Pilvipalveluiden käyttö Suomessa, palveluntarjoajien erot

Jante Haavanoksa

Haaga-Helia ammattikorkeakoulu
Tradenomi tietojenkäsittely
Opinnäytetyö
2025

Tiivistelmä

Tekijä(t)
Jante Haavanoksa

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Pilvipalveluiden käyttö Suomessa, palveluntarjoajien erot

Sivu- ja liitesivumäärä
20

Tässä opinnäytetyössä tutkittiin kolmen globaalin pilvipalveluntarjoajan – AWS:n, Azuren ja GCP:n – ominaisuuksia tietoturvan, kustannustehokkuuden ja suorituskyvyn näkökulmista. Lisäksi tarkasteltiin pilvipalveluiden vaatimusten määrittelyä sekä pohdittiin yritykselle sopivimman pilvipalveluntarjoajan valintaa.

Työssä käsiteltiin ensin pilvipalveluiden yleisiä määritelmiä ja eri toimitusmalleja. Tämän jälkeen perehdyttiin pilvipalveluiden vaatimusten määrittelyyn tietoturvan, kustannustehokkuuden ja suorituskyvyn osalta. Lopuksi analysoitiin kolmen palveluntarjoajan ominaisuuksia näiden vaatimusten näkökulmasta ja arvioitiin, mikä niistä soveltuisi parhaiten yrityskäyttöön.

Tämä kirjallisuuskatsaus muodostaa kokonaiskuvan keskeisistä tekijöistä, jotka tulee ottaa huomioon pilvipalveluntarjoajaa valittaessa.

Asiasanat
Pilvipalvelut, AWS, Azure, GCP, kustannustehokkuus, suorituskyky, tietoturva

Sisällys

1 Johdanto

Pilvipalveluiden käyttö Suomessa on ollut kasvussa jo vuosia. Vuonna 2022 pilvipalveluita käytti 81 % yrityksistä, ja kahdeksassa vuodessa osuus on kasvanut 30 prosenttia. (Tietotekniikan käyttö yrityksissä 2022). Pilvipalveluiden käyttö tarjoaa yrityksille joustavuutta, kustannustehokkuutta ja tietoturvallisuutta. Yhä useampi organisaatio uskoo lisäävänsä pilvipalveluiden käyttöä merkittävästi tulevaisuudessa (Huoltovarmuusorganisaatio, 2024). Pilvipalveluiden käyttöönottoon liittyy kuitenkin mieltä askarruttavia kysymyksiä, kuten mitä pilvipalveluiden käyttö tulee maksamaan ja onko se tietoturvallista. Keskityn tässä opinnäytetyössä vertailemaan Suomessa yleisimmin käytettyjä suurimpia pilvipalveluntarjoajia ja niiden eroja.

Tämän opinnäytetyön tarkoituksena on tutkia globaalien pilvipalvelutoimijoiden AWS:n, Azuren ja Googlen eroja ja pohtia niiden skaalautuvuutta suomalaisten yritysten käyttöön. Työssä tarkastellaan erityisesti palveluiden kustannustehokkuutta, suorituskykyä ja tietoturvaa. Lisäksi tavoitteena on selvittää datan sijainnin merkitys Suomessa toimiville yrityksille. Lopputuloksena pyritään tarjoamaan yrityksille käytännönläheisiä suosituksia, jotka helpottavat oikean pilvipalveluratkaisun valintaa liiketoiminnan tarpeisiin.

Tutkimuskysymyksinä tässä opinnäytetyössä toimivat seuraavat kysymykset:

- Miten pilvipalveluntarjoajat huomioivat tietoturvan palveluissaan?
- Mitä tarkoittavat pilvipalveluiden suorituskyky ja kustannustehokkuus?
- Mitkä tekijät vaikuttavat yrityksen pilvipalveluntarjoajan valintaan?

Tämä opinnäytetyö toteutetaan kirjallisuuskatsauksena. Tutkimus kerää tietoa avoimista lähteistä ja vertailee palveluntarjoajien eroja vastaten tutkimuksessa esitettyihin kysymyksiin.

Opinnäytetyö on jaettu kolmeen osaan. Ensimmäisessä osassa esitellään pilvipalveluiden yleiset periaatteet ja niiden käyttö Suomessa. Toinen osa käsittelee globaalien palveluntarjoajien eroja. Kolmannessa osassa esitetään johtopäätökset ja suositukset yrityksille pilvipalveluiden valinnasta.

Taulukko 1 esittää tutkimuskysymykset ja mistä luvuista löytyvät tietoperusta ja mistä tulokset.

Taulukko 1. Peittomatriisi

Alaongelma	**Tietoperusta (luku)**	**Tulokset (luku)**
Miten pilvipalveluntarjoajat huomioivat tietoturvan palveluissaan?	2.3	3.2.1, 3.2.2, 3.2.3
Mitä tarkoittavat pilvipalveluiden suorituskyky ja kustannustehokkuus?	2.4, 2.5	3.2.1, 3.2.2, 3.2.3
Mitkä tekijät vaikuttavat yrityksen pilvipalveluntarjoajan valintaan?	3.2	4

1.1 Käsitteet

Taulukko 2. Opinnäytetyön keskeiset käsitteet

Azure	Microsoftin tarjoama pilvialusta (Microsoft s. a.)
AWS	Amazon Web Services, Amazonin tarjoama pilvialusta (AWS s.a.).
GCP	Google Cloud Platform, Googlen tarjoama pilvialusta (Google Clous s.a.).
GDPR	General Data Protection Regulation, yleinen tietosuoja-asetus (European Council, Council of the European Union 2024).
Iaas	Infrastructure as a Service, IT-infrastruktuuri palveluna (Ipsale & Gilioli 2022, luku 1).
PaaS	Platform as a Service, sovelluskehitysalusta palveluna internetin (Ipsale & Gilioli 2022, luku 1).

SaaS	Software as a Service, sovellus palveluna internetin yli (Ipsale & Gilioli 2022, luku 1).
Julkinen pilvi	Pilvimalli, jossa pilvitila on jaettu useiden organisaatioiden kesken samassa palvelimessa (Google Cloud s.a.).
Yksityinen pilvi	Pilvimalli, jossa voi varata tietyn palvelimen ja luoda yksityiset yhteydet palvelimelle palveluntarjoajalta (Google Cloud s.a.).
Hybridpilvi	Pilvimalli, jossa hyödynnetään sekä julkista, että yksityistä pilvimallia (Google Cloud s.a.).
Monipilvi (Multi-Cloud)	Pilviympäristö, jossa yritys hyödyntää eri pilvipalvelumalleja eri palveluntarjoajilta (Google Cloud s.a.).
Pay-as-you-go	Kustannusmalli, jossa maksetaan käytetystä pilviresurssista sen mukaan, kun sitä käytetään (Lovett 16.6.2023).

2 Tietoperusta

Tässä kappaleessa käsitellään opinnäytetyön tietoperustaa, joka muodostaa teoreettisen taustan tutkimukselle. Kappaleessa tarkastellaan pilvipalveluita yleisesti sekä niiden keskeisiä palvelumalleja. Lisäksi perehdytään pilvipalveluiden vaatimusten määrittelyyn, erityisesti tietoturvan osalta. Kappaleessa käsitellään myös pilvipalveluiden kustannustehokkuutta ja suorituskykyä. Tietoturvan osalta tarkastellaan pilvipalveluiden turvallisuusvaatimuksia, kustannustehokkuuden kohdalla eri hinnoittelumalleja ja resurssien optimointia, ja suorituskyvyn osalta suorituskykyyn vaikuttavia tekijöitä. Tämä tietoperusta luo pohjan myöhemmälle pilvipalveluntarjoajien vertailulle ja analyysille.

