Teemu Manninen

PILVIPALVELUIDEN PALVELU-TASOSOPIMUSTEN TIETOTURVANÄKÖKULMA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Manninen, Teemu
Pilvipalveluiden palvelutasosopimusten tietoturvanäkökulma
Jyväskylä: Jyväskylän yliopisto, 2023, 35 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Riekkinen, Janne

Pilvipalveluiden suosio on kasvanut huomattavasti niiden tarjoamien etujen, kuten skaalautuvuuden, saavutettavuuden ja kustannustehokkuuden vuoksi. Monista eduista huolimatta datan tallentaminen pilveen ja sen käsitteleminen pilvessä aiheuttaa asiakkaille suurta huolta yksityisyyteen ja tietoturvaan liittyen. Palvelutasosopimukset ovat palveluntarjoajien ja asiakkaiden välisiä lainvoimaisia sopimuksia, joissa määritellään kyseessä olevan palvelun laatu, sen taso sekä osapuolten roolit ja vastuut. Palvelun muihin ominaisuuksiin, kuten suorituskykyyn ja saatavuuteen verrattuna palvelutasosopimuksissa ei kuitenkaan kuvata tietoturvaan liittyviä tekijöitä riittävän kattavasti. Tämä tutkielma toteutettiin kirjallisuuskatsauksena ja siinä tarkasteltiin pilvipalveluiden palvelutasosopimuksia keskittyen niiden tietoturvanäkökulmaan. Kirjallisuuskatsauksen tarkoituksena oli löytää esiin nousevia haasteita liittyen tietoturvan esittämiseen pilvipalveluiden palvelutasosopimuksissa, sekä löytää kirjallisuudessa ehdotettuja ratkaisuja näihin haasteisiin. Lisäksi tutkielmassa pyrittiin muodostamaan ajantasainen kuva käytössä olevista menetelmistä perehtymällä nykyisiin alalla vallitseviin käytänteisiin ja toimenpiteisiin tietoturvan tason kuvaamiseksi. Keskeisimmät tutkielmassa havaitut haasteet liittyivät tietoturvan reaaliaikaiseen monitorointiin, työkalujen automaattiseen toimeenpanoon sekä tietoturvan määrällistämiseen ja sen tason mittaamiseen. Tutkielmassa esitetyt ratkaisut keskittyivät joko yhden tai useamman haasteen ratkaisemiseen. Ratkaisuille oli yhteistä olemassa olevien viitekehysten laajentaminen tai parantaminen. Jotta asiakkaat kykenisivät vertailemaan tietoturvan tasoa eri palveluntarjoajien välillä, ratkaisujen omaksumisen tulisi olla yhtenäistä palveluntarjoajien kesken.

Asiasanat: pilvipalvelu, palvelutasosopimus, tietoturva, pilvilaskenta

ABSTRACT

Manninen, Teemu
Information security aspect of cloud services' service level agreements
Jyväskylä: University of Jyväskylä, 2023, 35 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Riekkinen, Janne

The use of cloud services has become increasingly popular due to its many benefits, such as scalability, accessibility, and cost-effectiveness. However, the security of data stored and processed on cloud services is still a major concern for the consumers. Service level agreements are legislative contracts between the cloud service provider and the customer, in which the quality of service, and the roles and responsibilities are defined. However, the security aspect isn't covered well enough in the service level agreements compared to other attributes such as performance and availability. The methodology of this thesis was a literature review which investigated the information security aspect of cloud services' service level agreements. The aim of the literature review was to find the challenges in presenting information security in the service level agreements of cloud services, as well as presented solutions to these challenges. In addition, the state-of-the-art practices of presenting the security level of cloud services were discussed in the thesis. The primary challenges found in the literature review were related to real-time monitoring of the security level, automatic implementation of security tools, and quantifying and measuring security. The solutions found in the thesis focused on extending existing frameworks or improving them. For consumers to be able to compare the security levels of different service providers, the adaptation of the solutions should be consistent among the service providers.

Keywords: cloud service, service level agreement, information security, cloud computing

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Datan kysyntä sekä verkkokäyttäjien määrä ovat kasvaneet merkittävästi viime vuosina. Lisäksi perinteisestä IT-infrastruktuurista ja sen hallinnoinnista on tullut kallista. Näin on syntynyt tarve ulkoistetuille IT-ratkaisuille. (Tabrizchi & Kuchaki Rafsanjani, 2020.) Pilvilaskenta on mahdollistanut tietoteknisten resurssien tarjoamisen asiakkaille palveluna verkon välityksellä. Pilvipalveluiden yleistymisellä on ollut valtava vaikutus IT-alaan, kun palveluntarjoajat pyrkivät tarjoamaan toinen toistaan tehokkaampia, luotettavampia ja kustannustehokkaampia pilvialustoja. Myös yritykset ovat alkaneet muokkaamaan liiketoimintamallejaan hyötyäkseen pilvipalveluiden tuomista eduista. (Verma & Kaushal, 2011.) Monista eduista huolimatta pilvipalveluihin liittyy myös ongelmia ja haasteita. Merkittävimpinä näistä on mainittu turvallisuuden ja yksityisyyden haasteet (Halabi & Bellaiche, 2018; Khalil, Khreishah & Azeem, 2014; Verma & Kaushal, 2011). Pilvipalveluiden alle kuuluu huomattava määrä erilaisia teknologioita sekä lähestymistapoja, jonka vuoksi myös tietoturvan huomioiminen on monimutkaista (Rak ym., 2013).

Tarjotun pilvipalvelun laadusta ja tasosta sekä osapuolten vastuista ja rooleista sovitaan asiakakkaan ja palveluntarjoajan solmimassa palvelutasosopimuksessa (Goo, Kishore, Rao & Nam, 2009). On kuitenkin havaittu, että nykyiset palvelutasosopimukset keskittyvät pääasiallisesti saatavuuteen ja suorituskykyyn eivätkä huomioi tietoturvaa riittävästi (Bernsmed, Jaatun, Meland & Undheim, 2011; Nugraha & Martin, 2022). Näin ollen asiakkaalle saattaa jäädä epävarmuus hankkimansa palvelun tietoturvan tasosta. Viime vuosina pilvipalveluista onkin tullut yksi merkittävimmistä aiheista tietoturvan tutkimuksessa (Tabrizchi & Kuchaki Rafsanjani, 2020). Tässä tutkielmassa käsitellään pilvipalveluita ja niiden palvelutasosopimuksia. Aihetta on rajattu keskittymään näiden molempien tietoturvanäkökulmaan. Aiheeseen liittyvässä tutkimuksessa ja kirjallisuudessa voidaan havaita paljon haasteita ja avoimia kysymyksiä. Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Mitä haasteita liittyy tietoturvanäkökulmaan pilvipalveluiden palvelutasosopimuksissa?

- Mitä ratkaisuja pilvipalveluiden palvelutasosopimusten tietoturvanäkökulman haasteisiin on esitetty?

Tutkielma on toteutettu kirjallisuuskatsauksena. Lähdekirjallisuuden etsimiseen on käytetty Google Scholar- ja JYKDOK-tietokantoja. Hakusanoina on käytetty seuraavia termejä tai niiden yhdistelmiä: ”Cloud computing”, ”Cloud services”, ”Cloud Security”, ”Service level agreement”, ”SLA”. Lähteiden valinnassa on pyritty ottamaan huomioon viittausten määrä ja ajantasaisuus. Moni lähteistä kuitenkin ajoittuu vuoden 2010 lähelle, sillä pilvipalveluiden suosio alkoi kasvaa ja käyttö yleistyä sinä ajankohtana. Lisäksi aihe on suhteellisen spesifi, jonka vuoksi viittausten määrät eivät ole kaikissa aihetta koskevissa julkaisuissa suuria.

Tutkielman rakenne koostuu johdannosta, kolmesta sisältöluvusta sekä yhteenvedosta. Ensimmäisessä sisältöluvussa käsitellään ensin pilvipalveluita yleisesti sekä palvelu- ja käyttöönottomalleittain, ja sen jälkeen pilvipalveluiden tietoturvaa eri palvelu- ja käyttöönottomalleissa. Toisessa sisältöluvussa perehdytään palvelutasosopimuksiin, niiden tarkoitukseen, sisältöön sekä elinkaareen. Lisäksi luvussa tarkennutaan erityisesti pilvipalveluita koskeviin palvelutasosopimuksiin. Kolmannessa sisältöluvussa vastataan aluksi ensimmäiseen tutkimuskysymykseen tuomalla esiin kirjallisuudessa esiintyneitä tietoturvan haasteita pilvipalveluiden palvelutasosopimuksissa. Tämän jälkeen vastataan toiseen tutkimuskysymykseen esittämällä kirjallisuudesta löytyviä ratkaisuehdotuksia ilmenneisiin haasteisin. Lisäksi luvussa keskustellaan nykyisistä tietoturvaa koskevista toimintatavoista ja käytänteistä, joiden mukaan pilvipalveluntarjoajat toimivat. Yhteenvetoluvussa keskustellaan kirjallisuuskatsauksen keskeisimmistä löydöksistä, johtopäätöksistä, tutkielman rajoittuneisuudesta sekä jatkotutkimuksen suunnasta.

2 PILVIPALVELUIDEN TIETOTURVA

Tässä luvussa käsitellään pilvipalveluita ja pilvilaskentaa. Aluksi käsitteet määritellään yleisellä tasolla, jonka jälkeen perehdytään pilvilaskennan ominaisuuksiin ja piirteisiin sekä esitetään pilvipalveluiden eri käyttöönotto- ja palvelumallit. Näihin liittyvät, tutkielmassa käytettävät käsitteet määritellään. Luvun lopuksi keskitytään pilvipalveluiden tietoturvaan sekä siinä esiintyviin haasteisiin ja määritellään siihen liittyviä käsitteitä.

2.1 Pilvipalvelut

Pilvipalvelu ja pilvilaskenta ovat jo vakiintuneita ja yleisessä käytössä olevia termejä. Termi ”pilvi” tässä asiayhteydessä alkoi yleistymään vuonna 2006, kun Googlen senaikainen toimitusjohtaja Eric Schmidt käytti sanaa kuvailemaan liiketoimintamallia, jossa tarjotaan palveluita internetin välityksellä (Zhang, Cheng & Boutaba, 2010). Tiedettävästi termi on kuitenkin tätä vanhempi, ja sitä on käytetty ensimmäisen kerran vuonna 1997 (Lin & Chen, 2012). Idea pilvipalveluiden kaltaisesta mallista syntyi jo vuonna 1966, kun Douglas Parkhillin kirjassa ”The Challenge of the Computer Utility” esitettiin ajatus mallista, jossa ihmisille tarjottaisiin tietoteknisiä resursseja ikään kuin julkishyödykkeiden tavoin (Zhang ym., 2010).

