Konsta Valkonen

PILVIPALVELUMALLIEN TURVALLISUUSHAASTEET

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2014

TIIVISTELMÄ

Valkonen, Konsta
Pilvipalvelumallien turvallisuushaasteet
Jyväskylä: Jyväskylän yliopisto, 2014, 33 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja: Ojala, Arto

Viime vuosina pilvipalveluiden houkuttelevat ominaisuudet, kuten saavutetut kustannussäästöt, ovat mullistaneet ICT-alaa. Mahdollisuus hankkia IT-resursseja käyttöperusteisesti ja joustavasti kysyntään vastaten, ovat muuttaneet tapaa, jolla liiketoiminta hyödyntää ja tarjoaa IT-palveluja. Muutokseen liittyy monia haasteita. Pilvilaskennan ja -palveluteknologioiden kannalta suurin yksittäinen haaste on turvallisuus. Tutkielmassa tutkittiin pilvipalveluihin sisältyviä turvallisuushaasteita, sekä selvitettiin miten ne sisältyvät eri pilvipalvelumalleihin. Tutkielmassa käsiteltiin pilvipalvelumallien eroavaisuuksia ominaisuuksien, sovellusten, vastuun jakautumisen, turvallisuuden ja haasteiden näkökulmista. Tutkimuksen tarkoituksena oli selventää turvallisuushaasteiden ja pilvipalvelumallien suhdetta. Tutkimus toteutettiin kirjallisuuskatsauksena ja sen keskeisenä tuloksena havaittiin, että turvallisuushaasteita luokitellaan harvoin pilvipalvelumalleittain, vaikka haasteet ovat keskeinen osa pilvipalveluiden turvallisuuden tutkimuskenttää.

Asiasanat: pilvilaskenta, pilvipalvelu, pilvipalvelumalli, turvallisuushaaste, turvallisuusuhka, tietoturva

ABSTRACT

Valkonen, Konsta
Security challenges in cloud service models
Jyväskylä: University of Jyväskylä, 2014, 33 p.
Information Systems Science, Bachelor's thesis
Supervisor: Ojala, Arto

Over the last few years benefits like cost savings achieved via cloud computing have revolutionized the ICT-sector. The possibility of acquiring IT-related resources in a pay-per-use manner mixed with elasticity enabling operation based on-demand, is changing the way business utilizes and offers IT-services. Biggest challenges in the adoption of cloud computing and cloud service technologies lie in security. This study focused on the security challenges within cloud service models. Differences between cloud service models were examined from features, applications, responsibilities, securities and challenges point of view. The aim of the study was to investigate the relation between cloud security issues and cloud service models. The research was conducted as a literature review. The key result of the study was that security challenges are rarely categorized according to cloud service models.

Keywords: cloud computing, cloud service, cloud service model, security challenge, security threat, information security

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Nykypäivän teknologioiden menestys riippuu vahvasti niiden tehokkuudesta, helppokäyttöisyydestä sekä ennen kaikkea tietoturvan ja kontrollin asteesta (Ramgovind, Eloff & Smith, 2010). Edellisen vuosikymmenen puolivälin jälkeen keskustelu tietokoneyhteydestä (engl. *computing*) viidentenä perushyödykkeenä veden, sähkön, kaasun ja teleliikenteen lisäksi on lisääntynyt. Tietokonepohjaisia palveluja "hyödykkeistetään" ja toimitetaan tänä päivänä perushyödykkeitä vastaavaan tapaan: käyttäjillä on pääsy hyödykkeen ääreen riippumatta siitä, missä palvelu tuotetaan tai kuinka se toimitetaan. Usein palveluiden käytöstä myös veloitetaan perushyödykkeitä vastaavaan tapaan: käyttömäärän perusteella. Erityisesti kehitys pilvipalveluissa on edistänyt visiota tietokoneen käytön muuttumisesta perushyödykkeeksi (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009b). Mahdollisuus maksaa hankituista palveluista käyttöasteen perusteella (engl. *pay-as-you-go*) sekä vastata kysyntään operationaalisella joustavuudella, on muuttanut yritysten tapaa hyödyntää IT-resursseja: paikallisen IT-infrastruktuurin sijaan on alettu hyödyntää ulkoisten tietokeskuksien resursseja (Fernandes, Soares, Gomes, Freire & Inácio, 2013). Ulkoistettuja resursseja hallinnoivat pilvipalvelujen tarjoajat. Pilvipalveluissa korostuu nimenomaan tehokkuus ja helppokäyttöisyys. Sen sijaan informaation tietoturvan ja kontrollin säilyttäminen sekä varmistaminen on entistä haastavampaa. Ramgovind ym. (2010) mukaan turvallisuuden hallinta on suurin haaste pilvipalveluteknologiaa implementoidessa. Tätä väitettä tukee osaltaan myös markkinatutkimus, kuten International Data Corporationin (IDC) vuosittainen kysely pilvipalveluiden haasteista ja hyödyistä.

Marston, Li, Bandyopadhyay, Zhang ja Ghalsasi (2011) mukaan viime vuosien kehitys pilvilaskennassa on potentiaalisesti tietokoneen historian suurimpia harppauksia. He kuitenkin korostavat, miten pilvilaskennan potentiaali vaatii realisoituakseen vallitsevien haasteiden selkeää ymmärtämistä niin asiakkaan kuin palveluntarjoajankin puolelta (Marston ym., 2011).

Tänä päivänä on yleistä saada pääsy digitaaliseen sisältöön Internetin välityksellä olematta riippuvainen, tai edes tietoinen, tietoa isännöivästä infrastruktuurista. Isännöivä infrastruktuuri koostuu yleisimmin ympäri vuorokauden ylläpidettävistä tietokeskuksista (engl. *data center*), joiden kautta tarjotaan asi-

akkaalle yhteys, tallennustila, sekä ohjelmistoalusta. Palveluntarjoajan motiivina toimii liiketoimintapotentiaali, joka pohjautuu palveluun pääsystä veloitettavaan maksuun. Asiakasta pilvipalvelussa viehättävät mahdolliset kustannusedut, joita saavutetaan, jos vastaavaa palvelua ei tarvitse itse tuottaa ydinliiketoiminnan lisäksi. (Buyya ym., 2009b.).

Alan kasvua kuitenkin hidastaa eräs tekijä: turvallisuus. IDC:n kyselyssä, jossa selvitettiin IT-johtajien ja tietohallinnon vastuuhenkilöiden käsityksiä suurimmista pilvipalveluiden haasteista ja hyödyistä, on turvallisuus arvotettu haasteista suurimmaksi. Vuoden 2008 tutkimuksen mukaan yli 74% vastaajista pitää turvallisuutta suurimpana haasteena pilvipalveluissa (Gens, 2008). Tästä syystä ei ole yllättävää, että pilvipalvelumarkkinoita leimaavat myös haasteet datan yksityisyyden ja suojan varmistamisessa (Subashini & Kavitha, 2011). On loogista, että turvallisuus- ja yksityisyysnäkökulmien ymmärtäminen on kriittistä myös pilvipalveluiden menestymisen kannalta (Takabi, Joshi & Ahn, 2010). Palveluiden menestyminen ei kuitenkaan ole kaikki kaikessa. Turvallisuushaasteet koskevat kaikkea dataa, jota pilvipalveluihin tallennetaan. Datan lisäksi haasteet koskevat jokaista henkilöä ja yritystä, joiden yksityistä tietoa päätyy tallennettavaksi pilvipalveluihin. Datan turvallisuuden takaamisen pilviympäristöissä tekee haastavaksi eritoten se, että jokaisella pilvipalvelun tasolla, pilvipalvelumallilla (infrastruktuuri, alusta, ohjelmisto), on omat huolensa turvallisuuden suhteen (Kandukuri, Paturi & Rakshit, 2009).

Tässä tutkimuksessa keskitytään nimenomaan eri pilvipalvelumalleihin sisältyviin turvallisuushaasteisiin. Johdanto-luvussa käsitellään pilvipalveluiden markkinaympäristöä yleisesti. Lisäksi esitetään syitä ja hyötyjä, joiden vuoksi pilvipalvelut ovat saaneet suuren roolin ICT-alalla viime aikoina. Johdannon yhteydessä esitellään myös tutkimusongelma ja -kysymys, sekä avataan tutkimusmenetelmää ja tiedonhakuprosessia.

Seuraava luku, Pilvilaskenta ja pilvipalvelumallit, koostuu tutkimuksen keskeisten käsitteiden määritelmistä. Luvussa esitetään määritelmiä tutkimusongelman kannalta relevanteille käsitteille: pilvilaskenta, pilvipalvelu, pilvipalvelumalli. Keskeistä tässä luvussa on kiinnittää huomiota pilvipalvelumallien välisiin eroihin ja yhteyksiin. Lisäksi esitetään esimerkkejä pilvipalvelujen sovellusmahdollisuuksista palvelumalleittain.

Kolmas luku, Pilvipalvelumallien turvallisuushaasteet, on tutkielman pääluku. Aluksi luvussa käsitellään turvallisuutta yleisesti pilvipalveluiden kontekstissa, perustellaan turvallisuuden merkitystä, sekä avataan mitä turvallisuudella pilvipalveluiden kontekstissa tarkoitetaan. Tämän jälkeen huomautetaan vastuun jakautumisesta pilvipalveluiden tapauksessa. Yleiseltä tasolta edetään turvallisuusuhkiin, joita liitetään eri pilvipalvelumalleihin. Lopuksi esitetään jaottelu turvallisuushaasteita, joita lähdekirjallisuudessa pilvipalvelumalleihin yhdistetään. Jaottelu vastaa tutkielman tutkimuskysymykseen, sekä on tutkielman keskeinen tulos.

Neljännessä luvussa esitetään tutkielman yhteenveto, sekä pohditaan tutkimusprosessin ja tulosten hyväksyttävyyttä. Lisäksi korostetaan seikkoja, joita tutkija näkee pohdinnan arvoiseksi aiheen kannalta.

1.1 Pilvipalveluiden potentiaali ja hyödyt

Monet uskovat pilvipalveluiden mullistavan ICT-alan vallankumouksellisesti (Dillon, Wu & Chang, 2010). Pilvipalvelut ilmiönä ovat olleet vahvasti pinnalla viime vuosina niin uutisissa, alan tutkimuksessa, yleisessä keskustelussa kuin liike-elämässäkin. Ilmiön esiinnousun ennakoidaan muuttavan perustavanlaatuisesti sen, miten IT-palveluita tarjotaan, keksitään, kehitetään, toimitetaan, skaalataan, päivitetään, ylläpidetään tai miten niistä veloitetaan (Marston ym., 2011). Pilvipalvelut vähentävät kustannuksia liittyen ohjelmistojen ja ohjelmistoalustojen (laitteistojen) ylläpitämisestä siirtämällä infrastruktuuria verkkoon (Vaquero, Rodero-Merino, Caceres & Lindner, 2008). Murroksen myötä ohjelmistojen viehättävyys palveluna lisääntyy. Myös laitteistojen suunnittelu ja hankinta joutuvat etsimään uusia suuntauksia. (Armbrust ym., 2010.).

