Olli-Pekka Erola

# PILVIPALVELUIDEN TIETOTURVALLISUUS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

# TIIVISTELMÄ

Erola, Olli-Pekka
Pilvipalveluiden tietoturvallisuus
Jyväskylä: Jyväskylän yliopisto, 2015, 29 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja: Makkonen, Pekka

Mahdolliset säästöt liiketoiminnan kustannuksissa ajaa yhä useampia organisaatioita harkitsemaan pilvipalveluihin siirtymistä. Pilvipalvelut mahdollistavat organisaatiolle muun muassa suuremmat ja tehokkaammat IT-resurssit sekä maksun käytön mukaan. Infrastruktuuri on organisaation käytössä jatkuvasti riippumatta ajasta tai paikasta. Ulkopuolisen palveluntarjoajan liittyminen organisaation toimintaan on tuonut kuitenkin mukanaan mahdollisuuksien lisäksi myös haasteita. Suurimmat haasteet pilvipalveluissa liittyvät niiden tietoturvallisuuteen. Tämän tutkielman tarkoituksena oli tutustua tarkemmin pilvipalveluihin sekä niiden ominaispiirteisiin. Pilvipalveluja tarkasteltiin niin palvelukuin käyttöönottomallienkin mukaan. Tutkielman päätavoitteena oli kuitenkin löytää haasteita, joita pilvipalveluiden tietoturvallisuuteen liittyy. Tutkielma toteutettiin kirjallisuuskatsauksena ja keskeisinä tuloksina tietoturvallisuuden haasteista voidaan pitää tietoliikenteen ja datan turvallisuuden ongelmia. Datan kontrollin siirtäminen organisaation toimitilojen ulkopuolelle aiheuttaa useimmat tietoturvallisuuteen liittyvistä haasteista. Toisena keskeisenä tuloksena voidaan pitää palveluntarjoajan ja asiakkaan välisen luottamuksen merkitystä, johon perustuu moni asia tietoturvallisuuden yhteydessä.

Asiasanat: pilvipalvelu, palvelumalli, tietoturvallisuus, turvallisuushaaste, luottamus

# ABSTRACT

Erola, Olli-Pekka
Information security of cloud computing
Jyväskylä: University of Jyväskylä, 2015, 29 p.
Information Systems, Bachelor's Thesis
Supervisor: Makkonen, Pekka

The potential savings in business costs drives more and more organizations consider moving to cloud computing. Cloud computing enables higher and more effective IT-resources and pay-per-use model for organizations. The infrastructure is available continuously for organization despite of time and place. Service provider coming outside from organization has brought more possibilities but some issues too. The biggest issues related to cloud computing is information security. The aim of this thesis was to explore more cloud computing and the main characteristic of it. The view of cloud computing was based on service models and deployment models. The main goal of this thesis was to find challenges regarding to information security of cloud computing. This thesis was based on literature review and key results regarding challenges of information security were difficulties with communications and data control. Most of the security issues are caused because data is controlled outside of organization's premises. Another key result was the importance of trust between service provider and customer. Many issues in information security are based on that.

Keywords: cloud computing, service model, information security, security issue, trust

# KUVIOT

# SISÄLLYS

# 1 JOHDANTO

Internetin jatkuvasti kehittyessä kuluttajille on tarjolla yhä uusia ja tehokkaampia palveluita, joiden avulla resursseja pystytään entistä paremmin hyödyntämään. Suurempien etujen myötä on muodostamassa yhä vahvempi visio siitä, että tietokoneiden käyttö nähdään jonain päivänä viidentenä hyödykkeenä veden, sähkön, puhelimen ja polttoaineen rinnalla. Tietokone ja sen tarjoamat resurssit hyödykkeenä tarkoittaa sitä, että tarpeen vaatimaa päivittäistä käyttöä varten perustoiminnot ovat yhteisön saatavilla. Tätä visiota kohti mentäessä yhä uusia tietokoneeseen liittyviä palveluita on esitelty ja tuotu yhteiskunnan käyttöön. Yksi viimeisimmistä palveluista on pilvipalvelut. (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009.) Pilvipalvelut ovat olleet hyvin vahvasti pinnalla viime aikoina niin uutisissa, IT-alan tutkimuksissa kuin myös liike-elämässä. Armbrust ym. (2010) korostavat sitä, miten innovatiivisten kehittäjien ei tarvitse enää huolehtia pääoman keräämisestä laitteistoa varten tai henkilöstökustannuksien kasvusta vain siitä syystä, että he pääsisivät toteuttamaan itseään ja ideoitaan. Heidän ei tarvitse huolehtia siitä, että palveluun sijoitetaan liikaa eikä se vastaakaan odotuksia. Myös kalliiden resurssien hukkaaminen tai yllättävän suosion saavuttaminen tietyllä palvelulla ei tuota ylitsepääsemättömiä hankaluuksia resurssien riittämättömyyden suhteen. Pilvipalveluiden joustavuus resurssien tarjonnassa ja maksun periminen käytön mukaan ratkaisevat useita ongelmia. Tämän takia niiden suosio onkin jatkuvasti kasvanut ja kerännyt enemmän mielenkiintoa IT-alalla.

Buyyan ym. (2009) mukaan nykypäivänä on kuluttajille yleistä päästä käsiksi internetin sisältöön ja palveluihin huolehtimatta siitä, minkälainen infrastruktuuri taustalla on ja miten sitä ylläpidetään. Yleensä infrastruktuuri pitää sisällään tietokoneita ja datakeskuksia, joita ylläpidetään ja valvotaan kellon ympäri palveluntarjoajan toimesta. Tämä mahdollistaa kuluttajille sen, että palveluita on saatavilla jatkuvasti, riippumatta ajasta tai paikasta. Myös pilvipalvelut perustuvat juuri tähän. Ne tarjoavat organisaatiolle mahdollisuuksia kapasiteetin lisäämiseen ilman sijoittamista uuteen infrastruktuuriin, lisähenkilöstön palkkaamiseen tai uuden ohjelmiston lisenssiin. Organisaatio saa nopeasti käyt-

töönsä lisäresursseja, resurssien elastisuutta, nopean toimituksen ja uusia mahdollisuuksia datan säilyttämiseen. (Subashini & Kavitha, 2011.)

Zissis ja Lekkas (2012) painottavat sitä, että samalla kun pilvipalveluiden suosio on kasvanut, myös huoli niiden tietoturvallisuudesta on lisääntynyt. Perinteisten tietoturvaan liittyvien mekanismien riittävyyttä on kyseenalaistettu pilvipalveluiden tarjoamien uusien ominaisuuksien myötä. Varsinkin tietojen ja datan luovuttaminen organisaation ulkopuolelle herättää pelkoa monissa. Lorin (2009) mukaan käyttäjiltä vaaditaan suurta luottoa sekä hyväksyntää sitä kohtaan, että heidän tietojansa päätyy palveluntarjoajan kontrolliin. Ramgovind, Eloff ja Smith (2010) pitävät tietoturvallisuutta tärkeimpänä asiana, kun puhutaan uuden teknologian menestymisestä markkinoilla. Tämä korostaa sitä, kuinka tärkeää on selvittää mitkä asiat koetaan suurimpina haasteina pilvipalveluiden tietoturvallisuudessa. Tutkielman tutkimusongelmaksi asetettiin tämän takia seuraava:

- Mitkä ovat suurimmat haasteet pilvipalveluiden tietoturvallisuudessa?

Vastausta tutkimusongelmaan lähdettiin selvittämään kirjallisuuskatsauksen avulla, jota varten aineisto hankittiin Googlen Scholar -palvelua käyttäen. Kirjallisuutta haettiin tutkimukseen liittyvien asiasanojen avulla. Artikkeleiden valinnassa kriteereinä pidettiin julkaisupaikkaa sekä viittauksien määrää. Koska pilvipalvelut tutkimusaiheena on suhteellisen uusi asia, myös suurin osa lähdemateriaalista on hyvin tuoretta. Kuitenkin viittauksia lähdemateriaalille on kertynyt runsaasti, joten sitä voidaan pitää laadukkaana.

Tutkielmassa määritellään ensiksi tarkemmin pilvipalveluita sekä tutustutaan niiden ominaispiirteisiin. Myös palvelumallit sekä käyttöönottomallit käydään läpi. Tämän jälkeen siirrytään käsittelemään tietoturvallisuutta. Ensin korostetaan tietoturvan merkitystä pilvipalveluille, minkä jälkeen käsitellään erilaisia tietoturvaan liittyviä haasteita ja tarkastellaan niitä lähemmin palvelumalleittain. Yhteenvedossa vastataan tarkemmin tutkimusongelmaan ja ehdotetaan mahdollisia jatkotutkimusaiheita.

# 2 PILVIPALVELUT

Tässä luvussa määritellään tarkemmin pilvipalveluja ja luodaan selkeämpää kuvaa niistä. Kirjallisuudesta on löydettävissä useita erilaisia määritelmiä pilvipalveluille. Tämän takia ensimmäinen alaluku keskittyy itse pilvipalvelun käsitteen määrittelemiseen. Siinä tutustutaan piirteisiin sekä ominaisuuksiin, jotka määrittelevät pilvipalveluja. Tämän jälkeen tarkastellaan lähemmin tärkeimpiä pilvipalvelumalleja, jotka ovat kirjallisuudessa laajasti tunnistettuja. Viimeinen alaluku keskittyy käyttöönottomalleihin, jotka määrittelevät pilvipalveluja käytön mukaan.