Yhdysvaltain kauppaministeriöön kuuluva The National Institute of Standards and Technology (NIST) julkaisi dokumentin vuonna 2011, joka koskee pilvilaskentaa ja sen määrittelyä. Dokumentin määritelmä pilvilaskennasta on yleisimmin käytetty ja sitä voidaan pitää virallisimpana määritelmänä termille. Siinä pilvilaskenta määriteltiin toimintamalliksi, joka mahdollistaa pääsyn aina saatavilla ja kaikkialla läsnä oleviin, jaettaviin ja konfiguroitaviin tietoteknisiin resursseihin, jotka ovat nopeasti otettavissa käyttöön tai poistettavissa käytöstä. Näihin resursseihin kuuluvat esimerkiksi palvelimet, tallennustila, tietoverkot sekä sovellukset. (Mell & Grance, 2011.) Pilvipalveluntarjoajat tarjoavat näitä resursseja asiakkailleen palveluina. Pilvipalvelut noudattavat käyttöpohjaisen

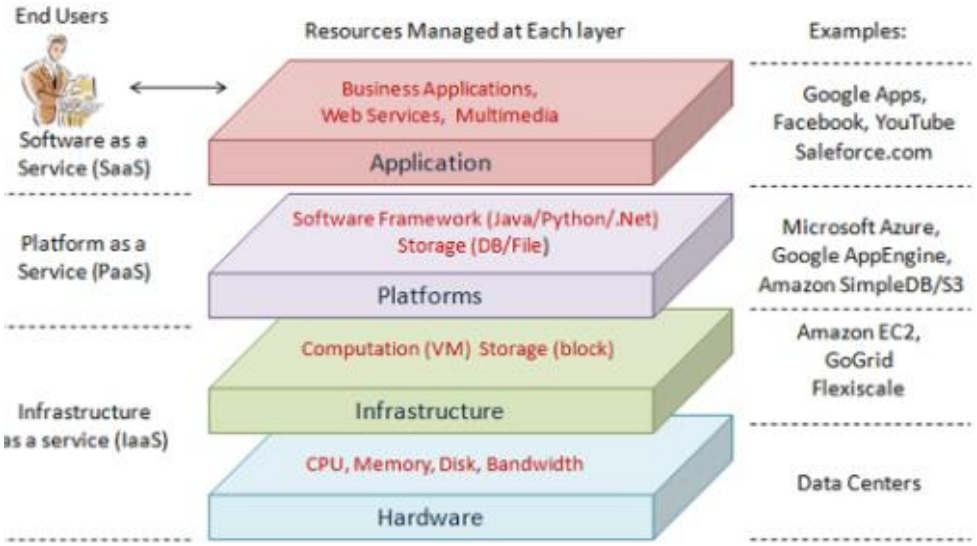
hinnoittelun perustuvaa mallia, jossa asiakas maksaa palveluista niiden käytön mukaan ja vastavuoroisesti palveluntarjoaja veloittaa asiakasta sen käytön mukaisesti. Mallista käytetään termejä ”pay-per-use” tai ”charge-per-use”. (Xiong & Chen, 2015.) Mallin ansiosta pilvipalveluista ei koidu suuria kustannuksia niiden käyttöönoton yhteydessä.

NIST:in dokumentissa lueteltiin viisi pilvipalveluiden keskeistä ominaisuutta. Niihin kuuluvat itsepalvelu tarvittaessa, laaja pääsy verkkoon, resurssien yhdistäminen, nopea elastisuus sekä mitattava palvelu (Mell & Grance, 2011). Ominaisuudet määriteltiin seuraavasti:

- Itsepalvelulla tarvittaessa tarkoitetaan asiakkaan mahdollisuutta varata resursseja palveluntarjoajalta tarpeidensa mukaan automaattisesti, ilman vuorovaikutusta ihmisen kanssa (Mell & Grance, 2011).
- Laajalla verkkoon pääsyllä tarkoitetaan asiakkaan pääsyä pilvipalvelun ominaisuuksiin verkon välityksellä eri laitteita, kuten puhelinta, kannettavaa tietokonetta tai tablettia käyttäen (Mell & Grance, 2011).
- Resurssien yhdistäminen tarkoittaa, että palveluntarjoajan resurssit ovat yhdistetty moniasiakaskäyttöön. Erilaisia fyysisiä ja virtuaalisia resursseja määrätään ja siirretään dynaamisesti asiakkaiden kysynnän mukaan. (Mell & Grance, 2011.)
- Nopea elastisuus tarkoittaa, että resursseja voidaan varata tai vapauttaa joustavasti ja nopeasti vastaamaan niiden kysyntää (Mell & Grance, 2011).
- Mitattavalla palvelulla tarkoitetaan resurssien käytön hallintaa ja optimointia hyödyntämällä palvelun tyypille sopivaa mittausmenetelmää. Resurssien käyttöä voidaan valvoa, ja raportoida. Tämä tarjoaa läpinäkyvyyttä käytetystä palvelusta niin palveluntarjoajalle kuin asiakkaalle. (Mell & Grance, 2011.)

2.1.1 Pilvipalveluiden palvelumallit

Yleisesti pilvipalveluita tarjotaan kolmena erilaisena palvelumallina. Näitä ovat ohjelmisto palveluna (Software-as-a-Service, SaaS), sovellusalusta palveluna (Platform-as-a-Service, PaaS) ja infrastruktuuri palveluna (Infrastructure-as-a-Service, IaaS) (Tabrizchi & Kuchaki Rafsanjani, 2020). Palvelumalleihin kuuluva arkkitehtuuri voidaan jakaa neljään kerrokseen: sovelluskerros, alustakerros, infrastruktuurikerros sekä laitteistokerros. (Zhang ym., 2010). Arkkitehtuuri on esitetty kuviossa 1.



KUVIO 1 Pilvilaskennan arkkitehtuuri (Zhang ym., 2010)

Ohjelmisto palveluna-mallissa, eli SaaS-mallissa asiakkaat käyttävät internetin välityksellä palveluntarjoajan tarjoamaa ohjelmistoa, joka pyörii palveluntarjoajan palvelimella. Nämä ohjelmistot ovat käytettävissä erilaisilla laitteilla joko verkkoselaimen tai sovelluksen käyttöliittymän kautta. Mallissa asiakas ei kontrolloi pilven infrastruktuuria eikä sovelluksen ominaisuuksia, lukuun ottamatta joitain mahdollisia sovelluksen käyttäjäkohtaisia asetuksia. (Mell & Grance, 2011.) Kun infrastruktuuri ei ole asiakkaan hallinnassa, ei asiakkaalle aiheudu infrastruktuurin ylläpitämiseen liittyviä kustannuksia (Basu ym., 2018). Lisäksi toisin kuin perinteisemmissä, ostettavissa ja paikallisesti asennettavissa ohjelmistoissa, SaaS-mallissa asiakkaat ostavat sovelluksen käyttöoikeuden tilaustyyppisesti palveluntarjoajalta (Benlian & Hess, 2011).

SaaS-mallista seuraavaa, tasoa alempana olevaa mallia kutsutaan sovellusalusta palveluna-malliksi, eli PaaS-malliksi. Siinä palveluntarjoaja tarjoaa asiakkaalle infrastruktuurin, jonka avulla asiakas voi kehittää sovelluksia ja ottaa käyttöön kehittämiään tai hankkimiaan sovelluksia (Mell & Grance, 2011). Kehittämisen ja käyttöönoton lisäksi PaaS-malliin sisältyy sovelluksen suunnittelu, testaaminen ja ylläpito (Velte, Velte & Elsenpeter, 2010). Mallissa palveluntarjoaja hallitsee alla olevaa pilvi-infrastruktuuria ja sen tukemia ohjelmointikieliä, kirjastoja, palveluita sekä työkaluja. Asiakas pystyy hallitsemaan käyttöönotettuja sovelluksia ja mahdollisesti myös joitain sovellusta ylläpitävän ympäristön konfiguraatioon liittyviä asetuksia. (Mell & Grance, 2011.)

Kolmesta mallista viimeisimpänä ja hierarkiassa alimpana mallina on infrastruktuuri palveluna-malli, eli IaaS-malli. Mallissa palveluntarjoaja tarjoaa asiakkaalle resursseja datan prosessointiin, tallennustilaa, verkkoyhteyksiä ja muita keskeisiä laskentaresursseja (Mell & Grance, 2011). Palvelimista, palvelinkaapeista ja datakeskuksista aiheutuvien kustannusten sijaan asiakkaat voivat suoraan vuokrata näitä resursseja palveluntarjoajilta ja maksaa näistä re-

sursseista käytön mukaan (Velte ym., 2010). Tässäkään mallissa asiakas ei hallinnoi alla olevaa pilvi-infrastruktuuria, mutta kykenee hallinnoimaan käyttöjärjestelmiä, tallennuskapasiteettia, käyttöönotettuja ohjelmistoja sekä mahdollisesti hallinnoimaan rajatusti tiettyjä verkkoyhteyksien komponentteja, esimerkiksi palomuureja (Mell & Grance, 2011). Vastatakseen asiakkaiden käyttämien resurssien laskevaan tai kasvavaan kysyntään, palveluntarjoajat käyttävät mallissa laajalti virtualisaatiota. Virtualisaation perusstrategiana on ottaa käyttöön itsenäisiä virtuaalikoneita, jotka ovat eristetty sekä perustana olevasta fyysisestä laitteistosta että muista virtuaalikoneista. (Dillon, Wu & Chang, 2010.)

Myös muita palvelumalleja pilvipalveluille on esitetty, yhtenä esimerkkinä niistä Dillonin ym. (2010) artikkelissa mainittu Data storage-as-a-Service, DaaS-malli, joka heidän mukaansa voidaan luokitella erikoistyyppiseksi IaaS-palvelumalliksi. Tässä tutkielmassa käsittellään kuitenkin vain kolmea, yleisesti hyväksyttyä ja määriteltyä mallia: SaaS, PaaS ja IaaS.

2.1.2 Pilvipalveluiden käyttöönottomallit

Pilvipalvelut voidaan luokitella niiden käyttöönottomallien mukaan. Yleisimpiä käyttöönottomalleja on neljä kappaletta. Niitä ovat yksityinen pilvi, yhteisöpilvi, julkinen pilvi sekä hybridipilvi. Näiden lisäksi on myös olemassa virtuaalinen yksityinen pilvi (engl. virtual private cloud). (Dillon ym., 2010.)

Yksityisen pilven mallissa pilvi-infrastruktuuri toimitetaan yhden organisaation käyttöön. Saman organisaation eri liiketoimintayksiköt voivat kuitenkin käyttää palvelua. Sen voi omistaa tai sitä voi hallinnoida joko organisaatio itse, jokin kolmas osapuoli tai jokin näiden yhdistelmä. (Mell & Grance, 2011.) Dillon ym. (2010) esittivät artikkelissaan syitä yksityisen pilvimallin houkuttelevuudelle. Sen avulla voidaan maksimoida ja optimoida olemassa olevien, organisaation sisäisten resurssien hyödyntäminen. Tietoturvaan, luottamukseen ja yksityisyyteen liittyvät huolenaiheet tekevät yksityisestä pilvestä hyvän vaihtoehdon organisaatioille. Myös datansiirrosta paikallisen IT-infrastruktuurin ja julkisen pilven välillä aiheutuu melko huomattavia kustannuksia. Lisäksi organisaatiot vaativat täyttä kontrollia palomuuriensa takana tapahtuvista kriittisistä tehtävistä. (Dillon ym., 2010.) Yksityinen pilvimalli tarjoaakin suurimman hallinnan turvallisuuden, luotettavuuden ja suorituskyvyn osalta. Mallia on kuitenkin kritisoitu sen samankaltaisuuden vuoksi perinteisiin palvelinfarmeihin nähden. (Zhang ym., 2010.)

Yhteisöpilvimallissa useampi organisaatio muodostaa ja jakaa yhteisesti saman pilvi-infrastruktuurin sekä vaatimukset ja toimintaperiaatteet (Dillon ym., 2010). Sitä voi hallinnoida ja sen voi omistaa yksi tai useampi yhteisön organisaatio, kolmas osapuoli tai jokin näiden yhdistelmä (Mell & Grance, 2011). Mallin huonona puolena on avoimena olevat kysymykset palveluiden käyttökatkoihin sekä sopimusten ja turvallisuuden vaikutuksiin liittyen, esimerkiksi datan levittyneisyys usealle organisaatiolle ja alueelle (Basu ym., 2018).

Julkisen pilven mallissa palveluita tarjotaan suurelle yleisölle tai suurille yrityksille. Mallin hyötynä on sen varma skaalautuvuus ja luotettavuus. (Basu ym., 2018.) Zhang ym. (2010) mukaan julkisen pilven mallissa hienojakoinen

datan, verkkojen ja turvallisuusasetusten hallinta on kuitenkin puutteellista, mikä voi olla haitaksi liiketoiminnalle. Asiakkaat voivat myös olla tietämättömiä siitä, minkä tyyppistä tallennustilaa palveluntarjoajat käyttävät sekä mihin maantieteelliseen sijaintiin asiakkaiden dataa tallennetaan. Tästä syystä organisaatiot joutuvat tekemään kompromisseja joidenkin turvallisuuteen liittyvien näkökulmien suhteen valitessaan julkisen pilven mallin. (Basu ym., 2018.) Mallissa palveluntarjoajalla on täysi omistus siitä sekä sen toimintaperiaatteista ja laskutusmallista (Dillon ym., 2010).