Pilvipalveluiden potentiaali on monisyistä. Esimerkiksi startup-yritysten kynnys ohjelmistopalvelun kehittämiseen ja julkaisuun madaltuu pilvipalveluja käytettäessä, sillä pääomaa tai henkilöstöresursseja ei tarvitse enää sitoa esimerkiksi palvelintilaan (Armbrust ym., 2010). Yritykset ja organisaatiot saavuttavat tehokkuutta siirtämällä tietoresursseja verkkoon, jonka kautta resurssien hallinnan kustannukset alenevat (Vaquero ym., 2008). Palveluista voidaan veloittaa käytön mukaan, mikä madaltaa pienten ja keskisuurten yritysten kynnystä kilpailla suurempien yritysten kanssa (Marston ym., 2011). Joustavuus, jolla voidaan kohdentaa tietokoneresurssit suoraan tarpeeseen investoimatta infrastruktuuriin etukäteen, on IT-alalle ennenäkemätöntä. Pieni yritys ei ole ikinä ennen voinut hyväksikäyttää tuhannen tietokoneen laskentatehoa tunnin ajan investoimatta tuhanteen tietokoneeseen. Joustavuuden kautta kysynnän vaihteluihin voidaan myös vastata liki välittömästi. IT-resurssien joustavuus, jota saavutetaan skaalautuvuuden avulla, on alalla ennennäkemätöntä. (Armbrust ym., 2010.). Voitaneen siis sanoa, että kiinnostus pilvipalveluita kohtaan perustuu potentiaaliin tarjota kustannusedullista skaalautuvaa tallennustilaa sekä prosessointitehoa (Watson, 2012).

Markkinatutkimuksessa pilvipalveluihin on ladattu suuria odotuksia. Gartner Research arvioi tutkimuksissaan pilvipalveluihin liittyvän liiketoiminnan saavuttavan 150 miljardin dollarin arvon vuoteen 2014 mennessä (Marston ym., 2011). Vastaavasti AMI Partners arvioi pienten ja keskisuurten yritysten kuluttavan yli 100 miljardia dollaria pilvipalveluihin vuoteen 2014 mennessä (Marston ym., 2011). Merrill Lynch on arvioinut vuonna 2008 pilvipalveluiden markkinapotentiaalin 160 miljardin dollarin suuruiseksi - 95 miljardia dollaria liittyen liiketoiminnan ja tuottavuuden sovelluksiin ja loput 65 miljardia liittyen internetmainontaan. Samana vuonna Morgan Stanley on arvioinut pilvipalvelut huomattavaksi teknologiatrendiksi. (Buyya ym., 2009b.).

1.2 Tutkimusongelma ja tutkimuskysymys

Hypestä huolimatta ICT-ala ei mullistu mutkitta. Subashinin ja Kavithan (2011) mukaan yritykset edelleen siirtävät palveluitaan pilviympäristöön vastahakoisesti. Heidän mukaansa turvallisuus on suurin pullonkaula alan kasvun tiellä. Lisäksi he toteavat, että markkinoita leimaavat edelleen datan yksityisyyteen ja suojeluun liittyvät huolet. (Subashini & Kavitha, 2011.).

Pilvipalveluihin liitetään lukuisia turvallisuushaasteita liittyen tietoturvaan, järjestelmien haavoittuvaisuuteen, verkkoturvallisuuteen, luottamukseen palvelun tarjoajan ja asiakkaan välillä, identiteetin varmistamiseen, standardeihin ja säädöksiin, suunnitteluvirheisiin, laillisuusperusteisiin, varmuuskopiointiin, kontrolliin, läpinäkyvyyteen sekä lisensointiin liittyen (Armbrust ym., 2010; Sarwar & Khan, 2013; Subashini & Kavitha, 2011; Zissis & Lekkas, 2012). Haasteita voidaan siis erotella monista lähtökohdista.

Pilvipalveluita välitetään pääosin kolmen palvelumallin kautta: SaaS, IaaS, PaaS (Subashini & Kavitha, 2011). Palvelumallit eroavat toisistaan siltä osin, minkälaisia palveluita niiden kautta välitetään. Tutkimuksen tavoitteena on eritellä eri pilvipalvelumalleihin sisältyviä turvallisuushaasteita sekä korostaa palvelumallien välistä suhdetta turvallisuuden kannalta. Lisäksi tutkitaan yleisemmän tason turvallisuushaasteita. Keskeistä on selvittää, sisällytetäänkö turvallisuushaasteita tiettyyn pilvipalvelumalliin.

Tutkimuksen tekemistä motivoi tiedottomuus siitä, miten hyvin pilvipalveluiden turvallisuusnäkökulmia tosiasiassa ymmärretään ja otetaan huomioon. Pyrkimyksenä on saada kokoon kattava kuva turvallisuushaasteista, joita eri pilvipalvelumalleihin sisältyy. Tutkimuksen tutkimuskysymykseksi asetetaan:

Mitä turvallisuushaasteita eri pilvipalvelumalleihin sisältyy?

1.3 Tutkimusmenetelmä ja tiedonhankinta

Tutkielma toteutetaan kirjallisuuskatsauksena Jyväskylän Yliopiston Tietojenkäsittelytieteiden laitoksen määrittelemän ohjeen mukaisesti. Lähteitä on pääosin etsitty Google Scholar -palvelua käyttäen. Useimmat artikkelit löytyivät tunnetuista ICT-alan tieteellisistä tietokannoista kuten Association for Computer Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE) sekä Springer. Pilviteknologiaan vihkiytyneitä lehtiä kuten Journal of Cloud Computing and Services Sciences hyödynnettiin myös. Lisäksi teknologiaan omistautuneiden instituutioiden kuten Cloud Security Alliancen julkaisuja käytettiin. Lähteiden relevanssia on arvioitu referointimäärän sekä julkaisuvuoden perusteella. Tutkielmassa on pyritty hyödyntämään mahdollisimman tuoretta tutkimustietoa, sillä pilvipalvelut ovat muodostuneet merkittäväksi ICT-alan trendiksi vasta viime vuosina. Tutkielman lähdemateriaali on pääosin julkaistu vuoden 2008 jälkeen. Lähdemateriaali on lisäksi pyritty pitämään laaja-alaisena valitsemalla lähteitä ympäri maailmaa.

Lähdemateriaalia haettiin asiasanoilla ja niiden yhdistelmillä. Ensimmäisellä hakukierroksella suodatettiin löydettyjä artikkeleita aiheen sopivuuden mukaan. Toisella kierroksella haettiin samoilla avainsanoilla artikkeleja, joissa viitattiin ensimmäisellä kierroksella löydettyihin artikkeleihin. Tällä tavoin onnistuttiin löytämään yleisimpiä lähtökohtia turvallisuushaasteisiin viitaten.

2 Pilvilaskenta ja pilvipalvelumallit

Tässä luvussa määritellään tutkielman keskeiset käsitteet: *pilvilaskenta*, *pilvipalvelu* sekä *pilvipalvelumallit*. Pilvilaskentaa lähestytään teknologialle ominaisten piirteiden kautta. Palvelumallit määritellään ja esitetään laajalti referoituja lähtökohtia mukaillen. Lisäksi sivutaan *pilviympäristöä* eri toimijoineen. Kyseisiin toimijoihin viitataan myös *aktoreilla.* Luvussa pyritään antamaan kokonaiskuva siitä, miten palveluntarjoajat välittävät palveluja asiakkaille pilviympäristössä. Tutkielmassa pilvilaskennalla viitataan englannin kielen termiin *cloud computing*. Pilvipalvelu taas viittaa termiin *cloud service*. Tässä tutkielmassa pilvilaskennan teknologioiden avulla tarjottua palvelua pidetään *pilvipalveluna*. Pilvipalvelua ja *pilveä* käytetään usein synonyymeina. On hyvä huomioida, että pilvilaskennan termistö ja määritelmät kehittyvät edelleen alan kehityksen myötä (Mell & Grance, 2009).

2.1 Pilvilaskennan määrittely

Pilvilaskennalle on useita määritelmiä, joista moni keskittyy vain tiettyyn teknologian osaan (Vaquero ym., 2008). Toisaalla todetaan, että määritelmiä tuntuu löytyvän juuri niin monta, kuin aiheeseen löytyy kommentoijiakin (Marston ym., 2011). National Institute of Standards and Technologyn (NIST) määritelmä pilvilaskennalle on paljon siteerattu – tästä syystä määritelmä valitaan tutkielmassakin keskeiseksi. Määritelmän lisäksi kootaan yleisesti pilvilaskennan ominaispiirteitä. Ominaispiirteiltään pilvipalvelut eroavat perinteisistä IT-ratkaisuista.

NIST määrittelee pilvilaskennan (engl. *cloud computing*) *malliksi, joka mahdollistaa kaikkialta saavutettavan (paikkaan sitomattoman), vaivattoman (aikaan sitomattoman) ja tarvittaessa käyttöönotettavan pääsyn internetin kautta käytettäviin tietokoneresursseihin (esimerkiksi tietoverkot, serverit, tallennustila, sovellukset ja palvelut), jotka voidaan toimittaa minimaalisin hallintaresurssein tai palveluntarjoajan vuorovaikutuksin* (Mell & Grance, 2011). Määritelmässään Mell ja Grance (2011) esittävät pilvilaskennalle viisi ominaispiirrettä:

- Tarvittaessa käyttöönotettava itsepalvelu
- Palveluun pääsy erilaisilla päätelaitteilla
- Jaetut, yhteiskäyttöiset tietokoneresurssit (engl. *resource pooling*)
- Välitön tai pikainen joustavuus
- Mitattava palvelu

Tarvittaessa käyttöönotettavalla itsepalvelulla tarkoitetaan sitä, että asiakas voi ottaa käyttöönsä tietokoneresursseja olematta ihmiskontaktissa palveluntarjoajan kanssa. Palveluita voidaan käyttää erilaisilla päätelaitteilla. Tällä tarkoitetaan sitä, miten resurssit ovat saatavilla internetin kautta (esim. selainpohjainen sovellus) monien eri päätelaitteiden kuten älypuhelimien, tablettien tai pöytäkoneiden kautta. Tietokoneresurssien yhteiskäytöllä viitataan palveluntarjoajan eri fyysisiin ja virtuaalisiin resursseihin, joita voidaan osoittaa dynaamisesti käyttäjille heidän tarpeidensa mukaisesti. Joustavuudella tarkoitetaan resurssien skaalautuvuutta sekä sisään että ulospäin sillä tavoin, että resurssit voidaan kohdentaa asiakkaan tarpeen mukaan. Palvelun mitattavuus taas viittaa siihen, että resurssien käyttöä voidaan kontrolloida ja optimoida, sillä tallennustilaa, prosessointia, kaistan käyttöä ja esimerkiksi aktiivisia käyttäjiä voidaan jollain tasolla mitata. Mittaamisen kautta voidaan edistää läpinäkyvyyttä asiakkaan ja palveluntarjoajan välillä, sillä käyttöä kyetään monitoroimaan, kontrolloimaan sekä raportoimaan tarkoituksenmukaisesti. (Mell & Grance, 2011.).

