Saku Temonen

PILVITALLENNUKSEN KÄYTTÖ JA HAASTEET – YRITYKSEN NÄKÖKULMA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Temonen, Saku
Pilvitallennuksen käyttö ja haasteet – yrityksen näkökulma
Jyväskylä: Jyväskylän yliopisto, 2016, 24 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Ojala, Arto

Pilvitallennus on monien yritysten kannalta houkutteleva vaihtoehto perinteisiin tiedon tallennusmedioihin verrattuna. Pilvitallennuksen tarjoama skaalautuvuus, kustannustehokkuus ja helppokäyttöisyys ovat keskeisiä pilvitallennuksen käyttöön liittyviä etuja. Pilvitallennuksen tietoturvaongelmat ovat kuitenkin esteenä pilvitallennuksen käyttöönottoon, eivätkä pilvipalveluntarjoajat voi varmuudella taata asiakkailleen datan luottamuksellisuuden, eheyden ja saatavuuden säilymistä pilvitallennusta käytettäessä.

Tutkielmassa käsitellään pilvitallennukseen liittyviä hyötyjä, käyttötarkoituksia sekä haasteita kirjallisuuskatsauksen keinoin. Saadut tulokset pohjautuvat pilvitallennusta ja pilvipalveluita käsitteleviin tieteellisesti luotettaviin artikkeleihin ja konferenssijulkaisuihin. Tutkielman tuloksena saadaan laajempi ymmärrys pilvitallennukseen liittyvistä eduista ja haasteista. Tämä ymmärrys on hyödyllistä sekä yritysten ja pilvipalveluntarjoajien kannalta, sillä sen avulla voidaan kehittää palveluiden laatua, pyrkiä ratkaisemaan ongelmia ja arvioida, onko pilvitallennuksen hyödyntäminen kannattavaa.

Asiasanat: pilvipalvelu, pilvitallennus, tietoturva

ABSTRACT

Temonen, Saku
Usage and challenges of cloud storage – business perspective
Jyväskylä: University of Jyväskylä, 2016, 24 p.
Information Systems, Bachelor's Thesis
Supervisor(s): Ojala, Arto

Cloud storage is a tempting option for many businesses in comparison to more traditional forms of storage. The scalability, cost effectiveness and ease-of-use of cloud storage are essential benefits related to usage of cloud storage. Information security problems of cloud storage can be an obstacle to adoption of cloud storage and cloud service providers can't guarantee the confidentiality, integrity and availability of their customer's data when cloud storage is used.

This thesis addresses the benefits, uses and challenges related to cloud storage by means of literature review. The results are based on scientifically trustworthy articles and conference publications. As a result of the thesis, a broader understanding of the benefits and challenges related to cloud storage is gained. This understanding is beneficial to both businesses and cloud service providers, as it can be used to improve the quality of the services, solve problems and evaluate whether or not using cloud storage is beneficial.

Keywords: cloud storage, cloud computing, information security

KUVIOT

SISÄLLYS

1 JOHDANTO

Pilvipalvelut ovat viimeisen vuosikymmenen taitteen jälkeen suurta mielenkiintoa niin yritysten kuin tiedeyhteisön keskuudessa herättänyt informaatioteknologinen toimintamalli, jossa tietoteknisiä resursseja myydään asiakkaille palveluna. Laitehankintojen sijaan yritykset ja yksityiset henkilöt voivat vuokrata tietoteknisiä resursseja, kuten laskentatehoa sekä tallennustilaa. (Armbrust ym., 2010.) Informaatioteknologia-alan tutkimus- ja konsultointiyritys Gartner (2010) nimesi pilvipalvelut tärkeimmäksi strategiseksi teknologiaksi yritysten kannalta vuodelle 2011.

Pilvitallennus on pilvipalvelu, jossa asiakkaalle tarjottu resurssi on tallennustila palveluntarjoajan omistamissa laitteissa esimerkiksi datakeskuksissa (Slamanig & Hanser, 2012). Tällöin tallennustilaa vuokraava taho voi hyötyä pilvipalveluihin liittyvistä eduista, kuten kustannustehokkuudesta, skaalautuvuudesta sekä toteutuksen helppoudesta (Wu, Ping, Ge, Wang & Fu, 2010). Houkuttelevista hyödyistä huolimatta pilvipalveluihin ja siten pilvitallennukseen liittyvät tietoturvaongelmat nähdään suurena haasteena pilvipalveluiden käytön suhteen (Zissis & Lekkas, 2012).

Tutkielman tavoitteena on kirjallisuuskatsauksen keinoin tutkia pilvitallennuksen hyötyjä ja käyttötarkoituksia sekä haasteita yritysten kannalta. Tutkimuskysymykset ovat *miten yritykset hyödyntävät pilvitallennusta?* ja *mitä haasteita pilvitallennukseen liittyy yritysten näkökulmasta?* Ensimmäisellä tutkimuskysymyksellä halutaan saada selville, millä tavalla yritykset hyödyntävät pilvitallennusta liiketoiminnassaan. Sekä pilvitallennuksen mahdolliset käyttötavat että siitä saatavat hyödyt ovat mahdollisia vastauksia ensimmäiseen tutkimuskysymykseen. Toisen tutkimuskysymyksen tarkoitus on avata pilvitallennuksen käyttöön liittyviä haasteita yritysten kannalta. Tällä tarkoitetaan pilvitallennuksen käytöstä aiheutuvia riskejä ja ongelmatilanteita.

Tutkimus rajataan yrityksiin, sillä yksityishenkilöiden ja yritysten pilvitallennukseen liittyvät käyttötavat, hyödyt ja haasteet ovat liian erilaisia yrityksiin verrattuna. Samasta syystä rajauksen ulkopuolelle jätetään pienet yritykset, koska pienten yritysten pilvitallennuksen käyttö voi olla hyvinkin rajallista ja siihen liittyvät haasteet voivat poiketa suuresti muista yrityksistä. Tutkimuksen

näkökulma pilvitallennukseen on monella tavoin käytännönläheinen, joten pilvitallennusta ei käsitellä kovinkaan syvällisesti teknologisesta näkökulmasta. Toisaalta pilvitallennukseen liittyvään taloudelliseen puoleen ei perehdytä perinpohjaisesti, vaikka sitä saatetaan sivuta.

Pilvitallennuksen tarkempi tutkimus ja siihen liittyvien hyötyjen, käyttötarkoitusten ja haasteiden ymmärrys on tärkeää niin yritysten kuin palveluntarjoajien kannalta. Haasteet on tunnettava, jotta niihin osataan kehittää ratkaisuja. Tieteellinen kirjallisuus ei ole juurikaan keskittynyt nimenomaan pilvitallennukseen, vaan usein hyötyjä ja käyttötarkoituksia on tarkasteltu pelkästään pilvipalveluiden näkökulmasta ilman erillistä kohdennusta pilvitallennukseen.

