Infrastruktuuri-pilvipalveluiden tietoturvauhat ja niiden hallinta

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Kesäkuu 2026
Viivi Tirkkonen

TURUN YLIOPISTO
Tietotekniikan laitos

Viivi Tirkkonen: Infrastruktuuri-pilvipalveluiden tietoturvauhat ja niiden hallinta

LuK-tutkielma, 27 s.
Tietojenkäsittelytiede
Kesäkuu 2026

Pilvipalveluiden lisääntyneen käytön ja yleistymisen myötä ovat myös pilvipalveluiden tietoturvauhat lisääntyneet. Koska pilvipalvelut saavat jatkuvasti enemmän yksityistä dataa käyttöönsä, on niiden tietoturvan hallinnan merkitys koko ajan suurempi. Infrastruktuuri pilvipalveluna jaetaan verkon välityksellä useille asiakkaille ja siinä ilmenevät juuri pilvipalveluiden ominaisuuksille oleelliset tietoturvauhat. Näitä uhkia ja näiden uhkien hallintaan tarvittavia keinoja käydään tässä tutkimuksessa läpi. Tämä tutkielma on toteutettu kirjallisuuskatsauksena.
Tutkielman kohteena on Infrastruktuuri-pilvipalveluna palveluiden tietoturva. Tutkielmassa pyritään tuomaan esiin yleisimpiä ja aineiston perusteella eniten mainittuja uhkia sekä niiden hallintakeinoja. Tutkimuksen tulokset osoittavat, että infrastruktuuri-pilvipalveluiden uhat perustuvat fyysiseen infrastruktuuriin, verkkoon, virtualisointiin, identiteetin- ja pääsynhallintaan, sekä dataan. Tulosten perusteella tutkielmassa päätellään suurimpien uhka-alueiden olevan verkko, virtualisointi ja identiteetin- ja pääsynhallinta, joihin pilvipalveluiden tietoturvan jaettu vastuu, moniasiakasympäristö ja palveluiden jako verkon välityksellä vaikuttavat eniten. Uhkien hallinnassa tulokset jaetaan ennaltaehkäisyyn, uhkien havainnointiin ja vastatoimenpiteisiin sekä palautumiskeinoihin. Tulosten kautta todetaan oleellisimmaksi uhkien ennaltaehkäisy keinot ja tutkielmassa pohditaan uhkien ratkaisuksi ennaltaehkäisymallia, johon sisältyy uhkien havainnointi, suojaukset, vahva tunnistautuminen ja valtuutukset, sekä huolelliset asetukset ja päivitys.

Asiasanat: pilvipalvelu, inftrastruktuuri pilvipalveluna, IaaS, tietoturva, tietoturvauhka, uhkien hallinta

Sisällys

Kuvat

Taulukot

1 Johdanto

Pilvipalvelut ovat yleistyneet ja niitä hyödyntävät laajasti niin yksilöt kuin organisaatiotkin. 2000-luvun alun jälkeen organisaatioiden pilvipalveluiden käyttö on ollut suurimmillaan ja sen odotetaan vielä kasvavan [1]. Pilvipalveluiden käytön yleistyminen pohjautuu pääosin pilvipalveluiden ominaisuuksiin, jotka mahdollistavat näiden palveluiden kustannustehokkuuden, käyttönopeuden ja skaalautuvuuden [2].

Pilvipalvelut tarjoavat palveluja etäältä, internetin välityksellä, jolloin asiakkaan ei itse tarvitse huolehtia koko palvelun ylläpidosta. Näin asiakkaan on helppo valita haluamansa palvelu, oli tarve sitten erilliselle tallennustilalle tai kokonaiselle sovellukselle. Pilvipalveluiden joustavuuden takia niitä on helppo hyödyntää monissa eri tarkoituksissa.[3]

Pilvipalvelut saavat käyttöönsä paljon julkista sekä yksityistä tietoa. Erityisesti COVID-19 -pandemian jälkeen on ollut paljon puhetta siitä, kuinka paljon ihmiset luottavat tietojansa pilvipalveluille vaikka eivät ole tietoisia sen toiminnasta lainkaan. Monet työpaikat ovat myös siirtyneet hybridi malliin tai kokonaan etätyömahdollisuuksiin, joiden kautta pilvipalveluita käytetään entistäkin enemmän. [1], [2], [4]

Kun pilvipalveluiden käyttö on yleistynyt ja lisääntynyt huomattavasti, ovat myös niihin koskevat uhatkin. Pilvipalveluiden uhkien hallinnassa voidaan hyödyntää perinteisiä tietotekniikan keinoja, mutta ne eivät ole täysin riittäviä pilvipalveluiden erilaisen infrastruktuurin suojaamiseen. Pilvipalveluiden olemuksen takia niissä

esiintyy myös monia peruspalveluille epätyypillisiäkin tietoturvauhkia. Nämä palvelut toimivat julkisten verkkojen välityksellä, joka tekee niiden tietoturvan hallinnasta entistäkin vaikeampaa. Tietoturvauhat sekä yleisesti pilvipalveluiden tietoturvallisuus ovat suurimpia haasteita pilvipalveluille ja hidastuttavat näiden palveluiden kehitystä ja kasvua. [1], [2], [4], [5]

Koska pilvipalvelut saavat hallintaansa suuret määrät tietoa, on niiden tietoturvallisuus erityisen tärkeää. Sekä palveluntarjoajalla että käyttäjällä on vastuu tietoturvasta ja mahdollisiin tietoturvauhkiin täytyy varautua parhain mahdollisin keinoin ja pyrkiä ennakoimaan heikkouksia tiedonsiirrossa ja tietojen säilytyksessä. Näihin uhkiin varautuminen ja turvallisuuden lisääminen pilvessä onnistuu tehostamalla pilvipalveluiden eri osa-alueita, jotka ovat uhkille alttiita. Esimerkiksi Infrastruktuuri-pilvipalveluilla näitä osa-alueita ovat virtualisointi, verkkoyhteydet ja tallennustilan hallinta. [1], [2]