## 2.1 Pilvipalveluiden määritteleminen

Pilvipalveluiden tarkempaa ymmärtämistä ja määrittelemistä varten on hyvä tarkastella lähemmin niille ominaisia piirteitä ja sitä, mikä tekee palvelusta nimenomaan pilvipalvelun. Pilvipalvelu käsitteenä on melko uusi ja sille on löydettävissä kirjallisuudesta useita erilaisia määritelmiä. Kuitenkin Zhangin, Chengin ja Boutaban (2010) mukaan itse pääajatus pilvipalveluiden takana ei ole uusi. Jo 1960-luvulla John McCarthylla oli visio siitä, että tietokoneen toiminnot ja tehokkuus olisivat kaikkien saatavilla samalla tavalla kuin muut julkiset palvelut. Myös termiä ”pilvi” on käytetty useissa eri konteksteissa. Termin käyttö alkoi todella kerätä suosiota sen jälkeen, kun Googlen toimitusjohtajana vuonna 2006 toiminut Eric Schmidt käytti sitä kuvatakseen palvelun tarjoamista internetin välityksellä. Siitä lähtien termiä on käytetty pääasiassa markkinoinnin yhteydessä kuvamaan ideoita monessa eri kontekstissa liittyen palveluntarjoamiseen. (Zhang ym., 2010.)

Vaquero, Rodero-Merino, Caceres ja Lindner (2008) tuovat artikkelissaan esille sen, että pilvipalveluista puhuttaessa tekniikoiden monipuolisuus tekee kokonaiskuvan hahmottamisen vaikeaksi. Innostuksen ja suosion kasvaminen pilvipalveluiden ympärillä on omalta osaltaan vaikuttanut siihen, että niiden määritteleminen on monimutkaista. Epäselvyys pilvipalveluiden määrittelemi-

sessä on näin ollen johtanut siihen, että termistä on tullut yleispätevä nimitys lähes kaikille ratkaisuille, jotka liittyvät tietotekniikan ulkoistamiseen. Grossman (2009) sen sijaan nostaa esille sen, että vaikka pilvipalveluille ei ole vakiintunutta määritelmää, termiä voi pitää yleispätevänä nimityksenä sille, kun palveluita ja resursseja tarjotaan internetin välityksellä. Suurin osa tarkemmista määritelmistä keskittyykin ainoastaan tiettyyn teknologian osaan (Vaquero ym., 2008). Yksi kirjallisuudessa erittäin paljon viittauksia saanut lähde on Mellin ja Grancen (2011) artikkeli, joka tarjoaa hieman tarkemman määritelmän termille. Heidän mukaansa pilvipalvelut tarjoavat kaikkialla läsnä olevan, ajasta ja paikasta riippumattoman palvelun, joka mahdollistaa pääsyn internetin kautta käytettävissä oleviin tietokoneresursseihin.

Vaikka pilvipalveluiden tarkka määritteleminen on hankalaa, on olemassa piirteitä, jotka ovat yhteisiä pilvipalveluille ja antavat tarkemman kuvan niistä. National Institute of Standards and Technology (NIST) on määritellyt pilvipalveluille viisi ominaista piirrettä. Nämä piirteet ovat Mellin ja Grancen (2011) mukaan itsepalvelullisuus, laaja tavoitettavuus, yhteiskäytettävät resurssit, palvelun joustavuus sekä palvelun mitattavuus. Itsepalvelullisuudella tarkoitetaan sitä, että asiakas pystyy äkillisen tarpeen vaatiessa itse hyödyntämään tiedonkäsittelyyn vaadittavia lisäresursseja ilman, että hänen täytyy olla yhteydessä palveluntarjoajaan. Laajalla tavoitettavuudella tarkoitetaan sitä, että palveluun päästään käsiksi internetin välityksellä niin tietokoneelta, kuin myös tabletilta tai älypuhelimelta. (Dillon, Wu & Chang, 2010.) Resurssien yhteiskäytöllä Mell ja Grance (2011) tarkoittavat sitä, että yhden palveluntarjoajan resurssit ovat useamman asiakkaan käytössä. Neljäntenä mainittu joustavuus viittaa siihen, että palvelun tarjoamat resurssit joko lisääntyvät tai vähentyvät, riippuen käyttäjämäärästä ja muusta palveluun kohdistuvasta kuormituksesta. Joustavuus ja skaalautuvuus voidaan nähdä tärkeimpinä syinä puhuttaessa pilvipalveluiden noususta ja kehittymisestä (Wang ym., 2010). Viimeiseksi mainitulla palvelunkäytön mitattavuudella viitataan siihen, että resurssien käyttöä pystytään tarkkailemaan, kontrolloimaan ja raportoimaan. Tämä taas edesauttaa palvelun läpinäkyvyyttä sekä asiakkaalle että palveluntarjoajalle. (Mell & Grance, 2011.)

Vaquero ym. (2008) ovat yrittäneet löytää omassa tutkielmassaan tarkempaa määritelmää pilvipalveluille tutustutamalla laajasti saatavilla olevaan kirjallisuuteen ja sieltä löytyviin erilaisiin rajauksiin. He ovat koonneet omaan tutkielmaansa monen eri asiantuntijan kuvauksen pilvipalveluista ja näin ollen pyrkineet luomaan paremman kokonaiskuvan siitä, miten ne tulisi määritellä. Kirjallisuuteen tutustumisen perusteella he löysivät pilvipalveluille tunnusomaisia piirteitä, jotka toistuvat kuvauksissa. Vaqueron ym. (2008) mukaan kirjallisuuden määritelmissä toistuvia ominaispiirteitä pilvipalveluille ovat:

- Käyttäjäystävällisyys
- Virtualisointi
- Internetkeskeisyys
- Monimuotoiset resurssit
- Automaattinen mukautuminen

- Skaalautuvuus
- Resurssien optimointi
- Käytön perusteella tapahtuva veloitus
- Palvelutasosopimukset
- Infrastruktuuritason palvelusopimukset

Kaiken kaikkiaan kirjallisuuteen tutustumalla voi päätyä siihen, että vaikka pilvipalveluiden tarkka määritteleminen on haastavaa ja määritelmiä löytyy monia, niiden ominaispiirteitä tarkkailemalla ne ovat tunnistettavissa. Tiivistetysti sanottuna pilvipalvelut ovat ryhmä tietokoneita datakeskuksissa, jotka tarjoavat käyttäjälle resursseja ja palveluita internetin välityksellä (Sultan, 2010). Näitä resursseja ovat esimerkiksi tietoverkot, serverit, sovellukset ja tallennustila (Mell & Grance, 2011).

## 2.2 Pilvipalvelumallit

Jotta pilvipalveluista saisi luotua entistä tarkemman kuvan, on syytä tutustua eri malleihin, joiden avulla niitä luokitellaan. Sultanin (2010) mukaan käsitys siitä, minkä tyyppisiä palveluita pilvi tarjoaa, auttaa huomattavasti kokonaiskuvan hahmottamisessa ja pilvipalveluiden kokonaisvaltaisessa ymmärtämisessä. Yleisesti ottaen kirjallisuudessa pilvipalvelumallit jaetaan kolmeen eri luokkaan (Vaquero ym., 2008; Tsai, Sun & Balasooriya, 2010; Mell & Grance, 2011; Dinh, Lee, Niyato & Wang, 2013). Nämä kolme eri luokkaa ovat:

- Ohjelmisto palveluna (Software as a Service, Saas)
- Sovellusalusta palveluna (Platform as a Service. Paas)
- Infrastruktuuri palveluna (Infrastructure as a Service, IaaS)

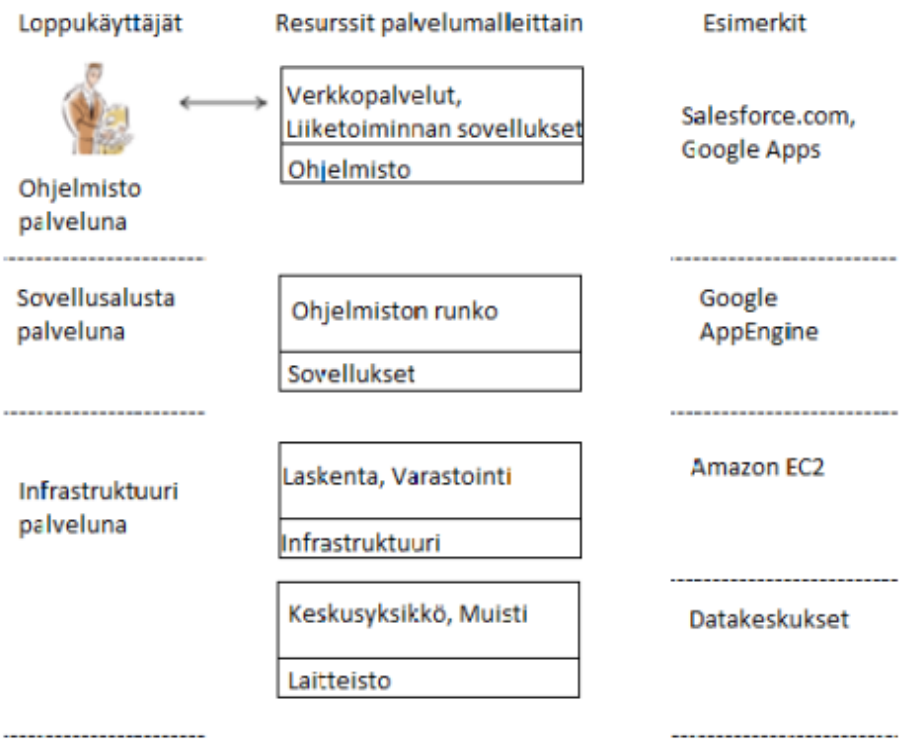
Zhang ym. (2010) tuovat esille näiden kolmen tason lisäksi myös laitteistokerroksen, johon koko pilvipalvelut perustuvat. Laitteistokerros pitää sisällään infrastruktuurin ja resurssit, johon pilvipalvelut perustuvat. Laitteistokerroksen vastuulla ovat pilvipalveluiden fyysiset resurssit, johon kuuluvat muun muassa serverit, reitittimet, kytkimet sekä virta- ja jäähdytysjärjestelmät. Tyypillisesti datakeskukset pitävät sisällään kaiken tämän laitteiston, jonka avulla pilvipalveluja pystytään tarjoamaan asiakkaille.