Pilvilaskennalla viitataan myös sovelluksiin, joita tarjotaan palveluina internetissä, sekä niitä pyörittäviin laitteistoihin ja järjestelmäohjelmistoihin datakeskuksissa, jotka muodostavat pohjan kyseisille sovelluksille. *Pilvellä* taas tarkoitetaan datakeskusten laitteistoja ohjelmistoineen. (Armbrust ym., 2010.).

Vaquero ym. (2008) kokoavat artikkelissaan vallitsevia määritelmiä pilvilaskennalle. He ovat koonneet yhteen seuraavat kirjallisuudessa toistuneet pilvilaskennan ominaispiirteet (Vaquero ym., 2008):

- Käyttäjäystävällisyys (engl. *User Friendliness*)
- Virtualisointi (engl. *Virtualization*)
- Internetkeskeisyys (engl. *Internet Centric*)
- Resurssien monimuotoisuus (engl. *Variety of Resources*)
- Automaattinen sopeutuminen (engl. *Automatic Adaptation*)
- Skaalautuvuus (engl. *Scalability*)
- Resurssien optimointi (engl. *Resource Optimization*)
- Veloitus käytön perusteella (engl. *Pay per Use*)
- Palvelutasosopimukset (engl. Service SLAs)
- Infrastruktuuritasosopimukset (engl. *Infrastructure SLAs*)

Buyya, Pandey ja Vecchiola (2009a) vertailevat määritelmänsä pohjaksi pilvilaskentaa klusterilaskentaan (engl. *cluster computing)* ja ristikkäislaskentaan (engl. *grid computing).* He määrittelevät pilven *rinnakkaiskäytettäväksi ja jaettavaksi systeemiksi, joka koostuu kokoelmasta keskenään yhteydessä olevia ja virtualisoituja tietokoneita, joiden resursseja voidaan välittää dynaamisesti* (Buyya ym., 2009b). Palvelun ja resurssien taso perustuu asiakkaan ja palveluntarjoajan välille neuvoteltuihin palvelutasosopimuksiin (engl. *service level agreement, SLA).* Pilvelle omi-

naisiksi piirteiksi määritellään *vahva tuki virtualisoinnille* sekä *dynaamisesti kohdennettavat palvelut*, joita välitetään *internetkäyttöliittymien* kautta. (Buyya ym., 2009a.).

Marston ym. (2011) toteavat pilven keskeisen teknologian koostuvan *monikäytöstä, virtualisoinnista* ja *internetpalveluista.* Monikäyttö (engl. *multitenancy*) tarkoittaa yhden ohjelmiston kykyä palvella monia asiakkaista siten, että jokaisen käyttäjän päätteelle ei tarvitse erikseen asentaa ohjelmistoa (Marston ym., 2011). Internetpalvelulla viitataan W3C:n määritelmään, jonka mukaan internetpalvelu on *ohjelmistosysteemi, joka on suunniteltu tukemaan yhdessä toimivaa päätteestä päätteeseen vuorovaikutusta tietoverkon välityksellä* (W3C, 2004). Virtualisoinnin avulla piilotetaan käyttäjältä laitealustan fyysiset piirteet siten, että käyttäjä havaitsee ainoastaan abstraktin laitealustan (Marston ym., 2011).

2.2 Pilvipalvelumallit

Useassa lähteessä pilvipalvelut määritellään välitettävän kolmen palvelumallin kautta (Banerjee ym., 2011; Khorshed, Ali & Wasimi, 2012; Marston ym., 2011; Mell & Grance, 2011; Ojala, 2012; Sadashiv & Kumar, 2011; Zissis & Lekkas, 2012). Tämän yleisen erottelun lisäksi erotetaan monia muita palvelumalleja, kuten tallennustila palveluna (engl. *Datastorage-as-a-Service*), työpöytä palveluna (engl. *Desktop-as-a-Service*), tietoturva palveluna (engl. *Security-as-a-Service*), viestintä palveluna (engl. *Communication-as-a-Service*), liiketoimintaprosessit palveluna (engl. *Business process-as-a-Service*) tai holistisesti x/kaikki palveluna (engl. *X-as-Service* ja *Everything-as-a-Service*) (Kumar, 2012; Rimal, Choi & Lumb, 2009). Yleisesti palvelumalleja kuitenkin jaotellaan seuraavasti:

- Sovellukset palveluna (engl. *Software-as-a-Service, SaaS*)
- Sovellusalusta palveluna (engl. *Platform-as-a-Service, PaaS*)
- Infrastruktuuri palveluna (engl. *Infrastructure-as-a-Service, IaaS*)

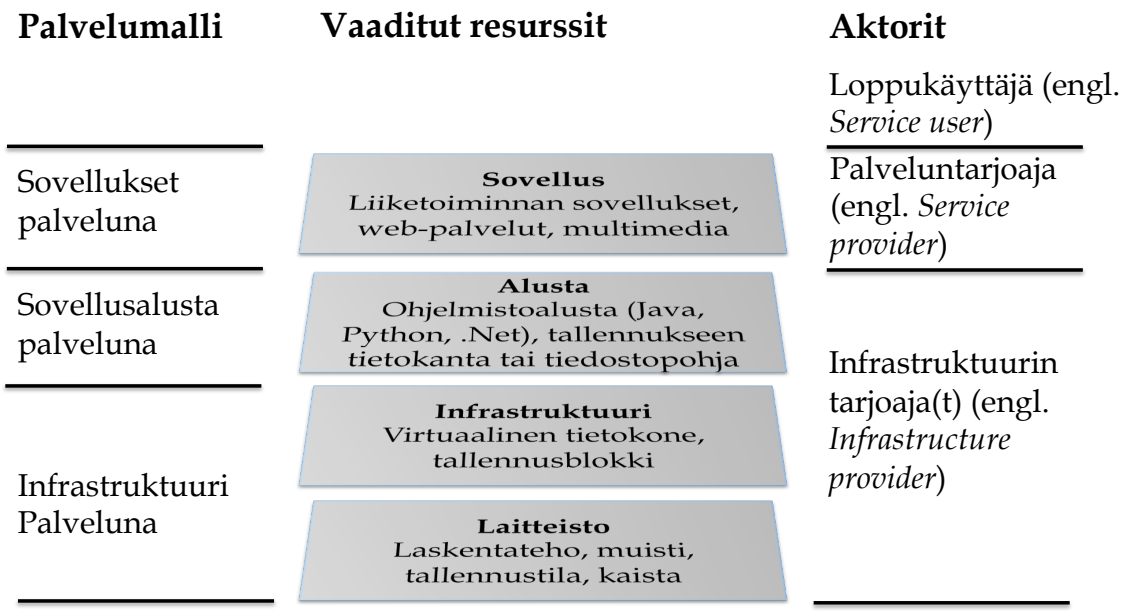
Infrastruktuurilla (IaaS) luodaan palveluille alusta (PaaS), jonka päälle voidaan edelleen toteuttaa ohjelmistoja (SaaS) (Subashini & Kavitha, 2011). Palveluarkkitehtuuri voidaan nähdä kerrostuneena kokonaisuutena. On kuitenkin hyvä ottaa huomioon, että palveluntarjoajat voivat olla täysin erillisiä toisistaan.

Pohjimmainen taso, IaaS, mullisti tavan, jolla liiketoiminta nykyään investoi IT-infrastruktuuriin (Fernandes ym., 2013). Tällä tasolla tarjotaan palveluntarjoajille perustietokoneresursseja, kuten tallennus- ja prosessointikapasiteettia sekä verkkoyhteyksiä, joiden päälle palveluntarjoajat voivat käyttöjärjestelmin sekä ohjelmistoin kehittää palvelujansa (Mell & Grance, 2011). Virtualisoinnin avulla voidaan jakaa ja kohdentaa resursseja palveluntarjoajien tarpeen mukaisesti (Vaquero ym., 2008). Mallin myötä poistui asiakkaan tarve investoida omaan IT-infrastruktuuriin ja sen hallintaan. Massiivisten investointien sijaan asiakkaan on mahdollista keskittyä ydintoimintaansa ja maksaa ainoastaan resursseista, joita käytetään. (Fernandes ym., 2013.). Esimerkkeinä infrastruktuu-

rista palveluna voidaan pitää Amazonin S3- ja EC2 -palveluita (Marston ym., 2011).

Sovellusalustalla (PaaS) voidaan lisätä abstraktiotasoa tarjoamalla infrastruktuurin lisäksi valmis ohjelmisto- tai kehitysalusta, jossa palveluntarjoaja voi kehittää ja ajaa sovelluksiaan (Buyya ym., 2009b; Vaquero ym., 2008; Fernandes ym., 2013). Hyviä esimerkkejä sovellusalustoista palveluna ovat Microsoftin Azure -palvelualusta sekä Googlen AppEngine (Marston ym., 2011).

Palveluarkkitehtuurin päällimmäisellä tasolla tarjotaan ohjelmistoja palveluna (Buyya ym., 2009b). SaaS ei niinkään viittaa tapaan, jolla ohjelmistoja kehitetään, kuten PaaS, vaan enemmänkin liiketoimintamalliin, jolla ohjelmistoja toimitetaan (Fernandes ym., 2013). SaaS-malli parantaa asiakkaan operationaalista tehokkuutta siirtämällä vastuun ohjelmiston päivittämisestä ja ylläpidosta palveluntarjoajalle (Fernandes ym., 2013). Tällä palvelutasolla käyttäjä ei pääse hallinnoimaan palvelua henkilökohtaisia konfiguraatioasetuksia syvemmin, mutta saa pääsyn ja käyttöoikeuden ohjelmistoihin, joita pilvipalveluntarjoaja isännöi (Mell & Grance, 2011). Sovelluksia palveluna tarjoavat esimerkiksi Google Apps -ohjelmistot, Salesforce sekä henkilökohtaiset selainsovellukset kuten Twitter, Facebook ja Gmail (Marston ym., 2011). Alla olevalla kuvalla (kuvio 1) havainnollistetaan palveluarkkitehtuuria sekä aktoreita, jotka muodostavat *pilviympäristön.*



KUVIO 1 Pilviympäristö (Zhang, Cheng & Boutaba, 2010)

Kaikkien palvelumallien käytännön operointi toteutetaan IT-infrastruktuurin avulla. IT-infrastruktuuriin kuuluvat esimerkiksi tilat, joihin laitteisto (esim. serverit ja verkkolaitteet) järjestetään, sekä käyttöjärjestelmät, joilla laitteistoa hallitaan. Palvelumallien päällä toimii tietoverkko, useimmiten Internet, jonka

kautta palveluita välitetään pilvien ja asiakkaiden välillä. (Fernandes ym., 2013.).