2.1 Pilvipalvelut yleisesti

Pilvi on tallennustilaa, johon pääsee käsiksi internetyhteyden yli. Kolmannen osapuolen palveluntarjoajat varmistavat fyysisten laitteiden toiminnan sekä palvelinsalien fyysisen tietoturvan. Pilvi tarjoaa yksityisille henkilöille ja yrityksille palveluita, kuten laskentatehoa, tallennustilaa ja tietokantoja. Pilvitila on skaalautuvaa, mikä mahdollistaa ylläpitokustannusten minimoinnin varaamalla pilviresursseja käyttötarpeen mukaan. (Microsoft s.a.)

Pilveä voi käyttää moniin eri käyttötarkoituksiin. Yleisimpiä käyttötarkoituksia kaikentyyppisten organisaatioiden keskuudessa ovat pilven käyttö tallennustilana ja varmuuskopiointiin, katastrofinpalautukseen, virtuaalityöpöytiin, ohjelmistokehitykseen ja -testaukseen, data-analytiikkaan ja verkkosovelluksiin. Pilvi on ketterää, joustavaa ja kustannustehokasta. Pilviresurssin käyttöönotto voi tapahtua minuuteissa, ja yritykset voivat keskittyä liiketoiminnan kehittämiseen resurssien etukäteen varaamisen sijaan. Pilvipalveluntarjoajat mahdollistavat organisaatioiden globaalin laajentumisen tarjoamalla mahdollisuuden varata pilvitilaa ympäri maailmaa sijaitsevista konesaleistaan. Tämä mahdollistaa liiketoiminnan laajentamisen lähemmäksi loppukäyttäjiä, vähentäen viivettä ja parantaen käyttökokemusta. (AWS s.a.)

Pilveä on tarjolla erilaisina palvelumalleina. Näitä ovat julkisen pilven palvelumalli, yksityisen pilven palvelumalli, hybridpilvimalli, joka on yhdistelmä edellä mainituista palvelumalleista, sekä monipilvimalli, jossa hyödynnetään useampaa kuin yhtä pilvimallia useilta pilvipalveluntarjoajilta. Julkinen pilvi on malli, jossa pilvitila on jaettu useiden organisaatioiden kesken yhdellä palvelimella. Yksityinen pilvi tarkoittaa, että yritys voi varata tietyn palvelimen ja luoda yksityiset yhteydet palvelimelle palveluntarjoajalta. Yksityinen pilvi mahdollistaa pilvipalvelun käytön yrityksille, jotka edellyttävät tarkkoja tietoturvavaatimuksia. Hybridpilvimalli hyödyntää sekä julkista, että yksityistä pilvimallia, mahdollistaen arkaluontoisen tiedon tallentamisen vaatimustenmukaiseen yksityiseen pilveen ja samalla hyödyntäen julkisen pilven skaalausmahdollisuutta integroimalla tiedot eri kerroksilla. Monipilvimalliksi kutsutaan mallia, jossa yritys hyödyntää eri pilvipalvelumalleja eri palveluntarjoajilta.

Tämän mallin avulla voidaan hyödyntää eri palveluntarjoajien tarjoamia ominaisuuksia liiketoiminnassa. (Google Cloud s.a.)

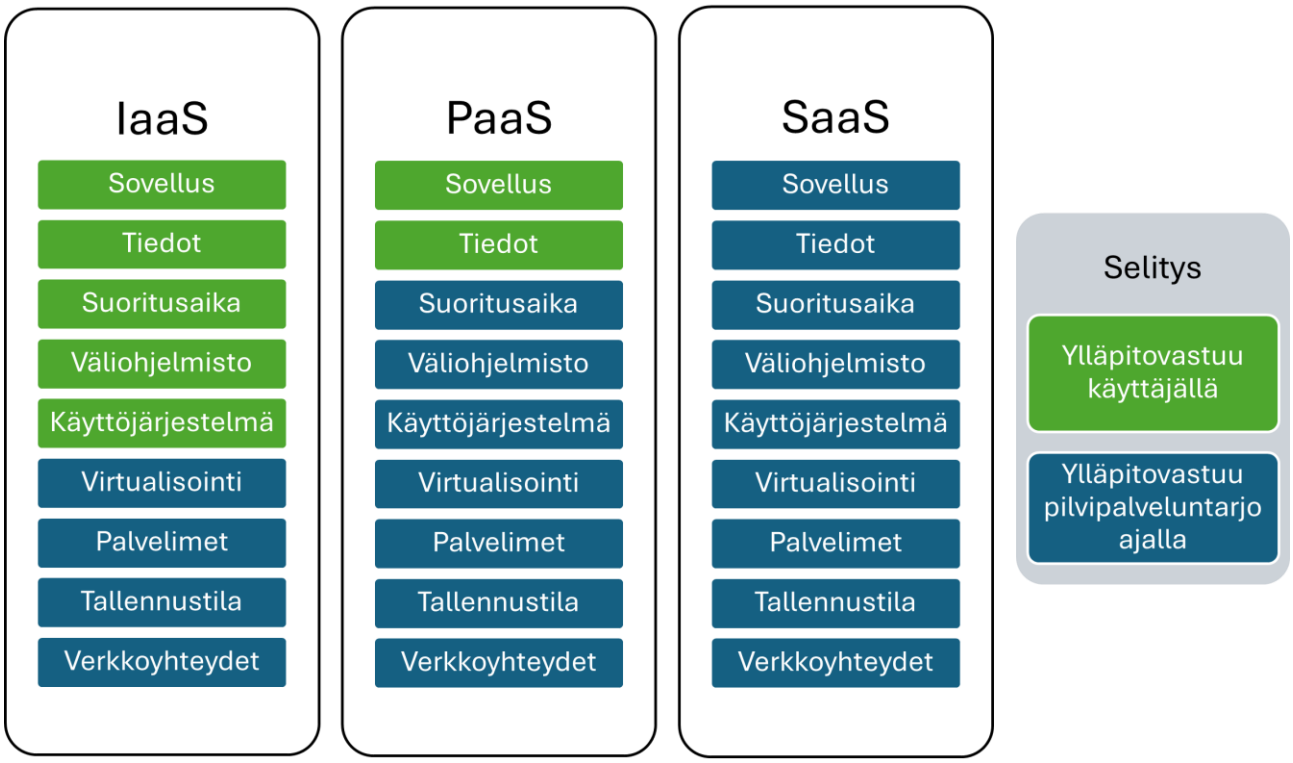
Edellä mainittujen pilvipalveluiden toimitusmallien lisäksi pilvipalvelut voidaan jakaa kolmeen eri alaluokkaan: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) ja Software as a Service (SaaS).

IaaS-mallissa vuokrataan koko IT-infrastruktuuri, kuten virtuaalikoneet, tallennustila, verkkoyhteydet ja käyttöjärjestelmät. Tässä mallissa käyttäjä on vastuussa näiden palveluiden hallinnasta, kun taas pilvipalveluntarjoaja vastaa fyysisestä arkkitehtuurista ja virtualisointi-infrastruktuurista. (Ipsale & Gilioli 2022, luku 1.)

PaaS-mallissa käyttäjän vastuulla on sovellus ja sen kehittäminen, kun taas pilvipalveluntarjoaja vastaa palvelimesta, tallennustilasta ja verkkoyhteyksistä (Ipsale & Gilioli 2022, luku 1).

SaaS-mallissa pilvipalveluntarjoaja vuokraa sovelluksia käyttäjille, jolloin käyttäjien ei tarvitse huolehtia ohjelmistojen tai laitteistojen hallinnasta – tämä vastuu kuuluu täysin pilvipalveluntarjoajalle (Ipsale & Gilioli 2022, luku 1).