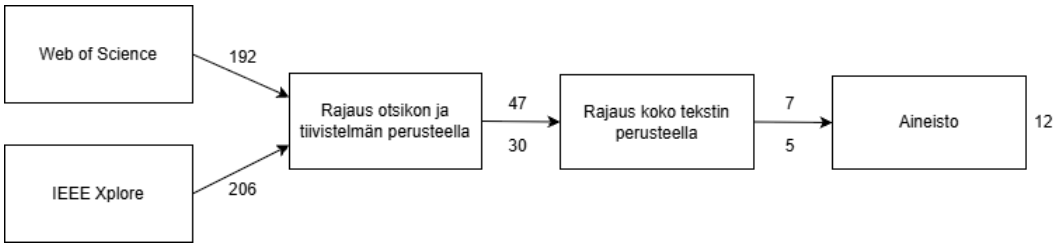
Tässä tutkielmassa keskitytään erityisesti infrastruktuuri palveluna (engl. infrastructure as a service, IaaS) – pilvipalveluihin. Tavoitteena on aineiston perusteella pyrkiä kartoittamaan IaaS-pilvipalveluita koskevia tietoturvauhkia sekä erityisesti näihin uhkiin liitettyjä mahdollisia hallinta- ja ennaltaehkäisykeinoja. Tutkimuskysymykset tälle tutkielmalle ovat seuraavat:

TK1: Mitkä ovat IaaS-pilvipalveluiden tietoturvauhkia?

TK2: Mitä tapoja on IaaS-pilvipalveluiden tietoturvauhkien ja tietoturvan hallintaan?

Tutkielman tiedonhaku toteutettiin kahdesta tietokannasta: Web of Science ja IEEE Xplore. Molemmissa tietokannoissa hakulausekkeena toimi *(cloud OR "cloud service*" OR "cloud computing") AND (IaaS OR "infrastructure as a service") AND security*. Tämän lisäksi hakutulokset rajattiin aikaisintaan vuoteen 2019, jotta artikkelit olisivat vielä mahdollisimman ajankohtaisia.

Näillä hakukriteereillä saatiin aluksi Web of Science -hakukannasta 192 artikkelia, jotka seuraavassa vaiheessa rajattiin otsikon ja tiivistelmän perusteella 47 artikkeliin. Näistä 47 artikkelista valittiin tekstin silmäilyn perusteella lopullisesti seitsemän artikkelia. Tekstin silmäilyssä kiinnitettiin huomiota siihen, kuinka hyvin artikkeli vastaa tutkimuskysymyksiin, sekä samassa vaiheessa poistettiin artikkelien duplikaatit. IEEE Xplore-hakukannassa tällä samalla haulla saatiin 206 artikkelia, jotka seuraavaksi otsikon ja tiivistelmän perusteella rajattiin 30 artikkeliin, ja myöhemmin tekstin silmäilyn jälkeen vielä viiteen artikkeliin. Tämä aineiston hakuprosessi on esitelty kaaviona kuvassa 1.1. Tutkielman aineistoon valittiin lopulta 12 artikkelia.



Kuva 1.1: Aineiston hakuprosessi

Tässä tutkielmassa käydään ensin läpi pilvipalveluiden perustoimintaa ja palvelu- sekä käyttöönottomalleja luvussa 2. Luvussa 3 keskitytään tietoturvaan pilvipalveluissa, miten sen vastuujako toimii asiakkaan ja palveluntarjoajan välillä, sekä kerrotaan pilvipalveluihin liittyvistä erilaisista tietoturvauhkista. Tulokset käydään läpi luvussa 4 ja tutkimuskysymyksiin vastataan. Tämän jälkeen luvussa 5 on pohdintaa tuloksista ja luvussa 6 yhteenveto tutkielmasta.

2 Pilvipalvelut ja niiden toiminta

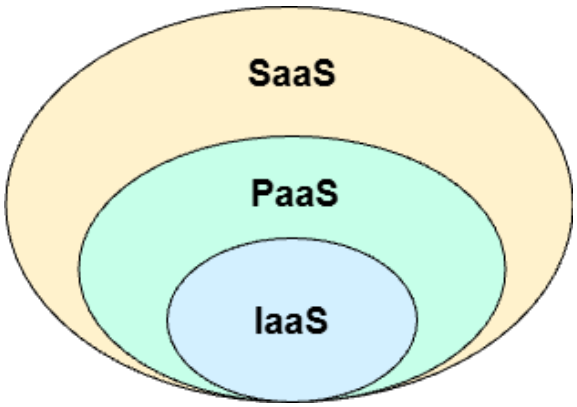
Tässä luvussa käydään läpi pilvipalveluiden toimintaa ja erilaisia malleja. Aluksi vertaillaan erilaisia pilvipalvelumalleja ja kerrotaan tarkemmin juuri IaaS-palvelumallista ja sen toiminnasta sekä käyttökohteista. Lisäksi virtualisointi avataan käsitteenä tarkemmin ja lopussa tarkastellaan vielä erilaisia pilvipalveluiden käyttöönottomalleja.