Laitteistokerroksen niin sanotusti näkyvämpää osaa kutsutaan infrastruktuurin kerrokseksi. Prodanin ja Ostermannin (2009) mukaan infrastruktuurin tarjoaminen asiakkaille antaa heidän käyttöönsä modernin laitteiston vapauttamalla samalla heidät sen ylläpidosta ja huoltamisesta. Mell ja Grance (2011) määrittelevät infrastruktuuritason tietokoneresurssien tarjoamiseksi, minkä avulla asiakkaat pystyvät ajamaan omia ohjelmiaan. Asiakas ei vastaa ohjelmien taustalla olevasta laitteistosta, vaan kontrolloi ainoastaan käyttöjärjestelmää sekä tallennustilaa. Voidaan siis sanoa, että infrastruktuurin tarjoaminen vähen-

tää asiakkaiden tarvetta investoida omiin laitteistoihin ja resursseihin. Ulkoistuksen avulla niitä on saatavilla enemmän ja ne ovat tehokkaampia. Tsai ym. (2010) mainitsevat esimerkkeinä infrastruktuuritasosta Amazonin EC2-palvelun sekä Microsoftin Azuren.

Infrastruktuuritason päälle rakennettu sovellusalusta (PaaS) pitää sisällään käyttöjärjestelmän ja sovellusten rungon (Zhang ym., 2010). Mell ja Grance (2011) mainitsevat sovellusalustan pitävän sisällään työkaluja asiakasta varten, joiden avulla asiakas pystyy kehittämään itselleen sopivia sovelluksia. Asiakas ei hallinnoi tai kontrolloi taustalla olevaa infrastruktuuria, vaan hän vastaa ainoastaan palvelun tarjoamien resurssien kehittämisestä. Tsai ym. (2010) nostavat esille sen, että sovellusalusta ei yleensä vaadi ohjelmistojen latauksia tai asennuksia. Sovellusalusta myös mahdollistaa työskentelyn ryhmien välillä, jotka sijaitsevat maantieteellisesti eri paikoissa. Esimerkkinä sovellusalustasta Tsai ym. (2010) mainitsevat Googlen App Enginen.

Päällimmäiseksi tasoksi pilvipalvelumalleissa luokitellaan ohjelmistopalvelu (SaaS). Ohjelmistopalvelun taso pitää sisällään todelliset pilven tarjoamat sovellukset. (Zhang ym., 2010.) Prodanin ja Ostermannin (2009) mukaan tällä tasolla ohjelmisto tai sovellus tarjotaan asiakkaalle internetin välityksellä, ilman tarvetta asentaa ja suorittaa uusia ohjelmia omalla tietokoneella. Palveluntarjoaja huolehtii ylläpidosta läpinäkyvästi, mikä vähentää välikäsiä asiakkaan ja palveluntarjoajan välillä. Sovellukset ovat asiakkaan saatavilla eri laitteiden avulla esimerkiksi selaimen välityksellä (Mell & Grance, 2011). Prodan ja Ostermann (2009) nostavat esille myös sen, että ohjelmistotaso on asiakkaalle rajoittavampi kuin infrastruktuuritaso, koska ohjelmistotaso tarjoaa asiakkaalle ainoastaan olemassa olevat palvelut, ilman asiakkaan mahdollisuutta kehittää uusia. Tsai ym. (2010) nostavat ohjelmistotason esimerkeiksi Google Maps–palvelun sekä Salesforce.com -sivuston. Alta löytyvä kuvio (kuvio 1) vetää yhteen pilvipalvelumallit ja niiden suhteen toisiinsa.




KUVIO 1 Pilvipalvelumallien yhteenveto (Zhang ym., 2010)

Kuviosta löytyvien palvelumallien lisäksi Fernandes, Soares, Gomes, Freire ja Inácio (2014) tuovat esille kaikki palveluna -mallin (Anything as a Service, Xaas). Tällä viitataan siihen, että pilvipalvelut pystyvät tukemaan ja tarjoamaan kaikkia palveluja aina personoidusta palvelusta suuriin resursseihin. Esimerkkeinä mainitaan muun muassa turvallisuus palveluna sekä reititys palveluna. (Fernandes ym., 2014.)

## 2.3 Käyttöönottomallit

Vaikka pilvipalvelut ovat yleisesti tunnistettu lähinnä sen pohjalta, että tietokoneiden laskentatehoa ja resursseja on tarjottu julkisena palveluna, niitä voidaan tarkastella myös muunlaisen käytön perusteella. Huolimatta itse palvelumallista pilvipalvelu voidaan luokitella käytön mukaan joko julkiseksi, yksityiseksi tai hybridimalliksi. (Buyya, Broberg & Goscinski, 2010.) Näiden kolmen lisäksi Mell ja Grance (2011) mainitsevat myös yhteisöllisen pilven. Yhteisöllisellä pilvellä tarkoitetaan heidän mukaansa palvelua, joka on tarjolla tietyille organisaatioille ja niiden jäsenille, jotka ovat tekemisissä saman asian kanssa. Yhteisölli-

sen pilven omistus ja hallinnointi voi olla kaikilla sitä käyttävillä organisaatioilla, vain yhdellä niistä tai kolmannen osapuolen käsissä.

Zhang ym. (2010) määrittelevät julkisen käyttöönottomallin tilanteeksi, jossa palveluntarjoajan resurssit ovat suuren yleisön saatavilla. Julkisen käyttöönottomallin tarjoaminen on kannattavaa palveluntarjoajalle, koska se ei vaadi alkupääoman sijoittamista infrastruktuuriin eikä palveluntarjoaja kanna kaikkia riskejä infrastruktuurista. Dillon ym. (2010) nostavatkin esille sen, että julkinen pilvipalvelu on johtavassa asemassa käyttöönotosta puhuttaessa. Negatiivisia puolia julkisessa palvelussa ovat puutteet tarkassa kontrollissa datan, yhteyksien ja tietoturvan suhteen. Liiketoiminnan monissa eri skenaarioissa tämä tarkoittaa sitä, että julkisen palvelun käyttö ei välttämättä ole tehokasta. (Zhang ym., 2010.)

Yksityinen käyttöönottomalli on Dillonin ym. (2010) mukaan palvelu, jossa koko infrastruktuuri on yksittäisen organisaation käytössä. Sitä hallinnoi joko kolmas osapuoli tai organisaatio itse, riippuen siitä, missä se sijaitsee. Dillon ym. (2010) mainitsevat myös sen, että yksityinen pilvi tarjoaa parhaimmat mahdollisuudet organisaation olemassa olevien resurssien optimaaliseen hyödyntämiseen. Zhang ym. (2010) sen sijaan kritisoivat yksityistä mallia siitä, että ne nähdään usein samanlaisina kuin perinteiset ja patentoidut saatavilla olevat palvelut. Myöskään selvää rahallista säästöä ei tule esimerkiksi siitä, että palveluun ei tarvitsisi sijoittaa pääomaa etukäteen.

Hybridi käyttöönottomalli perustuu yksityisen ja julkisen mallin yhdistelmiin (Calheiros, Ranjan, Beloglazov, De Rose & Buyya, 2011). Zissis ja Lekkas (2012) tarkentavat määritelmää siten, että hybridin mallin osat ovat itsenäisiä kokonaisuuksia, joita yhdistää patentoitu tai standardoitu teknologia, mikä mahdollistaa sovellusten ja datan siirtämisen. Hybridimalli mahdollistaa enemmän joustavuutta verrattuna julkiseen tai yksityiseen malliin. Erityisesti se mahdollistaa tarkemman kontrollin dataan samalla kuitenkaan unohtamatta sitä, että resursseja on tarpeen vaatiessa enemmän saatavilla. Negatiivisena puolena hybridimallista mainitaan valinnan vaikeus siinä, mikä on paras jako julkisen ja yksityisen mallin välillä, kun valitaan komponentteja hybridiä varten. (Zhang ym., 2010.) Dillonin ym. (2010) mukaan organisaatiot käyttävät hybridimallia silloin, kun ne yrittävät parantaa kilpailukykyään ulkoistamalla toisarvoisia liiketoiminnan osia pilveen samalla, kun kontrolli tärkeimmistä aktiviteeteista säilyy yksityisessä pilvessä.