Kuva 1 esittää vertailun näistä palveluista.



Kuva 1. Pilvipalvelumallien hallintavastuut (mukaillen Ipsale & Gilioli 2022, luku 1.)

2.2 Pilvipalveluiden vaatimusten määrittely

Pilvipalveluntarjoajaa valitessa on tärkeää määritellä pilvipalvelulle asetettavat vaatimukset, jotta se vastaa organisaation tarpeita ja tukee liiketoiminnan tavoitteita. Vaatimusten määrittelyssä tulee huomioida muun muassa tietoturva, kustannustehokkuus ja suorituskyky. Selkeästi määritellyt vaatimukset auttavat vertailemaan eri palveluntarjoajia ja varmistamaan, että valittu ratkaisu täyttää sekä tekniset että liiketoiminnalliset odotukset.

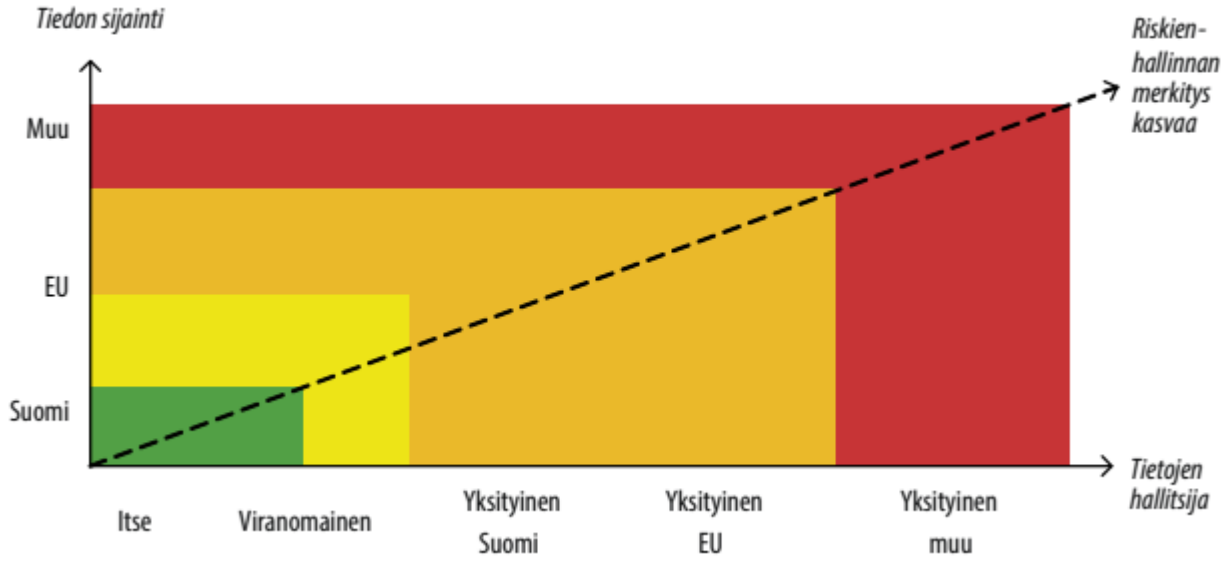
2.3 Tietoturva

Kyberturvallisuuskeskus on laatinut pilvikriteeristön (PiTuKri) tukemaan viranomaisia pilvipalvelujen turvallisuuden arvioinnissa ja hallinnassa, mutta se on hyödynnettävissä myös kaupallisille toimijoille (Pahlman 16.1.2024). Katakri on turvallisuusauditointikriteeristö, jota voidaan soveltaa myös pilvipalveluiden tietoturvaan. Sen avulla arvioidaan kohdeorganisaation ympäristöjä, joissa käsitellään tietoa, sekä niiden salassapitoa ja tietojen paljastumisen ehkäisyä. (Ulkoministeriö s.a.)

Yleisiä kansainvälisiä vaatimusten viitekehyksiä ovat ISO-standardit. Tietoturvallisuuden hallintaan tarkoitettu ISO 27000 -standardi tarjoaa yrityksille ja organisaatioille ohjeita tietoturvan hallintaan. Joissain tapauksissa organisaatiot voivat edellyttää tiettyjen standardien noudattamista, esimerkiksi kilpailutuksissa tai alihankkijoiltaan. Standardit helpottavat myös tuotteiden ja palveluiden sertifiointia. (SFS, Suomen Standardit s.a.)

Näiden lisäksi Euroopan unionin vuonna 2018 voimaan tullut yleinen tietosuoja-asetus (GDPR, General Data Protection Regulation) asettaa tarkat vaatimukset yrityksille ja organisaatioille henkilötietojen keräämiseen ja käsittelyyn (European Council, Council of the European Union 2024).

Tiedon sijainnilla on merkitystä riskien hallinnassa. Tietosuojalait, kuten GDPR, voivat asettaa vaatimuksia datan sijainnille. Valtiovarainministeriön päätöksen mukaisesti julkisen hallinnon organisaatioille on laadittu linjaus tietojen käsittelystä pilvipalveluissa. Sen mukaan tietoa voidaan käsitellä julkisessa pilvipalvelussa, kun tietoturvasta ja -suojasta on asianmukaisesti huolehdittu. Riskienhallinnan merkitys kasvaa, kun tieto ja palvelut sijaitsevat yhä kauempana Suomesta ja hallinta siirtyy muille toimijoille. Tämä esitetään kuvassa 2. (Valtioneuvosto. 2018.)



Kuva 2. Tiedon sijainnin ja hallinnan merkitys riskienhallinnassa (Valtioneuvosto. 2018).

2.4 Kustannustehokkuus

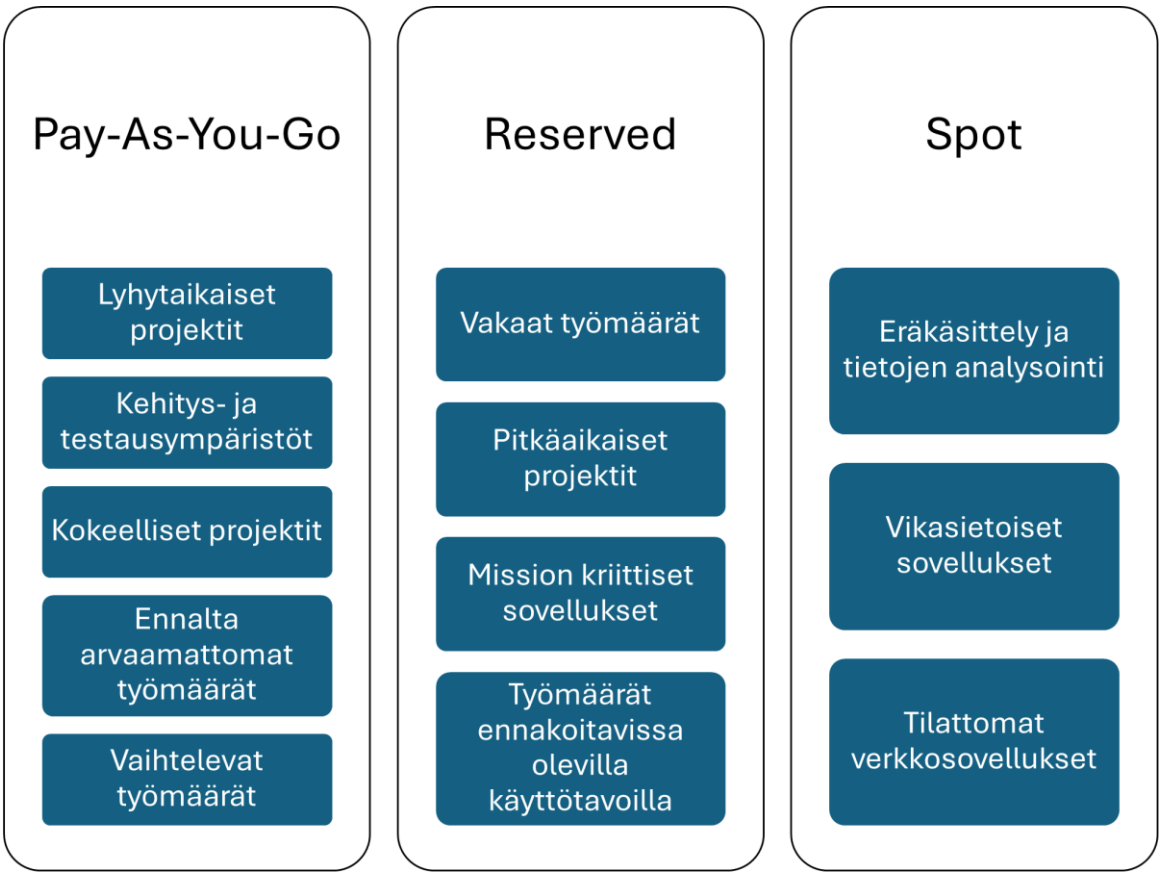
Kustannustehokkuuteen vaikuttavat hinnoittelumallit, joita ovat muun muassa pay-as-you-go-, reserved- ja spot-mallit. Lisäksi palveluntarjoajilla voi olla erilaisia säästöohjelmia, joissa sitoudutaan yleensä vähintään vuodeksi maksamaan tietty kuukausittainen summa käytetystä palvelusta. (Lovett 16.6.2023.)