Kirjallisuuskatsaus pohjautuu pääosin verkosta löytyviin tieteellisiin lähteisiin, joista suurin osa on joko tieteellisiä artikkeleita tai konferenssijulkaisuja. Kaksi tärkeintä lähteiden etsimisen kanavaa olivat Jyväskylän yliopiston kirjaston elektronisten aineistojen PCI-haku sekä bibliografinen tietokanta Scopus. Tieteellisiä lähteitä valittaessa lähteiden tieteellistä luotettavuutta arvioitiin sekä silmämääräisesti että Julkaisufoorumin tieteellisten laatuarvioiden perusteella.

Luvussa 1 avataan pilvipalveluiden konseptia, ominaispiirteitä sekä siihen liittyviä palvelu- ja käyttöönottomalleja. Ensimmäisen pääluvun tavoitteena on auttaa ymmärtämään pilvipalveluiden konseptia, jotta voidaan ymmärtää myöhemmissä kappaleissa käsiteltävää pilvitallennusta paremmin. Toisessa pääluvussa käsitellään pilvitallennuksen määritelmä, sekä siihen liittyviä hyötyjä ja käyttötarkoituksia. Kolmannessa luvussa puolestaan tutkitaan pilvitallennukseen liittyviä haasteita, jotka pääasiassa liittyvät tietoturvaan.

2 PILVIPALVELUT

Pilvi tietoteknisenä käsitteenä on rinnastettavissa pilveen meteorologisena terminä. Ilmakehässä esiintyvän, vesipisaroista koostuvan pilven tavoin tietotekninen pilvi koostuu useista erillisistä osista, jotka yhdessä muodostavat asiakkaan näkökulmasta yhtenäisen kokonaisuuden. Näitä osia ovat esimerkiksi datakeskuksissa sijaitsevat tietokonelaitteistot sekä niihin liittyvät ohjelmistot. (Armbrust ym., 2010.)

Suomen Viestintäviraston (2014) määritelmän mukaan pilvipalveluilla viitataan pilvessä olevien tietoteknisten resurssien tarjoamiseen asiakkaalle palvelun muodossa verkon välityksellä. Tarjotut tietotekniset resurssit voivat olla esimerkiksi laskentatehoa, tallennustilaa tai sovellusohjelmia (Mell & Grance, 2010). Pilvipalveluihin liittyy tyypillisesti myös liiketoimintamalli, jossa asiakas maksaa käyttämistään resursseista käyttöasteen mukaan (Gong, Liu, Zhang, Chen & Gong, 2010).

Tämän pääluvun alaluvuissa esiteltävät pilvipalveluiden ominaispiirteet, palvelu- ja käyttöönottomallit perustuvat pääosin yhdysvaltalaisen teknologiaa ja standardeja käsittelevän National Institute of Standards and Technologyn (NIST) pilvipalveluiden määritelmään, joka on muodostunut tiedeyhteisön keskuudessa standardimääritelmäksi. NIST:n määritelmän mukaan pilvipalveluihin liittyy viisi ominaispiirrettä, ja pilvipalvelut voidaan jakaa kolmeen palvelumalliin ja neljään jakelumalliin (Mell & Grance, 2010).

2.1 Ominaispiirteet

Mell ja Grance (2010) esittävät, että pilvipalveluille voidaan määritellä viisi keskeistä ominaispiirrettä, joita ovat itsepalvelullisuus, käyttö verkon kautta päätelaitteesta riippumatta, resurssien yhteiskäyttö, nopea elastisuus sekä tarkka ja valvottu resurssien käyttö. Nämä viisi tekijää yhdessä tekevät pilvipalveluista joustavan palvelun, jossa käytetystä laskentatehosta, sovelluksesta, tallennustilasta tai muusta palvelusta maksetaan käytön määrän mukaan (Mell & Grance, 2010).

Pilvipalvelun itsepalvelullisuudella tarkoitetaan asiakkaan kykyä vaikuttaa saatavien tietoteknisten resurssien määrään ilman palveluntarjoajan väliintuloa (Srinivasan, Sarukesi, Rodrigues, Manoj & Revathy, 2012). Käytännössä itsepalvelullisuus tarkoittaa asiakkaan kykyä mukautua tarpeiden mukaan joko laskemalla tai kasvattamalla saatavien resurssien määrää ilman asiakkaan ja palveluntarjoajan välisestä vuorovaikutuksesta aiheutuvaa viivettä.

Kyky käyttää pilvipalveluita verkon välityksellä esimerkiksi selaimella riippumatta käytössä olevasta päätelaitteesta on yksi pilvipalveluiden tunnuspiirteistä (Mell & Grance, 2010). Tämän ansiosta pilvipalveluita voidaan hyödyntää myös etänä tai muilla laitteilla kuin pöytätietokoneilla, kuten kannettavilla tietokoneilla ja mobiililaitteilla. (Zhang, Cheng & Boutaba, 2010.)

