible Markup Language) -viestillä SOAP -kuoressa. SOAP tulee sanoista Simple Object Access Message.

Taulukko 1 Tutkimuksessa käytetyt lyhenteet sekä erikoissanasto

1.6 Aikaisemmat tutkimukset

Tämän tutkimuksen alueelta on haasteellista löytää vastaavia aikaisempia tutkimuksia, mutta löytyy kuitenkin tutkimuksia, joissa on tutkittu hyvin läheltä asioita tämän tutkimuksen kanssa. Seuraavassa esitelty muutama, jotka ovat lähellä tämän tutkimuksen kontekstia.

Pavan ja muut (2008) tutkimuksessa ongelman lähtökohtana on ollut myrkkykaasut pelastuskohteessa. He ovat tutkineet miten Internetin kautta voitaisiin selvittää pelastuskohteen ilman myrkkypitoisuudet. Pavan ja muiden tutkimus on samassa kontekstissa ja keräävät tietoa Internetin kautta, mutta eivät käsittele tutkimuksessaan kuitenkaan pilvipalveluita eikä muutenkaan viranomaisten yhteistyötä.

Urpila (2011) omassa opinnäytetyössään on käsitellyt pelastusyksikön ajoneuvon teknisen järjestelmien ja laitteiden käyttäjätarpeita sopimuspalokunnissa. Tässä tutkimuksessa Urpila on keskittynyt selvittämään mitä sovelluksia sopimuspalokuntien hälytysajoneussa varsinaiset käyttäjät näkevät tarpeellisiksi. Tästä työstä sain tutkimukseeni lisää tietoa siitä millaisia järjestelmiä paloautoissa yleensä on. Urpilan tutkimuksen pohjalta selvisi, että suurin osa paloauton järjestelmistä liittyy tavalla tai toisella tilanteen johtamiseen tai paikantamiseen.

Junttila ja Rantama (2011) tutkimuksessaan Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa ”PELTI” ovat käsitelleet nimenomaan VIRVE -verkon tulevaisuutta, mutta vain verkon ja sen kehittämisen kannalta ei niinkään palveluiden kehittämisen näkökulmasta. Mutta tästä Junttilan ja Rantaman tutkimuksesta sain hyvän ymmärryksen VIRVE -verkosta ja siitä miten sitä voitaisiin kehittää verkkoteknisesti.

Cerri ja muut (2008) tutkimuksessaan Kohti tietopilveä (engl. Towards Knowledge in the Cloud) ovat selvittäneet miten eri pelastustoimintaan osallistuvien työ helpottuu, kun kaikki heidän tarvitsemansa tieto olisi pilvipalveluissa. Tässä tutkimuksessa pysytään yleisellä tasolla eikä sitä kiinnitetä minkään valtion toimintaan. Cerri ja muut eivät myöskään ota kantaa millaista pilvipalvelumallia kannattaisi käyttää eivätkä he myöskään selvitä lakeja, jotka vaikuttavat viranomaistoimintaan. He eivät myöskään ole tutkineet, millaisia tietoturva-asioita pilvipalveluihin siirtymiseen liittyy.

1.7 Työn tärkeys ja rationaalisuus

Kuten aikaisemmin on tullut jo ilmi, pelastustoiminnassa on ongelmia tiedonvälityksen kannalta niin viranomaisten välillä, kuin myös teknisesti. Suomessa on vielä paljon alueita, joita VIRVE -verkko ei kata, tällöin pitäisi kehittää jotain korviketta, jolla tieto saataisiin eteenpäin toisille viranomaisille. Tässä tutkimuksessa selvitetäänkin juuri sitä miten ilman VIRVE -verkkoa voitaisiin toimia kohteessa.

Pilvipalvelut ovat kasvava trendi niin yrityspuolella kuin myös valtiontoiminnassa. Kustannusten hallinta on yksi tekijä, joka ajaa tutkimaan pilvipalveluiden mahdollisuuksia. Kustannustehokkuuden vastapuolena on tietoturvallisuuden hallinta. Pilvipalveluiden turvallisuus onkin noussut puheenaiheeksi, jolloin asiakkaat miettivät tai niiden ainakin tulisi miettiä tarkasti, mikä muuttuu, kun siirrytään omista konesaleista yleisiin konesaleihin, joista ei välttämättä edes tiedetä missä koneet fyysisesti tulevat sijaitsemaan. Yritysten tietohallintoja painostetaan kustannustehokkuuteen ja saattaa olla, että ns. ylemmältä taholta tulee määräys, että kustannussyistä pitää siirtyä pilvipalveluihin. Näillä päättäjillä, jotka ovat siellä ylemmällä taholla, on mielessä vain kustannukset eivätkä välttämättä osaa

ajatella, että tietoturvasyistä pilvipalveluja ei voida edes käyttää tai sitten pitää hyvin tarkasti määritellä erinäisiä vastuita SLA -sopimuksissa (Service Level Agreement).

Tutkimuksessa selvitetään mitä pilvipalveluja Suomen Erillisverkot Oy VIRVE -runkoverkon ylläpitäjänä voisi tarjota viranomaisille ja tarkemmin pelastustoiminnassa mukana oleville viranomaisille. Tämän lisäksi selvitetään mitkä lait, asetukset sekä ohjeet tulee ottaa huomioon, kun suunnitellaan pilvipalveluita juuri pelastustoiminnassa oleville viranomaisille. Lisäksi selvitetään mitä tietoturvauhkia yleensä pilvipalveluihin liittyy, sillä juuri tietoturvaa pidetään yleisesti yhtenä suurena tekijänä miksi pilvipalvelut eivät vielä ole täysin lyöneet läpi nykypäivän markkinoilla.

Aikaisemmin mainittu katvealue ongelma on yksi tämän tutkimuksen tärkeistä tutkimuskohdista. Miten katvealueella voidaan toimia, kun tietojärjestelmät eivät saa verkkoyhteyttä sekä miten tieto saadaan tällöin liikkumaan? Nämä ovat kysymyksiä johon haetaan tällä tutkimuksella arkkitehtuuriratkaisua. Ratkaisussa pyritään siihen, että olemassa oleviin järjestelmiin ei tarvitsisi tehdä suuria muutoksia, vaan ne toimisivat kuten ennenkin.

Hallinnon turvallisuusverkkohankkeessa (TUVE) suunnitellaan ja toteutetaan valtion ylimmälle johdolle ja yli 30 000 turvallisuusviranomaiskäyttäjälle oma turvallinen, korkean varautumisen tietoverkko (Valtiovarainministeriö/TUVE-yksikkö, 2011). Suojatun verkon käyttäjiä ovat ministeriöiden lisäksi valtion yleisen järjestyksen ja turvallisuuden, maanpuolustuksen, pelastustehtävien sekä väestönsuojelun kannalta keskeiset viranomaiskäyttäjät kuten puolustusvoimat, poliisi, pelastusviranomaiset, rajavartiolaitos ja hätäkeskukset (Valtiovarainministeriö/TUVE-yksikkö, 2011). TUVE -verkko ja -palvelut tulevat olemaan myös muiden yhteiskunnan turvallisuuden kannalta keskeisten toimijoiden käytettävissä (Valtiovarainministeriö/TUVE-yksikkö, 2011). TUVE -verkon kehityksen myötä viranomaisten yhteistyön mahdollisuudet paranevat entisestään. Tästä tutkimuksesta voi olla heille TUVE -verkon palveluiden kehityksessä hyötyä.

1.8 Rajaukset

Tutkimuksessa keskitytään selvittämään pelastustoiminnan parantamista Suomessa vuonna 2011. Lisäksi rakennetaan kokonaisarkkitehtuuriratkaisu pelastustoiminnalle, jonka avulla tiedon välittämistä voitaisiin parantaa. Tutkimuksessa ei ole lähdetty selvittämään tarkemmin eri sovelluksia, joita pelastustoiminnassa käytetään, vaan on lähdetty siitä, että heillä on tietoteknisiä sovelluksia, joita käytetään hälytyksen tekemiseen sekä pelastustoiminnan johtamiseen. Sovellusten on oletettu käyttävän relaatiotietokantaa. Lopputuloksena syntynyt ratkaisu kuvaa tarkoituksella kokonaisarkkitehtuuria eikä teknistäarkkitehtuuria tai sovellusarkkitehtuuria, sillä tässä tutkimuksessa ei ole taroitus mennä kovin tekniselle osa-

alueelle, vaan halutaan tarkoituksella pysyä yleisesti ymmärretyllä tasolla ja näin palvella laajempaa lukijakuntaa.

Kokonaisarkkitehtuuria rakennettaessa on oletettu, että olemassa olevaa relaatiotietokantateknologiaa ja osaamista halutaan käyttää myös tulevaisuudessa, tiedon hajauttamisessa halutaan käyttää hyödyksi olemassa olevia ohjelmistoja, jotta vähennetään rakentamisen, testaamisen ja ylläpidon kustannuksia ja tiedon hajauttamiseen käytetään avoimen lähdekoodin ohjelmistoa, jotta sen toimintaa voidaan itse muuttaa hajautuksen ohjauksen takia, esimerkiksi tiedon prioriteetin ja verkon kapasiteetin osalta. Lisäksi ajoneuvon arkkitehtuurin NoSQL -tietokantana on keskitytty avoimen lähdekoodin ohjelmistoon nimeltä CouchDB.

Ratkaisumallissa on myös oletettu, että hälytysajoneuvolla on jonkinlainen verkkoyhteys tai se osaa sen luoda. Tässä tutkimuksessa ei ole tarkemmin selvitetty miten teknisesti verkkoyhteys luodaan eri hälytysajoneuvojen välille, vaan on yleisellä tasolla tutkittu mitä verkkoyhteyksiä hälytysajoneuvolla voisi olla.

Tutkimuksessa keskitytään vain yleisempiin pilvipalvelujen sekä pilvimallien selvittämiseen. Pilvipalveluista selvitetään mitä ne ovat sekä miten eri pilvipalveluissa vastuujaot käytännössä menevät.

Tutkimuksessa on myös selvitetty Suomen lakeja, säädöksiä sekä ohjeita mitkä liittyvät tässä tutkimuksessa esitettyyn ratkaisumalliin eli kokonaisarkkitehtuuriratkaisuun. Näistä on selvitetty vain ne osat, jotka liittyvät tässä tutkimuksessa esitettyyn ratkaisuun.

Pilvipalveluja mietittäessä tulee ottaa huomioon myös tietoturva-asiat. Tietoturvauhkien selvitys on rajattu OWASP:n ja CSA:n esittämiin tietoturvauhkiin. Näiden uhkien perusteella on kasattu 5 -kohtainen uhkataulukko, jossa on näiden kahden perusteella luotu 5 tärkeintä uhkaa, jotka on sitten käsitelty tämän tutkimuksen kontekstissa.

1.9 Tutkimuksen rakenne

Tutkimuksen ensimmäisessä luvussa perehdytään tutkimuksen aihealueeseen. Luvussa käydään läpi tutkimuksen taustoja selvittämällä osapuolia ja niiden tehtäviä tämän tutkimuksen kontekstissa. Siinä käydään myös läpi tämän tutkimuksen rajauksia sekä tarkastellaan tutkimuksen tärkeyttä ja rationalisuutta. Lisäksi käydään läpi aikaisempia muiden tekemiä tutkimuksia samasta aihepiiristä.

Toisessa luvussa esitellään tutkimusmenetelmä, jota tässä tutkimuksessa on käytetty. Luvussa myös käydään läpi miten menetelmää on tässä tutkimuksessa hyödynnetty sekä lisäksi esitellään tutkimuskysymykset. Kolmannessa luvussa suoritetaan tutkimuksen kirjallisuustutkimusosio, jossa keskitytään tämän tutkimuksen kannalta tärkeisiin osakokonaisuuksiin.

Neljännessa luvussa keskitytään itse tutkimuksen tuloksiin. Siinä esitellään tutkimuksen tuloksena syntynyt malli eli tässä tapauksessa kokonaisarkkitehtuuri pelastustoiminnan parantamiseksi. Viides luku on tutkimuksen keskusteluosuus, jossa pohditaan tutkimustulosten järkevyyttä sekä tuotantokepoisuutta, lisäksi pohditaan miten tutkimusta voitaisiin jatkaa tai mitä muita tutkimusaiheita tutkimus on herättänyt. Viidennen luvun jälkeen tulee yhteenveto, jossa tiivistetään tämän tutkimuksen tulokset.

Yhteenvedon jälkeen esitellään tutkimuksesta löytyvät kuvat sekä taulukot. Yhteenvedon jälkeen on lueteltu kaikki tässä tutkimuksessa käytetty viittausmateriaali. Viitaukset ovat aakkosjärjestyksessä ja niistä on kerrottu mahdollisimman tarkasti, jotta lukija voi tarkistaa alkuperäisen viittauksen niin halutessaan. Osa viittauksista ovat viittauksia Internet -sivustolle, näissä viittauksissa on kerrottu milloin viittaus on tehty.

Liitteenä 1 on INEEE organisaation järjestämään konferensiin ”3rd INEE Conference: ENERGY, ENVIRONMENT, DEVICES, SYSTEMS, COMMUNICATIONS, COMPUTERS” lähettämäni paperin julkaistavaksi sekä esitettäväksi. Konferenssi pidetään 18-20.4.12 Rovaniemellä. Liitteeseen 1 olen tiivistänyt kaikki tutkimukseni tärkeimmät aiheet sekä tulokset. Liitteen 1 kirjoitukseen ovat myös osallistuneet Jyri Rajamäki sekä Paresh Rathod.

Liitee 2 on laajennettu versio liitteestä 1, NAUN -ohjeiden mukaisesti julkaistavaksi NAUN/INTERNATIONAL JOURNAL OF COMMUNICATIONS -lehdessä. Liitteen 2 kirjoitukseen ovat myös osallistuneet Jyri Rajamäki sekä Paresh Rathod. Laajennetussa versiossa vertaan liitteen 1 tutkimuksen pilvimallia Saksassa tehtyyn SPIDER -projektin tuloksiin. SPRIDER –projektissa lähtökohtana oli parantaa Saksan viranomaisten sekä yksityisten yritysten kommunikaatiota SOA –arkkitehtuurin avulla. SPIDER –projektissa kehittettiin myös PRML (Protection and Rescue Markup Language) standardi ehdotus helpottamaan viranomaisten välistä viestinvaihtoa.

2 Tutkimusmenetelmä

Tässä osiossa selvitetään tutkimuksessa käytetty tutkimusmetodi sekä miten menetelmää on käytetty, jotta on voitu vastata tutkimuskysymyksiin. Tutkimuksen menetelmäksi olen valinnut suunnittelutieteellisen tutkimuksen, sillä tutkimuksessa pyritään luomaan IT artefakti, jolla helpotetaan/parannetaan olemassa olevaa ongelmaa.

2.1 Suunnittelutieteellinen tutkimuksen kuvaus

Tutkimusmetodin valinnalla ratkaistaan tutkimuksen tekotapa, tätä helpottaakseen Järvinen ja Järvinen (2004) jakavat tutkimusotteet ensin kahteen luokkaan sen mukaan tutkitaanko reaalimaailmaa vai symbolijärjestelmiä. Esimerkkinä symbolijärjestelmistä Järvinen ja Järvinen (2004) nimeää matemaattiset tutkimusotteet. Reaalimaailman tutkimusotteet koskevat joko sitä millainen reaalitodellisuus on, eli miten asiat nyt ovat, tai innovaation hyödyllisyyden tutkimista, eli sitä miten asiat voisivat olla. Reaalimaailmaa koskevat tutkimusotteet voidaan jakaa käsitteellis-teoreettisiin otteisiin, ja empiirisiin otteisiin, jotka joko testaavat olemassa olevaa teoriaa tai luovat uutta teoriaa. Innovaation hyödyllisyyttä voidaan tarkastella sekä innovaation toteuttamisen että sen arvioinnin näkökulmasta.

March & Smith (1995) mukaan tietojärjestelmätieteen tutkimus voidaan jakaa kahteen eri pääosaan luonnontieteelliseen sekä suunnittelutieteelliseen. Luonnontieteellinen tutkimus on luonteeltaan deskriptiivistä ja siinä yritetään ymmärtää informaatioteknologian luonnetta. Preskriptiivisen tutkimuksen tavoitteena on parantaa informaatioteknologian suorituskykyä. (March & Smith, 1995). Hevnerin ja muiden (2004) mukaan suunnittelututkimuksen tavoitteena on hyödyllisyys. Suunnittelutieteen tuloksena Hevnerin ja muiden (2004) mukaan tietojärjestelmätieteessä luodaan tarkoituksen mukainen IT artefakti, joka käsittelee tärkeätä organisaation ongelmaa. Suunnittelutiede luo ja arvioi organisatoristen ongelmien ratkaisuun tarkoitettuja ja tunnistettuja liiketoimintatarpeita vastaavia tietoteknisiä artefakteja (Hevner ja muut, 2004). Suunnittelutieteellinen paradigma on pohjimmiltaan ongelmanratkaisuparadigma (Hevner ja muut, 2004).

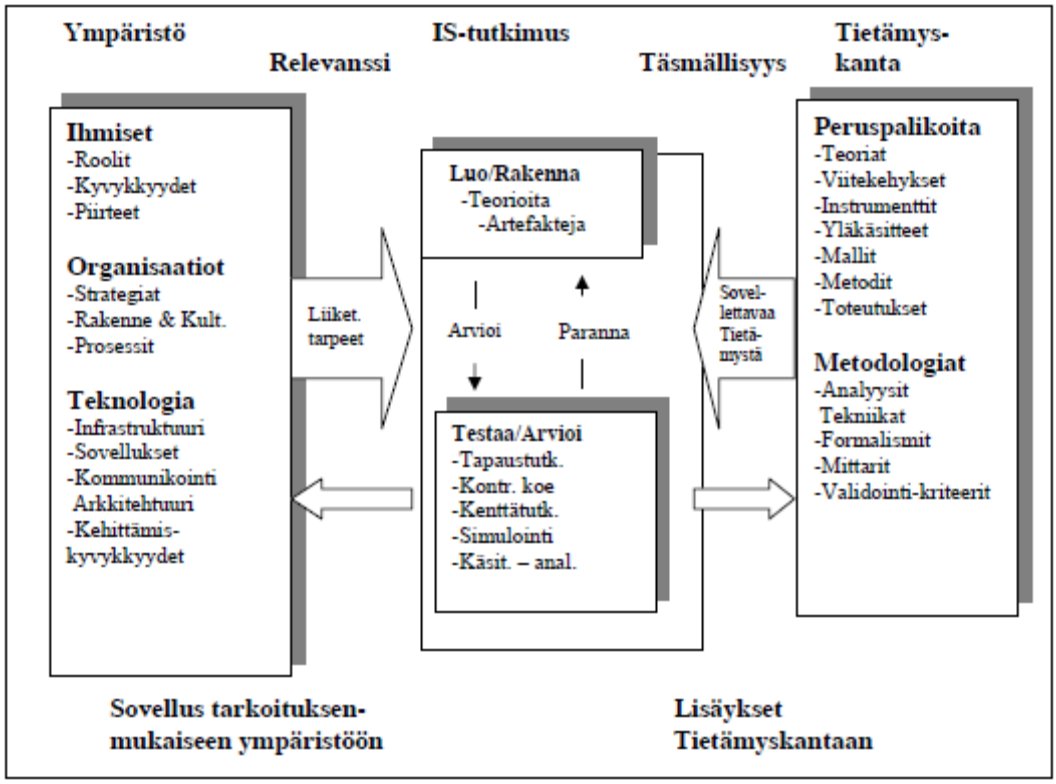
Järvinen ja Järvinen (2004) toteavat tutkimusidean liittyvän johonkin ongelmaan tai kysymykseen, johon halutaan saada vastaus. Esimerkiksi suunnittelutieteellisessä tutkimuksessa lähtökohtana on jokin kohdeympäristön tutkimuskohde tai ongelma. Työympäristössä voi olla esimerkiksi huonosti tai tehottomasti toimiva artefakti, jonka toimintaa halutaan parantaa. Tutkijalla voi olla jo mielessä parannusehdotus, jonka hyvyyttä voidaan tutkia rakentamalla parempi artefakti ja analysoida oliko ratkaisu parempi kuin vanha. Voidaan myös rakentaa kokonaan uusi artefakti, innovaatio, ratkaisemaan jokin työympäristön ongelma. (Järvinen ja Järvinen, 2004; Hevner, March ja Park, 2004.)

March & Smith (1995) kehittämä tietojärjestelmätieteen tutkimuskehys jakauttuu luonnontieteelliseen sekä suunnittelutieteelliseen lähestymistapaan, joka on kuvattu alla olevassa taulukossa.

Tutkimussuoritteet	Suunnittelutiede		Luonnontiede	
	Rakentaa	Arvioida	Luoda teoriaa	Testata teoriaa
Käsitteet				
Mallit				
Menetelmät				
Toteutukset				

Taulukko 2 Tutkimuksen viitekehys (March ja Smith, 1995)

Taulukossa 2 tutkimussuoritteet ovat suunnittelutieteellisen tutkimuksen tulokset: käsitteet, mallit, menetelmät sekä toteutukset. Taulukon vaakasuunnassa kuvataan suunnittelu- ja luonnotieteelliset aktiviteetit: artefaktien luominen tai rakentaminen, artefaktien arvioiminen, teorioiden luominen ja teorioiden perustelu. Käsitteet muodostavat tutkimuksen sanaston. Mallit kuvaavat käsitteiden välisiä suhteita. Menetelmät ovat joukko ohjeita, joiden avulla suoritetaan itse tehtävä. Toteutus on artefaktin raelisointia sen omassa toimintaympäristössä. Toteutuksella testataan artefaktin käsitteitä, malleja ja menetelmiä. Hevnerin ja muiden (2004) mukaan suunnittelututkimus koostuu kahdesta perusaktiviteetistä: rakentaa (engl. build) ja evaluoida (engl. evaluate). Hevnerin ja muiden (2004) mukaan rakentaminen on artefaktin rakennusprosessi tietettyä tarkoitusta varten, kun taas evaluointi eli arviointi on määrittelyprosessi, joka kertoo kuinka hyvin atrefakti toimii. Ongelmalliseksi artefaktin toiminnallisuuden arvioinnin tekee sen toimintaympäristö. Mikäli artefaktin toimintaympäristöä ei tunneta tarpeeksi hyvin, niin se voi aiheuttaa väärin perustein kehitetyn artefaktin tai artefaktin käyttöönotto voi aiheuttaa ei haluttuja sivuvaikutuksia. Heverin ja muiden (2004) mukaan iso haaste onkin osata ennakoida artefaktin käytön mahdollisia sivuvaikutuksia ja varmistaa, että mahdolliset ei toivotut sivuvaikutukset pystyttäisiin välttämään.



Kuva 3 Informaatiosysteemien tutkimuksen viitekehys (Hevner ja muut, 2004)

Hevner ja muut (2004) täydentävät edellä kuvatun Marchin ja Smithin (1995) viitekehystä kuvan 3 kuvatulla tavalla. Kuvan vasemmalla puolella ympäristö kuvaa ongelma-alueen. Ympäristössä ovat tavoitteet, tehtävät, ongelmat ja mahdollisuudet, jotka määrittelevät liiketetoimintatarpeet sellaisina kuin oraganisaatiossa toimivat ihmiset ne näkevät (Järvinen ja Järvinen, 2004). Ympäristössä toimivat ihmiset näkevät liiketoimintatarpeet sen mukaan missä roolissa he toimivat sekä millaiset kyvyt heillä on hahmottaa liiktoimintatarpeita. Organisaatiossa olemassa olevat strategiat, rakenteet sekä prosessit voivat omalta osaltaan vaikuttaa ihmisen näkemyksiin liiketoimintatarpeista. Liiketoimintatarpeita asemoidaan nykyiseen teknologiseen infrastruktuuriin, sovelluksiin, kommunikointiarkkitehtuureihin ja kehittämismahdollisuuksiin (Järvinen ja Järvinen, 2004). Käyttäytymistieteellinen (engl. Behavioral science) lähestymistapa pyrkii selittämään tai ennustamaan yksilöityä liiketoimintatarvetta arvioinnin ja testauksen kautta. Hevnerin ja muiden (2004) mukaan käyttäytymistieteellinen tutkimus tähtää totuuteen. Voidaan myös suorittaa suunnittelututkimus, jossa rakennetaan ja arvioidaan artefakti liiketoiminnan tunnistettuihin tarpeisiin (Järvinen ja Järvinen, 2004). Kun käyttäytymistiede tähtää totuuteen, niin suunnittelutieteessä haetaan hyötyjä. Kumpikin edellä mainittu tapa tukee toisiaan, sillä artefaktin rakentamisessa tarvitaan rakenneosia, joista on saatu totuudellista tietoa käyttäytymistieteellisen tutkimuksen avulla. Artefaktin rakentamisen tai arvioinnin yhteydessä voi löytyä heikkouksia käyttäytymistieteellisestä teoriasta (Järvinen ja Järvinen, 2004). Tietämyskanta sisältää peruspalikoita sekä metodologioita. Peruspalikoihin lasketaan teoriat, viitekehykset, instrumentit, yläkäsitteet, mallit, metodit ja toteutukset, joita

käytetään teorian luonti- ja artefaktin rakennusvaiheessa. Metodologiat sisältävät ohjeita ja mittareita, joiden avulla arvoioidaan teorioita sekä artefakteja.

Järvinen (2005) ohjeistaa tutkimusmetodia valittaessa tarkastelemaan tutkimuskysymystä. Tutkimus kuuluu todennäköisesti suunnittelutieteellisen tutkimuksen piiriin, jos tutkimuskysymys sisältää verbejä rakentaa, muuttaa tai parantaa.

2.2 Tutkimuskysymykset

Tutkimusaiheen valintaan liittyy Järvisen ja Järvisen (2004) mukaan kolme seikkaa: (1) alkuperäisillä tutkimuskysymyksillä kuvataan sitä mitä aiheesta halutaan tietää; (2) tutkimuksen perusteluilla etsitään vastausta siihen miksi halutaan tietää; ja (3) täsmentävien kysymysten avulla pyritään etsimään vastauksia alkuperäisiin kysymyksiin. Tarkoituksena on selkeyttää tutkimuksen kohdetta ja ongelman asettelua sekä selvittää esimerkiksi sitä tuottaisiko tutkimus aidosti uusia löydöksiä.

Tämän tutkimuksen tutkimuskysymykset ovat:

1) Miten voidaan parantaa hälytysajoenuvojen toiminnallisuutta katvealueella pelastustoiminnassa Suomessa?
2) Miten pilvipaveluita voitaisiin hyödyntää pelastustoiminnassa ja miten se parantaisi pelastustoimia?
3) Miten nykyisen VIRVE -verkon palveluita voitaisiin parantaa pelastustoiminnan tehostamiseksi?