2.1 Pilvipalvelumallit

Pilvipalvelut voidaan jakaa kolmeen eri päämalliin, joita ovat *infrastruktuuri palveluna* IaaS, *alusta palveluna* (engl. platform as a service, PaaS) ja *sovellus palveluna* (engl. software as a service, SaaS) [6]. Nämä mallit kuvaavat pilvipalveluiden eri kerroksia (kuva 2.1). Kerroksilla tarkoitetaan palvelumallien syvyyttä ja asiakkaan vastuuosaa palvelun ylläpidosta. Päällimmäinen kerros on asiakkaalle vähiten vastuuta jättävä kerros, kun taas alin kerros antaa asiakkaalle eniten vastuuta. Alin kerros toimii resurssina, jota voi hyödyntää monin keinoin, kun taas päällimmäinen kerros on valmis sovellus, jota käytetään siihen tarkoitetuin keinoin.

Päällimmäisenä kerroksena on SaaS-kerros, joka sisältää valmiit vuokrattavat ohjelmistot, kuten Google-sovelluksen. Tämän alla oleva kerros on PaaS-kerros, joka tarjoaa asiakkaalle alustan omien sovellustensa kehitykseen. Esimerkiksi Microsoft Azure toimii PaaS-kerroksella. Alimpana kerroksena on IaaS-kerros, joka tarjoaa itse

infrastruktuurin ja toimii pohjana muillekin kerroksille, sillä sen päälle rakentuvat PaaS ja SaaS -kerrokset. [7]



Kuva 2.1: Pilvipalvelumallit kerroksina

Kun SaaS-palvelut tarjoavat valmiita sovelluksia ja PaaS-palvelut kehitysalustoja, IaaS-pilvipalvelut tarjoavat tallennustilaa, virtuaalipalvelimia ja verkkoja. Näitä palveluita jaetaan asiakkaille internetin välityksellä ja ne toimivat usein käyttöperusteisilla maksuilla, jotka mahdollistavat monien palveluiden samanaikaisen ja tehokkaan hyödyntämisen. [8]

IaaS-palvelut antavat myös käyttäjilleen eniten liikkumisvaraa ja omaa vastuuta verrattuna PaaS- ja SaaS-palvelumalleihin. SaaS palveluissa käyttäjien vastuulle jää vain itse sovelluksen käyttö sekä omien päätelaitteiden turvaaminen ja suojaaminen. Sovelluksen käyttöön liittyviä vastuita ovat myös oma tiedonhallinta, käyttöoikeuksien hallinta sekä identiteetin- ja pääsynhallinta-infrastruktuuri (IAM) käyttäjän päädystä. Palveluntarjoaja on vastuussa kaikesta muusta sovelluksen toiminnasta ja myös osin identiteetin- ja pääsynhallinta-infrastruktuurista. [3], [9]

PaaS-palveluissa käyttäjä saa enemmän hallintavastuuta sovelluksesta ja osasta väliohjelmistoa. PaaS-palveluissa palveluntarjoaja on muuten vastuussa koko alustan toiminnasta, mutta käyttäjälle jää alustan hallinnointi ja sen päälle rakentaminen omalle vastuulleen. SaaS-mallin vastuualueiden lisäksi PaaS-mallissa on käyttäjän vastuulla siis myös osa sovelluksesta ja verkosta. [3], [9]

2.2 IaaS-palvelumalli

IaaS-pilvipalvelumallin kerrosta voidaan myös kutsua virtualisointikerrokseksi, sillä tämän palvelumallin tarjoamat palvelut luodaan virtualisointi teknologioiden avulla. Näitä palveluita ovat erilaiset pilviresurssit ja tallennustilat. [10]

IaaS-palveluissa palveluntarjoajan vastuulla on infrastruktuurin, virtualisointialustan ja virtuaalikoneen pyörittäminen ja kunnostus. Käyttäjälle jää vastuu siitä mihin IaaS-palvelun resursseja käytetään ja miten. Käyttäjä on vastuussa sovelluksesta, väliohjelmistosta ja käyttöjärjestelmästä. IaaS-palvelumallissa vastuunjako on suoraviivaisempi kuin SaaS- ja PaaS-palvelumallissa. Jaettua vastuuosaa on muita malleja vähemmän. [3]

SaaS-palvelumallissa vastuu sovelluksesta jakaantuu molemmille, käyttäjälle sekä tarjoajalle. PaaS-palvelumallissa taas väliohjelmiston vastuu jakautuu käyttäjälle sekä tarjoajalle. IaaS-palvelun vastuunjako on selkeä, sillä usein tarjottuna palveluna toimii jo valmiiksi luotu yksittäinen resurssi, jota käyttäjä lainaa omiin tarkoituksiinsa. Vastuu tästä resurssin toimivuudesta on palveluntarjoajalla, ja vastuu resurssin käytöstä sekä muusta mihin resurssia käytetään on käyttäjän. [3], [11]

2.2.1 IaaS-palvelumallin käyttökohteet

IaaS-palveluilla voidaan tarjota monia virtuaalisen ympäristön resursseja, joita asiakas voi hyödyntää internetin kautta ohjelmistorajapintojen (APIen) avulla. Nämä ohjelmistorajapinnat mahdollistavat kommunikaation ja tiedonjaon eri pilviohjelmistojen ja infrastruktuurien välillä. Ne toimivat siis taustalla viestien ohjeistajina ja kuljettajina. [12] IaaS-palveluiden tarjoamia resursseja ovat esimerkiksi palvelimet, virtualisointi ja virtuaalikoneet, tallennustila, palomuurit, verkkolaitteet ja kuormantasaaja ohjelmistot. Etäpalveluiden lisäksi IaaS-palvelut voivat tarjota käyttöjärjestelmiä näiden pilvipalveluiden käytön helpottamiseksi. [6], [8]