Hybridipilvimallissa pilvi-infrastruktuuri koostuu kahdesta tai useammasta erillisestä pilvi-infrastruktuurista, jotka ovat uniikkeja mutta ovat sidottuina toisiinsa teknologisilla ratkaisuilla, jotka mahdollistavat datan ja sovellusten siirrettävyyden (Mell & Grance, 2011). Malli tarjoaa julkiseen tai yksityiseen malliin nähden enemmän joustavuutta samalla mahdollistaen myös palveluiden laajentamisen tai supistamisen tarpeen mukaan. Huonona puolena mallissa on sen suunnittelun vaatima tarkkuus päätettäessä komponenttien parasta jakoa julkisen ja yksityisen pilven välillä. (Zhang ym., 2010.) Yhtenä esimerkkinä hybridimallin käyttötavasta Dillon ym. (2010) kertovat organisaation voivan rajata ei niin tärkeät ja toissijaiset toiminnallisuudet julkiseen pilveen, samalla hallitsemalla ydintoimintoja yksityisen pilven kautta. Näin organisaatio voi optimoida resurssien käyttöään parantaakseen ydinkompetenssejaan (Dillon ym., 2010).

Virtuaalinen yksityinen pilvi on vaihtoehtoinen ratkaisu vastaamaan sekä julkisen että yksityisen pilven rajoitteisiin. Se on alusta, joka pyörii julkisten pilvien päällä. Suurena erona on, että malli hyödyntää virtuaalista erillisverkkoa (VPN), mikä mahdollistaa palveluntarjoajille oman topologian ja turvallisuusasetusten suunnittelemisen. Virtuaalinen yksityinen pilvi virtualisoi palvelinten ja sovellusten lisäksi myös tiedonsiirtoverkon. (Zhang ym., 2010.)

2.2 Tietoturva

Pilvipalveluiden käytöllä on monia etuja organisaatioille, mutta lisäksi niiden käyttöön liittyy kuitenkin myös haasteita ja ongelmia. Mallin käyttö johtaa pilveen tallennettujen ja siellä käytettävien resurssien tietoturvan hallinnan menettämiseen, sillä organisaatiot ulkoistavat IT-resurssinsa ulkoisen osapuolen omistamille pilvialustoille (Al Morsy, Grundy & Ibrahim, 2011). Tietoturva onkin suuri huolenaihe pilvipalveluiden käyttöönottoon liittyen. Pilvipalveluiden käytön omaksumisesta seuraa abstraktiokerroksen syntyminen fyysisen tallennustilan tai palvelinten ja palvelun käyttäjän välille. Tällöin asiakkaan täytyy luottaa täysin pilvipalveluntarjoajaan informaationsa yksityisyyden ja tietoturvan suhteen. (Basu ym., 2018.) Lainsäädäntö on myös tärkeää ottaa huomioon, sillä resurssit voivat sijaita maantieteellisesti käytännössä missä maassa tahansa. Asiakkaan tulee noudattaa oman maansa lakeja ja lisäksi myös sen maan lakeja, jossa data on varastoituna. (de Chaves, Westphall & Lamin, 2010.)

Armbrust ym. (2010) mukaan turvallisuus onkin yleisimmin esitetty vastalause pilvipalveluiden käyttöön liittyen. Rachana, Banu, Ahammed ja Parameshachari (2017) esittivät artikkelissaan International Data Corporationin (IDC) vuonna 2009 suorittaman tutkimuksen pilvipalveluiden haasteista ja ongelmista. Tutkimuksen tulokset ovat esitettynä kuviossa 2. Tulosten mukaan tietoturvaa pidettiin pilvipalveluiden merkittävimpänä haasteena. Luna, Taha, Trapero ja Suri (2017) mainitsivat artikkelissaan tietoturvan varmistamisen ja läpinäkyvyyden olevan yhä edelleen kaksi päätekijää, jotka mahdollistavat asiakkaan luottamuksen pilvipalveluntarjoajiin. Lisäksi Tabrizchin ja Kuchaki Rafsanjanin (2020) mukaan pilvipalveluiden tietoturvaan ja yksityisyyteen liittyvät haasteet vaativat lisää tutkimusta. Voidaan siis todeta tietoturvan olleen alusta asti, ja olevan yhä edelleen suuri haaste pilvipalveluille.

KUVIO 2 IDC:n toteuttama tutkimus pilvipalveluiden haasteista

Tietoturvan tärkeitä ominaispiirteitä ovat luottamuksellisuus, eheys ja saatavuus. Niiden toteutumista pidetään turvallisten järjestelmien suunnittelun perustana. (Zissis & Lekkas, 2012.) Näiden piirteiden lisäksi Heiserin ja Nicolettin (2008) mukaan pilvipalveluiden uniikkien ominaisuuksien vuoksi riskienarviointia tarvitaan myös palautumisen, yksityisyyden ja oikeudellisten haasteiden, kuten säännösten noudattamisen ja auditoinnin suhteen. Pilvimalli mahdollistaakin uudenlaisia tietoturvahyökkäyksiä. Hyökkääjä voi esimerkiksi sijoittaa resurssinsa samaan paikkaan kohteensa resurssien kanssa. Tämän jälkeen hyökkääjän on mahdollista yrittää hyökätä virtualisaatiokerrokseen ja fyysiseen laitteistoon. (Hay, Nance & Bishop, 2011.)

2.2.1 Palvelumallien tietoturva

Pilvipalveluiden monimutkaisen luonteen vuoksi myös tietoturvan huomioiminen on haastavaa. Jokaisella palvelumallilla on erilaisia toteutustapoja, joka

tekee palvelumalleille standardoitujen tietoturvamallien kehittämisestä monimutkaista. Eri mallit voivat myös olla käytössä rinnakkain samalla pilvialustalla, mikä taas vaikeuttaa turvallisuuden hallintaa entisestään. (Al Morsy, Grundy & Müller, 2010.)

Ohjelmisto palveluna-mallissa eli SaaS-mallissa organisaation data tallennetaan palveluntarjoajan datakeskukseen yhdessä muiden asiakasorganisaatioiden datan kanssa. Lisäksi palveluntarjoaja voi replikoida dataa moniin eri maantieteellisiin sijainteihin korkean saatavuuden varmistamiseksi. Mallissa asiakkaan täytyy luottaa, että palveluntarjoaja käyttää kunnollisia toimenpiteitä tietoturvan takaamiseksi. (Subashini & Kavitha, 2011.) Palveluntarjoajan puutteellinen tietoturva web-sovelluksissa jättää pilvipalveluun haavoittuvuuksia. Tämä korostuu etenkin SaaS-mallissa. (Halabi & Bellaiche, 2017.) The Open Worldwide Application Security Project (OWASP, ei pvm.) listasi 10 suurinta web-sovellusten turvallisuusriskiä vuodelta 2021, joita ovat: epäonnistunut pääsynvalvonta, kryptografiset puutteellisuudet, erilaiset injektiot, kuten SQL-injektiot, turvaton suunnittelu, tietoturvan konfiguroinnin virheet, haavoittuvien ja vanhentuneiden komponenttien käyttö, identiteetinhallinnan ja autentikoinnin epäonnistuminen, ohjelmiston ja datan eheyden puuttellisuus, lokien ja turvallisuuden monitoroinnin puute sekä palvelinpuolen pyynnön väärentäminen. Pilvi-infrastruktuurissa ylläpidettävät web-sovellukset tulisikin validoida ja skannata mahdollisten haavoittuvuuksien löytämiseksi (Al Morsy ym., 2010). Web-sovellusten haavoittuvuuden lisäksi mallissa tulee kuitenkin ottaa huomioon myös muita tietoturvauhkia. Kun dataa siirretään verkon välityksellä, tulee palveluntarjoajan ottaa huomioon luonnollisesti myös tietoverkkojen ja tiedonsiirron turvallisuus. Halabin ja Bellaichen (2017) mukaan useimmat palveluntarjoajat yleensä suojautuvatkin näihin kohdistuvia hyökkäyksiä vastaan käyttämällä SSL- ja TLS-protokollia tietoliikenteen salaamiseen. Tiedonsiirtoon ja tietoturvaan kohdistuvat hyökkäykset eivät tietenkään ole yksinomaan SaaS-mallin ongelma, vaan ne koskevat tietoliikennettä yleisesti. SaaS-malli perii myös PaaS- ja IaaS-mallien tietoturvaongelmat, sillä malli toimii niiden päällä (Al Morsy ym., 2010).

Kun SaaS-malli perii alempien kerrosten tietoturvaongelmat, samalla logiikalla myös PaaS-malli perii sen alapuolella olevat IaaS-malliin liittyvät tietoturvaongelmat. PaaS-mallissa asiakas on vastuussa kehittämiensä ja ylläpitämiensä sovellusten tietoturvasta. Palveluntarjoajan vastuulla on eristää asiakkaidensa sovellukset ja työtilat toisistaan. (Takabi, Joshi & Ahn, 2010.) Moniasiakaskäyttö, tutkielmassa aiemmin määritelty pilvipalveluiden ominaisuus, aiheuttaa haasteita tietoturvalle myös PaaS-mallissa. Moniasiakaskäytön alusta isännöi ja suorittaa usean eri asiakkaan ohjelmistoja. Tämä tarjoaa pahantahtoisille käyttäjille suoria väyliä häiritä muiden komponenttien suorittamista. Alustassa tulee olla varmuus siitä, ettei minkään asiakkaan pahantahtoinen tai viallinen koodi pysty häiritsemään muiden käyttäjien koodin tai alustan itsensä suorittamista. Moniasiakaskäyttö voidaan tehdä turvalliseksi käyttöjärjestelmätasolla ottaen huomioon viisi keskeistä osa-aluetta. (Rodero-Merino, Vaquero, Caron, Muresan & Desprez, 2012.) Niitä ovat:

- Pääsynhallinta, mikä voidaan toteuttaa mekanismilla, joka valtuuttaa käyttäjän pyynnöt järjestelmäoperaatioiden suorittamiseen (Rodero-Merino ym., 2012).
- Integroitu palomuurin toiminnallisuus, kuten esimerkiksi IP Filter, IPsec-protokollat ja VPN-tekniikat. (Rodero-Merino ym., 2012)
- Datan salaus siirrettävänä olevalle tai tiedostojärjestelmään tallennetulle datalle. (Rodero-Merino ym., 2012)
- Muistialueiden suorittamisen estäminen, joka voidaan toteuttaa NX-lippuja (No execute) käyttämällä (Rodero-Merino ym., 2012).
- Prosessien eristäminen, joka voidaan toteuttaa mekanismeilla, jotka luovat erilliset osoiteavaruudet jokaiselle prosessille. Näin prosessi ei pääse käsiksi muistialueisiin sen osoiteavaruuden ulkopuolelta. (Rodero-Merino ym., 2012.)

PaaS-malli voi tarjota ohjelmointirajapintoja (API) erilaisten toiminnallisuuksien hallintaan. Nämä rajapinnat tulisi eristää muistitasolla. Lisäksi niissä tulisi olla implementoituna turvallisuusominaisuudet ja -standardit. (Al Morsy ym., 2010.) Ramgovindin, Eloffin ja Smithin (2010) mukaan virtuaalikoneet toimivat PaaS-kerroksen katalyytteina ja niitä täytyy suojata pilven haittaohjelmia vastaan. He luettelivat artikkelissaan olennaisiksi tekijöiksi sovellusten eheyden säilyttämisen sekä hyvin valvotut ja tarkat autentikoinnin tarkistukset datansiirrossa kaikissa verkon kanavissa.

