Tuomas Änäkkälä

PILVILASKENNAN TIETOTURVAONGELMAT

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Änäkkälä, Tuomas
Pilvilaskennan tietoturvaongelmat
Jyväskylä: Jyväskylän yliopisto, 2017, 34 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaajat: Moilanen, Panu ja Palonen, Teija

Pilvilaskennalla viitataan hajautetun laskennan malliin, jossa laskentaresursseja tarjotaan Internetin välityksellä palveluina. Nämä laskentaresurssit voidaan tarjota nopeaa, tarpeen vaatiessa sekä minimaalisella palveluntarjoajan vuorovaikutuksella. Pilvilaskentaa pidetään vakuuttavana mallina, sillä se tarjoaa tehokkaita resursseja alhaisilla kustannuksilla. Pilvilaskennasta on muodostunut yksi IT-alan nopeimmin kasvavista segmenteistä.

Pilvilaskennan turvallisuuteen liittyy kuitenkin paljon epäselvyyttä. Turvallisuuden hallitseminen pilviympäristössä ei ole poikkeavaa tavallisesta IT-ympäristöstä, mutta tavalliset turvallisuuskeinot eivät ole pilviympäristössä riittäviä. Pilvilaskennan käyttäjät hyötyvät matalista käyttökustannuksista, mutta altistuvat samalla uusille turvallisuusuhille.

Tämän kirjallisuuskatsauksen tarkoituksena oli selvittää, millaisia tietoturvaongelmia pilvilaskennan palvelumalleihin liittyy. Kirjallisuuskatsauksessa selvitettiin myös, millaisia uhkia pilvilaskenta muodostaa datan luotettavuudelle, eheydelle sekä saatavuudelle. Tutkielman keskeisin löydös osoitti pilvilaskentaan liittyvän merkittäviä turvallisuusongelmia, jotka vaihtelevat muun muassa palvelumalleittain. Turvallisuusongelmat ja dataan kohdistuvat uhat aiheutuvat pilvilaskennan pääpiirteistä sekä käytetyistä teknologioista.

Asiasanat: pilvilaskenta, pilvipalvelu, palvelumalli, turvallisuusongelma, turvallisuusuhka

ABSTRACT

Änäkkälä, Tuomas
Security issues in cloud computing
Jyväskylä: University of Jyväskylä, 2017, 34 p.
Information Systems, Bachelors Thesis
Supervisors: Moilanen, Panu and Palonen, Teija

Cloud computing refers to distributed computing paradigm, in which computing resources are delivered over the Internet as services. These resources can be delivered rapidly, on demand and with minimal service provider interaction. Cloud computing is a convincing concept, as it offers powerful resources with low costs. Cloud computing has emerged to be one of the most rapidly increasing segments in IT-industry.

There is plenty of uncertainty related to cloud computing security. Security governance in cloud environment is no different than security governance in traditional IT-systems, but traditional security measures aren't sufficient in cloud environment. Cloud computing users can benefit from low costs, but at the same time they are exposed to new security threats.

Purpose of this literature review was to find out which kind of security issues concern cloud computing service models. This literature review also clarifies which threats does cloud computing pose to confidentiality, integrity, and availability of data. Key finding of the study was that there are many security issues related to cloud computing, which vary depending on the service model. Security issues and threats to data originate from key characteristics and technologies of cloud computing.

Keywords: cloud computing, cloud service, service model, security issue, security threat

KUVIOT

SISÄLLYS

1 JOHDANTO

Pilvilaskennalla viitataan Internetin välityksellä palveluina tarjottaviin ohjelmistoihin sekä laitteistoihin, joilla kyseiset palvelut tarjotaan (Armbrust ym., 2010). Dataa sekä sovelluksia voidaan säilyttää pilvessä (engl. *cloud*), josta ne ovat aina saavutettavissa (Ryan, 2013). Pilvilaskentaa pidetään vaikuttavana mallina, sillä se tarjoaa tehokkaita datan käsittely- sekä tallennusresursseja alhaisilla kustannuksilla (Younis, Merabti, & Kifayat, 2013). Käyttäjien ei tarvitse huolehtia resurssien, kuten laitteiston, ohjelmiston ja infrastruktuurin ostamisesta lopullisesti, vaan resursseja voidaan hyödyntää käyttömaksuperusteisesti (engl. *pay-as-you-use*) (Srinivasan, Sarukesi, Rodrigues, Manoj, & Revathy, 2012).

Pilvilaskennan tehokkaat ominaisuudet kannustavat niin yrityksiä kuin esimerkiksi valtionjohtoa siirtymään pilvilaskennan pariin (Younis ym., 2013). Pilvilaskentaan on selvästi siirrytty, sillä siitä on muodostunut yksi nopeimmin kasvavista IT-alan segmenteistä (Popović & Hocenski, 2010). Pilvilaskennan markkinoiden odotettiin olevan vuonna 2009 56.8 miljoonaa dollaria (USD), ja vuonna 2014 jopa 148 miljoonaa dollaria (USD). Kasvavat markkinat todistavat, että pilvilaskentaa pidetään varsin lupaavana alustana. (Almorsy, Grundy, & Müller, 2016.)

Vaikka pilvilaskenta tarjoaa merkittäviä hyötyjä, liittyy siihen myös ongelmia. International Data Corporationin (IDC) tutkimuksen mukaan 74% IT-alan toimitus- ja tietohallintojohtajista pitää turvallisuutta suurimpana pilvilaskentaan liittyvänä haasteena (Subashini & Kavitha, 2011). Pilvilaskenta luo uudenlaisia turvallisuusriskejä heikentäen esimerkiksi tavallisten suojausmekanismien tehokkuutta (Zissis & Lekkas, 2012). Käyttäjien kannalta pilvilaskentaan siirtyminen tarkoittaa alhaisia käyttökustannuksia, mutta samalla altistumista uusille turvallisuusongelmille (Srinivasan ym., 2012).

1.1 Tutkimusongelma ja -kysymykset

Pilvilaskenta mallina koostuu useista eri komponenteista, joista keskeisimpänä ovat pilvilaskennan palvelumallit. Turvallisuuden hallitseminen pilviympäristössä ei ole yksioikoista, sillä palvelumalleihin kohdistuu selkeästi erilaisia turvallisuusongelmia. (Subashini & Kavitha, 2011.) Tässä tutkielmassa pilvilaskennan turvallisuusongelmia tutkitaan Mellin ja Grancen (2011) tunnistamien palvelumallien kautta. Ensimmäinen tutkimuskysymys on:

- Millaisia tietoturvaongelmia pilvilaskennan palvelumalleihin liittyy?

Tietoturva-alan tutkimuksessa esitetään usein myös kolme tietoturva-attribuuttia, jotka ovat luottamuksellisuus, eheys sekä saatavuus. Nämä attribuutit ovat jo useita vuosikymmeniä toimineet eräänlaisena tietoturvallisuuden mallina (Cherdantseva & Hilton, 2013). Turvallisuus liittyy vahvasti näihin kolmeen attribuuttiin, ja attribuutteja pidetään turvallisen järjestelmän kulmakivinä (Zissis & Lekkas, 2012). Tässä tutkielmassa tarkastellaan kuinka tietoturva-attribuutit toteutuvat pilviympäristössä, ja mitä turvallisuusongelmia pilviympäristöön liittyy näiden attribuuttien näkökulmasta. Toinen tutkimuskysymys on:

- Millaisia uhkia pilvilaskenta muodostaa datan luottamuksellisuudelle, eheydelle sekä saatavuudelle?

1.2 Tutkimusmenetelmä

Tutkimus toteutettiin kirjallisuuskatsauksena. Kirjallisuuskatsauksen tarkoituksena on keskustella valikoiden sekä argumentoiden tutkimustiedon kanssa (Hirsjärvi, Remes, & Sajavaara, 2003). Lähdeaineistona käytettiin Google Scholar –palvelulla kerättyä materiaalia. Lähdeaineistoa kerättäessä lähteet taulukoitiin, ja niiden kannalta kiinnitettiin huomiota viittausten määrään sekä julkaisuiden ilmestymisvuoteen. Lähteet tarkastettiin myös vertaisarvioinnin kannalta. Edellä mainittujen keinojen lisäksi Julkaisufoorumi-palvelulla tarkastettiin julkaisukanavien tasoluokitus. Lähteet ja niiden tiedot kerättiin myös taulukkoon. Lähdeaineiston etsimisessä hakusanoina käytettiin seuraavia sanoja tai yhdistelmiä: cloud computing, cloud computing security, cloud computing threats, information security, iaas security, saas security, paas security, cloud vulnerabilities, privacy in cloud.

1.3 Tutkielman rakenne

Luvussa kaksi tutustutaan pilvilaskentaan ja määritellään pilvilaskenta käsitteenä. Luvussa tutkitaan myös pilvilaskennan pääpiirteitä, sekä esitetään pilvilaskennan palvelumallit. Luvussa kolme käsitellään pilvilaskennan turvallisuutta. Turvallisuusongelmia tutkitaan aluksi pilvilaskennan pääpiirteiden kautta. Sen jälkeen luvussa tarkastellaan niitä turvallisuusongelmia, jotka liittyvät pilvilaskennan palvelumalleihin. Luvussa kolme vastataan ensimmäiseen tutkimuskysymykseen. Neljännessä luvussa tutkitaan tietoturva-attribuutteihin kohdistuvia uhkia pilviympäristössä. Tunnistetut tietoturva-attribuutit ovat luottamuksellisuus, eheys sekä saatavuus. Neljännessä luvussa vastataan toiseen tutkimuskysymykseen. Viides luku on yhteenveto. Yhteenvedossa esitetään tutkielman keskeiset löydökset, jatkotutkimusaiheet, rajoitteet sekä arvioidaan tutkielma.

2 PILVILASKENTA

Pilvilaskenta on saanut alkunsa hajautetun laskennan (engl. *grid computing),* tarvelähtöisen tietojenkäsittelyn (engl. *utility computing)* ja Software-as-a-Service -mallin yhdistymisestä. Hajautetun laskennan tavoitteena 1990-luvun alkupuolella oli yhdistää korkean suorituskyvyn tietokoneita tukemaan vaativia laskutoimituksia sekä data-intensiiviä ohjelmistoja. (Zissis & Lekkas, 2012.) Foster, Zhao, Raicu ja Lu (2008) tosin väittävät, että pilvilaskenta ei ole ainoastaan kehittynyt hajautetusta laskennasta, vaan myös tukeutuu siihen sekä sen infrastruktuuriin.