2.2.2 Virtualisointi

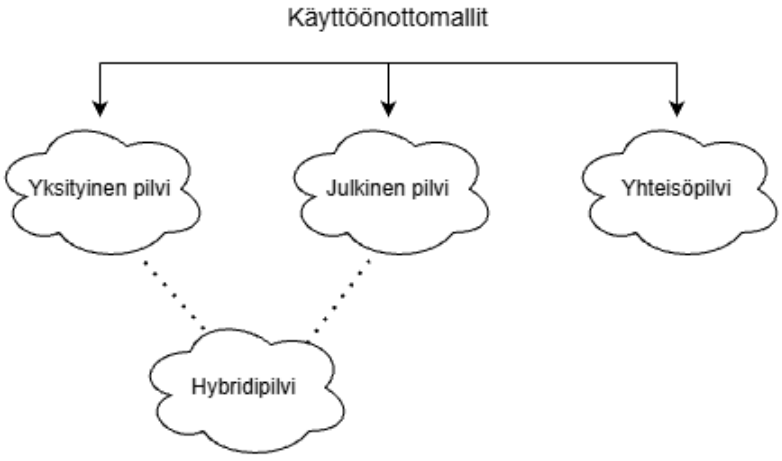
Virtualisointi on ydinosa pilvipalveluita ja se mahdollistaa pilvipalveluiden ja niiden eri resurssien irrallistamisen fyysisistä koneista. Virtualisointi tekniikan avulla fyysisten tietokonelaitteistojen käyttö voi olla tehokkaampaa, sillä yksi tietokonelaitteisto pystyy pyörittämään montaa systeemiä samanaikaisesti ja yksi systeemi pystyy myös toimimaan monella tietokonelaitteistolla samanaikaisesti. Virtualisointi tarjoaa infrastruktuuria, jonka avulla on mahdollista hyödyntää samaa tietokonelaitteistoa monen asiakkaan käyttöön. Tämä onnistuu tarkemmin virtuaalikoneiden avulla. [1], [5], [6]

Tekninen *virtuaaliympäristö* on tietokonejärjestelmä, joka on fyysisestä laitteesta irrallaan. Se ilmentää kaikkia pilvipalvelumalleja, mutta on oleellisin IaaS-palvelumallille, sillä sen palvelut toimivat suoraan virtualisointikerroksen päällä ja käytännössä kaikki pilviresurssit ovat virtualisoitavissa. Tässä virtuaaliympäristössä *host* (isäntäjärjestelmä/-kone) toimii hypervisor-ohjelmistoa suorittavana alustana. Tällä hypervisor-ohjelmistolla toimivat kaikki muut virtualisointiympäristön järjestelmät. [8], [13]

Hypervisor (HV)-ohjelmisto tai virtuaalikonemonitori (engl. Virtual Machine Monitor, *VMM*) on ohjelmistoalusta fyysisen laitteiston ja virtuaalikoneiden välillä. Se toimii virtualisointiympäristöjen eristäjänä. Näitä virtualisointiympäristöjä kutsutaan *Virtuaalikoneiksi* (engl, Virtual Machine, *VM*), jotka ovat tietokonesysteemiä esittäviä simulaatioita. Se tarkoittaa eristettyä osaa isäntäjärjestelmästä, joka luulee olevansa oma tietokoneensa. Virtuaalikone on siis malli isäntäkoneesta, joka toimii tiedostojen avulla ja esittää oikeaa tietokonetta. Näitä virtuaalikoneita voi isäntäkoneella olla monia. [8], [13]

2.3 Pilvien käyttöönottomallit

Pilvien käyttöönottomallit jakavat pilvipalvelut erilaisiin tyyppeihin resurssien pääsyoikeuksien perusteella [8]. Näitä käyttöönottomalleja ovat julkinen pilvi, yksityinen pilvi, hybridipilvi sekä yhteisöpilvi (kuva 2.2). Julkinen pilvi, yksityinen pilvi ja hybridipilvi ovat pää-käyttöönottomalleja. Hybridipilvi yhdistää joidenkin pilvien ominaisuuksia yhteen ja yhteisöpilvi on erillinen, muunneltu versio yksityisestä ja julkisesta pilvestä. [3]



Kuva 2.2: Pilvipalveluiden käyttöönottomallit, perustuu lähteen [14] kuvaan.

Julkinen pilvi tarkoittaa käyttöönottomallia, jota jaetaan verkon ja ohjelmointirajapintojen avulla kaikille asiakkaille samanaikaisesti. Tällöin pilvi on yleisesti ulkoisessa sijainnissa ja pilviympäristö voi olla monen tahon, esimerkiksi organisaatioiden ja yhtiöiden, omistuksessa ja kontrolloitavana. Tämä tekee julkisen pilven tietoturvasta heikomman muihin käyttöönottomalleihin nähden, varsinkin jos on epäselvyyksiä siitä kuka pilven resurssit omistaa ja missä ne sijaitsevat. Hyökkäyksiltä suojautuminen on tällöin hankalampaa. [5], [15] Näistä syistä julkinen pilvi onkin yleensä hakkereiden hyökkäyksien kohteena [16].

Yksityinen pilvi on yksityisessä käytössä vain yhdellä asiakkaalla, ja pilvi sijaitsee tämän asiakkaan omilla laitteilla, asiakkaan omien suojauksien takana. Vain

tällä asiakkaalla, esimerkiksi organisaatiolla, on pääsy tämän pilven tarjoamiin palveluihin. Yksityisessä pilvessä asiakkaalla on myös eniten hallintaa palvelusta, esimerkiksi tietoturvasta ja datasta [3]. [15]

Hybridipilvi yhdistää eri käyttöönottomalleja uudeksi kokonaisuudeksi. Hybridipilvi on yhdistelmä vähintään kahdesta pilvimallista [5]. Tämä mahdollistaa pilven sijainnin operoinnin siellä missä halutaan ja mikä on järkevintä, ulkoisessa sijainnissa tai omilla laitteilla. Hybridipilven tietoturvallisuus voi olla vahva, koska hybridipilvi pystyy yhdistämään muiden käyttöönottomallien hyvät puolet. Tietoturvallisuus on vahvana erityisesti yksityisiä resursseja käyttäessä, mutta hybridipilven tietoturva voi myös olla matala, jos resurssit ovat julkisia [3]. [15]