Pilvipalveluja voidaan jaotella myös toteutustavan perusteella. NIST erottelee neljä toteutustapaa pilvipalveluille, joita mukaillaan alla (Mell & Grance, 2011). Toimitustapoja ei tutkielman viitekehyksessä huomioida, mutta todellisuudessa ne kuitenkin vaikuttavat turvallisuushaasteisiin merkittävästi.

- *Julkinen pilvi* (engl. *public cloud*) viittaa pilveen, joka on julkisesti avoin ja vapaasti itsepalveluna käyttöönotettavissa. Resursseja voidaan tarjota käyttöön korvausta vastaan (Rimal ym., 2009).
- *Yhteisöllinen pilvi* (engl. *community cloud*) vastaa käytännössä samaa kuin yksityinen pilvi, mutta käyttö voidaan jakaa monen samaa tarvetta kokevan asiakkaan kesken.
- *Hybridipilvi* (engl. *hybrid cloud*) on yhdistelmä kahdesta tai kolmesta yllämainitusta toimitustavasta.
- *Yksityisessä pilvessä* (engl. *private cloud*) infrastruktuuri tarjotaan asiakkaan omaan käyttöön. Vastuu pilven ylläpidosta voi olla joko asiakkaalla itsellään tai kolmannella osapuolella. Datan ja prosessien ollessa asiakkaan omassa hallinnassa, eivät julkisten pilvien tietoverkkojen kaistanleveyden, turvallisuuden tai laillisuusvaatimusten tuomat rajoitteet ole niin huomattavia.

NIST:n erottelemat toimitustavat ovat laajalti referoituna alan tutkimuksessa (Aguiar, Zhang & Blanton, 2014; Gul, Rehman & Islam, 2011; Wang, Wang, Ren & Lou, 2009; Sabahi, 2011; Subashini & Kavitha, 2011; Yang & Chen, 2010). Yllä lueteltujen toimitustapojen lisäksi kirjallisuudessa erotetaan harvemmin esiintyvä toimitustapa: virtuaalinen yksityinen pilvi (engl. *virtual private cloud*, VPC) (Fernandes ym., 2013; Zhang ym., 2010). VPC:llä viitataan alustaan, jota ajetaan minkä hyvänsä yllä luetellun toimitustavan päällä (Fernandes ym., 2013). VPC hyödyntää virtuaalista erillisverkkoa, tuttavallisemmin VPN-teknologiaa, jonka avulla voidaan tarjota eristettyjä resursseja asiakkaille (Fernandes ym., 2013; Zhang ym., 2010). VPN mahdollistaa palveluntarjoajalle omien turvallisuusasetusten, kuten palomuurisääntöjen, hyödyntämisen (Zhang ym., 2010).

2.3 Pilvipalvelumallien soveltaminen

Marston ym. (2011) toteavat, että pilvipalvelut madaltavat kynnystä IT-innovointiin. Heidän mukaansa pilvien avulla markkinoille voidaan tuoda täysin uudenlaisia sovelluksia. Esimerkiksi esitetään mobiilisovelluksia, jotka ovat tietoisia päätelaitteen sijainnista, ympäristöstä ja kontekstista siten, että sovellukset voivat reaaliajassa olla vuorovaikutuksessa käyttäjään joko sensorisen, käyttäjän antaman tai riippumattoman tietolähteen tarjoaman informaation avulla. (Marston ym., 2011.). Konkreettinen esimerkki on esimerkiksi sääsovellus, joka puhelimen sijaintiin pohjautuen hakee dataa sääpalveluiden tarjoamista ennusteista ja informoi käyttäjää sään muutoksista. Voidaan olettaa, että pil-

vipalvelupohjaisia vuorovaikutuksellisia sovellusinnovaatioita kehitetään yhä enemmän. Seuraavassa taulukossa (taulukko 1) esitetään pilvipalveluiden sovellusmahdollisuuksia palvelumalleittain.

SaaS	**PaaS**	**IaaS**
Sähköposti	Business Intelligence	Varmuuskopiointi
Toimistotyökalut	Tietokannat	Palautuspalvelut
Laskutus	Kehitysalustat	Tallennuskapasiteetti
Asiakassuhteen	Testausalustat	Raakadatan säilytys
hallinta	Integraatiosovellukset	Serveriresurssit
Sisällönhallinta	Alustat sovellusten	Palveluiden hallinta
Dokumenttien hallinta	välittämiseen	Sisällön välitys
Yhteistyövälineet		verkot (engl. *Content*
Varainhallinta		*Delivery Networks*)
Myyntityökalut		
Sosiaaliset verkot		
ERP		

TAULUKKO 1 Pilvipalvelujen sovelluksia (Liu ym., 2011)

3 Pilvipalvelumallien turvallisuushaasteet

Luku on tutkielman pääluku. Aluksi luodaan yleiskuva turvallisuudesta pilvipalveluiden kontekstissa sekä avataan palvelumallien riippuvuussuhteita. Seuraavaksi käsitellään toimijoiden vastuun jakautumista. Kolmas alaluku on luvussa keskeisin. Siinä tutustutaan turvallisuushaasteiden luokitteluihin, sekä esitellään pilvipalveluihin sisältyviä turvallisuusuhkia. Uhkien jatkoksi esitellään kirjallisuudesta löytyneitä pilvipalvelumalleittain jaoteltuja turvallisuushaasteita. Jaottelulla vastataan tutkielman tutkimuskysymykseen. Neljännessä alaluvussa käsitellään haasteiden käsittelyn haasteellisuutta, sekä turvallisuusnäkökulmia, jotka ovat yleisemmällä tasolla, eivätkä suoraan liitettävissä palvelumalleihin.

3.1 Turvallisuus pilvipalveluiden kontekstissa

Pilvipalveluiden avulla asiakas voi välttää start-up-kustannuksia, pienentää operationaalisia kustannuksia sekä parantaa ketteryyttä saamalla tietoresursseja ja palveluita välittömästi käyttöön tarpeen ilmaantuessa. Hyötyjen lisäksi on huomioitava turvallisuuden ja yksityisyyden näkökulmat, joihin pilvipalvelujen erityiset arkkitehtuuriset ominaisuudet tuovat monenlaisia haasteita. Turvallisuus- ja yksityisyysnäkökulmien ymmärtäminen sekä oikeiden ratkaisujen löytäminen niiden huomioimiseksi on kriittistä myös pilvipalvelun menestymisen kannalta. (Takabi ym., 2010.).

Turvallisuuskysymyksiä voidaan pohtia monista näkökulmista, joka selvästi jakaa tutkimuskenttääkin. Fernandes ym. (2013) kiteyttävät, että vaikka pilvipalveluiden ominaispiirteet ovat melko hyvin ymmärretty, ovat turvallisuusseikat edelleen arvoituksellisia. Tutkimuksessaan he kartoittavat kattavasti pilvipalveluiden tutkimuskenttää. He löytävät, että jopa 322 artikkelia 504:stä pilvispesifistä artikkelista keskittyvät turvallisuuteen vuosien 2008 ja 2012 aikana (Fernandes ym., 2013). Voitaneen todeta, että pilvipalveluiden turvallisuus on alan tutkimuksessa keskeistä.

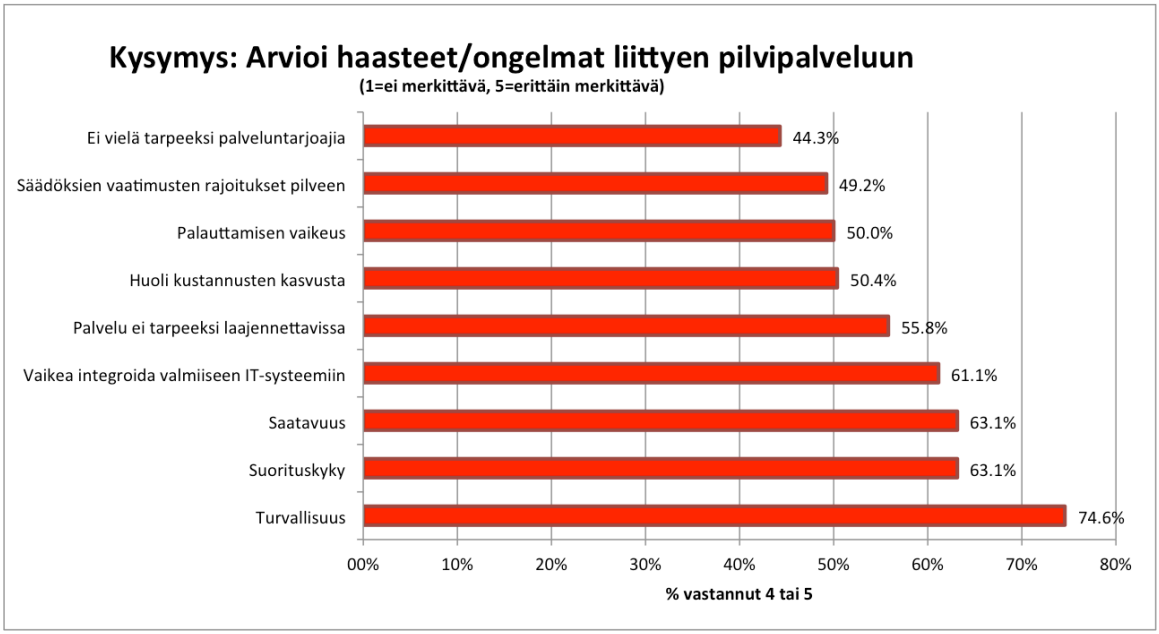
Turvallisuudella viitataan pilvipalveluiden kontekstissa usein tietoturvaan, jolla tarkoitetaan keinoja suojata informaatiota ja ympäröiviä systeemejä luvattomalta pääsyltä, käytöltä, julkaisulta, keskeytyksiltä, muokkaamiselta tai tu-

hoamiselta (Liu ym., 2011). Yksityisyydellä viitataan yksityistiedon (engl. *personal information*) ja yksityiseksi tunnistettavan tiedon (engl. *personally-identifiable information*) varmistettuun, kunnolliseen ja johdonmukaiseen keräämiseen, prosessointiin, viestimiseen sekä käyttöön (Liu ym., 2011).

Pilvipalveluissa asiakkaan data on tallennettuna suuriin datakeskuksiin, jotka tarjoavat myös prosessointitehoa. Asiakkaalla ei välttämättä ole eksaktia tietoa prosessoivasta serveristä tai tallennustilasta, tai edes niiden sijainnista. Asiakas joutuu siis suurilta osin luottamaan palveluntarjoajaan datan saatavuuden ja turvallisuuden suhteen. Luottamusta rakennetaan palvelutasosopimuksin (engl. *Service Level Agreement, SLA*), joissa dokumentoidaan asiakkaan ja palveluntarjoajan välinen suhde tarpeineen, vastuineen ja vaatimuksineen. (Kandukuri ym., 2009.).