Myös IaaS-mallissa virtuaalikoneiden turvallisuus on tärkeää. Niiden käyttöjärjestelmät ja työkuormat tulee suojata yleisiltä perinteisiin palvelimiin kohdistuvilta hyökkäyksiltä, kuten haittaohjelmilta ja viruksilta. (Al Morsy ym., 2010). Asiakkaiden vastuu turvallisuudesta kasvaa sitä mukaan, mitä alemmas hierarkiassa siirrytään (Iqbal ym., 2016). He voivat käyttää omia toimenpiteitä tietoturvan takaamiseksi omien tarpeiden ja riskien mukaisesti. Mallissa virtuaalikoneiden turvallisuus on asiakkaan vastuulla. (Al Morsy ym., 2010.) Basu ym. (2018) kuitenkin mainitsivat, että käyttäjät eivät voi yksin suojata virtuaalikoneiden luottamuksellisuutta täysin, sillä mikä tahansa sisäinen tai ulkoinen taho, joka omaa erikoisoikeudelliset käyttöoikeudet, pääsee lukemaan tai manipuloimaan virtuaalikoneessa sijaitsevia palveluita. Vaikka Al Morsy ym. (2010) mainitsivat virtuaalikoneiden turvallisuuden olevan asiakkaan vastuulla, heidän mukaansa kuitenkin jotkin virtuaalikoneen turvallisuuteen liittyvät tekijät, kuten virtuaalikoneen levykuvan sekä virtuaalikonemonitorin turvallisuus ovat palveluntarjoajan vastuulla. El Balmanyn, Asimin & Tbatoun (2018) mukaan palveluntarjoaja toimittaa ja hallinnoi koko arkkitehtuurin pinoa ja hallitsee virtuaalikonemonitoria tietoliikenteen kuunteluun. Heidän mukaansa asiakkaan vastuulle jää oman ympäristönsä turvaaminen sisäisiltä ja ulkoisilta uhkilta. Näin ollen kyseessä on jaettu vastuu tietoturvasta asiakkaan ja palveluntarjoajan kesken. Virtuaalikonemonitori on ohjelmisto, joka hallinnoi ja monitoroi virtuaalikoneita. Sen pitäminen mahdollisimman yksinkertaisena ja pienenä vähentää haavoittuvuuksien esiintymistä. (Basu ym., 2018.) Onnistuneilla hyökkäyksillä virtuaalikonemonitoreihin on mittavat seuraukset, sillä hyökkäys

vaikuttaa koko virtuaaliseen ympäristöön ja siinä sijaitseviin virtuaalikoneisiin vain yhden kohteen sijaan (Iqbal ym., 2016). Virtuaalikoneen tulisikin olla turvallinen sen juuritasolla niin, että mikään käyttöoikeus virtuaalisessa ympäristössä ei anna vieraalle mahdollisuutta päästä isäntäjärjestelmään käsiksi (Subashini & Kavitha, 2011).

2.2.2 Käyttöönottomallien tietoturva

Pilvipalveluiden palvelumallien lisäksi myös niiden eri käyttöönottomalleilla on eroavaisuuksia tietoturvan ja sen huomioimisen suhteen. Ne monimutkaistavat pilvipalveluiden tietoturvan kokonaisuutta entisestään.

Kuten aiemmin käsiteltiin, yksityisen pilven mallin voi omistaa joko organisaatio, kolmas osapuoli tai näiden yhdistelmä. Jos organisaatio operoi ja hallinnoi infrastruktuuria omissa tiloissaan, silloin mallin tietoturvaan ei liity uniikkeja lisähaasteita (Zissis & Lekkas, 2012). Muihin malleihin verrattuna yksityinen malli on tietoturvan kannalta paras vaihtoehto. Turvallisuus ja yksityisyys ovatkin sen ainoa suuri etu (Goyal, 2014). Vaikka yksityisen mallin tietoturvan arkkitehtuuri on luotettavampi muihin malleihin nähden, liittyy siihen silti riskejä ja haasteita. Virtualisointitekniikat ovat suosittuja yksityisen pilven mallissa. (Bhadauria & Sanyal, 2012.) Näin ollen aiemmin käsitellyt virtualisoinnin tietoturvan tekijät tulevat vahvasti esille tässä mallissa. Bhadauria ja Sanyal (2012) korostivat artikkelissaan virtuaalikonemonitoriin kohdistuvien riskien analysointia. Halabi ja Bellaiche (2017) mainitsivat virtuaalikoneen levykuvan ja virtuaalikoneen isäntäkoneesta toiseen siirtämisen turvallisuuden olevan välttämätöntä asiakkaiden arkaluonteisen tiedon turvaamiseksi. Isäntäkäyttöjärjestelmän turvallisuus ja ajantasaisuus on äärimmäisen tärkeää, sillä hyökkääjän hallitessa sitä, voi hän myös hallita muita käyttöjärjestelmiä. Isäntäkäyttöjärjestelmä tulisikin pitää minimaalisena ja jatkuvasti ajantasaisena. (Mathisen, 2011.) Organisaatioiden tulee myös olla määrittänyt omat turvallisuuspolitiikkansa turvatakseen järjestelmät sisäisiltä hyökkäyksiltä. Myös aikaisemmin käsitelty pääsynhallinta ehkäisee sisäisiä hyökkäyksiä. Lisäksi, jos organisaatio hallinnoi ja operoi pilvi-infrastruktuuria omissa tiloissaan, tulee fyysiseen turvallisuuteen liittyvät tekijät huomioida.

Julkisen pilven mallissa palveluntarjoajien tarjoamat turvallisuuden oletustoimenpiteet eivät välttämättä vastaa organisaatioiden omia yksityiskohtaisia vaatimuksia ja tarpeita (Goyal, 2014). Tietoturvan kolme tärkeää vaatimusta ovat jo aiemmin mainitut luottamuksellisuus, eheys ja saatavuus. Nämä tulee toteutua kaikissa datan elinkaaren vaiheissa (Bhadauria & Sanyal, 2012). Datan luottamuksellisuus on Verman ja Kaushalin (2011) mukaan yksi vaikeimmista asioista taata julkisen pilven mallissa. Kun julkiset pilvet kasvavat, samalla kasvaa myös pilvipalveluntarjoajan työvoiman määrä, ja näin yhä useammalla työntekijällä on pääsy asiakkaiden dataan. Tämä tarkoittaa sitä, että potentiaalisten luottamuksellisuutta rikkovien lähteiden määrä lisääntyy. (Verma & Kaushal, 2011.) Näin ollen myös julkisen pilven mallissa pääsynhallinta on tärkeää ottaa huomioon. Lisäksi tarve joustavuudelle, suorituskyvylle ja vikatoleranssille johtaa laajamittaiseen datan monistamiseen, josta seuraa hyökkääjälle

potentiaalisten kohteiden määrän lisääntyminen (Verma & Kaushal, 2011). Datan eheyden takaamiseksi voidaan noudattaa ACID-periaatetta. Lyhenne ACID tulee sanoista atomicity (atomisuus), consistency (yhdenmukaisuus), isolation (eristyneisyys) ja durability (pysyvyys). Tiivistetysti, atomisuus tarkoittaa, että transaktio suoritetaan täysin tai ei ollenkaan, yhdenmukaisuudella tarkoitetaan datan tilaa ennen ja jälkeen transaktion, eristyneisyydellä tarkoitetaan, että samanaikaiset transaktiot pidetään erillä toisistaan ja pysyvyydellä viitataan onnistumisen tai epäonnistumisen vaikutukseen transaktiolle. (Tabrizchi & Kuchaki Rafsanjani, 2020.) Palvelunestohyökkäykset ovat yksi suuri palveluiden ja datan saatavuuteen vaikuttava syy (Basu ym., 2018) Näitä hyökkäyksiä vastaan voidaan käyttää tunkeilijan havaitsemisjärjestelmiä (IDS). Ne tarjoavat tietoturvaan liittyviä lisätoimenpiteitä tutkimalla tietoliikennettä, lokitiedostoja ja käyttäjien toimintaa. (Vieira, Schulter, Westphall & Westphall, 2009.) Lisäksi on huomionarvoista, että Bernsmed ym. (2011) mukaan kaikkein ovelimmat hyökkäykset jäävät monesti havaitsematta. Myös luonnonilmiöt, kuten tulvat ja tulipalot voivat uhata datan saatavuutta (Basu ym., 2018). Niitä vastaan olisi järkevää suojautua valitsemalla datakeskukselle mahdollisimman turvallinen sijainti ja noudattamalla paloturvallisuutta. Julkisen pilven mallissa useat asiakkaat jakavat saman pilvi-infrastruktuurin, jolloin datavuodot asiakkaiden välillä ovat mahdollisia (Bhadauria & Sanyal, 2012). Niiden kohdalla tulee esiin datan eristämisen tärkeys.

Kuten aiemmin käsiteltiin, yhteisöpilvimallin voi omistaa yksi tai useampi yhteisön organisaatio, kolmas osapuoli tai näiden yhdistelmä. Se ei ole siis täysin yksityinen, joten siihen voidaan päätellä vaikuttavan edellä mainittujen julkisen sekä yksityisen pilven mallien tietoturvaongelmat. Sama pätee myös hybridipilvimalliin, sillä se on yhdistelmä yksityisiä ja julkisia malleja. Virtuaalinen yksityinen pilvi on julkisten pilvien päällä pyörivä alusta, jossa hyödynnetään VPN:ää. Sen myötä palveluntarjoajien on mahdollista suunnitella oma verkkotopologia ja turvallisuusasetukset. Palveluntarjoajien tulee siis ottaa huomioon näiden tietoturva sekä aiemmin läpikäydyt julkisen pilven tietoturvaongelmat. Voidaan huomata, että pilvipalveluiden tietoturva ei ole yksinomaan palveluntarjoajan eikä asiakkaan vastuulla, vaan kyseessä on jaettu vastuu. Palveluntarjoajat ja asiakkaat sopivat niin tietoturvan kuin muidenkin alueiden vastuista palvelutasosopimuksissa (Tabrizchi & Kuchaki Rafsanjani, 2020).

3 PALVELUTASOSOPIMUKSET

Tässä luvussa perehdytään palvelutasosopimuksiin. Aluksi määritellään palvelutasosopimus käsitteenä, jonka jälkeen tutustutaan niiden sisältöön, tarkoitukseen ja elinkaareen. Toisessa alaluvussa käsitellään palvelutasosopimuksia ja niihin liittyviä piirteitä pilvipalveluiden näkökulmasta.

3.1 Yleistä palvelutasosopimuksista

Palvelutasosopimuksia (Service Level Agreement, SLA) on käytetty 1980-luvulta lähtien monella osa-alueella, kuten tietoverkoissa ja web-palveluissa (Serrano ym., 2016). Palvelutasosopimus edustaa tarjottuun palveluun liittyvää sopimusta asiakkaan ja palveluntarjoajan välillä. (Rana, Warnier, Quillinan, Cojocarasu & Brazier, 2008). Palvelutasosopimusten peruspiirteisiin kuuluu Goo ym. (2009) mukaan keskeisten toimintaperiaatteiden, prosessien omistajien, heidän roolien ja vastuiden määritteleminen sekä tuotteen tai palvelun suorituskyvyn tavoitetasojen määritteleminen. Palvelutasosopimukset koostuvat joukosta palvelutasotavoitteita (Service Level Objective, SLO). Näitä voidaan arvioida mitattavan datan eli palvelutasomittareiden (Service Level Indicator, SLI) avulla. (Bernsmed ym., 2011.) Palveluntarjoajan tulee ylläpitää sopimuksessa määritelty palvelun laadun taso. Sopimuksen tulee myös sisältää rangaistuksiin liittyvät ehdot, mikäli palveluntarjoaja epäonnistuu toimittamaan palvelua sopimuksessa sovitulla tasolla. Sovittu rangaistus voi olla esimerkiksi palvelun käytöstä sovitun maksun väheneminen tai hinnan vähentäminen ja lisäkompensaatio seuraavan rikkomuksen sattuessa. Yleensä rahallisten sanktioiden suuruus riippuu asiakkaalle aiheutuneiden menetysten suuruudesta. (Rana ym., 2008.)