2.3 Suunnittelun lähtökohdat

Esittelen seuraavassa Hevnerin ja muiden (2004) määrittelemän 7 kohtaisen ohjeen suunnittelutieteellisen tutkimuksen tekemiseksi sekä kerron miten sovellan ohjeita tässä tutkimuksessa.

1. *Suunnittele/luo artefakti*: Suunnittelutieteellisen tutkimuksen tuloksena syntyy IT-artefakti tiettyyn kohdeorganisaation ongelmaan. IT-artefakti on toteutus, mutta se voi myös olla malli, metodi tai käsite, jolla ratkaistaan liiketoiminnallinen ongelma.
    - Tässä tutkimuksessa on tavoitteena luoda malli, jonka avulla parannetaan Suomen pelastustoiminnan viestinsiirtoa. Mallina tästä tutkimuksesta syntyy kokonaisarkkitehtuuri, jossa myös kuvataan miten pilvipalveluilla voidaan parantaa pelastustoimia sekä miten voidaan vähetää katvealue ongelmia.
2. *Painota suunnittelussa liiketoiminnan relevanttiutta*: Tutkimus on relevanttia, mikäli sen tuloksena tai sen avulla ratkaistaan kohdeorganisaation ongelma.

- Tässä tutkimuksessa pyritään rakentamaan malli hyvin ajankohtaiseen ongelmaan, katvealue ongelmat ovat pelastustoiminnan kannalta hankalia. Lisäksi valtiovarainministeriö on tällä hetkellä toteuttamassa hallinnon yhteistä turvallisuusverkko hanketta TUVE, jonka tarkoituksena on parantaa viranomaisten välistä tiedonsiirtoa, joka on myös yksi tämän tutkimuksen lähtökohdista.

3. *Osoita artefaktin relevanttius evaluoimalla se*: Oikein suunniteltujen ja määriteltyjen arviointimetodien avulla voidaan riittävällä tarkkuudella osoittaa artefaktin hyödyllisyys, laatu ja vaikutus.
    - Tässä tutkimuksessa syntyneitä tuotoksia arvioidaan työyhteisössäni kolleegoiden toimesta. Syntyneen mallin toimintaa ei käytännössä testata, vaan sen toimivuus arvioidaan teoriassa kolleegoiden toimesta.
4. *Tuota tutkimuksella uutta tietoa, uusia menetelmiä tai merkittävä artefakti*: Tehokas suunnittelutieteellinen tutkimus tarjoaa selkeitä kontribuutioita artefaktien muodossa, lisäyksinä tietämyskantaan peruspalikoina tai metodologioina.
    - Tässä tutkiumuksessa lisätään peruspalikoita mallin muodossa tietämyskantaan. Lisäksi tietämyskantaan saadaan tietoja pilvipalveluista, niihin kohdistuvista tietoturvauhkista sekä mallia koskevista lakipykälistä.
5. *Painota tutkimuksessa tieteellistä tarkkuutta*: Tutkimuksen tulisi tuottaa selkeästi ja täsmällisesti kuvattua uutta tietoa ja ymmärrystä suunnitellun artefaktin, konstruointitietämyksen ja mahdollisesti suunnittelua koskevien metodologioiden alueella.
    - Tässä tutkimuksessa pyritään tutustumaan mahdollisimman kattavasti alan aiempiin tutkimuksiin, joissa on tutkittu samaa asiaa tai jotka ovat lähellä samaa aihetta. Lisäksi perehdytään eri pilvipalvelumalleihin, tutkimuksessa syntyvään malliin vaikuttaviin lakeihin, säädöksiin sekä ohjeisiin, jotka koskevat viranomaistoimintaa. Lisäksi mallin luomisen yhteydessä perehdytään palvelukeskeiseen arkkitehtuuriin sekä nousevaan tietokantatrendiin NoSQL.
6. *Tarkastele suunnitteluprosessia ratkaisujen etsintäprosessina*: Tutkimusprosessissa käytettävissä olevilla toimenpiteillä ja resursseilla haetaan ratkaisua tutkimusongelmaan reunaehtojen, kuten kohdeympäristön aiheuttamien rajoitusten puitteissa. Tämä edellyttää riittävää tietämystä sekä tutkimuksen lähtötilanteesta että tavoitetilasta. Vaikka suunnittelutieteellisessä tutkimuksella ei välttämättä löydetä heti parasta mahdollista ratkaisua, voidaan iteratiivisuudella löytää lopulta riittävän hyviä ja käyttökelpoisia artefakteja.
    - Tässä tutkimuksessa lähdetään rakentamaan mallia siihen miten tiedonsiirtoa voitaisiin parantaa katealueella sekä hyödyntäen pilvipalveluita.

Ensimmäisellä iteraatiokierroksella selvitetään käsitteitä sekä haetaan mallia yhdellä pilvipalvelumallilla sekä yhdellä kokonaisarkkitehtuuriratkaisulla.

7. *Välitä uudet tulokset sekä tutkija- että soveltajayhteisölle*: Tutkimuksen tulokset tulee esitellä sekä teknologia- että johtamisorientoituneelle yleisölle. Teknologiaorientoitunut yleisö tarvitsee riittävän yksityiskohtaisen kuvauksen artefaktin toteuttamiseksi ja käytettäväksi kohdeorganisaatiossa. Johtamisorientoitunut yleisö tarvitsee riitävät yksityiskohtaiset kuvaukset päättääkseen otetaanko tutkimuksen tulokset käyttöön.

2.4 Aineiston keräys

Kirjallisuuden, artikkeleiden sekä julkaisujen lisäksi aineistoa on hankittu haastattelemalla Suomen Erillisverkko Oy:stä Antti Koposta. Koposelta on saatu tietoja VIRVE -verkosta ja sen nykytilanteesta. Pelastustoimesta on saatu tietoja haastattelemalla Antti Juntusta pelastusopistosta.

3 Kirjallisuustutkimus

Tässä osiossa käydään läpi teoriaa, joka liittyy kokonaisarkkitehtuuriratkaisuun, joka syntyy tämän tutkimuksen tuloksena. Pilvipalveluista tarkastellaan eri pilvimallit, pilvipalvelumallit sekä pilvipalveluihin liittyvät vastuujaot. Kun on saatu käsitys pilvipalveluista, niin selvitetään millaisia tietoturvauhkia niihin kohdistuu, jotta kokonaisarkkitehtuurissa osattaisiin ottaa niihin kantaa ja näin saada ratkaisusta mahdollisimman tietoturvallinen, sillä onhan kyseessä kuitenkin viranomaistoimintaan liittyvä palvelu. Viranomaistoimintaa säädetään Suomessa lakien, säädösten ja ohjeiden avulla. Tässä osiossa selvitetään yleisemmin vaikuttavat lait, säädökset sekä ohjeet, jotta lopullisesta ratkaisusta tulisi näiden mukainen. Laeista, säädöksistä sekä ohjeista haetaan tukea kokonaisarkkitehtuuriratkaisun rationaalisuudelle. Edellä mainituilla kohdilla on saatu aikaan perusteltu ratkaisu yhteistyön parantamiseksi, mutta näillä tiedoilla ei vielä ratkota katveongelmaa, joka on kuitenkin yksi iso ongelma. Katvealue ongelman selvittämiseksi on tutkittu uutta tietokantamallia NoSQL ja selvitetty miten sitä voitaisiin hyödyntää. NoSQL sekä palvelukeskeisen arkkitehtuurin (SOA) selvitys tuovat rakennuspalikoita kokonaisarkkitehtuurin rakentamiseen. Tässä osiossa selvitettyjen asioiden avulla voidaan rakentaa perusteltu, palvelukeskeinen, turvallinen ja yhteistyötä parantava kokonaisarkkitehtuuri.

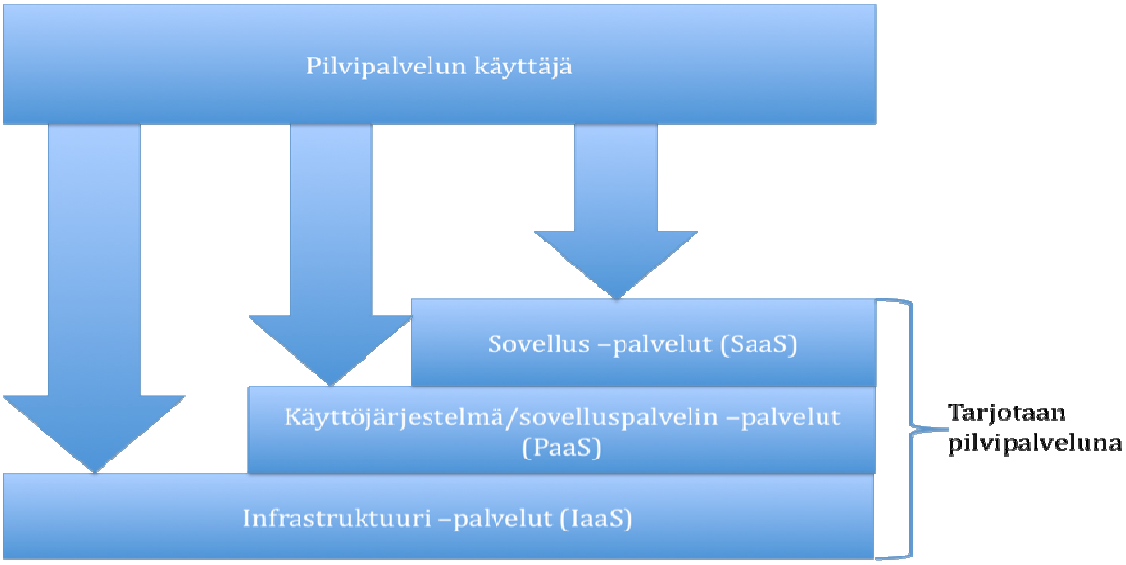
3.1 Pilvipalvelut

Pilvipalveluun mennään käyttämään teknologiaa silloin kun sitä tarvitaan ja käytetään niin kauan kuin tarvitaan eikä minuuttiakaan pidempään (Reese, 2009). Sinun ei tarvitse asentaa tietokoneen työpöydälle mitään etkä maksa teknologiasta silloin, kun et niitä käytä.(Reese, 2009). Reese (2009) mukaan pilvipalveluita on kahdenlaisia: sovellus- ja infrastruktuuripalveluita. Reese (2009) on määritellyt kolme kriteeriä, joiden avulla voidaan selvittää onko tarjottava palvelu pilvipalvelua vai ei. Seuraavassa ko. kolme kriteeriä:

1. Palvelu on saatavissa joko internet -selaimen kautta tai web service API:n kautta.
2. Ei tarvita pääomaa palvelun aloittamiseksi.
3. Maksat vain sen mitä käytät silloin, kun käytät.

Alla olevassa kuvassa 4 on kuvattu millaisia palveluita pilvipalvelut tarjoavat. Kuvasta nähdään, että pilvipalveluiden käyttäjä voi kasata palveluista haluamansalaisen kokoonpanon. Käyttäjä voi ostaa esimerkiksi vain infrastruktuuri palveluita eli konekapasiteettia ja rakentaa itse loput tai sitten hän voi ostaa sovelluksen käyttöoikeuksia, jolloin konekapasiteetti ja käyttöjärjestelmä kapasiteetti tulevat mukana. Tällöin palvelun ostajan ei tarvitse muistaa tehdä mitään muuta kuin maksaa kuukausittainen lasku ja seurata kapasiteetin käyttöä.

Kuten kuvasta 4 nähdään, niin pilvipalveluna tarjotaan infrastruktuuri – palveluita (Infrastructure as a Service (IaaS)), käyttöjärjestelmä/ sovelluspalvelin – palveluita (Platform as a Service (PaaS)) sekä sovellus – palveluita (Software as a Service (SaaS)).

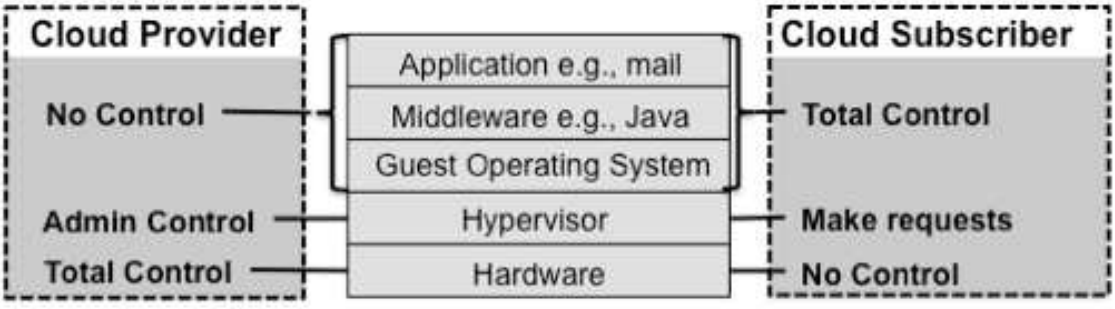


Kuva 4 Pilvipalvelut

Seuraavassa käydään vastuualueet läpi pilvipalveluittain. Jokaisen kohdalla tarkastellaan kuka vastaa ja mistä eli mitä pilvipalvelun tarjoaja kontrolloi ja mitä pilvipalvelun käyttäjä.

Infrastruktuuri -palvelut (IaaS)

Kuvassa 5 Badger ja muut (2011) ovat kuvanneet sovelluskerroksittain vastuualueet pilvipalvelun tarjoajan sekä sen palveluja käyttävän osapuolen välillä.

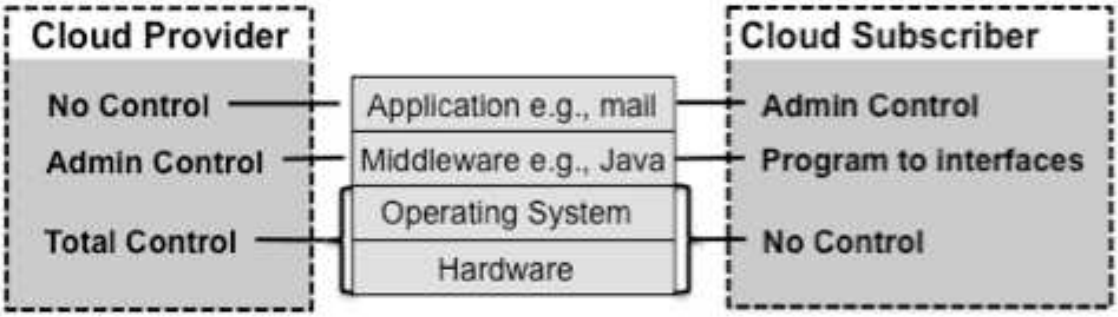


Kuva 5 Vastuualueet IaaS palveluissa (Badger ja muut, 2011)

Badger ja muut (2011) ovat jakaneet vastuut siten, että pilvipalvelujen käyttäjä IaaS -palveluissa vastaavat itse sovelluksesta(Application), sen tarvitsemasta sovelluspalvelin ohjelmistosta (Middleware) sekä käytetystä käyttöjärjestelmästä. Pilvipalvelun toimittaja vastaa sekä kontrolloi itse fyysisiä koneita sekä niiden päälle rakennettuja virtuaalikoneita.

Hypervisorilla tässä tapauksessa tarkoitetaan monitorointi ohjelmistoa, jolla hallinnoidaan rakennettuja virtuaalikoneita.

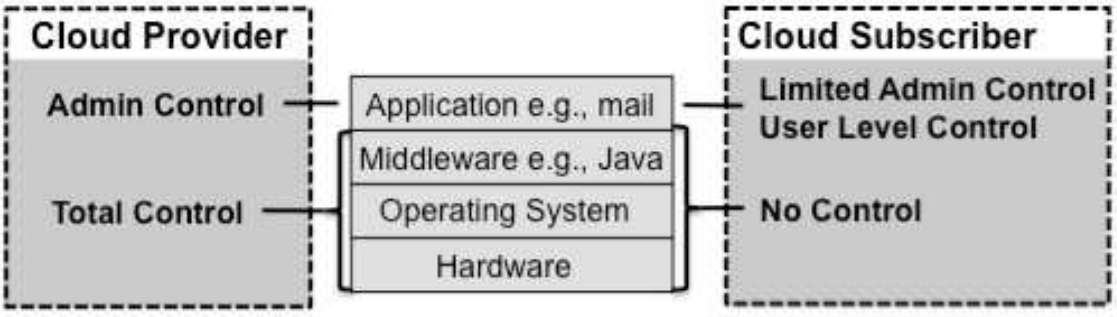
Käyttöjärjestelmä/ sovelluspalvelin -palvelut (PaaS)



Kuva 6 Vastuualueet PaaS palveluissa (Badger ja muut, 2011)

Kuten kuvasta 6 huomataan, niin IaaS -palveluihin nähden Badger ja muiden (2011) mukaan PaaS -palveluissa pilvipalvelun toimittaja hallinnoi fyysisten koneiden sekä käyttöjärjestelmän lisäksi sovelluspalvelin ohjelmistoista kuten esimerkiksi Java -sovellusten ajoympäristöstä. Pilvipalvelun toimittaja huolehtii pilvipalvelun käyttäjälle valmiin sovelluskehitysympäristön, joka lähtee fyysisistä koneista aina kehitystyökaluihin asti. Pilvipalvelun käyttäjä hyödyntää kehitysalustaa sekä vastaa niiden päälle rakennetuista sovelluksista. IaaS -palveluun nähden pilvipalvelun toimittajalle tulee lisäksi vastuu sovelluspalvelinohjelmistoista ja käyttäjän tarvitsemista muista kehitysvälineistä.

Sovellus -palvelut (SaaS)



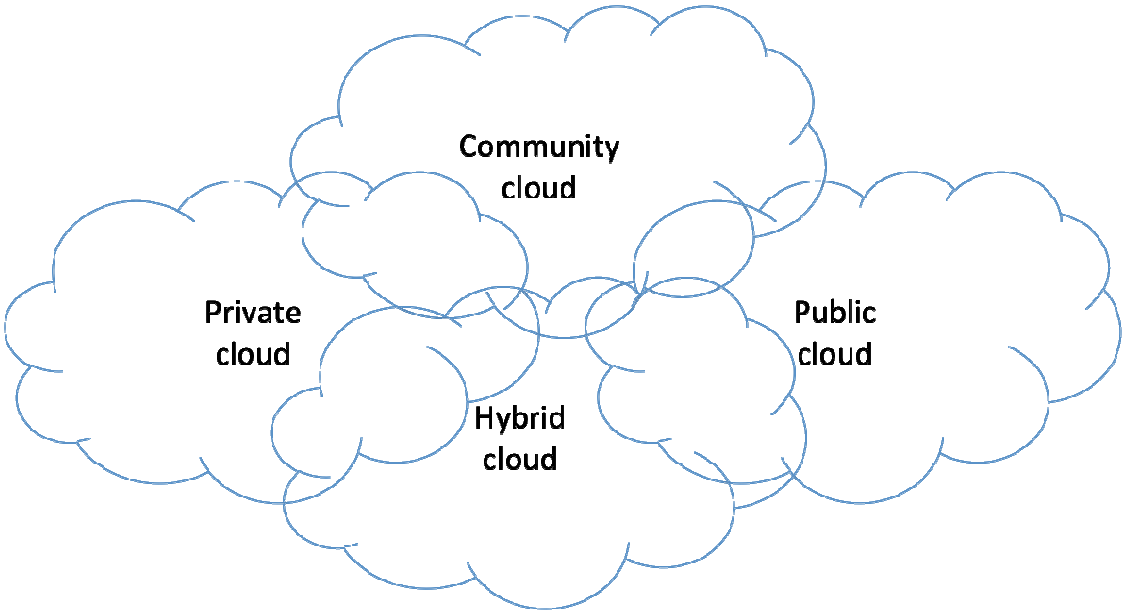
Kuva 7 Vastuualueet SaaS palveluissa (Badger ja muut, 2011)

Kuten kuvasta 7 huomataan, niin SaaS -palveluissa Badger ja muiden (2011) mukaan pilvipalvelun tarjoaja vastaa lähes kaikesta. Tässä mallissa pilvipalvelun käyttäjällä eli ostajalla on vain rajatut hallinnointioikeudet sovellustasolle. Käytännössä tämä tarkoittaa sitä, että pilvipalvelun käyttäjä voi hallinnoida ostamansa sovelluksen resursseja ja muokata sitä rajatuin määrin omaan tarkoitukseensa. SaaS -malli on käyttäjän kannalta helpoin, sillä

hänen ei tarvitse huolehtia edes tarvittavista lisensseistä, vaan riittää, että huolehtii kuukausikuluista.

3.2 Pilvipalvelumallit

Pilvipalvelut jaetaan yksityisiin pilviin (engl. private cloud), yleisiin/julkisiin pilviin (engl. public cloud), yhteisö pilviin (engl. Community cloud) sekä näiden sekoitukseen hybridi – pilviin (engl. hybrid cloud). Alla olevassa kuvassa 8 kuvataan näiden pilvimallien yhteydet toisiinsa.



Kuva 8 Eri pilvipalvelumallit

Kuvasta 8 nähdään, että Hybrid -sekä Community -pilvimallit ovat sekoituksia muista pilvemalleista. Private -ja Public -pilvimallit ovat yksittäisiä mallejaan, jotka eivät koostu muista malleista. Seuraavassa käsitellään kuvan 8 pilvimalleja tarkemmin.

Yksityinen pilvimalli (engl. private cloud)

Kun yritys haluaa perustaan keskitetyn palvelun, jolla he tarjoavat palveluita yrityksen muille projekteille tai organisaatioyksiköille, kutsutaan tätä palvelua yksityiseksi pilveksi, sillä se toimii vain yrityksen sisällä. Reese (2009) mukaan, kun yritys haluaa virtualisoida sovelluspalvelimiaan tai tietokantapalveluita, niin silloin se perustaa yksityisen pilven. Reese (2009) mukaan avainhyöty yksityisestä pilvestä on kontrolloitavuus. Kuvan 4 mukaisia pilvipalveluita voidaan rakentaa tarjolle myös yksityisissä pilvissä. Tällöin sovellukset ovat

luonnollisesti yrityksen omia. Näissä yksityisissä pilviratkaisuissa pitää vain olla tarkkana sovellusten lisensioinnin kanssa, sillä useasti tuotteiden lisenssit ovat jollain tavalla sidoksissa konetehoon esimerkiksi CPU määriin ja jotkut menevät vielä tarkemmalle tasolle ja hinnoittelevat jopa CPU ydin kohtaisesti. Mikäli ei ole tarkkana saattaa yksityisen pilven rakentamisesta tulla todella kallis.

Yleinen- / julkinenpilvimalli

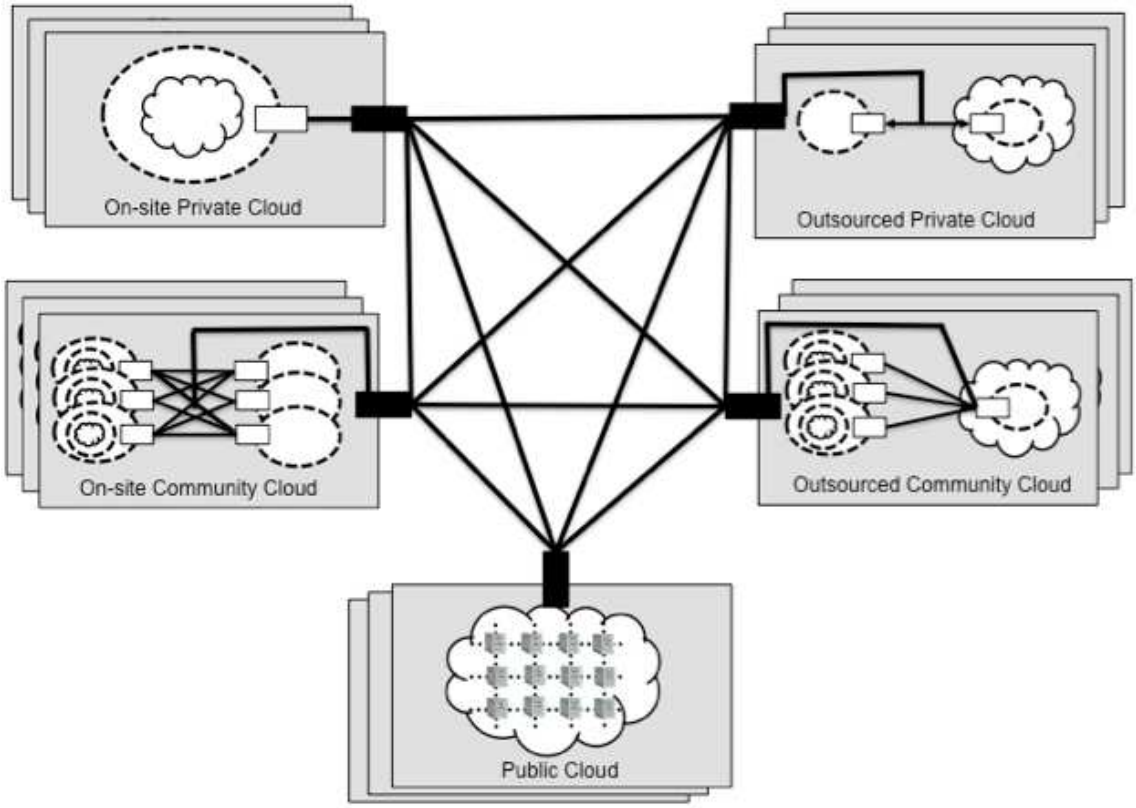
Julkisena pilvipalveluna tunnetaan mm. Amazon:n tarjoamat pilvipalvelut. Aikaisemmin mainitut Reese (2009) määrittelemät kolme kriteeriä pilvipalveluille koskevat juuri julkisia pilvipalveluita. Julkisissa pilvipalveluissa yrityksellä ei ole itsellään kiinni pääomaa konekapasiteetissa eikä tarvitse välittää sovellusten lisensoinnista, sillä niistä vastaa pilvipalvelun toimittaja. Julkisen pilvipalvelun tapauksessa asiakas hakee yleisiä IT –ratkaisuja, jotka vastaisivat heidän liiketoimintatarpeisiinsa (Oracle, 2010). Oracle (2010) mukaan julkisia pilvipalveluita tarjoavalla yrityksellä tulee olla prosessit standardoitu, jotta palvelua pystyy toimittamaan laadukkaasti. Tämä helpottaa pilvipalveluita käyttävän yrityksen toimintaa, sillä IT –resurssien hankita on formaalia ja täten helppoa.