Ensisijaisen tärkeää pilvipalveluiden kannalta on datakeskusten turvallisuus. Datakeskukset rakennetaan usein geologiset ja ympäristölliset seikat kuten sijainti, lämpötila, kosteus sekä maanjäristysriski huomioon ottaen (Fernandes ym., 2013). Muita aspekteja liittyen datakeskusten turvallisuuteen ovat poliittiset, hallinnolliset sekä energian kulutukseen ja säästöön liittyvät seikat (Fernandes ym., 2013). Chow ym. (2009) mukaan pilvipalveluntarjoajat väittävät toiminta-ajan jatkuvuuden (engl. *uptime*) vastaavan hyvin sitä, mitä jatkuvuus olisi käyttäjän yksityiselläkin datakeskuksella. Fernandes ym. (2013) mukaan palveluntarjoajat varmistavat toiminta-ajan (jopa 99,99%) sekä virheensiedon juuri vahvojen fyysisten perustuksien kautta.

Turvallisten datakeskusten varmistamisen lisäksi itse datan turvallisuuden takaaminen on pilviympäristössä hankalaa, sillä jokaisella palvelutasolla (infrastruktuuri, alusta, ohjelmisto) on omat huolensa turvallisuuden suhteen (Kandukuri ym., 2009). Turvallisuutta pidetään suurimpana pullonkaulana alan kasvussa. Lisäksi markkinoita leimaavat edelleen huolet datan yksityisyydestä ja suojasta. Mitä enemmän informaatiota pilviin tallennetaan, sitä suuremmaksi on kasvanut myös huoli niiden turvallisuudesta. (Subashini & Kavitha, 2011.). International Data Corporationin (IDC) tutkimus osoittaa (kuvio 2), että turvallisuuden hallintaa on pidetty vuonna 2008 suurimpana haasteena pilvipalveluita implementoidessa (Gens, 2008).

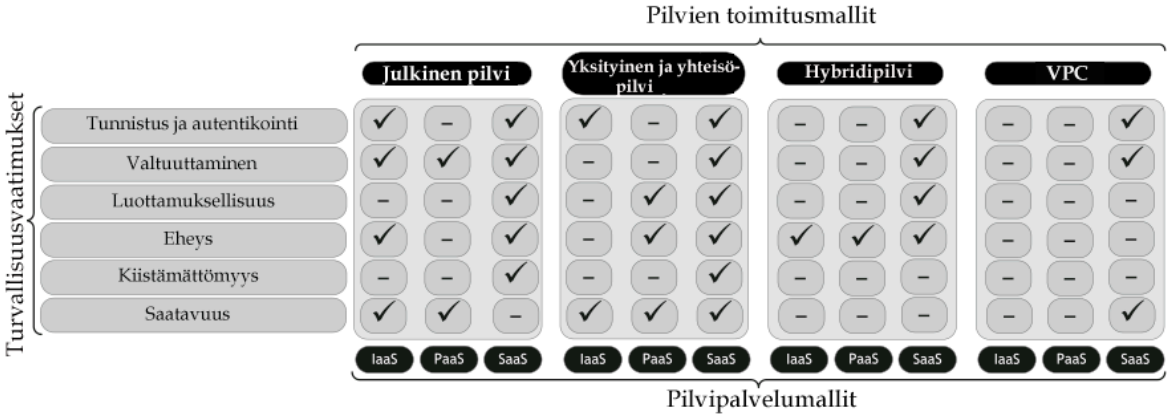


KUVIO 2 Pilvipalvelujen haasteita (Gens, 2008)

On huomattava, että turvallisuusaspekti liittyy kaikkiin pilviympäristön palvelutasoihin aina fyysisistä tietoresursseista palveluina tarjottaviin sovelluksiin (Liu ym., 2011). Kokonaisarkkitehtuuri rakentuu päällekkäisistä palveluista: infrastruktuuri (IaaS) luo palvelulle pohjan, jonka päälle rakennetaan sovellusalusta (PaaS), johon edelleen kehitetään sovelluksia (SaaS) (Subashini & Kavitha, 2011). Koska sekä palvelujen ominaisuudet, että tietoturvariskit periytyvät aina alemmalta palvelumallilta ylemmälle, voidaan sanoa, että palvelumallit asettavat eritasoisia vaatimuksia turvallisuudelle ja yksityisyydelle (Subashini & Kavitha, 2011; Takabi ym., 2010). Samaisesta syystä turvallisuutta ei voida asettaa yksittäisen aktorin vastuulle, vaan vastuu jakautuu kaikkien aktorien kesken, joskaan ei tasaisesti (Liu ym., 2011). Voidaan ajatella, että mitä alemmaksi palveluntarjoaja palvelumalleissa asettuu, sitä suuremmaksi muodostuu asiakkaan vastuu turvallisuuden varmistamisesta ja hallinnasta (Brunette & Mogull, 2009). Edelleen voidaan todeta, että vastuut turvallisuudesta palveluntarjoajan ja asiakkaan välillä vaihtelevat paljon palvelumalleittain (Subashini & Kavitha, 2011). Yleisesti pilvipalvelusysteemin täytyy Liu ym. (2011) mukaan varmistaa seuraavia turvallisuusvaatimuksia:

- käyttäjän tunnistaminen, autentikointi
- valtuuttaminen, autorisointi
- palvelun saatavuus
- luottamuksellisuus
- identiteetin hallinta
- datan koskemattomuus, eheys
- tarkastettavuus
- turvallisuuden monitorointi
- tapaturmaan reagointi

Ramgovind ym. (2010) ovat visualisoineet pilvipalveluiden turvallisuusvaatimuksia toimitus- ja palvelumalleittain.



KUVIO 3 Pilvipalvelujen turvallisuusvaatimuksia (Ramgovind ym., 2010)

3.2 Vastuun jakautuminen palvelumalleittain

Kuten edellä todettiin, vastuu pilvipalveluiden turvallisuudesta ei jakaudu tasaisesti. Pilvipalveluiden parissa on erityisen tärkeää huomioida organisaation (asiakkaan) ja palveluntarjoajan roolit sekä vastuut, eritoten riskien hallinnan ja palveluvaatimusten suhteen (Jansen & Grance, 2011). Armbrust ym. (2010) mukaan pilvipalveluihin liitetään monia samoja turvallisuushaasteita kuin suuriin datakeskuksiin. Heidän mukaan erottava tekijä pilvipalveluiden haasteissa on kuitenkin se, että vastuu jakautuu potentiaalisesti monen sidosryhmän kesken (Armbrust ym., 2010).

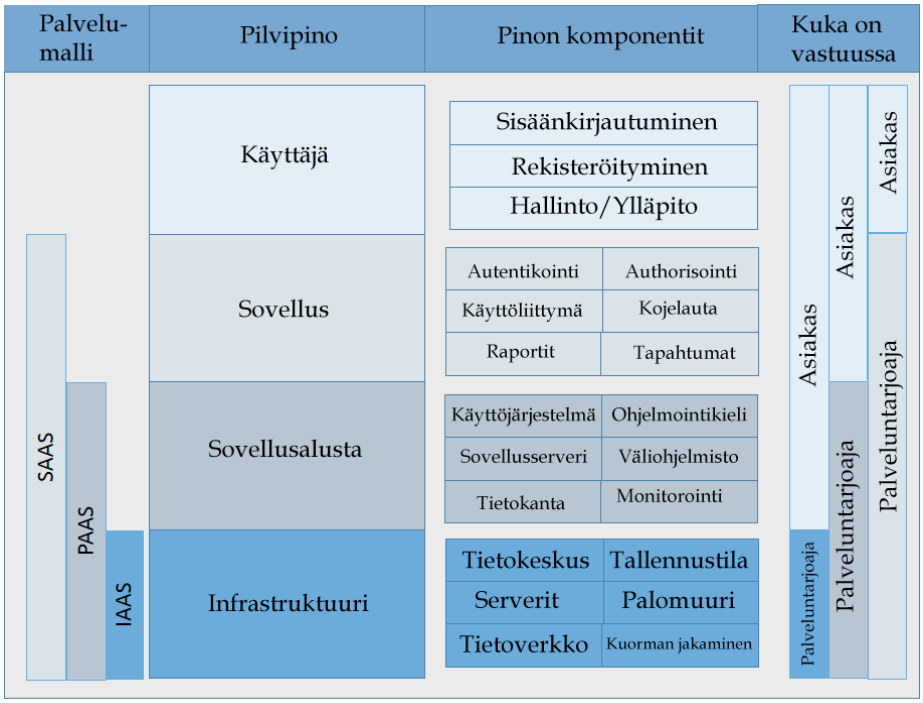
Yleisesti SaaS-tasolla palveluntarjoajat tarjoavat asiakkaille valmiiksi integroituja toimintoja. Toiminnot on "paketoitu" valmiiksi sillä tavoin, että asiakkaalle ei jää mahdollisuuksia laajentaa palvelua. Näin ollen vastuu palvelun turvallisuudesta jää enimmäkseen palveluntarjoajalle. SaaS-tasolla palvelun taso, turvallisuus, valvonta sekä odotukset vastuun ja palveluntarjoajan suhteen tulee neuvotella palvelusopimuksiin. (Brunette & Mogull, 2009.). Lisäksi täytyy muistaa, että vastuu tarkoituksenmukaisesta palvelun käytöstä, laillisuusperusteista sekä yksilötason tietoturvasta ovat kaikissa tapauksissa myös loppukäyttäjän (kuviossa 4 käyttäjän) vastuulla.

PaaS-tasolla asiakkaalle tarjotaan alusta, jonka päälle asiakas voi kehittää sovelluksia. Tästä syystä alustan on oltava laajennettavampi, mikä tarkoittaa sitä, että alustasta karsitaan myös valmiiksi integroituja turvallisuusominaisuuksia. Vastuu alustan ja sovelluksen turvallisuudesta siirtyy enemmän asiakkaalle, mutta avaa samaan aikaan mahdollisuuksia lisätä turvallisuutta tarpeiden mukaan. (Brunette & Mogull, 2009.). Palveluntarjoajan vastuu tietoturvasta siis kevenee verrattuna SaaS-tasoon.

IaaS-tason palvelun tulee olla mahdollisimman hyvin laajennettavissa. Käytännössä siis vastuu sovellustason (käyttöjärjestelmät, ohjelmistot, sisältö) hallinnasta ja turvallisuudesta siirtyy asiakkaalle siten, että palveluntarjoaja on

vastuussa ainoastaan laitteiston ylläpidosta ja käynnissä pitämisestä. (Brunette & Mogull, 2009.). Subashini ja Kavithan (2011) mukaan infrastruktuurin palvelutasolla korkeamman tason turvallisuus jää asiakkaan vastuulle, sekä vaatimuksiksi pilveen siirrettäville ohjelmistoille.

Michael Kavis (2014) selkeyttää blogissaan (kavistechnology.com, viitattu 4.3.2014) pilviympäristöä, sekä eritoten vastuun jakautumista palvelumalleittain. Kuvio 4 havainnollistaa sitä, miten asiakkaan ja palveluntarjoajan vastuut jakautuvat palvelumalleittain, sekä minkälaisia komponentteja vastuualueisiin liittyy.