Yhteisöpilvi on ykstityisen ja julkisen pilven välimaasto. Tämä käyttöönottomalli on jaettu tietyn yhteisön kesken, esimerkiksi organisaatioiden, joilla on samat resurssitarpeet. Tällöin pilvi voi tarpeen mukaan olla sijainniltaan ulkoistettu tai omilla laitteilla. Yhteisöpilvi on julkista pilveä kalliimpi vaihtoehto, mutta antaa vahvempaa tietoturvaa siihen verrattuna. [3], [5], [15]

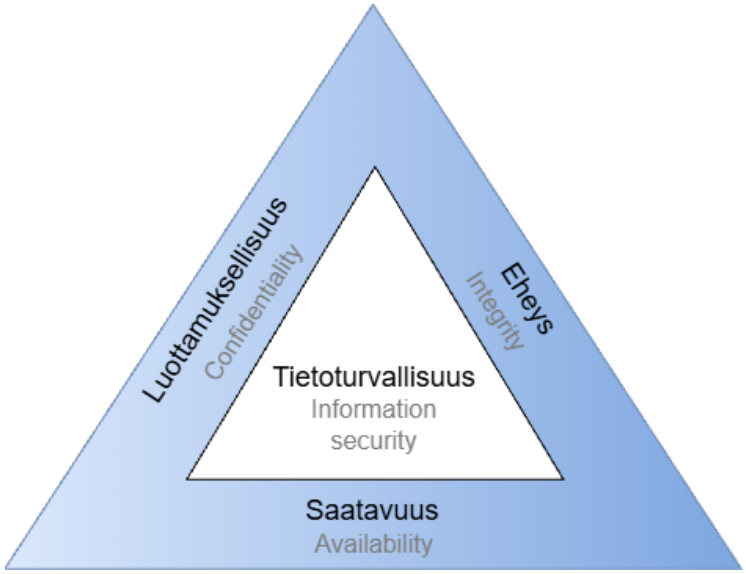
3 Tietoturva pilvipalveluissa

Tässä luvussa tarkastellaan pilvipalveluiden tietoturvan merkitystä, miten tietoturvaa on tässä tutkielmassa tarkasteltu ja vastuunjakoa erityisesti IaaS-pilvipalvelumallin kannalta. Lisäksi tuodaan esiin joitain IaaS-pilvipalveluja koskevia tietoturvauhkia ja avataan näitä käsitteitä sekä niiden toimintaa enemmän.

3.1 Tietoturvan merkitys pilvipalveluissa

Pilvipalveluiden tietoturvaa tarkastellaaan *CIA-kolmion* (kuva 3.1) avulla. CIA-kolmio sisältää kolme periaatetta: *luottamuksellisuus* (engl. Confidentiality), *eheys* (engl. Integrity) ja *saatavuus* (engl. Availability). Tiedon turvaaminen perustuu näihin kolmeen periaatteeseen, jotka yhdessä pitävät tietoympäristön turvallisena ja luotettavana, sekä luovat näin itse tietoturvallisuuden (engl. information security). Kun pilviympäristö saavuttaa luottamuksellisuuden, eheyden ja saatavuuden, on tämä ympäristö tietoturvallinen. [17]

Luottamuksellisuus tarkoittaa sitä, että käyttäjien tiedot pysyvät yksityisinä ja luvattomien pääsyn lukemaan, muokkaamaan tai poistamaan tietoja on estetty. Eheys viittaa itse tiedon luotettavuuteen, mikä tarkoittaa, ettei kukaan ulkopuolinen ole muokannut tietoa. Saatavuus on viimeinen osa ja se viittaa siihen, että asiakkailla on esteetön pääsy tietoihin ja palveluihin. Ilman saatavuutta asiakas ei pääse käsiksi resursseihinsa ja palvelun taso heikkenee. [1]



Kuva 3.1: CIA-kolmio

IaaS-palvelumalli on hakkereille mieluinen pilvimalli ja sen väärinkäyttö on yksi suurimmista pilvipalveluiden tietoturvauhkista. Tämä on siksi, että IaaS-ympäristössä on helppo luoda käyttäjätili väärillä henkilötiedoilla ja toimia näin väärän henkilöllisyyden suojassa. [18] CIA-kolmion täydellinen turvaaminen IaaS-ympäristössä on siis vaativaa [19]. Jotta pilviympäristö on turvallinen, täytyy kaikki sen osa-alueet olla turvattuina. IaaS-pilviympäristöllä näitä oleellisimpia osa-alueita ovat virtualisointi, verkkoyhteydet ja tallennustilan hallinta. [2]

3.2 Tietoturvan vastuunjako asiakkaan ja palveluntarjoajan välillä IaaS-mallissa

IaaS-pilvipalveluissa palveluntarjoaja on vastuussa palvelun ja tarjoamiensa resurssien ylläpidosta ja toiminnasta. Nämä sisältävät tarjotun ohjelman ylläpitoon tarvittavien tallennustilojen ja tietokoneiden hallinnan ja ylläpidon. Käyttäjä on vastuussa palvelulle rakentamansa tai palvelun avulla ylläpitämästään omasta ohjelmasta ja sen ylläpidosta. [11]