Pilvilaskennan erot hajautettuun laskentaan ovat selvät, vaikka samankaltaisuuksiakin löytyy. Pilvilaskennassa solmut (engl. *nodes*) ovat virtualisoitu, ja ne tarjotaan tarpeen mukaan dynaamisesti verkon välityksellä (Buyya, Yeo, & Venugopal, 2008). Pilvilaskennasta tehokkaan tekee juurikin virtualisointi, ja se on myös yksi suurimmista eroista hajautetun laskennan sekä pilvilaskennan välillä (Zissis & Lekkas, 2012).

Vaikka hajautettu laskenta ja pilvilaskenta voivat vaikuttaa samankaltaisilta, on kuitenkin kyse kahdesta eri mallista. Yleisen mielipiteen mukaan pilvilaskennan katsotaan sekä kehittyneen, että tukeutuneen hajautettuun laskentaan (Zissis & Lekkas, 2012). Tässä luvussa määritellään tarkemmin pilvilaskenta käsitteenä. Luvussa tarkastellaan pilvilaskennan palvelu- ja käyttöönottomalleja, sekä pilvilaskennan pääpiirteitä.

2.1 Pilvilaskennan määritelmä

Pilvilaskennan määritteleminen ei ole täysin yksioikoista. Määritelmät ovat hyvin vaihtelevia, ja pilvilaskennan termeihin liittyy huomattavasti epäselvyyttä (Armbrust ym., 2010; Foster ym., 2008). Lyhimpiin määritelmiin kuuluu Armbrustin ym. (2010) määritelmä, jonka mukaan ”pilvilaskenta viittaa palveluina tarjottuihin ohjelmistoihin, laitteistoon ja laitteiston ohjelmistoon sekä palvelinkeskukseen, jota kautta kyseiset palvelut tarjotaan”. Määritelmä

jää puutteelliseksi, sillä siinä ei esitetä tarkemmin niitä osia, joista pilvilaskenta koostuu. Onnistuneesti määritelmässä tunnistetaan pilvilaskennalle ominaiset palveluina tarjottavat ohjelmistot.

Fosterin ym. (2008) antamaa määritelmää voidaan pitää hieman kattavampana, vaikka myös siinä on puutteita. Heidän määritelmänsä mukaan pilvilaskenta on:

> Laajamittainen hajautetun laskennan paradigma, jota ohjaa skaalaedut, (engl. *economies of scale*) jossa jaetussa paikassa (engl. *pool)* sijaitsee abstraktoidut, virtualisoidut, dynaamisesti skaalattavat hallinnoidut laskentakapasiteetit, tallennustilat, alustat ja palvelut, jotka tarjotaan tarpeen vaatiessa ulkoisille asiakkaille Internetin välityksellä (Foster ym., 2008).

Foster ym. (2008) tunnistavat siis pilvilaskennan käsittävän asiakkaalle Internetin välityksellä tarjottavat abstraktoidut, virtualisoidut ja dynaamisesti skaalattavat resurssit. Pilvilaskennassa nämä resurssit tarjotaan yleensä palveluina, mutta sitä määritelmässä ei kuitenkaan tuoda esille. Määritelmässä ei myöskään tunnisteta pilvilaskennan palvelu- tai käyttöönottomalleja. Näistä syistä määritelmä jää hieman ontuvaksi.

Marston, Li, Bandyopadhyay, Zhang ja Ghalsasi (2011) pyrkivät tiivistämään pilvilaskennan ominaisuudet sekä hyödyt niin liiketoiminnallisesta- kuin teknillisestäkin perspektiivistä. He määrittelevät pilvilaskennan seuraavasti:

> Se [pilvilaskenta] on informaatioteknologian palvelumalli, jossa laskentapalvelut (niin laitteisto kuin ohjelmisto) tarjotaan tarpeen vaatiessa asiakkaalle Internetin välityksellä itsepalvelutavalla, riippumatta laitteesta ja sijainnista. Laatuvaatimukset täyttävät tarjottavat palvelut ovat dynaamisesti skaalattavia, nopeasti tarjottavissa, virtualisoituja sekä tarjottavissa minimaalisella palveluntarjoajan vuorovaikutuksella. Käyttäjät maksavat palvelusta käyttökulun mukaisesti ilman merkittävää alkuinvestointia, ja pilvipalvelut sisältävät mittausjärjestelmän joka jakaa laskentaresurssit sopiviin lohkoihin. (Marston ym., 2011.)

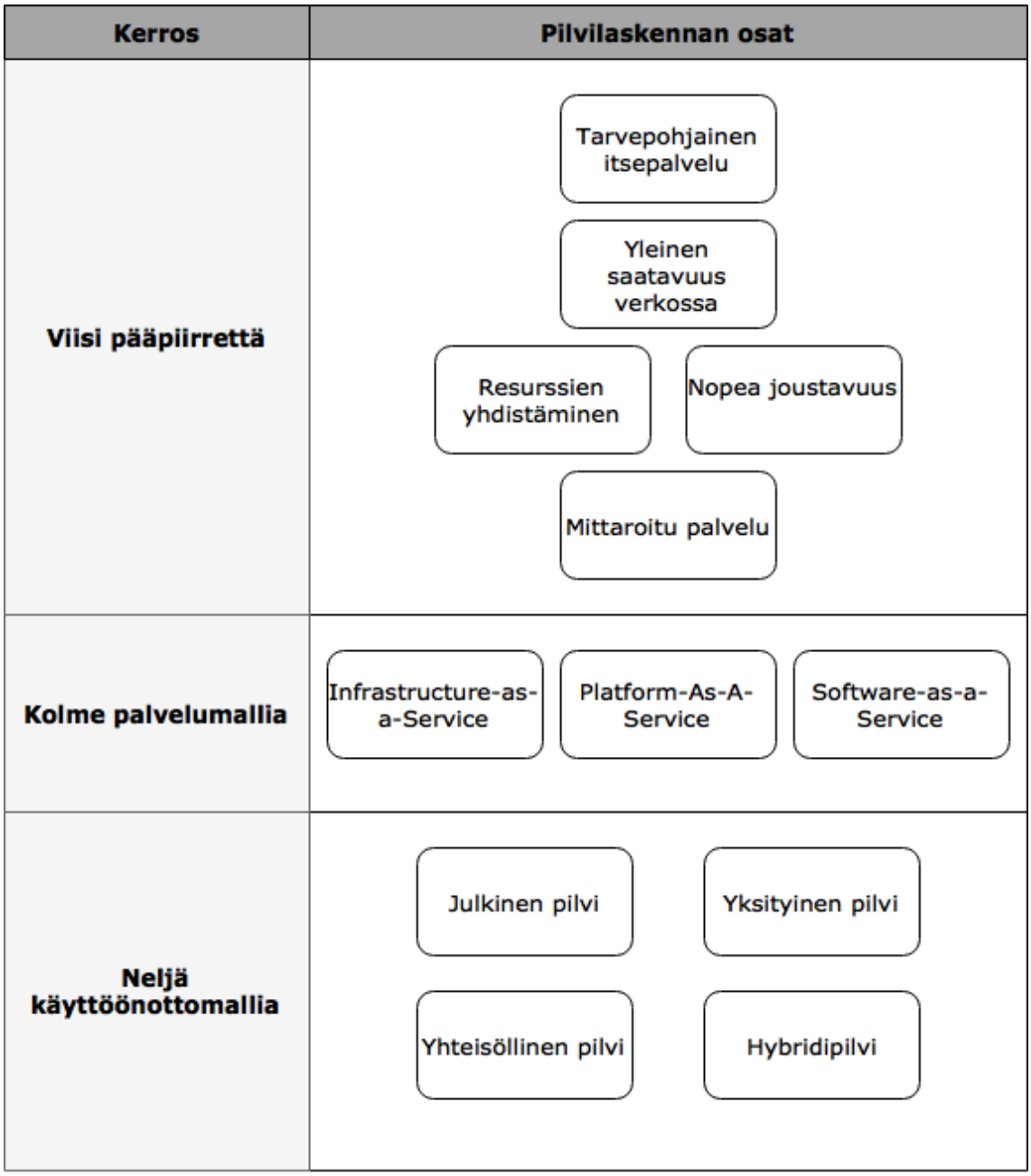
Määritelmä on kattavampi kuin aiemmin esitetyt määritelmät, sekä yhteneväinen Fosterin ym. (2008) antaman määritelmän kanssa. Myös tämä määritelmä jää kuitenkin puutteelliseksi palvelu- sekä käyttöönottomallien sekä pääpiirteiden osalta.

Kattavin määritelmä pilvilaskennasta löytyy National Institute of Standards and Technologyn (NIST) julkaisusta. Tämä määritelmä esiintyy useissa pilvilaskentaa käsittelevissä tutkimuksissa (Savu, 2011; Subashini & Kavitha, 2011; Takabi, Joshi, & Ahn, 2010). Kyseinen julkaisu on poikkeuksellinen, sillä siinä määritellään pilvilaskenta mallina, tunnistetaan pilvilaskennan palvelu-, sekä käyttöönottomallit ja pilvilaskennan pääpiirteet. NIST määrittelee pilvilaskennan seuraavasti:

> Pilvilaskenta on malli, jolla mahdollistetaan ajasta ja paikasta riippumaton, kätevä, tarpeen vaatiessa saatava verkkoyhteys jaettuun paikkaan (engl. *pool*), jossa sijaitsevat konfiguroitavissa olevat laskentaresurssit (esim. verkkoyhteydet,

palvelimet, tallennustila, ohjelmistot ja palvelut), jotka voidaan tarjota nopeaa sekä minimaalisella vaivalla tai palveluntarjoajan vuorovaikutuksella. Pilvimalli koostuu viidestä pääpiirteestä, kolmesta palvelumallista sekä neljästä käyttöönottomallista. (Mell & Grance, 2011.)

NIST:n antamaa määritelmää pilvilaskennasta havainnollistetaan seuraavassa kuviossa (kuvio 1). Kuviossa esitetään pilvilaskennan viisi pääpiirrettä, kolme palvelumallia sekä neljä käyttöönottomallia. Kuviossa esitettyjä pilvilaskennan osia tutkitaan tarkemmin seuraavissa luvuissa.



KUVIO 1 Pilviympäristön osat (AlZain, Pardede, Soh & Thom, 2012)

2.2 Pilvilaskennan pääpiirteet

Mell ja Grance (2011) tunnistavat pilvilaskennalle viisi ominaista pääpiirrettä (kuvio 1). Nämä viisi pääpiirrettä luovat ikään kuin perustan, johon useissa tutkimuksissa nojataan.

Tarvepohjainen itsepalvelu. Käyttäjä saa pääsyn laskentaresursseihin, kuten verkkotallennustilaan ilman vuorovaikutusta palveluntarjoajan henkilöstön kanssa. (Mell & Grance, 2011.)