KUVIO 4 Vastuun jakautuminen palvelumalleittain (Kavis, 2014)

On keskeistä huomata, miten pilviasiakkaat (kuviossa 4 asiakkaat) ovat vastuussa sovellustason turvallisuudesta samaan aikaan, kun pilventarjoajat (kuviossa 4 palveluntarjoajat) ovat vastuussa fyysisen ja loogisen tason turvallisuudesta (Fernandes ym., 2013). Vastuu jakautuu aktorien kesken välissä olevilla palvelutasoilla.

3.3 Turvallisuushaasteet ja -uhat pilvipalvelumalleittain

Turvallisuushaaste on yleinen termi, jolla kuvataan esimerkiksi tapahtumaa tai toimintaa, joko ohjelmiston tai laitteiston toimimatonta kokoonpanoa tai sovelluksen aukkoja, jotka eivät toimi oletettavalla tavalla turvallisuuden kontekstissa (Fernandes ym., 2013). Tietoturvan tutkimuskentällä sovelletaan monia termejä kuten *uhkaa*, *haavoittuvuutta, hyökkäystä* tai *riskiä* kuvaamaan kyseessä ole-

vaa aihetta. Uhka on toiminta tai tilanne, jossa voidaan hyödyntää olemassa olevaa haavoittuvuutta (Dahbur, Mohammad & Tarakji, 2011). Haavoittuvuudella taas tarkoitetaan virhettä tai heikkoutta systeemissä, johon uhka kohdistuu (Dahbur ym., 2011). Riskillä tarkoitetaan todennäköisyyttä, jolla uhan toteuttaja hyödyntää haavoittuvuutta (Fernandes ym., 2013). Riski realisoituu yleensä hyökkäyksen ja liiketoimintaa heikentävien vaikutusten muodossa (Fernandes ym., 2013). Tässä tutkielmassa pyritään keskittymään haasteisiin, joita pilvipalvelumalleihin sisältyy. Lisäksi lähdekirjallisuudessa viitataan *vaatimuksiin*, joita pilvijärjestelmälle asetetaan. Tutkielmassa vaatimusten katsotaan tarkoittavan samaa kuin haasteet.

Pilvipalveluiden turvallisuushaasteita erotellaan lähdekirjallisuuden perusteella palvelumalleittain hyvin rajoitetusti. Tutkielman näkökulma on tässä mielessä haastava, mutta jättää varaa pohdinnalle. Lähdekirjallisuudesta havaitaan, että turvallisuushaasteita luokitellaan monin eri perustein. Esimerkiksi Grobauer, Walloschek ja Stocker (2011) luokittelevat turvallisuushaasteita *pilvispesifisiin* ja *yleisiin* haasteisiin. Zissis ja Lekkas (2012) luokittelevat uhkia viiteen eri kategoriaan: *tilinhallinta*, *pahansuovat sisäpiiriläiset*, *konsolin turvallisuuden hallinta*, *datan kontrolli* sekä *monikäytön haasteet*. Tämän luokittelun lisäksi he erottelevat haasteita erikseen palvelumalleittain, kuten tekevät myös Subashini ja Kavitha (2010). Sengupta, Kaulgud & Sharma (2011) taas jaottelevat haasteita neljään kategoriaan, joista ensimmäinen on pilven *infrastruktuuri, alusta ja isännöity koodi*. Toisena kategoriana he esittelevät *datan*, kolmantena *pääsyn* sekä viimeisenä, neljäntenä kategoriana, *sääntöjen noudattamisen* (Sengupta ym., 2011). Kattavimman viitekehyksen pilvipalveluiden turvallisuushaasteisiin tarjoaa Fernandes ym. (2013). Heidän luokittelunsa pohjautuu kahdeksaan kategoriaan, jota mukaillaan taulukossa 2.

Turvallisuushaasteiden luokittelu	
Pääsy	Fyysinen pääsy, valtuudet, autentikointi, authorisointi, identiteetin hallinta, anonymiteetti
Tallennus ja laskentateho	Datan tallennus, epäluotettava laskentateho, saatavuus, salausmenelmät, levyn puhdistus/ siivous, haittaohjelmat
Ohjelmisto	Alustat ja viitekehykset, käyttöliittymä
Virtualisointi	Levyosien hallinta, virtuaalikoneiden monitorointi, virtualisoidut verkkoratkaisut, liikkuvuus, virtuaalikoneiden tasot, haittaohjelmat, saatavuus
Sääntöjen noudattaminen ja laillisuusperusteet	Hallinto, vastuuvelvollisuus, laillisuusongelmat, asetukset, rikostekniset velvollisuudet
Tietoverkko	Mobiilialustat, kehän turvallisuus
Luottamus	Pilveen siirtyminen, ihmisfaktori, maine, anonymiteetti, tarkastettavuus
Internet ja palvelut	APT:t (engl. *Advanced persistent threat)* ja pahansuovat ulkopuoliset, protokollat ja standardit, web-palvelut ja –teknologiat, saatavuus

TAULUKKO 2 Turvallisuushaasteiden luokittelua (Fernandes ym., 2013)

Yllä luetelluista jaotteluista huomataan, että haasteiden jaottelua harvemmin tehdään pohjautuen pilvipalveluiden toimitustapoihin tai palvelumalleihin. Suoraan palvelumalleittain turvallisuushaasteita havaittiin lähdekirjallisuudessa eroteltavan vain kahdessa artikkelissa (Subashini & Kavitha, 2010; Zissis & Lekkas, 2012).

Cloud Security Alliance (CSA) jaottelee turvallisuusuhkia palvelumalleittain. Nämä uhat ovat kirjallisuudessa laajasti referoituna, tästä syystä tutkielmassakin jaottelu otetaan lähtökohdaksi. Taulukossa 3 esitetään CSA:n määrittelemät uhat, jotka on järjestetty vakavuuden mukaan siten, että ylintä uhkaa pidetään vakavimpana (CSA, 2013).

Uhkien jaottelu palvelumalleittain	IaaS	PaaS	SaaS
1. Datan vuotaminen	x	x	x
2. Datan katoaminen	x	x	x
3. Tilin tai palvelun kaappaus	x	x	x
4. Turvattomat käyttöliittymät ja API:t	x	x	x
5. Palvelunestohyökkäykset	x	x	x
6. Pahansuovat sisäpiiriläiset	x	x	x
7. Pilvipalvelujen rikollinen hyödyntäminen ja hyväksikäyttö	x	x	
8. Puutteellinen tarpeen kartoitus (engl. *due diligence*)	x	x	x
9. Jaetun teknologian haasteet (eristys ja monikäyttö)	x	x	x

TAULUKKO 3 Uhkien jaottelu palvelumalleittain (CSA, 2013)

CSA ei, kuten taulukosta huomataan, jätä montaa solua tyhjäksi. Vaikuttaa siltä, että CSA:n tulkinnassa kaikki uhat liittyvät lähes kaikkiin palvelumalleihin. CSA:n uhkien jaottelu selittää osaltaan havaintoa siitä, että haasteiden jaottelua tehdään hyvin vähän palvelumalleittain. Voidaankin kysyä, miksi haasteita jaoteltaisi palvelumalleittain, jos lähes kaikkiin palvelumalleihin kohdistuu samat uhat? Tutkielman näkökulmassa turvallisuusuhkiin vastataan haasteiden ja vaatimusten kautta.

Palvelumalleista SaaS on se malli, joka palvelee yhä laajemmin yritysten IT-palveluja (Subashini & Kavitha, 2011). Palvelumallin kautta saavutetaan operationaalista tehokkuutta ja kevyempi kulurakenne. Silti monet yritykset joutuvat kokemaan epämukavuutta SaaS:n parissa, sillä malli ei tarjoa kattavaa läpinäkyvyyttä siihen, miten yrityksen tiedot ovat tallennettu ja suojattu. Huolet palveluntarjoajan sisäisistä väärinkäytöksistä, ohjelmistojen haavoittuvuudesta sekä systeemien saatavuudesta herättävät pelkoa arkaluonteisen datan tai taloudellisen edun menettämisestä. (Subashini & Kavitha, 2011.).

Zissis ja Lekkas (2011) sekä Subashini ja Kavitha (2011) erottelevat kullekin palvelumallille ominaisia turvallisuushaasteita. Taulukkoon 4 on koottu turvallisuushaasteita, joita he sisällyttävät SaaS-palvelumalliin.

Subashini ja Kavitha (2011)	Zissis ja Lekkas (2012)
Datan turvallisuus, sijainti, eheys, rikkoutuminen, luottamuksellisuus ja erottelu	Yksityisyys monikäyttöympäristöissä
Virtualisoinnin haavoittuvaisuus	Datan suojelu paljastumiselta (engl. *Exposure*)
Dataan pääsy, identiteetin hallinta ja sisäänkirjautumisprosessi; todentaminen (engl. *Authentication*) ja valtuuttaminen (engl. *Authorization*)	Pääsyn kontrollointi
Tietoverkon turvallisuus	Viestiyhteyksien suojelu
Internetsovelluksen turvallisuus, varmuuskopiointi	Ohjelmistojen turvallisuus
Palvelun saatavuus	Palvelun saatavuus

TAULUKKO 4 Turvallisuushaasteita SaaS-palvelutasolla

Yllä olevien haasteiden lisäksi täytyy ottaa huomioon esimerkiksi internetselainten turvallisuus, sillä SaaS-palvelut ovat enimmäkseen selainpohjaisia sovelluksia (Liu ym., 2011). On huomioitava, että palvelumallien kerrostuneisuus tuo kompleksisuutta haasteiden käsittelyyn, sillä yksittäinen haaste voi liittyä yhteen tai useampaan palvelumalliin. Esimerkiksi pääsyn kontrollointi on varmasti haaste kaikilla palvelutasoilla.

PaaS tarjoaa kehitysympäristön, jossa kehittäjät voivat rakentaa ohjelmistoja tietämättä tarkemmin, minkälaisen infrastruktuurin päällä kehitystä tehdään. Kehitysympäristöä ja käyttöjärjestelmää pyörittävä infrastruktuuri voidaan nähdä abstraktina kehittäjän näkökulmasta. PaaS on yleensä SaaS:ia laajennettavampi ja muokattavampi, sisältäen vähemmän sisäänrakennettuja turvallisuusominaisuuksia. Tämä voi luoda kehittäjälle, joka on tällä tasolla myös asiakkaan roolissa, joko haasteen ylläpitää tai mahdollisuuden lisätä turvallisuutta alustassa. (Subashini & Kavitha, 2011.). Zissis ja Lekkas (2012) erottelevat turvallisuusvaatimuksia fyysiselle sekä ohjelmisto- ja virtuaalitasoille. Heidän näkökulmassaan sekä PaaS että IaaS kuuluvat ohjelmisto- ja virtuaalitasoon. Tällä tasolla he korostavat turvallisuushaasteina pääsyn kontrollointia, ohjelmistojen turvallisuutta, datan turvallisuutta (data liikkeessä, data levossa, datan rippeet (engl. *remanence*)), pilven hallinnan kontrollointia, turvallisia virtualisoituja osioita (engl. *images*) sekä niiden suojaa, sekä lisäksi viestiyhteyksien turvallisuutta. (Zissis & Lekkas, 2012.).