Yhteisöllinen -pilvimalli

Yhteisöllinen pilvimalli on eri ryhmien tai yhteisöjen jakama sekä omistama pilvi. Yleensä kaikki yhteisön tai ryhmän jäsenet tuntevat toisensa, jolloin tässä pilvimallissa tietoturvariskit ovat pienemmät kuin muissa pilvimalleissa. Tätä pilvimallia voi tarjota jokin kolmasosapuoli tai sitten joku yhteisön jäsen, mutta pääpointti on kuitenkin se, että kaikki yhteisön tai ryhmän jäsenet jakavat keskenään kaikki pilven tarjoamat resurssit. Yhteisöllinen pilvimalli ei ole riippuvainen kolmansista osapuolista, jolloin se on avoimempi standardien ja tiedon suhteen, mutta silti se tarjotaan palveluna (Briscoe ja Marinos, 2009).

Hybridi -pilvimalli

Hybridi –pilvipalvelua ei oikeastaan kukaan voi suoraan tarjota, sillä Hybridi –pilvi koostuu sekä julkisesta pilvestä, että yksityisestä pilvestä. Yritys voi rakentaa oman yksityisen pilven ja tarjota sovelluksensa julkisen osan julkisen pilven kautta näkyville internet käyttäjille. Tällä pilvimallilla yritys voi hyödyntää sekä julkisen että yksityisen pilvimallin hyvät puolet.



Kuva 9 Hybridi -pilvimalli (Badger ja muut, 2011)

Kuvassa 9 Badger ja muut (2011) ovat kuvanneet hybridi -pilvimallia. Kuvasta 9 nähdään miten hybridi -pilvimalli voi koostua kaikista muista edellä kuvatuista pilvimalleista sekä siitä voi tulla kaikkia malleja yhdistelemällä kovinkin monimutkainen ja vaikeasti hallittava.

3.3 Tunnetut tietoturvauhat

OWASP (2010) on kasannut 10 heidän mielestään tärkeintä turvallisuusperiaatetta, jotka listattu alla olevassa taulukossa 3.

Nro	Uhka	Kuvaus	Palvelumalli, jota koskee
1	Hyökkäyspintojen minimointi	Rajataan toimintojen näkyvyyttä vain tietyille käyttäjäryhmille.	IaaS, PaaS ja SaaS
2	Turvallisten oletusasetusten käyttö	Oletuksena asennetaan turvalliset oletusasetukset, jotta myös ne käyttäjät, jotka eivät kiinnitä huomiota turvallisiin toimintatapoihin, käyttäisivät sovellusta turvatusti.	IaaS, PaaS ja SaaS
3	Vähäisimpien oikeuksien periaate	Annetaan jokaiselle käyttäjäryhmälle vain ne oikeudet, joita he tarvitsevat liiketoiminnallisiin tarkoituksiin.	IaaS, PaaS ja SaaS
4	Syvyyssuuntainen	Käytetään kerroksellista rakennetta, jolloin	IaaS, PaaS ja SaaS

	puolustus	vähennetään tietoturvariskiä, kun hyväksikäytetty haavoittuvuus ei altista koko ohjelmaa, vaan hyökkäykset pysähtyvät seuraavan kerroksen turvamekanismeihin.	
5	Virheiden turvallinen käsittely	Keskitetty ja systemaattinen virheiden hallinta parantaa sovelluksen turvallisuutta.	IaaS, PaaS ja SaaS
6	Ulkoisten palvelujen varmistus	Kaikki ulkoisista palveluista tulevat tiedot tulee tarkistaa ja tarvittaessa sanitoida.	SaaS
7	Tehtävien eriyttäminen	Tehtävät tulee erottaa siten, että kussakin roolissa oleva voi valtuuttaa erikseen määriteltävän menettelytavan mukaisesti alistettuihin rooleihin kuuluvia käyttäjiä, mutta ei vaikuttaa omiin valtuuksiinsa.	IaaS, PaaS ja SaaS
8	Vältä piilotusta turvakeinona	Piilotus (engl. Security through obscurity) on heikko turvallisuuskontrolli, jossa luotetaan siihen, että jos käyttäjä ei näe haavoittuvuuksia, niitä ei voi hyväksi käyttää. Sen käyttämistä ainoana suojausmenetelmänä tulee välttää. Esimerkiksi lähdekoodin salaaminen ei tulisi olla ainoa suojamekanismi vaan vain osa syvyyssuuntaista puolustusta	IaaS, PaaS ja SaaS
9	Yksinkertaiset turvallisuusrakenteet	Yksinkertaiset turvarakenteet ovat yleensä nopeampia toteuttaa ja suorittaa. Lisäksi yksikertainen ja suoraviivaiseksi rakennettu koodi on ylläpidettävämpää ja vähemmän altis sekä loogisille, että ohjelmointivirheille.	IaaS, PaaS ja SaaS
10	Tietoturvapoikkeamien asianmukainen käsittely	Tietoturvapoikkeamalla tarkoitetaan sellaisia tapahtumia tai epäiltyä tapahtumaa joka vaikuttaa heikentävästi kokonaisturvallisuuteen. Tietoturvapoikkeama tulee ilmoittaa viipymättä tietoturvaorganisaatiossa lähimmälle vastuuhenkilölle. Turvallisuuspoikkeamien ilmoittamiseen ja käsittelyyn tulee olla dokumentoitu ohje, joka on helposti kaikkien asianosaisten saatavilla. Nopea reagointi minimoi aiheutuneita vahinkoja tehokkaasti.	IaaS, PaaS ja SaaS

Taulukko 3 OWASP Top 10 uhat (OWASP, 2010)

CSA (2010) on listannut seuraavassa taulukossa 4 olevat tietoturvauhat, jotka koskevat pilvipalveluita.

Nro	Uhka	Kuvaus	Palvelumalli, jota koskee
1	Pilvipalvelujen väärinkäyttö	IaaS -palveluita käytetään väärin esimerkiksi silloin, kun he tarjoavat ilmaiseksi testiaikaa.	IaaS ja PaaS

		Tätä testiaikaa käyttävät eri massa viestimet (engl. Spammers) hyödykseen, jolloin rangaistuksen mahdollisuuden ovat olemattomat. PaaS -palvelut joutuvat erillaisten hyökkäysten kohteiksi, mutta esimerkkinä salasanojen ja käyttäjätunnusten hakkeronti sekä CAPTCHA selvitys farmeja.	
2	Epäluotettavat rajapinnat sekä API:t	Pilvipalvelut tarjoavat erinäisiä rajapintoja niin sovellusten kuin käyttöpalveluiden hallinnointiin. Tällöin riskinä on eri hallintaohjelmien hallintarajapinnat ja niiden turvallisuus.	IaaS, PaaS ja SaaS
3	Vihamieliset työntekijät	Vihamielinen työntekijä voi tehdä hallaa pilvipalveluissa monille organisaatioille varsinkin, jos työntekijä pystyy luomaan käyttäjä ja antamaan sille oikeudet, tämän jälkeen tekemään hallaa niillä ja sitten poistamaan käyttäjän, jolloin kaikki todisteet häviävät.	IaaS, PaaS ja SaaS
4	Jaettu teknologia	Yleensä IaaS -palveluissa jaetaan eri käyttäjien kesken esim. CPU:ta ja muita konetason kapasiteettejä ja tämä on tehty virtualisoimalla palvelimia. Itse virtualisointiin liittyvät uhat tulevat tässä kyseeseen.	IaaS
5	Data hävikki tai vuoto	Mikäli pilvipalveluissa on käytetty heikkoja salauksia tai huonoja suojaamattomia rajapintoja tai pilvipalvelun käyttämissä sovelluksissa on vuotoja, niin se on uhka tiedon hävikin suhteen.	IaaS, PaaS ja SaaS
6	Käyttäjätilin tai palvelun kaappaus	Käyttäjätunnusten ja salasanojen kalastelun (engl. Phishing) riski ei häviä pilvipalvelujen myötä.	IaaS, PaaS ja SaaS
7	Tuntematon riskiprofiili	Tässä tarkoitetaan uhkaa, jossa ei ole suunnitelmaa siihen esimerkiksi, että miten on hallinnoitu tietoturvapäivitykset ja miten järjestelmä lokit on huolehdittu. Vaikka palvelut siirretään pilvipalveluun, niin näistä on silti huolehdittava.	IaaS, PaaS ja SaaS

Taulukko 4 Tärkeimmät uhat pilvipalveluissa (Badger ja muut, 2011)

Kun verrataan OWASP (2010) antamia turvallisuusperiaatteita CSA (2010) vastaaviin, niin huomataan suuria yhtäläisyyksiä. Molemmissa otetaan kantaa ympäristössä käytettyihin liittymiin, käyttäjien mahdollisesti aiheuttamiin vaaratilanteisiin sekä tietoturvaohjeistuksiin.

Pilvipalveluilla on myös positiivisia tietoturvaominaisuuksia, kun mietitään jokapäiväistä aineiston käsittelyä, niin luottamukseen liittyvistä riskeistä huolimatta käyttäjien tiedostot

ovat usein todellisuudessa paremmassa tallessa pilvessä kuin käyttäjien tietokoneilla sekä saatavuuden että turvallisuuden kannalta (Oza ja muut, 2010). Nykypäivänä käyttäjillä on useasti kannettavia tietokoneita, jotka on helppo varastaa, jolloin pilvessä olevat aineistot ovat paremmassa suojassa kuin omalla kannettavalla tietokoneella. Toinen yleisin ongelma/ vaara on se, että ei oteta varmuuskopiota tarpeeksi usein. Yleensä pilvipalvelut tarjoavat automaattisen varmuuskopioinnin sinne tallennetulle aineistolla, sillä Oza ja muiden (2010) mukaan pilvipalveluissa tietoturvasta yleisellä tasolla huolehtivat tietoturva-alan ammattilaiset.

3.4 Lainsäädäntö, direktiivit ja suositukset

Arkaluontoisten tietojen kuten henkilötietojen suojaamista on pyritty vahvistamaan lainsäädännön avulla. Suomessa yksityisyyden suojan käsite perustuu ihmisoikeussopimuksiin, kansainvälisiin säädöksiin ja Suomen perustuslakiin. (Syrjänen, 2008) Euroopan unionin jäsenmaana Suomen tulee ottaa lainsäädännössään huomioon myös EU-maita koskevat direktiivit (Syrjänen, 2006). Laajemmassa merkityksessä tietosuojaa ja yksityisyyttä voidaan pitää osana yksilön perusoikeuksia, joista säädetään Suomen perustuslaissa. Perustuslain toisen luvun kymmenennessä pykälässä on säädetty yksityiselämän ja luottamuksellisen viestin suojasta (Suomen perustuslaki 11.6.1999/731, 1999). Syrjäsen (2006) mukaan Euroopan neuvoston tietosuojasopimus ja suositukset sekä tietosuojadirektiivi ovat ohjanneet Suomen lainsäädäntöä merkittävimmin.

Tietosuojadirektiivin pohjalta on säädetty vuonna 1999 voimaan tullut henkilötietolaki (Järvinen, 2010). Henkilötietolain mukaan sen tarkoituksena on toteuttaa yksilön yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (Henkilötietolaki 22.4.1999/523, 1999). Alkuperäisessä direktiivissä henkilötietojen käsittelyllä tarkoitetaan mm. tietojen keräämistä, tallentamista, järjestämistä, säilyttämistä, luovuttamista, suojaamista ja tuhoamista (Tietosuojadirektiivi 95/46/EY, 1995). Henkilötietolaki on ensisijaisesti säädetty henkilötietoja käsitteleviä tahoja ajatellen, asettaa lainsäädäntö silti vaatimuksia myös henkilötietoja käsitteleville järjestelmille sekä niiden suunnittelemiselle.

Viranomaistoiminnassa Julkisuuslain 6 luku määrittelee viranomaisen salassapitovelvoitteet ja salassapitoon liittyvän käsittelysäännöstön. Viranomaisen asiakirja on pidettävä salassa, jos se tässä tai muussa laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. (Julkisuuslaki 621/1999).

Salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi. (Julkisuuslaki 621/1999). Julkisuuslakia on edelleen tarkennettu julkisuusasetuksella nimeltään Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030.

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030 tarkentaa Julkisuuslaissa määriteltyä salassapitoa koskevia säädöksiä. Asetus määrittää hyvän tiedonhallintotavan, jota viranomaisena toimivan tulee noudattaa tietojen käsittelyssä. Asetus määrittelee erityissuojattavien luokitusjärjestelmän sekä asettaa kriteerit tietojen luokitukselle. Asetus myös ohjeistaa viranomaisia viestinnässä.

Valtionhallinnon viranomaisten viestintää suunniteltaessa ja toteutettaessa on otettava huomioon viestinnän merkitys viranomaiselle säädettyjen tehtävien tehokkaassa hoitamisessa sekä viranomaisen ja kansalais- ja etujärjestöjen välisessä yhteistyössä. (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030)

VAHTI-ohjeet ovat Valtionhallinnon tietoturvallisuuden ohjausryhmän (VAHTI) laatima ohjekokoelma. Ohjeet eivät ole velvoittavia, mutta toimivat ”de facto” standardina määritettäessä julkisen hallinnon tietoturvallisuuteen liittyviä menettelytapoja ja ratkaisuita. Tässä tutkimuksessa esitettävän kokonaisarkkitehtuurin kannalta tärkeimpiä VAHTI -ohjeita ovat Sisäverkko-ohje, Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta sekä Ohje valtionhallinnon keskeisten tietojärjestelmien turvaamisesta.

Sisäverkko-ohje, joka ottaa kantaa verkkojen arkkitehtuuriin sekä niiden tietoturvaan. Valtiovarainministeriön (VM) Sisäverkko-ohjeen tavoitteena on yhtenäistää ja tehostaa menettelyitä sisäverkkojen rakentamisessa sekä tukea sopivan tietoturvatason käyttöönottoa organisaatioissa. (VAHTI 3/2010, 2010)

Valtiovarainministeriön Ohjeen tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta tavoitteena on tehostaa ja yhdenmukaistaa lain viranomaisen toiminnan julkisuudesta (621/1999) perusteella 1.7.2010 annetun ja 1.10.2010 voimaantulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanoa. Ohjeen mukaisella toiminnalla viranomainen voi saavuttaa toiminnassaan ja yhteistyössään asetuksen mukaisen tietoturvatason, joka tasapainottaa riskienhallinnan ja kustannustehokkuuden. (VAHTI 2/2010, 2010)

Ohjeen valtionhallinnon keskeisten tietojärjestelmien turvaamisesta tavoitteena on helpottaa valtion keskeisten tietojärjestelmien tietoturvallisuuden parantamista ja näiden järjestelmien turvaamisen erityiskysymysten tunnistamista. (VAHTI 5/2004, 2004)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) -kriteeristö, jonka perusteella määrätyt turvallisuusviranomaiset (DSA, Designated Security Authority) suorittavat turvallisuusauditoinnit. Kriteeristö nivoo yhteen lainsäädännöstä, kansainvälisistä turvallisuussopimuksista ja standardeista sekä kansallisista viranomaismääräyksistä ja suosituksista tulevat turvallisuuvaatimukset. Vaatimustasot noudattava tietoturvatasojen (TTT) kuvaamia tasoja (perustaso, korotettu taso, korkea taso).

Turvallisuusauditointikriteeristö jakautuu neljään pääosioon: hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Auditointitapahtumassa tulee huomioida näiden kaikkien neljän osion vaatimukset, eli niitä ei ole rakennettu itsenäisiksi kokonaisuuksikseen. Jokaiselle osiolle on laadittu kolmiportainen vaatimusluokittelu, joka vastaa paraikaa laajamittaisesti käyttöön otettavia turvallisuustasokäsitteitä – perustaso, korotettu taso ja korkea taso. Näitä täydentävät edellä mainitut lähtötason suositukset. (KATAKRI, 2009)

3.5 NoSQL

Julkisten internet-sivustojen suuri suosio ja erilaiset vertaisverkkoja käyttävät tiedostojakoratkaisut ovat poikineet hajautusratkaisuja, joita vielä muutama vuosi takaperin ei ollut olemassa.

Joidenkin sivustojen, esimerkiksi Google, Facebook, Yahoo tai Ebay, massiivisen suuren suosion takia sivustojen ylläpito on joutunut kehittämään perinteisestä tietokantapalvelimien skaalaamisesta poikkeavia tiedonhallinnan ratkaisuja, koska niihin pohjautuvat ratkaisut ovat olleet liian kalliita tai eivät yksinkertaisesti ole pystyneet selviytymään tarvittavista tietomääristä. Viime vuosina yksittäisten yritysten omiin tarkoituksiinsa tekemiä NOSQL-ratkaisuja on julkaistu avoimena lähdekoodina, jolloin niiden suosio perinteisissä internet-ratkaisuissa on lähtenyt nousuun. (Perdue, 2010).

Cattelin (2010) mukaan NoSQL tietokantoja on vaikea kuvata, sillä ne ovat kehittyneet hetkessä ja niissä on erilaisia tietomalleja sekä toiminnallisuuksia. Cattelin (2010) mukaan perustietoelementtejä voidaan kutsua joko objekteiksi, dokumenteiksi tai alkioiksi. Cattell (2010) kirjaa seuraat 4 tunnusmerkkiä NoSQL tietokannoille.

1. NoSQL -tietokannat tarjoavat hyvin vähän jos ollenkaan valmiiksi määriteltyjä malleja (engl. schema) toisin kuin suurin osa yleisemmin tunnetuista relaatiotietokannoista.

Kun ei ole valmiiksi määriteltyä tietomallia, vaan tietokanta olio voi sisältää lukemattoman määrän ennalta määrittelemättömiä määreitä (engl. attributes), niin tämä helpottaa ohjelmien jatkokehitystä, sillä aikaisemmin syntynyttä tietomallia on helppo muuttaa.

2. NoSQL -tietokannoilla on yksinkertainen kyselyrajapinta SQL prosessoinnin sijasta. Cattelin (2010) mukaan toiset sanovat, että tämä parantaisi suorituskykyä, mutta Cattelin (2010) mielestä SQL -lauseista vain voidaan saada hitaita esimerkiksi liian monella tietokantataulun liitoksella (engl. union).
3. Cattelin (2010) mukaan tärkein NoSQL -tietokantojen ominaisuus on kymmenien tai jopa satojen noodien skaalautuvuus tarjoten kuitenkin 100% ACID semantiikan jaettavalle tiedolle. ACID tulee sanoista atomisuus(engl. Atomicity), eheys (engl. Consistency), eristyneisyys(engl. Isolation) ja pysyvyys (engl. Durability). ACID tarkoittaa, että pyritään turvaamaan tietojen eheys kaikissa tilanteissa. Atomisuus tarkoittaa, että pyritään suorittamaan transaktiot kokonaan tai ei ollenkaan. Eheydellä tarkoitetaan sitä, että transaktio siirtää tietokannan toisesta eheästä tilasta toiseen. Eristyneisyydellä tarkoitetaan sitä, että transaktiot toimivat toisistaan tietämättä. Pysyvyydellä tarkoitetaan sitä, että sitoutumisen jälkeen puutokset pysyvät virhetilanteissakin.
4. NoSQL tarjoaa korkean käytettävyyden, joka on tärkeää, jotta saadaan useamman koneen skaalautuvuus hyödylliseksi.

Cattelin (2010) mukaan NoSQL -tietokannat voidaan jakaa kolmeen eri ryhmään niiden tietomallin sekä toimintojen mukaan, jotka ovat

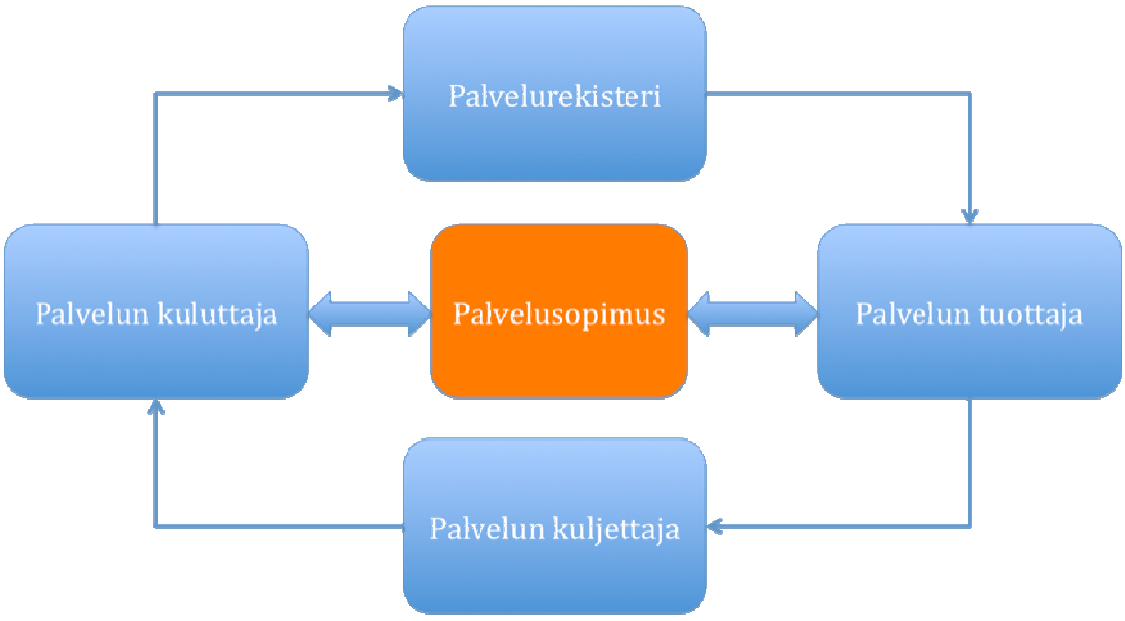
1. Avain - arvo -pari varasto, jossa Brooksin (2011) ja Cattelin (2010) mukaan on tietueita, jotka ovat täynnä määrittelemätöntä tietoa indeksoituna avaimella. Brooksin (2011) mukaan nämä kannat eivät yleensä kuvaa tietueen sisältämää tietoa vaan jättävät tämän tehtävän järjestelmälle, joka tietokantaa käyttää. Cattelin (2010) mukaan tämän ryhmän NoSQL -tietokannat tarjoavat tietojen kopioinnin tietokannan toipumista varten, tietojen järjestelyn useamman kannan välillä sekä tietojen peruspysyvyyden.
2. Dokumentti -varasto, joka Cattelin (2010) mukaan tarjoaa enemmän toiminnallisuutta avain - arvo -pari varastoon. Cattelin (2010) mukaan dokumentti -varasto ymmärtää sinne tallennettavan objektin tai dokumentin rakenteen. Objekti tai dokumentti voi sisältää kuinka paljon tahansa nimettyjä määreitä, jotka voivat olla numeroita, kirjaimia tai jopa toisia olioita.
3. Sarakejoukko -tietovarasto, joka Cattelin (2010) mukaan tarjoaa tiedot enemmän perinteisemmän relaatiotietokannan tavoin, mutta kuitenkin dynaamisin määrin määreitä.

3.6 Palvelukeskeinen arkkitehtuuri (SOA) perusteet

Tässä selvitetään SOA:n (Service Oriented Architecture) peruskäsitteet eikä paneuduta sen tarkemmin SOA:n saloihin.

SOA, eli palvelukeskeinen arkkitehtuuri, on nimensä mukaisesti arkkitehtuurimalli, joka lähtee palveluista, niiden tuottamisesta sekä niiden hyödyntämisestä (kuluttaminen). SOA ei ole teknologia tai väline eikä edes standardi. SOA on ensisijaisesti filosofia, viitemalli ja suunnittelumalli. SOA:ssa lähtökohtana on organisaation toiminnan edellyttämät ja tuottamat palvelut, joiden avulla toimintaprosessit toteuttavat ja realisoituva tietoteknisesti. (Mickos, 2008).

Mickoksen (2008) mukaan SOA lähtee paradigmana palveluista, joita toinen osapuoli tuottaa ja toinen kuluttaa. Osapuolten välillä palveluiden toimittamista säätelee palvelusopimus. Mickoksen (2008) mukaan palvelun tuottamiseen tarvitaan jokin kuljetin, siirtotie, välittäjä tai muu mekanismi. Mickoksen (2008) mukaan yleisesti ottaen mielletään palvelut julkaistaviksi jonkin palvelurekisterin kautta. Hurwitzin ja muiden (2009) mielestä SOA rekisteri on erittäin tärkeä sillä keskeinen viittaus paikka palvelukeskeisessä arkkitehtuurissa. Hurwitzin ja muiden (2009) mukaan SOA rekisteri sisältää kaiken tiedon (metadata) SOA - komponenteista. Alla olevassa kuvassa 10 on kuvattu yllä mainitut SOA:n elementit.

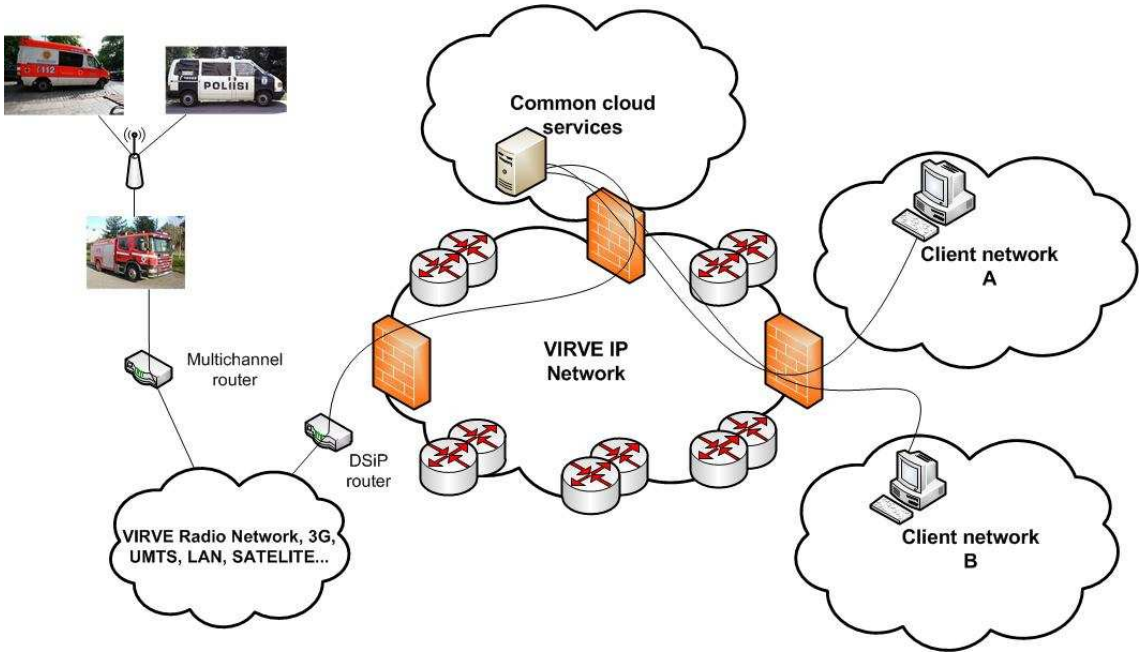


Kuva 10 SOA:n elementit (Mickos, 2008)

Hurwitz ja muut (2009) kuvaa palvelukeskeistä arkkitehtuuria seuraavalla 4 kohdalla:

1. SOA:n avulla rakennettaan liiketoimintalähtöisiä järjestelmiä. Hurwitzin ja muiden (2009) mukaan SOA arkkitehtuurilla ei voida rakentaa kaikenlaisia sovelluksia, vaan ainoastaan liiketoimintalähtöisiä sovelluksia.
2. SOA on mustalaatikko (engl. black-box) komponentti arkkitehtuuri. Hurwitzin ja muiden (2009) mukaan SOA peittää taakseen komponenttien monimutkaisuuden aina kun se on mahdollista. Mustalaatikko -malli mahdollistaa jo olemassa olevien liiketoimintapalvelujen uudelleenkäytön tarjoamalla yksinkertaisen sovittimen (engl. adapter) niille riippumatta siitä miten ne on rakennettu.
3. SOA -komponentit on sidottu löyhästi toisiinsa. SOA -komponentit siirtävät tietoja toiselle komponentille, joka taas lähettää sen seuraavalle tai palauttaa vastauksen edelliselle. Kutsut ovat yksinkertaisia ja automaattisia. Jokainen SOA komponentti tarjoaa toiselle jonkinlaisen pienen ja yksinkertaisen palvelun.
4. SOA -komponentit on organisoitu liiketoimintaprosesseihin tuottamaan hyvin kuvattua palvelua. Hurwitzin ja muiden (2009) mukaan yksinkertaisista SOA -komponenteista rakennetaan hyvinkin monimutkaisia liiketoimintapalveluita.