Kun tarkastellaan palvelutasosopimusten elinkaarta, voidaan sen ajatella jakautuvan eri vaiheisiin. Rana ym. (2008) mukaan näihin vaiheisiin kuuluvat: palveluntarjoajan löytäminen, palvelutasosopimuksen määrittely, sopimusehtojen hyväksyminen, monitorointi sopimusehtojen rikkomisen varalle, sopimuk-

sen irtisanominen sekä rangaistukset sopimusrikkomustilanteissa. Palveluntarjoajan löytämisen vaiheessa etsitään potentiaalisia, tiettyyn profiiliin sopivia palveluntarjoajia. Lopputuloksena on palveluntarjoaja, tai lista niistä, jotka tarjoavat asiakkaan tarpeisiin sopivia palveluita. Seuraava vaihe on palvelutasosopimuksen määrittely. Siinä voidaan käyttää nimen ja arvon pareja, joissa nimi viittaa tiettyyn palvelutasotavoitteeseen ja arvo kuvaa asiakkaan pyytämää laadun tai palvelun tasoa. Tämä vaihe vaikuttaa muihin vaiheisin, etenkin monitorointiin. Tämän jälkeinen vaihe on sopimusehtojen hyväksyminen. Vaiheessa on tärkeää olla yhteisymmärryksessä termistön semantiikan kanssa. (Rana ym., 2008.) Monet lähteet tuovat esiin sopimusten solmimiseen liittyvän neuvotteluvaiheen (Carvalho, Andrade, de Castro, Coutinho & Agoulmine, 2017; Dillon ym., 2010; Halabi & Bellaiche, 2017; Verma & Kaushal, 2011). Rana ym. (2008) eivät kuitenkaan tätä mainitse erikseen vaan sisällyttävät sen sopimusehtojen hyväksymisvaiheeseen. Neuvottelu voi olla moniosainen prosessi, joka muodostuu tarjousten ja vastatarjousten esittämisestä. Tavoitteena on päästä yhteisymmärrykseen palvelutasotavoitteista esimerkiksi jonkin tietyn ajan puitteissa. Voidaan kuitenkin tulla lopputulokseen, jossa yhteisymmärrystä ei saavuteta. (Rana ym., 2008.) On myös mahdollista, että palvelutasosopimuksen ehdot eivät ole neuvoteltavissa, vaan palveluntarjoaja sanelee ehdot täysin. Tämä on yleistä julkisen pilven mallissa. (Goyal, 2014.) Kun palvelutasosopimus on määritelty, alkaa monitorointivaihe (Rana ym., 2008). Loogisempi järjestys olisi kuitenkin tästä poiketen aloittaa monitorointivaihe sopimusehtojen hyväksymisen jälkeen. Tässä vaiheessa myös luonnollisesti palvelu on otettu käyttöön, jotta sitä voidaan monitoroida. Monitorointivaiheessa tarkastellaan sovittuja palvelutasotavoitteita ja todellista toteutunutta palvelun tasoa (Rana ym., 2008). Mahdollisten rikkomusten lisäksi monitoroinnin avulla voidaan myös allokoida lisää resursseja tarpeen vaatiessa. (Bernsmed ym., 2011). Näin ollen palvelutason monitorointi on tärkeää myös palveluntarjoajalle. Rana ym. (2008) mukaan palvelutasosopimus voidaan irtisanoa, kun määritelty palvelu on valmis ja sopimuksessa määritelty ajanjakso päättyy tai jos palveluntarjoaja ei pysty enää tarjoamaan palvelua, esimerkiksi yrityksen joutuessa selvitystilaan. European Telecommunications Standards Instituten (ETSI) raportissa (2012) palvelun elinkaaren vaiheisiin lueteltiin kuuluvan: löytäminen ja valinta, toimittaminen ja käyttö sekä lopettaminen. Palvelun elinkaaren vaiheiden voidaan huomata olevan joiltain osin samankaltaisia palvelutasosopimuksen elinkaaren vaiheiden kanssa.

3.2 Pilvipalveluiden palvelutasosopimukset

Pilvipalveluiden käyttöönotto on luonut uusia haasteita sekä palveluntarjoajille että asiakkaille, erityisesti palvelun laadun suhteen (Bernsmed ym., 2011). Näin ollen palvelutasosopimuksilla on tärkeä rooli palveluiden käyttöönotossa. Oikeanlaiset palvelutasosopimukset ovat Subramanianin ja Jeyarajin (2018) mu-

kaan edellytys pilvipalveluille ominaisten käyttöpohjaisen hinnoittelun mallien selviytymiselle. Web-palveluiden palvelutasosopimusten kuvailemiseen on kaksi pääasiallista spesifikaatiota. Ensimmäinen on Open Grid Forumin (OGF) kehittämä WS-Agreement. Toinen on IBM:n kehittämä Web Service Level Agreement (WSLA) viitekehys. WSLA koostuu XML-pohjaisesta palvelutasosopimusten määrittelykielestä ja palvelutasosopimusten neuvottelun, monitoroinnin ja sopimusrikkomuksia seuraavien toimenpiteiden hallinnoimisesta. (Bernsmed ym., 2011.) Molemmat näistä ovat koneluettavassa muodossa. Bianco, Lewis ja Merson (2008) mainitsivatkin, että palvelutasosopimusten tulee olla koneluettavassa muodossa, jotta niitä voidaan tulkita ajon aikana. Patelin Ranabahun ja Shethin (2009) mukaan WSLA viitekehys sisältää pääasiassa kolme entiteettiä. Niitä ovat:

- osapuolet. Osapuolia voivat olla palveluntarjoaja, asiakas ja kolmas osapuoli. Näistä kaikista tulee tehdä kuvaus. kolmansien osapuolien tehtäviä voivat olla esimerkiksi palvelun parametrien mittaaminen tai toimenpiteiden tekeminen rikkomusten esiintyessä, mikäli palveluntarjoaja tai asiakas on delegoinut näitä tehtäviä kolmannelle osapuolelle. (Patel ym., 2009).
- palvelutasosopimuksen parametrit. Ne määritellään erilaisten mittareiden avulla. Kaksi merkittävää tyyppiä mittareille ovat resurssimittarit, jotka voidaan johtaa suoraan palveluntarjoajan resursseista ilman prosessoimista, sekä koostetut mittarit, jotka ovat useiden resurssimittareiden yhdistelmiä. Esimerkkinä tällaisesta mittarista voisi olla transaktiot tunnissa. (Patel ym., 2009.)
- palvelutasotavoitteet. Ne ovat joukko formaaleja ilmauksia, joilla on ”josniin”-rakenne. Rakenteen ”jos”-kohtaan sisältyy jokin ehto, ja ”niin”-kohtaan jokin toimenpide, joka tulee suoritetuksi ehdon täyttyessä. (Patel ym., 2009.)

Serrano ym. (2016) mukaan pilvipalveluiden palvelun laadusta puuttuu yhtenäinen perusta. Samankaltaisia huomioita tekivät myös Ghahramani, Zhou ja Hon (2017), joiden mukaan olemassa olevista pilvipalveluiden palvelun laatua koskevista määritelmistä puuttuu helposti ymmärrettävissä oleva taksonomia. Palveluiden laatu ja luotettavuus ovat tärkeitä näkökulmia palvelukeskeisessä arkkitehtuurissa. Palveluita koskevat vaatimukset kuitenkin vaihtelevat asiakkaiden välillä. (Patel ym., 2009.) Palveluiden laadun yhtenäisen perustan luominen voikin tästä syystä olla haastavaa. Lisäksi myös pilvipalveluiden moniulotteisen luonteen voi ajatella aiheuttavan lisää haasteita. Bernsmed ym. (2011) mukaan palvelun laatua tarkastellessa kahteen ominaisuuteen, käyttövarmuuteen ja suorituskykyyn, kiinnitetään eniten huomiota. Käyttövarmuus määritellään yleensä palvelun saatavuuden ja luotettavuuden yhdistelmänä. Luotettavuudella tarkoitetaan kykyä tarjota palvelua ilman katkoja. Suorituskykyä kuvataan esimerkiksi sillä, kuinka monta bittiä välitetään tai prosessoidaan sekunnissa, tai vasteajalla, eli kuinka kauan jonkin tehtävän suorittaminen kestää. (Bernsmed ym., 2011.)

Bianco ym. (2008) jakoivat palvelun laatuun mahdollisesti liittyvät ominaisuudet mitattavissa oleviin ja mittaamattomiin ominaisuuksiin. Mitattavia ominaisuuksia ovat tarkkuus, saatavuus, kapasiteetti, kustannukset, viive, toimittamiseen liittyvä aika, luotettava viestintä ja skaalautuvuus. Tarkkuutta mitattaessa keskitytään palvelussa tapahtuvien virheiden esiintyvyyteen. On esimerkiksi mahdollista esittää virheiden lukumäärän keskiarvo tietyllä aikavälillä. Saatavuudessa keskitytään keskimääräiseen aikaan, joka on kulunut ennen kuin palvelussa ilmenee vika. Sitä mitataan tyypillisesti todennäköisyytenä sille, onko palvelu käytettävissä, kun sitä tarvitsee. Voidaan myös esittää aika, joka kuluu toimintahäiriöiden tunnistamiseen tai vikatilanteesta palautumiseen. Kapasiteetilla tarkoitetaan lukumäärää rinnakkaisista pyynnöistä, jotka palvelu pystyy käsittelemään tietyllä aikavälillä. Kustannukset voidaan määritellä esimerkiksi pyyntökohtaisesti tai tiettyyn datamäärään perustuen. Viivettä voidaan mitata esimerkiksi pyynnön saapumisen ja sen suoritetuksi tulemisen välisellä ajalla. Toimittamiseen liittyvästä ajasta yksi esimerkki on aika, joka kuluu, kun uusi käyttäjä on saatu otettua käyttöön. Luotettavassa viestinnässä keskitytään viestin toimittamisen takaamiseen. On mahdollista määrittää, toimitetaanko viesti esimerkiksi tasan kerran vai enintään kerran, sekä tukeeko palvelu viestien lähettämistä oikeassa järjestyksessä. Skaalautuvuudella tarkoitetaan palvelun kykyä kasvattaa tietyllä aikavälillä onnistuneiden operaatioiden määrää. Tälle voidaan esimerkiksi määrittää jokin maksimiarvo. (Bianco ym., 2008.)

Mittaamattomilla ominaisuuksilla tarkoitetaan sellaisia ominaisuuksia, joita ei pystytä mittaamaan automaattisesti jostain annetusta näkökulmasta (Bianco ym., 2008). Niitä ovat yhteentoimivuus, muunneltavuus ja turvallisuus. Yhteentoimivuudessa keskitytään kommunikoivien entiteettien joukon kykyyn jakaa informaatiota keskenään. Tätä varten voidaan määrittää palvelun tukemia standardeja. Muunneltavuudella tarkoitetaan todennäköisyyttä sille, kuinka usein palvelu tai sen osa tulee muuttumaan. Turvallisuuden osalta keskitytään järjestelmän kykyyn vastustaa luvatonta käyttöä antaen samalla oikeutetuille käyttäjille pääsyn palveluun. Turvallisuutta voidaan kuvata myös järjestelmän kykynä tarjota kiistämättömyyttä, luottamuksellisuutta, eheyttä, varmuutta sekä auditointia. On mahdollista määrittää metodeja datan salaukseen sekä palveluiden ja käyttäjien todentamiseen ja valtuuttamiseen. (Bianco ym., 2008.)

Organisaatioiden on myös mahdollista hyödyntää toiminnassaan useamman kuin yhden palveluntarjoajan pilvipalveluita. Tällaista strategiaa kutsutaan monipilvistrategiaksi. Sen ideana on asiakkaan pääsy resursseihin useilta eri palveluntarjoajilta, jotka eivät ole sopineet keskenään resurssiensa liittämisestä tai toimintansa yhdistämisestä. Usean infrastruktuurin käyttö voi auttaa asiakkaita heidän mahdollisesti monimutkaisiin tarpeisiinsa vastaamisessa. (Casola, De Benedictis, Rak & Villano, 2018.) Mikäli yksittäinen palveluntarjoaja ei pysty tarjoamaan vaatimuksia täyttäviä palveluita, on järkevää harkita monipilvistrategiaa. Rampérez, Soriano, Lizcano, Aljawarneh ja Lara (2021) perustelivat monipilvistrategian käyttöönottoa resurssien käytön huippujen käsittelemisellä, kustannusten optimoimisella, ehtojen, kuten sijaintiin liittyvien lakien noudattamisella sekä korkealla saatavuudella, joka voidaan saavuttaa repli-

koinneilla tai varmuuskopioinneilla, mikäli esimerkiksi yhdessä palvelussa esiintyy käyttökatko. Casola ym. (2018) luettelivat monipilvistrategian hyödyiksi yrityksen suorituskyvyn parantamisen, kustannusten pienentämisen ja turvallisuuden parantamisen.