Yleisimpänä mallina pidetään pay-as-you-go-mallia, jossa maksetaan käytetystä pilviresurssista sen mukaan, kun sitä käytetään. Tässä mallissa ei tarvitse sitoutua maksusopimuksiin, ja se on joustavasti skaalattavissa. Se sopii erityisesti lyhytaikaisiin projekteihin sekä kehitys- ja testausympäristöihin. (Lovett 16.6.2023.)

Reserved-mallissa varataan tietty määrä pilvikapasiteettia tietyksi ajanjaksoksi. Palveluntarjoajan mukaan sitoudutaan yleensä maksamaan varatusta kapasiteetista vuodeksi tai kolmeksi vuodeksi. Tämän mallin etuna ovat kustannussäästöt, jotka toteutuvat, kun työmäärä on tiedossa ennakkoon. Se sopii erityisesti vakaille työkuormille ja pitkäaikaisille projekteille. (Lovett 16.6.2023.)

Spot-mallissa käyttämättömiä pilviresursseja on saatavilla alennettuun hintaan. Tämä malli sopii silloin, kun työkuorma on joustava. Hyviä käyttötapauksia ovat muun muassa tietojen analysointi, vikasietoiset sovellukset ja tilattomat verkkosovellukset. Palveluntarjoaja voi kuitenkin lopettaa resurssin lyhyelläkin varoitusajalla, joten jatkuvaa käyttöä vaativat projektit eivät sovellu tähän malliin. (Lovett 16.6.2023.)

Kuvassa kolme on esitetty hinnoittelumallit ja niiden suositellut käyttötarkoitukset mukaillen Channing Lovettin blogikirjoituksen kuvaa.



Kuva 3. Hinnoittelumallit ja suositellut käyttötarkoitukset (mukaillen Lovett 16.6.2023.)

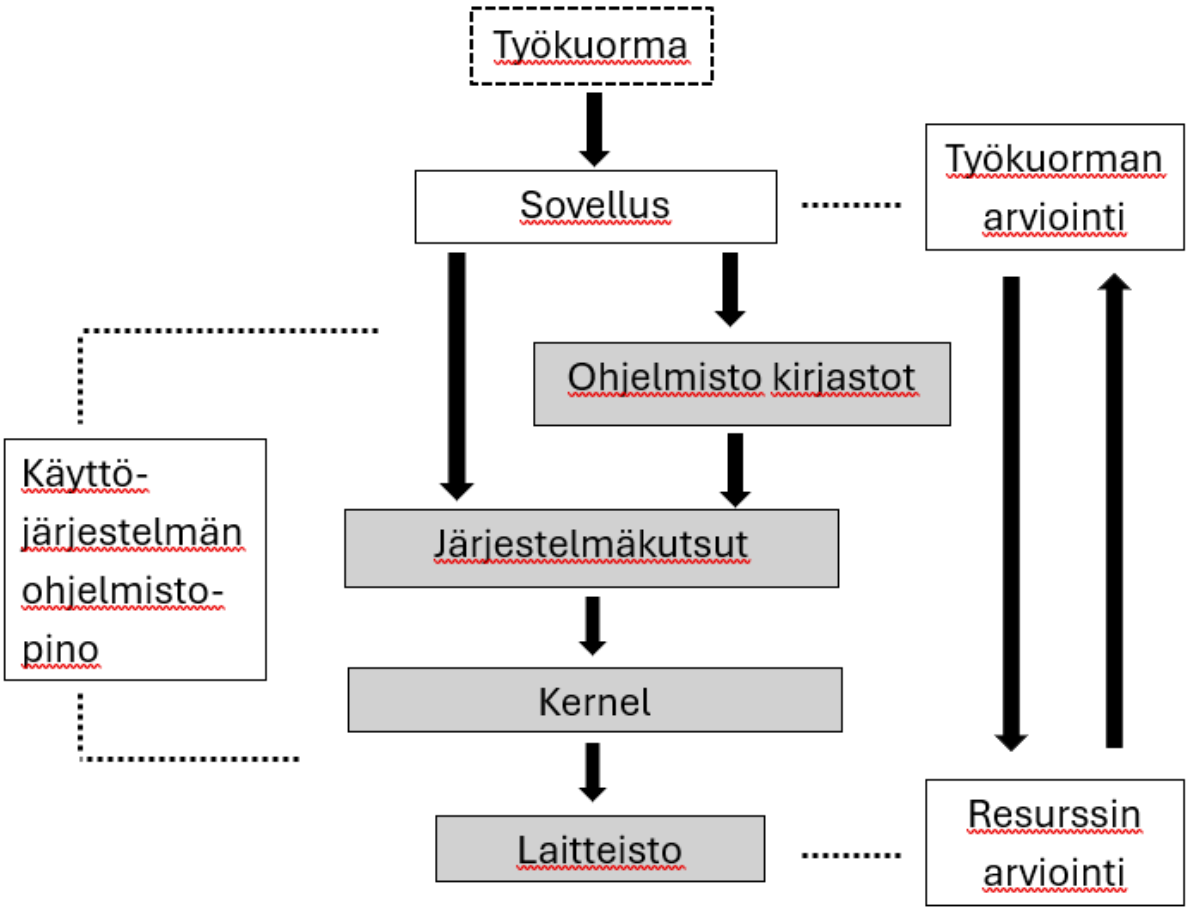
2.5 Suorituskyky

Suorituskyvyssä tulee ottaa huomioon pilviresurssien kyky käsitellä tarvittavia tehtäviä. Suorituskykyyn vaikuttavat pilviresurssille määritellyt ominaisuudet, kuten muistin määrä ja prosessorin tehokkuus, verkkoyhteydet ja ohjelmistot. Palveluntarjoajilla on myös erilaisia palvelutasosopimuksia (SLA), joissa määritellään palveluntarjoajan lupaukset asiakkaalle keskeytymättömästä palvelusta. (Dierolf, Nucci & Sevilla 19.2.2025)

Suorituskyky kattaa koko järjestelmän fyysisestä laitteistosta ohjelmistopinoihin. Pilvipalvelun tarvittavat resurssit määritellään yleensä kehitysvaiheessa käyttötarpeen ja projektin mukaan. Suorituskykyä on analysoitava koko kehitysprosessin ajan ja myös sen jälkeen. Jos palvelun kuormitus kasvaa, resursseja on lisättävä. Resurssien arviointi vaatii yleensä järjestelmävalvojien ja sovelluskehittäjien yhteistyötä, ja jokaisella näkökulmalla on omat vahvuutensa. (Gregg 2013, luku 1)

Suorituskyvyn arviointi voi olla haastavaa, ja siihen liittyy usein ongelmia. Suorituskyky on osittain subjektiivista – se, mikä yhdelle on 'huono' suorituskyky, voi toiselle olla 'hyvä'. Tähän vaikuttavat muun muassa kehittäjien ja käyttäjien odotukset palvelun suhteen. Hyvänä käytäntönä voidaan pitää selkeää tavoitteiden asettelua, esimerkiksi määrittelemällä, millaista vasteaikaa resurssilta odotetaan. (Gregg 2013, luku 1)

Kuvassa neljä on suorituskykyanalyysi, jossa ohjelmistopinoa lähestytään resurssin ja työmäärän näkökulmista.