4 Kokonaisarkkitehtuuri



Kuva 11 Ratkaisun kokonaisarkkitehtuuri karkeasti

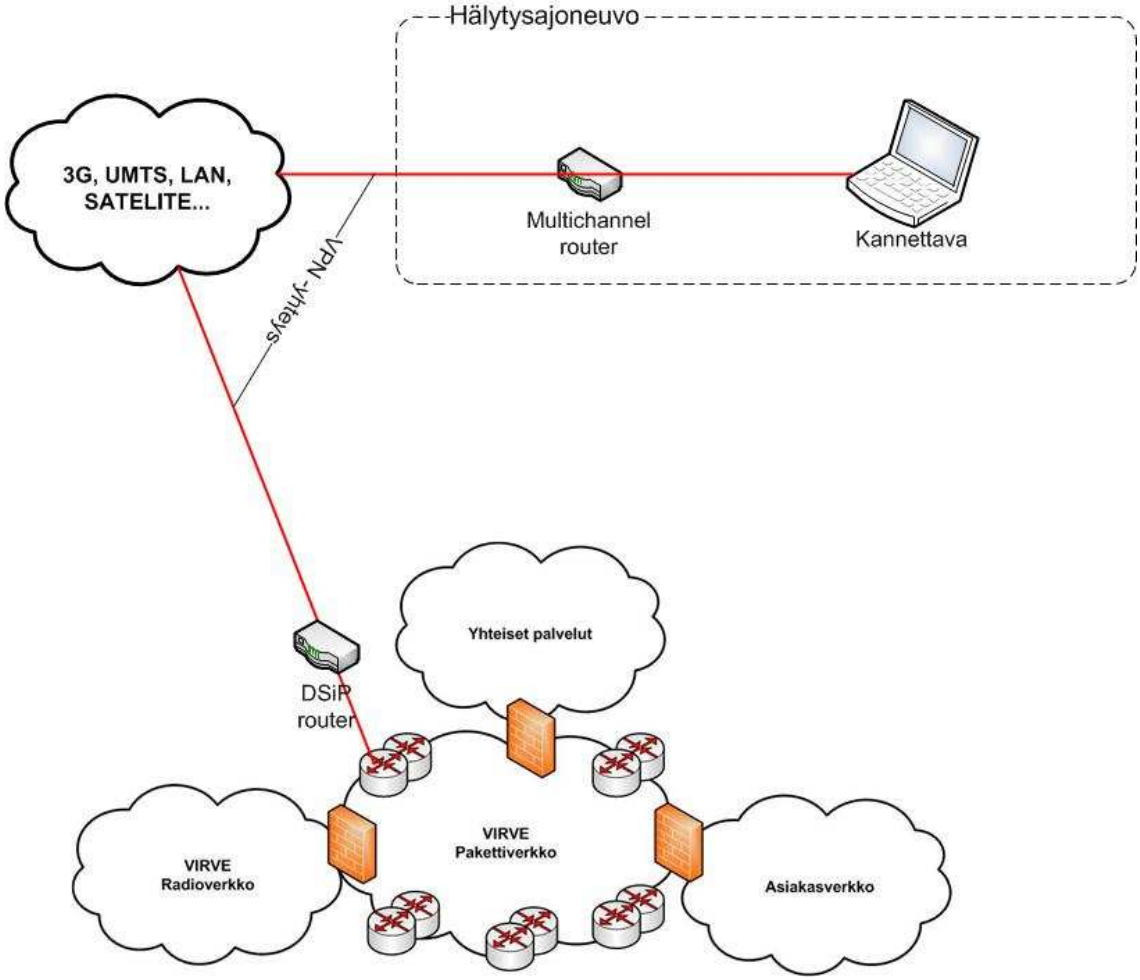
Kokonaisarkkitehtuuri kuvaa, kuinka organisaation toimintaprosessit, tiedot ja järjestelmät toimivat kokonaisuutena.(JulkICT, 2011, Winter ja muut, 2007). Tutkimuksen tuloksena syntynyt kuvan 11 mukainen kokonaisarkkitehtuuri, josta nähdään miten eri viranomaiset voisivat yhdistää palvelujaan Suomen Erillisverkot Oy:n ylläpitämän VIRVE -pakettiverkon avulla. VIRVE -pakettiverkon yhteisissä palveluissa voitaisiin tarjota kaikille yhteisiä pilvipalveluita. Pilvipalvelujen avulla saataisiin helpotettua viranomaisten välistä tiedonvaihtoa.

VIRVE -pakettiverkko on rakennettu siten, että jokaisesta asiakasverkosta toiseen asiakasverkkoon tai yhteisiin palveluihin tapahtuva liikenne kulkee VIRVE -pakettiverkon kautta, joka toimii myös runkoverkkona. Runkoverkossa asiakasverkot on kuitenkin rajattu palomuureilla siten, että pääsyä eri verkkoihin voidaan rajata. Asiakasverkossa tapahtuva asiakkaan omien sovellusten välinen liikenne pysyy asiakasverkossa, joka osaltaan lisää tietoturvallisuutta, mutta vaikeuttaa sekä tuo lisäkustannuksia sovellusten ylläpidolle. (Lehto ja muut, 2012)

4.1 Tietoliikenneyhteydet

Häytysajoneuvoista tultaisiin olemaan yhteydessä joko suoraan runkoverkon kautta yhteisiin pilvipalveluihin tai asiakasverkossa oleviin järjestelmiin. Tutkimuksen ratkaisuehdotuksessa on mahdollistettu myös, että Hälytysajoneuvot voisivat olla yhteydessä runkoverkkoon

Internetin kautta. Yhteys Internetin kautta mahdollistaisi yhteydet mahdollisten WLAN -verkkojen tai 3G -yhteyksien kautta silloin, kun VIRVE -verkko ei ole saatavilla. Tämä vähentäisi katvealueita, joilla ei VIRVE -verkko tällä hetkellä ole näkyvissä. Internetin kautta tapahtuva liikenne pitäisi tietysti suojata, jotta kukaan ei pääsisi häiritsemään viranomaistoimintaa tai saamaan arkaluontoista materiaalia haltuunsa. Yhtenä suojauskeinona on VPN -suojaus kuten kuvassa 12 on kuvattu.



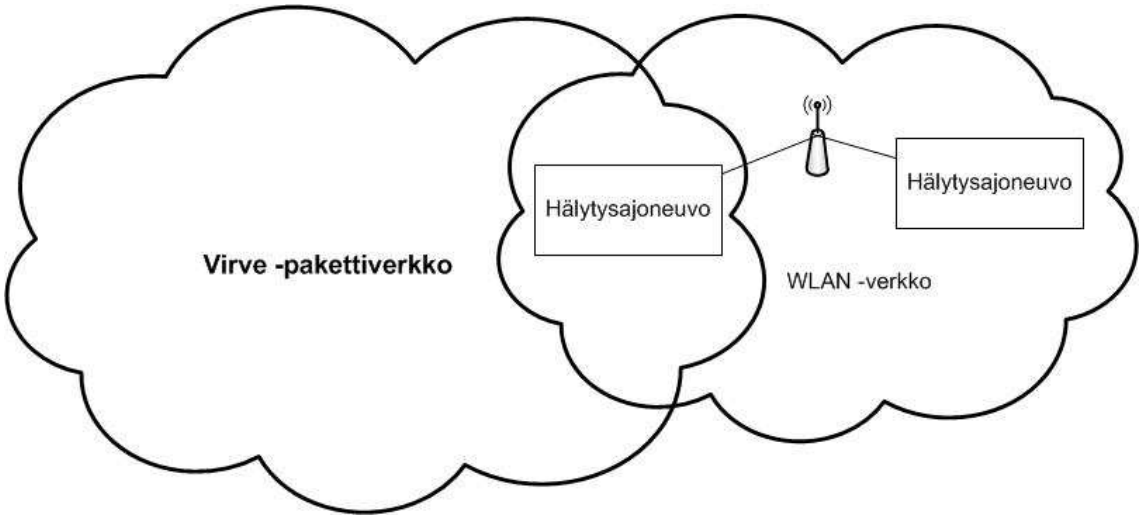
Kuva 12 Yhteys hälytysajoneuvosta Virve -verkkoon

VPN on lyhenne sanoista Virtual Private Network, joka vapaasti suomennettuna tarkoittaa virtuaalista sisäverkkoa. Määritelmänsä mukaisesti VPN tarkoittaa joko laitteisto- tai ohjelmistototeutuksena tehtävää ratkaisua, jolla organisaation sisäverkko voidaan ulottaa turvallisesti turvattoman julkisen verkon, kuten Internetin yli. (Viestintävirasto, 2007)

Vaikka mahdollistettaisiinkin WLAN- tai 3G- verkon käyttö, niin Suomessa on silti vielä alueita, joissa ei ole minkäänlaista mahdollisuutta päästä Internetiin taikka VIRVE -verkkoon. Katvealueen raja saattaa olla muutamista sadoista metreistä tai jopa lyhyemmistä matkoista kiinni ettei yhteyttä yhteisiin palveluihin saada. Tällöin mahdollisuutta saada kuitenkin

tarvittavat tiedot esimerkiksi johtokeskukseen tai hätäkeskukseen voitaisiin parantaa rakentamalla langaton verkko samalla paikalla olevien hälytysajoneuvojen välille, sillä joku hälytysajoneuvoista saattaa olla jonkun verkon kuuluvuusalueella ja saada tiedot reititettyä eteenpäin. Tutkimuksen yhtenä pääideana onkin, että hälytysajoneuvot voisivat luoda keskenään esimerkiksi tähtiverkon, jossa jokainen hälytysajoneuvo on yhteydessä toisiinsa ja ne replikoivat tietonsa keskenään, jolloin kaikilla hälytysajoneuvoilla on jatkuvasti samat tiedot käytettävissä.

Alla olevassa kuvassa 13 on kuvattu miten yksi hälytysajoneuvo on alueella, josta on yhteys VIRVE -runkoverkkoon, mutta toisella ajoneuvolla ei ole. Tämä ajoneuvo, jolla ei ole yhteyttä suoraan VIRVE -verkkoon saa kuitenkin siirrettyä tarvittavat tiedot sinne toisen ajoneuvon kautta.

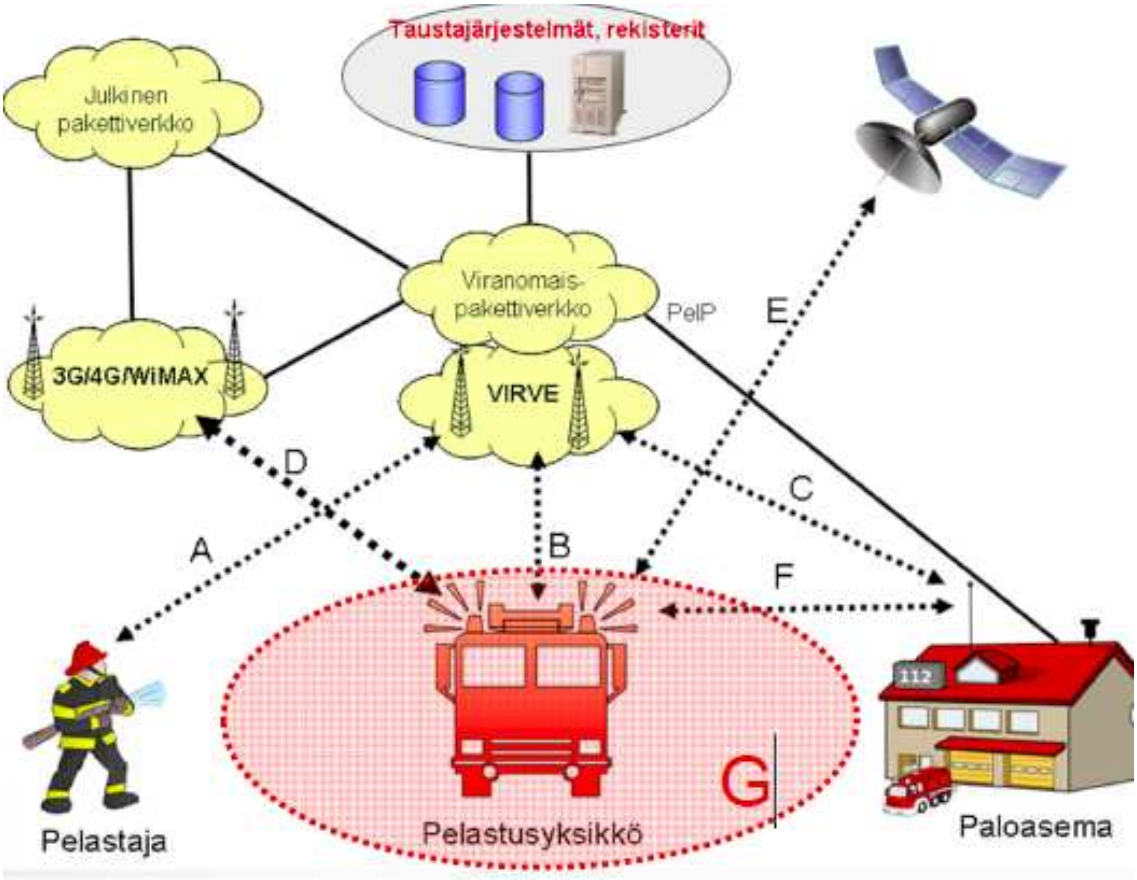


Kuva 13 Kuuluvuusalueen laajentaminen WLAN -verkon avulla

Jotta eri hälytysajoneuvot voisivat toimia tietojen välittäjinä, pitäisi eri viranomaisilla olla käytössä yhteisistä palveluista samat ohjelmistot. Tämä siksi, että tapahtuma paikalla eri hälytysajoneuvot ovat yleisemmin eri viranomaisten. Näin ratkaisuehdotus saataisiin hyödynnettyä kokonaisvaltaisesti, mutta ratkaisuvaihtoehto toimii myös vaikka yhteinen WLAN -verkko toimisi vain yhden viranomaisajoneuvotyypin esimerkiksi paloautojen välillä.

Junttila ja Rantama (2011) tutkimuksessaan ovat verranneet eri tiedonsiirtomahdollisuuksia. Kuvassa 14 nähdään heidän tulevaisuuden visiot mitä tiedonsiirtoteitä ja mihin tarkoitukseen he ovat visioineet. Kuvassa 14 Junttila ja Rantama (2011) ovat visioineet langattomat tiedonsiirto rajapinnat seuraavasti. Kuvan siirtotie A on VIRVE -ilmarajapinta käsiradiopuhelimeen, B on VIRVE:n ilmarajapinta ajoneuvoradioon/modeemiin, C on VIRVE:n ilmarajapinta asemaradioon/modeemiin, D on Ilmarajapinta kaupallisiin verkkoihin, E on

satelliittiyhteys, F on pelastusyksikön ja paloaseman välinen WLAN -rajapinta sekä G on pelastusyksiköiden välinen WLAN verkko.



Kuva 14 Langattoman tiedonsiirron rajapinnat (Junttila ja Rantama, 2011)

Tutkimuksessaan Junttila ja Rantama ovat myös visioineet, että WLAN -verkko voisi olla yksi tulevaisuuden tiedon siirtoväylä pelastusyksiköiden välillä. Junttila ja Rantama (2011) tuovat uuden termin WLAN paloposti, joka tarkoittaa hälytysajoneuvon sekä julkisen WLAN -verkon välistä yhteyttä.

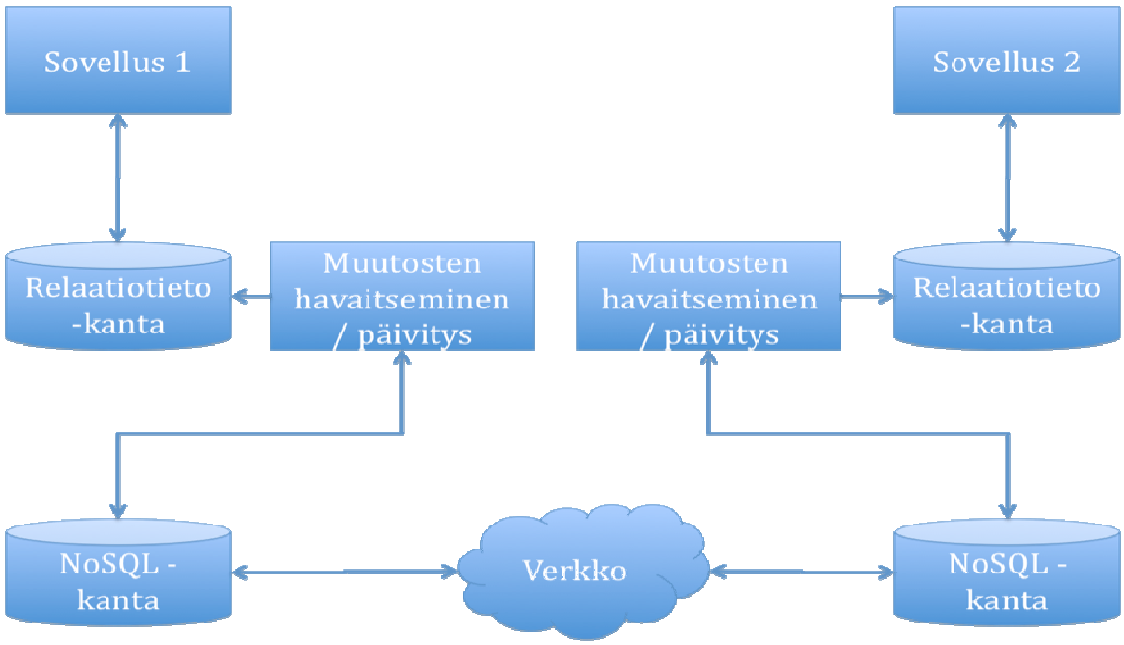
Junttilan ja Rantaman (2011) mukaan VIRVE -verkossa on mahdollista siirtää dataa, mutta tällä hetkellä verkon kapasiteetti ei riitä kuin 2-4 kbit/s (TETRA Rel 1) tiedonsiirto nopeuteen. Jotta pilvipalveluja voitaisiin tarjota järkevästi eli tarpeeksi nopealla tiedonsiirrolla, pitää VIRVE -verkon tiedonsiirto nopeutta parantaa. Junttilan ja Rantaman (2011) mukaan VIRVE -verkkoa ollaan jo nopeutettu leveäkaistaiseen (TETRA Rel 2) tiedonsiirtoon, mutta se ei ole vielä valtakunnan kattava ja sillä on tähän mennessä vain parannettu lyhytsanomien välitystä ruuhkaisemmilla seuduilla. Jotta todella pilvipalveluita voitaisiin suunnitella tarjottavan VIRVE -verkosta, niin VIRVE -verkko tulisi kehittää laajakaista verkoksi (TETRA Rel 3). Junttilan ja Rantaman (2011) mukaan tämä tarkoittaa sitä, että TETRA -tekniikkaan on saatu aikaiseksi laajakaistaratkaisu sekä viranomaisille pitää löytää oma taajuusalue

viranomaisviestintään. Juntila ja Rantama (2011) näkevät, että tämä voisi kuitenkin olla mahdollista 2010 -luvun loppupuolella tai 2020 -luvun alussa.

VIRVE -, Sateliitti -, WLAN -ja 3G -verkkojen lisäksi on olemassa myös muita verkkoja, joiden kautta voidaan tietoa siirtää. Miten näitä kaikkia verkkoa voitaisiin hyödyntää parhaan mahdollisen kuuluvuuden saavuttamiseksi? Tähän kysymykseen Holström, Rajamäki ja Hult ovat hakeneet ratkaisua tutkimuksessaan Tulevaisuuden ratkaisut ja teknologiat julkisen turvallisuuden tietoliikenteessä - DSiP tietoliikenneratkaisu turvalliseen monikanavaiseen tietoliikenteeseen. Holström, Rajamäki ja Hult (2011) ovat tutkineet miten Distributed Systems intercommunication Protocol® (DSiP) -ratkaisua voitaisiin hyödyntää julkisella turvallisuuspuolella, johon pelastustoimikin kuuluu. DSiP -kommunikointiratkaisu mahdollistaa tiedon siirron minkä tahansa verkon yli, niin IP kuin ei IP -pohjaisten verkkojen ja monioperaattori ympäristöjen mukaan lukien sateliitti, 3G, GPRS, UMTS, HDSPA, IP-verkko, TETRA, sarja yhteydet ja radio modeemi yhteyksien kautta (Holström, Rajamäki ja Hult, 2011). Holströmin, Rajamäen ja Hultin (2011) mukaan muiden monikanava ratkaisujen yhtenä ongelmana on ollut VPN -tunnelin luonti eri yhteyksiin, sillä VPN -tunneli luodaan aina per yhyteys. DSiP -ratkaisu tuo tähän ongelmaan Holströmin, Rajamäen ja Hultin (2011) mukaan ratkaisun. Holströmin, Rajamäen ja Hultin (2011) mukaan DSiP -peittää taakseen tietoliikenteen avausmekanismit, jolloin sovellus, joka tarvitsee verkkoyhteyttä ei tiedä mitä verkkoa se tulee käyttämään. DSiP -protokolla on kehitetty tarjoamaan yhdenmukaisen ja deterministisen tietoliikennemetodin reitittimien ja sovellusmoduulien välille (Nordman ja muut, 2003). Jotta katvealue ongelmaa saataisiin vähennettyä, niin DSiP on yksi vaihtoehto. DSiP:n hyödyntäminen tarkoittaisi sitä, että hälyytysajoneuvoissa tulisi olla monikanavareitittimet, jotka tukevat DSiP -protokollaa.

4.2 Hajautusratkaisu

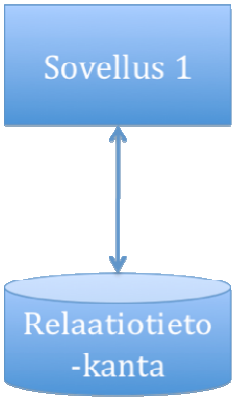
Seuraavassa kuvataan hajautusratkaisu, jota hyödyntämällä voidaan rakentaa avoimen lähdekoodin ohjelmistoa hyödyntäen hajautettava ratkaisu relaatiotietokantaa hyödyntäviin sovelluksiin. Seuraavassa kuvassa 15 on kuvattu miten hajautus voidaan tehdä.



Kuva 15 Hajautusratkaisu: Kokonaiskuva

Kuvan 15 mukaisella ratkaisulla päästään siihen, että kaikissa hälytysajoneuvoissa on sama tieto käytettävissä sekä jokaisessa hälytysajoneuvossa voi myös päivittää tietoja. Jotta tietojen replikointi toimisi, niin ratkaisu tarvitsee jonkunlaisen verkkoyhteyden. Seuraavassa käydään tarkemmin läpi hajautusratkaisun eri vaiheet.

4.2.1 Tietokantaoperaatioiden kirjoitus relaatiotietokantaan



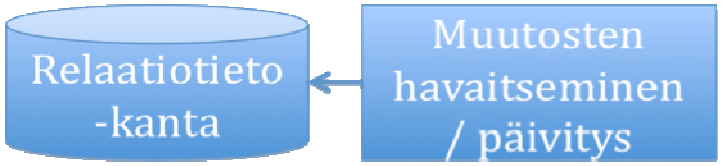
Kuva 16 Tietokantaoperaatioiden kirjoitus relaatiotietokantaan

Kuvan 16 sovellus 1 päivittää tietokantaa jollakin tavalla esimerkiksi päivittämällä, lisäämällä tai poistamalla sieltä tietoja. Sovellus 1 voi olla tehty millä tahansa arkkitehtuurilla sekä ohjelmointikielellä, sillä ei ole vaikutusta tässä esitettyyn hajautusratkaisuun. Sovellus 1 voidaan tehdä tietokantaoperaatiot siten kuin ne on tehty ennenkin, sillä tässä ehdotettu hajautusratkaisu ei aiheuta minkäänlaisia muutoksia olemassa olevaan järjestelmään.

Myöhemmin tässä tutkimuksessa tulen esittämään tässä esitetystä hajautusratkaisusta vielä muutetun version, jota voidaan käyttää silloin, kun tehdään uutta järjestelmää. Tässä myöhemmin esitettävässä ratkaisussa tulen esittämään vaihtoehtoja sille miten sovellusten tulisi tehdä tietokantaoperaatiot.

Kun sovellus 1 on kirjoittanut tietokantaoperaation, niin relaatiotietokanta kirjoittaa siitä tiedon tietokantalokiin. Tietokantaloki on joukko ensiö- ja toisiolokitiedostoja, joihin tallentuvat kaikki tietokannan muutoksista kertovat lokitietueet. Tietokantalokia käytetään sitoutumisjänteen muutosten peruutuksessa (jos muutoksia ei ole vielä vahvistettu) ja tietokannan palautuksessa eheään tilaan (IBM, 2002).