Hyötyjen lisäksi strategiaan liittyy myös haittoja ja haasteita. Kuten tässä sekä edellisessä luvussa käsiteltiin, pilvipalveluiden käyttöönottoon ja niihin liittyvien palvelutasosopimusten solmimiseen liittyy pilvipalveluiden monimutkaisen luonteen vuoksi monia erilaisia haasteita ja näkökulmia jo yhtä palvelua koskien. Jos esimerkiksi palvelun tasossa on puutteita IaaS-kerroksella, aiheutuu haittaa ja mahdollisia sopimusrikkomuksia myös SaaS-kerroksella (Serrano ym., 2016). Jos organisaatio päättää käyttää monipilvistrategiaa, moninkertaistuu samalla myös haasteiden ja mahdollisten ongelmien määrä. Tällöin asiakkaiden tulee esimerkiksi solmia palvelutasosopimuksia useamman palveluntarjoajan kanssa. Mahdollisten palveluntarjoajien lukumäärä ja niiden eroavaisuudet johtavat useisiin teknologisiin ja hallinnollisiin esteisiin, joiden taustalla on syy puuttuvista, yleisesti käytettävistä standardeista ja suurten palveluntarjoajien haluttomuudesta sellaisia kohtaan (Rampérez ym., 2021). Myös usean palvelutasosopimuksen monitorointi voi olla haastavaa. Palveluntarjoajien käytössä ei ole yhtenäisiä mittareiden joukkoja, joiden avulla palvelun tasoa voitaisiin monitoroida (Rampérez ym., 2021). Pilvipalveluiden dynaamisen luonteen vuoksi palvelun laadun monitoroinnin tulee olla jatkuvaa (Ghahramani ym., 2017).

4 TIETOTURVAN ESITTÄMINEN PILVIPALVELUIDEN PALVELUTASOSOPIMUKSISSA

Kuten tutkielmassa aiemmin käsiteltiin, tietoturva on suurin huolenaihe organisaatioille niiden pohtiessa pilvipalveluiden käyttöönottoa. Olennainen osa käyttöönottoa on asiakkaan ja palveluntarjoajan välinen palvelutasosopimus, jossa on keskeistä palvelun tason määrittäminen. Niin kuin todettiin, palvelun tason määrittelemisessä keskitytään eniten ominaisuuksiin, kuten suorituskykyyn ja käyttövarmuuteen. Nugrahan ja Martinin (2022) mukaan olemassa olevat palvelutasosopimukset jättävät tietoturvavaatimukset vähäiselle huomiolle. Näin ei kuitenkaan tulisi olla, vaan tietoturvanäkökulma tulisi huomioida paremmin sen tärkeyden vuoksi. Seuraavissa alaluvuissa käsitellään pilvipalveluiden palvelutasosopimuksissa ilmeneviä haasteita tietoturvanäkökulman suhteen, esitettyjä keinoja haasteiden ratkaisemiseksi sekä nykyisiä käytänteitä aiheeseen liittyen.

4.1 Tietoturvan haasteet

Tietoturvan hallinnointi pilviympäristöissä on vähemmän kehittynyttä verrattuna operaationaaliseen suorituskyvyn hallinointiin (Kaaniche, Mohamed, Laurent & Ludwig, 2017). Luna ym. (2017) toivat saman ongelman esiin. Heidän mukaansa pilvipalveluiden palvelutasosopimusten tietoturvan hallinnoinnin tekniikoissa on huomattavia aukkoja. Niin kuin edellisessä luvussa todettiin, palvelun tason hallinta edellyttää mitattavissa olevien parametrien määrittämistä. Turvallisuuden osalta sen tasoa kuvaavia mittareita on vaikea löytää, sillä pilvipalveluiden turvallisuuden määrällistäminen on haastavaa (Halabi & Bellaiche, 2018). Tämän voidaan päätellä johtuvan pilvipalveluiden monimutkaisuudesta. Lisäksi tietoturvan hallinnan kehittymättömyys muihin osa-alueisiin verrattuna voi mahdollisesti johtua juuri pilvipalveluiden turvallisuuden määrällistämisen haasteellisuudesta. Myös Bernsmed ym. (2011) mainitsi-

vat turvallisuuden mittaamisen olevan haasteellista. Heidän mukaansa jopa pidempään toiminnassa olleen pilvipalvelun turvallisuuden tasoa voi olla vaikeaa varmistaa. European Telecommunications Standards Instituten raportissa (2012) huomautettiin, että turvallisuus ei yleisesti ole arvioitavissa palvelun laadun parametrien monitoroinnilla, vaan laatu varmistetaan hyväksymällä palveluntarjoajan käyttämät järjestelmät, prosessit ja käytänteet siihen liittyen. Myös Lee, Kavi, Paul ja Gomathisankaran (2015) toivat tämänkaltaisia huomioita esille. Heidän mukaansa palveluntarjoajat eivät ota palvelutasosopimusten tietoturvanäkökulmaa riittävän vakavasti, ja että niissä mainitaan vain, mitä turvallisuuteen liittyviä palveluita tarjotaan. Lisäksi he mainitsivat, että erillisissä dokumenteissa voi olla kuvailtuna suositeltuja tietoturvan ylläpitoon liittyviä toimia, mutta nämä dokumentit eivät ole kuitenkaan lainvoimaisia sopimuksia, kuten palvelutasosopimukset.

Aiemmin mainittu turvallisuuden hallinnoinnin puutteellisuus sekä palveluntarjoajien väliseen objektiiviseen vertailuun käytettävien metodien puutteellisuus tekevät Kaaniche ym. (2017) mukaan luotettavien palveluiden tarjoamisen mahdottomaksi palveluntarjoajille. Palveluntarjoajat voivat vain olettaa minkä tyyppistä dataa asiakkaat generoivat ja käsittelevät. Näin ollen ne eivät ole tietoisia asiakkaidensa mahdollisista räätälöidyistä turvallisuusvaatimuksista. (Luna ym., 2017.) Halabi ja Bellaiche (2018) antoivat esimerkin tapauksesta, jossa asiakkaan käsittelemä data on äärimmäisen arkaluontoista. Tässä tilanteessa asiakas heidän mukaansa etsii palveluntarjoajan, joka tarjoaa parhaan tietoturvan tason tiedon varastointiin. He kertovat näin ollen asiakkaan joutuvan tekemään palveluntarjoajan valinnassa kompromisseja muiden ei niin tärkeiden palvelun laadun osa-alueiden suhteen. Myös Al Morsy ym. (2010) mainitsivat asiakkaiden joutuvan mahdollisesti tekemään kompromisseja turvallisuuden ja suorituskyvyn välillä. He korostivat, että mitä korkeampi turvallisuuden taso on, sitä enemmän tietoturvan työkaluja ja mekanismeja on käytössä, joka puolestaan vaikuttaa enemmän palvelun suorituskykyyn.

Tietoturva ja pilvipalvelut voivat olla teknisesti haastavia aiheita. Olisi hyödyllistä, jos asiakasorganisaatiosta löytyisi asiantuntevia henkilöitä, jotta turvallisuuden taso voitaisiin taata. Luna ym. (2017) toivatkin esille haasteen siitä, kuinka muut kuin asiantuntijat etenkin pienissä ja keskisuurissa yrityksissä voivat arvioida täyttyykö palvelulta vaadittu turvallisuuden taso. Tämä on tärkeää, sillä Kaaniche ym. (2017) mukaan tietoturvan vaatimusten määrittelemisessä tarvitaan tarkkaa harkintaa. Turvallisuusvaatimusten määrittelemisessä keskitytään usein tapahtumiin, joiden ei tule toteutua. Sen vuoksi niitä on vaikeaa käyttää syötteenä palvelutasosopimusten mallissa. (Bernsmed ym., 2011.) Palvelutasosopimusten tietoturvan monitorointi voi monimutkaistua helposti, sillä asiakkaan ja palveluntarjoajan välille voi muodostua aukko semanttisuuden suhteen. Näin voi käydä, jos asiakkaalla on yksityiskohtaiset vaatimukset mutta ei asiantuntijuutta tietoturvan taksonomiaan, ja jos palveluntarjoaja haluaa ilmaista turvallisuuden tason yksityiskohtaisten mittareiden mukaan. (Kaaniche ym., 2017.)

Pilvipalveluiden dynaamisen luonteen sekä heterogeenisten rajapintojen ja työkalujen vuoksi palvelutasosopimusten monitorointi on hankalaa. Palvelutasosopimusten tietoturvan monitorointi on vielä haastavampaa, johtuen useista syistä. Usein tehtävät uudelleenkonfiguroinnit vaativat turvallisuuden monitorointijärjestelmältä tietoturvan muutosten automaattista mukautumista. Monitoroinnin toimintatapoja ei välttämättä ole määritelty riittävän kattavasti tukemaan sopimusrikkomusten havaitsemista. Useisiin monitoroinnin toimintoihin liittyy lokien analysointi. Tähän liittyen ilmenee ongelmia lokien säilyttämisen toimintatapojen sekä lokien pääsynhallinnan määrittelemisessä. (Kaaniche ym., 2017.) Lokitiedostot sisältävät usein arkaluontoista tietoa, joten tämä on tärkeää huomioida. Näiden lisäksi Kaaniche ym. (2017) luettelivat lisää haasteita turvallisuuden monitoroinnissa. Ulkoistetut palvelut koostuvat joukosta alajärjestelmiä, jotka ovat osana lukuisissa interaktioissa, jolloin heidän mukaansa monitoroitavan palvelun taso riippuu siihen kuuluvien alajärjestelmien turvallisuuden tasosta. He huomauttivat, että myös jokaisen alajärjestelmän turvallisuuden taso on riippuvainen muiden siihen yhteydessä olevien alajärjestelmien turvallisuuden tasosta. Viimeiseksi he mainitsivat tietoturvan tason kokonaisuuden olevan koottu arvio lomitettujen tietoturvan ja yksityisyyden ominaisuuksien joukosta.

Kuten jo tiedämme, pilvipalveluille on ominaista palvelumallien käyttöpohjainen hinnoittelu. Hinta määräytyy palvelutasosopimuksissa määriteltävien resurssien käytön ja vaaditun palvelun tason kautta. Tämän voidaan päätellä aiheuttavan uudenlaisen haasteen sen suhteen, kuinka hinnoitella turvallisuus ja sen taso. Löytämässäni kirjallisuudessa tai käyttämässäni lähdekirjallisuudessa ei tätä haastetta kuitenkaan käsitelty.

4.2 Nykyiset käytänteet ja ratkaisut haasteisiin

Nykyään pilvipalveluntarjoajat ovat alkaneet uudistamaan palvelutasosopimustensa ehtoja niin, että ne sisältävät myös tietoturvaan liittyviä ehtoja. Näin on tehty sen vuoksi, että asiakkaat pitävät tietoturvaa kriittisenä asiana. (Kaaniche ym., 2017.)

Halabin ja Bellaichen (2018) mukaan ei ole pilvipalvelua, joka voi taata asiakkaalle täyden tyytyväisyyden kaikkien tietoturvavaatimusten osalta ilman, että joitain tarpeita tulisi laittaa etusijalle toisiin nähden. Yksi aiemmin käsitellyistä haasteista oli tietoturvan vaatimusten määrittely. Niiden tunnistaminen voidaan suorittaa riskianalyysin avulla, jossa tunnistetaan jokaista komponenttia koskevat uhat ottamalla huomioon sen luonne sekä vuorovaikutus muiden komponenttien kanssa. Näin voidaan määrittää tarvittavat toimenpiteet uhkien toteutumisen pienentämiseksi. (Casola ym., 2018.) Tulee kuitenkin huomioida, että adekvaatin riskianalyysin toteuttaminen vaatii ammattitaitoa ja asiantuntijuutta aihepiiristä.