Zhang ym. (2010) mainitsevat näiden mallien lisäksi vielä virtuaalisen yksityisen pilven (Virtual Private Cloud, VPC). Tätä pidetään vaihtoehtoisena ratkaisuna yksityisen ja julkisen pilven rajoitteisiin. Virtuaalinen pilvi on pohjimmiltaan palvelu, joka toimii julkisten pilvien päällä. Suurin ero on siinä, että virtuaalinen pilvi mahdollistaa palveluntarjoajille omien turvallisuusasetusten määrittelemisen, joista esimerkkinä voi mainita palomuuriasetukset. Zhang ym. (2010) mainitsevat palveluntarjoajien valinnasta eri käyttöönottomallien välillä sen, että valinta perustuu useimmiten liiketoiminnan näkymiin. Esimerkiksi laskentaan keskittyvät tieteelliset sovellukset pääsevät oikeuksiinsa julkisessa pilvessä kustannustehokkuuden takia. Todennäköisesti yksi käyttöönottomalli

nousee suositummaksi kuin toiset ja onkin ennustettu, että hybridimalli nousee päärooliin monessa organisaatiossa. Samalla kuitenkin virtuaalinen pilvi on kasvattanut jatkuvasti suosiotaan. (Zhang ym., 2010.)

# 3 TIETOTURVALLISUUS

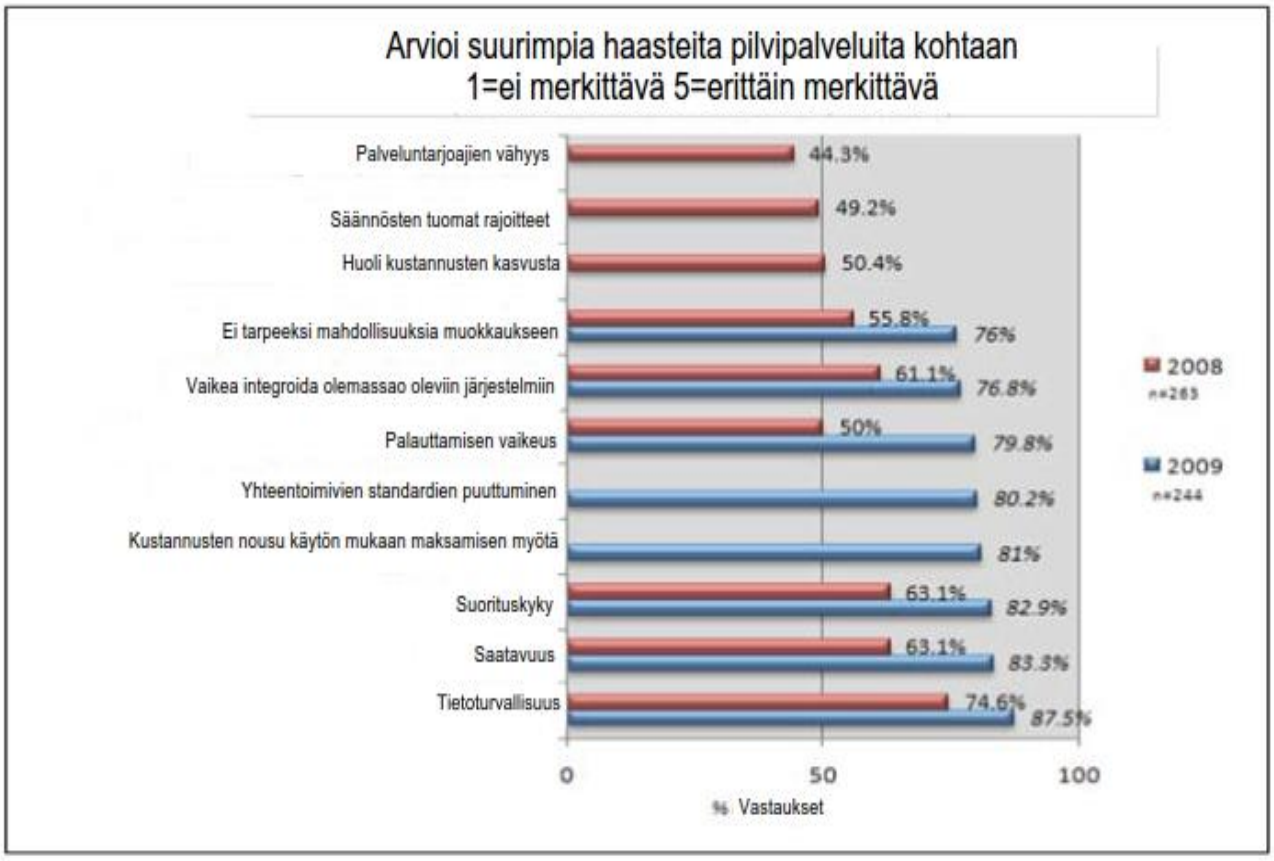
Tämä luku on tutkielman pääluku ja se keskittyy vastamaan tutkimuskysymykseen. Ensimmäinen alaluku korostaa tietoturvan merkitystä pilvipalveluille ja sitä, miksi sen huomioiminen on niin tärkeää. Toinen alaluku keskittyy tietoturvallisuuteen liittyviin haasteisiin ja ongelmiin, jotka ovat kirjallisuuteen tutustumalla löydettävissä. Kolmas alaluku jakaa turvallisuushaasteita hieman tarkemmin palvelumalleittain.

## 3.1 Tietoturvan merkitys pilvipalveluissa

Tämän päivän tietoyhteiskunnassa tietoturva yleisesti voidaan nähdä kriittisenä osana organisaatioiden päivittäistä toimintaa. Bulgurcu, Cavusoglu ja Benbasat (2010) nostavat esille sen, miten nykyaikana useat organisaatiot ovat suuresti riippuvaisia tietojärjestelmistä, mikä on johtanut siihen, että niihin liittyvät riskit täytyy tiedostaa. Tietoturvallisuuteen liittyvät riskit ovat suuren luokan haaste organisaatioille, koska riskien toteutuessa seuraukset voivat olla vakavia. Tietoturvan varmistaminen onkin noussut monissa organisaatioissa yhdeksi johtoportaan tärkeimmistä tehtävistä. (Bulgurcu ym., 2010.)

Tietoturvan merkitystä ei voi vähätellä pilvipalveluista puhuttaessa. Vaikka pilvipalvelut voivat vähentää informaatiotekniikan kustannuksia huomattavasti, monet organisaatiot eivät innostu niistä johtuen siitä, että luottamus niiden tietoturvaan on hyvin heikkoa (Santos, Gummadi & Rodrigues, 2009). Santos ym. (2009) nostavat esiin tutkielman, johon osallistui yli 500 johtajaa ja IT-manageria yli seitsemästätoista maasta. Kyseisessä tutkielmassa johtajat mainitsivat sen, että pilvipalveluiden eduista huolimatta he luottavat enemmän jo olemassa oleviin järjestelmiin, kun puhutaan kontrollista dataan ja järjestelmien turvallisuuteen. Yksi suurimmista huolen aiheista liittyy siihen, kuinka palveluntarjoaja voi vahingossa tai tarkoituksella päästä käsiksi organisaation dataan. Datan vuotaessa ja joutuessa vääriin käsiin organisaatiolle voi aiheutua suuria taloudellisia ja imagollisia tappioita. (Santos ym., 2009.) Ramgovind ym.

(2010) nostavat omassa artikkelissaan esille International Data Corporationin tekemän tutkimuksen, joka selvitti pilvipalveluiden suurimpia haasteita. Tutkimuksen tulokset käyvät ilmi alla oheisesta kuviosta (kuvio 2). Kuten kuviosta näkyy, tietoturvallisuus koetaan suurimpana ja kasvavana haasteena mietittäessä pilvipalveluihin siirtymistä. Tämä korostaa sitä, miten suuri merkitys tietoturvalla on pilvipalveluille.




KUVIO 2 Haasteita pilvipalveluille (Ramgovind ym., 2010)

Myös Jensen, Schwenk, Gruschka ja Iacono (2009) nostavat esille sen, miten eduista huolimatta pilvipalvelut ja niiden käyttöönotto huolestuttavat monia. Oman datan antaminen muiden käsiin jopa maan rajojen ulkopuolelle ja eri sääntelyn alle saavat monet organisaatiot pitäytymään lähellä sijaitsevien datakeskusten asiakkaina.