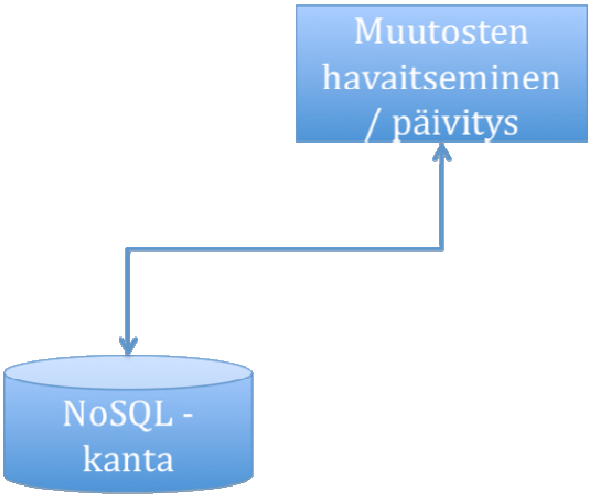
4.2.2 Muutosten luku relaatiotietokannasta



Kuva 17 Muutosten luku relaatiotietokannasta

Jotta relaatiotietokantaan kirjoitetut muutoksen saataisiin kirjoitettua NoSQL -tietokantaan, niin joudutaan kirjoittamaan itse ohjelma, joka tutkii relaatiotietokannan kirjoittamaa tietokantalokia, kuten kuvassa 17 on kuvattu. Tutkimusta kirjoitettaessa näyttää siltä, että muutoksen havaitseminen ja muutoksen siirto hajautuksesta huolehtivaan NoSQL -tietokantaan pitää tehdä räätälöidyllä sovelluksella. Tilanne voi kuitenkin muuttua avoimen lähdekoodin ratkaisujen osalta lähivuosina, koska erityylisten tietokantaratkaisujen yhteiskäyttö on voimakkaasti esillä internet -ratkaisuja kehittävissä sovelluskehittäjäyhteisöissä. Jo tällä hetkellä puhutaan hybridiratkaisuista erityisesti julkisessa pilvipalvelun ja yrityksien sisäisten tietokantojen yhdistämisessä (Harrison, 2011).

4.2.3 Tallennus NoSQL -tietokantaan



Kuva 18 Tallennus NoSQL -tietokantaan

Kuvassa 18 kuvataan hajautusratkaisun vaihetta 3, jossa räätälöidyn ohjelman avulla kirjoitetaan tiedot NoSQL -tieotokantaan. Kuten kohdassa 5.1.5 mainitaan, niin NoSQL .tietokannat tarjoavat yksinkertaisemman rajapinnan tietokantaoperointiin kuin relaatiotietokannat. Tässä hajautusmallissa esimerkki NoSQL -tyyppiseksi tietokannaksi on valittu CouchDB. CouchDB tarjoaa JSON -tyyppisen kyselyrajapinnan, jolloin tietokantaan voidaan tehdä avain-arvo -pari tyyppisiä tietokantaoperaatioita REST (Representational State Transfer) -rajapinnan kautta.

JSON on lyhenne sanoista JavaScript Object Notation. JSON on yksinkertainen tiedonsiirtomuoto, jossa tiedot lähetetään avain-arvo -pareina. Esimerkki JSON -tiedonsiirtomuodosta, jossa kuvataan OPERAATIO niminen viesti, jonka id eli yksilöivä tunniste on 12345 ja viesti sisältää UPDATES ja INSERTS toiminteita eli päivityksiä sekä lisäyksiä. UPDATE kohta sisältää yksittäiset UPDATE eli päivitysoperaatiot ja vastaavasti INSERT kohta sisältää kaikki yksittäiset lisäysoperaatiot.

```
{”OPERATIONS”: {
  ”id”: ”12345”,
  ”UPDATES”: {
        ”UPDATE”: [
          {”id”: ”1”, ”value”: ”3” },
          {”id”: ”2”, ”value”: ”1” }
        ]
   }
  ”INSERTS”: {
        ”INSERT”: [
          {”id”: ”3”, ”value”: ”4” },
        ]
   }
 }
}
```

Selvyydeksi sama yleisemmin tunnetussa XML -muodossa:

```
<OPERATIONS id=”12345”>
  <UPDATES>
    <UPDATE id=”1” value=”3” />
    <UPDATE id=”2” value=”1” />
  </UPDATES>
  <INSERTS>
    <INSERT id=”3” value=”4” />
  </INSERTS>
</OPERATIONS>
```

REST -rajapinnan kautta voidaan käyttää http -operaatioita POST, GET, PUT ja DELETE, jotta voidaan tehdä 4 perus tietokantaoperaatiota: luoda uusi tietue, lukea tietue, päivittää tietue sekä poistaa tietue (Anderson ja muut, 2010).

4.2.4 Replikointi

Kuva 19 Replikointi

Kuvassa 19 kuvataan hajautusratkaisun vaihetta 4, jossa NoSQL -tietokannat replikoivat muutoksensa verkon yli. Muutoksen replikointi tapahtuu NoSQL-kannan tarjoamin keinoin, jotka vaihtelevat kannoittain. Osa NoSQL-ratkaisuista on sellaisia, että ne eivät toimi paikallisessa ympäristössä riittävän hyvin. Esimerkiksi Google BigTable ja osa sen avoimen lähdekoodin johdannaisista (esimerkiksi HBase) perustuu hajautetun tiedostojärjestelmän käyttöön, joka asettaa rajoituksia sen käytölle paikallisessa ja katkonaisessa ympäristössä. Tästä syystä tässä tutkimuksessa keskitytään CouchDB:n tarjoamaan replikointiin.

Andersonin ja muiden (2010) mukaan CouchDB replikoi kannan muutokset käyttäen HTTP/Sprotokollaa ja JSON-muotoa. CouchDB on ns. dokumenttiorientoitunut kanta, eli se tallettaa JSON-muotoisia dokumentteja rivien ja sarakkeiden tai avain/arvo-parien sijaan (Anderson ja muut, 2010). Replikointi perustuu REST-toimintamalliin, jossa sanomat välitetään HTTP-verbien mukaisilla pyynnöillä kannasta toiseen, esimerkiksi päivitys lähetetään PUT-sanomana. CouchDB ei ylläpidä itse hajautusverkkoa, vaan se tekee replikointia minkä tahansa sille annetussa URL-osoitteessa vastaavan toisen CouchDB-instanssin kanssa. Näin ollen hajautusverkon ylläpito on räätälöitävä erikseen, tosin se voidaan tallettaa CouchDB-kantaan, jolloin rakenne hajautuu kaikille kannoille. CouchDB perustuu versioivaan talletustapaan. Konfliktitilanteessa kanta tallettaa molemmat versiot ja antaa sovelluksen tai käyttäjän päättää kumpi on oikeassa (Anderson ja muut, 2010). CouchDB

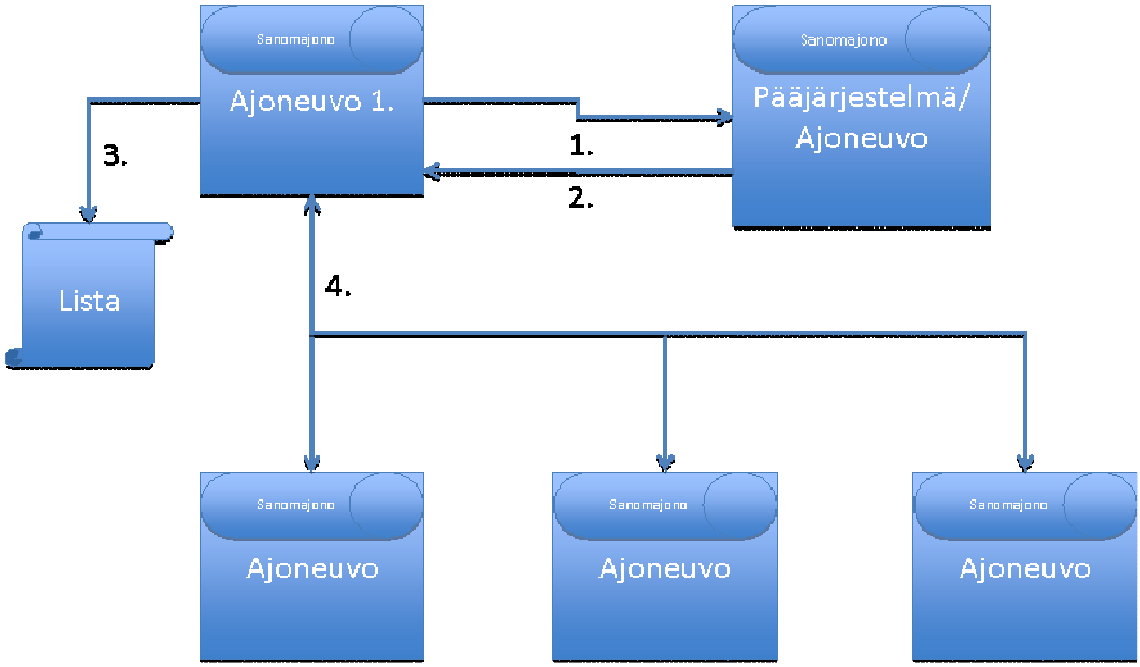
käyttää konfliktien havaitsemiseen ja automaattiseen ratkomiseen vektorikelloon perustuvaa ratkaisua, joten se on riippumaton tietokanta -instanssien keskinäisestä kellonaikojen synkroinnista (Anderson ja muut, 2010). Jokainen tietokanta kuitenkin huolehtii siitä, että on eheässä tilassa. Monen tietokannan muodostama hajautusverkko on lopulta eheä (engl. eventually consistent), kun tiedot ovat replikoituneet kaikkiin verkon tietokantoihin.

CouchDB-replikoinnin käynnistämiseen on useita eri vaihtoehtoja.

1. Jos hajautusverkon rakenne on kohtalaisen pysyvä eli kohde tietokannat ovat tyypillisesti samoja, voidaan CouchDB asettaa replikoimaan tiedot automaattisesti.
2. Jos hajautusverkko muuttuu voimakkaasti, voidaan CouchDB replikointi käynnistää ajoittain tai muutostapahtuman yhteydessä kannan ulkopuolisella ohjelmalla lähettämälle kannalle komento.

Vaihtoehdossa 2, jossa replikointi käynnistetään ulkopuolisen ohjelman toimesta voitaisiin yhtenä vaihtoehtona ajatella sanomajono -toimintoja. Tässä replikointi voitaisiin käynnistää sanomajonoon lähetettävän viestin avulla. Käynnistysviestin lähettäjänä voisi toimia muutosten havaitsemiseen rakennettu räätälöityohjelma.

4.2.5 Replikoinnin käynnistys.



Kuva 20 Päivityksen käynnistys

Kuvassa 20 on kuvattu miten tämä voisi käytännössä toimia. Kun ajoneuvossa oleva järjestelmä halutaan ottaa käyttöön, niin ensimmäisenä järjestelmä yrittää ottaa yhteyttä pääjärjestelmää tehdäkseen tunnistautumisen. Mikäli yhteys saadaan, niin tunnistautuminen

suoritetaan käyttäjän tunnuksilla sekä esimerkiksi ajoneuvon tunnisteella tai sitten vain järjestelmän tunnisteella, mikäli katsotaan, että toiminnan kannalta ajoneuvon järjestelmän käyttäjällä ei ole merkitystä. Kun tunnistautuminen on onnistunut, niin vastauksena pääjärjestelmä palauttaa ajoneuvolle oikeusryhmät, joilla rajataan siirrettäviä tietoja ajoneuvoon. Mikäli sitten käy niin, että ajoneuvo ei saa yhteyttä pääjärjestelmään, niin tässä tapauksessa on kaksi vaihtoehtoa: 1. Ilman tunnistautumista ajoneuvon ohjelmaa ei saa käyttöön. Tämä on tietoturvan kannalta paras vaihtoehto, mutta käytännössä tämä voi aiheuttaa ongelmia. Ajatellaan tilannetta, että jostain syystä ajoneuvon järjestelmä jouduttaisiin käynnistämään uudelleen katvealueella, josta ei saada yhteyttä pääjärjestelmään, tällöin järjestelmällä ei olisi käyttöä, joka taas voi vaarantaa varallisuutta tai jopa ihmishenkiä. 2. vaihtoehdossa ilman tunnistamista, ajoneuvon ohjelmalla olisi kuitenkin perusoikeusryhmät tai minimioikeusryhmät, joilla ohjelman saa käyttöön tarvittavilla minimi- / perustiedoilla. Tällöin ohjelma saataisiin käynnistettyä myös katvealueella ja ohjelmalla olisi käytännön toiminnassa jotain hyötyä. Itse kutsu pääjärjestelmään tulisi kuitenkin olla helppo ja nopea suorittaa eikä kutsuvan järjestelmän arkkitehtuurilla saa olla tässä merkitystä. Kutsu pitää myös olla suojattu, sillä kutsussa liikkuu arkaluontoista materiaalia, kuten esimerkiksi käyttäjätunnuksia ja salasanoja. Vastaus tulee myös olla suojattu, sillä siinä liikkuu oikeusryhmätietoja, jotka saadessaan tunkeutuja voi saada tietoonsa arkaluontoista tietoa muista järjestelmistä simuloidessaan ajoneuvon ohjelmaa. Tunnistautumisliittymä voitaisiin toteuttaa Web Service -tekniikalla. Web Service tekniikalla tehty liittymä voidaan suojata WS-Security:n avulla. WS-Security on käsitteellinen malli, joka tiivistää eri suojausteknologiat vaatimuksiksi sekä valtuutuksiksi (Rosenberg ja muut, 2004).

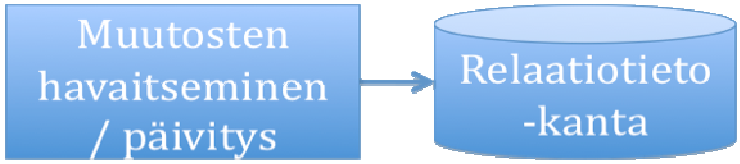
Tunnistautumisen onnistuttua tavalla tai toisella, niin seuraavaksi ohjelma lukaisee tietokannassaan olevasta listauksesta kaikkien hajautusverkostossa olevien ohjelmien osoitteet, joilta se voi pyytää päivitykset. Jotta päivitys olisi mahdollisimman nopea, niin sen ohjelman, jolta päivitystä pyydetään, tulisi olla mahdollisimman lähellä sekä mahdollisimman nopean yhteyden päässä. Miten tämä sitten voitaisiin havainnoida ennen päivityspyynnön lähettämistä? Ohjelma, voisi ensin kysyä kaikilta muilta hälytysajoneuvoilta niiden sijaintitiedot, jolloin ohjelma pystyy päättelemään mikä näistä muista ohjelmista on lähinnä. Samalla ohjelma voisi ottaa aikaa sijaintipyynnön kyselynkestosta, jolloin se voi päätellä mikä ohjelmista vastasi nopeimmin. Tämä testi ei välttämättä kerro mikä ohjelmista on nopeimman yhteyden päässä, mutta se ainakin kertoo sen, mikä ohjelmista pystyy palvelemaan nopeimmin.

Ajoneuvon valinnan jälkeen, luodaan päivityspyyntöviesti, joka sisältää tiedon ohjelmasta sekä ajoneuvosta. Viestissä lähetetään päivityspyyntö sekä tunnistautumisesta saadut oikeusryhmät. Tunnistautumistietojen lisäksi viestissä menee vastausjono, johon

päivitystiedon lähettävä ohjelma toimittaa päivitystiedot. Oikeusryhmätietojen lisäksi viestissä voisi mennä muita päivitystietoja rajaavia määreitä, jolloin ei tarvitse välttämättä siirtää aina kaikkia tietoja, jos ne ei kaikkia ari ajoneuvoja kiinnosta ja näin saadaan myös vähennettyä verkkoliikennettä.

Jokaisen ajoneuvon ohjelma siis sisältää oman sanomajonon ja sanomajonon ylläpitämistä varten jokaisessa ajoneuvossa on siten sanomajonopalvelin. Jotta ajoneuvon arkkitehtuurin rakentamisesta ei tulisi liian kallis toteuttaa, niin markkinoilla on tällä hetkellä hyviäkin avoimen lähdekoodin lisensseillä tuotettuja sanomajonopalvelimia. Mainittakoon tässä yhteydessä Apache:n ActiveMQ. Sanomajonojen arkkitehtuuri menisi siten, että kyselyyn tarkoitetut sanomajonot olisivat jokaisella ajoneuvolla ja vastausjonot kyselevällä ajoneuvolla. Eli jos ajoneuvo X kysyy ajoneuvolta Y päivitystietoja, niin ajoneuvo X lähettää kyselyn ajoneuvo Y:llä olevaan sanomajonoon ja toimittaa kyselyviestissä vastausjonon tiedot, joissa vastausjonon osoite viittaa ajoneuvolla X olevaan sanomajonoon. Tällä arkkitehtuurilla päästään siihen, että ajoneuvo X tietää, että kysely lähti ja ajoneuvo Y lähettää vastauksen vain, mikäli ajoneuvo X on vielä yhteydessä verkkoon. Näin ei jää turhia kyselyitä eikä vastauksia roikkumaan. Toisaalta mikäli vastausjonotkin olisivat kyselyn kohteella eli esimerkin tapauksessa ajoneuvo Y:llä ja kummatkin sanomajonot olisivat persistoiduttu tietokantaan eli määritelty pysyväisiksi, jolloin ohjelman sammuessa kyselyt sekä vastaukset tallennettaisiin esimerkiksi tietokantaan tai tiedostojärjestelmään. Mikäli meneteltäisiin näin, niin tässä vaihtoehdossa on ongelmana se, että turhia viestejä jäisi roikkumaan sanomajonoihin sekä ohjelmat saisivat jo vanhentuneita tietoja. Mutta hyvänä puolena tässä vaihtoehdossa olisi se, että kyselyt ja vastaukset menisivät aina perille. Se kumpi näistä vaihtoehdoista olisi paras, niin voidaan vasta sanoa kokemusten jälkeen.

4.2.6 Muuttuneiden tietojen päivitys kohde kantaan



Kuva 21 Muuttuneiden tietojen päivitys kohde kantaan

Muutosten saavuttua NoSQL -pohjaiseen tietokantaan, niin räätälöity muutostenhallintakomponentti lukee NoSQL -tietokantaan tulleet muutokset ja suorittaa ne ajoneuvon relaatiotietokantaan, kuten kuvassa 21 on kuvattu. Mahdollisen ongelmakohdan tässä voi aiheuttaa relaatiotietokannan päälle rakennettu järjestelmä. Mikäli järjestelmässä on käytetty jotain muistinvaraista tekniikkaa esimerkiksi JPA (Java Persistence Api) tietokannan käsittelyyn, niin se ei välttämättä huomaa sen ohi tehtyjä tietokantaoperaatioita. Riippuen tekniikasta, jolla kyselyt on tehty, että tarjoaako se

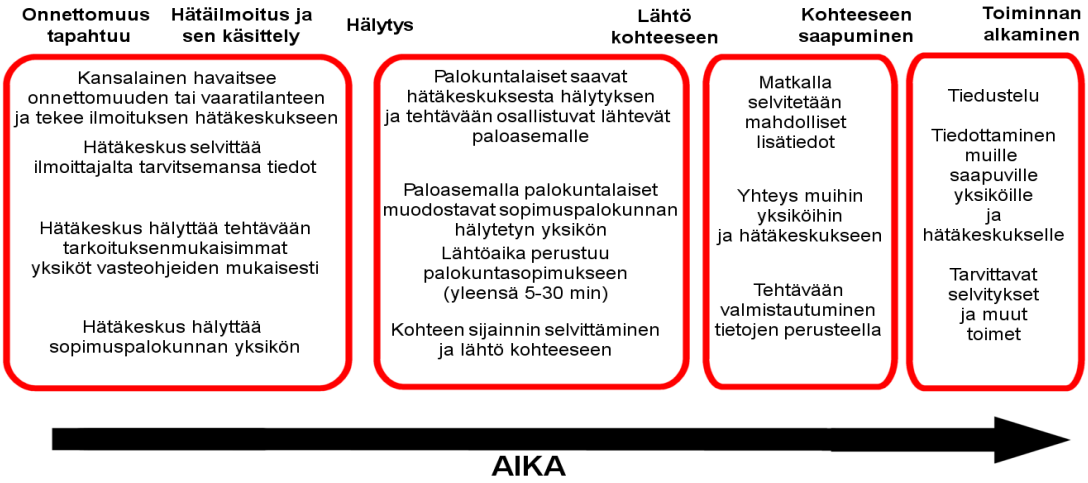
valmiiksi rajapintaa, jolla voitaisiin muutostenhallintakomponentista komentaa sitä päivittämään muistinsa tietokannasta vai tarvitseeko järjestelmään toteuttaa kyseinen rajapintapalvelu.

4.3 Pilvipalvelujen hyödyntäminen

Kuten aikaisemmin on jo mainittu, niin Suomen Erillisverkot Oy:n ylläpitämästä viranomaisverkosta (VIRVE) voisi tarjota erilaisia pilvipalvelja eri viranomaisille. Eri viranomaisten omat verkot ovat jo nyt tänä päivänä yhteydessä VIRVE -runkoverkkoon. Tämä mahdollistaa sen, että VIRVE -runkoverkosta voitaisiin aloittaa tarjoamaan pilvipalveluja suht helposti eri viranomaisille, sillä tarvittavat yhteydet eri verkkojen suhteen on jo olemassa.

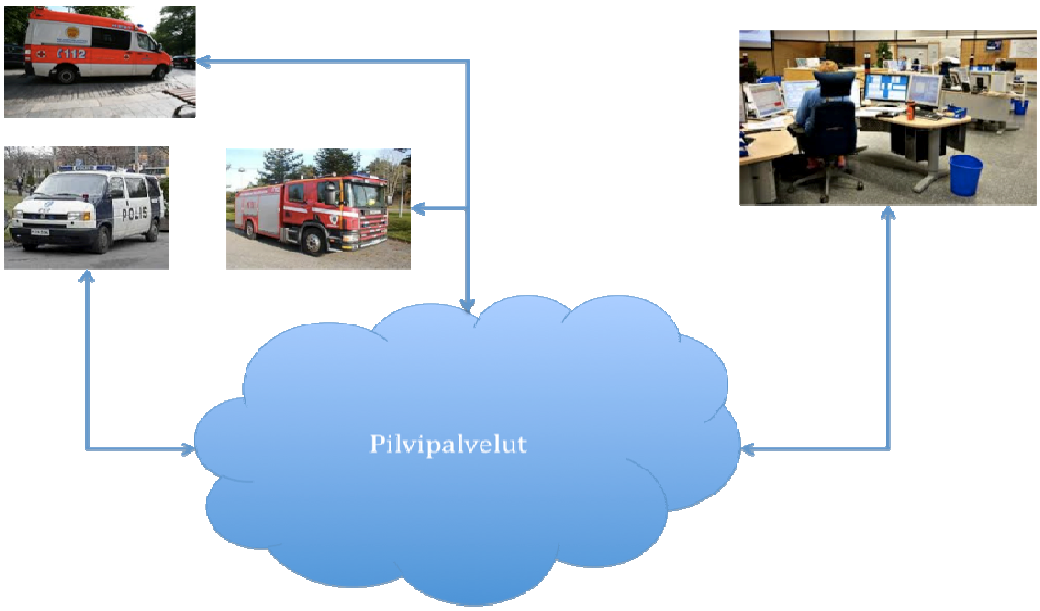
Yhteisillä pilvipalveluilla saataisiin helpotettua sovellusten ylläpitoa sekä parannettaisiin niiden saatavuutta. Kuten aikaisemmin jo on mainittu, niin yhteiset pilvipalvelut myös edistäisivät viranomaisten keskinäistä tiedon vaihtoa, mikäli näin haluttaisiin. Pilvipalveujen avulla myös vähennettäisiin sovellusten ylläpitokustannuksia, sillä toisin kuin nyt, niin jokaisen viranomaisen ei tarvitse enää itse huolehtia sovellusten ylläpidosta vaan siitä huolehdittaisiin keskitetysti. Tämä tietysti riippuu siitä millaisia pilvipalveluita tultaisiin tajoamaan sekä millaisia pilvipalveluja oltaisiin valmiit hankkimaan.

Mitä hyötyä sitten yhteisistä pilvipalveluista voisi käyttännössä olla? Alla olevassa kuvassa 22 Urpila (2011) on kuvannut opinnäytetyössään sopimuspalokunnan näkemyksen hälytystehtävien etenemisen eri vaiheita. Kuvasta nähdään, että hälytykset yleensä lähtevät liikenteeseen siitä, että kansalainen tekee havainnon ja ilmoittaa siitä hätäkeskukseen. Hätäkeskus tämän jälkeen hälyttää tehtävään vasteohjeiden mukaan tarkoituksen mukaisen yksikön tai yksiköt. Palokunta saatuaan hätäkeskukselta hälytyksen muodostaa sopimuspalokunnan hälytetyn yksikön ja selvittävät kohteen sijainnin ja lähtevät kohteeseen. Matkalla pelastusyksikkö selvittaa mahdollisia lisätietoja ja luovat yhteyksiä muihin yksiköihin ja hätäkeskukseen. Toimintaan paikalla kuuluu tiedottaminen muille saapuville yksiköille sekä hätäkeskukselle.



Kuva 22 Palokunnan hälytystehtävän (Urpila, 2011)

Miten sitten pilvipalvelut voisivat parantaa Urpilan (2011) kuvaamaa toimintoketjua? Itse ketjun osa-alueet tulisivat todennäköisemmin pysymään samoina, mutta se miten tieto tulisi tässä tutkimuksessa ehdotetun kokonaisarkkitehtuurimuutoksen myötä liikkumaan eri vaiheissa tulisi muuttumaan. Kuvassa 23 on kuvattu miten tieto tulisi liikkumaan ehdotetussa mallissa.