Tarjotakseen asiakkailleen läpinäkyvyyttä ja varmuutta tietoturvan tasosta, monet pilvipalveluntarjoajat ovat hankkineet standardisoituihin viitekehyksiin, kuten International Organization for Standardizationin (ISO) 27002 -standardiin, pohjautuvia tietoturvan sertifikaatteja (Luna, Suri, Iorga & Karmel, 2015). ISO 27002 -standardin tarkoitus on osoittaa sopivia tietoturvan toimenpiteitä. Carvalho ym. (2017) mukaan palveluntarjoajien käyttämiä tietoturvan standardeja ja viitekehyksiä ovat ISO 27017 -standardi, Cloud Security Alliancen (CSA) Cloud Control Matrix sekä jo aiemmin mainitun NIST:n julkaisu 800-53. Näitä käyttämällä palveluntarjoajat voivat heidän mukaansa lisätä palveluidensa luotettavuutta. Luna ym. (2015) toivat myös esille ISO 27002 -standardin ja vielä silloin tekeillä olleen 27017 -standardin, CSA:n Cloud Control Matrixin sekä NIST:n saman julkaisun. Cloud Control Matrixiin kuuluu ”Consensus Assessments Initiative Questionnaire”(CAIQ), joka voisi vapaasti suomennettuna tarkoittaa yksimielisyyden arviointien alustavaa kyselylomaketta. Se tarjoaa alalla hyväksyttyjä tapoja dokumentoida pilvipalveluiden tietoturvatoimenpiteitä. Siihen sisältyy yli 160 kysymystä, joihin asiakkaat mahdollisesti haluavat tietää vastauksia. (Luna, Ghani, Vateva & Suri, 2012.)

Amazon Web Services on Amazonin perustama pilvipalvelu. Sen verkkosivuilla (Amazon, ei pvm.) on käsitelty tietoturvastandardien ja -sertifikaattien noudattamista heidän tarjoamissa palveluissaan. Sivulla on kattava luettelo erilaisista standardeista, sertifikaateista sekä viitekehyksistä. Olennaisimpia näistä ovat edellä mainitut CSA:n ja NIST:n viitekehykset sekä ISO:n standardit. Sivulla mainittuja ISO-standardeja ovat 9001, 22301, 27001, 27017, 27701 sekä 27018. Myös Microsoftin tarjoaman pilvipalvelu Azuren verkkosivuilta (Microsoft, ei pvm.) löytyy samankaltainen luettelo tietoturvastandardien, sertifikaattien ja viitekehysten noudattamisesta. Siinä on mainittuna CSA:n viitekehyksiä, ISO:n standardit 20000–1, 22301, 27001, 27017, 27018, 27701 sekä 9001 ja NIST:n julkaisut 800–161, 800–171, 800–53, Cybersecurity Framework (CSF) ja 800–63.

Aiemmin käsiteltyjen haasteiden ratkaisemiseksi aiheeseen liittyvässä kirjallisuudessa on esitetty monia erilaisia viitekehyksiä ja malleja. Monet niistä pohjautuvat Secure Provisioning of Cloud Services (SPECS) viitekehykseen. Se on Euroopan komission projekti, joka esittää tietoturvan palvelutasosopimuksiin perustuvan pilven turvallisuuden hallinnoinnin viitekehyksen (Luna ym., 2015). SPECS tarjoaa tekniikoita ja työkaluja tietoturvan parametrien neuvottelemiseen, vaatimusten mukaisten tietoturvaominaisuuksien automaattiseen käyttöönottoon, reaaliaikaiseen monitorointiin sekä turvallisuuden tason vaihteluun reagoimiseen ja mukautumiseen (Casola, De Benedictis, Rak & Villano, 2015).

Casola ym. (2015) ovat osallisena SPECS -projektissa, ja he esittivät artikkelissaan ratkaisun turvallisuuden monitoroinnin haasteeseen. Heidän ratkaisunsa perustui olemassa oleviin turvallisuuden monitoroinnin työkaluihin ja se voidaan integroida SPECS -viitekehykseen. Ratkaisussa he tunnistivat SPECS:n monitorointiin liittyvät komponentit, palvelutasosopimusten hallinnoinnin alustan, monitoroitavan kohteen sekä näiden kaikkien väliset suhteet ja esittivät ratkaisunsa arkkitehtuurin. He huomauttavat, että heidän ratkaisunsa on konfi-

guroitavassa useilla eri tavoilla esitetyn konfiguraation lisäksi. Tukeakseen ratkaisunsa toimivuutta, Casola ym. (2015) toteuttivat tapaustutkimuksen, jossa esitettyä arkkitehtuuria hyödynnetään haavoittuvuuksien monitoroinnissa.

Myös Halabi ja Bellaiche (2018) esittivät ratkaisun, joka voidaan sisällyttää SPECS -viitekehykseen. Heidän ratkaisunsa keskittyi useampaan haasteeseen. Ratkaisussa esitettiin standardoitu, määrällisessä ja mitattavassa muodossa oleva tapa esittää tietoturvan palvelutasosopimus, laskentamalli turvallisuuden ominaisuuksien tason arviointiin, metodi palveluntarjoajien valintaan ja vertailuun tietoturvan näkökulmasta sekä malli monitorointiin ja sopimusrikkomusten ennustamiseen.

Casola, De Benedictis, Eraşcu, Modic ja Rak (2017) esittivät artikkelissaan tietoturvan palvelutasosopimuksen mallin, joka pohjautuu tutkielmassa aiemmin mainittuun WS-agreementiin sekä NIST:n ja ISO:n tietoturvan standardisointiin. Ratkaisu on osa SPECS -projektia. Heidän mallinsa mahdollistaa tietoturvan menetelmien automaattisen toimeenpanon kartoittamalla asiakkaan tietoturvan vaatimukset palvelutasosopimuksesta. Auttaakseen asiakkaita vaatimusten määrittelyssä, heidän ratkaisunsa tarjoaa palvelutasosopimuksen tietoturvaa koskevan mallipohjan. Casola ym. (2017) esittämä ratkaisu ottaa huomioon oikeanlaiset tietoturvakyvykkyydet sekä mitattavien palvelutasotavoitteiden mittarit. Mallissa käyttöönottoon kuuluva komponentti mahdollistaa monitorointiin liittyvien mekanismien konfiguroinnin. Heidän esittämään malliin kuuluvan, Ratkaisijaksi nimetyn komponentin avulla muodostuu vaatimukset täyttävien palveluiden palvelutasosopimuksien tarjouksia, joita asiakas voi hyödyntää palveluntarjoajien vertailuun.

Kaaniche ym. (2017) esittivät artikkelissaan palvelutasosopimuksia kuvaamaan käytettävän rSLA-kielen laajentamista, joka on Ruby-ohjelmointikieleen perustuva täsmäkieli (domain-specific language). Heidän ratkaisussaan rSLA-kieltä laajennettiin kuvaamaan tietoturvan vaatimuksia sekä tarjoamaan tarvittavat mekanismit, joiden avulla voidaan automaattisesti asentaa tietoturvan palvelutason hallinnointia koskevat resurssit.

Luna ym. (2017) keskittyivät artikkelissaan palvelutarjoajien turvallisuuden tason vertailun haasteisiin ja pilven turvallisuuden määrällistämiseen. He hyödynsivät kvantitatiivista menettelytapojen puumallia sekä kvantitatiivista hierarkiaprosessia tietoturvan palvelutason arviointiin. He esittivät kaksi käyttötapausta demonstroidakseen tekniikoiden hyödyllisyyttä. Muista poiketen he myös käsittelivät asiaa palveluntarjoajan näkökulmasta toteuttamalla herkkyysanalyysin turvallisuuden palvelutasosta. Sen avulla heidän mukaansa palveluntarjoajat voivat ottaa selvää parametreista, jotka asiakkaiden vaatimusten mukaan vaikuttavat eniten turvallisuuden kokonaistasoon. Lisäksi analyysi kertoo heidän mukaansa palveluntarjoajille, mitä turvallisuuden tasossa tulee parantaa, jotta vaadittu taso voidaan saavuttaa.

Taulukossa 1 on havainnollistettu edellä käsiteltyjen ratkaisujen kattavuutta suhteessa tämän luvun ensimmäisessä alaluvussa esille nousseisiin tietoturvan haasteisiin. Taulukkoon on merkitty, mihin yksittäisiin haasteisiin esitetyt ratkaisut vastasivat.

TAULUKKO 1 Esitettyjen ratkaisuiden laajuus osa-alueittain

	Lähde					
Tietoturvan haasteet		Casola ym. (2015)	Casola ym. (2017)	Halabi ja Bellaiche (2018)	Kaaniche ym. (2017)	Luna ym. (2017)
	Määrällistäminen ja mittaaminen	✓	✓	✓		✓
	Vaatimusten määrittely		✓		✓	
	Palveluntarjoajien vertailu		✓	✓		✓
	Reaaliaikainen monitorointi	✓	✓	✓		
	Hinnoittelu					
	Työkalujen automaattinen toimeenpano	✓	✓	✓	✓	

5 YHTEENVETO

Tämän kandidaatintutkielman tarkoituksena oli perehtyä pilvipalveluiden palvelutasosopimusten tietoturvaan sekä sen esittämisessä ilmeneviin haasteisiin ja kirjallisuudessa esitettyihin keinoihin näiden haasteiden ratkaisemiseksi. Tutkielma toteutettiin kirjallisuuskatsauksena. Tutkielman ensimmäisessä sisältöluvussa käsiteltiin pilvipalveluita yleisesti sekä palvelu- ja käyttöönottomalleittain. Lisäksi luvussa perehdyttiin pilvipalveluiden tietoturvauhkiin ja niihin liittyviin ratkaisuihin eri palvelu- ja käyttöönottomalleissa. Seuraavassa sisältöluvussa keskityttiin palvelutasosopimuksiin. Luvussa käsiteltiin aluksi palvelutasosopimusten tarkoitusta ja sisältöä yleisesti, jonka jälkeen perehdyttiin pilvipalveluita koskeviin palvelutasosopimuksiin. Viimeisessä sisältöluvussa vastattiin molempiin tutkimuskysymyksiin sekä käsiteltiin nykyisiä käytänteitä tietoturvan esittämiseen pilvipalveluissa ja niiden palvelutasosopimuksissa.

Ensimmäisen tutkimuskysymyksen tarkoituksena oli selvittää, minkälaisia haasteita ilmenee tietoturvan esittämisessä pilvipalveluiden palvelutasosopimuksissa. Toinen tutkimuskysymys koski erilaisten esitettyjen ratkaisujen löytämistä näihin haasteisiin.

Pilvilaskenta ja pilvipalvelut eivät ole teknologiana tai aiheena uusia. Tämän vuoksi suuri osa lähdekirjallisuudesta sijoittuu 2010-luvulle, jolloin niidensuosio alkoi kasvaa. Palveluntarjoajien määrä on kasvanut ja pilvipalveluiden käyttö on yleistynyt entisestään. Tämän voidaan sanoa johtuvan niiden ominaisuuksien tuomista eduista. Käyttäjät pääsevät käyttämään palveluita internetin välityksellä sijainnista riippumatta. Lisäksi asiakkaat voivat skaalata käyttämiään resursseja tarpeidensa mukaan. Keskeisin etu on kustannustehokkuus, kun asiakkaiden ei tarvitse ostaa tai ylläpitää omaa laitteistoa, vaan he maksavat resursseista niiden käytön mukaan.

Monista eduista huolimatta organisaatiot saattavat epäröidä pilvipalveluiden käyttöönottoa. Suurimpana syynä tälle huomattiin olevan tietoturvaan ja yksityisyyteen liittyvät uhat. Pilvipalveluiden eri palvelu- ja käyttöönottomallit tekevät tietoturvatoimenpiteistä ja niiden huomioimisesta monimutkaisempaa. Huolenaiheita yksityisyydestä ja tietoturvasta aiheuttivat esimerkiksi moniasiakaskäytön sekä resurssien jakamisen ja ulkoistamisen mukanaan tuomat

tietoturvauhkat. Palveluntarjoajien tulee siis huolehtia palveluidensa riittävästä turvallisuuden tasosta.