IaaS mahdollistaa yrityksille helposti käyttöönotettavia tietoresursseja, joiden avulla yritykset voivat keskittyä ydinosaamiseensa kohdentamatta resursseja IT-infrastruktuurin hankintaan ja hallintaan. Kustannusten kannalta järjestelyllä saavutetaan säästöä, mutta palveluna hankittu infrastruktuuri tarjoaa ainoastaan perustietoturvaa. (Subashini & Kavitha, 2011.).

Subashini ja Kavitha (2011) liittävät IaaS-tason turvallisuushaasteisiin virtualisoinnin potentiaaliset turvallisuusreiät. Lisäksi heidän mukaansa on haasteellista taata datan luotettavuus, sillä datan omistajuuden säilyttämisen kontrollointi on vaikeaa datan sijainnin riippumattomuuden takia (Subashini & Kavitha, 2011). Toisin sanoen: kun dataa säilytetään "jossain", "kaikkialla" tai "siellä täällä", muodostuu datan omistajuuden hallinnointi entistä monimutkaisemmaksi. Subashinin ja Kavithan (2011) mukaan infrastruktuurin turvallisuushaasteisiin kuuluu lisäksi fyysinen ja ympäristöllinen turvallisuus.

Tässä tutkimuksessa oletetaan fyysisen laitteiston kuuluvan infrastruktuuri-tasoon, eikä sitä erotella omaksi tasokseen, kuten Zissis ja Lekkas (2012) tekevät. He asettavat fyysisen laitteiston turvallisuusvaatimuksiksi lakiperusteisen pilvilaskennan (ts. asiakkaan dataa ei käytetä väärin), laitteiston turvan ja luotettavuuden, sekä tietoverkon suojauksen resursseineen (Zissis & Lekkas, 2012). Tutkimuksen viitekehyksessä nämä haasteet liitetään infrastruktuuri-tasoon.

Alla olevaan taulukkoon (taulukko 5) on koottu lähdekirjallisuudesta löydettyjä turvallisuushaasteita, joita on jaoteltu palvelumalleittain. Taulukko vastaa tutkimuksen tutkimuskysymykseen erottelemalla pilvipalvelumalleihin sisältyviä turvallisuushaasteita. Taulukkoon 5 koottuja haasteita täytyy tarkastella kriittisesti, sillä ne edustavat ainoastaan haasteita, joita on kirjallisuudessa valmiiksi eroteltu palvelumalleittain. Taulukoidut haasteet siis edustavat vain osaa haasteista, joita pilvipalveluihin kaiken kaikkiaan sisältyy.

SaaS	PaaS	IaaS
• Autentikointi • Authorisointi • Datan eheys • Datan erottelu • Datan luottamuksellisuus • Dataan pääsy • Datan rikkoutuminen • Datan sijainti • Datan suojelu paljastumiselta • Datan turvallisuus • Identiteetin hallinta • Internetsovelluksen turvallisuus • Ohjelmistojen turvallisuus • Palvelun saatavuus • Pääsyn kontrollointi • Selaimen turvallisuus • Sisäänkirjautumisprosessi • Tietoverkon turvallisuus • Varmuuskopiointi • Viestiyhteyksien suojelu • Virtualisoinnin haavoittuvuus • Yksityisyys monikäyttöympäristössä	• Datan turvallisuus (data liikkeessä, data levossa, datan rippeet (engl. *remanence*)) • Haaste/mahdollisuus kattavien turvallisuusominaisuuksien hyödyntämisestä • Ohjelmistojen turvallisuus • Pilven hallinnan kontrollointi • Pääsyn kontrollointi • Turvalliset virtualisoidut osiot (engl. *images*) sekä niiden suoja • Sisäänrakennettujen turvallisuusominaisuuksien puute	• Datan luotettavuus • Fyysinen turvallisuus • Laitteiston turvallisuus ja luotettavuus • Lakiperusteinen pilvilaskenta • Tietoverkon suojaus sekä siihen osoitetut resurssit • Turvallinen virtualisointi • Virtualisoinnin potentiaaliset turvallisuusreiät • Ympäristöllinen turvallisuus

TAULUKKO 5 Turvallisuushaasteet palvelumalleittain

3.4 Haasteita haasteissa

Lähdekirjallisuus käsittelee pilvipalveluiden haasteita kirjavasti. Näkökulmat käsittelevät haasteita esimerkiksi teknisistä (Khorshed ym., 2012; Mohamed,

Abdelkader & El-Etriby, 2012), liiketoiminnallisista (Marston ym., 2011) sekä ohjeellisista (Brunette & Mogull, 2009; Buyya ym., 2009a; Jansen & Grance, 2011) lähtökohdista. Haasteiden käsittely turvallisuuden kontekstissa on myös subjektiivista, joka varmasti osaltaan lisää kirjavuutta.

Haasteita on paljon, eikä niiden jaottelemiseksi tutkimusta tehdessä havaittu yhtä yleisesti hyväksyttyä taksonomiaa. Yleisluontoiseksi määritettävät haasteet leimaavat lähdekirjallisuutta. Yleisluontoisella tarkoitetaan tässä yhteydessä sitä, että haastetta ei tarkemmin määritellä liittyväksi mihinkään toimitusmalliin, palvelumalliin, aktoriin tai yksityiskohtaiseen uhkaan tai ongelmaan. Yleisien haasteiden kautta voidaan kuitenkin muodostaa holistista näkemystä pilviympäristön turvallisuushaasteista. Vaikuttaa siltä, että useissa lähteissä turvallisuushaasteita ei ole luokiteltu tarkemmin. Ramgovind ym. (2010) mukaan esimerkiksi markkinatutkimusyhtiö Gartner (2008) listaa turvallisuushaasteita, joita organisaatioiden ja päättäjien tulee ottaa huomioon perusedellytyksinä pilvipalveluihin siirtyessä. Näkökulma on hyvin lavea eikä kerro, kenen vastuulla haasteiden huomioiminen on tai mihin palvelutasoon turvallisuushaasteita voidaan liittää. Haasteiden jäädessä luokittelemattomiksi ja ilman selkeää tärkeysjärjestystä, voi haasteisiin olla vaikea myös vastata konkreettisesti. Silti tutkimukset korostavat seikkoja, jotka on hyvä ottaa huomioon palvelusopimuksia ja -suhteita rakennettaessa. Alla mukaillaan Gartnerin (2008) esittämiä turvallisuushaasteita (Ramgovind ym., 2010):

1. Etuoikeutettu pääsy palveluun - kenellä on pääsy dataan? Kuka on vastuussa ylläpitävien tahojen palkkaamisesta ja johtamisesta?
2. Säädelty sopimusten/lain/sääntöjen noudattaminen - suostuuko palveluntarjoaja ulkoiseen auditointiin turvallisuuden varmistamiseksi?
3. Datan sijainti - tarjoaako palveluntarjoaja kontrollia datan sijaintiin?
4. Datan erottelu - ovatko salausmenetelmät käytössä kaikilla palvelun tasoilla? Ovatko menetelmät asianmukaisesti suunnitellut ja testatut?
5. Palautuminen - mitä datalle tapahtuu onnettomuustapauksissa? Miten nopeasti palauttaminen tapahtuu sekä miten laajaa palauttamista tarjotaan?
6. Tutkimuksellinen tuki - onko palveluntarjoajalla resursseja avustaa laittoman tai sopimattoman toiminnan tapauksissa?
7. Pitkän ajan uskottavuus - mitä datalle tapahtuu, jos palveluntarjoajan liiketoiminta loppuu?

Ottamalla huomioon Gartnerin korostamia turvallisuushaasteita, voidaan Ramgovind ym. (2010) mukaan yrityksissä rakentaa syvällisempää ymmärrystä pilvipalveluiden soveltuvuudesta organisaation tarpeisiin.

Vastaavaan tapaan turvallisuushaasteita erotellaan useassa lähteessä. Alla olevassa taulukossa (taulukko 6) erotellaan lisäksi Takabin ym. (2010) sekä Pearson ja Benameurin (2010) tunnistamia turvallisuus- ja yksityisyyshaasteita. Jo alla luetelluista haasteista huomataan, että tematiikka tuntuu toistuvan – ai-

noastaan termejä käytetään eri tavoin ja eri järjestyksessä. Lähdekirjallisuuden pohjalta havainto vaikuttaa toistuvan.

Takabi ym. (2010)	Pearson ja Benameur (2010)
Käyttäjän tunnistaminen ja identiteetin hallinta	Palveluun pääsy
Sisäänkirjautumisen kontrollointi	
Käytäntöjen integrointi	Standardoinnin puute
Turvallinen palvelun hallinta, luottamuksen hallinta	Monikäyttöinen ympäristö, palvelun saatavuus
Yksityisyyden ja datan suojelu	Datan elinkaaren hallinta, varmuuskopiointi
Organisatorinen turvallisuuden hallinta	Auditointi

TAULUKKO 6 Yleisiä turvallisuushaasteita

Kirjallisuuden pohjalta voidaan korostaa kriittisiksi turvallisuushaasteiksi seuraavia haasteita, sillä vähintään nämä haasteet toistuvat suoraan tai epäsuoraan monissa turvallisuushaasteita käsitellyissä lähteissä:

1. Sisäänkirjautumisen ja palveluun pääsyn kontrollointi
2. Selkeät käytännöt ja standardit
3. Palvelun saatavuus
4. Turvallinen monikäyttöympäristö (datan sijainti, erottelu ja palauttaminen)
5. Datan tarkoituksenmukainen hallinta, suojelu ja varmuuskopiointi
6. Organisatorinen kyvykkyys hallita yhteistyösuhteita (auditointi, luottamus ja tutkimuksellinen tuki)

4 Yhteenveto

Tässä tutkielmassa tutkittiin pilvipalvelumalleihin sisältyviä turvallisuushaasteita. Tutkimus toteutettiin kirjallisuuskatsauksena. Tutkimuksen keskeinen havainto on, että turvallisuushaasteita harvemmin jaotellaan palvelumalleittain. Jaottelun tarpeellisuus onkin kyseenalaista, sillä palveluarkkitehtuuri on lähtökohtaisesti kerrostunut, sekä haasteet vaikuttavat holistisesti yhteen tai useampaan palvelutasoon. Taulukon 5 jaottelu turvallisuushaasteista on tutkimuksen keskeinen tulos ja vastaa tutkimuksen tutkimuskysymykseen.