Yleinen saatavuus verkossa. Resurssit ovat saatavilla verkkoyhteyden avulla ja käytettävissä eri alustoilla, kuten matkapuhelimella tai kannettavalla tietokoneella. (Mell & Grance, 2011.) Resurssien käyttö ei ole kytköksissä niiden fyysiseen sijaintiin tai tapaan tarjota niitä (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009).

Resurssien yhdistäminen. Palveluntarjoaja yhdistää resursseja, kuten tallennustilaa ja muistia voidakseen palvella useita asiakkaita käyttäen moniasiakkuus-mallia (engl. *multi-tenant model*), jossa fyysiset ja virtuaaliset resurssit kustomoidaan vastaamaan asiakkaan tarpeita (Mell & Grance, 2011). Asiakkaalla ei yleensä ole tietoa resurssien tarkasta sijainnista, mutta asiakas kykenee mahdollisesti määrittelemään sen valtiotasolla (Buyya ym., 2009; Mell & Grance, 2011).

Nopea joustavuus. Resurssit voidaan tarjota joustavasti, joissain tapauksissa myös automaattisesti. Resurssit ovat usein asiakkaan tarpeen mukaan skaalautuvia. (Buyya ym., 2009; Mell & Grance, 2011).

Mittaroitu palvelu. Pilvipalvelut kontrolloivat ja optimoivat resursseja automaattisesti. Resurssien käyttöä voidaan tarkkailla, kontrolloida ja raportoida, jotta palvelu on läpinäkyvää asiakkaalle sekä palveluntarjoajalle. (Mell & Grance, 2011.)

Pääpiirteet eivät rajoitu ainoastaan Mellin ja Grancen (2011) esittämiin viiteen pääpiirteeseen, sillä tutkimuksissa on nostettu esille myös muita pilvilaskennalle tunnusomaisia ominaisuuksia. Pilviympäristössä luotettavuus (engl. *reliability*) kasvaa, sillä useiden fyysisten sijaintien käyttäminen edesauttaa esimerkiksi tuhosta tai katastrofista selviytymisessä. Palvelinkeskukset sijaitsevat usein lähellä edullisia voimalaitoksia, suurissa ja edullisissa kiinteistöissä. Pilvilaskentaa ohjaa siis skaalaedut sekä kustannustehokkuus. (Buyya ym., 2009.)

Pilvilaskenta on kestävää, sillä resurssien käyttö on optimoitua. Optimoitu resurssien käyttö johtaa tehokkaisiin sekä hiilineutraaleihin järjestelmiin. (Buyya ym., 2009). Pilvilaskennan palveluorientoituneisuus käy ilmi helppokäyttöisistä palveluista. Palveluiden alla oleva infrastruktuuri on abstraktoitu pois käyttäjältä. (Gong, Liu, Zhang, Chen, & Gong, 2010.) Pilvilaskennassa käytetty infrastruktuuri on jaettu virtualisoimalla, joten yhden osan toiminta ei vaikuta muihin osiin (Gong ym., 2010). Virtualisoimalla jaettu infrastruktuuri, eli irtonainen liitos (engl. *loose coupling*) on hyvin lähellä Mellin ja Grancen (2011) tunnistamaa pääpiirrettä, resurssien yhdistämistä.

Pilviympäristölle ominaista on myös vahva virhetoleranssi sekä liiketoimintamalli. Palveluiden toiminnan kannalta virheiden hallinta on kriittistä. Virheiden hallintaan käytetään ohjelmistoja ja mekanismeja niin infrastuktuuri- kuin ohjelmistotasollakin (Gong ym., 2010). Pilvilaskentaa ja esimerkiksi hajautettua laskentaa erottaa selvästi pilvilaskennan liiketoimintamalli. Siinä missä hajautettua laskentaa hyödyntää lähinnä valtiovalta sekä yliopistot, pilvilaskennan takana ovat suuret IT-yhtiöt. Pilvilaskentaan liittyykin useasti käyttöperusteinen hinnoittelu (engl. *pay-per-use*). (Gong ym., 2010.)

2.3 Pilvilaskennan palvelumallit

NIST määrittelee pilvipalveluille kolme palvelumallia (kuvio 1), jotka ovat Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), ja Software-as-a-Service (SaaS) (Mell & Grance, 2011). Nämä palvelumallit rakentuvat kerroksittain, mutta ovat toisistaan riippumattomia (Ali, Khan, & Vasilakos, 2015).

Software-as-a-Service. Kuluttaja käyttää palveluntarjoajan sovelluksia palveluntarjoajan infrastruktuurilla. Nämä sovellukset ovat käytettävissä esimerkiksi internet-selaimella tai ohjelmalla. Kuluttaja ei vastaa infrastruktuurin ylläpidosta, mutta hänellä voi olla rajattuja oikeuksia esimerkiksi ohjelmistojen asetuksiin. (Mell & Grance, 2011.) Google Apps on esimerkki SaaS-mallilla tarjotusta ohjelmistosta (Rong, Nguyen, & Jaatun, 2013).

Platform-as-a-Service. Kuluttajalle tarjotaan infrastruktuuri, jonka avulla hän voi käyttää ja hallita itse kehittämiään tai hankkimiaan ohjelmistoja. Palveluntarjoaja puolestaan hallitsee infrastruktuurin sekä määrittää tuetut kielet, kirjastot, palvelut ja työkalut. (Mell & Grance, 2011.) Google App Engine on esimerkki PaaS-mallilla tarjotusta alustasta (Rong ym., 2013).

Infrastructure-as-a-Service. Kuluttajalle tarjotaan laskentaresursseja, tallennuskapasiteettia, verkkoyhteyksiä tai muita tietojenkäsittelyresursseja. Kuluttaja ei hallinnoi pilvi-infrastruktuuria, mutta hän voi hallita käyttöjärjestelmiä, tallennustilaa ja käyttöönotettuja ohjelmistoja. (Mell & Grance, 2011.) Esimerkiksi Amazon EC2 on IaaS-mallilla tarjottu infrastruktuuri (Rong ym., 2013).

Näihin kolmeen palvelumalliin ei juurikaan ole kohdistettu kritiikkiä muutamaa poikkeusta lukuun ottamatta. Armbrust ym. (2010) toteavat, että esimerkiksi IaaS- ja PaaS-mallien hyväksytyt määritelmät vaihtelevat laajasti, sekä raja infrastruktuurin ja alustan välillä ei ole kovinkaan selkeä. He pitävät näitä kahta palvelumallia enemmänkin toistensa kaltaisina kuin huomattavasti erilaisina (Armbrust ym., 2010). IaaS- sekä PaaS-mallien eroavaisuudet ovat kuitenkin selkeästi huomattavissa Mellin ja Grancen (2011) määritelmästä.

Myös muita palvelumalleja on esitetty, mutta niiden osalta kirjallisuus jää melko suppeaksi. SaaS-mallin rinnalle on esitetty esimerkiksi Hardware-as-a-Service -mallia (HaaS) sekä Data-as-a-Service –mallia (DaaS). HaaS-mallilla

voidaan tarjota IT infrastruktuuria, joten HaaS-malli muistuttaakin huomattavasti IaaS-mallia. DaaS-mallin mukaisesti data on saatavilla palveluna, ja sitä voidaan muokata Internetin välityksellä aivan kuin se sijaitsisi paikallisessa tallennustilassa. (L. Wang ym., 2008.) Nämä esitetyt mallit ovat ajalta, jolloin pilvilaskennan tutkimus oli vasta aluillaan. Se selittää osaksi eroavia määritelmiä, sillä pilvilaskennan käsitteistöä ei oltu vielä laajamittaisesti tutkittu.

Resource-as-a-Service (RaaS) edustaa viime vuosina esitettyä uutta palvelumallia. RaaS-malli kulminoituu IaaS-mallista, mutta resurssit tarjotaan ainoastaan muutamiksi sekunneiksi kerrallaan. (Agmon Ben-Yehuda ym., 2012.) RaaS-mallista kirjallisuutta on niukasti, tosin malli saattaa hyvinkin tulevaisuudessa nousta tunnetummaksi.

Uutena mallina on esitetty myös Everything-as-a-Service (XaaS). XaaS-malli kuvaa uutta IT-alan trendiä, jossa ohjelmia voidaan enenevissä määrin tarjota palveluna. XaaS-mallin osalta tutkijat eivät ole kuitenkaan vielä päässeet yhteisymmärrykseen mallin määritelmästä. (Duan ym., 2015.) Kunhan määritelmästä päästään yhteisymmärrykseen, saattaa XaaS-malli hyvinkin tulevaisuudessa nousta suositummaksi sekä tunnetummaksi RaaS-mallin ohella.

2.4 Pilvilaskennan käyttöönottomallit

Käyttöönottomallilla kuvataan tapaa, jolla pilvilaskennan resurssit tarjotaan. Käyttöönottomalleiksi esitetään usein neljää mallia, jotka Mell ja Grance (2011) ovat identifioineet. Nämä mallit ovat yksityinen pilvi, julkinen pilvi, yhteisöllinen pilvi ja hybridipilvi. Käyttöönottomallit ovat riippumattomia palvelumalleista (Dillon ym., 2010). Esimerkiksi SaaS-ohjelmisto ei ole sidottu tiettyyn käyttöönottomalliin.

Yksityinen pilvi tarjotaan käyttöön ainoastaan yhdelle organisaatiolle. Sitä voi hallinnoida joko organisaatio, kolmas osapuoli tai niiden yhdistelmä. (Mell & Grance, 2011.)

Julkinen pilvi on tarkoitettu vapaaseen käyttöön suurelle yleisölle tai organisaatiolle. Sitä hallinnoi palveluntarjoaja. (Mell & Grance, 2011.) Loppukäyttäjä voi käyttää tarpeensa mukaan julkisen pilven tarjoamia skaalautuvia resursseja (Rong ym., 2013).

Yhteisöllinen pilvi tarjoaa infrastruktuurin käyttöön usealle organisaatiolle, jotka jakavat samankaltaiset kiinnostuksen kohteet. Sitä voi hallinnoida yksi tai useampi yhteisön organisaatio, kolmas osapuoli tai edellisten yhdistelmä. (Mell & Grance, 2011.) Esimerkiksi Siemens IT Solutions and Servicesin tarjoama media-alan palvelu Media Cloud on esimerkki yhteisöllisestä pilvestä (Rong ym., 2013).

Hybridipilvi on yhdistelmä kahdesta tai useammasta erilaisesta pilven infrastruktuurista. Ne ovat itsenäisiä kokonaisuuksia, mutta toiminnan kannalta sidottuja toisiinsa. Hybridipilven yhdistelmä voi koostua joko yksityisestä, julkisesta tai yhteisöllisestä pilvestä. (Mell & Grance, 2011.) Yleensä

hybridipilven tarkoituksena on mahdollistaa sen toimivuus korkean kysynnän aikana (Rong ym., 2013).