Koska IaaS-pilvipalvelu antaa käyttäjälle eniten valtaa verrattuna muihin pilvipalvelumalleihin, antaa se myös käyttäjälle eniten vastuuta tietoturvasta. On käyttäjän vastuulla huolehtia omien tietojensa hallinnasta ja niiden käytöstä, sekä omien päätelaitteiden suojauksista ja yksityisyysasetuksista. Käyttäjien käyttöoikeuksien hallinta sekä identiteetin- ja pääsynhallinta-infrastruktuuri ovat myös asiakkaan vastuualueina tietoturvan kannalta. Lisäksi sovellus, verkon hallinta ja käyttöjärjestelmän suojaukset ovat asiakkaan huolehdittavissa, jotta pilven tietoturvallisuus pysyy vahvana. Palveluntarjoajan vastuulla on vain pitää huolta isäntäkoneen, verkon ja datakeskuksen kyberturvallisuudesta ja tietojen yksityisyydestä niiden kautta. [9]

Turvallisuudenhallintaan on oikeudet siis yleensä käyttäjällä, mutta nämä vastuualueet käyttäjän ja palveluntarjoajan välillä voivat vaihdella käyttöönottomallista riippuen. Esimerkiksi IaaS-palvelun fyysinen ja virtualisointi turvallisuus voi olla täysin palveluntarjoajan vastuulla, ja IT systeemi, käyttöjärjestelmä, sovellukset ja data asiakkaan vastuulla. Vastuujako jakautuu tällöin hypervisorilla. Esimerkki tästä on Amazonin EC2 palvelu. [10]

3.3 Erilaiset tietoturvauhat IaaS-mallissa

Pilvipalveluiden tietoturvauhat voidaan jakaa ulkoisiin, sekä sisäisiin tietoturvahyökkäyksiin, käyttäjävirheisiin ja systeemivirheisiin. Ulkoiset tietoturvahyökkäykset ovat palveluiden ulkopuolelta suoritettavia tietoturvahyökkäyksiä, ja sisäiset tietoturvahyökkäykset ovat palvelun sisältäpäin, esimerkiksi asiakkaan toimesta, suoritettavia tietoturvahyökkäyksiä. Käyttäjävirheet viittaavat käyttäjien vastuulla olleisiin alueisiin ja niihin kohdistuneisiin virheisiin, kun taas systeemivirheet viittaavat palvelun suunnittelussa tai päivityksissä tulleisiin virheisiin, sekä järjestelmän bugeihin. Seuraavaksi mainitaan joitain hyökkäyksiä ja uhkatyyppejä.

Väärin konfiguroinnit viittaavat vahingollisiin että tahallisiin asetusten väärin konfigurointeihin. Ne ovat yksi suurimmista tietoturvahaasteista pilvipalveluille, sillä

ne mahdollistavat monia haavoittuvuuksia, joita hyökkääjät voivat hyödyntää. [3] **Sisäpiiriuhka** tarkoittaa uhkaa ja hyökkäystä palvelun sisältäpäin jonkin käyttäjän puolesta. Palvelun käyttäjä hyödyntää asemaansa palvelun asiakkaana päästäkseen muiden käyttäjien tietoihin. Käyttäjän on mahdollista päästä näihin tietoihin käsiksi esimerkiksi verkkoyhteyksien tai konfiguraatio muunnosten kautta. [20]

Porttiskannauksessa hyökkääjä onnistuu pääsemään kohdelaitteeseen ja tutkimaan palvelimen portteja, jolloin hyökkääjä voi saada tietoonsa kohdelaitteen haavoittuvuuksia. Porttiskannaus mahdollistaa esimerkiksi DoS-hyökkäykset. [3] **DoS-** (engl. Denial of Service) ja **DDoS-**(engl. Distributed Denial of Service) **hyökkäykset** ovat palvelunestohyökkäyksiä. Hyökkääjä esittää asiakasta ja lähettää monia pyyntöjä ja viestejä palvelimelle, jotta palvelin ylikuormittuisi. Tarkoituksena on saada palvelin kiireiseksi ja saatavuudeltaan estyneeksi muille käyttäjille. Tällaiset palvelunestohyökkäykset ovat lisääntyneet huomattavasti. [21]

Ero DoS- ja DDoS-hyökkäyksien välillä on ainoastaan siinä kuinka monta lähdettä tähän hyökkäykseen käytetään. DoS-hyökkäys toteutetaan yhdestä lähteestä, kun taas DDoS-hyökkäyksessä hyödynnetään monta lähdettä samanaikaisesti hyökkäyksen toteuttamiseen. Kun DDoS-hyökkäyksessä viestejä/ pyyntöjä lähetetään näiltä kaikilta koneilta samanaikaisesti, on se tehokkaampaa kuin vain yhdeltä koneelta hyökkääminen. Tämä voidaan toteuttaa esimerkiksi bottiverkkoa hyödyntämällä. [3], [21]

Väliintulohyökkäys (engl. Man in the Middle -attack) on kyberhyökkäys, jossa hyökkääjä pääsee kommunikaatiossa kahden osapuolen, kahden käyttäjän tai käyttäjän ja palvelun, väliin. Tästä hyökkääjä pystyy salakuunnella keskustelua ja saada yksityisiä tietoja. [3] **Sivukanavahyökkäys** tarkoittaa tietoturvahyökkäystä, jossa salaisia tietoja pyritään hankkimaan fyysisen toiminnan, kuten taajuuden, kautta [20]. **Virtuaalikoneiden sivukanavahyökkäys** on tilanne, jossa hyökkääjän ja uhrin VM jakaa samaa fyysistä laitteistoa ja hyökkääjän onnistuessa irroitta-

maan itsensä oman virtuaalikoneensa eristyksistä, pääsee hyökkääjä käsiksi fyysiseen tallennuslaitteistoon. Hyökkääjä pystyy fyysisten resurssien kautta tarkkailemaan uhrin toimintaa ja saamaan yksityisiä tietoja. [1], [20]