Kandukuri, Paturi ja Rakshit (2009) mainitsevat artikkelissaan sen, miten pilvipalveluiden arkkitehtuuri riippuu yleisesti siitä, minkälaisia palveluja ne tarjoavat. Data on keskitetty datakeskuksiin, joiden sijainnista asiakkaalla ei välttämättä ole lainkaan tietoa. Asiakkaiden tulee siis luottaa palveluntarjoajaan sekä datan saatavuuden että sen turvallisuuden suhteen. Jotta luottamusta pystyttäisiin rakentamaan, on sitä varten luotu palvelutasosopimukset. Ne ovat

standardoituja dokumentteja, jotka kuvaavat suhdetta palveluntarjoajan ja vastaanottajan välillä. (Kandukuri ym., 2009.) Takabin, Joshin ja Ahnin (2010) mukaan pilvipalveluille tulisi luoda alusta, joka tukisi sopimusneuvotteluja palveluntarjoajan ja asiakkaan välillä sekä helpottaisi sopimuksen toimeenpanon seurantaa. Koska turvallisuus, yksityisyys sekä luottamus ovat vaikeasti mitattavissa olevia asioita, on sopimuksen noudattamista vaikea seurata. Kuitenkin asiakkaan tulisi pystyä luottamaan palveluntarjoajan lupauksiin ja siihen, että sopimuksessa mainittuja asioita kunnioitetaan ja muun muassa tietoturvasta huolehditaan. Usein vaaditaankin kolmas osapuoli, joka seuraa sopimusten noudattamista ja raportoi rikkomuksista. (Takabi ym., 2010.)

Yksilöiden ja organisaatioiden tietoa siirretään yhä enemmän ja enemmän pilveen. Samalla kun datan määrä pilvessä lisääntyy, huoli tietoturvallisuutta kohtaan kasvaa koko ajan. (Subashini & Kavitha, 2011.) Subashini ja Kavitha (2011) mainitsevat artikkelissaan sen, miten kolme eri palvelumallia asettaa jokainen oman haasteensa tietoturvallisuuden takaamiseen. Palvelumallien turvallisuuteen liittyvät riskit siirtyvät tasolta toiselle samalla tavalla kuin kyvykkyydetkin. Tämä asettaa jokaiselle tasolle oman haasteensa. Vastuu turvallisuudesta asiakkaan ja palveluntarjoajan välillä riippuu siis paljon siitä mallista, mihin palvelu pohjautuu. Pearson ja Benameur (2010) nostavat esille sen, miten vaikeata perinteisiä turvallisuuteen liittyviä malleja on soveltaa pilvipalveluiden ympäristöön. Varsinkaan käyttöönottoon liittyvät hybridit ja julkiset pilvet eivät sovellu perinteisten turvallisuuteen liittyvien standardien alaisuuteen, koska datan käsittely niissä voi tapahtua luotettavien ja tunnettujen rajojen ulkopuolella.

Ramgovind ym. (2010) painottavat sitä, miten organisaatioiden tulee olla tietoisia nykyisistä huolenaiheista, joita pilvipalveluita kohtaan tunnetaan. Ilman oleellista tietoa ja kyseisten aihealueiden tunnistamista strategisten päätösten tekeminen siirtymisestä pilvipalveluiden pariin muodostuu vaikeaksi. Ramgovind ym. (2010) mainitsevat kansainvälisen standardisoimisjärjestön laatiman standardin, joka määrittelee sen, mitä tietoturvallisuuden yleisesti ottaen tulisi pitää sisällään. Vaikka tämä standardi koskee pääosin perinteisiä palveluja pilvipalveluiden sijasta, sen tulisi olla ohjenuorana myös pilvipalveluille niiden turvallisuutta miettiessä. Tämä takaisi sen, että niitä voitaisiin pitää tehokkaana ja turvallisena palveluna. Ramgovind ym. (2010) luettelevat yleiseen tietoturvaan liittyvästä standardista vaatimuksia, joihin myös pilvipalveluiden tulisi vastata. Nämä vaatimukset ovat:

- Tunnistaminen ja todennus
- Valtuuttaminen
- Luottamus
- Eheys
- Kiistämättömyys
- Saatavuus

Tunnistamisella ja todennuksella viitataan siihen, että yksittäiset pilven käyttäjät olisivat tunnistettavissa esimerkiksi käyttäjänimen ja salasanan avulla. Riippuen palvelumallista, yksittäiset käyttäjät tulee tunnistaa ja heille voidaan jakaa oikeuksia sen mukaisesti. (Ramgovind ym., 2010.) Zissisin ja Lekkasin (2012) mukaan puutteet käyttäjän tunnistamisessa ja todentamisessa voivat johtaa siihen, että dataan päästään luvattomasti käsiksi. Valtuuttamisella pyritään Ramgovindin ym. (2010) mukaan siihen, että palvelun koskemattomuutta pystyttäisiin ylläpitäjän toimesta kontrolloimaan jakamalla oikeuksia palvelun eri toimintoihin ja ominaisuuksiin.

Zissis ja Lekkas (2012) määrittelevät luottamuksen siten, että valtuutetuilla henkilöillä on mahdollisuus päästä käsiksi suojattuun dataan. Ramgovindin ym. (2010) mukaan luottamuksen rooli on suuri, kun puhutaan kontrollin säilymisestä organisaation datan suhteen. Varsinkin julkisen pilven tapauksessa luottamuksen rooli korostuu, johtuen niiden laajasta saatavuudesta ja tavoitettavuudesta. Kun organisaation dataa siirretään pilveen, riski sen joutumisesta vääriin käsiin nousee välittömästi, koska se on useampien osapuolien tavoitettavissa (Zissis & Lekkas, 2010).

Datan eheyttä voidaan pitää kriittisenä jokaisessa järjestelmässä. Eheys on helposti saavutettavissa yksinkertaisten järjestelmien kanssa toimittaessa, joilla on vain yksi tietokanta. Kun siirrytään monimutkaisempiin järjestelmiin, jossa on useita tietokantoja ja sovelluksia, vaikeudet lisääntyvät. Vielä vaikeampaa datan eheyden takaaminen on, kun siirrytään pilvipalveluihin, joissa on saatavilla lukuisia sovelluksia kolmannen osapuolen tarjoamana. (Subashini & Kavitha, 2011.) Zissisin ja Lekkasin (2012) mukaan eheys on kriittinen tekijä palvelujen tietoturvasta puhuttaessa. Eheydellä viitataan siihen, että data on muokattavissa, poistettavissa ja tuotettavissa vain valtuutetuilla osapuolilla.

Kiistämättömyydellä tietoturvan yhteydessä tarkoitetaan sitä, että muutokset palvelun sisällä ovat jäljitettävissä. Tämä onnistuu esimerkiksi sähköisten allekirjoitusten ja aikaleimojen seuraamisen avulla. (Ramgovind ym., 2010.) Zissin ja Lekkasin (2012) mukaan kiistämättömyyden avulla varmistetaan se, että yksikään sähköisessä liiketoiminnassa mukana ollut ei voi kiistää osallistumistaan.

Pilvipalveluiden tietoturvasta puhuttaessa saatavuuden merkitys on hyvin suuri. Saatavuus on avainasemassa, kun puhutaan valinnasta yksityisen, julkisen ja hybridin käyttöönottomallin välillä. Saatavuuden kohdalla palvelutasosopimuksen merkitys korostuu, koska sen avulla pystytään määrittelemään vastuun jakautuminen palveluntarjoajan ja asiakkaan välillä. (Ramgovind ym., 2010.) Subashini ja Kavitha (2011) korostavat sitä, miten palvelun tulee olla saatavilla kellon ympäri. Tämä edellyttää muutoksia arkkitehtuurissa ja infrastruktuurin tasolla, jotta tavoitettavuus pystytään takaamaan. Tästä syystä tietoturvan kannalta olennainen haaste on se, että turvallisuutta ei unohdeta saatavuuden kustannuksella. Palveluntarjoajan tulee huolehtia saatavuuden pysymisestä oikeiden henkilöiden keskuudessa.

Jansen (2011) painottaa datan sijainnin merkitystä pilvipalveluiden tietoturvasta puhuttaessa. Kun organisaatio itse huolehtii palvelimistaan ja tietoko-

nekeskus sijaitsee jopa samassa rakennuksessa, on helpompaa luottaa siihen, että data säilyy paremmin turvassa. Organisaatio on tietoinen palvelimien sijainnista ja voi itse kontrolloida sitä, kenellä on fyysisesti mahdollista päästä niihin käsiksi. Pilvipalveluihin siirryttäessä datan ja datakeskusten sijainti on usein organisaatiolle tuntematon. Tämä johtaa suureen epätietoisuuteen siitä, onko data varmasti turvassa ja tarvittavat toimenpiteet sen turvaamiseksi tehty. Varsinkin jos tietoa ja dataa siirretään organisaation kotimaan rajojen ulkopuolelle, astuu kuvioihin uusi lainsäädäntö sekä uudet rajoitteet. On hyvin vaikeaa taata datan turvallisuus vieraassa maassa, jossa lait ja säädökset voivat poiketa hyvinkin paljon tunnetuista. (Jansen, 2011.) Pilvipalveluiden tulisi siis pystyä takaamaan se, että data ja datakeskukset ovat turvassa, vaikka niiden sijainti onkin tuntematon. Kaiken kaikkiaan tietoturvan merkitys pilvipalveluille on kiistaton, kun puhutaan organisaatioiden mahdollisesta siirtymisestä pilvipalveluiden pariin.