Tutkimuksissa esitetyissä käyttöönottomalleissa ei ole havaittavissa merkittäviä eroavaisuuksia. Armbrust ym. (2010) eivät tuo esille käyttöönottomallin käsitettä, mutta tunnistavat kuitenkin julkisen sekä yksityisen pilven. Heidän mukaansa julkinen pilvi tarjotaan käyttöperusteisella maksulla suurelle yleisölle. Yksityistä pilveä ei tarjota suurelle yleisölle vaan organisaatiolle, joka on tarpeeksi suuri hyötyäkseen pilvilaskennan hyvistä puolista. (Armbrust ym., 2010.)

Näiden lisäksi yhdeksi käyttöönottomalliksi on tunnistettu virtuaalinen yksityinen pilvi (engl. *virtual private cloud*). Virtuaalinen yksityinen pilvi on yhdistelmä organisaation olemassa olevasta IT-infrastruktuurista ja Amazonin julkisesta pilvestä. Julkisesta pilvestä varataan eristettyjä resursseja, joita voi käyttää VPN-yhteydellä. (Dillon ym., 2010.) Virtuaalista yksityistä pilveä ei voida Mellin ja Grancen (2011) määritelmän mukaan laskea hybridipilveksi, sillä se ei ole yhdistelmä kahdesta tai useammasta erilaisesta pilven infrastruktuurista.

3 PILVILASKENNAN TURVALLISUUSONGELMAT

Turvallisuuden hallitseminen pilviympäristössä ei suurimmilta osin ole poikkeavaa turvallisuuden hallitsemisesta tavallisessa IT-ympäristössä (Chen & Zhao, 2012; Cloud Security Alliance, 2009). Pilvilaskennan turvallisuuteen koetaan kuitenkin liittyvän edelleen paljon epäselvyyttä. Epäselvyys on osasyy siihen, miksi turvallisuutta pidetään pilvilaskennan suurimpana huolenaiheena. (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013.) Epäselvyys aiheutuu pilvilaskennassa käytetyistä teknologioista ja pilvilaskennan pääpiirteistä (Cloud Security Alliance, 2009).

Epäselvyyden ratkaisemiseksi pilvilaskennan turvallisuutta on tutkittu laajasti. Osa tutkimuksista keskittyy pilvilaskennan turvallisuuteen ainoastaan yleisellä tasolla. Koska pilvilaskenta koostuu muun muassa useista eri palvelumalleista, on turvallisuusongelmia mahdollista tarkastella palvelumalleittain. Palvelumalleittain tarkastelu on järkevää, sillä jokaiseen palvelumalliin liittyy eroavia turvallisuusriskejä sekä –ongelmia (Subashini & Kavitha, 2011).

Tässä luvussa määritellään aluksi turvallisuus pilviympäristössä, sekä tarkastellaan pilvilaskennan pääpiirteisiin liittyviä turvallisuusongelmia. Lopuksi luvussa tarkastellaan pilvilaskennan turvallisuusongelmia palvelumalleittain ja vastataan ensimmäiseen tutkimuskysymykseen. Tutkielman kontekstissa turvallisuusongelmien katsotaan käsittävän pilvilaskentaan liittyvät haasteet, riskit sekä heikkoudet. Vastaavan lähestymistavan ovat ottaneet esimerkiksi Hashizume ym. (2013), jotka käsittelevät turvallisuusongelmia samaan tapaan eräänlaisena ylätason terminä.

3.1 Pilvilaskennan turvallisuus

Pilvilaskennan turvallisuus käsitteenä tarkoittaa kaikkia niitä näkökantoja, joilla pilvilaskentaa pyritään tekemään turvalliseksi (Ryan, 2013). Vaikka Zhen ja

Zhao (2012) väittävät, että turvallisuuden hallitseminen pilviympäristössä ei ole juurikaan poikkeavaa, toteavat Subashini ja Kavitha (2011), että esimerkiksi SaaS-mallin turvaamiseksi tavalliset turvallisuuskeinot eivät ole riittäviä. Turvallisuuden hallitseminen pilviympäristössä voi siis käsittää samoja keinoja kuin turvallisuuden hallitseminen tavallisessa IT-ympäristössä, mutta nämä keinot eivät ole pilviympäristössä yksinään riittäviä. Pilviympäristö on huomattavasti poikkeava tavallisesta IT-ympäristöstä.

Koska pilvilaskennassa käytetyt teknologiat sekä sen pääpiirteet muodostavat ongelmia, täytyy pilvilaskennan palveluntarjoajien selvittää tavanomaisten turvallisuushaasteiden lisäksi myös itse pilviteknologian muodostamat haasteet. Tästä syystä pilvilaskennan turvallisuus voidaan jakaa tavanomaisiin turvallisuushaasteisiin sekä pilven turvallisuushaasteisiin (Rong ym., 2013). Tavanomaisilla turvallisuushaasteilla tarkoitetaan niitä haasteita, jotka liittyvät yleisesti viestintäteknologiaan, sekä täten myös pilvilaskentaan. Pilven turvallisuushaasteet taas käsittävät ne haasteet, jotka aiheutuvat itse pilvilaskennasta. (Rong ym., 2013.)

Pilvilaskennan turvallisuutta käsitellessä ei ole kovinkaan relevanttia keskittyä tavanomaisiin haasteisiin. Tästä syystä seuraavassa alaluvussa käsitellään pilven turvallisuushaasteita, eli pilvilaskennasta aiheutuvia turvallisuushaasteita. Myöhemmissä alaluvuissa pilven turvallisuushaasteita tarkastellaan palvelumalleittain.

3.2 Pilvilaskennan turvallisuushaasteet

Pilven turvallisuushaasteiden kriittisin huolenaihe liittyy yksityisyyteen sekä käyttäjän datan luottamuksellisuuteen. Käyttäjät haluavat tietää missä heidän datansa sijaitsee ja kuka sitä hallinnoi. (Rong ym., 2013.) Datan ulkoistaminen tarkoittaa käytännössä sitä, että asiakkaat menettävät fyysisen hallinnan datastaan (Z. Xiao & Y. Xiao, 2013). Käyttäjät haluavat myös olla varmoja, ettei esimerkiksi palveluntarjoaja väärinkäytä kriittistä informaatiota (Rong ym., 2013). Ryan (2013) pitääkin palveluntarjoajan mahdollisuutta datan väärinkäyttöön ainutlaatuisimpana pilvilaskennan muodostamana turvallisuusuhkana.

Pilviympäristössä palveluntarjoajille on tyypillistä, että dataa sijoitellaan fyysisesti eri sijainteihin (Sabahi, 2011). Tällä pyritään yleisesti varmistamaan palvelun saatavuus. Rong ym. (2013) esittävät, että datan sijoittelusta johtuen resurssien sijainti saattaa muodostaa turvallisuusongelmia. Koska resurssit saattavat sijaita muilla lainsäädännöllisillä alueilla, saattavat kiistatilanteet olla jopa pilvipalveluntarjoajien hallitsemattomissa (Rong ym., 2013). Fyysisen hallinnan menettämisestä onkin muodostunut yksi pilvilaskennan suurimmista epävarmuustekijöistä (Z. Xiao & Y. Xiao, 2013). Resurssien sijaitseminen muilla lainsäädännöllisillä alueilla tarkoittaa myös sitä, että tallennettua informaatiota ei koske ainoastaan palveluntarjoajan menettelytavat, vaan myös sen maan lainsäädäntö, jossa palveluntarjoaja sijaitsee (Rong ym., 2013). Datan

ulkoistaminen ja säilytys pilvessä useassa eri sijainnissa luo myös oikeudellisia haasteita esimerkiksi liittyen datan yksityisyyteen (Zissis & Lekkas, 2012). Resurssien sijaintiin liittyvät ongelmat eivät kuitenkaan liity yksityiseen pilveen. Yksityinen pilvi sijaitsee usein käyttäjän tiloissa, jolloin dataa ei ulkoisteta.

Myös pääpiirteiden mukainen resurssien yhdistäminen luo useita turvallisuusongelmia. Virtualisoidussa ympäristössä useiden käyttäjien data sijaitsee samalla fyysisellä palvelimella (Z. Xiao & Y. Xiao, 2013). Koska data on jaettu ainoastaan virtualisoimalla, luo resurssien yhdistämisen uhkia liittyen datan yksityisyyteen ja luottamuksellisuuteen (A. Behl & K. Behl, 2012; Zissis & Lekkas, 2012). Resurssien yhdistämisestä aiheutuvat turvallisuusongelmat eivät ole kuitenkaan välttämättä läsnä yksityisessä pilvessä, sillä yksityisen pilvi tarjotaan käyttöön yhdelle organisaatiolle. Resursseja ei ole jaettu, joten samalla fyysisellä palvelimella ei sijaitse useiden organisaatioiden dataa.

3.3 Pilvilaskennan palvelumalleihin kohdistuvat turvallisuusongelmat

Tässä luvussa käsitellään pilvilaskennan turvallisuusongelmia palvelumalleittain. Koska palvelumallit ovat huomattavasti toisistaan eroavia, eroaa ominaisuuksien lisäksi myös palvelumallien turvallisuus ja sen hallitseminen. Turvallisuusongelmia käsitellään palvelumalleittain järjestyksessä IaaS, PaaS sekä SaaS. Syy käsittelyjärjestykselle löytyy pilvipalvelumallien kerrosmaisesta arkkitehtuurista, jossa palvelumallit nähdään rakentuvan päällekkäin (kuvio 1). Näin ollen esimerkiksi SaaS-malli on jossain määrin riippuvainen alempien kerroksien turvallisuudesta, mutta loppujen lopuksi tärkeimmässä roolissa turvallisuutta ajatellessa on kuitenkin itse SaaS-malli (Abbas, Farooq, & Afghan, 2015).

3.3.1 Infrastructure-as-a-Service -mallin turvallisuusongelmat

Pilvilaskenta nojaa vahvasti virtualisointiin, ja virtualisointia voidaan pitää yhtenä pilvilaskennan suurimpana mahdollistajana. Virtualisointiin liittyvä turvallisuus ei kuitenkaan ole yksioikoista. Teoriassa virtualisoinnilla voidaan käsitellä tietoturvaongelmia, mutta käytännössä se on haastavaa, sillä virtualisointiin itsessään liittyy paljon turvallisuusongelmia (Gajek, Liao, & Schwenk, 2007). IaaS-mallin turvallisuusongelmat aiheutuvat pitkälti virtualisoinnista, sillä mallilla tarjotaan ainoastaan infrastruktuuria (Hussein & Khalid, 2016).