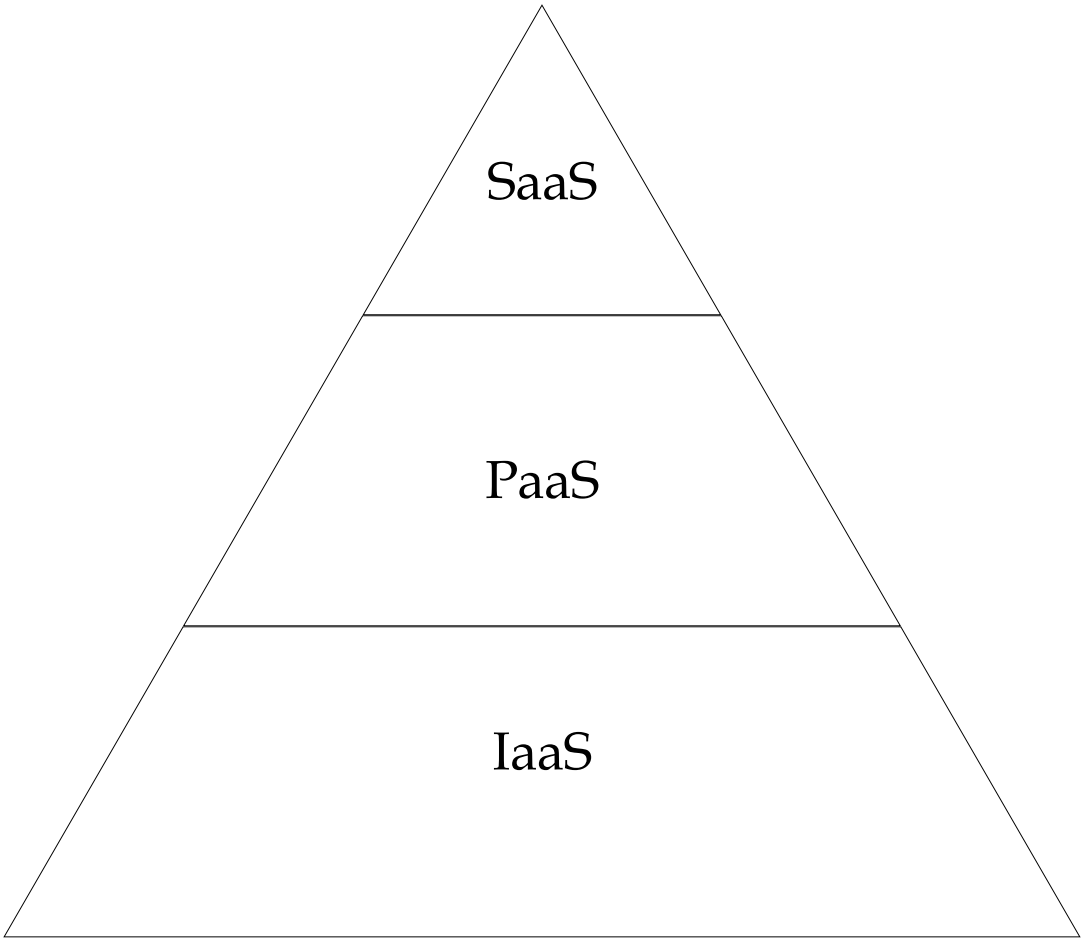
Resurssien yhteiskäyttö viittaa siihen, että palveluntarjoajan tarjoamat tietotekniset resurssit ovat useiden käyttäjien käytettävissä samanaikaisesti, mukautuen dynaamisesti asiakkaiden tarpeiden mukaisesti. Yhteiskäytön seurauksena asiakas ei voi täsmällisesti tietää käytössä oleviin resursseihin liittyvän fyysisen laitteiston maantieteellistä sijaintia. (Mell & Grance, 2010.)

Elastisuudella tarkoitetaan pilvipalveluista puhuttaessa asiakkaan kykyä kasvattaa tai vähentää saatavien resurssien määrää tarpeen mukaan ilman katkoja palvelun toiminnallisuudessa (Agrawal, El Abbadi, Das & Elmore, 2011). Elastisuuden ollessa nopeaa resurssien säännöstely on reaaliaikaista. Nopean elastisuuden ja itsepalvelullisuuden toteutuessa asiakkaan näkökulmasta pilvipalvelut tarjoavat käytännössä rajattoman määrän resursseja. (Armbrust ym., 2010.)

Resurssien tarkka ja valvottu käyttö ovat käytännössä edellytyksiä käyttöasteeseen pohjautuvalle liiketoimintamallille sekä resurssien määrän automaattiselle muokkaamiselle. Toisaalta resurssien käytön mittaaminen tekee pilvipalvelusta itsestään läpinäkyvää sekä asiakkaan että palveluntarjoajan kannalta. (Mell & Grance, 2010.)

2.2 Palvelumallit

Tyypillisesti pilvipalveluiden palvelumallit jaotellaan kolmeen luokkaan, jotka ovat Software as a Service (SaaS) eli ohjelmisto palveluna, Platform as a Service (PaaS) eli alusta palveluna ja Infrastructure as a Service (IaaS) eli infrastruktuuri palveluna. (Mell & Grance, 2010.) Tätä kuviossa 1 havainnollistettua kolmiportaista mallia kutsutaan myös SPI-malliksi (Hashizume, Rosado, Fernández-Medina & Fernandez, 2013).



KUVIO 1 Palvelumallien kolmiportainen SPI-malli

Palvelumalleista pintapuolisin SaaS tarjoaa asiakkaalle selaimen välityksellä toimivan ohjelmiston, josta maksetaan kertamaksun sijaan jatkuvasti esimerkiksi kuukausimaksuilla. Palveluntarjoaja on vastuussa kaikesta SaaS-ohjelmaan liittyvästä toiminnallisuudesta ja sen alaisesta pilvi-infrastruktuurista, jolloin asiakkaan ei tarvitse huolehtia esimerkiksi ohjelman tai laitteiston ylläpidosta lainkaan. (Mell & Grance, 2010; Godse & Mulik, 2009.) Eräs esimerkki SaaS-palveluista on Googlen verkon välityksellä tarjoama toimisto-ohjelmisto Google Docs (Srinivasan ym., 2012).

PaaS-palvelumallissa asiakas saa käyttöönsä verkon välityksellä toimivan sovellusalustan, jossa asiakas voi kehittää, testata, käyttöönottaa ja ylläpitää omia ohjelmistojaan. SaaS-palvelumallin tavoin asiakas ei kuitenkaan voi vaikuttaa sovellusalustan alaiseen infrastruktuuriin. (Mell & Grance, 2010; Viega,

2009.) Googlen tarjoama sovellusalusta Google App Engine on tyypillinen esimerkki PaaS-palvelusta (Srinivasan ym., 2012).

Kolmiportaisen SPI-mallin monipuolisimmassa IaaS-palvelumallissa asiakas pääsee vaikuttamaan pilvi-infrastruktuuriin säätämällä käytettävissä olevien resurssien, kuten tallennustilan tai prosessointitehon määrään, samalla maksaen palvelusta käytettyjen resurssien määrän mukaisesti. Tällöin asiakas voi säästää kuluissa resurssien käytön määrän ollessa huipputasoa alhaisempi verrattuna oman laitteiston ylläpitoon (Mell & Grance, 2010; Viega, 2009). Amazonin EC2 on eräs esimerkki IaaS-palvelusta (Dillon, Wu & Chang, 2010).

Yleisesti tiedeyhteisön keskuudessa hyväksytty SPI-malli on kuitenkin saanut osakseen myös kritiikkiä. Kächele, Spann, Hauck ja Domaschka (2013) kritisoivat tätä kolmiportaista mallia siitä, kuinka IaaS ja PaaS kattavat niin useita erityyppisiä palveluita, ettei tällainen luokittelu ole riittävää. Tiedeyhteisön keskuudessa on kuitenkin myös käytetty palvelumallien alaluokkia, joista eräs esimerkki on tallennustila palveluna eli Storage as a Service (StaaS), jonka voidaan katsoa olevan IaaS-palvelumallin alaluokka (Brunette & Mogull, 2009).