Kuva 4. Analyysinäkymä suorituskyvystä (mukaillen Gregg 2013 luku 1)

3 Tutkimuksen toteutus

Tässä kappaleessa esitellään tutkimusmenetelmäksi valittu kuvaileva kirjallisuuskatsaus sekä tutkimuksessa hyödynnettävä kirjallisuus. Lisäksi kappaleessa tarkastellaan globaalien pilvipalveluntarjoajien toimintaa ja vertaillaan niiden keskeisiä ominaisuuksia, kuten tietoturvaa, kustannustehokkuutta ja suorituskykyä. Tämä tarkastelu luo pohjan tutkimuksen myöhemmille osioille, joissa pohditaan palveluntarjoajien ja pilvimallien valintaa liiketoiminnan näkökulmasta.

3.1 Tutkimusmenetelmän esittely

Narratiivinen kirjallisuuskatsaus, eli kuvaileva kirjallisuuskatsaus, on menetelmä, jossa esitellään aiempia tutkimuksia aiheesta. Sen tarkoituksena on tarjota teoreettisia näkökulmia valitun tutkimusaineiston pohjalta. Katsauksen avulla voidaan kyseenalaistaa aiempaa tutkimusta, tunnistaa tutkimustarpeita tai vahvistaa olemassa olevaa tietoa. Lisäksi se syventää tutkijan ymmärrystä aiheesta ja mahdollistaa aiheen tulkinnan sekä teorian muodostamisen intuitiivisesti ja omien mielleyhtymien pohjalta. (Vilkka 2023, luku 1.2.1)

Kirjallisuutena tässä opinnäytetyössä on käytetty pilvipalveluntarjoajien omia verkkosivustoja sekä O'Reillystä löytyviä teoriakirjoja, jotka käsittelevät pilvipalveluntarjoajia ja niiden ympäristöjen hallintaa. Lisäksi lähteinä on hyödynnetty tieteellisiä artikkeleita ja raportteja, jotka tarjoavat syvällisempää analyysiä pilvipalveluiden tietoturvasta, kustannustehokkuudesta ja suorituskyvystä. Näiden lähteiden avulla muodostetaan kattava käsitys aiheesta ja varmistetaan tutkimuksen teoreettinen perusta.

3.2 Globaalit pilvipalveluntarjoajat

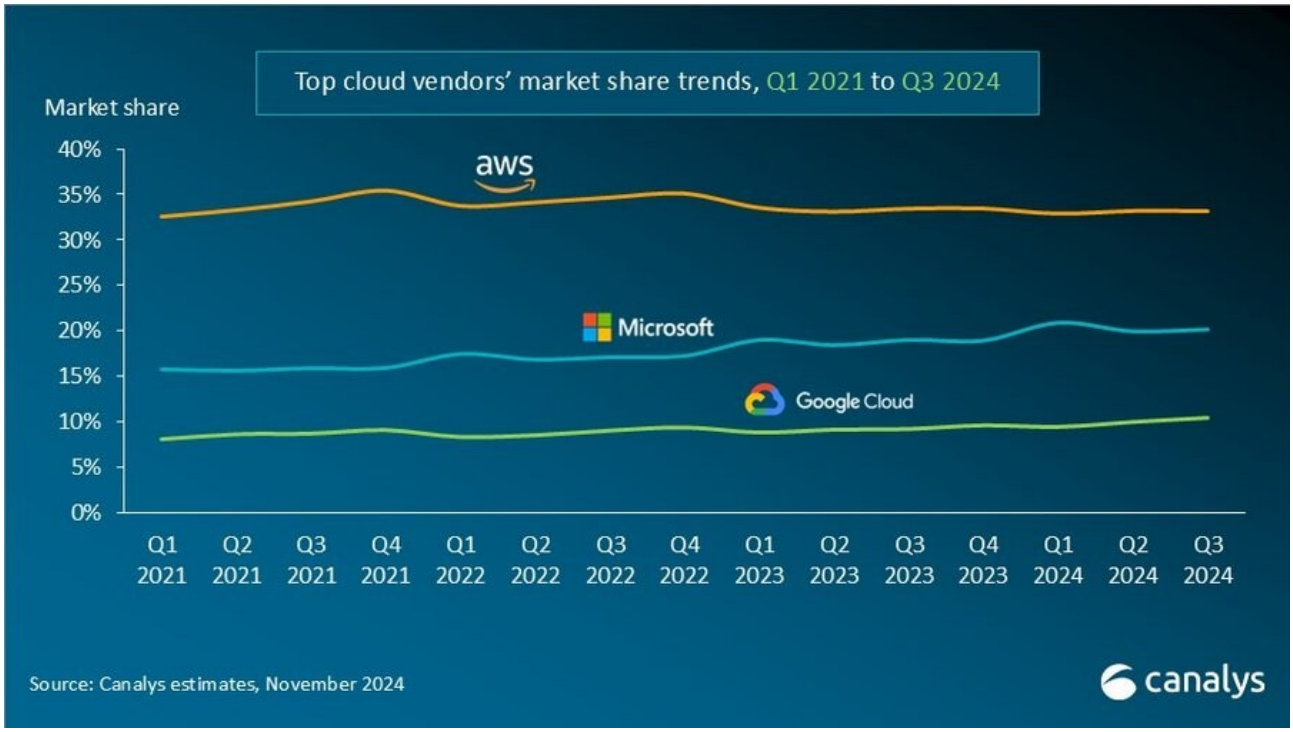
Digitalisaation kehitys on lisännyt pilvipalveluiden suosiota suomalaisten yritysten ja organisaatioiden IT-strategiassa. Tietoturva ja lainsäädäntö ovat keskeisiä tekijöitä, jotka vaikuttavat suomalaisten yritysten pilvipalveluntarjoajan valintaan. Suomen markkinoilla toimii sekä globaaleja että kotimaisia palveluntarjoajia. (Tieturi 14.3.2025.) Tässä osiossa tarkastellaan kolmen suosituimman globaalin palveluntarjoajan ominaisuuksia ja niiden sopivuutta suomalaisten yritysten tarpeisiin.

Suomessa käytetyimmät globaalit palveluntarjoajat ovat Amazon, Microsoft ja Google. Kansainvälinen pilvipalvelu sopii yrityksille, jotka käsittelevät suuria tietomääriä ja tarvitsevat joustavia IT-ratkaisuja. Sen etuina pidetään skaalautuvuutta, korkeaa saatavuutta ja suorituskykyä. Lisäksi näillä palveluntarjoajilla on laaja valikoima valmiita IT-palveluita ja sovelluksia. (Tieturi 14.3.2025.)