## 3.2 Haasteita tietoturvallisuudessa

Popovicin ja Hocenskin (2010) mukaan turvallisuuteen liittyvät haasteet tulee selvittää, jotta pilvipalveluista saisi kaiken mahdollisen hyödyn irti. Chow ym. (2009) ovat jakaneet turvallisuuteen liittyvät haasteet kolmeen pääkategoriaan, jotka ovat perinteinen turvallisuus, saatavuus sekä kolmannen osapuolen datan kontrollointi. Perinteinen turvallisuus pitää sisällään tietokoneisiin ja verkkoon liittyvät tunkeutumiset, jotka ovat mahdollistuneet ainakin osittain pilveen siirtymisen myötä. Palveluntarjoajat puolustelevat itseään toteamalla sen, että turvallisuuteen liittyvät tekijät ovat kehittyneempiä ja testatumpia kuin keskivertoisella organisaatiolla. (Chow ym., 2009.) Chow ym. (2009) kategorisoivat kriittisten sovellusten ja datan turvallisuuden saatavuuteen liittyviin haasteisiin. Kolmannen osapuolen datan kontrolloinnilla viitataan siihen, miten ylimääräisen osapuolen ylläpitämät sovellukset ja data ovat monimutkaisia, eikä kovin hyvin ymmärrettyjä. Kolmannen osapuolen haasteisiin liittyy myös mahdollinen kontrollin puute sekä läpinäkyvyyden ongelmat. Näiltä ongelmilta suojautuakseen monet organisaatiot ovat päätyneet rakentamaan käyttöönsä yksityisen pilvipalvelun. (Chow ym., 2009.)

Perinteisistä turvallisuuden haasteista Chow ym. (2009) mainitsevat muun muassa palveluntarjoajan haavoittuvuuden, tietojen kalastelun palveluntarjoajalta sekä valtuuttamisen. Palveluntarjoajan haavoittuvuudella tarkoitetaan mahdollisia tietoturva-aukkoja sen järjestelmissä, jotka aiheuttavat uhan asiakkaan tietojen säilyvyydelle. Tietojen kalastelulla pyritään sen sijaan saamaan palveluntarjoajaa luovuttamaan herkkäluontoista tietoa. Valtuuttamisen ongelmat liittyvät siihen, kun organisaatio siirtää toimintaansa uuteen ympäristöön. Organisaation valtuuksien jakamisen runko on suunniteltu usein perinteisten palvelujen pariin, joten ne eivät automaattisesti sovi uuteen pilvipalvelun ympäristöön. (Chow ym., 2009.)

Saatavuuteen liittyvät haasteet koskevat sitä, että järjestelmä pystyy jatkamaan toimintaansa, vaikka jotkut sen osat eivät toimisikaan halutulla tavalla. Saatavuus viittaa sekä dataan että ohjelmistoihin, mutta myös laitteiston saatavuuteen tarpeen niin vaatiessa. (Zissis & Lekkas, 2012.) Chow ym. (2009) mainitsevat saatavuudesta sen, että vaikka pilvipalveluilla tavoitellaan yleensä helpompaa tavoitettavuutta, ne mahdollistavat myös useamman yksittäisen mahdollisuuden hyökkäyksille ja epäonnistumisille. Saatavuuden haasteisiin voidaan lukea myös palveluntarjoajan rehellisyys. Asiakkaan tulee luottaa siihen, että palveluntarjoaja uskollisesti ylläpitää asiakkaan sovelluksia sekä siihen, että sovellukset suorittavat tehtävänsä ja antavat päteviä tuloksia. (Chow ym., 2009.)

Chow ym. (2009) mainitsevat kolmannen osapuolen tuomista haasteista muun muassa sopimusten tuomat haasteet ja palveluntarjoajan suorittaman vakoilun. Ongelmia muodostuu, kun käytetään toisen organisaation infrastruktuuria, johon ei välttämättä päde samat turvallisuuteen liittyvät seikat kuin omaan ja tuttuun järjestelmään. Pahimmassa tapauksessa myös palveluntarjoaja voi syyllistyä asiakkaiden tietojen vakoiluun. (Chow ym., 2009.) Pearson (2009) korostaa sitä, miten tärkeää kehittäjille on suunnitella palvelut niin, että yksityisyyden suoja säilyy. Käyttäjät ovat useasti epäileviä sitä kohtaan, miksi palveluntarjoajat vaativat henkilökohtaisia tietoja ja voivatko ne päätyä vääriin käsiin. Käyttäjät ovat myös huolissaan siitä, onko heidän tietonsa riittävän hyvin suojattuna pilvipalvelujen ympäristössä. (Pearson, 2009.)

Yksityisyyden varjelu nousee muutenkin suureen rooliin pilvipalveluista puhuttaessa. Tässä tulee kuitenkin ottaa huomioon konteksti, jossa pilvipalvelu ja sovellukset toimivat. Toiset palvelut pitävät sisällään yleisen tason tietoja, kun taas toiset voivat pitää sisällään hyvinkin kriittistä dataa. Tämä johtaa siihen, että tiettyjen palveluiden haasteet yksityisyyden suojaamisessa ovat suuremmat kuin toisten. (Pearson & Benameur, 2010.) Oleellinen osa pilvipalveluiden toimintaa on muiden organisaatioiden kanssa jaettu infrastruktuuri. Kun data varastoidaan ja prosessoidaan muualla kuin organisaation sisässä, se tuo mukanaan uusia uhkia tietoturvallisuudelle. Tiedon virtuaalisuuden ja jakamisen kasvaminen johtaa siihen, että pilvessä olevan datan suojaaminen on erittäin tärkeää. (Pearson, 2009.) Tässä tapauksessa suureen rooliin nousee luottamus palveluntarjoajaa kohtaan. Jansen ja Grance (2011) korostavat sitä, miten suuri luottamus organisaatiolla tulee olla palveluntarjoajaa kohtaan, koska ne luopuvat monista asioista liittyen turvallisuuteen ja yksityisyyteen siirtyessään pilvipalveluihin.

Jansen ja Grance (2011) erittelevät ja korostavat tarkemmin luottamusta ja sen merkitystä tietoturvallisuudelle. Tietoturvallisuuden merkityksen yhteydessä mainittu datan sijainti näyttelee suurta roolia myös tässä tapauksessa. Kun organisaation dataa ja sovelluksia siirretään pilvipalveluiden ympäristöön, niihin käsiksi pääsevien sisäpiiriläisten määrä kasvaa. Perinteisessä organisaatiossa työskenneltäessä sisäpiiriin voivat kuulua työntekijöiden lisäksi myös organisaation yhteistyökumppanit, joilla on pääsy järjestelmiin. Pilvipalvelun yhteydessä sisäpiiriin uusina jäseninä ei tule pelkästään palveluntarjoaja, vaan

mahdollisesti myös muut organisaatiot, jotka käyttävät samoja sovelluksia. Tämä aiheuttaa sen, että riski datan valumisesta vääriin käsiin kasvaa useamman osapuolen työskennellessä samassa ympäristössä. (Jansen & Grance, 2011.) Chenin ja Zhaon (2012) mukaan datan ja yksityisyyden turvaaminen pilvipalveluissa on samanlaista kuin perinteisten palveluiden parissa. Heidän mukaansa kuitenkin pilvipalveluiden avoimuus ja useat käyttäjät tuovat omat erikoisuuteensa ja vaikeudet niiden turvallisuuden takaamiseen.

Useissa kirjallisuuden lähteissä korostetaan haasteita liittyen datan turvallisuuteen ja epätietoisuuteen siitä, missä data itse asiassa sijaitsee (Jansen & Grance, 2011; Popovic & Hocenski, 2010; Dikaiakos, Katsaros, Mehra, Pallis & Vakali, 2009; Pearson & Benameur, 2010.) Sabahi (2011) korostaa kahta luontaista asiaa dataan liittyen, kun organisaatio siirtyy pilvipalveluihin. Nämä kaksi asiaa ovat siirtyminen paikalliselta koneelta muualle sekä siirtyminen yhden käyttäjän mallista usean käyttäjän malliin. Tämä aiheuttaa sen, että datan vuotaminen on suurimpia organisaation riskejä pilvipalveluiden käyttöönottoon liittyen. (Sabahi, 2011.) Dikaiakos ym. (2009) mainitsevat sen, miten siirtyminen uuden sukupolven datakeskusten pariin luo uusia haasteita datan turvallisuuden takaamiseen. Data voi sijoittua maantieteellisesti hyvin laajalle alueelle ja epäluotettavien palveluntarjoajien alaisuuteen, mikä aiheuttaa valtavaa uhkaa datan yksityisyyden säilymiselle. Chenin ja Zhaon (2012) mukaan datan laaja leviäminen aiheuttaa myös sen, että turvallisuusrikkomuksen sattuessa on vaikea paikallistaa tarkkaa fyysistä paikkaa sille, missä uhka on toteutumassa. Pearson ja Benameur (2010) nostavat datan turvallisuusongelmista esiin sen elinkaaren seuraamisen. Asiakkaan tulisi olla varma siitä, että hänen tietonsa oikeasti poistuvat järjestelmistä, kun hän niin haluaa. Tällä hetkellä tätä ei juuri pystytä todistamaan, vaan luotetaan ainoastaan siihen, että palveluntarjoajalle ei ole mahdollista palauttaa asiakkaan poistamia tietoja. Toisaalta taas Kandukurin ym. (2009) mukaan palveluntarjoajan tulisi pystyä mahdollisen katastrofin ja tietojen tahattoman häviämisen kohdalla löytämään keinot asiakkaiden oleellisten tietojen palauttamiseen. Tässä tapauksessa voidaan siis nähdä ristiriita, minkä takia luottamus palveluntarjoajaa kohtaan nousee suureen arvoon. Yleisesti ottaen dataan ja sen turvallisuuteen liittyy useita eri ongelmia, jotka ovat kirjallisuudessa laajasti tunnistettuina.