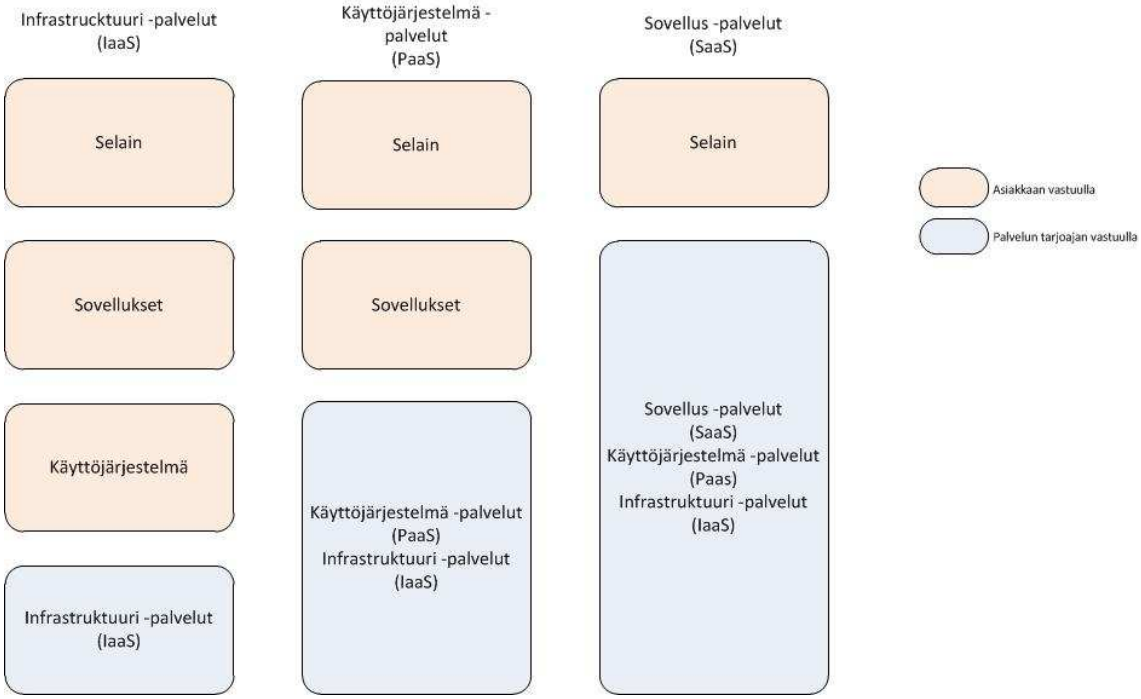


Kuva 23 Pilvipalvelujen hyödyntäminen

Karkeasti tietoliikkuisi siten, että edelleen kuten aikaisemminkin kansalainen ottaa yhteyttä hätäkeskukseen tehdäkseen hälytyksen. Hälytyskeskuksessa hälytyksen vastaanottava henkilö kirjaa hälytyksen yhteisiin pilvipalveluihin ja hälyttää vasteohjeiden mukaisesti tarkoituksenmukaisimmat yksiköt paikalle. Tässä vaiheessa tulisi se muutos, että hälytyskeskus voisi jatkaa lisätietojen syöttämistä järjestelmään sekä mahdollisesti suorittaa kohteen tarkemman sijainnin valmiiksi palokunnalle. Kun palokunta lähtee paikalle, niin heidän hälytysajoneuvossa oleva järjestelmä ottaisi yhteyden annetulla hälytyskoodilla yhteisiin pilvipalveluihin, josta se saisi kaikki hälytyskeskuksen syöttämät tiedot sekä jo mahdollisen kohteen tarkemman sijainnin. Tämän jälkeen palokunta voisi paikalle päästyään alkaa syöttämään samalla hälytyskoodilla tietoja yhteisiin palveluihin, josta tiedot olisivat saatavilla hätäkeskukselle sekä muille halytysajoneuvoille, jotka ovat tulossa tai ovat jo saapuneet paikalle. Tässä tutkimuksessa esitetty hajautusratkaisu toisi myös sen, että kaikkien osapuolten syötämät tiedot pysyisivät tallessa vaikka verkkoyhteyttä ei olisi saatavilla. Koska hälytysjoneuvot voivat keskustella keskenään paikallisen WLAN -verkon kautta, niin se parantaa tilannetiedon saatavuutta hätäkeskukselle, joka pystyy opastamaan kansalaista, joka on ilmoituksen tehnyt sekä opastamaan muita viranomaisia tai tarvittaessa lähettämään lisää yksiköitä paikalle.

Käytettäessä pilvipalveluita käyttäjät pääsevät helposti omiin tietoihinsa ja mikäli haluat, niin voivat helposti jakaa tietojaan muille Internetin kautta (Takabi ja muut, 2010). Kun otetaan Takabin ja muiden ajatus huomioon ja sovelletaan sitä tämän tutkimuksen kontekstissa, niin kuten yllä on kuvattu, hälytyskeskus ja eri viranomaiset saisivat helposti tietoa jaettua keskenään pilvipalvelujen avulla, mikäli niin halutaan, aina ei välttämättä haluta tietoa jakaa ja sekin on otettava huomioon pilvipalveluita suunniteltaessa.

4.4 Tarjottavat yhteiset pilvipalvelut sekä niiden vastuut



Kuva 24 Pilvipalvelut sekä vastuujako

Viranomaisverkosta voitaisiin tarjota kaikkia kuvan 24 mukaisia palveluja eri viranomaisille, mutta tämän tutkimuksen ratkaisuehdotuksessa lähdetään siitä, että asiakkaat eli tässä tapauksessa eri viranomaisten omaksi huoleksi jäisi ainoastaan asiakassovelluksen (engl. Client) ylläpitäminen ja sen huolehtiminen hälytysajoneuvoon. Myös kaikki muu infrastruktuuri, joka tulee itse hälytysajoneuvoon kuuluu jokaisen viranomaisen vastuulle. Tällöin puhutaan pilvipalvelumallista SaaS, jossa asiakas hankkii sovellusten käyttöoikeutta.

Tässä tapauksessa IaaS -palvelumallissa VIRVE -verkosta tarjottaisiin vain virtualisoituja rautatason palveluja. Tässä palvelumallissa ei vielä päästä siihen, että se pakottaisi viranomaiset jakamaan tietoja, sillä siinä jokaisella asiakkaalla olisi kuitenkin omat järjestelmänsä vaikka ne pyörisivätkin samassa fyysisessä raudassa. IaaS -palvelumallissa fyysinen rauta kuitenkin jaetaan virtualisoinin avulla erillisiksi virtuaalikoneiksi, jotka asiakkaalle näkyvät erillisinä fyysisinä koneina. IaaS -palvelumallissa olisi jo kuitenkin se säästö hyöty, että rautatason palvelujen ylläpitomaksut vähenisivät sekä itse ylläpito helpottuisi.

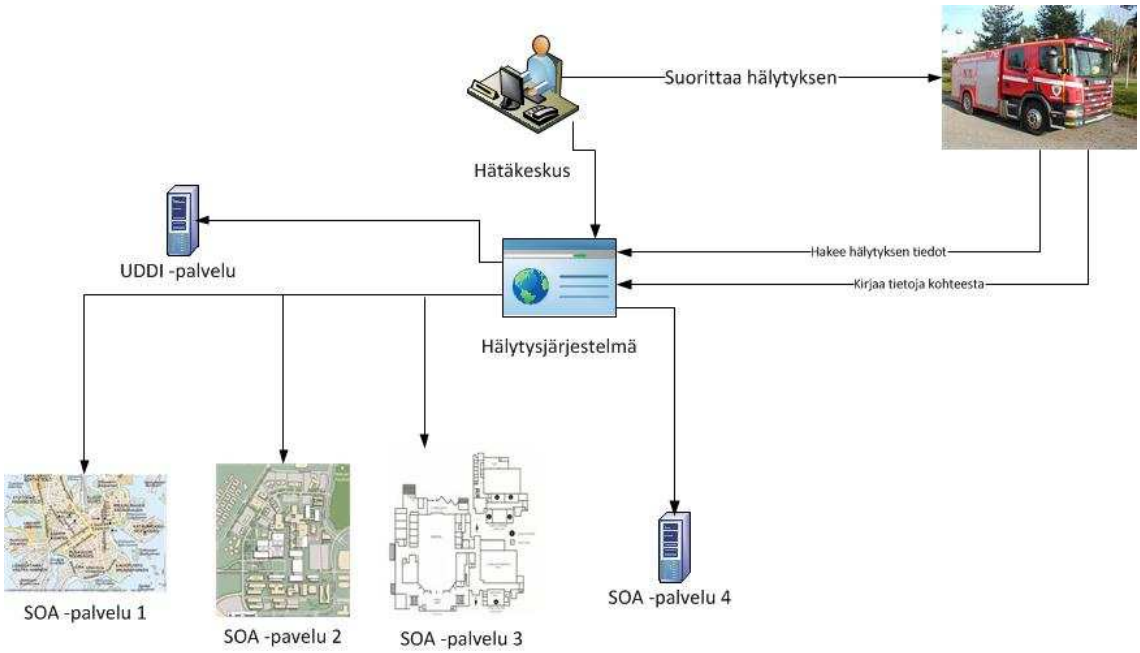
PaaS -pilvipalvelumallissa asiakkaat ostaisivat rautapalveluiden lisäksi käyttöjärjestelmän palveluna, jolloin asiakkaiden tulisi kuitenkin vielä huolehtia itse sovelluksista ja niiden asennuksista sekä yllöpidoista. Tällä mallilla oltaisiin kuitenkin jo yhtä pykälää lähempänä arkkitehtuuria, joka tässä tutkimuksessa on esitetty, mutta itse sovellukset olisivat vielä

erillisnä palveluina eri asiakkailla. PaaS -mallissa asiakkaalla olisi kuitenkin suuremmat oikeudet järjestelmään ja sen kehittämiseen.

SaaS -pilvipalvelumallissa asiakas ostaa pilvipalvelun tarjoajalta, joka tässä tapauksessa olisi Suomen Erillisverkot Oy, sovelluksen käyttöoikeutta. Tässä mallissa pilvipalvelun tarjoajalla on suurin vastuu palvelun toimivuudesta sekä saatavuudesta. Asiakas vastaa SaaS -mallissa vain omista käyttäjistään sekä heidän oikeuksista. Tämä malli on toisaalta asiakkaan kannalta helppo ja helposti saatavilla oleva, mutta kolikon kääntöpuolena tässä on se, että asiakkaalla ei ole juuri minkäänlaisia oikeuksia järjestelmän jatkokehitysten suhteen. Mikäli ostettava palvelu ei täysin vastaakaan asiakkaan odotuksia, niin asiakas ei itse voi tehdä päätöksiä järjestelmän muutoksista tai jatkokehityksistä, vaan ainoa mitä he voivat tehdä järjestelmän kehittämiseksi ovat muutospyynnöt pilvipalvelun toimittajalle ja toivoa, että järjestelmää kehitetään. Toinen suuri ongelma SaaS -palveluissa on se, että järjestelmä muutokset näkyvät heti kaikille samanaikaisesti. Tästä voi olla ongelmia, mikäli kaikki asiakkaat eivät halua tehtäviä päivityksiä samaan aikaan. Tämä edellä esitetty ongelma on kuitenkin kierrettävissä siten, että samasta ohjelmasta tarjotaan eri versioita eri asiakkaille, mutta se sotii vastaan ideaa, jossa eri viranomaiset käyttäisivät samaa ohjelmaa, jotta tieto viranomaisten välillä liikkuisi saumattomasti.

SaaS -pilvipalvelumallin avulla päästään tässä tutkimuksessa esitettyyn arkkitehtuuriratkaisuun, jossa kaikki viranomaiset käyttävät samoja sovelluksia ja tätä kautta siirtävät saumattomasti tietoja keskenään. Kuten aikaisemmin jo on mainittu, niin pilvipalvelun tarjoajalla tässä mallissa on suurin vastuu. Käytännön kannalta on kuitenkin järkevintä, että vastuu palvelujen saatavuudesta sekä kehittämisestä on keskitetty. Palvelujen keskittämisellä päästään siihen, että saadaan pienennettyä valtion IT -kustannuksia, jotka ovat tänä päivänä olleet aika suuret. Valtion ICT -kulut ovat vuonna 2009 olleet 1,8% Suomen valtion menoista (Benson, 2010), joka on aika suuri kulu, joten kulujen pienentämisestä ei ole ainakaan haittaa.

4.5 Palvelukeskeisen arkkitehtuurin (SOA) hyödyntäminen



Kuva 25 Palvelukeskeisen arkkitehtuurin hyödyntäminen

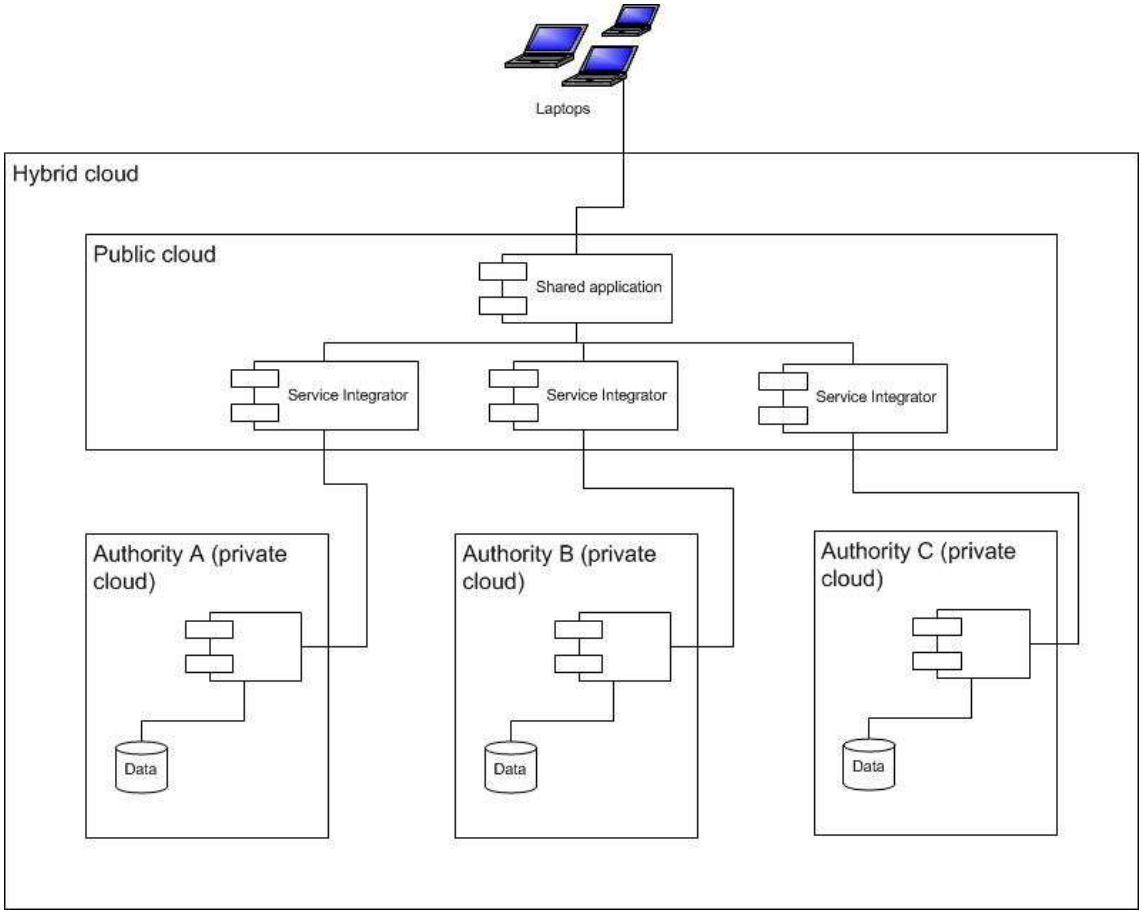
Tulevaisuudessa yhteisissä pilvipalveluissa tarjottavia sovelluksia voitaisiin rakenttaa palvelukeskeisen arkkitehtuurin avulla, myös olemassa olevia järjestelmiä voitaisiin laajentaa SOA:n avulla. SOA -mallissa eri viranomaiset, kuvassa 25 SOA -palvelut, voisivat rakentaa yksittäisiä palvelukomponentteja, jotka yksinään suorittavat jonkin tietyn yksittäisen tehtävän (engl. Task). Näitä palveluita yhdistämällä voitaisiin rakentaa kokonaisia järjestelmiä. Yleisessä pilvipalvelussa ylläpidettäisiin keskitetty palvelurekisteriä UDDI -palvelinta, jonne jokainen viranomainen voisi rekisteröidä omia kehittämiään palveluita. Näiden palvelujen avulla esimerkiksi saataisiin tehtyä tarvittavia hakuja eri viranomaisten olemassa olevista rekistereistä. Näin kasattu sovellus voitaisiin sitten tarjota yleisenä SaaS -mallin mukaisena palveluna VIRVE -runkoverkon pilvipalveluista.

Jokapäiväinen toiminta helpottuisi sekä nopeutuisi, kun rakennettaisiin hälytysjärjestelmä yllä kuvatun SOA -mallin mukaisesti. Pelatuslaissakin (2003) todetaan 4 luvun 12§, että pelastustoimi on suunniteltava ja toteutettava siten, että onnettomuuksien ehkäisy on järjestetty ja että onnettomuus- ja vaaratilanteissa tarvittavat toimenpiteet voidaan suorittaa viivytyksettä ja tehokkaasti. Kuten kuvassa 25 on kuvattu, niin hälytyskeskus suorittaisi hälytyksen lisäyksen sekä käynnistäisi kohteen tarkan paikannuksen saatujen tietojen perusteella. Hälytysjärjestelmä hyödyntäisi olemassa olevia toisia järjestelmiä paikkatietojen hakemiseen ja yhdistäisi näin saadut tiedot ja lisäisi ne hälyksen tietoihin. Hälytyskeskus suorittaisi itse halytyksen ja antaisi hälytyksen yhteydessä hälytysajoneuvossa olevalle järjestelmälle hälytyksen koodin. Hälytysajoneuvossa oleva järjestelmä kävisi

hälytyksen saatuaan hakemassa hälytyskeskuksen syöttämät tiedot hälytysjärjestelmästä. Näin päästäisiin siihen, että hälytykseen lähtiöillä olisi jo valmiiksi tiedossa kohde, joten sitä ei enää tarvitsisi lähteä hakemaan mistään papereista, kuten Santasalo ja muut (2010) tutkimuksessaan ovat selvittäneet. Santasalo ja muut (2010) selvityksen mukaan tänä päivänä palomestari hälytyksen saatuaa aloittaa kohteen selvityksen manuaalisesti kirjojen avulla. Kohteeseen päästyään hälytyshenkilökunta voisi syöttää samaan järjestelmään tietoja mitä kohteessa tapahtuu tai on tapahtunut. Näin tieto saataisiin mahdollisimman pian muiden viranomaisten käyttöön.

Koska viranomaistoimintaa rajoittavat Suomen laki ja säädökset ja jotkut ovat samat eri viranomaisille ja toisen eivät, niin SOA -arkkitehtuurin avulla, jokainen viranomainen vastaisi kuitenkin itse kehittämästään palvelusta sekä sen lainmukaisuudesta. Koska VIRVE -runkoverkosta on pääsy eri asiakas verkkoihin, niin asiakkaiden itse kehittelemänsä SOA -palvelut voitaisiin tarjota pilvipalvelun kautta ja itse palvelut olisivat vain yhteydessä asiakasverkossa oleviin muihin järjestelmiin. Tällä ratkaisulla saadaan kasvatettua palvelujen saatavuutta. Ratkaisun pullonkaulana olisi tällöin ne sovellukset tai palvelut, joita SOA -palvelu käyttäisi asiakkaan omasta verkosta, sillä niiden saatavuudesta vastaisi asiakas itse kuten ennenkin.

Takabin ja muiden (2010) esittelemän Secure Cloud -tietoturvamallin ideana on SOA maisesti integroida useita eri pilvipalveluja yhteen siten, että ne muodostavat yhtenäisen ja turvallisen järjestelmän. Secure Cloud -tietoturvamallissa otetaan kantaa juuri eri palveluiden väliseen integraatioon. Suurimpana ongelmana Takabi ja muut (2010) ovat nähneet palveluiden väliset käyttäjän tunnistamiset, hallinnan sekä pääsynvalvonnan. Takabi ja muut (2010) ehdottavatkin, että SOA maisesti jokaiselle palvelulle rakennettaisiin Service Integrator -luokka, joka vastaisi yllä mainituista käyttäjän tunnistamisista, hallinnasta sekä pääsynvalvonnasta. Tässä tutkimuksessa esitetyssä mallissa tämä tarkoittaisi sitä, että eri viranomaiset rakentaisivat omien palvelujensa eteen Service Integrator -luokan, jotta tästä saataisiin täydellinen ja kaikkia palveleva ja hallittu kokonaisuus, niin arkkitehtuurillisesti Service Integrator on rajapinta (engl. Interface), jonka jokaisen palvelun tarjoaja tulisi toteuttaa (engl. implement).



Kuva 26 Palvelukeskeinen pilvipalvelumalli

Kuvassa 26 on kuvattu mahdollinen pilvipalvelu ratkaisu Suomen viranomaisille, jossa viranomaisilla on yksityiset pilvipalvelut, joiden avulla eh voivat suojata arkaluotoisia tietojaan. Julkisesta pilvestä oleva sovellus käyttää kuitenkin viranomaisten tarjoamia Service Integrator -palveluita, jotka huolehtivat intergraation tietoturvaan liittyvistä asioista. Näin toimittaessa viranomaiset rakentaisivat palvelukeskeisen arkkitehtuurin (SOA) mukaisia palveluita yksityisiin pilviinsä ja tarjoaisivat niitä julkisen pilven kautta. Tästä syntyisi Hybrid -mallinen pilvipalvelu, jossa yhdistettäisiin yksityisiä pilvipalveluita sekä julkisiä palveluja. Kaikki pilvipalvelut olisivat kuitenkin tarjottu Suomen Erillisverkot Oy:n toimesta keskitetysti VIRVE -verkon yhteisistä pilvipalveluista.

4.6 Kokonaisarkkitehtuurin tietoturva

Seuraavassa taulukossa 5 on rakennettu tämän tutkimuksen yhtenä tuloksena malli, jossa on lueteltu 5 tärkeintä tietoturvauhkaa, jotka tämän tutkimuksen kokonaisarkkitehtuuriratkaisussa tulee ottaa huomioon.

Nro	Asia	Kuvaus
1	Aineisto luokitukset	Pitää ottaa huomioon millaista aineistoa järjestelmässä tullaan käyttämään. Aineiston tietoturvaluokitukset vaikuttavat suojaustasoihin sekä siihen voidaanko edes pilvipalveluja edes käyttää.
2	Jaettu teknologia	Päättäjän pitää huomioida, että pilvipalveluissa on myös muita käyttäjiä, jolloin tietoturvauhkat eivät tule vain suoraan internetistä vaan tietoturvauhan voi aiheuttaa toisessa järjestelmässä oleva tietoturva-aukko.
3	Vähäisimpien oikeuksien periaate	Huolehditaan siitä, että ei tule ns. vaarallista yhdistelmää, jossa yhdellä käyttäjällä on liian suuret oikeudet. Vaarallinen yhdistelmä tulee silloin, kun käyttäjä voi esimerkiksi luoda käyttäjätunnuksen ja antaa sille oikeuksia sekä tehdä muutoksia järjestelmään ja tämän jälkeen poistaa käyttäjätunnus, jolloin ei jää jälkiä muutoksesta.
4	Syvyyssuuntainen puolustus	Huolehditaan siitä, että järjestelmässä on useita arkkitehtuurillisia kerroksia, jolloin saadaan paras turva siihen olennaisimpaan eli aineistoon.
5	Tietoturvapoikkeamien asianmukainen käsittely	Huolehdittava siitä, että on olemassa tietoturvaohjeistus, jossa otetaan kantaa siihen miten tietoturvapoikkeamissa toimitaan sekä muihin tietoturvaan liittyviin asioihin. Huolehdittava, että SLA -sopimukset ovat kunnossa.

Taulukko 5 Viisi tärkeintä tietoturvauhkaa

Tämä malli on syntynyt kirjallisuustutkimuksessa selvitettyjen CSA:n sekä OWASP:n listaamien tietoturvauhkien pohjalta sekä osaksi omien huomioiden pohjalta. CSA eikä OWASP ole kiinnittäneet huomiota itse aineistonluokituksiin vaikka heidän listaamansa tietoturvauhat pyrkivätkin suojaamaan juuri aineistoa. Aineisto on kuitenkin se yrityksen tärkein suojattava kohde. Tärkeintä on päättäjän ensimmäisenä selvittää millaista aineistoa järjestelmässä käsitellään, jotta hän voisi miettiä voidaanko pilvipalveluita hyödyntää lainkaan ja jos voidaan, niin millaista pilvimallia tulisi käyttää ja mitä pilvipalveluja voidaan käyttää. Se, että aineisto on luokiteltu salaiseksi, niin ei automaattisesti tarkoita sitä, että pilvipalveluita ei voitaisi käyttää. Tässä tapauksessa voitaisiin esimerkiksi harkita hybridi -mallia, jossa aineisto olisi turvassa yksityisessä pilvessä ja järjestelmän julkinen osa olisi julkisessa pilvessä.

Jaettu teknologia on haasteellinen, sillä päättäjien tulee huomioida, että tietoturvariski ei välttämättä tulekaan omasta järjestelmästä, vaan uhkan voi aiheuttaa jonkin toisen käyttäjän

järjestelmässä oleva tietoturva-aukko. Päättäjien tulee selvittää tarkasti, että voidaanko tällaisen riskin kanssa tulla toimeen vai pitääkö pilvipalvelun tarjoajalta saada ns. ulkopuolinen yksityinen pilvipalvelu, jossa itse palvelut ovat yrityksen ulkopuolella, mutta kuitenkin rajattu siten, että kyseisen pilven palvelut ovat vain yhden yrityksen käytössä.

Vähäisempien oikeuksien periaatteessa kuten taulukossa 5 on kuvattu, niin päättäjän on tärkeää huolehtia siitä, että ei pääse syntymään sellaisia ”super” käyttäjiä, jotka pääsisivät tekemään hallaa järjestelmässä. Pilvipalveluissa päättäjän tulee edellyttää pilvipalvelun tarjoajalta, että heidän hallinnoijat eivät myöskään saa liian isoja oikeuksia hallinnointiin. Esimerkiksi pilvipalvelun ostajan tulisi vaatia, että pilvipalveluiden hallinnoinnissa ei ole yhtä käyttäjää, joka voisi luoda koneille käyttäjätunnuksen sekä antaa sille esimerkiksi pääkäyttäjän oikeudet. Tällä yhdistelmällä saadaan jo aikaiseksi ongelmia.