Taulukko 3. Palveluntarjoajien kuvaus ja soveltuvuus yritykselle (Tieturi 14.3.2025)

Palveluntarjoaja	**Kuvaus**	**Soveltuvuus**
Amazon Web Services (AWS)	Maailman suurin pilvipalvelu, laaja valikoima palveluita.	Suuret yritykset, startupit.
Microsoft Azure	Integroituu hyvin Microsoftin tuotteisiin, kuten Office 365:een.	Yritykset, joilla on Microsoft-ekosysteemi.
Google Cloud Platform (GCP)	Vahva data-analytiikassa ja tekoälypalveluissa.	Data-analytiikkaa hyödyntävät yritykset.

Näistä palveluntarjoajista globaalisti suosituin on AWS. Vuoden 2024 kolmannella vuosineljännekselllä suurin kasvu edelliseen vuoteen verrattuna oli Google Cloudilla, joka kasvoi 36 %. Microsoftin kasvu oli 33 %, kun taas AWS raportoi 19 % kasvua. (Canalys 19.11.2024.)



Kuva 5. Kolmen suurimman pilvipalveluntarjoajan kasvu vuosina 2021–2024 (Canalys 19.11.2024)

3.2.1 Amazon Web Services (AWS)

Suurin ja suosituin palveluntarjoaja, AWS, jonka pilviliiketoiminta alkoi vuonna 2006, hallitsee globaalia pilvimarkkinaa. Sillä on laajin datakeskusverkosto, joka kattaa 22 aluetta (region) ja 69 saatavuusaluetta (availability zone). (Lähteenmäki 22.11.2023.)

AWS:llä on monia tietoturvatyökaluja. Erityisen tärkeää tietoturvan kannalta on varmistaa, että tietoturva-asetukset on konfiguroitu oikein, sillä väärin konfiguroidut asetukset voivat johtaa tietoturvaloukkauksiin. On hyvä huolehtia siitä, että pääsyoikeudet on määritelty oikeille käyttäjille ja että oikeudet rajoittuvat vain tarpeellisiin tietoihin. (Tieturi 17.6.2024.) AWS:ssä pääsynhallintatyökalu on AWS Identity and Access Management (IAM), jolla hallitaan käyttäjätunnuksia ja käyttöoikeuksia. IAM tukee myös kaksivaiheista tunnistautumista, jolla varmistetaan turvallinen kirjautuminen käyttäjätunnuksilla. (MGT-COMMERCE. s.a.)

Pääsynhallinnan lisäksi on hyvä suojautua mahdollisilta DDoS-hyökkäyksiltä eli palvelunestohyökkäyksiltä, jotka voivat aiheuttaa palvelukatkoksia ja häiritä liiketoimintaa (Tieturi 17.6.2024). Tähän tarkoitukseen on AWS Shield, joka auttaa suojaamaan AWS:ssä toimivia verkkosovelluksia. Palvelu tunnistaa ja torjuu automaattisesti kehittyneitä verkkotason hyökkäyksiä (AWS. s.a.).

Muita hyödyllisiä AWS:n tietoturvapalveluita ovat; AWS Key Management Service (KMS) – luo ja hallinnoi tietojen salaamiseen käytettäviä salausavaimia. Amazon GuardDuty – monitoroi lokitietoja uhkien havaitsemiseksi. Se tarkkailee ja analysoi tapahtumia sekä työkuormia ja tarjoaa tietoturvahavaintoja koneoppimisen avulla. AWS CloudTrail – tallentaa suoritetut API-kutsut sekä käyttäjien, palveluiden ja AWS-resurssien toimenpiteet lokitietoihin. Amazon Inspector – arvioi AWS-resurssien tietoturvaa automaattisesti ja tunnistaa mahdolliset tietoturva-aukot sekä yhteensopivuusongelmat. AWS Config – seuraa resurssien määritystilaa ennalta määriteltyjen sääntöjen perusteella ja tunnistaa mahdolliset muutokset. Amazon Macie – käyttää koneoppimista ja tunnistaa datan arkaluontoisuuden, kuten henkilötiedot. AWS WAF (Web Application Firewall) – suojaa ja tunnistaa yleisimmät verkkohyökkäykset. Sen avulla voidaan määrittää sääntöjä ja ehtoja saapuvien HTTP- ja HTTPS-pyyntöjen suodattamiseksi. Amazon VPC (Virtual Private Cloud) – tarjoaa loogisesti eristetyn osan AWS-pilvestä, jossa voidaan käynnistää AWS-resursseja määritellyssä virtuaalisessa verkossa. (MGT-COMMERCE. s.a.)

AWS:n hinnoittelu perustuu käytön mukaan hinnoitteluun eli pay-as-you-go -malliin. AWS:llä on työkalu AWS Cost Explorer, jonka avulla voi seurata ja hallita AWS-kustannuksia ja -käyttöä ajan mittaan. AWS:llä on myös työkalu, jolla voi laskea palveluiden hinnan ennen sen ostamista. (AWS. s.a.)

3.2.2 Microsoft Azure

Suomessa on vahva Microsoft-historia, minkä vuoksi Azure on vakiinnuttanut asemansa suomalaisten yritysten keskuudessa. Azure on luonnollinen valinta yrityksille, jotka hyödyntävät Microsoft-arkkitehtuuria, kuten Office 365 -ympäristöä ja muita Microsoft-tuotteita. Lisäksi Suomessa on enemmän Microsoft-kumppaneita kuin AWS- tai Google-kumppaneita. (Lähteenmäki 22.11.2023.)

Myös Azurella on omat tietoturvatyökalunsa. Azurella on lisäksi identiteetti- ja pääsynhallintaratkaisut, joilla tunnistetaan ja suojataan haitallisilta kirjautumisyrityksiltä sekä määritetään mahdolliset vahvat todennusvaihtoehdot (Azure s.a.).

Muita Azuren tietoturvaratkaisuja ovat; Microsoft Defender for Cloud – suojaa pilviresursseja eri ympäristöissä, tunnistaa tietoturva-aukkoja ja antaa suosituksia niiden korjaamiseksi. Se tarjoaa yhtenäisen tietoturvan hallinta-alustan, jolla voi suojata pilviresursseja ennakoivasti. Key Vault – salaisuuksienhallintatyökalu, joka suojaa salausavaimia ja muita pilvisovellusten ja -palveluiden käyttämiä salaisuuksia. Azure DDoS Protection – palvelunestohyökkäysten torjuntatyökalu, joka valvoo jatkuvasti verkkoliikennettä ja suodattaa haitallisen liikenteen ennen kuin se saavuttaa pilviresurssin. Azure Information Protection – auttaa hallinnoimaan ja suojaamaan sähköpostia, asiakirjoja ja arkaluontoisia tietoja, joita jaetaan yrityksen ulkopuolelle. Application Gateway – suojaa verkkosovelluksia haavoittuvuuksilta ja hallinnoi verkkoliikennettä. (Azure s.a.)

Azuren hinnoittelumalleihin kuuluvat sekä käytönmukainen hinnoittelu että erilaiset tilausvaihtoehdot, kuten yhden tai kolmen vuoden tilauslaskutusmalli. Azuressa on myös helppo seurata kustannuksia Cost Management -työkalun avulla. (Microsoft Learn 22.1.2025.)

3.2.3 Google Cloud Platform (GCP)

Suomalaisten keskuudessa vähiten tunnettu Google Cloud tarjoaa huippunopeat tiedonsiirrot, tehokkaan big datan prosessoinnin sekä monipuoliset tekoäly- ja koneoppimispalvelut. Lisäksi Google on tällä hetkellä ainoa näistä palveluntarjoajista, jolla on datakeskus Suomen rajojen sisällä. (Lähteenmäki 22.11.2023.)