Turvallisuushaasteiden tarkastelu palvelumalleittain antaa turvallisuudesta ylimalkaisen kuvan, sillä avoimiksi kysymyksiksi jää, liittyykö haaste palveluntarjoajaan, asiakkaaseen vai molempiin. Lähdekirjallisuudessa ainoastaan kahdessa artikkelissa (Subashini & Kavitha, 2011; Zissis & Lekkas, 2012) jaoteltiin turvallisuushaasteita suoraan palvelumalleittain. Havainnon perusteella voidaan kyseenalaistaa turvallisuushaasteiden jaottelun järkevyyttä palvelumalleittain. Ilman palvelumallien näkökulmaa pilvipalveluiden turvallisuushaasteita käsitellään lähdekirjallisuudessa hyvin kattavasti (Aguiar ym., 2014; Dillon ym., 2010; Dahbur ym., 2011; CSA, 2013; Fernandes ym., 2013; Gens, 2008; Kandukuri ym., 2009; Pearson & Benameur, 2010; Ramgovind ym., 2010; Takabi ym., 2010; Yang & Chen, 2010). Taulukkoon 5 on koottu palvelumalleittain jaotellut turvallisuushaasteet.

Tutkimustulos osoittaa, että turvallisuushaasteet eivät ole yksioikoisia tai suoraan sisällytettävissä palvelumalleihin. Yksittäinen turvallisuushaaste voi olla sisältymättä palvelumalliin tai sisältyä yhteen tai useampaan palvelumalliin. Tästä voidaan päätellä, että turvallisuushaasteen sisältymistä tiettyyn palvelumalliin tulee käsitellä varauksella. Lisäksi havaittiin, että pilvipalveluihin liittyvät turvallisuushaasteet ovat kompleksisia, ja vaativat tarkastelua monesta näkökulmasta. Organisaation kannalta turvallisuudenhallinta voi pilvipalveluiden parissa vaikuttaa monimutkaiselta, mikä on varmasti osasyy siihen, miksi turvallisuuskysymykset rajoittavat edelleen pilvipalvelumarkkinoiden kasvua (Gens, 2008; Subashini & Kavitha, 2011). Tutkimustuloksen merkitsevyyttä rajoittaa se, että turvallisuushaasteita ei tutkimuksen pohjalta voida suoraan liittää yksittäiseen aktoriin. Osasyy tähän on varmasti palvelutasosopimusten rajaaminen tutkimuksen ulkopuolelle. Tutkielman tulos jääkin yleisluontoisiksi huomioiksi haasteista, joita toimijoiden täytyy huomioida.

Yleisesti turvallisuudesta huomataan, että se on kokonaisvaltainen haaste, jonka vaatimukset tulee täyttää palvelumallista, toimitustavasta, uhasta tai aktorista riippumatta. Vaikuttaa myös siltä, että yhteneväistä kaiken kattavaa turvallisuuden viitekehystä on vaikea kehittää. Lähimmäksi kokonaiskuvaa vaikuttaa yltävän Fernandes ym. (2013). Heidän tutkimuksensa käsittelee suurta osaa pilvipalveluiden turvallisuuden tutkimustyöstä viime vuosilta, sekä kokoaa yhteen loogisen taksonomian haasteiden kirjosta aihealueittain (ks. taulukko 2).

Lisäksi haasteen käsitettä tulee tarkastella subjektiivisesta näkökulmasta, sillä haaste on lähtökohtaisesti subjektiivinen kokemus. Voidaan ajatella, että yhdelle yritykselle jokin turvallisuusaspekti voi olla haasteellinen, toiselle taas ei. Subjektiivisuus lisää tarkasteluun monimutkaisuutta entisestään.

Jatkotutkimusta voisi tehdä loppukäyttäjän tai asiakkaan kokemista hyödyistä ja haasteista pilvipalveluiden parissa. Tutkimusta kannattaisi rajata vielä tarkemmin tiettyyn toimijaan, toimitustapaan tai palvelumalliin. Mielenkiintoiseksi havaitaan myös palvelumallien ja toimitustapojen valintaprosessi. Palvelustasosopimuksin ja eri palvelukombinaatioiden kautta kohdennetaan hankittava palvelu yrityksen tarpeisiin ja resursseihin sopivaksi. Palvelutasosopimuksilla määritetään toimijoiden vastuut ja velvollisuudet turvallisuuden suhteen. Palvelutasosopimukset eivät tulleet tutkielmassa tarkemmin käsitellyiksi, vaikka ansaitsisivat lisähuomiota. Kuinka varmistaa organisaation kannalta turvallisin ja käytännöllisin mahdollinen pilvipalvelujen kombinaatio?

Tutkimuksen pohjalta oletetaan, että palveluntarjoajan ja asiakkaan välinen sopimus turvallisuuslähtökohdista on kriittisempää kuin se, mikä palvelumalli on kyseessä tai mitä turvallisuushaasteita palvelumalleihin voidaan liittää. Palvelutason valitseminen voikin muodostua ratkaisevaksi strategiseksi tekijäksi yrityksen menestymisen kannalta - tästä syystä valintaprosessin tutkiminen olisi mielenkiintoista. Sellaisen sopimuspohjan luominen, jolla turvallisuus kyetään takaamaan kaikkia osapuolia tyydyttävästi on erityisen tärkeää.

Lisäksi tulee muistaa, että pilvipalveluihin liitettävät turvallisuushaasteet ovat suurilta osin aivan vastaavia, kuin perinteisenkin IT-ympäristön turvallisuushaasteet (Brunette & Mogull, 2009). Yritykset ovat kasvavassa määrin riippuvaisia tietojärjestelmistä sähköistyvien palveluiden ja sähköisen kaupankäynnin myötä (Kankanhalli, Teo, Tan & Wei, 2003). Jo ennen pilvipalveluidenkin esiinmarssia on turvallisuus ollut järjestelmien peruslähtökohta ja haasteista merkittävin (Kankanhalli ym., 2003). Pilvilaskennan myötä perinteisten tietojärjestelmien resursseja siirretään pilviympäristöön. Keskeistä pilvilaskennassa onkin hallita tilannetta, jossa operationaalista vastuuta siirretään ulkopuoliselle toimijalle siten, että onnistutaan samalla kohtaamaan omat vastuuvelvoitteet (Brunette & Mogull, 2009).

Turvallisuus ei kuitenkaan ole ainoa näkökulma haasteisiin. Se on välttämätön lähtökohta pilvijärjestelmien sekä niiden toimittajien ja käyttäjien kannalta, mutta kattaa pilvipalveluihin sisältyvistä haasteista ainoastaan yhden kategorian. Haasteita tutkitaan nykyään, ja on hyvä tutkia jatkossakin, myös luottamuksen (Khan & Malluhi, 2010; Pearson & Benameur, 2010) ja yksityisyyden (Takabi ym., 2010; Pearson & Benameur, 2010) näkökulmista. Tässä tutkimuksessa kuitenkin rajoituttiin ainoastaan turvallisuuteen.

LÄHTEET

Aguiar, E., Zhang, Y. & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. *High Performance Cloud Auditing and Applications* (s. 3-33). New York: Springer.

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.

Banerjee, P., Friedrich, R., Bash, C., Goldsack, P., Huberman, B., Manley, J., Patel, C., Ranganathan, P. & Veitch, A. (2011). Everything as a service: Powering the new information economy. *Computer,* 44(3), 36–43.

Brunette, G. & Mogull, R. (2009). *Security guidance for critical areas of focus in cloud computing V2.1*. USA: Cloud Security Alliance. Haettu 19.3.2014 osoitteesta https://cloudsecurityalliance.org/csaguide.pdf

Buyya, R., Pandey, S. & Vecchiola, C. (2009a). Cloudbus toolkit for market-oriented cloud computing. *Cloud computing* (s. 24-44). Berlin: Springer-Verlag.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. & Brandic, I. (2009b). 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.

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 ACM Workshop on Cloud Computing Security*, (s. 85–90). New York: ACM.

Cloud Security Alliance. (2013). CSA: The notorious nine cloud computing top threats in 2013. Haettu 28.3.2014 osoitteesta https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Thre ats_in_2013.pdf

Dahbur, K., Mohammad, B. & Tarakji, A. B. (2011). A survey of risks, threats and vulnerabilities in cloud computing. *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*. New York: ACM.

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

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M. & Inácio, P. R. (2013). Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2), 113-170.

Gens, F. (2008, 2. lokakuuta). IT cloud services user survey, pt. 2: Top benefits & challenges. Haettu 13.3.2014 osoitteesta http://blogs.idc.com/ie/?p=210

Gul, I., Rehman, A. & Islam, M. (2011). Cloud computing security auditing. *The 2nd International Conference on Next Generation Information Technology* (s. 143–148). Gyeongju: IEEE.

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

Jansen, W. & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *National Institute of Standards and Technology Special Publication 800-144*.

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

Kankanhalli, A., Teo, H. H., Tan, B. C. & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139-154.

Kavis, M. J. (2014). Responsibilities in cloud. Haettu 4.3.2014 osoitteesta http://www.kavistechnology.com/blog/responsibilities-in-the-cloud/

Khan, K. M. & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT professional*, *12*(5), 20-27.

Khorshed, M. T., Ali, A. B. M. & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6), 833-851.

Kumar, A. (2012). World of cloud computing & security. *International Journal of Cloud Computing and Services Science*, 1(2), 53-58.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. & Leaf, D. (2011). NIST cloud computing reference architecture. *National Institute of Standards and Technology Special Publication 500-292*.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176-189.

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology Special Publication 800-145*.

Mohamed, E., Abdelkader, H. & El-Etriby, S. (2012). Enhanced data security model for cloud computing. *The 8th International Conference on Informatics and Systems* (s. 12-17). Kairo: IEEE.

Ojala, A. (2012). Software renting in the era of cloud computing. *2012 IEEE 5th International Conference on Cloud Computing* (s. 662-669). Honolulu: IEEE.

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* (s. 693-702). Indianpolis: IEEE.

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

Rimal, B. P., Choi, E. & Lumb, I. (2009). A taxonomy and survey of cloud computing systems. *2009 Fifth International Joint Conference on INC, IMS and IDC* (s. 44-51). Soul: IEEE.

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

Sarwar, A. & Khan, M. N. (2013). A review of trust aspects in cloud computing security. *International Journal of Cloud Computing and Services Science*, 2(2), 116-122.

Sadashiv, N. & Kumar, S. (2011). Cluster, grid and cloud computing: A detailed comparison. *6th International Conference on Computer Science Education* (s. 477–482). Singapore: IEEE.

Sengupta, S., Kaulgud, V. & Sharma, V. S. (2011). Cloud computing security--trends and research directions. *2011 IEEE World Congress on Services* (s. 524-531). Washington: IEEE.

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.

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

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.

W3C. (2004). Web services glossary. Haettu 23.1.2014 osoitteesta http://www.w3.org/TR/ws-gloss/#webservice

Wang, C., Wang, Q., Ren, K. & Lou, W. (2009). Ensuring data storage security in cloud computing. *17th International Workshop on Quality of Service* (s. 1–9). Charleston: IEEE.

Watson, P. (2012). A multi-level security model for partitioning workflows over federated clouds. *Journal of Cloud Computing*, 1(1), 1-15.

Yang, J. & Chen, Z. (2010, December). Cloud computing research and security issues. In *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on* (s. 1-3). Wuhan: 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.