Syvyyssuuntaisessa puolustuksessa on tärkeää, että jo sovelluskehitysvaiheessa huomioidaan tietoturva rakentamalla sovellukseen useampia arkkitehtuurillisia sovellustasoja, jolloin mahdollinen hyökkäys pysähtyy todennäköisemmin johonkin kerrokseen ennen kuin se pääsee suojattavaan kohteeseen eli aineistoon. Arkkitehtuuritasot rakentuvat osaksi muustakin kuin sovelluksen sisäisistä tasoista. Arkkitehtuuritasoina voidaan laskea myös fyysiset eri konetasot eli esimerkiksi sovellus voidaan jakaa www-palvelimelle, sovelluspalvelimelle sekä tietokantapalvelimelle, jolloin on rakennettu jo kolme eri tasoa. Kun nämä kolme eri tasoa eriytetään eri verkkosegmenteille ja laitetaan palomuurit väliin, niin hakkerin pitää päästä jo kolmesta palomuurista ennen kuin hän pääsee itse suojattavaan kohteeseen eli aineistoon.

Tietoturvapoikkeamien asianmukaisessa käsittelyssä päättäjien on huomioitava, että palvelusopimuksissa (SLA) on huomioitu se miten toimitaan pilvipalvelun toimittajan kanssa tietoturvapoikkeamatapauksessa. Tietoturvapoikkeamalla tarkoitetaan sellaisia tapahtumia tai epäiltyä tapahtumaa, joka vaikuttaa heikentävästi kokonaisturvallisuuteen. Tietoturvapoikkeamat voivat liittyä johonkin yksittäiseen turvallisuuden ulottuvuuteen, tai useampaan samanaikaisesti. Tietoturvatapahtumia ovat esimerkiksi:

- Tietomurto
- Tunkeutuminen järjestelmään tai tilaan
- Järjestelmän tai muun resurssin väärinkäyttö
- Haittaohjelmat
- Luottamuksellisten tietojen ”utelu” (sosiaalinen hakkerointi)
- jne.

Päättäjän tulee huomioida, että turvallisuuspoikkeamien ilmoittamiseen ja käsittelyyn tulee olla dokumentoitu ohje, joka on helposti kaikkien asianosaisten saatavilla.

Tarkasteltaessa taulukon 5 viittä eri tietoturvauhkaa tämän tutkimuksen kontekstissa, niin voidaan todeta, että suurimmat uhkat vältetään jo sillä, että kyseessä on viranomaisten oma sisäinen verkko, johon ei ulkopuolisilla ole pääsyä. Uhkataulukon kohta 1 eli aineistoluokitusten huomioiminen on viranomaistoiminnassa lähes selkeää, sillä voidaan olettaa, että viranomaiset ovat tietoisia, minkä luokituksen tietoja he käsittelevät, toiseksi suurin osa viranomaisista on turvallisuusselvitettyjä, jolloin he saavatkin nähdä luottamuksellisia tietoja.

Taulukon kohta 2 eli jaettu teknologia, voidaan todeta, että VIRVE -verkosta tarjottuja pilvipalveluita käyttävät vain viranomaiset eikä palveluja tarjota yleiseen Internettiin. Kun palveluita käyttävät vain viranomaiset, niin voidaan perustellusti sopia ja järjestää niin, että kaikki sovellukset, jotka tulevat pilvipalveluihin, niin käyvät läpi tietynlaisen tietoturva katselmoinnin, jolloin tietoturvaltaan vaarallisia sovelluksia ei kovin helposti pääse palveluihin.

Taulukon kohta 3 voidaan helposti hoitaa niin, että Suomen Erillisverkot Oy huolehtii pilvipalveluiden tarjoamisesta SaaS -palvelumallin mukaisesti, jolloin itse viranomaisille ei jää kuin sovellustason oikeudet. Tällöin viranomaisten pitää vain huolehtia siitä, että sovelluksen käyttäjille ei anneta liian suuria oikeuksia. Suomen Erillisverkot Oy:n tehtäväksi jää huolehtia siitä, että kenelläkään ylläpitäjällä ei ole liian suuria oikeuksia. Omien työntekijöiden aiheuttamilta uhilta voidaan suojautua, kun järjestetään käyttöoikeudet tehtävien mukaisesti ja tarvittaessa esim.irtisanomistilanteessa poistetaan kaikki käyttöoikeudet välittömästi (VAHTI 3/2010, 2010). Vaarallisten työyhdistelmien muodostuminen tulee estää (VAHTI 3/2010, 2010). Vaarallisessa työyhdistelmässä henkilö itse sekä suorittaa että hyväksyy tekemänsä suoritteen (VAHTI 3/2010, 2010).

Taulukon kohta 4 eli syvyyssuuntainen puolustus, tämä kohta pitää ottaa huomioon, kun rakennetaan sovellusarkkitehtuuria, että sovellus jaetaan tiettyihin osiin, jotka voidaan erikseen suojata. Tämä tutkimus esittelee palvelukeskeisen arkkitehtuurin (SOA), joka edesauttaa sovelluksen osittamista. Tässä tutkimuksessa ei oteta tarkempaa kantaa tekniseen arkkitehtuuriin, jossa käsiteltäisiin esimerkiksi pilvipalvelujen eri osien asettelemista eri verkkosegmentteihin ja näiden verkkosegmenttien suojaamista esimerkiksi palomuurien avulla, mutta SOA arkkitehtuurista syntyy yksittäisiä palveluita, joita voidaan suojata yksittäin. Syvyyssuuntainen puolustus tuokin sovellusarkkitehtuurin lisäksi haasteita teknisen arkkitehtuurin suunnitteluun.

Taulukon kohta 5 eli tietoturvapoikkeamien asianmukainen käsittely. Tämä voidaan hoitaa siten, että eri VIRVE -verkossa olevien viranomaisten kesken perustetaan nykyisen organisaation lisäksi niin sanottu tietoturvaorganisaatio, joka käsittelee VIRVE -verkossa

tapahtuneet tietoturvapoikkeamat. Koska Suomen Erillisverkot Oy toimisi VIRVE -verkossa pilvipalvelujen toimittajana, niin heidän vastuullaan olisi tietoturvapoikkeamien käsittelyyn tarkoitetun ohjeen ylläpito sekä huolehtiminen siitä, että kyseinen ohje on kaikkien saatavilla.

5 Keskustelua

Tässä tutkimuksessa oli tarkoituksena selvittää miten pelastustoimintaa voitaisiin parantaa katvealueella sekä pilvipalvelujen avulla. Tutkimus antaa hyvin pintapuolisen, mutta selkeän käsityksen pilvipalveluista sekä eri pilvipalvelumalleista. Pilvipalveluista tarkastellaan tarkemmin yleisiä vastuujakoja eri palvelumalleissa. Vastuujaot on hyvinkin tärkeä tieto päättäjille siinä vaiheessa, kun mietitään siirtymistä pilvipalveluihin, jotta osataan tehdä oikeat tietoturvasuunnitelmat. Kun vastuut ovat selvillä, osataan tietoturvasuunnitelmassa vaatia pilvipalvelun toimittajalta oikeita asioita (SLA) sekä tiedetään mistä itse joudutaan vastaamaan. Kirjallisuus selvitys näiltä alueilta on hyvin kapea, mutta näin yleisellä tasolla riittävä. Syventämällä kirjallisuus selvitystä sekä hankkimalla omakohtaista kokemusta olisi voitu syventää tietoutta pilvipalveluista.

Tutkimuksessa on pilvipalvelujen lisäksi selvitetty Suomen lakeja, säädöksiä sekä ohjeita, jotka vaikuttavat viranomaisten toimintaan tässä tutkimuksessa esitetyssä kokonaisarkkitehtuurissa. Tämän tutkimuksen yhteydessä ei kuitenkaan ole kahlattu läpi kaikkia mahdollisia vaikuttamia lakeja, säädöksiä sekä ohjeita, vaan on keskitytty niihin, joiden on oletettu vaikuttavan lopputulokseen. Tutkimus ei siis anna täyttä kuvaa Suomen lakiviidakosta, joista päättävän viranomaisen tulee olla tietoinen. Näiden lakien, säädösten ja ohjeiden on tarkoitus antaa lukijalle käsitys siitä, kuinka viranomaisille tehtäviä tietoteknisiä ratkaisuja valtio rajoittaa, säätää sekä valvoo. Jotta saataisiin täysi käsitys siitä mitkä lait, säädökset sekä ohjeet vaikuttavat tämän tutkimuksen kontekstissa, niin sitä varten pitäisi tehdä toinen tutkimus, joka voisi olla hyvinkin mielenkiintoinen tehtävä.

Lopputuloksena rakennettiin kokonaisarkkitehtuuri malli, joka on hyvin pieni osa kokonaisratkaisua. Verkkoteknisiä asioita käydään pintapuolisesti läpi, jotta lukija ymmärtää millaiseen verkkoratkaisuun kokonaisarkkitehtuuri on suunniteltu ja ymmärtää siinä olevat haasteet. Tästä tutkimuksesta voitaisiin jatkaa toisella tutkimuksella, jossa selvitettäisiin tarkemmin verkkoteknisiä kysymyksiä esimerkiksi miten VIRVE -puhelimia voitaisiin hyödyntää VIRVE -verkon kuuluvuuden parantamiseksi. TETRA -standardihan esittelee mahdollisuuden, että puhelimet voisivat muodostaa keskenään verkon ilman VIRVE -verkkoa eli toimia DMO (Direct Mode Operation) -moodissa. Tämän avulla päästäisiin siihen, että VIRVE -verkon ulkopuolellakin oleva laite pääsisi VIRVE -verkkoon käyttämällä toista laitetta siltana. Eli tässä tutkimuksessa esitetty WLAN -yhteys ei välttämättä ole ainoa mahdollinen tapa laajentaa VIRVE -verkon kuuluvuutta kohteessa. DSiP -ratkaisua on käsitelty hyvin pitapuolisesti, joten pelkästään hälytysajoneuvon ja VIRVE runkoveron välisestä liikenteestä voisi tehdä oman tutkimuksen.

Kokonaisarkkitehtuurissa esitetty hajautusratkaisu on hajautuksen kannalta hyvä idea ja toimiva, mutta se ei ratkaise kuin pienen osan ongelmista, joita syntyy, kun yritetään asentaa paikalliseksi sovellusta, jota ei alunperin ole sellaiseksi tarkoitettu. Yleensä monitasoarkkitehtuurin mukaisesti rakennetuissa sovelluksissa on eriytetty käyttöliittymmätaso, liiketoimintalogiikkataso sekä itse tiedon persistointitaso. Tässä tutkimuksessa esitetty hajautusratkaisu tuo helpotusta ainoastaan tiedon peristointitasolle, mutta aika useasti sovelluksella on liittymiä myös käyttöliittymätasolla sekä liiketoimintalogiikkatasolla. Kun mietitään tällaisen sovelluksen asentamista paikalliseksi, niin silloin tulee myös selvittää sen tarvitsemat liittymät. Tätä tutkimusta voitaisiin myös jatkaa siten, että selvitettäisiin millaisia liittymiä nykyisissä sovelluksissa on ja tutkittaisiin voitaisiinko nämä sovellukset saada toimimaan oikeasti ilman verkkoyhteyksiä. Tässä tutkimuksessa esitetty hajautusratkaisu kuitenkin ratkoo tärkeimmät eli tiedon saatavuuden ja eheyden ongelmat.

Katvealue ongelmaan tutkimuksessa löydettiin hyviä ratkaisuvaihtoehtoja. Yksi hyvä keksintö oli hajautusratkaisu, jonka avulla voidaan helposti muuttaa nykyiset järjestelmät toimimaan tietokantantoiminnalisuuden osalta paikallisesti. Tämä hajautusratkaisu ei kuitenkaan muuta sellaisia ohjelmia toimimaan täysin paikallisesti, joilla on integraatioita muihin järjestelmiin, joita ei ole asennettu paikallisesti samaan paikkaan. Hajautusratkaisun lisäksi katvealue ongelmaan esitetään ratkaisuksi muita verkkoyhteyksiä ja on käsitelty miten niitä voitaisiin turvallisesti hyödyntää. Näitä muita verkkoratkaisuja voisi tutkia myös tarkemmin esimerkiksi miten niiden saatavuudet sekä kapasiteetit vaikuttavat niiden hyödyntämiseen sekä soveltuvatko ne pelastustoimintaan.

Liitteessä 2 ”Cloud Computing with SOA Approach as Part of the Disaster Recovery and Response in Finland” olen verrannut tämän tutkimuksen tuloksia Saksalaisen SPRIDER (Security System for Public Institutions in Disastrous Emergency scenaRios) projektissa esitettyyn SOA pohjaiseen ratkaisuun. Tuloksena oli, että molemmat tutkimukset ovat lähteneet samoista ongelmista eli puutteelisesta tiedonvälityksestä pelastustoimintaan osallituvien viranomaisten välillä. SPIDER –projektissa oli lähdetty hakemaan ratkaisua SOA arkkiitehtuurista sekä yksi projektin tärkeistä tehtävistä oli kehittää standardi viranomaisten välillä tapahtuvaan viestiliikenteeseen. Projektissa kehittiin Protection and Rescue Markup Language (PRML) –malli, jonka projektin mukaan pitäisi vastata pelastustoiminnan nykyisiin ja tuleviin haasteisiin tiedonvälityksessä. PRML –mallia voidaan myös hyödyntää pilvipalvelujen puolella. PRML:stä on myös se hyöty, että eri sovellusvalmistajilla on helpompi luoda uusia sovelluksia pelastustoiminnan tarpeisiin, kun järjestelmien välinen tietoliikenne on standardoitu. Tutkimuksen tuloksena oli myös, että SOA ja pilvipalvelujen käyttö eivät poissulje toisiaan, vaan päinvastoin ne täydentävät toisiaan. SPIDER –projektin kehittelemää järjestelmien järjestelmää (engl. a System of Systems) mallin upottamista pilvipalveluihin voisi tutkia vielä

tarkemin uudella tutkimuksella. System of Systems –malli perustuu web service –tekniikkaan. Palvelun kutsujan ja palvelujen käyttäjän välinen liikenne turvataan WS-Securityn avulla. SPIDER –projektissa verkkoyhteytenä on käytetty TETRA –verkkoa, mutta ratkaisu ei ole sidottu niihin vaan voidaan myös hyödyntää muitakin tietoliikenne ratkaisuja.

6 Yhteenveto

Suomen pelastustoiminnassa tänä päivänä on ongelmana tiedonsiirto viranomaisten kesken sekä Suomessa olevat katvealueet. Kun kansalainen havaitsee esimerkiksi tulipalon, niin hän ilmoittaa siitä hälytyskeskukselle. Hälytyskeskus hälyttää tarvittavat yksiköt vasteohjeiden mukaisesti. Tässä vaiheessa palolaitos saa hälytyksen ja palomestari alkaa selvittämään manuaalisesti kirjastaan kohteen tarkempia tietoja. Kohteeseen päästyään pelastusyksikkö alkaa tiedottamaan muita yksiköitä sekä hälytyskeskusta tilanteesta.

Yllä olevan lyhyen tilannekuvauksestakin jo huomataan, että toiminnassa on kehitettävää. Miten toimintaa sitten voitaisiin kehittää? On kysymys, johon tällä tutkimuksella on haettu vastausta. Pilvipalvelut on yksi kehitysmahdollisuus parantaa tietojen saatavuutta niin viranomaisten kesken kuin yksikö sisälläkin.

Pilvimalleja on neljä: yksityinen (engl. private), julkinen (engl. public), yhteisöllinen (engl. community) ja hybridi (engl. Hybrid). Yksityinen pilvimalli on yrityksen sisälle rakennettu pilvipalvelu, josta yritys tarjoaa palveluita organisaation sisällä. Yhteisöllinen pilvimalli on eri ryhmien tai yhteisöjen jakama sekä omistama pilvi. Julkista pilvimallia tarjoaa kolmasosapuoli, josta yritykset voivat ostaa erilaisia pilvipalveluja. Hybridi pilvimalli on näiden kahden edellä kuvatun pilvimallin sekoitus, jossa yritys voi organisaation sisäisen eli yksityisen pilven lisäksi ostaa pilvipalvelua julkisesta pilvestä ja kun näissä kahdessa pilvimallissa olevat sovellukset keskustelevat keskenään, niin silloin syntyy hybridi pilvi. Pilvipalveluina yleensä tarjotaan konekapasiteettia eli infrastruktuuria, käyttöjärjestelmä/sovelluspalvelin kapasiteettiä sekä sovelluskapasiteettia. Eri pilvimalleissa voidaan tarjota edellä mainittuja pilvipalveluja. Pilvimalli kertookin sen kuinka laajalle pilvi on näkyvissä. Eri pilvipalvelumalleissa vastuujako ostajana ja pilvipalveluntarjoajan välillä muuttuu. Suurin vastuu ostajalla on IaaS -palvelumallissa ja pienin vastuu SaaS -palveluissa. IaaS -palveluissa asiakas ostaa rautatason palveluita, jolloin hän vastaa kaikesta sen päälle rakennetusta. SaaS -palveluissa ostetaan sovelluksen käyttökapasiteettia, jolloin ostajalla on vain rajattu käyttöoikeus ja rajattu hallinnointioikeus, jolloin suurin vastuu tietoturvasta jää pilvipalvelun tarjoajalle.

Tämän tutkimuksen pohjalta viisi tärkeintä tietoturvauhkaa, joita päättäjien pitäisi pohtia ovat: 1. Aineistoluokitukset, 2. Jaettu teknologia, 3. Vähäisempien oikeuksien periaate 4. Syvyyssuuntainen puolustus ja 5. Tietoturvapoikkeamien asianmukainen käsittely. Aineistoluokituksissa päättäjien pitää ottaa huomioon millaista aineistoa järjestelmässä tullaan käyttämään. Aineiston tietoturvaluokitukset vaikuttavat suojaustasoihin sekä siihen voidaanko edes pilvipalveluja edes käyttää. Jaetussa teknologiassa päättäjän pitää huomioida, että

pilvipalveluissa on myös muita käyttäjiä, jolloin tietoturvauhkat eivät tule vain suoraan omasta järjestelmästä vaan tietoturvauhan voi aiheuttaa toisessa järjestelmässä oleva tietoturva-aukko. Vähäisempien oikeuksien periaatteessa päättäjien tulee huolehtia siitä, että ei tule ns. vaarallista yhdistelmää, jossa yhdellä käyttäjällä on liian suuret oikeudet. Vaarallinen yhdistelmä tulee silloin, kun käyttäjä voi esimerkiksi luoda käyttäjätunnuksen ja antaa sille oikeuksia sekä tehdä muutoksia järjestelmään ja tämän jälkeen poistaa käyttäjätunnus, jolloin ei jää jälkiä muutoksesta. Syvyyssuuntaisessa puolustuksessa päättäjien tulee huolehtia siitä, että järjestelmässä on useita arkkitehtuurillisia kerroksia, jolloin saadaan paras turva siihen olennaisimpaan eli aineistoon. Tietoturvapoikkeamien asianmukaisessa käsittelyssä päättäjien tulee huolehtia siitä, että on olemassa tietoturvaohjeistus, jossa otetaan kantaa siihen miten tietoturvapoikkeamissa toimitaan sekä muihin tietoturvaan liittyviin asioihin.

Jotta ymmärtää tässä tutkimuksessa esitetyn mallin eli kokonaisarkkitehtuurin, niin pitää ymmärtää mitä pilvipalvelut ova sekä mitä tietoturvauhkat niihin vaikuttaa. Kokonaisarkkitehtuurissa on lähdetty siitä, että Suomen Erillisverkot Oy VIRVE -runkoverkon ylläpitäjänä voisi toimia pilvipalvelujen tarjoajana ja tarjoaisi VIRVE -verkon sisäisiä julkisia pilvipalveluita. Pilvipavelut tarjottaisiin SaaS -mallin mukaisesti, jolloin se edesauttaisi viranomaisten välistä tiedon siirtoa, kun he käyttäisivät samaa ohjelmistoa, josta he maksaisivat vain käyttöoikeusmaksua. Näin saataisiin parannettua viestinvaihtoa viranomaisten kesken, mutta tämä ei vielä ratkaise katvealue ongelmaa.

Katvealueen ongelmaa ratkaistaan tässä tutkimuksessa esitetyssä kokonaisarkkitehtuurissa hälytysajoneuvojen välisellä langattomalla (WLAN) ratkaisulla. Tässä mallissa jokin paikalla olevista hälytysajoneuvoista perustaisi paikallisen WLAN -verkon, johon muut hälytysajoneuvot liittysivät. WLAN -verkon perustajan tulisi olla jonkin muun tietoliikenneyhteyden kuuluvuusalueella, jotta muut, jotka ovat katvealueella pääsisivät tämän yhden solmun kautta verkkoon. Katvealueen pienentämiseksi esitellään myös DSiP -monikanavareitittimen hyödyntämistä, jolloin VIRVE -verkon sijasta voitaisiin hyödyntää myös muita verkkoja, kuten esimerkiksi 3G, UMTS, LAN, WLAN ja Sateliitti verkkoja. Mikäli kuitenkin oltaisiin alueella, josta ei verkkoa saada rakennettua tai sen aikaan saaminen vain vie liian kauan aikaa, niin tässä kokonaisarkkitehtuurissa esitellään myös ratkaisu siihen miten hälytysajoneuvossa sovellukset voivat toimia paikallisesti. Tässä mallissa on vain rajoituksena se, että siinä otetaan huomioon vain tietokantayhteydet eli mikäli sovellus tarvitsee muita yhteyksiä kuin tietokantayhteydet, niin tarvittavat sovellukset pitää olla myös paikallisesti asennettuna hälytysajoneuvoon. Tässä

tutkimuksessa esitetyn hajautusratkaisun avulla eri hälytysajoneuvot voivat paikallisesti ylläpitää käytännössä samaa sovellusta. Hajautusratkaisu huolehtii siitä, että kaikissa sen solmukohdissa eli halytysajoneuvoissa olevilla sovelluksilla on samat tiedot käytettävissä.

Kuvat

Taulukot

Liitteet

Lähdeluettelo

Anderson J. Chris, Jan Lehnardt and Noah Slater, 2010, CouchDB: The Definitive Guide Time to Relax, 1st Edition. O'Reilly Media, January 2010.

Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito, 2010. Security and Cloud Computing: InterCloud Identity Management Infrastructure. Dept. of Mathematics, Faculty of Engineering, University of Messina.

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030, haettu 5.12.2011 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Badger Lee, Grance Tim, Patt-Corner Robert, Voas Jeff, 2011, Cloud Computing Synopsis and Recommendations, National Institute of Standards and Technology Special Publication 800-146 Natl. Inst. Stand. Technol. Spec. Publ. 800-146, 84 pages (May 2011)

Benson Yrjö, 2010. Valtion ICT 2010-2013, Valtiovarainministeriö, IT-johtaja Benson Yrjö, 2.6.2010, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20100503JulkIT/04_Benson_ValtIT_R024.pdf, viitattu 2.12.2011

Brooks Jason, 2011, Does NoSQL Matter to Your Company?, EWeek September 19, 2011

Cattell Rick, 2010, Relational Databases, Object Databases, Key-Value Stores, Document Stores, and Extensible Record Stores: A Comparison, December 2010.

Cerri Davide, Emanuele Della Valle, David De Francisco Marcos, Fausto Giunchiglia, Dalit Naor, Lyndon Nixon, Kia Teymourian, Philipp Obermeier, Dietrich Rebholz-Schuhmann, Reto Krummenacher, ja Elena Simperl, 2008. Towards Knowledge in the Cloud, 8/2008. published on SEMELS'08: International Workshop on Semantic Extensions to Middleware: Enabling Large Scale Knowledge Applications; Part of OTM Conferences (COOPIS), Mexico, November 2008.

CSA, 2011, Cloud Security Alliance, Top Threats to Cloud Computing V1.0, Prepared by the Cloud Security Alliance March 2010

Gerard Briscoe ja Alexandros Marinos, 2009, Community cloud computing, arXiv:0907.2485v3 [cs.NI] 12 Oct 2009

George Reese, 2009. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O´Reilly Media 2009. ISBN: 978-0-596-15636-7.

Harrison Guy, 2011, Big Data and Emerging NoSQL Databases Shift to Hybrid Database Environments. http://www.idgconnect.com/blog-abstract/265/guy-harrison-global-big-data-emerging-nosql-databases-shift-hybrid-database-environments, viitattu 17.11.2011.

Hevner, A. et al 2004. Design Science in Information Systems Research. MIS Quarterly Vol. 28 No. 1, pp. 75-105.

Henkilötietolaki 22.4.1999/523. (1999). Haettu 4.12.2011 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Holtström John, Rajamäki Jyri ja Hult Taina, 2011. The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel-Communication. INTERNATIONAL JOURNAL OF COMMUNICATIONS Issue 3, Volume 5, 2011.

Hurwitz Judith, Bloor Robin, Kaufman Marcia ja Halper Fern, 2009. Service Oriented Architecture for Dummies 2nd edition. Wiley Publishing, Inc. ISBN: 978-0-470-37684-3

IBM, 2002. IBM DB2 Universal Database -ohjelma versio 8, Sanasto

JulkICT, 2011. Kokonaisarkkitehtuuri, JulkICT -toiminto, Valtiovarainministeriö, syyskuu 2011. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/Kokonaisarkkitehtuuri.pdf, viitattu 01.12.2011.s

Julkisuuslaki 621/1999, Laki viranomaisten toiminnan julkisuudesta 621/1999, haettu 5.12.2011 osoitteesta http://www.finlex.fi/fi/laki/alkup/1999/19990621

Junttila Kari ja Rantama Markku, 2011. Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa ”PELTI”. Pelastusopisto, T&K Palvelut, 2011

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Opinpajan kirja. Tampereen yliopis-topaino Oy Juvenes-Print, Tampere.

Järvinen, Petteri, 2010. Yksityisyys: Turvaa digitaalinen kotirauhasi. Jyväskylä: WSOYpro

KATAKRI, 2009. Kansallinen turvallisuusauditointikriteeristö, Sisäisen turvallisuuden ohjelman toisen vaiheen toimenpide 6.4. tp 2. Puolustusministeriö. 20.11.2009. ISBN: 978-951-25-2078-7 (pdf). Haettu 5.12.2011 osoitteesta http://www.defmin.fi/files/1525/Katakri.pdf

Lehto Jouni, Jyri Rajamäki ja Paresh Rathod, 2012. Conceptualised View on Can Cloud Computing Improve the Rescue Service in Finland? (Liite 1)

Mickos Jan, 2008. Tietojärjestelmien palvelukeskeinen kehittäminen. Puolustusvoimien Johtamisjärjestelmäkeskus Sarja 1 Nro 1/2008, Edita Prima Oy, Helsinki 2008. ISBN 978-951-25-1910-1.

Nordman Mikael, Lehtonen Matti, Holmström John, Ramstedt Kenneth ja Hämälainen Pekka, 2003, A TCP/IP BASED COMMUNICATION ARCHITECTURE FOR DISTRIBUTION NETWORK OPERATION AND CONTROL, 17th International Conference on Electricity Distribution Barcelona, 12-15 May 2003

Oracle, 2010. An Oracle White Paper in Enterprise Architecture, Achieving the Cloud Computing Vision, October 2010.