Virtualisoinnin turvallisuus IaaS-mallissa liittyy olennaisesti isäntätietokoneisiin. Isäntätietokoneet toimivat pilvilaskennan virtuaaliympäristön ohjauspisteinä, jotka voivat kommunikoida virtualisoitujen ohjelmien kanssa. Isäntätietokone voi muun maussa sammuttaa tai käynnistää virtuaalitietokoneita uudelleen, määrittää laitteistoasetuksia kuten prosessorien

määrää ja verkonkäyttöä sekä tarkastella, kopioida ja mahdollisesti jopa muokata virtuaalitietokoneen levyllä olevaa dataa. (Dawoud, Takouna, & Meinel, 2010; Hussein & Khalid, 2016.) Koska isäntätietokone hallinnoi virtuaalikoneita, sen vaarantuminen asettaa myös mahdollisesti virtuaalikoneet vaaraan. Isäntätietokoneiden vaarantumista pidetään IaaS-mallissa pahimpana mahdollisena turvallisuusriskinä. (Dawoud ym., 2010.)

Yksi suurimmista IaaS-mallin turvallisuusuhista on isäntätietokoneen ominaisuuksien väärinkäyttö. Isäntätietokoneen ominaisuudet ovat pilvilaskennan kannalta tärkeitä, joten isäntätietokone on myös hyökkääjän kannalta kiinnostava kohde. Toisaalta väärinkäyttöön ei aina liity ulkoista tekijää, sillä järjestelmänvalvoja, tai kuka tahansa henkilö kohotetuilla oikeuksilla voi väärinkäyttää isäntätietokoneen ominaisuuksia (Dawoud ym., 2010; Hussein & Khalid, 2016). Ihmiset ja henkilöstö ovat usein tietoturvassa heikoimmat lenkit.

Toinen turvallisuusuhka aiheutuu isäntätietokoneiden sekä virtuaalitietokoneiden välisestä kommunikoinnista. Virtuaalitietokoneiden verkkoliikenteen jokainen paketti kulkee aina isäntätietokoneen kautta (Dawoud ym., 2010). Siksi isäntätietokone voi monitoroida virtuaalitietokoneiden liikennettä sekä ohjelmistoja (Dawoud ym., 2010). Monitorointia voidaan väärinkäyttää, jolloin virtuaalitietokoneiden verkkoliikenne saattaa paljastua.

Väärinkäytön estämiseksi ja IaaS-mallin turvallisuuden varmistamiseksi virtuaalitietokoneiden suojaaminen on elintärkeää (Hussein & Khalid, 2016). Virtuaalitietokone voidaan suojata hypervisorilla. Hypervisori, eli Virtual Machine Monitor (VMM) on ohjelmisto, jolla eristetään virtuaalikoneet. Siksi VMM on tärkeä linkki turvallisuuden kannalta – jos VMM:n turvallisuus vaarantuu, vaarantuu potentiaalisesti myös kaikkien virtuaalikoneiden turvallisuus. (Hashizume ym., 2013.) VMM:n vaarantuminen on siis käytännössä yhtä suuri riski kuin isäntätietokoneen vaarantuminen. Turvallisuuden kannalta täydellinen VMM:n eristäminen on vielä saavuttamatta (Subashini & Kavitha, 2011).

Vaikka Hussein ja Khalid (2016) korostavat virtualisoinnin turvallisuuden tärkeyttä, on fyysisen turvallisuuden varmistaminen on vähintäänkin yhtä tärkeää (Subashini & Kavitha, 2011). IaaS-mallin kohdalla palveluntarjoaja vastaa virtualisoinnin lisäksi myös fyysisestä turvallisuudesta. Fyysinen turvallisuus käsittää infrastruktuurin suojaamisen esimerkiksi katastrofeilta sekä tahallisilta tai tahattomilta vahingoilta (Subashini & Kavitha, 2011). Fyysinen turvallisuus on tärkeää, sillä virheet tai ongelmat fyysisessä koneessa vaikuttavat virtuaalikoneisiin. Sama pätee myös toisin päin. (Ertaul, Singhal, & Saldamli, 2010.)

IaaS-mallin turvallisuus riippuu fyysisestä turvallisuudesta sekä virtualisoinnin turvallisuudesta. Mallia voidaan pitää suhteellisen turvallisena, sillä sisäänrakennettujen ominaisuuksien vähäisyys siirtää vastuuta turvallisuudesta käyttäjälle. Kunhan virtualisointiohjelmisto on aukoton, käyttäjällä on paremmat mahdollisuudet hallita turvallisuutta (Subashini &

Kavitha, 2011). Infrastruktuurin abstraktoinnista johtuen käyttäjä on vastuussa käyttöjärjestelmän, ohjelmistojen sekä datan turvallisuudesta (Cloud Security Alliance, 2009).

3.3.2 Platform-as-a-Service -mallin turvallisuusongelmat

PaaS-mallin turvallisuus jakautuu kahteen pääosa-alueeseen: alustan turvallisuuteen sekä käyttäjän ohjelmistojen turvallisuuteen (Hashizume ym., 2013). Alustan turvallisuudella viitataan niihin ohjelmistoihin, jotka palveluntarjoaja välittää käyttäjälle. Käyttäjän ohjelmistoilla taas viitataan niihin ohjelmistoihin, joita voidaan ajaa sekä rakentaa (engl. *build*) palveluntarjoajan välittämien ohjelmistojen avulla. PaaS-malli on suunnattu ohjelmistokehittäjille, joten turvallisuusongelmat liittyvät ohjelmistojen kehittämiseen.

Käyttäjän kannalta yksi suurimmista turvallisuusuhista aiheutuu suhteista kolmansiin osapuoliin, sillä PaaS-mallissa käyttäjällä on usein mahdollisuus käyttää tavallisten ohjelmointikielien lisäksi myös kolmansien osapuolien web-komponentteja (Mather, Kumaraswamy, & Latif, 2009). Web-komponenteilla tarkoitetaan esimerkiksi useita lähde-elementtejä, jotka ovat integroitu yhdeksi yksiköksi (Hashizume ym., 2013). Nämä web-komponentit ovat julkaistuja web-palveluita, joita voidaan käyttää ohjelmistojen kehittämisen tukena (Yang & Papazoglou, 2002). Käytettäessä kolmansien osapuolien web-komponentteja, on käyttäjä riippuvainen näiden komponenttien saatavuudesta. Myös komponenttien mahdolliset turvallisuusongelmat periytyvät, aiheuttaen uhkia datan sekä verkkoyhteyden turvallisuudelle. (Hashizume ym., 2013.)

Toinen suuri turvallisuusuhka aiheutuu ohjelmistokehittämisen nopeista sykleistä. Nopeilla sykleillä viitataan jatkuvaan ominaisuuksien lisäämiseen. Käyttäjien tuleekin pystyä varmistamaan nopeiden kehityssyklien ohella myös jokaisen uuden ohjelmistoversion turvallisuus. Turvallisuuden ja nopeiden syklien hallitsemiseksi ohjelmistokehitystekniikoiden tulee olla joustavia. (Ertaul ym., 2010.) Käyttäjän ohjelmistojen turvallisuus ei ole ainoastaan riippuvainen hyvistä turvallisuuskäytänteistä, sillä jokainen päivitys PaaS-mallin alustassa voi vaikuttaa myös käyttäjän ohjelmistojen turvallisuuteen (Hashizume ym., 2013).

Kolmas turvallisuusuhka liittyy PaaS-mallin alla olevaan infrastruktuuriin. Vaikka käyttäjien ohjelmistot olisivat turvallisia, eivät käyttäjät voi varmistaa käyttämänsä ympäristön turvallisuutta. Infrastruktuurin ja resurssien sijainti voi olla myös haastavaa määrittää. Näin ollen eri alueiden lainsäädännölliset seikat voivat huomattavasti vaikuttaa datan turvallisuuteen sekä yksityisyyteen. (Hashizume ym., 2013.) Jaetun infrastruktuurin käyttäminen altistaa esimerkiksi tietovuodolle, sillä jokainen käytetty resurssi toimii kommunikointikanavana (Sandikkaya & Harmanci, 2012). Infrastruktuurin turvallisuus on PaaS-mallissa palveluntarjoajan vastuulla, eikä käyttäjä voi osaltaan vaikuttaa sen turvallisuuteen.

Infrastruktuurin turvallisuus on kytköksissä objektien jaotteluun eri isäntätietokoneille ympäri pilveä. Palveluntarjoajan tulee kyetä kontrolloimaan sekä tarkkailemaan pääsyä resursseihin. Turvallisuuden kannalta myös oikeuksien hallitseminen tulee pystyä hoitamaan standardisoidulla tavalla. (Sandikkaya & Harmanci, 2012.) PaaS-mallin turvallisuus ei kuitenkaan palveluntarjoajan kannalta ole huomattavasti eroava IaaS-mallista ja sen turvallisuudesta. Pilviympäristön kerrosmaisesta arkkitehtuurista johtuen alempien kerroksien turvallisuusongelmat periytyvät. Palveluntarjoajan kannalta etenkin alustaan ja infrastruktuurin liittyviä turvallisuusongelmia on käsitelty luvussa 3.3.1.

PaaS-mallin turvallisuuteen vaikuttaa paljon sisäänrakennettujen ominaisuuksien vähäisyys, joka voidaan nähdä niin uhkana kuin mahdollisuutenakin. PaaS-mallissa vastuuta turvallisuudesta siirretään palveluntarjoajalta käyttäjälle. Siksi käyttäjä saattaa kohdata monimutkaisia turvallisuushaasteita rakentaessaan ohjelmistoja (Hashizume ym., 2013). Yleensä sisäänrakennettujen ominaisuuksien vähäisyys nähdään kuitenkin mahdollisuutena, sillä se tarjoaa käyttäjälle mahdollisuuden luoda ylimääräisä turvallisuuskerroksia (D. Puthal, B. P. S. Sahoo, S. Mishra, & S. Swain, 2015; Hashizume ym., 2013; Subashini & Kavitha, 2011).

Hashizume ym. (2013) toteavat PaaS-mallin turvallisuutta käsittelevää kirjallisuusmateriaalia olevan vähemmän. PaaS-malli onkin turvallisuuden kannalta ainutlaatuinen sillä, siinä yhdistyy sekä IaaS- että SaaS-mallien ominaisuuksia. SaaS-mallilla tarjotaan valmiita ohjelmistoja ja PaaS-mallilla työkaluja, joilla näitä ohjelmistoja voidaan rakentaa (Hashizume ym., 2013). Molemmat mallit rakentuvat IaaS-mallin päälle. Siksi myös turvallisuusongelmissa on yhtymäkohtia, eikä itse PaaS-malliin kohdistu selvästi erotettavissa olevia ongelmia.