2.3 Käyttöönottomallit

Pilvipalveluiden käyttöönottomallit kuvaavat, kuka pilvipalvelun tarjoaa ja kenelle se on suunnattu. Mell & Grance (2012) määrittelevät neljäksi käyttöönottomalliksi julkisen, yksityisen, yhteisö- ja hybridipilven.

Julkinen pilvi on yleisin pilvipalvelun käyttöönottomalli, jossa palveluntarjoaja tarjoaa omistamansa pilven suuren yleisön käyttöön (Srinivasan ym., 2012). Tällöin palveluntarjoaja voi myös itse päättää pilvipalvelun mahdollisesta hinnasta ja sen käyttöön liittyvistä säännöistä. Aikaisemmin mainitut Amazon EC2 ja Google App Engine ovat esimerkkejä julkisessa pilvessä toteutetuista pilvipalveluista. (Dillon ym., 2010.)

Yksityinen pilvi on yksittäisen yrityksen käyttöön tarkoitettu pilvi, joka voi olla joko yrityksen itsensä tai ulkopuolisen toimijan hallinnoima (Srinivasan ym., 2012). Yksityisen pilven tarkoituksena on saavuttaa pilvipalveluista saatavat teknologiset edut ilman julkiseen pilveen liittyviä turvallisuusriskejä. (Dillon ym., 2010.)

Yhteisöpilvestä puhuttaessa kyse on usean organisaation yhdessä ylläpitämästä ja käyttämästä pilvestä, jonka käytössä vallitsee organisaatioiden yhteinen arvomaailma ja säännöt (Mell & Grance, 2010). Yhteisöpilveä käyttävät organisaatiot luovat yhdessä skaalautuvan pilven sekä siihen liittyvän hallinnollisen tasapainon. (Dillon ym., 2010.)

Hybridipilvi puolestaan on kahden tai useamman edellä mainitun käyttöönottomallin yhdistelmä, jossa erityyppiset pilvet toimivat rinnakkain erillisinä kokonaisuuksina (Mell & Grance, 2010). Tällöin dataa ja ohjelmistoja voidaan siirtää pilvestä toiseen. Yleisin hybridipilven käytön syy lienee tarve saavuttaa yksityisen pilven tuomat edut samalla ylläpitäen toista käyttöönottomallin pilveä. (Dillon ym., 2010.)

3 PILVITALLENNUKSEN KÄYTTÖ

Pilvitallennus on eräs pilvipalvelun alalaji, jossa yksinkertaisimmillaan asiakas saa käyttöönsä palveluntarjoajan tarjoamaa informaation tallennustilaa etänä internetin välityksellä. Muina pilvitallennuksen ominaisuuksia voivat olla muun muassa varmuuskopiointi, tiedon jakaminen sekä tiedon synkronointi. (Slamanig & Hanser, 2012.) Pilvitallennukseen liittyvät piirteet ja arkkitehtuuri on kuitenkin hankala määritellä täsmällisesti (Wu ym., 2010). Pilvitallennuksen voidaan katsoa olevan SPI-mallin IaaS-palvelumallin alainen luokka, johon viitataan joskus myös nimikkeellä StaaS (Storage as a Service) eli tallennustila palveluna (Brunette & Mogull, 2009). Pilvitallennuksen on ennustettu olevan keskeisin tiedon tallennusmuoto yritysten keskuudessa (Slamanig & Hanser, 2012).

Tämän pääluvun on tarkoitus tarkastella, miten ja miksi yritykset hyödyntävät pilvitallennusta. Tämä tarkoittaa sekä mahdollisia pilvitallennuksen käyttötarkoituksia sekä pilvitallennuksen käytöllä tavoiteltavia hyötyjä. Ensimmäisessä alaluvussa esitellään pilvitallennukseen liittyviä positiivisia ominaisuuksia, ja toisessa nostetaan esiin pilvitallennuksen hyödyntäminen varotoimenpiteenä.

3.1 Hyödyt ja ominaisuudet

Monet pilvitallennukseen liittyvät hyödyt ovat suoraan johdettavissa pilvipalveluihin liittyvistä ominaispiirteistä, mutta osa liittyy myös pilvitallennuksen ja perinteisen tiedon tallentamisen eroihin. Keskeisiä pilvitallennuksen tarjoamia hyötyjä ovat muun muassa joustavuus, saatavuus verkon välityksellä, helppous sekä taloudelliset hyödyt.

3.1.1 Elastisuus

Ehkä yksinkertaisin pilvipalveluihin ja siten myös pilvitallennukseen liittyvä hyöty on skaalautuvuus sekä pilvipalveluiden ominaispiirteeksikin määritelty nopea elastisuus (Mell & Grance, 2010). Skaalautuvuus tarkoittaa kykyä mu-

kauttaa käsiteltävien resurssien määrää. Elastisuus puolestaan viittaa samaan resurssien määrän kasvattamiseen tai laskemiseen, mutta dynaamisessa mielessä. Nopeasti elastinen järjestelmä voi mukauttaa resurssien määrää ilman katkoja palvelussa. (Agrawal ym., 2011.) Pilvipalveluiden ansiosta elastisuus on myös pienten ja keskisuurten yritysten saavutettavissa. Ilman pilvipalveluita, käytettävien tietoteknisten resurssien määrän muokkaaminen oli pitkä, kuukausia ellei jopa vuosia kestävä prosessi. (Owens, 2010.) Elastisuuden ansiosta käytettävien resurssien määrä on asiakkaan näkökulmasta käytännössä rajaton (Armbrust ym., 2010). Samalla resurssien käyttö on kustannustehokasta, sillä ainoastaan käytetyistä resursseista maksetaan, eikä ole tarvetta ylläpitää ylimääräistä tallennustilaa kasvuvaraa varten (Wu ym., 2010). Nämä edellä mainitut tekijät tekevät pilvitallennuksesta kilpailukykyisen vaihtoehdon perinteiseen, yrityksen itse ylläpitämään tallennusmediaan verrattuna.

3.1.2 Helppous

Pilvitallennuksen käyttö yrityksen sisällä on myös monin tavoin yksinkertaisempaa yrityksen kannalta kuin omien tallennuslaitteistojen käyttäminen. Pilvitallennusta hyödyntäessä yrityksen ei tarvitse huolehtia laitteistoon liittyvästä huollosta tai päivityksistä, ja pelkkä internet-selain riittää sen käyttöön ja hallintaan (Gupta, Seetharaman & Raj, 2013; Wu ym., 2010). Yksi pilvipalveluiden ominaispiirteistä, käyttö verkon välityksellä, tarjoaa yrityksen työntekijöille mahdollisuuden työskennellä myös etänä, samalla mahdollistaen tallennuksen synkronoinnin yrityksen eri toimipisteiden välillä (Mell & Grance, 2010; Slamanig & Hanser, 2012). Myös pilvitallennuksen käyttöönotto on huomattavasti helpompaa, kuin vastaavan tallennuslaitteiston toteuttaminen perinteisen mallin mukaisesti (Wu ym., 2010). Onnistuneen pilvitallennuksen käyttöönoton ansiosta yritys voi täten keskittyä omaan ydinosaamiseensa, saavuttaen kilpailuetua kilpailijoihin verrattuna (Garrison, Kim & Wakefield, 2012).