Palveluntarjoajat ja asiakkaat solmivat palvelutasosopimuksia, joissa sovitaan palvelun tasosta. Kirjallisuuskatsauksesta kävi kuitenkin ilmi, että nykyhetkellä käytettävät palvelutasosopimukset keskittyvät eniten suorituskykyyn sekä saatavuuteen, ja tietoturva on jäänyt sen tärkeydestä huolimatta vähäiselle huomiolle. Kirjallisuudessa esitettiin monia tietoturvanäkökulman haasteita, jotka voivat olla syynä tälle. Yhtenä havaintona esiin nousi tietoturvan määrällistämisen ja mittaamisen haasteellisuus. On kuitenkin huomionarvoista, ettei tämä haaste koske yksinomaan pilvipalveluita, vaan liittyy tietoturvaan yleisesti. Oikeanlaisten tietoturvavaatimusten määrittely on tärkeää, ja se voi olla haastavaa ilman oikeellista semantiikka tai riittävää asiantuntemusta. Palveluiden tason reaaliaikainen monitorointi on oleellinen osa palvelutasosopimuksia. Näin voidaan esimerkiksi havaita mahdollisia sopimusrikkomuksia. Havaittiin, että pilvipalveluiden monitorointi on niiden dynaamisuuden ja heterogeenisuuden vuoksi haasteellista. Lisäksi tietoturvan monitoroinnin havaittiin olevan vielä haastavampaa. Tähän esitettyjä syitä olivat usein tapahtuvat uudelleenkonfiguroinnit, jotka vaativat myös tietoturvaominaisuuksien automaattista mukauttamista, puutteelliset toimintatavat sopimusrikkomusten havaitsemiseen sekä palveluiden koostuminen useista keskenään vuorovaikutuksessa olevista alajärjestelmistä. Pilvipalveluiden tietoturvan havaittiin olevan monimutkainen kokonaisuus, jonka vuoksi sen esittäminen palvelutasosopimuksissa on osoittautunut haasteelliseksi.

Kirjallisuuskatsauksessa nousi esille erilaisia projekteja ja viitekehyksiä, joiden tavoitteena on helpottaa tietoturvan tason esittämistä. Havaittiin myös, ettei olemassa olevat keinot ole riittäviä, ja monet kirjoittajat esittivät omia ehdotuksiaan ongelmien ratkaisemiseksi. Monet näistä ratkaisuista pohjautuivat olemassa oleviin viitekehyksiin sekä laajensivat niitä. Ratkaisujen keskiössä olikin nykyisten käytäntöjen riittämättömyys ja niiden parantaminen. Ne keskittyivät reaaliaikaiseen monitorointiin, palveluntarjoajien tietoturvan tason vertailuun, tietoturvan määrällistämiseen ja mittaamiseen sekä tietoturvaominaisuuksien automaattiseen toimeenpanoon.

Nykyisten käytänteiden selvittämisessä otettiin esimerkiksi kaksi suosittua pilvipalvelua, Amazon Web Services ja Microsoft Azure. Tehtiin havainto, ettei kumpikaan ole omaksunut esitettyjä tai muita samankaltaisia ratkaisuja. Sen sijaan molemmat ovat listanneet verkkosivuilleen erilaisia tietoturvan standardeja ja viitekehyksiä, joita he lupaavat noudattaa. Jotta pilvipalveluiden tietoturvaa käsiteltäisiin niiden palvelutasosopimuksissa nykyistä paremmin, tulisi palveluntarjoajien ottaa käyttöön jokin esitettyjen ratkaisujen mukainen tapa. Jotta ratkaisusta olisi asiakkaille hyötyä, tulisi linjan olla yhtenäinen palveluntarjoajien välillä, joka taas vaatisi ratkaisuna toimivan viitekehyksen standardisointia. Aihetta voisi myös tarkastella toisesta näkökulmasta. Voitaisiin ajatella, onko tietoturvan nykyistä parempi määrällistäminen ja mittaaminen välttämätöntä, vai olisiko riittävää jatkaa nykyisten käytänteiden mukaan ilmoittamalla standardit ja viitekehykset, joita palveluntarjoajat noudattavat.

Pilvilaskenta ja -palvelut ovat aiheena hyvin laajoja, johtuen esimerkiksi niihin kuuluvista useista palvelu- ja käyttöönottomalleista. Näin ollen tutkielman pituuden rajoittamiseksi tiettyjä asioita, kuten palvelu- ja käyttöönottomallien tietoturvaa käsiteltiin hieman pintapuolisesti. Lisäksi ISO-standardien käsittely jäi myös pintapuoliseksi, sillä ne ovat maksullisia, jonka vuoksi niiden sisältöä ei voitu tarkastella syvemmin.

Nykyisessä muodossa olevat tietoturvan palvelutasosopimukset eivät ole täysin mitattavassa ja monitoroitavassa muodossa. Näihin liittyvien parametrien määrittelyyn liittyvä tutkimus on kuitenkin aktiivista. (Halabi & Bellaiche, 2018.) Näin ollen aihe vaatii jatkotutkimusta ja suunta siihen on jo olemassa. Tietoturvan tason mittaamiseen liittyvät ongelmat eivät koske yksinomaan pilvipalveluita, vaan tietoturvaa yleisesti. Tähän liittyvät mahdollisesti löydettävät ratkaisut auttaisivat kuitenkin myös parantamaan tietoturvan esittämistä pilvipalveluiden palvelutasosopimuksissa.

LÄHTEET

Al Morsy, M., Grundy, J., & Ibrahim, A. S. (2011). *Collaboration-Based Cloud Computing Security Management Framework*. 364–371.

Al Morsy, M., Grundy, J., & Müller, I. (2010, tammikuuta). *An Analysis of the Cloud Computing Security Problem*. Proceedings of the APSEC 2010 Cloud Workshop.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58.

Azure compliance documentation. (ei pvm.). Microsoft Corporation. Noudettu 10. huhtikuuta 2023, osoitteesta https://learn.microsoft.com/en-us/azure/compliance/

Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., & Sarkar, P. (2018). *Cloud computing security challenges & solutions-A survey*. 347–356.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246.

Bernsmed, K., Jaatun, M. G., Meland, P. H., & Undheim, A. (2011). *Security SLAs for Federated Cloud Services*. 202–209.

Bhadauria, R., & Sanyal, S. (2012). Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. *International Journal of Computer Applications*, *47*(18), 47–66.

Bianco, P., Lewis, G. A., & Merson, P. (2008). *Service Level Agreements in Service-Oriented Architecture Environments*. Carnegie Mellon University Software Engineering Institute.

Carvalho, C., Andrade, R. M. de C., Castro, M. F. de, Coutinho, E. F., & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. *Computers and Electrical Engineering*, *59*, 141–152.

Casola, V., De Benedictis, A., Eraşcu, M., Modic, J., & Rak, M. (2017). Automatically Enforcing Security SLAs in the Cloud. *IEEE Transactions on Services Computing*, *10*(5), 741–755. https://doi.org/10.1109/TSC.2016.2540630

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2015, syyskuuta). *SLA-Based Secure Cloud Application Development: The SPECS Framework*. 2015 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC).

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2018). Security-by-design in multi-cloud applications: An optimization approach. *Information Sciences*, *454*, 344–362.

CLOUD - SLAs for Cloud services (TR 103 125 V1.1.1). (2012). ETSI.

Compliance Programs—Amazon Web Services (AWS). (ei pvm.). Amazon Web Services, Inc. Noudettu 10. huhtikuuta 2023, osoitteesta https://aws.amazon.com/compliance/programs/

de Chaves, S. A., Westphall, C. B., & Lamin, F. R. (2010, maaliskuuta). *SLA Perspective in Security Management for Cloud Computing*. Sixth International Conference on Networking and Services.

Dillon, T., Wu, C., & Chang, E. (2010). *Cloud Computing: Issues and Challenges*. 27–33.

El Balmany, C., Asimi, A., & Tbatou, Z. (2018). IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors. *Procedia Computer Science*, *134*, 328–333.

Ghahramani, M. H., Zhou, M. C., & Hon, C. T. (2017). Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services. *IEEE/CAA Journal of Automatica Sinica*, *4*(1), 6–18.

Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2009). The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study. *MIS Quarterly*, *33*(1), 119–145.

Goyal, S. (2014). Public vs Private vs Hybrid vs Community—Cloud Computing: A Critical Review. *International Journal of Computer Network and Information Security*, *6*(3), 20–29.

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications*, *33*, 55–65.

Halabi, T., & Bellaiche, M. (2018). A broker-based framework for standardization and management of Cloud Security-SLAs. *Computers & security*, *Vol.75*, 59–71.

Hay, B., Nance, K., & Bishop, M. (2011). *Storm clouds rising: Security challenges for IaaS cloud computing*. 1–7.

Heiser, J., & Nicolett, M. (2008). *Assessing the Security Risks of Cloud Computing*. Gartner.

Iqbal, S., Kiah, L. M., Anuar, N. B., Daghighi, B., Wahab, A. W. A., & Khan, S. (2016). Service delivery models of cloud computing: Security issues and open challenges. *Security and Communication Networks*, *9*(17), 4726–4750.

Kaaniche, N., Mohamed, M., Laurent, M., & Ludwig, H. (2017). *Security SLA based monitoring in clouds*. 90–97.

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers & security*, *3*(1), 1–35.

Lee, C.-Y., Kavi, K. M., Paul, R. A., & Gomathisankaran, M. (2015). *Ontology of Secure Service Level Agreement*. 166–172.

Lin, A., & Chen, N.-C. (2012). Cloud computing as an innovation: Percepetion, attitude, and adoption. *International Journal of Information Management*, *32*(6), 533–540.

Luna, J., Ghani, H., Vateva, T., & Suri, N. (2012, tammikuuta). *Quantitative Assessment of Cloud Security Levels: A Case Study*. International Conference on Security and Cryptography (SECRYPT).

Luna, J., Suri, N., Iorga, M., & Karmel, A. (2015). Leveraging the Potential of Cloud Security Service-Level Agreements through Standards. *IEEE Cloud Computing*, *vol. 2*, *3*, 32–40.

Luna, J., Taha, A., Trapero, R., & Suri, N. (2017). Quantitative Reasoning about Cloud Security Using Service Level Agreements. *IEEE Transactions on Cloud Computing*, 457–471.

Mathisen, E. (2011). *Security challenges and solutions in cloud computing*. 208–212.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards & Technology.

Nugraha, Y., & Martin, A. (2022). Cybersecurity service level agreements: Understanding government data confidentiality requirements. *Journal of Cybersecurity*, *2022*(Volume 8).

OWASP Top Ten. (ei pvm.). Noudettu 3. maaliskuuta 2023, osoitteesta https://owasp.org/www-project-top-ten/

Patel, P., Ranabahu, A., & Sheth, A. (2009). Service Level Agreement in Cloud Computing. *Cloud Workshops at OOPSLA09*.

Rachana, C. R., Banu, R., Ahammed, G. F. A., & Parameshachari, B. D. (2017). *Cloud Computing – A Unified Approach for Surveillance Issues*. *225*.

Rak, M., Suri, N., Luna, J., Petcu, D., Casola, V., & Umberto, V. (2013, joulukuuta). *Security as a service using an SLA-based approach via SPECS*. Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science - Volume 02.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010). *The management of security in Cloud computing*. 1–7.

Rampérez, V., Soriano, J., Lizcano, D., Aljawarneh, S., & Lara, J. A. (2021). From SLA to vendor-neutral metrics: An intelligent knowledge-based approach for multi-cloud SLA-based broker. *International Journal of Intelligent Systems*, *37*(12), 10533–10575.

Rana, O., Warnier, M., Quillinan, T. B., Cojocarasu, D., & Brazier, F. (2008). Managing Violations in Service Level Agreements. *Grid Middleware and Services*, 349–358.

Rodero-Merino, L., Vaquero, L. M., Caron, E., Muresan, A., & Desprez, F. (2012). Building safe PaaS clouds: A survey on security in multitenant software platforms. *Computers & Security*, *31*(1), 96–108.

Serrano, D., Bouchenak, S., Kouki, Y., de Oliveira Jr., F. A., Ledoux, T., Lejeune, J., Sopena, J., Arantes, L., & Sens, P. (2016). SLA guarantees for cloud services. *Future Generation Computer Systems*, *54*, 233–246.

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.

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28–42.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532.

Takabi, H., Joshi, J. B., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy*, *8*(6), 24–31.

Velte, A., Velte, T., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach*.

Verma, A., & Kaushal, S. (2011). *Cloud computing security issues and challenges: A survey*. 445–454.

Vieira, K., Schulter, A., Westphall, C., & Westphall, C. (2009). Intrusion Detection for Grid and Cloud Computing. *IT Professional*, *12*(4), 38–43.

Xiong, K., & Chen, X. (2015). *Ensuring Cloud Service Guarantees via Service Level Agreement (SLA)-Based Resource Allocation*. 35–41.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*, 7–18.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592.