3.3.3 Software-as-a-Service -mallin turvallisuusongelmat

SaaS-mallin kohdalla huomionarvoista on se, että mallin turvallisuus on kerrosmaisesta arkkitehtuurista johtuen jossain määrin riippuvainen myös alempien kerroksien turvallisuudesta (Abbas ym., 2015; Ali ym., 2015). SaaS-mallin turvallisuuden suurin ero aiheutuu vastuunjaosta, joka on täysin poikkeava verrattuna aiemmin esitettyihin palvelumalleihin. SaaS-mallin lukuisat sisäänrakennetut ominaisuudet tarkoittavat pienempää joustavuutta, siten siirtäen vastuun turvallisuudesta täysin palveluntarjoajalle.

Vastuunjako ilmenee palveluntarjoajan ja käyttäjän välisessä suhteessa, sillä SaaS-mallissa käyttäjä on täysin riippuvainen palveluntarjoajasta sekä palveluntarjoajan turvallisuudesta (AlZain, Pardede, Soh, & Thom, 2012; Choudhary, 2007; Subashini & Kavitha, 2011). Turvallisuutta monimutkaistaa entisestään se, että palveluntarjoaja voi isännöidä ohjelmistoa omilla palvelimillaan, tai ulkoistaa ohjelmiston isännöinnin kolmannen osapuolen tarjoajalle. Tämä aiheuttaa merkittävästi epätietoisuutta. Käyttäjän on lähes mahdoton varmistaa, onko palveluntarjoaja ottanut tarvittavat

turvallisuusmääritykset huomioon. (Subashini & Kavitha, 2011.) Datan sijainnin määrittäminen voi olla myös vaikeaa. Tämä saattaa johtaa oikeudellisiin kiistoihin esimerkiksi datan omistajuudesta (Ali ym., 2015). Myös datan hallinnoiminen vaikeutuu käyttäjän näkökulmasta (Abbas ym., 2015; Rong ym., 2013; Sabahi, 2011; Subashini & Kavitha, 2011).

Vastuunjaon ohella merkittävimmät turvallisuusongelmat liittyvät web-ohjelmiston turvallisuuteen. Verizon Businessin julkaiseman raportin mukaan 39% kaikista hyökkäyksistä kohdistuu ohjelmistokerrokseen. Tämä määrä on kasvavassa trendissä. (Baker, Hylender, & Valentine, 2008.) Siten myös SaaS-mallissa ohjelmistokerroksen turvallisuus on merkittävässä roolissa. SaaS-mallin ohjelmistoihin kohdistuvat samat turvallisuusongelmat kuin mihin tahansa web-ohjelmistoihin, mutta SaaS-mallin ohjelmistoille tavalliset turvallisuusratkaisut eivät ole kuitenkaan riittäviä. Tämä johtuu pilviympäristön arkkitehtuurista, sillä pilviympäristössä ohjelmistojen heikkouksien seuraukset voivat olla tuhoisat. Myös pilviarkkitehtuurin mukainen resurssien jakaminen vakavoittaa ongelmaa entisestään. (Ali ym., 2015.) Yleisin ohjelmistokerrokseen kohdistuva hyökkäys on yleensä SQL-injektio. SQL-injektio on hyökkäys, jonka avulla hyökkäyksen kohde saadaan suorittamaan hyökkääjän komentoja. (OWASP, 2013.) Mikäli ohjelmisto on altis SQL-injektiolle, voi koko ohjelmiston data olla vaarassa (Ali ym., 2015; Kim & Vouk, 2014; Subashini & Kavitha, 2011).

Identiteetin hallintaan sekä pääsynvalvontaan liittyvät heikkoudet ovat yksi kymmenestä suurimmasta web-applikaation turvallisuuteen liittyvistä riskeistä (OWASP, 2013). Identiteetin hallinta sekä pääsynvalvonta ovat molemmat IT-ohjelmistojen kriittisiä funktioita, joilla pyritään varmistamaan riittävä datan sekä resurssien suojaamisen taso (Almulla & Yeun, 2010). Pilviympäristössä näihin funktioihin liittyy merkittäviä tietoturvaongelmia. Nämä ongelmat ovat korostuneessa roolissa, sillä ne voivat helposti johtaa esimerkiksi sensitiivisen datan paljastumiseen (Younis ym., 2013). Pilviympäristö monimutkaistaa näitä funktioita, sillä useat käyttäjät jakavat samat fyysiset resurssit. Organisaatioiden näkökulmasta identiteetin hallinta on entistä vaikeampaa, sillä organisaatioiden olemassa olevien valtuutusmekanismien siirtäminen pilviympäristöön voi olla ongelmallista. (Ali ym., 2015.) Hyvin integroiduilla identiteetin hallinnan sekä pääsynvalvonnan ratkaisuilla, kuten single sign-on –hallinnalla voidaan ratkaista näitä ongelmia (IBM, 2014).

SaaS-mallin turvallisuuden kannalta verkko on luonnollisesti kriittinen komponentti. SaaS-ohjelmisto tarjotaan Internetin välityksellä, joten data kulkee aina verkon välityksellä. Jotta tietovuodoilta ja muilta mahdollisilta ongelmilta voidaan välttyä, tulee data salata vahvoja salaustekniikoita, kuten SSL- sekä TSL-kerroksia käyttäen. (Subashini & Kavitha, 2011.) Tutkijat ovat kuitenkin identifioineet useita tietoturvaongelmia kohdistuen näihin laajasti käytössä oleviin salaustekniikoihin (Kim & Vouk, 2014). Vaikka verkkoyhteyteen liittyvät tietoturvaongelmat ovat joissain tutkimuksissa esitetty SaaS-mallin tietoturvaongelmina, liittyvät ne enemmänkin viestintäteknologiaan yleisesti.

Verkkoyhteyteen liittyvät turvallisuusongelmat vaikuttavat myös SaaS-malliin, mutta eivät aiheudu itse SaaS-mallin ominaisuuksista.

4 DATAAN KOHDISTUVAT UHAT PILVILASKENNASSA

Pilvilaskennassa data altistuu uudenlaisille uhille, jotka eivät välttämättä kohdistu paikallisesti tallennettuun dataan. Nämä uhat aiheutuvat datan ja palveluiden ulkoistamisesta kolmansille osapuolille. Datan ulkoistaminen vaikeuttaa sen turvallisuuden hallitsemista. (Hashizume ym., 2013.) Kun käyttäjä ulkoistaa datansa, hän menettää samalla sen fyysisen hallinnan (A. Behl & K. Behl, 2012). Fyysisen hallinnan menettäminen vaikeuttaa merkittävästi datan luottamuksellisuuden, eheyden sekä saatavuuden varmistamista. Ulkoistettu data sijaitsee jaetussa ympäristössä, jossa fyysiset resurssit ovat jaettu useiden käyttäjien kesken (Ali ym., 2015). Tämä herättää useita huolenaiheita liittyen esimerkiksi datan luottamuksellisuuteen. Tässä luvussa vastataan toiseen tutkimuskysymykseen, eli millaisia uhkia pilvilaskenta muodostaa datan luottamuksellisuudelle, eheydelle sekä saatavuudelle?

4.1 Luottamuksellisuuteen liittyvät uhat

Luottamuksellisuus tarkoittaa, että ainoastaan valtuutetut osapuolet voivat käyttää dataa. Pilviympäristössä uhkia luottamuksellisuuteen luo käyttäjien, ohjelmistojen ja kytkettyjen laitteiden kasvanut määrä. Koska dataan voidaan päästä käsiksi useista eri pisteistä, kasvaa samalla luottamuksellisuuteen kohdistuvien uhkien määrä. (Zissis & Lekkas, 2012.) Sen lisäksi myös pilvilaskennan moniasiakkuusmalli luo potentiaalisia uhkia luottamuksellisuudelle, sillä useiden käyttäjien data sijaitsee etenkin julkisessa pilvessä samalla fyysisellä palvelimella (A. Behl & K. Behl, 2012; Zissis & Lekkas, 2012).

Luottamuksellisuutta pidetään pilviympäristön yhtenä suurimpana huolenaiheena. Uhat luottamuksellisuudelle aiheutuvat usein datan ulkoistamisesta pilvipalvelimille, joita hallinnoi mahdollisesti epäluotettavat

palveluntarjoajat. (Z. Xiao & Y. Xiao, 2013.) Luottamuksellisuus voi vaarantua tahattomasti, sillä infrastruktuuri on jaettu ainoastaan virtualisoimalla. Poistettaessa dataa palvelimelta saattaa siitä jäädä jäänteitä, jotka voivat tahdonvastaisesti paljastua. (Zissis & Lekkas, 2012.) Ulkoistettua dataa voi uhata myös eri alueiden lainsäädännölliset asetukset, paljastaen datan osittain tai mahdollisesti kokonaan. On myös mahdollista, että data voidaan luovuttaa kolmansille osapuolille ilman omistajan lupaa. (Younis ym., 2013.) Siksi pilvilaskentaa hyödyntävien osapuolien tulee suhtautua kriittisesti esimerkiksi palveluntarjoajan valintaan.

On kiistelty, voidaanko luottamuksellisuus pilviympäristössä varmistaa täysin. Salaustekniikoilla voidaan parantaa datan luottamuksellisuutta, mutta datan salaaminen yksinään ei ole riittävä ratkaisu (Chen & Zhao, 2012). Myös Ryanin (2013) mukaan luottamuksellisuus pyritään tällä hetkellä varmistamaan yhdessä lainsäädännön, sopimusten sekä hyvien käytänteiden avulla. Palveluntarjoajat pyrkivät tekemään kaikkensa, jotta esimerkiksi pääsy dataan voidaan rajoittaa mahdollisimman vähälle määrälle työntekijöitä. Kuitenkin suurilla yrityksillä kuten Googlella on ollut ongelmia työntekijöidensä kanssa, jotka ovat laittomasti käsitelleet asiakkaan dataa (Ryan, 2013). Käyttäjän on tärkeää tiedostaa, että sisäinen hyökkääjä, kuten palveluntarjoajan työntekijä voi olla uhaksi luottamuksellisuudelle (Kumar, Meena, Singh, & Vardhan, 2015).

Täysin luottamuksellinen datan käsittely pilviympäristössä on tavoite, mutta tällä hetkellä sitä ei voida saavuttaa ilman palveluntarjoajan pääsyä selkotekstiseen dataan (Rong ym., 2013). Ryanin (2013) mukaan tutkijat kuitenkin pyrkivät löytää teknologian avulla ratkaisun, jonka avulla datan omistajalle voitaisiin taata datan säilyminen luottamuksellisena.