3.1.3 Taloudellisuus

Kolmas keskeinen pilvitallennukseen liittyvä etu on taloudelliset hyödyt. Pilvipalvelun ominaispiirteiden, tarkan ja mitatun käytön sekä nopean elastisuuden ansiosta yritys maksaa ainoastaan käyttämistään resursseista eikä ylimääräistä (Mell & Grance, 2010). Pilvitallennusta käytettäessä yrityksen ei tarvitse huolehtia operationaalisista kustannuksista kuten laitteiston ylläpidosta, huollosta tai laitehankinnoista. Tällöin infrastruktuuriin liittyvät taloudelliset riskit, kuten laitteistovioista aiheutuneet kulut, siirtyvät palveluntarjoajan vastuulle (Zhang ym., 2010). Toisaalta pilvipalveluille tyypillisen skaalautuvuuden ja saatavuuden saavuttaminen tallennuksessa olisi käytännössä mahdotonta suurimmalle osalle yrityksistä ilman pilvitallennusta. (Wu ym., 2010.) Kynnys aloittaa pilvitallennuksen käyttö on myös huomattavasti matalampi kuin perinteisen tallennusmedian kanssa, mikä on erityisen tärkeää esimerkiksi pienyritysten kannalta (Gupta ym., 2013).

3.2 Varmuuskopiointi

Pilvitallennuksen käyttö keskeisimpänä yrityksen tallennuskanavana ei ole ainoa pilvitallennuksen käyttötarkoitus, vaan sitä voidaan käyttää myös keinona varautua vastoinkäymisiin. Yrityksen keskeisen informaation varmuuskopiointi ei ole pilvipalvelun tuoma uusi konsepti, vaan on ollut osa yritysten kykyä varautua ja elpyä ongelmatilanteista jo pitkään (Wu ym., 2010). Varmuuskopioinnin ulkoistamisen voidaan nähdä olevan yritysten kannalta houkutteleva vaihtoehtona sen kustannustehokkuuden ja yksinkertaisen toteutuksen ansiosta. Useimmat pilvitallennuksen varmuuskopiontipalvelut toimivat sekä asiakkaan että palveluntarjoajan laitteisiin integroidun ohjelmiston avulla. (Vrable, Savage & Voelker, 2009.) Ulkoistamalla varmuuskopioinnin pilvipalveluntarjoajalle yritys säästyy myös tallennusmedian hankintaan ja ylläpitoon liittyviltä kuluilta (Rahumed, Chen, Tang, Lee & Lui, 2011).

Yritykset voivat hyödyntää pilvitallennuksen tarjoamaa varmuuskopiointia myös katastrofeista elpymisen (engl. *disaster recovery*) välineenä. Katastrofista elpymisellä viitataan yrityksen kykyyn palauttaa informaatioteknologiansa toiminnallisuus nopeasti ja tehokkaasti ongelmatilanteiden yhteydessä. Yrityksen kannalta voi olla tärkeää säilyttää varmuuskopiot muualla kuin yrityksen omissa tiloissa esimerkiksi tulipalon kannalta, mikä puolestaan toteutuu pilveen tehtävässä varmuuskopioinnissa automaattisesti. (Fallara, 2003.) Pilvessä olevat varmuuskopiot soveltuvat hyvin katastrofista elpymiseen, sillä käyttöasteeseen pohjautuvasta hinnasta johtuen synkronoidun varmuuskopion ylläpitäminen ei vaadi paljoa resursseja ennen varsinaista ongelmatilannetta (Wood ym., 2010).

4 PILVITALLENNUKSEN HAASTEET

Vastapainona lukuisiin pilvipalveluihin liittyviin hyötyihin voidaan nostaa huoli pilvipalveluiden tietoturvasta. Monet yritykset näkevät tietoturvan keskeisenä esteenä pilvipalveluiden käyttöönoton suhteen (Grobauer, Walloschek & Stöcker, 2011; Ren, Wang & Wang, 2012; Zissis & Lekkas, 2012). Eräänä syynä suureen tietoturvahaasteiden määrään voidaan nähdä useat eri pilvipalveluihin liittyvät teknologiat, jotka siten tuovat omat heikkoutensa ja riskinsä mukana pilvipalveluiden toimintaan (Hashizume, Rosado, Fernández-Medina & Fernandez, 2013). Toisaalta perinteisten tiedon suojausmenetelmien toimivuus pilviympäristössä on kyseenalaista (Zissis & Lekkas, 2012).

Tietoturvan keskeisenä tehtävänä pilvipalveluiden kontekstissa on turvata tiedon luottamuksellisuus, eheys ja saatavuus. (Kaufman, 2009; Zissis & Lekkas, 2012). Näiden kolmen tekijän voidaan ajatella olevan suojatun pilvitallennusjärjestelmän kolme keskeistä rakennuspalasta. Datan luottamuksellisuus viittaa siihen, että vain valtuutetut käyttäjät ja järjestelmät voivat saada suojatun datan käyttöönsä. Pilviympäristössä luottamuksellisuuden toteutumista vaikeuttaa suuri pilvessä olevien osapuolten, laitteiden ja sovellusten määrä. Datan eheys puolestaan tarkoittaa sitä, että tallennettua dataa voi muokata ainoastaan valtuutetut lähteet. Tällöin ulkopuolisten lähteiden ei pitäisi voida toteuttaa dataan liittyviä operaatioita, kuten muokkausta tai poistoa. Saatavuudella tarkoitetaan sitä, että valtuutetuilla käyttäjillä on kyky saada haltuunsa ja muokata tallennettua dataa. (Zissis & Lekkas, 2012.) Tämä tutkielman pääluku tarkastelee seuraavaksi pilvitallennuksen käyttöön liittyviä haasteita näiden kolmen tietoturvan osa-alueen kautta.