Oza N.,Karppinen K. ja Savola R. 2010, User experience and security in the cloud - an empirical study in the finnish cloud consortium. Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, sivut 621 {628, 2010. doi: 10.1109/CloudCom.2010.114.

OWASP, 2010, The Open Web Application Security Project, http://www.owasp.org, viitattu 17.11.2011

Panda Debu, 2005. Web Services Architecture, http://onjava.com/onjava/2005/05/25/j2ee-services.html, viitattu 18.11.2011

Pavan Kumat Chitumalla, Douglas Harris, Bhavani Thuraisingham ja Latifur Khan, 2008, Emergency Response Applications, Dynamic Plume Modeling and Real-Time Routing, 1089-801/08/$25.00©2008 IEEE

Pelastuslaki (2003). Pelastuslaki 2003/ 438. Haettu 5.12.2011 osoitteesta http://www.finlex.fi/fi/laki/alkup/2003/20030468

Perdue Tim, 2010. 5 Things You Need To Know About NoSQL. http://newtech.about.com/b/2010/11/30/5-things-you-need-to-know-about-nosql.htm, viitattu 14.11.2011

Rajamäki Jyri, 2010. MOBI Mobile Object Bus Interaction, Laurea

Rosenberg Jothy, David L. Remy, 2004. Securing web services with WS-security : demystifying WS-security, WS-policy, SAML, XML signature and XML encryption. ISBN 0-672-32651-5

Salvatore T. March & Gerald F. Smith. Design and Science Reseach on Information Technology. Decision Support Systems, vol 15, no 4 (1995), s 251–266.

Santasalo Matti, Ikenna Ikeqwuono, Yasin Lossini, 2010. Services for fire & rescue personel, Laurea U.A.S Leppävaara. 13.12.2010.

Suomen Erillisverkot Oy, 2011, Verkkosivut http://www.erillisverkot.fi/suomen_erillisverkot_oy/yritys/, viitattu 12.12.2011.

Suomen perustuslaki 11.6.1999/731. (1999). Haettu 4.12.2011 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Syrjänen, Pentti. (2006). Yksityisyyden suoja ja henkilöarviointi. Acta Universitatis Tamperensis 1155. Väitöskirja. Tampereen yliopisto. Haettu 4.12.2011 osoitteesta http://acta.uta.fi/pdf/951-44-6646-2.pdf

Syrjänen, Pentti. (2008). Luotettava henkilöarviointi ja yksityisyyden suoja. Helsinki: Talentum

Takabi H., J.B.D. Joshi ja Gail-Joon Ahn. 2010. Securecloud: Towards a comprehensive security framework for cloud computing environments. Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual, sivut 393-398, 2010. doi: 10.1109/COMPSACW.2010.74.

Takabi H., J.B.D. Joshi ja Gail-Joon Ahn. 2010. Security and Privacy Challenges in Cloud Computing Environments. COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 1540-7993/10/$26.00 © 2010 IEEE, NOVEMBER/DECEMBER 2010

Tietosuojadirektiivi 95/46/EY. (1995). Virallinen lehti nro L 281 , 23/11/1995. Haettu 4.12.2011 osoitteesta http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FI:HTML

Urpila Tatu, 2011, Pelastusyksikön ajoneuvon teknisten järjestelmien ja laitteiden käyttäjätarpeet sopimuspalokunnissa, Opinnäytetyö Laurea Leppävaara, 11/2011.

VAHTI 5/2004, 2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Valtiovarainministeriö. ISBN 951-804-468-6 (PDF), haettu 5.12.2011 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20041201Valtio/01_VAHTI_5_2004.pdf

VAHTI 2/2010, 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Valtiovarainministeriö. ISBN 978-952-251-124-9 (PDF). Haettu 5.12.2011 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf

VAHTI 3/2010, 2010. Sisäverkko-ohje. Valtiovarainministeriö. ISBN 978-952-251-139-3 (PDF). Haettu 5.12.2011 osoitteesta http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/Sisaeverkko-ohje.pdf

Valtiovarainministeriö/TUVE-yksikkö, 2011. Hallinnon turvallisuusverkko TUVE. Valtiovarainministeriö, 4/2011.

Viestintävirasto, 2007, VPN, http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html, viitattu 1.12.2011

Winter Robert, Fischer Ronny, 2007. Essential Layers, Artifacts, and Dependencies of Enterprise Architecture, Journal of Enterprise Architecture - May 2007

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.

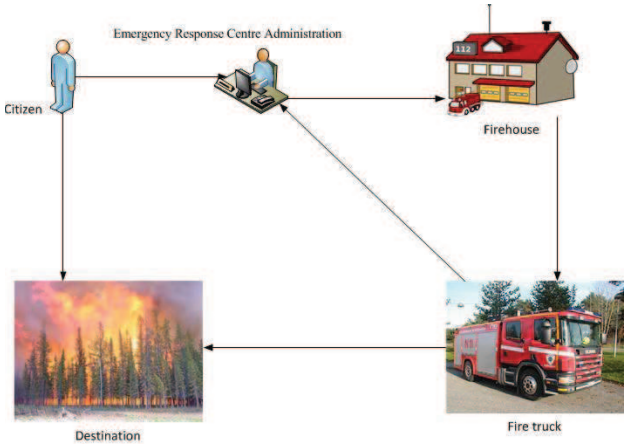


Fig. 1 Usual rescue scenario and process

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.

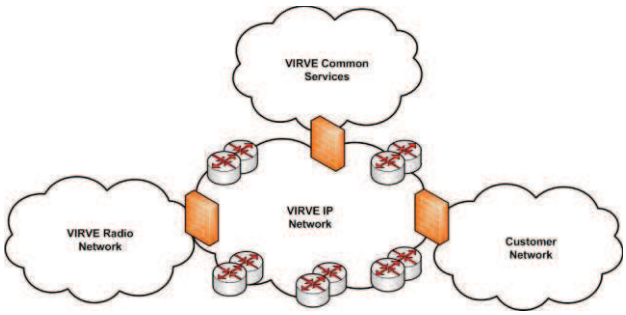


Fig. 2 High-level current VIRVE IP Network

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

(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].

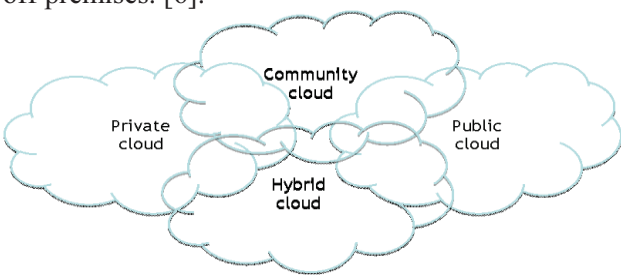


Fig. 3 Cloud computing deployment models

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.

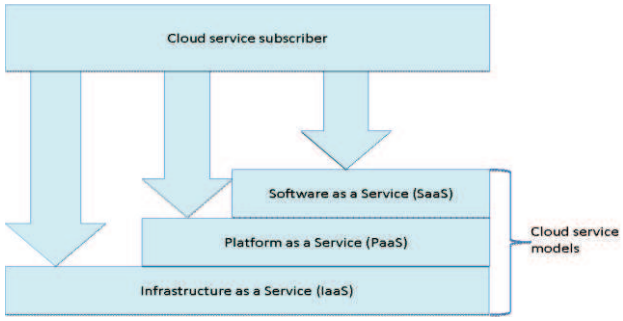


Fig. 4 Cloud service models

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

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.

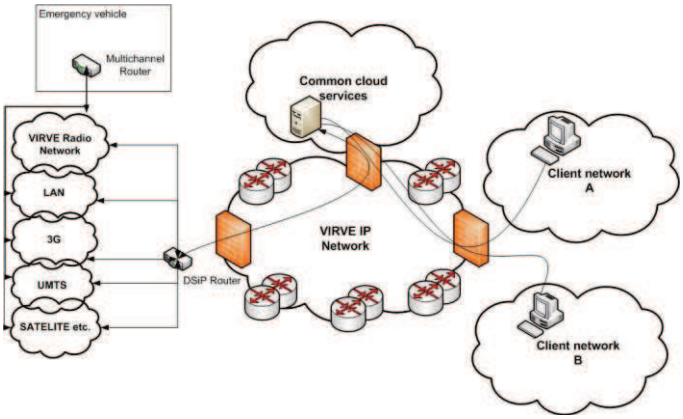


Fig. 5 Cloud computing inside VIRVE IP Network

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

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.

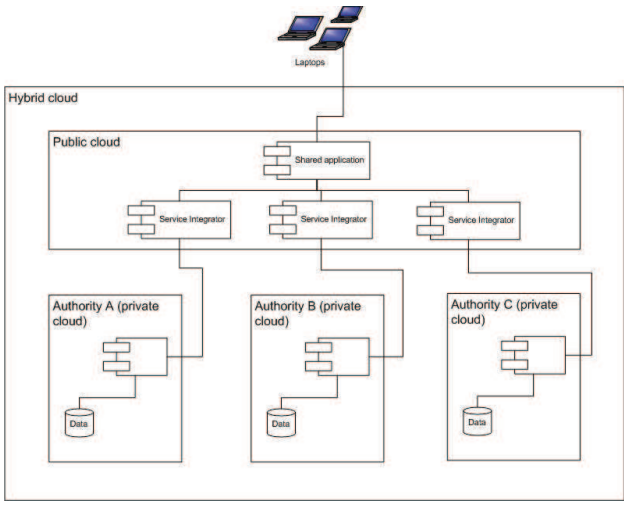


Fig. 6 The Hybrid cloud model with service oriented approach

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.

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

Cloud Computing with SOA Approach as Part of the Disaster Recovery and Response in Finland

Jouni Lehto, Jyri Rajamäki and Paresh Rathod

***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 combined with Service-Oriented Architecture (SOA) might be the answer for this problem. There are several solutions and guidelines available. This research paper explores which cloud computing deployment model and cloud service model could be suitable to address the problem along with Service-oriented approach. Further study also conducted on cloud services provided by the Public Authority Network (VIRVE) in Finland. The Cloud approach is compared to a System of Systems approach of SPIDER (Security System for Public Institutions in Disastrous Emergency scenaRios) project. The SPIDER project emphasises on enabling interoperable information sharing between public institutions for efficient disaster recovery and response. The paper presents conceptual view on usability of cloud and service-oriented computing in the disaster recovery and response services in Finland.**

***Keywords*— Cloud computing, Service-oriented architecture, Public authority network, Public safety communications, VIRVE, SPIDER.**

I. 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.

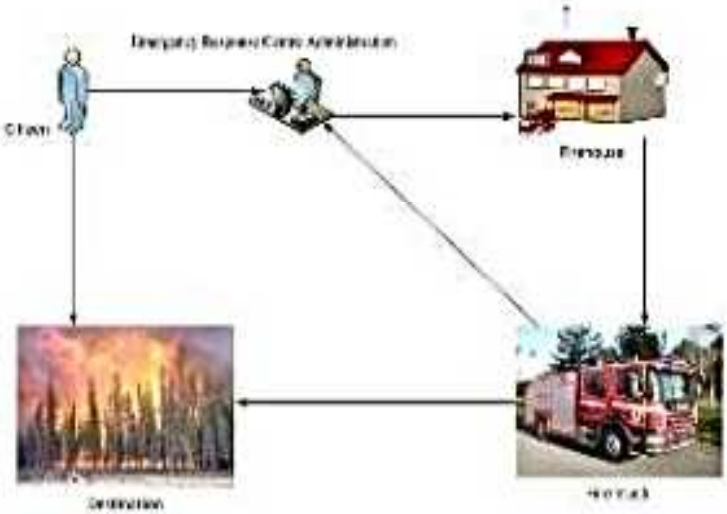


Fig. 1 Usual rescue scenario and process

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.

J. Lehto is post-graduate student at Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: lehto.jouni@gmail.com)

J. Rajamäki and P. Rathod are with the Laurea SID Leppävaara, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland. (e-mail: jyri.rajamaki@laurea.fi, paresh.rathod@laurea.fi).

The paper is structured as followed: In Section II, an overview of state-of-the-art for communication networks and data exchange between authorities in rescue process. In Section III, the problem is formulated; followed by problem solution in Section IV. Further, it compared to a System of Systems approach of SPIDER project in Section V. Finally, the conclusion derived in Section VI.

II. State-of-the-Arts

A. 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.

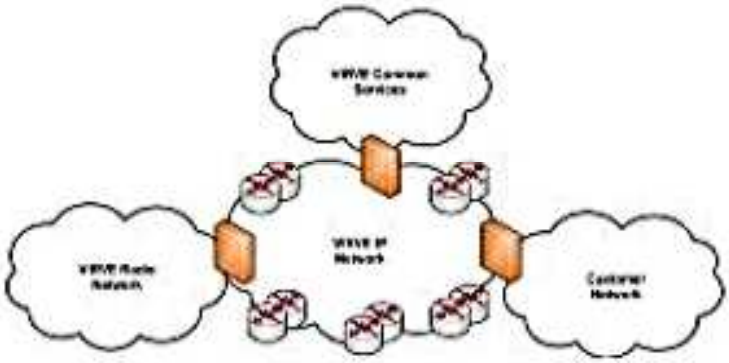


Fig. 2 High-level current VIRVE IP Network

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 [16].

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 I 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 around 100 kbit/s [17].

B. 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 a single organization comprising multiple consumers (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].

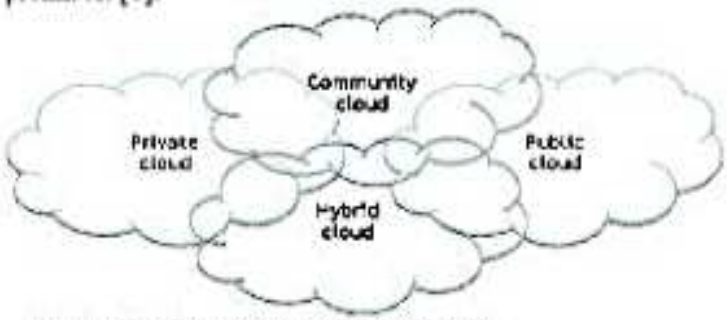


Fig. 3 Cloud computing deployment models

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.

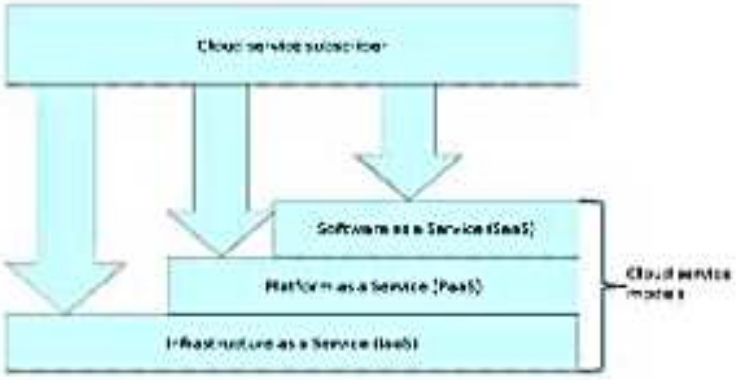


Fig. 4 Cloud service models

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.

C. *Service-Oriented Architecture (SOA)*

SOA is an architectural paradigm of which main characteristics are to promote loose coupling, reusability and interoperability during the designing an 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.

Fig. 5 SOA Architecture [10]

As shown in Fig. 5, there are three key components which are necessary to build a SOA services. Service provider can build a SOA service, but if the service is not published anywhere then no-one can use it because of invisibility of those services. That is why the service provider has to publish it in Discovery Agency. The Service requester will find

necessary service descriptions from Discovery Agency. With this description, the client can make the connection to the right service provider by adhering communication agreement and is able to use the SOA service.

Web services though not quite new have witnessed a remarkably wide acceptance in the industry as extremely vital means of implementing SOA. This acceptance is owing to the fact that, Web services are able to provide a distributed computing style which makes it possible to integrate heterogeneous applications across the Web. The Web services specifications are such that they are totally independent of any programming language, hardware and operating system, thereby enhancing loose coupling and interoperability between service requesters and providers hence fulfilling the loose coupling principle of SOA. [9]

III. Problem Formulation

The Rescue Service in Finland has a significant problem of communication with the other 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 [11].

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.

IV. 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. 6 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.

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.

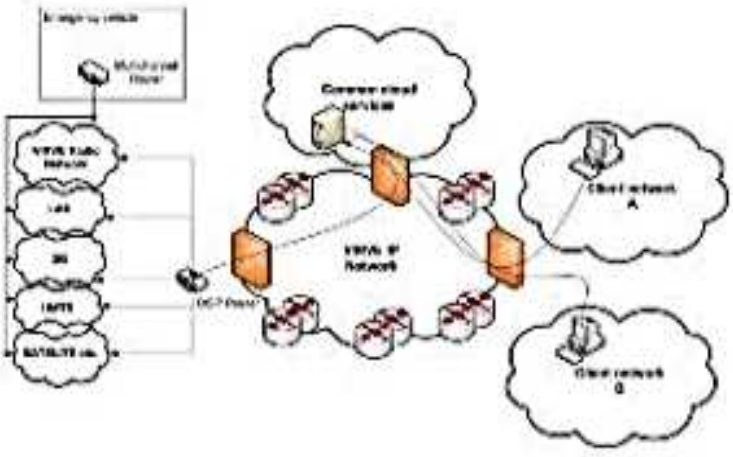


Fig. 6 Cloud computing inside VIRVE IP Network

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 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. 7 presents this model combination.

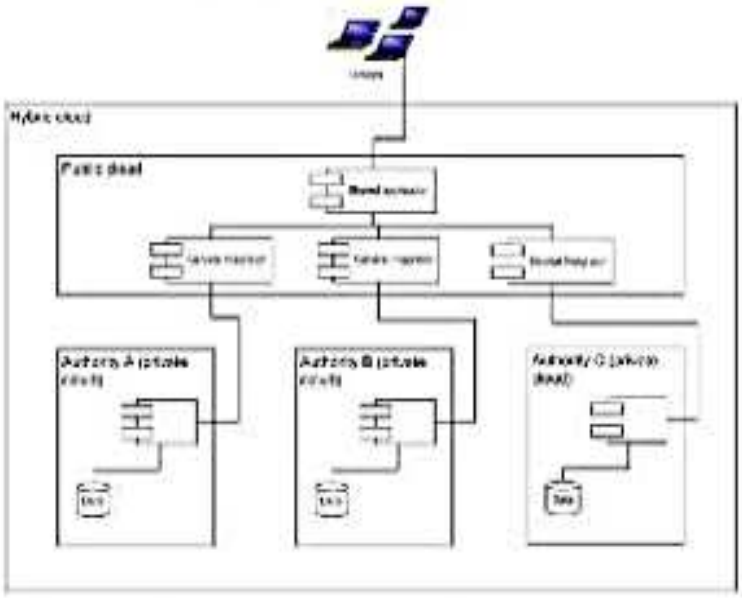


Fig. 7 The Hybrid cloud model with service oriented approach

SecureCloud [12] 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) [13] 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.

DSiP provides secure way to use different networks seamlessly, but there is also Inter-System Interface (ISI) over Satellite [14]. With ISI-based TETRA over Satellite, it is possible to use two different TETRA networks when there is no such terrestrial infrastructure existing. This is particularly usable in accidents which are near the border, and the rescue teams are from two different countries and they use their own TETRA networks.

As mentioned earlier the capacity of the TETRA network is very low and if this is the only network available at the site of an accident, somehow the capacity should be increased. Using Performance Enhancing Proxies (PEPs), it is possible to improve the performance of the TETRA network or any other networks per say.

In general, Performance Enhancing Proxies (PEPs) are designed to improve the end-to-end performance of

communication protocols by breaking the end-to-end connection into multiple connections. For example, this allows TCP to overcome the low window size problem when connections involve satellite links (RFC 3135). The end-systems are not aware of proxies and can run smoothly and without any significant change. There are many types of PEPs. PEP can either split the connection by pretending to be the opposite endpoint or interfere with the transmitted messages, also known as protocol spoofing. Further, PEPs can be either on both ends of the satellite link that cause the performance degradation or just at one end, which is far less common. [14]

V. Cloud Approach vs. Spider Approach

The project SPIDER (Security System for Public Institutions in Disastrous Emergency scenaRios) is part of the national research initiative Scenario based Civil Security Research and substantially funded by the German government [15].

The project SPIDER in nutshell: The project addresses same problem as this very research. Interoperability is supposed to be the key feature for managing disaster and crisis in the civil sector. The lack of continuous command structure and the resulting use of incompatible ICT systems inhibit the effective collaboration of all involved agencies and organizations [15]. The problem where they tried to find a solution seems to be same as well. All authorities who participating to the rescue process do not have the way to communicate and share necessary data with each other, even they are willing to. The project SPIDER has studied service-oriented approach and addressed said problem. The project provides SOA based solution to improve the rescue processes and services

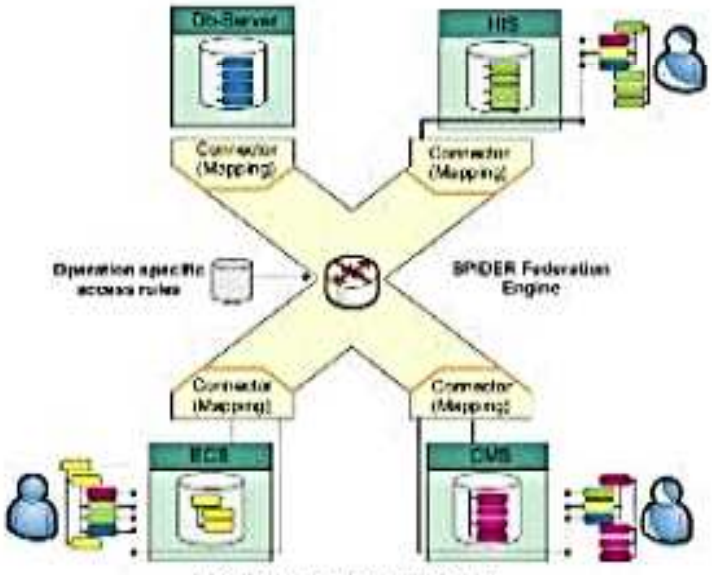


Fig. 8 Seamless Connection of Systems through SPIDER System [15]

To address above mentioned problems, SPIDER project has developed a System of Systems. It describes way for a better interoperability of information sharing between public institutions as well as private companies [15]. A System of Systems allows every organization to use their own existing software to access and work with the organization-specific data and seamless connection to the data in other organization network, as shown in Fig. 8. The cloud computing approach is almost similar. In Cloud approach, the organizations can maintain the organization-specific data through cloud services, and they can restrict the access to the sensitive data in private cloud. In System of Systems, it can continue to use the existing software. However, in cloud approach the idea is every organization will use the same software provided through hybrid cloud by cloud service provider. The cloud approach is broadly cost effective than the System of Systems, but demanding more changes in infrastructure. This way it might be more difficult to get in place.

The SPIDER project was not intended to develop a middleware for emergency communications; instead they aimed to develop a loose coupling among systems and standardization across various interfaces. Cloud approach has not taken clear stance on a loose coupling among systems or a share middleware used by the authorities and provided from public cloud. A System of Systems is based on web services, and two major components are Agents and Entities. The Agents describe a set of mandatory and optional services [15]. The Entities are information provider in the system, which is effectively a set of Agents and the corresponding human actors [15]. The connection between the Agents is secured with WS-I Security Basic Profile, and has to be installed for all the Agents. The WS-I Security Basic Profile is based on the certificates and uses for encrypting the communications. Therefore, there has to be a trustworthy Certificate Authority (CA) who is able to serve all involved organizations. In Cloud approach, they have not taken stance on how the connection between organizations realized and secured. Cloud approach could adopt similar approach as in a System of Systems approach; especially in the Service Integrator introduced earlier in this paper.

The SPIDER project's main focus was the development of a new Protection and Rescue Markup Language (PRML) as a common data model for the interaction of concerned components [15]. The PRML is supposed to meet current and future requirements concerning the information needs of rescue and emergency forces [15]. It guarantees sustainable interoperability of the systems by offering an extensible data format for communication purposes [15]. In Cloud approach, the PRML could be used in communication between the organizations' private and the public cloud services. This way the vendors of emergency information systems are able to build interconnections into their products and services.

In the SPIDER project, they relied on the TETRA network communication, but at the same time they are well aware of the lack of available data rate in TETRA. The System of Systems

also allows usage of the other networks. In addition, TETRA network is also one of the possible ways to enable communication in the Cloud approach. The DSiP enables the other networks to use secure communication with VPN protection and this could be also implemented in the System of System approach.

VI. Conclusion

The cloud computing deployment can enhance the communication between Finnish authorities. It could be also answer to reduce the ICT costs of the Finnish government. Selecting right cloud model also provides secure data communication and flexibilities

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

The VIRVE Radio Network is under constant improvement process and yet not ready 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 provision of cloud services even today. If authorities implement cloud services, it would reduce the ICT costs of the Finnish government; mainly because of service centralization. The centralization 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 application together, lot of time and resources are needed especially solving all the challenges of the integration. The same concept can mean different things for different organizations. These differences came from individual use of the applications by the authorities over the years. This concept problem can be solved using service-oriented architecture (SOA) like System of Systems approach in SPIDER project. In that case, every authority can have own service inventory and services can be composed as required; that also helps avoiding actual data conversion. The conversion take place at the integration level and reduces further complexities and problems.

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, Issue 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://cloudsecurityalliance.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] J. Rajamaki, T. Hult and P. Ofem, "ICT Integration of Public Protection and Disaster Relief: Services for Fire and Rescue Personnel", International Journal of Computers and Communications, Issue 3, Volume 5, 2011, pp. 119-132, ISSN: 2074-1294.

[10] M. Champion, C. Ferris & E. Newcomer et al (2002). Web Service Architecture. W3C Working Draft 2002 Available: http://www.w3.org/TR/2002/WD-ws-arch-20021114/

[11] Y. Benson, "Valtion ICT 2010-2013", Valtiovarainministerio, 2010, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20100503JulkIT/04_Benson_ValtIT_R024.pdf

[12] 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.

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

[14] R. Novak, "Viability of ISI-Based TETRA over Satellite", WSEAS Transactions on Communications, Issue 7, Volume 7, July 2008, pp. 765-775, ISSN:1109-2742

[15] S. Šubik, S. Rhode, T. Weber and C. Wietfield, "SPIDER: Enabling Interoperable Information Sharing between Public Institutions for Efficient Disaster Recovery and Response", Technologies for Homeland Security (HST), 2010 IEEE International Conference, pp. 190-196, ISBN: 978-1-4244-6047-2

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

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