4.2 Eheyteen liittyvät uhat

Eheydellä tarkoitetaan, että ainoastaan valtuutetut osapuolet voivat muokata dataa, ohjelmistoja tai laitteistoja. Datan eheys viittaa datan suojaamiseen, jotta dataa ei voida luvattomasti muokata, vääristellä tai poistaa. (Zissis & Lekkas, 2012.) Vaikka datan eheyden varmistaminen on erittäin tärkeää, ei sille ole kuitenkaan olemassa yleistä standardia (Rong ym., 2013).

Luottamuksellisuuden ohella myös eheyteen liittyvät uhat muodostavat yhden pilviympäristön suurimmista tuvallisuusriskeistä (AlZain ym., 2012). Eheys voi vaarantua useista eri syistä. Vuonna 2009 Google Docs –palvelussa tapahtui ohjelmistovirhe, josta aiheutui tietomurto (Cachin, Keidar, & Shraer, 2009). Cachin ym. (2009) toteavat myös Amazon S3 –palvelun kohdanneen hieman samankaltaisen laitteistosta johtuneen virheen, jonka johdosta käyttäjien tiedostoja korruptoitui. Datan eheys vaarantuu pilviympäristössä sen ulkoistamisen takia. Koska data sijaitsee palveluntarjoajan infrastruktuurissa, menettää käyttäjä datan hallinnan. Siksi dataa on mahdollista myös muokata ilman omistajan suostumusta (Rong ym., 2013).

Datan eheys voidaan varmistaa estämällä valtuuttamaton pääsy. Tämä voidaan toteuttaa esimerkiksi hyvillä pääsynhallintakeinoilla. Mikäli datan eheys kuitenkin vaarantuu, voivat pääsynhallintakeinot auttaa määrittämään datan eheyttä uhanneen osapuolen. (Zissis & Lekkas, 2012). Toisaalta valtuuttamattoman pääsyn varmistaminen ei välttämättä aina ole riittävä tapa varmistaa eheyttä, sillä data saattaa korruptoitua jo siirtovaiheessa (Cachin ym., 2009).

Pilviympäristön datan eheyden tarkistamiseen on olemassa useita keinoja. Myös tavanomaiset keinot datan eheyden tarkistamiseksi toimivat pilviympäristössä. (D. Puthal ym., 2015.) Tavanomaiset keinot eivät kuitenkaan ole kovin tehokkaita, sillä ne vaativat datan lataamisen pois pilviympäristöstä paljon kaistanleveyttä ja vieden paljon aikaa (B. Wang, Li, & Li, 2012). Kolmannet osapuolet tarjoavat jo keinoja, joiden avulla datan eheys voidaan varmistaa ilman yksityisen informaation sisällön paljastumista. Identiteetin salassapito kolmannen osapuolen tarkastajilta on tosin vielä avoin kysymys, johon tutkijat pyrkivät löytämään ratkaisuja. (D. Puthal ym., 2015.)

4.3 Saatavuuteen liittyvät uhat

Saatavuudella viitataan siihen, että kohde (esimerkiksi data, ohjelmisto tai laitteisto) on valtuutetun osapuolen saatavissa sekä käytettävissä tarpeen vaatiessa (Zissis & Lekkas, 2012). Järjestelmän kohdalla saatavuus käsittää muun muassa sen, että järjestelmän tulee pystyä jatkamaan toimintaa esimerkiksi tietomurron tapahtuessa (D. Puthal ym., 2015; Zissis & Lekkas, 2012). Varsinkin datan kohdalla saatavuus rasittaa paljon verkkoa, sillä dataa siirretään ja käsitellään yhä enenevässä määrin (Zissis & Lekkas, 2012).

Pilviympäristössä datan saatavuuteen vaikuttaa esimerkiksi itse pilvipalvelun saatavuus, onko palveluntarjoaja toiminnassa vielä tulevaisuudessa ja huolehtiiko palveluntarjoaja myös varmuuskopioinnista (Almulla & Yeun, 2010). Saatavuuden osalta käyttäjä on kuitenkin täysin riippuvainen palveluntarjoajasta. Palveluntarjoaja voi lakata tarjoamasta palvelua esimerkiksi taloudellisista syistä tai johtuen ongelmista ohjelmistojen tai palvelimien kanssa (Kumar ym., 2015). Saatavuutta voidaan uhata myös esimerkiksi palvelunestohyökkäyksillä. Nämä hyökkäykset perustuvat huomattavaan määrään kutsuja, jolloin tietty hyökkäyksen kohteena olevan palvelun saatavuutta voidaan uhata. (Z. Xiao & Y. Xiao, 2013.)

Pilvipalveluiden saatavuutta säädellään yleensä palvelutasosopimuksilla (engl. *service level agreement*). Nämä palvelutasosopimukset voivat kertoa saatavuuden vähimmäismäärän esimerkiksi prosenttilukuna. Palvelutasosopimuksilla ei kuitenkaan tavanomaisesti kateta eheyteen tai luottamuksellisuuteen liittyviä ongelmia (Z. Xiao & Y. Xiao, 2013). Siksi saatavuus on attribuuttina pilvilaskennan parissa hieman poikkeava. Palvelutasosopimukset ovat ainoastaan sopimuksia, eivätkä konkreettisia keinoja, joilla saatavuus voidaan taata. Palvelutasosopimuksilla on kuitenkin

merkittävä rooli pilvilaskennan saatavuudessa. Mikäli palvelutasosopimuksen mukaista saatavuutta ei tavoiteta, voi asiakas helposti menettää luottamuksen palveluntarjoajaan (Z. Xiao & Y. Xiao, 2013).

Saatavuus on varsinkin palveluntarjoajan kannalta suuri huolenaihe (Rong ym., 2013). Koska pilvipalvelut tulee olla saatavilla kaikkina vuorokauden aikoina, vaatii saatavuuden varmistaminen palveluntarjoajalta mittavia panostuksia (Subashini & Kavitha, 2011). Pilviympäristössä tapahtuva käyttökatko vaikuttaa yhtäaikaisesti suureen määrään asiakkaita. Esimerkiksi Amazonin palvelussa ollut käyttökatko vaikutti yhtäaikaisesti useaan verkkosivustoon, joihin kuului muun muassa Reddit ja Foursquare. (Rong ym., 2013).

Almullan ja Yeun (2010) mukaan paras keino varmistaa saatavuus on välttää siihen kohdistuvia uhkia. Saatavuuteen kohdistuvien uhkien tunnistaminen on kuitenkin haasteellista. Pilviympäristössä saatavuuden kohdistuvat uhat eivät ole ainoastaan ulkoisia, kuten tavallisessa IT-ympäristössä. Saatavuus voidaan pyrkiä varmistamaan varautumalla mahdollisiin palvelunestohyökkäyksiin sekä laitteiston tai ohjelmiston virheisiin (Subashini & Kavitha, 2011).

5 YHTEENVETO

Pilvilaskenta on tehokas konsepti, joka tarjoaa matalilla kustannuksilla tehokkaita ja nopeasti skaalautuvia laskentaresursseja. Laskentaresurssit tarjotaan palveluina Internetin välityksellä. Tarjottavat palvelut ovat helppokäyttöisiä ja aina saatavilla esimerkiksi matkapuhelimella tai kannettavalla tietokoneella. Pilvilaskenta on helppo tapa lisätä esimerkiksi laskentakapasiteettia ilman mittavia rahallisia panostuksia uuteen infrastruktuuriin. Pilvilaskennan merkittävät hyödyt ovat viime aikoina kannustaneet käyttäjiä siirtymään sen pariin. Tästä johtuen pilvilaskennasta on muodostunut yksi IT-alan nopeimmin kasvavista segmenteistä (Popović & Hocenski, 2010).

Pilvilaskenta mallina koostuu useista komponenteista. Mell ja Grance (2011) ovat antaneet pilvilaskennasta kattavan määritelmän. He tunnistavat pilvilaskennalle viisi ominaista pääpiirrettä, kolme palvelumallia sekä neljä käyttöönottomallia. Keskeisimpänä ovat palvelumallit, jotka rakentuvat kerroksittain. Nämä mallit ovat Infrastructure-as-a-Service, Platform-as-a-Service sekä Software-as-a-Service. Koska mallit rakentuvat kerroksittain, perivät ne alempien kerroksiensa ominaisuudet. Asialla on myös kääntöpuoli, sillä ominaisuuksien lisäksi periytyvät myös turvallisuusongelmat sekä uhat. Jokainen malli toimii kuitenkin itsenäisenä kokonaisuutena, joten malleihin kohdistuu myös eroavia turvallisuusongelmia.

Tutkielman tarkoituksena oli vastata tutkimuskysymykseen: millaisia tietoturvaongelmia pilvilaskennan palvelumalleihin liittyy? IaaS-malliin keskeisimmät löydökset osoittivat mallin tietoturvaongelmien muodostuvan virtualisoinnista. IaaS-mallissa käyttäjällä on parempi kontrolli turvallisuudesta, kunhan alustan virtualisointiohjelmisto on aukoton. Virtualisoinnin turvallisuuden kannalta isäntätietokoneiden suojaaminen on kriittistä.

PaaS-mallin kohdalla vastuu turvallisuudesta jakautuu käyttäjälle sekä palveluntarjoajalle. PaaS-mallin turvallisuusongelmat liittyvät turvalliseen ohjelmistokehittämiseen. Uhkia PaaS-mallin turvallisuudelle aiheuttaa kolmansien osapuolten web-komponenttien käyttäminen, nopeat kehityssyklit sekä tietämättömyys alla olevan infrastruktuurin turvallisuudesta. Koska PaaS-

malli rakentuu IaaS-mallin päälle, periytyvät IaaS-mallin turvallisuusongelmat. Palveluntarjoajan kannalta infrastruktuurin suojaaminen vaikuttaa merkittävästi PaaS-mallin turvallisuuteen.

SaaS-malli perii alempien kerrosten turvallisuusongelmat. SaaS-malliin kohdistuvat merkittävimmät turvallisuusongelmat aiheutuvat vastuunjaosta, web-ohjelmiston turvallisuudesta sekä identiteetin hallinasta ja pääsynvalvonnasta. Vastuunjako tarkoittaa käyttäjän kannalta täydellistä riippuvuutta palveluntarjoajasta ja palveluntarjoajan turvallisuudesta. Web-ohjelmiston turvallisuus on myös merkittävässä roolissa, sillä 39% kaikista hyökkäyksistä kohdistuu nimenomaan ohjelmistokerrokseen (Baker ym., 2008). Identiteetin hallintaan sekä pääsynvalvontaan liittyvät heikkoudet ovat yksi kymmenestä suurimmasta web-applikaatioihin kohdistuvista riskeistä. SaaS-malli monimutkaistaa näiden funktioiden toimintaa.