4.1 Luottamuksellisuus ja eheys

Datan luottamuksellisuuden ja eheyden turvaaminen lienee suurin haaste niin pilvipalveluiden kuin pilvitallennuksen saralla. Cloud Security Alliancen (2013) suorittama pilvipalvelualan ammattilaisille suunnattu kyselytutkimus päätyi

tulokseen, että datavuodot ja datan menetys ovat kaksi suurinta pilvipalveluihin liittyvää riskiä. Datavuodolla tarkoitetaan sitä, kun pilveen tallennettu data päätyy jonkun ulkopuolisen nähtäväksi (Cloud Security Alliance, 2013). Tällaiset datavuodot eivät kuitenkaan välttämättä ole tahallisia, vaan voivat olla seurausta pilvitallennukseen liittyvistä toimintamalleista. Laitteistoresurssien yhteiskäytön vuoksi on mahdollista, että yrityksen data sijaitsee samalla laitteella kuin toisen asiakkaan. Tällöin on olemassa riski, että joku ulkopuolinen pääsee tahattomasti käsiin yrityksen arkaluontoiseen dataan. (Srinivasan ym., 2012.)

Toinen datavuodon riskiä aiheuttava tekijä on datan remanenssi, jolla tarkoitetaan poistetusta datasta jäävää jäännöstä, joka voi johtaa datavuotoon (Zissis & Lekkas, 2012). Tällöin avautuu mahdollisuus toteuttaa retrospektiivisiä hyökkäyksiä, joiden tavoitteena on poistetun datan palauttaminen (Rahumed ym., 2011). Eräs tällainen tapa on datan kaivelu, jossa pilvitallennuspalvelun asiakas haalii käyttöönsä suuria määriä tallennustilaa ja pyrkii palauttamaan poistettua, arkaluontoista dataa omaan käyttöönsä (Zissis & Lekkas, 2012). Tämän ehkäisemiseksi tarvittaisiin takaus pilvipalveluntarjoajalta siitä, että tallennettu data voidaan luotettavasti poistaa. Ei ole kuitenkaan varmuutta, voivatko pilvipalveluntarjoajat tarjota vastaavanlaista varmaa tiedon poistoa. (Rahumed ym., 2011.) Tiedon varma poisto on huomattavasti helpompaa perinteistä tallennusmediaa käytettäessä, sillä esimerkiksi käytöstä poistetun kovalevyn voi hävittää, jolloin ulkopuoliset tahot eivät voi päästä poistettuun dataan käsiksi (Grobauer, 2009).

Eräs keino tiedon luottamuksellisuuden turvaamiseen on datan enkryptio ennen sen tallentamista pilveen. Tällöin kuitenkin esimerkiksi tiedon hakeminen tallennetusta datasta hankaloituu. Enkryptio on mahdollista toteuttaa tavalla, jolla datan haettavuus säilyy, mutta sen toteutus pilvitallennuksen etuja menettämättä on hankalaa. (Ren ym., 2012.) On myös huomioimisen arvoista, että kryptograafiset menetelmät yksin eivät riitä turvaamaan tallennetun datan luottamuksellisuutta (Van Djik & Juels, 2010).

Pilvitallennusta käyttäessään yritys ei voi samalla tavalla vaikuttaa tallennettuun dataan kuin käyttäessään omia, fyysisiä tallennuslaitteita. Tällöin yritys ei voi suoranaisesti tietää esimerkiksi tallennetun datan fyysistä sijaintia. (Kandakuri, Paturi & Rakshit, 2009.) Tämän seurauksena yritys itse ei voi valvoa ja ylläpitää datan eheyttä ja luottamuksellisuutta, vaan se jää palveluntarjoajan tehtäväksi (Wang, Wang, Ren & Lou, 2009). Tällöin yrityksen on luotettava siihen, että palveluntarjoaja takaa tallennetun datan luottamuksellisuuden, eheyden ja saatavuuden. (Zissis & Lekkas, 2012). Pilvipalveluihin keskeisesti liittyvän palvelutasosopimuksen voidaan nähdä olevan keskeinen osa tätä osapuolten välistä luottamusta. Palvelutasosopimus on laillisesti sitova palveluntarjoajan ja asiakkaan välinen sopimus, jossa määritellään tarjottuun pilvipalveluun liittyvät ehdot ja velvollisuudet. Oikein toteutettuna palvelutasosopimus tunnistaa ja määrittelee asiakkaan tarpeet, auttaa ymmärtämään palvelun sisältöä, yksinkertaistaa ongelmia, ehkäisee erimielisyyksiä, kannustaa dialogiin osapuolten välillä ongelmatilanteissa sekä ehkäisee epätodenmukaisia odotuksia palvelun suhteen. Tyypillisesti palvelutasosopimukset sisältävät muun muassa

tarjottujen palveluiden ja tietoturvan kuvaukset sekä lupauksen käytettävyysajasta. Palvelutasosopimuksen tulee kuitenkin olla riittävän kattava ollakseen merkityksellinen. (Kandakuri, Paturi & Rakshit, 2009.)

Pilvitallennukseen liittyvät moninaiset teknologiat aiheuttavat omalta osaltaan tietoturvaongelmia. Pilvitallennuspalveluiden pohjautuessa verkon kautta käytettävyyteen sekä verkkoselaimiin, tällöin IP-protokollan sekä selaimen heikkoudet kuten sessioiden kaappaamisen mahdollisuus ovat tekijöitä, joiden vuoksi tallennetun datan tietoturva on vaarassa (Grobauer ym., 2009). Myös useiden päätelaitteiden mahdollisuus avaa uusia tietoturvaongelmia. Mobiililaitteiden käyttö pilvitallennuksessa lisää esimerkiksi mobiilihaittaohjelmien, heikkojen langattomien verkkojen sekä mobiililaitteiden omien käyttöjärjestelmien heikkoudet pilvitallennuksen riskien joukkoon (Hashizume ym. 2013).

Osa yritysten tallentamasta datasta voi olla arkaluontoista muussakin kuin strategisessa mielessä. Esimerkkinä tällaisesta datasta on potilastiedot, joiden tietoturvan taso on usein määritelty laissa. (Srinivasan ym., 2012) Pilvitallennuksen käyttäminen vastaavanlaisen arkaluontoisen datan tallentamiseen on hankalaa, sillä esimerkiksi jotkin eurooppalaiset lait vaativat, että organisaatiot tietävät datan tallennussijainnin, mikä ei välttämättä ole pilvitallennuksen kontekstissa mahdollista (Zissis & Lekkas, 2012). Datan tallennussijainnin ollessa toisessa valtiossa, kyseisen valtion poikkeava lainsäädäntö voi omalta osaltaan hankaloittaa arkaluontoisen datan tallentamista pilveen (Rong, Nguyen & Jaatun, 2013).