Googlella on monia tietoturvatyökaluja, joilla suojata pilviympäristöä. Myös Googlella on vastaavat ominaisuudet kuin AWS:llä ja Azurella turvata pilviympäristöä. Googlen identiteetin- ja käyttöoikeushallinnan avulla on mahdollista määrittää, että käyttäjillä ja palveluilla on vain tarvitsemansa käyttöoikeudet (Google Cloud s.a.).

Muita tärkeitä tietoturvatyökaluja Googlella ovat; Google Cloud Armor – verkkosovellusten suojaustyökalu, joka suojaa palvelunestohyökkäyksiltä. Security Command Center – auttaa tunnistamaan

haavoittuvuuksia, havaitsemaan uhkia ja valvomaan vaatimustenmukaisuutta. Cloud Key Management Service (KMS) – salaisuuksienhallintatyökalu salausavaimien hallintaan. VPC Service Controls – auttaa arkaluontoisen datan suojaamisessa. Cloud Data Loss Prevention – alusta, joka on tarkoitettu arkaluontoisten tietojen tarkistukseen, luokitteluun ja muokkaamiseen. (Google Cloud s.a.)

Google Cloudin hinnoittelumalleihin kuuluvat sekä käytönmukainen hinnoittelu että tilausmallit. Kustannuksia on helppo seurata Googlen Cost Management -työkalulla, jolla voi optimoida tekoälypohjaisia suosituksia sekä luoda kuluista hälytyksiä tai kiintiörajoja. (Google Cloud s.a.)

4 Tulokset - Suosituksia pilvipalveluratkaisun valintaan

Tutkimuksen tavoitteena oli selvittää pilvipalveluntarjoajien erot ja ominaisuudet sekä esittää suosituksia eri liiketoimintaratkaisuille. On kuitenkin todettu, ettei pilvipalveluratkaisun valintaan ole yksiselitteisesti oikeaa tai väärää vastausta. On suositeltavaa välttää vendor lockia eli lukittautumista yhteen palveluntarjoajaan. Monet asiantuntijat neuvovat hyödyntämään monipilvimallia (multicloud) ja varmistamaan, että palvelut ovat siirrettävissä pilvestä toiseen. (Lähteenmäki 22.11.2023; Tieturi 14.3.2025).

Tietoturvaratkaisujen osalta pilvipalveluntarjoajilla on omat työkalunsa tietoturvan hallintaan ja uhkilta suojautumiseen. On kuitenkin tärkeää varmistaa, että datan säilyttäminen on GDPR:n mukaista. Koska globaalien pilvipalveluntarjoajien datakeskukset saattavat sijaita EU-alueen ulkopuolella, on suositeltavaa varmistaa henkilötietojen säilytyspaikka. Monet yritykset suosivatkin hybridipilvimallia, jossa suuret tietomäärät ja IT-ratkaisut toteutetaan globaalissa pilvessä, mutta arkaluontoinen data säilytetään Suomen rajojen sisällä olevassa pilvipalvelussa (Tieturi 14.3.2025).

Pilvipalveluiden käytöllä voidaan saavuttaa kustannussäästöjä valitsemalla oikeat pilvipalvelumallit. Esimerkiksi laitekustannuksia voidaan vähentää hyödyntämällä IaaS- ja SaaS-pilvipalvelumalleja, joissa kulut määräytyvät palvelun käytön mukaan. Laitehankintojen lisäksi säästöjä syntyy IT-osaston työkuormassa, sillä laitteiden ylläpidosta vastaa pilvipalveluntarjoaja. Lisäksi kustannusten optimointia helpottaa skaalautuva hinnoittelu. (Tieturi 14.3.2025).

Pilvipalveluiden käytön suosio kasvaa jatkuvasti, ja palveluntarjoajat kehittävät palveluitaan. On tärkeää pysyä ajan tasalla palveluiden muutoksista. Pilvipalveluiden hallinta vaatii osaamista, joten yritysten on suositeltavaa panostaa pilvipalveluosaamiseen, jotta niitä voidaan hyödyntää tehokkaasti ja turvallisesti (Tieturi 14.3.2025). Yksi hyvä vaihtoehto on hankkia kumppani, joka vastaa pilvipalveluiden hallinnasta. Tällöin yritykset voivat keskittyä omaan liiketoimintaansa, kun IT-kumppani huolehtii pilvipalveluiden ylläpidosta.

5 Pohdinta

Opinnäytetyössä selvitettiin pilvipalveluiden tietoturvaa, kustannustehokkuutta ja suorituskykyä. Nämä ominaisuudet ovat keskeisiä pilvipalveluiden tehokkaalle hyödyntämiselle. Tutkimuksessa tarkasteltiin kolmen eri globaalin pilvipalveluntarjoajan ominaisuuksia ja vertailtiin niiden sopivuutta yrityksille.

Tutkimuksessa selvisi, että pilvipalveluntarjoajien erot ovat hyvin pieniä, eikä pilvipalveluiden valintaan ole yksiselitteisesti oikeaa tai väärää ratkaisua. Tärkeintä on pilvipalveluiden tehokas hallinta ja ymmärrys niiden konfiguroinnista, jotta niitä voidaan hyödyntää parhaalla mahdollisella tavalla ja saavuttaa hyödyt kustannustehokkuuden, suorituskyvyn ja tietoturvan osalta. Pilvipalveluiden valintaan vaikuttavat monet tekijät, jotka riippuvat täysin yrityksen tarpeista.

Digitalisaation myötä pilvipalvelut kehittyvät jatkuvasti, mikä tuo mukanaan sekä uusia ominaisuuksia että haasteita. Teknologioiden muuttuessa myös pilvipalveluiden tietoturvaan, kustannuksiin ja suorituskykyyn liittyvät kysymykset kehittyvät. Jatkuva muutos edellyttää yrityksiltä jatkuvaa osaamisen kehittämistä, erityisesti tietoturvan osalta.

Tutkimuksessa esitettiin palveluntarjoajien vertailua tasapuolisesti ajankohtaisiin ja luotettaviin lähdeaineistoihin perustuen. Koska pilvipalvelut muuttuvat jatkuvasti, tutkimuksen tulokset kuvaavat tämän hetken tilannetta, mutta voivat muuttua ajan kuluessa. Lähdevalinnassa panostettiin asiantuntijoiden julkaisuihin ja palveluntarjoajien omaan dokumentaatioon, jotta tutkimukseen saatiin monipuolista näkökulmaa pilvipalveluiden valinnasta. Lähdeaineisto perustui julkisesti saatavilla olevaan tietoon, mikä varmistaa tutkimuksen eettisyyden säilymisen.

Jatkotutkimuksessa voitaisiin tarkastella eri toimialojen tapoja hyödyntää pilvipalveluita ja tuoda esiin niiden käytännön haasteita. Lisäksi voitaisiin selvittää, kuinka hybridipilvi- ja monipilvimallit vaikuttavat yritysten päätöksentekoon pilvipalveluratkaisuja valittaessa.

5.1 Oma oppiminen

Opinnäytetyöprosessi oli mielenkiintoinen ja kartutti kokemusta tutkimustyön toteuttamisesta sekä projektinhallinnasta. Työ vaati erityisesti suunnittelua ja ajanhallintaa, jotta projekti eteni aikataulussa. Tämän tutkimuksen myötä opin lisää pilvipalveluista sekä niiden tietoturvasta, kustannustehokkuudesta ja suorituskyvystä. Lisäksi syvensin ymmärrystäni kirjallisuuskatsauksesta tutkimusmenetelmänä ja tiedon analysoinnista.