Toiseksi tutkimuskysymykseksi asetettiin: millaisia uhkia pilviympäristö muodostaa datan luottamuksellisuudelle, eheydelle sekä saatavuudelle? Tutkielman keskeisin löydös osoitti pilviympäristön muodostavan datalle uudenlaisia uhkia, jotka eivät välttämättä olisi läsnä paikallisessa tallennustilassa. Nämä uhat aiheutuvat datan ulkoistamisesta sekä moniasiakkuusmallista, jotka vaikeuttavat merkittävästi datan turvallisuuden hallitsemista.

Suurin luottamuksellisuuteen kohdistuva uhka aiheutuu datan ulkoistamisesta eri lainsäädännöllisille alueille. Myös datan eheys voi vaarantua ulkoistamisesta aiheutuen. Pilviympäristössä eheyden varmistaminen on haastavaa. Vaikka eheyden varmistaminen on tärkeää, ei sille kuitenkaan ole yleistä standardia (Rong ym., 2013). Saatavuuteen vaikuttaa merkittävästi palveluntarjoajan toiminta sekä varmuuskopiointi. Saatavuutta uhkaa käyttäjän täysi riippuvuus palveluntarjoajasta., sillä palveluntarjoaja voi lakata tarjoamasta palveluita esimerkiksi taloudellisista syistä. Palvelunestohyökkäykset ovat vakavia saatavuuteen kohdistuvia uhkia.

Datan luottamuksellisuus ja eheys ovat suurimpia huolenaiheita pilviympäristön datan turvallisuudessa. Koska luottamuksellisuutta ja eheyttä ei voida täysin varmistaa, olisivat ne tulevaisuudessa mielenkiintoisia tutkimuskohteita. Tutkia voisi esimerkiksi sitä, miksi attribuuttien varmistaminen on haasteellista ja millä keinoin täydellinen luottamuksellisuus sekä eheys voitaisiin saavuttaa. Toisaalta pilvipalvelut vaihtelevat merkittävästi tallennustilasta valmiisiin ohjelmistoihin, joten täysin toimivan mallin rakentaminen saattaisi olla haasteellista. Luottamuksellisuus ja eheys voivat olla yksinkertaisempia saavuttaa silloin, kun pilvipalvelua käytetään ainoastaan tallennustilana.

Tämän tutkielman tarkoituksena oli vastata esitettyihin tutkimuskysymyksiin. Tutkielma suoritettiin kirjallisuuskatsauksena, ja aineisto kerättiin Google Scholar –palvelua käyttäen. Aineistona käytettiin pääasiassa tieteellisiä julkaisuja. Julkaisuja valittaessa kiinnitettiin huomiota niiden julkaisupäivämäärään, viittausten määrään sekä siihen, olivatko julkaisut vertaisarvioituja. Käytetyt lähteet taulukoitiin. Taulukkoon kirjattiin myös

lähteistä edellä mainitut seikat. Erilaiset yritysraportit ynnä muut julkaisut edustavat ei-akateemista aineistoa, jota tutkielmassa käytettiin harkinnanvaraisesti. Tutkielman rajoitteeksi osoittautui liian laajat tutkimuskysymykset. Pilvilaskennan turvallisuusongelmia ei kovinkaan usein käsitellä palvelumalleittain, mutta tutkielma kuitenkin todistaa kyseisen lähestymistavan mahdolliseksi sekä toimivaksi.

LÄHTEET

A. Behl, & K. Behl. (2012). An analysis of cloud computing security issues. In *Information and Communication Technologies (WICT), 2012 World Congress on* (pp. 109–114). https://doi.org/10.1109/WICT.2012.6409059

Abbas, R., Farooq, A., & Afghan, S. (2015). A Security Model for SaaS in Cloud Computing. *University of Engineering and Technology Taxila. Technical Journal*, *20*(4), 103–110.

Agmon Ben-Yehuda, O., Ben-Yehuda, M., Schuster, A., & Tsafrir, D. (2012). The Resource-as-a-service (RaaS) Cloud. In *Proceedings of the 4th USENIX Conference on Hot Topics in Cloud Ccomputing* (pp. 12–12). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2342763.2342775

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*(Journal Article), 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. *arXiv:1609.01107 [Cs]*. Retrieved from http://arxiv.org/abs/1609.01107

Almulla, S. A., & Yeun, C. Y. (2010). Cloud computing security management. In *2010 Second International Conference on Engineering System Management and Applications* (pp. 1–7).

AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). Cloud Computing Security: From Single to Multi-clouds. In *2012 45th Hawaii International Conference on System Sciences* (pp. 5490–5499). https://doi.org/10.1109/HICSS.2012.153

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A View of Cloud Computing. *Commun. ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Baker, W. H., Hylender, C. D., & Valentine, J. A. (2008). Verizon Business 2008 Data Breach Investigations Report. Retrieved from http://verizonbusiness.com/resources/databreachreport.pdf

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities (pp. 5–13). Presented at the High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on, Ieee.

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 Gener. Comput. Syst.*, *25*(6), 599–616. https://doi.org/10.1016/j.future.2008.12.001

Cachin, C., Keidar, I., & Shraer, A. (2009). Trusting the Cloud. *SIGACT News*, *40*(2), 81–86. https://doi.org/10.1145/1556154.1556173

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647–651). https://doi.org/10.1109/ICCSEE.2012.193

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance amp; Security. In *2013 International Conference on Availability, Reliability and Security* (pp. 546–555). https://doi.org/10.1109/ARES.2013.72

Choudhary, V. (2007). Software as a Service: Implications for Investment in Software Development. In *40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007* (p. 209a–209a). https://doi.org/10.1109/HICSS.2007.493

Cloud Security Alliance. (2009). Security Guidance For Critical Areas of Focus in Cloud Computing. *Cloud Security Alliance*, (Journal Article).

D. Puthal, B. P. S. Sahoo, S. Mishra, & S. Swain. (2015). Cloud Computing Features, Issues, and Challenges: A Big Picture. In *Computational Intelligence and Networks (CINE), 2015 International Conference on* (pp. 116–123). https://doi.org/10.1109/CINE.2015.31

Dawoud, W., Takouna, I., & Meinel, C. (2010). Infrastructure as a service security: Challenges and solutions. In *2010 The 7th International Conference on Informatics and Systems (INFOS)* (pp. 1–8).

Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. In *2010 24th IEEE International Conference on Advanced Information Networking and Applications* (pp. 27–33). https://doi.org/10.1109/AINA.2010.187

Duan, Y., Fu, G., Zhou, N., Sun, X., Narendra, N. C., & Hu, B. (2015). Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends. In *2015 IEEE 8th International Conference on Cloud Computing* (pp. 621–628). https://doi.org/10.1109/CLOUD.2015.88

Ertaul, L., Singhal, S., & Saldamli, G. (2010). Security Challenges in Cloud Computing. *Proceedings of the 2010 International Conference on Security and Management SAM'10*. Retrieved from https://www.researchgate.net/publication/267697749_Security_Challenges_in_Cloud_Computing

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud computing and grid computing 360-degree compared (pp. 1–10). Presented at the Grid Computing Environments Workshop, 2008. GCE'08, Ieee.

Gajek, S., Liao, L., & Schwenk, J. (2007). Breaking and Fixing the Inline Approach. In *Proceedings of the 2007 ACM Workshop on Secure Web Services* (pp. 37–43). New York, NY, USA: ACM. https://doi.org/10.1145/1314418.1314425

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The Characteristics of Cloud Computing. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 275–279). https://doi.org/10.1109/ICPPW.2010.45

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.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2003). *Tutki ja kirjoita* (6.-9. painos). Kustannusosakeyhtiö Tammi.

Hussein, N. H., & Khalid, A. (2016). A survey of Cloud Computing Security challenges and solutions. *International Journal of Computer Science and Information Security*, *14*(1), 52–56.

IBM. (2014). Manage identities and access for continuous compliance and reduced risk.

Kim, D., & Vouk, M. A. (2014). A survey of common security vulnerabilities and corresponding countermeasures for SaaS. In *2014 IEEE Globecom Workshops (GC Wkshps)* (pp. 59–63). https://doi.org/10.1109/GLOCOMW.2014.7063386

Kumar, M., Meena, J., Singh, R., & Vardhan, M. (2015). Data outsourcing: A threat to confidentiality, integrity, and availability (pp. 1496–1501). Presented at the Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, IEEE.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems*, *51*(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, Inc.

Mell, P. M., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Gaithersburg, MD, United States: National Institute of Standards & Technology.

OWASP. (2013). The Ten Most Critical Web Application Security Risks. Retrieved from https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf

Popović, K., & Hocenski, Ž. (2010). Cloud computing security issues and challenges (pp. 344–349). Presented at the MIPRO, 2010 proceedings of the 33rd international convention, IEEE.

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Special Issue on Recent Advanced Technologies and Theories for Grid and Cloud Computing and Bio-Engineering*, *39*(1), 47–54. https://doi.org/10.1016/j.compeleceng.2012.04.015

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, *86*(9), 2263–2268. https://doi.org/10.1016/j.jss.2012.12.025

Sabahi, F. (2011). Cloud computing security threats and responses (pp. 245–249). Presented at the Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, IEEE.

Sandikkaya, M. T., & Harmanci, A. E. (2012). Security Problems of Platform-as-a-Service (PaaS) Clouds and Practical Solutions to the Problems. In *2012*

IEEE 31st Symposium on Reliable Distributed Systems (pp. 463–468). https://doi.org/10.1109/SRDS.2012.84

Savu, L. (2011). Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges. In *2011 International Conference on Computer and Management (CAMAN)* (pp. 1–4). https://doi.org/10.1109/CAMAN.2011.5778816

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

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. https://doi.org/10.1016/j.jnca.2010.07.006

Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security Privacy*, *8*(6), 24–31. https://doi.org/10.1109/MSP.2010.186

Wang, B., Li, B., & Li, H. (2012). Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. In *2012 IEEE Fifth International Conference on Cloud Computing* (pp. 295–302). https://doi.org/10.1109/CLOUD.2012.46

Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D., & Karl, W. (2008). Scientific Cloud Computing: Early Definition and Experience. In *2008 10th IEEE International Conference on High Performance Computing and Communications* (pp. 825–830). https://doi.org/10.1109/HPCC.2008.38

Yang, J., & Papazoglou, M. P. (2002). Web Component: A Substrate for Web Service Reuse and Composition. In *Advanced Information Systems Engineering* (pp. 21–36). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-47961-9_5

Younis, Y. A., Merabti, M., & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. *Liverpool John Moores University, United Kingdom, Tech.Rep*, (Journal Article).

Z. Xiao, & Y. Xiao. (2013). Security and Privacy in Cloud Computing. *IEEE Communications Surveys & Tutorials*, *15*(2), 843–859. https://doi.org/10.1109/SURV.2012.060912.00182

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006