Hyper jacking tai **hypervisor-hyökkäys** on kyberhyökkäys, jonka kohteena on hypervisor. Hyökkääjä yrittää saada hallintaansa hypervisoria suoraan tai asettamalla toisen hypervisorin nykyisen alle. Kun hyökkääjä onnistuu, saa hän hallintaansa käyttöjärjestelmän ja koko pilven. [7] **Virtuaalikonepako** (engl. VM Escape) tarkoittaa virtuaalikoneen kautta suoritettavaa tietoturvahyökkäystä. Ohjelma, joka on yhdessä virtuaalikoneessa ajettavana, pääsee oman ajoympäristönsä ulkopuolelle, eli kyseisen virtuaalikoneen eristyksistä pois. Tällöin se voi päästä käsiksi palvelimen muihin virtuaalikoneisiin tai isäntäjärjestelmään. Hyökkäyksen onnistuessa hyökkääjä voi päästä hallitsemaan isäntäkonetta ja muita virtuaalikoneita, jolloin hyökkääjä pääsee myös muiden asiakkaiden yksityisiin tietoihin käsiksi. Virtuaalikonepako alkaa hyökkääjän koodista virtuaalikoneessa, jonka avulla hyökkääjä pääsee käsiksi hypervisoriin. Tällainen hyökkäys on yleensä mahdollista konfiguraatio tai hypervisor haavoittuvuuksien kautta, jotka mahdollistavat haittakoodien lähettämisen virtuaalikoneessa. [1], [13]

4 IaaS-palveluiden tietoturvauhkien kartoitusta ja niiden hallintakeinoja

Tässä luvussa siirrytään tutkielman tuloksiin ja avataan tutkimuskysymyksien vastauksia. Ensin käydään läpi erilaisia IaaS-pilvipalveluiden tietoturvauhkia ja niihin liittyviä alueita. Sitten tarkastellaan tietoturvan hallintaa ja luetellaan joitain erityisesti IaaS-pilvipalveluille oleellisia tietoturvan hallintakeinoja.

4.1 Tunnistettuja uhkia

Aineistossa käydään läpi IaaS-pilvipalveluihin keskittyviä uhkia, jotka voidaan jakaa viiteen kategoriaan. Nämä kategoriat ja aineisto on esitetty taulukossa 4.1. Taulukossa tämä jako on seuraava: Fyysinen infrastruktuuri, verkko, virtualisointi, identiteetin- ja pääsynhallinta (IAM), sekä Data. Nämä kategoriat jakavat uhat eri alueisiin, jotka viittaavat niiden kautta toteutettuihin tai niihin alueisiin kohdistettuihin uhkiin. Lisäksi taulukossa näkyy mitkä artikkelit käyvät läpi uhkien välttämis- ja hallintatapoja.

Nämä viisi kategoriaa, joilla uhat on pyritty erottelemaan toisistaan, eivät täysin poissulje toisiaan. Monissa artikkeleissa tuodaan esiin uhkia, jotka voidaan lajitella kahteen tai useampaankin taulukon 4.1 kategoriaan. Tämä uhkien jako on kuitenkin selkein tapa jakaa uhat omiin osa-alueisiin ja nähdä mihin osiin IaaS-palvelumallia liittyy eniten uhkia.

Taulukko 4.1: Aineisto luokiteltuna uhkien alueiden perusteella

Aineisto	Fyysinen infrastruktuuri	Verkko	Virtualisointi	Identiteetin- ja pääsyn-hallinta (IAM)	Data	Välttämis- ja hallinta-tavat
Abdullayeva (2023) [10]	x	x	x	x	x	x
Abu-Alhaija et al. (2022) [20]		x	x	x	x	x
Aburukba et al. (2022) [1]	x	x	x	x		x
Almadhoor et al. (2021) [6]						x
Charu et al. (2024) [2]		x		x	x	x
Chatterjee et al. (2020) [18]						x
Chaudhari et al. (2023) [15]		x	x	x	x	x
Jangjou & Sohrabi (2022) [3]		x	x	x	x	x
Mikail & Pranggono (2019) [5]		x	x	x	x	x
Mokgetse & Sridaran (2019) [7]			x		x	
Parast et al. (2022) [8]	x		x			x
Sahu & Nene (2021) [19]	x	x	x	x	x	x

Konfiguraatio ja hallinta ei ole yksi kategorioista, vaikka se onkin oleellinen uhka-alue IaaS-palveluille. Se viittaa palveluiden konfigurointiin ja asetuksiin liittyviin uhkiin. Lähes kaikki artikkelit toivat esiin konfigurointiin liittyviä heikkouksia, jotka muodostuvat uhkiksi, sillä palvelut voivat niiden kautta olla alttiita tahallisille hyökkäyksille ja virheellisille ongelmille kuten tietovuodoille. Tämä ei kuitenkaan ole oma kategoriansa aineistotaulukossa, sillä konfiguraatio ja hallinta yleensä liittyvät myös kaikkiin muihin kategorioihin.

Fyysinen infrastruktuuri tarkoittaa fyysiseen laitteistoon liittyviä uhkia. Fyysinen laitteisto ja koneet ovat IaaS-palvelussa palveluntarjoajan ylläpitämiä, mutta niihin koskevat uhat ja haitat vaikuttavat suoraan myös itse palvelun toimintaan ja tietoturvaan. Jos pilvipalvelu-infrastruktuuria katsotaan kerroksina ja SaaS- sekä PaaS-kerrokset ovat IaaS-kerroksen päällä, on laitteistokerros IaaS-kerroksen alla. Tämä laitteistokerros on pilvipalveluiden fyysinen infrastruktuuri. [1], [10], [19]