Ammatillisen kehittymisen kannalta kartutin syvällisempää osaamista pilvipalveluntarjoajista ja niiden työkaluista. Opinnäytetyön aihe tuki nykyistä työnkuvaani teknisenä asiantuntijana, ja sen myötä hankittu tieto on suoraan hyödynnettävissä työssäni.

Suurimpia haasteita prosessissa olivat aikataulussa pysyminen, aiheen rajaaminen sopivaksi mutta kiinnostavaksi kokonaisuudeksi sekä ajankohtaisen lähdemateriaalin löytäminen. Aikataulu-haasteista selvisin tekemällä opinnäytetyötä tiettynä ajankohtana viikosta, joka sijoittui viikonlopuille. Tämä hieman pidensi odotettua aikataulua, mutta sain opinnäytetyön valmiiksi ajoissa.

Aiheen rajauksen jouduin tekemään melko suppeaksi ja pintapuoliseksi, sillä pilvipalveluiden ominaisuudet muodostavat laajoja kokonaisuuksia. Koen kuitenkin, että tämä ratkaisu toimi hyvin juuri tähän opinnäytetyöhön. Lähdemateriaalin ajankohtaisuuden varmistamiseksi pyrin hyödyntämään tutkimus- ja asiantuntija-artikkeleita, joissa oli selkeästi ilmoitettu niiden kirjoitushetki.

Kaiken kaikkiaan opinnäytetyö kasvatti ammatillista osaamistani ja tarjosi arvokkaan oppimiskokemuksen, jonka myötä koen onnistuneeni opinnäytetyön tekemisessä.

Lähteet

AWS. s.a. About AWS. Luettavissa: https://aws.amazon.com/about-aws/. Luettu: 16.3.2025.

AWS. s.a. AWS Shield. Luettavissa: https://aws.amazon.com/shield/. Luettu: 29.3.2025.

AWS. s.a. What is AWS Billing and Cost Management? Luettavissa: https://docs.aws.amazon.com/cost-management/latest/userguide/what-is-costmanagement.html. Luettu: 29.3.2025.

AWS. s.a. What is cloud computing? Luettavissa: https://aws.amazon.com/what-is-cloud-computing/. Luettu: 8.2.2025.

Azure. s.a. Identity and access management (IAM). Luettavissa: https://azure.microsoft.com/en-us/products/category/identity. Luettu: 29.3.2025.

Azure. s.a. Security. Luettavissa: https://azure.microsoft.com/en-us/products/category/security. Luettu: 29.3.2025.

Canalys. 19.11.2024. Global cloud spending surged 21% in Q3 2024. Luettavissa: https://canalys.com/newsroom/global-cloud-services-q3-2024. Luettu: 22.3.2025.

Dierolf, B., Nucci, R., Sevilla, D. 19.2.2025. How to Choose a Cloud Service Provider: A Comprehensive Guide. Guru Technologies, Inc. Luettavissa: https://www.getguru.com/reference/how-to-choose-a-cloud-service-provider. Luettu: 16.3.2025.

European Council, Council of the European Union. 2024. The general data protection regulation. Luettavissa: https://www.consilium.europa.eu/en/policies/data-protection-regulation/. Luettu: 22.02.2025.

Google Cloud. s.a. Google Cloud pricing. Luettavissa: https://cloud.google.com/pricing?hl=fi. Luettu: 29.3.2025.

Google Cloud. s.a. Security and identity. Luettavissa: https://cloud.google.com/security/products/security-and-identity?hl=fi. Luettu: 29.3.2025.

Google Cloud. s.a. What is Cloud Storage? Luettavissa: https://cloud.google.com/learn/what-is-cloud-storage?hl=fi. Luettu 8.2.2025.

Gregg, B. 2013. Systems Performance: Enterprise and the Cloud. Addison-Wesley Professional. Boston. E-kirja. Luettu: 16.3.2025.

Huoltovarmuusorganisaatio, 2024. Selvitys pilvipalveluiden käytöstä. Luettavissa: https://www.huoltovarmuuskeskus.fi/files/9236c056ef2a4fdc230a8d16fdbc64e46f6fb51f/selvitys-pilvipalveluiden-kaytosta-2024-valmis-002.pdf. Luettu: 25.1.2025.

Ipsale, M., Gilioli, M. 2022. Google Cloud Certified Professional Cloud Network Engineer Guide. Packt Publishing. Birmingham. E-kirja. Luettu 15.2.2025.

Lovett, C. 16.6.2023. Top Cloud Cost Models That Leverage Cost Efficiency. Tierpoint. Luettavissa: https://www.tierpoint.com/blog/cloud-cost-models/. Luettu: 16.3.2025.

Lähteenmäki, T. 22.11.2023. AWS, Azure vai Google Cloud? Vai onko sillä väliä? Gapps Group Blogi. Luettavissa: https://www.gappsgroup.com/fi/blogi/aws-azure-vai-google-cloud-vai-onko-silla-valia/. Luettu: 22.3.2025.

MGT-COMMERCE. s.a. Top 15 Amazon Web Services Cloud Security Tools. Luettavissa: https://www.mgt-commerce.com/blog/amazon-web-services-cloud-security/. Luettu: 29.3.2025.

Microsoft Learn. 22.1.2025. What is Microsoft Billing? Luettavissa: https://learn.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview. Luettu: 29.3.2025.

Microsoft. s. a. What is Azure? Luettavissa: https://azure.microsoft.com/en-us/explore/. Luettu: 16.3.2025.

Microsoft. s.a. What is cloud? Luettavissa: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud. Luettu: 8.2.2025.

Pahlman, S. 2024. Uusi kriteeristö ohjaa pilvipalveluiden turvalliseen käyttöön. Traficom. Luettavissa: https://www.traficom.fi/fi/ajankohtaista/blogit/uusi-kriteeristo-ohjaa-pilvipalveluiden-turvalliseen-kayttoon. Luettu: 15.2.2025.

SFS, Suomen Standardit s.a. Mitä standardi tarkoittaa? Luettavissa: https://sfs.fi/standardeista/mika-on-standardi/. Luettu: 22.02.2025.

SFS, Suomen Standardit s.a. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Luettavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/. Luettu: 22.02.2025.

Tietotekniikan käyttö yrityksissä 2022. Tilastokeskus. Luettavissa: https://stat.fi/julkaisu/cktvztyy82z790b55dz6j23q3. Luettu 25.1.2025.

Tieturi. 14.3.2025. Pilvipalvelu Suomessa – Hyödyt, haasteet ja suosituimmat palveluntarjoajat. Tieturi blogi. Luettavissa: https://www.tieturi.fi/blogi/pilvipalvelu-suomessa-hyodyt-haasteet-ja-suosituimmat-palveluntarjoajat/. Luettu: 22.3.2025.

Tieturi. 14.3.2025. Pilvipalvelun valinta 2025 – AWS vs Azure vs Google Cloud. Tieturi blogi. Luettavissa: https://www.tieturi.fi/blogi/pilvipalvelun-valinta-2025-aws-vs-azure-vs-google-cloud/. Luettu: 30.3.2025.

Tieturi. 17.6.2024. Tietoturvahyökkäysten minimoiminen AWS-ympäristöissä. Tieturi blogi. Luettavissa: https://www.tieturi.fi/blogi/tietoturvahyokkaysten-minimoiminen-aws-ymparistoissa/. Luettu: 29.3.2025.

Ulkoministeriö s.a. Katakri – tietoturvallisuuden auditointityökalu viranomaisille. Luettavissa: https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille. Luettu: 22.2.2025.

Valtioneuvosto. 2018. Julkisen hallinnon pilvipalvelulinjaukset. Valtiovarainministeriö. Helsinki. Luettavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/161294. Luettu: 27.2.2025.

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Art House. Helsinki. E-kirja. Luettu: 27.2.2025.