Kaikki pilvitallennuksen tietoturvariskit eivät kuitenkaan ole seurausta teknologisista heikkouksista. On kuitenkin muistettava, että ihminen on usein tietoturvan heikoin lenkki. Puutteellinen tietoturvaosaaminen yrityksen työntekijöiden keskuudessa voi johtaa esimerkiksi helposti murrettaviin käyttäjätunnuksiin ja salasanoihin. Toisaalta pilvipalveluiden yhteydessä myös palveluntarjoaja voi tehdä kriittisiä virheitä henkilöstön suhteen, esimerkiksi palkaten henkilökuntaa suorittamatta perusteellista henkilön taustatukimusta. Joillain palveluntarjoajan työntekijöillä, kuten järjestelmävastaavilla voi olla käytännössä rajaton pääsy pilveen tallennettuun dataan. (Hashizume ym., 2013.)

On kuitenkin huomioimisen arvoista, että suuri osa tässä alaluvussa mainituista datan luottamuksellisuuteen ja eheyteen liittyvistä ongelmista ovat seurausta julkisen pilven ominaispiirteistä (Zissis & Lekkas, 2012). Yritys voi siis tarvittaessa välttyä suurelta osalta näistä pilvitallennuksen haasteista käyttämällä tallennukseen esimerkiksi yksityistä pilveä.

4.2 Saatavuus

Pilvipalveluiden käyttämästä, laajan luotettavuuden ja saatavuuden mahdollistavasta arkkitehtuurista huolimatta käyttökatkot palvelussa ovat mahdollisia. Palveluntarjoajan luvatessa palvelutasosopimuksessa 99.999 % käytettävyysaikaa, voi yritys kuitenkin odottaa palvelussa olevan hetkellisiä käyttökatkoja

jopa 8.76 tunnin verran vuosittain. Tämän vuoksi pilvitallennusta hyödyntävän yrityksen tulisi varautua hetkellisiin käyttökatkoihin, jottei yrityksen liiketoiminta esty täysin katkojen ajaksi. (Jansen, 2011.)

Myös pidempiaikaiset tai pysyvät katkot pilvipalvelun toiminnassa ovat mahdollisia esimerkiksi palveluntarjoajan konkurssin tai laitteiden tuhoutumisen yhteydessä. Äärimmäinen esimerkki tällaisesta on pilvitallennuspalvelu Omnidrive, joka lakkautti toimintansa vuonna 2008 varoittamatta käyttäjäkuntaansa. (Jansen, 2011.)

Pilvipalveluihin liittyvät käyttökatkot voivat olla myös seurausta tahallisista hyökkäyksistä palvelua kohtaan. Esimerkkejä tällaisista ovat palvelunestohyökkäykset, joissa ulkopuolinen taho lähettää palvelimelle suuria määriä pyyntöjä, jotka yksi kerrallaan kasvattavat niiden käsittelemiseen vaadittavaa palvelimen työmäärää. Palvelunestohyökkäykset ovat poikkeuksellisen tehokkaita pilvipalveluita vastaan, sillä pilvipalvelun vastaus palvelunestohyökkäykseen on kasvattaa käytettyjä laskennallisia resursseja, minkä voidaan puolestaan tavallaan nähdä auttavan hyökkääjää palvelun katkoksen aiheuttamisessa. Käytännössä hyökkääjän ei tarvitse käyttökatkoa aiheuttaakseen lähettää pyyntöjen tulvaa kaikille pilven palvelimille, vaan ainoastaan yhdelle. Epäsuorana palvelunestohyökkäyksen vaikutuksena myös muut samalla laitteistolla toimivat palvelut voivat estyä toimimasta, tai pahimmassa tapauksessa pilvi pyrkii vastaamaan hyökkäykseen laajentamalla resurssien käyttöä toiseen pilveen, jolloin toinenkin pilvi saattaa kaatua suuren laskennallisen työtaakan seurauksena. (Jensen, Schwenk, Gruschka & Iacono, 2009.) Pilvipalveluiden hyödyntämän resurssipohjaisen laskutuksen vuoksi palvelun hinta voi nousta äärimmäisen paljon palvelunestohyökkäysten yhteydessä (Jansen, 2011).

4.3 Muut haasteet

Tietosuojaongelmien lisäksi pilvitallennukseen liittyy myös toimittajalukkona tunnettu ilmiö, jossa asiakkaan on hankalaa tai kallista siirtää tallennettua dataa palveluntarjoajalta toiselle. Tällöin asiakas ei voi helposti esimerkiksi vaihtaa toiseen palveluntarjoajaan oman palveluntarjoajan nostaessa hintoja. Pahimmassa tapauksessa toimittajalukko voi johtaa tietojen menettämiseen palveluntarjoajan liiketoiminnan lakkaamisen yhteydessä. Toimittajalukko on seurausta siitä, että pilvipalveluntarjoajien käyttämät tiedon tallennuksen ohjelmointirajapinnat poikkeavat toisistaan niin laajalti, että tiedon siirtäminen palveluntarjoajalta toiselle ei ole helposti toteutettavissa. (Armbrust ym., 2010.) Haasteellista toimittajalukoissa voi olla myös se, että palveluntarjoajien itsensä voidaan nähdä hyötyvän toimittajalukkoa kannustavan palvelun tarjoamisesta. (Rong ym., 2013).

Myös käyttöasteeseen pohjautuvaan laskutusmalliin liittyy haasteita. Käyttäjällä ei ole keinoja tarkistaa näiden resurssien kulutustietojen oikeellisuutta. Toisaalta joitain tietoteknisiä resursseja ei voida virtualisoinnista riip-

pumatta eristää täysin yhden käyttäjän aiheuttamaksi. Myös viat pilvitallennusohjelmistossa tai tungos pilvipalvelussa voivat kasvattaa asiakkaan kuluttamia resursseja. Näin ollen se resurssien määrä, josta asiakas maksaa palveluntarjoajalle voi poiketa todellisesta käytettyjen resurssien määrästä. (Ren ym., 2012.)

5 YHTEENVETO

Tutkielman tavoitteena oli selvittää pilvitallennukseen liittyviä hyötyjä, käyttötarkoituksia sekä haasteita kirjallisuuskatsauksen avulla. Moni artikkeli ei suoranaisesti käsitellyt pilvitallennusta, joten joissain kohdin vaadittiin soveltavaa ajattelua, jotta pilvitallennuksen näkökulma saatiin tuotua esiin.

Pilvitallennuksen hyötyjä ja käyttötarkoituksia tutkittaessa keskeisimmiksi hyödyiksi nousivat tallennustilan määrän skaalautuvuus ja elastisuus, toteutuksen helppous yrityksen kannalta sekä sen käyttöön liittyvät taloudelliset hyödyt. Toisena käyttötarkoituksena perinteisen tiedon tallennuksen ohella löydettiin varmuuskopiointi varotoimenpiteenä.