Cloud Security Alliance (CSA) on omassa julkaisussaan jaotellut tarkemmin turvallisuushaasteita niiden vakavuuden mukaan. Julkaisua varten kerättiin toimialan asiantuntijoiden mielipiteitä, joiden pohjalta muodostettiin lista suurimmista uhkista pilvipalveluiden tietoturvaa kohtaan. Lista pitää sisällään seuraavat yhdeksän asiaa, joista ensimmäistä pidetään kaikkein vakavimpana ja viimeistä vähiten vakavana. (CSA, 2013.)

1. Datan vuotaminen
2. Datan häviäminen
3. Tilin kaappaus
4. Turvattomat käyttöliittymät

5. Palvelunestohyökkäys
6. Sisäiset uhkat
7. Pilvipalveluiden väärinkäyttö
8. Riittämätön tarvekartoitus
9. Jaetun teknologian haavoittuvuus

Listassa ensimmäisinä mainitut datan vuotaminen ja häviäminen ovat asioita, joita jokaisessa organisaatiossa pelätään. Dataa voi päätyä kilpailijoiden käsiin tai se voi kadota lopullisesti. Vaikka dataan liittyvät riskit ovat luokiteltu kaikista vakavimmiksi, huomioon tulee ottaa myös palveluntarjoajaan kohdistuvat haasteet. Käyttöliittymän turvattomuus voi aiheuttaa tilin kaappaamisen tai mahdollistaa palvelunestohyökkäykset. Molemmat näistä aiheuttavat pahimmillaan suurta haittaa organisaation toiminnalle. Kuudentena listalla mainitut sisäiset uhkat liittyvät nykyisiin tai entisiin työntekijöihin, jotka haluavat omalla toiminnallaan vaikeuttaa organisaation toimintaa pilvipalveluiden parissa. Sisäisten uhkien jälkeen listalla mainittu pilvipalveluiden väärinkäyttö viittaa tilanteeseen, jossa pilvipalveluiden suurta kapasiteettia käytetään esimerkiksi salauksen avaamiseen. Normaalisti hakkeri joutuu kamppailemaan tietokoneen rajallisten resurssien kanssa, jolloin toiminta voi viedä hyvinkin paljon aikaa. Sen sijaan pilvipalveluiden suurien resurssien avulla hakkerin on mahdollista murtaa salaus jopa minuuteissa. Toiseksi viimeisenä mainittu riittämätön tarvekartoitus tarkoittaa tilannetta, jossa organisaatio ei ole täysin ymmärtänyt pilvipalveluiden todellista luonnetta. Tämä voi johtaa siihen, että pilveen siirretään dataa ja toimintoja ilman ymmärrystä siitä, mitä riskejä pilvipalveluiden käyttö tuo mukanaan. Viimeisenä listalla oleva jaetun teknologian haavoittuvuus tarkoittaa yksinkertaisesti sitä, että useamman asiakkaan käytössä olevat palvelut mahdollistavat suuremman haavoittuvuuden verrattuna yksityiseen käyttöön. (CSA, 2013.)

Kaiken kaikkiaan listasta voidaan huomata, että dataan liittyviä ongelmia pidetään asiantuntijoiden keskuudessa kaikista uhkaavimpina. Asiakkaiden luottamus palveluntarjoajaa kohti korostuu datan ongelmista puhuttaessa. Tämän lisäksi listan perusteella palveluntarjoajan roolia ei voi väheksyä. Turvallisen käyttöliittymän luominen voi ratkaista monta tietoturvaan liittyvää haastetta. Myös organisaation tulee kantaa vastuu tutustumalla riittävästi pilvipalveluihin sekä niiden tärkeimpiin ominaisuuksiin. Tämä mahdollistaa oikeiden ratkaisujen tekemisen sen suhteen, mitä toimintoja kannattaa siirtää pilveen ja mitä ei.

## 3.3 Haasteita palvelumalleittain

Tutkielmassa jo esitetyt kolme palvelumallien pääluokkaa asettavat jokainen omat vaatimuksensa tietoturvallisuudelle. Myös mainittu uhkien ja mahdollisuuksien periytyminen tasolta toiselle aiheuttaa omat ongelmansa. Infrastruktuuri on pohjana sovellusalustalle, jolle vuorostaan ohjelmistotaso pohjustaa

toimintansa. Subashini ja Kavitha (2011) ovat eritelleet tarkemmin tietoturvallisuuden haasteita palvelumalleittain. Ohjelmistotasolla nousee taas kerran esiin asiakkaan luottamus palveluntarjoajaa kohtaa. Asiakkaan tulee luottaa siihen, että palveluntarjoaja huolehtii tarpeellisista turvallisuuteen liittyvistä toimenpiteistä. Myös usean asiakkaan käytössä olevat järjestelmät aiheuttavat haasteita sen suhteen, miten huolehtia asiakkaiden datan näkymättömyydestä muille samaa ohjelmistoa käyttäville. Suurimmat ohjelmistotason ongelmat ylipäätänsä liittyvät useasti mainittuun datan turvallisuuteen. Ohjelmistotasolla tulee huolehtia datan turvallisuuden lisäksi osatekijöistä, jotka takaavat sen. Näitä tekijöitä ovat esimerkiksi datan sijainti ja siihen pääsy, luottamuksellisuus, eheys, eristäminen ja varmuuskopioiden luominen. (Subashini & Kavitha, 2011.) Datan turvaamisen lisäksi Zissis ja Lekkas (2012) mainitsevat ohjelmistotason haasteista yhteyden ja istunnon kaappaamisen sekä yksityisyyden rikkomisen. Subashini ja Kavitha (2011) korostavat turvallisuuden takaamiseksi sitä, että palveluun käsiksi pääsemistä kontrolloidaan. Organisaation tulee olla tarkkana, että entisten työntekijöiden oikeudet poistetaan järjestelmistä. Ohjelmistotason palveluissa käyttäjän tunnistaminen ja valtuuksien jakaminen on suuressa roolissa. Tämän avulla pystytään hillitsemään mahdollisia vuotoja datan suhteen ja takamaan hieman parempi suojautuminen haasteilta.

Subashinin ja Kavithan (2011) mukaan sovellustasolla palveluntarjoaja pystyy antamaan osan kontrollista asiakkaille, jotta sovellusten luominen tulee mahdolliseksi. Kuitenkin kaikki turvallisuus ohjelmistotason alapuolella tulisi kuulua pääosin palveluntarjoajalle ja asiakkaan tulee luottaa siihen, että data pysyy koskemattomana. Sovellustason on tarkoitus tarjota asiakkaille mahdollisuuksia rakentaa omia sovelluksiaan sen päälle. Tämän tarkoittaa sitä, että se on enemmän laajennettavissa verrattuna ohjelmistoalustaan. Tämä taas tarkoittaa sitä, että tietoturvallisuuden suhteen tulee ottaa huomioon useampi asia. Valmiina olevia komponentteja on vähemmän, mutta laajennukset ja joustavuus mahdollistavat useampien komponenttien lisäämisen. Zissis ja Lekkas (2012) lukevat sekä sovellustason että infrastruktuuritason saman kategorian alle. He kutsuvat tasoa virtuaaliseksi tasoksi. Virtuaalisella tasolla käytön kontrollointi, kommunikoinnin turvallisuus ja turvallisuuden luominen ovat haasteita, joihin sen tulee vastata. Heidän mukaansa sovellustason turvallisuushaasteet liittyvätkin ohjelmiston muokkauksiin ja tätä kautta syntyviin mahdollisiin tietoturva-aukkoihin. Asiakas ei välttämättä ota kaikkia turvallisuuteen liittyviä seikkoja huomioon, kun hän pääsee muokkaamaan omia sovelluksiaan. Tämän takia sovellustason vastuun jakautuminen ja syyllisten etsintä voi olla hankalaa tietoturvarikkomuksen sattuessa. Hashizume, Rosado, Fernández-Medina ja Fernandez (2013) korostavat sovellustasosta sitä, miten se ei tarjoa pelkästään perinteisiä ohjelmointikieliä asiakkaiden käyttöön. Tämän lisäksi tarjolla on myös kolmannen osapuolen komponentteja ja niiden yhdistelmiä. Yhdistelmät ovat useamman yksinäisen komponentin muodostamia joukkoja. Näiden yksittäisten kolmansien osapuolten tarjoaminen erilaisten komponenttien mukana periytyvät myös niiden ongelmat, mitkä omalta osaltaan lisäävät sovellustason haasteita tietoturvallisuudessa.

Subashinin ja Kavithan (2011) mukaan infrastruktuurin tasolla kehittäjän kontrolli tietoturvasta on paremmalla tasolla verrattuna muihin. Suurta roolia näyttelevä luottamus on pääroolissa myös infrastruktuurin tasolla. Nykypäivänä suurin osa datasta on sähköisessä muodossa, joten sen kontrollista luopuminen vaatii luottamusta palveluntarjoajaa kohtaan. Infrastruktuurin tasolla tulee huomioon ottaa myös käyttöönottomalli. Julkisen pilvipalvelun kohdalla tietoturvariskit ovat suurimmat, kun taas yksityisen kohdalla niitä voidaan pitää huomattavasti pienempinä. Zissis ja Lekkas (2012) mainitsevat infrastruktuuritason turvallisuushaasteista itse laitteiston turvallisuuden. Fyysinen laitteisto voi altistua muun muassa varkauksille ja luvattomille muokkauksille. Laitteistosta puhuttaessa myös väärinkäytön mahdollisuudet tulee ottaa huomioon. Koska datakeskukset sijaitsevat fyysisesti jossain, ei luonnonkatastrofin mahdollisuutta voi sivuuttaa. Pahimmillaan katastrofi voi tuhota datakeskuksen hyvin pahoin, jolloin asiakkaan datan säilyvyys on suuressa vaarassa.