Pilvitallennukseen liittyvät haasteet osoittautuivat lukumäärältään mittaviksi. Monien teknologioiden ja toimijoiden yhdistyessä pilven kautta datan luottamuksellisuuden, eheyden ja saatavuuden turvaaminen on hankalaa. Pahimmassa tapauksessa pilveen tallennettu arkaluontoinen data voi päätyä vääriin käsiin tai jopa kadota kokonaan.

Tutkimuksen tuloksena saatujen hyötyjen, käyttötarkoitusten ja haasteiden kautta voidaan analysoida, onko pilvitallennuksen käyttäminen kannattavaa yrityksen kannalta. On kuitenkin mahdotonta antaa kattavaa vastausta siitä, ovatko pilvitallennuksen tarjoamat edut houkuttelevampia kuin niiden vastapainona olevat tietoturvariskit. Pilvitallennuksen kannattavuuden analyysi tulisi tehdä yrityskohtaisesti yrityksen tarpeet huomioiden, mutta pilvitallennuksen etujen ja haasteiden ymmärtämisen pitäisi olla hyödyksi sitä päätöstä tehtäessä.

Vaikka pilvitallennusta on povattu tulevaisuuden keskeisimmäksi tallennustavaksi, lukuisista pilvitallennuksen käyttöön liittyvistä riskeistä johtuen on mahdollista, että pilvitallennusta käytettäisiin pääasiassa tukevana toimintona esimerkiksi varmuuskopiointiin eikä yrityksen tärkeimpänä tallennuskanavana. Toisaalta ei voida sulkea pois vaihtoehtoa, että pilvitallennukselle löydetään myös uusia käyttötarkoituksia.

Pilvitallennus on yhä kehittyvä ilmiö, johon liittyvän teknologian ja tutkimuksen voidaan olettaa kehittyvän entisestään tulevien vuosien aikana. On mielenkiintoista nähdä, kuinka esimerkiksi siihen liittyviin tietoturvahaasteisiin

saadaan kehitettyä toimivia ratkaisuja. Olisi myös toivottavaa, että tieteellisessä kirjallisuudessa huomioitaisi kattavammin pilvitallennusta omana ilmiönään eikä vain eräänä osana pilvipalveluiden suurta joukkoa.

Mahdollisia jatkotutkimusaiheita on lukuisia. Jokaista löydettyä hyötyä, käyttötarkoitusta tai haastetta voisi varmasti tutkia syvällisemmin, analysoiden niihin liittyvää teknologiaa, parannusmahdollisuuksia sekä haasteita. Toisaalta vastausten etsiminen moninaisiin pilvitallennuksen haasteisiin olisi sekä mielekästä että kannattavaa pilvitallennuksen tulevaisuuden kannalta.

LÄHTEET

Agrawal, D., El Abbadi, A., Das, S., & Elmore, A. J. (2011, January). Database scalability, elasticity, and autonomy in the cloud. *Database Systems for Advanced Applications* (2-15). Springer Berlin Heidelberg.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.

Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance, 1-76.

Cloud Security Alliance (2013). The Notorious Nine: Cloud Computing Top Threats in 2013.

Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), (27-33). IEEE.

Fallara, P. (2003). Disaster recovery planning. *Potentials*, IEEE, 22(5), 42-44.

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. *Communications of the ACM*, 55(9), 62-68.

Gartner.com (2010). Gartner Identifies the Top 10 Strategic Technologise for 2011. Haettu 20.1.2016 osoitteesta : http://www.gartner.com/newsroom/id/1454221

Godse, M., & Mulik, S. (2009). An approach for selecting software-as-a-service (SaaS) product. *IEEE International Conference on Cloud Computing* (155-158). IEEE.

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The characteristics of cloud computing. 2010 39th International Conference on Parallel Processing Workshops (ICPPW), (275-279). IEEE.

Grobauer, B., Walloschek, T., & Stöcker, E. (2011). Understanding cloud computing vulnerabilities. *Security & privacy*, IEEE, 9(2), 50-57.

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, 33(5), 861-874.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1-13.

Jansen, W. (2011). Cloud hooks: Security and privacy issues in cloud computing. *44th Hawaii International Conference on System Sciences* (HICSS), (1-10). IEEE.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. *IEEE International Conference on Cloud Computing* (109-116). IEEE.

Kandukuri, B. R., Paturi, V. R., & Rakshit, A. (2009). Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE.

Kächele, S., Spann, C., Hauck, F. J., & Domaschka, J. (2013). Beyond IaaS and PaaS: An extended cloud taxonomy for computation, storage and networking. *In Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing* (pp. 75-82). IEEE Computer Society.

Mell, P., & Grance, T. (2010). The NIST Definition of Cloud Computing. *Communications of the ACM*, 53(6), 50.

Owens, D. (2010). Securing Elasticity in the Cloud. *Communications Of The ACM*, 53(6), 46-51. doi:10.1145/1743546.1743565

Rahumed, A., Chen, H. C., Tang, Y., Lee, P. P., & Lui, J. (2011). A secure cloud backup system with assured deletion and version control. *2011 40th International Conference on Parallel Processing Workshops* (ICPPW) (160-167). IEEE.

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, (1), 69-73.

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, 39(1), 47-54.

Slamanig, D., & Hanser, C. (2012). On cloud storage and the cloud of clouds approach. International Conference for Internet Technology and Secured Transactions, (649-655). IEEE.

Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2012, August). State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. *Proceedings of the international conference on advances in computing, communications and informatics* (pp. 470-476). ACM.

Viega, J. (2009). Cloud computing and the common man. *Computer*, (8), 106-108.

Viestintävirasto (2014),, Pilvipalveluiden turvallisuus: Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä. Haettu 11-1-2016 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Vrable, M., Savage, S., & Voelker, G. M. (2009). Cumulus: Filesystem backup to the cloud. *ACM Transactions on Storage* (TOS), 5(4), 14.

Wang, C., Wang, Q, Ren, K, Lou, W. (2009). "Ensuring data storage security in Cloud Computing," *17th International Workshop on Quality of Service*, 2009. IWQoS.

Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., Van Der Merwe, J., & Venkataramani, A. (2010). Disaster recovery as a cloud service: Economic benefits & deployment challenges. *2nd USENIX workshop on hot topics in cloud computing* (pp. 1-7).

Wu, J., Ping, L., Ge, X., Wang, Y., & Fu, J. (2010). Cloud storage as the infrastructure of cloud computing. *2010 International Conference on Intelligent Computing and Cognitive Informatics (ICICCI),* (380-383). IEEE.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, 1(1), 7-18.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3), 583-592.