Subashini ja Kavitha (2011) korostavat sitä, että vaikka pilvipalvelut ovat kehittynyttä teknologiaa, ne perustuvat samalle pohjalle kuin internetin palvelut. Tämä tarkoittaa sitä, että perinteiset internetiin liittyvät tietoturvahaasteet liittyvät myös pilvipalveluihin. Pilvipalveluiden yhteydessä haasteet ovat vain huomattavasti suurempia. Pilvipalveluiden protokollat ja suojausmekanismit perustuvat perinteisiin palveluihin, vaikka vaatimukset niiden tietoturvallisuutta kohtaan ovat selvästi suuremmat.

# 4 YHTEENVETO

Tämän tutkielman tarkoituksena oli kirjallisuuteen tutustumalla löytää haasteita, jotka liittyvät pilvipalveluiden tietoturvallisuuteen. Tämän lisäksi tutustuttiin tarkemmin pilvipalveluihin, niiden ominaispiirteisiin sekä palvelu- ja käyttöönottomalleihin. Kirjallisuuteen tutustamalla huomattiin se, että pilvipalveluille ei ole yhtä selkeää määritelmää. Kirjallisuuden määritelmät ovat kuitenkin hyvin samankaltaisia. Useimmat niistä määrittelevät pilvipalveluita ulkopuolisten resurssien ja laskentatehon tarjoamisena, joista maksu tapahtuu käytön mukaan. Tämä mahdollistaa organisaatioiden mahdolliset säästöt IT-kustannuksissa. Pilvipalvelumallit jaettiin kirjallisuudessa yleisesti kolmeen tasoon, jotka ovat infrastruktuuritaso, sovellustaso ja ohjelmistotaso. Tasojen mahdollisuudet ja ominaisuudet ovat periytyviä alemmalta tasolta ylöspäin mentäessä. Palvelumallien lisäksi kirjallisuuden avulla tutustuttiin myös käyttöönottomalleihin, joita ovat julkinen, yksityinen, yhteisöllinen ja hybridiin perustuva malli.

Kirjallisuuteen tutustumisen avulla selvisi se, että pilvipalveluiden positiivisten puolten lisäksi myös haasteet niihin liittyen on laajasti tunnistettu. Vaikka monet organisaatiot ovat siirtäneet toimintaansa pilveen, monet ovat sen myös jättäneet tekemättä, vaikka suuremmat resurssit ja pienemmät kustannukset olisivat mahdollisesti saatavilla. Yksi suurimmista syistä, mikä pitää organisaatiot poissa pilvipalveluiden parista, on puutteet ja huolet niiden tietoturvallisuutta kohtaan. Organisaatioiden data on yhä enemmän ja enemmän sähköisessä muodossa, jolloin tietoturvallisuus on tärkeä osa joka päivästä liiketoimintaa. Pilvipalveluiden kohdalla tietoturvallisuuden merkitys vain korostuu entistestään, kun kontrolli datasta luovutetaan palveluntarjoajan käsiin. Tämä voi johtaa suuriin vaikeuksiin ja epätietoisuuteen siitä, onko tarvittavat toimenpiteet ja suojaukset datan turvaamiseksi tehty. Vaikka pilvipalvet ovat suhteelisen tuore ilmiö, niiden pohjalla on kuitenkin perinteinen internet. Pilvipalveluiden tulisi siis pystyä vastaamaan vähintään samoihin tietoturvavaatimuksiin kuin perinteisten internetin kautta välitettävien palvelujen. Tämän lisäksi niiden tulee vastata pilvipalveluille ominaisiin haasteisiin, jotka suurelta osin liittyvät dataan ja sen kontrollointiin.

Voidaan siis sanoa, että pilvipalveluiden turvallisuushaasteet ovat huomattavasti suurempia verrattuna perinteisten palveluiden kohtaamiin haasteisiin.

Tutkielman tavoitteena oli löytää vastaus seuraavaan tutkimuskysymykseen:

- Mitkä ovat suurimmat haasteet pilvipalveluiden tietoturvallisuudessa?

Tutkielman sekä kirjallisuuskatsauksen avulla keskeisenä tuloksena ja vastauksena tutkimuskysymykseen voidaan pitää haasteita organisaation datan kontrolloinnissa pilvipalveluihin siirryttäessä. Kun organisaation dataa siirretään sen toimitilojen ulkopuolelle palveluntarjoajan käsiin, tulee eteen monia tietoturvallisuuteen liittyviä haasteita. Näitä ovat muun muassa datan vuotaminen, eheys ja siihen käsiksi pääseminen. Haasteita liittyy myös tunnistautumiseen sekä saatavuuteen, mitkä voivat aiheuttaa datan päätymistä organisaation sisäpiirin ulkopuolelle. Kaiken kaikkiaan suurimpana haasteena voidaan pitää datan joutumista vääriin käsiin. Erittäin suureen rooliin nousee asiakkaan luottamus palveluntarjoajaa kohtaan. Jotta asiakas siirtyisi pilvipalveluiden pariin, tulee hänen luottaa tarpeeksi siihen, että palveluntarjoaja tekee kaikkensa estääkseen tietoturvaongelmat.

Mahdolliset jatkotutkimusaiheet voisivat liittyä erilaisiin teknologioihin ja ratkaisuihin, joiden avulla pilvipalveluiden tietoturvallisuutta voitaisiin parantaa. Näin ollen useampi potentiaalinen käyttäjä uskaltaisi siirtyä niiden pariin. Olisi myös mielenkiintoista tutkia tarkemmin yksittäistä organisaatiota, joka käyttää pilvipalveluja. Tämä edesauttaisi tarkemman kuvan luomista siitä, miten tietoturvaongelmat koetaan käytännössä ja kuinka paljon niitä esiintyy.

# LÄHTEET


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

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Buyya, R., Broberg, J. & Goscinski, A. M. (2010). *Cloud computing: Principles and paradigms* John Wiley & Sons.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems,25*(6), 599-616.

Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A. & Buyya, R. (2011). CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Software: Practice and Experience, 41*(1), 23-50.

Chen, D. & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on,* (647-651). IEEE.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. (2009). Controlling data in the cloud: Outsourcing computation without outsourcing control. *Proceedings of the 2009 ACM Workshop on Cloud Computing Security,* (85-90). ACM.

Cloud Security Alliance (2013). The notorious nine: Cloud computing top threats in 2013. Haettu 28.5.2015 osoitteesta https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G. & Vakali, A. (2009). Cloud computing: Distributed internet computing for IT and scientific research. *Internet Computing, IEEE, 13*(5), 10-13.

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

Dinh, H. T., Lee, C., Niyato, D. & Wang, P. (2013). A survey of mobile cloud computing: Architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13*(18), 1587-1611.

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M. & Inácio, P. R. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*(2), 113-170.

Grossman, R. L. (2009). The case for cloud computing. *IT Professional, 11*(2), 23-27.

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

Jansen, W. & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST Special Publication, 800*, 144.

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L. L. (2009). On technical security issues in cloud computing. *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on,* (109-116). IEEE.

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

Lori, M. (2009). Data security in the world of cloud computing. *Co-Published by the IEEE Computer and Reliability Societies,* , 61-64.

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing,* (44-52). IEEE Computer Society.

Pearson, S. & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on,* (693-702). IEEE.

Popovic, K. & Hocenski, Z. (2010). Cloud computing security issues and challenges. *MIPRO, 2010 Proceedings of the 33rd International Convention,* (344-349). IEEE.

Prodan, R. & Ostermann, S. (2009). A survey and taxonomy of infrastructure as a service and web hosting cloud providers. *Grid Computing, 2009 10th IEEE/ACM International Conference on,* (17-25). IEEE.

Ramgovind, S., Eloff, M. M. & Smith, E. (2010). The management of security in cloud computing. *Information Security for South Africa (ISSA), 2010,* (1-7). IEEE.

Sabahi, F. (2011). Cloud computing security threats and responses. *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on,* (245-249). IEEE.

Santos, N., Gummadi, K. P. & Rodrigues, R. (2009). Towards trusted cloud computing. *Proceedings of the 2009 Conference on Hot Topics in Cloud Computing,* (3-3). San Diego, California.

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management, 30*(2), 109-116.

Takabi, H., Joshi, J. B. & Ahn, G. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security and Privacy, 8*(6), 24-31.

Tsai, W., Sun, X. & Balasooriya, J. (2010). Service-oriented cloud computing architecture. *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on,* (684-689). IEEE.

Vaquero, L. M., Rodero-Merino, L., Caceres, J. & Lindner, M. (2008). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review, 39*(1), 50-55.

Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J. & Fu, C. (2010). Cloud computing: A perspective study. *New Generation Computing, 28*(2), 137-146.

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.