Fyysiseen infrastruktuuriin kuuluu fyysiset järjestelmät ja palvelimet, virtalähteet, kytkimet, jäähdytysjärjestelmät, fyysiset verkkolaitteet ja muistit/tallennusti-

lat, sekä reitittimet. Fyysisen infrastruktuurin kautta IaaS-pilvipalveluille ovat uhkina pääosin laitteiston ja infrastruktuurin väärinkäyttö, laitteiston muokkaaminen, laitteistovarkaus ja -keskeytys, heikko infrastruktuurin hallinta ja hoito, sekä myös mahdolliset luonnonkatastrofit. [1], [10] Koska IaaS-palveluiden laitteistot ovat palveluntarjoajien vastuulla, ovat niihin liittyvät uhat 70% varmuudella sisäisten epäluotettavien toimijoiden aiheuttamia. [19]

Moniasiakkuus, eli palvelun kyky olla monen asiakkaan samanaikaisessa käytössä, luo myös paljon uhkia IaaS-palveluille. Samassa isäntälaitteessa toimivien on mahdollista päästä käsiksi salattuihin ja yksityisiin tietoihin tallennuslaitteiden kuten levyn, välimuistin ja muistin kautta. Tämä on mahdollista jos yksi VM pääsee irroittautumaan eristyksistään ja pääsemään käsiksi fyysisen laitteiston muistiin [1]. Virtuaalikoneiden sivukanavahyökkäys on esimerkki tästä. Normaali sivukanavahyökkäys on myös aina uhka fyysiselle laitteistolle [20]. Lisäksi tietovuodot fyysisen laitteiston kautta ovat uhkia. [8]

Verkko viittaa kaikkiin verkko- ja internet-yhteyksiin IaaS-palveluissa. Verkko on ydinosa näitä palveluita ja koska verkkoyhteyksien asema on niin merkittävä, lisää se myös itsessään verkkoon liittyviä uhkia [2]. Verkon välisiä yhteyksiä voidaan palveluilla jakaa eri tietokoneiden välisiin yhteyksiin sekä tietokoneen ja tallennuslaitteen välisiin yhteyksiin. Nämä yhteydet ovat vaarassa hyökkääjien väliinkäynniltä, jolloin tietoja voi päästä vääriin käsiin ja joutua väärennetyiksi. [1] Verkkoon liittyviä uhkia ovat esimerkiksi DDoS- ja DoS-hyökkäykset, väliintulo-hyökkäys, IP-osoitteen väärentäminen, verkkoyhteyksien häiriköinti, bottiverkot, verkkoliikenteen salakuuntelu ja porttiskannaus. [3], [5], [10]

Myös **virtualisointi** on suuri uhka-alue, sillä IaaS-malli perustuu siihen niin paljon. Nämä uhat viittaavat uhkiin millä tahansa virtualisoinnin osaalueella. Erityisesti virtualisoinnin tarjoama moniasiakkuus mahdollistaa uhkia virtualisoinnin kautta. Virtualisointiin liittyvät uhat keskittyvät hypervisoriin ja virtuaalikoneisiin,

sekä virtuaaliverkkoihin. Virtualisointia koskevat uhat ovat pääosin erilaisia tahallisia hyökkäyksiä ja näille hyökkäyksille altistavia seikkoja, jotka johtuvat virtualisoinnin konfiguroinneista ja toiminnasta [15]. [1]

Esimerkiksi virtuaalikoneen siirto ja palautus luovat uhkia palvelulle. Virtuaalikoneen siirto on mahdollista niin, ettei virtuaalikonetta sammuteta siirrossa, jolloin siirrossa olevan virtuaalikoneen ja kohdelaitteen väliin on hyökkääjällä mahdollisuus iskeä. Palautuksessa taas on kyse siitä, että virtuaalikone pystytään palauttamaan aikaisempaan tilaansa, jolloin aikaisemmin infektoitunut virtuaalikone voidaan palauttaa aikaisempaan tilaansa infektioiden kanssa. [3], [15] Yleisiä virtualisointia koskevia uhkia ja hyökkäyksiä ovat myös esimerkiksi hypervisor-hyökkäykset, virtuaalikonepako, sisäpiiriuhat, VM sivukanavahyökkäykset, DoS-hyökkäykset ja VM Hopping, jossa hyökkääjä onnistuu hyppäämään omalta virtuaalikoneeltaan toiselle. [1], [10], [15], [20]

Identiteetin- ja pääsynhallinnan, eli **IAM** (eng. Identity and Access Management) uhat liityvät autentikointiin ja valtuutuksiin, eli siihen kenellä on lupa päästä palveluun ja mitä hänellä on lupa palvelussa tehdä. Identiteetin- ja pääsynhallintaan liittyvät uhat viittaavat usein salasanojen väärinkäyttöön ja väärennettyihin henkilötietoihin. [2], [5] Esimerkiksi pilvitallennustilan kartoitushyökkäyksessä hyökkääjä arvaa verkkotunnuksen kaavan avulla koko tunnuksen, tai jopa kansioiden nimiä, vain luettelemalla eri vaihtoehtoja kaavan täytteeksi [7].

Identiteetin- ja pääsynhallintaan liittyvien uhkien seurauksena datan yksityisyys ja eheys voivat kärsiä, sillä dataan pääsevät käsiksi väärät henkilöt [2]. Näitä uhkia ovat myös kaiken tyyliset autentikoinnin ohitukset ja verkkoliikenteen seuranta sekä väärennökset. [3] Verkkoliikenteen väärennöksillä on mahdollista vaihtaa kuljetuksessa olevien datapakettien osoitteita ja seurannalla saada yksityisiä ja salaisia tietoja. [5]

Pilvipalveluiden saaman data- ja asiakasmäärän takia autentikointi on erityisen tärkeää. Autentikoinnin ja valtuutusten puutteellisuuksien vuoksi ulkopuoliset voivat saada yksityisiä tietoja. Käyttäjien pääsynhallinta tasojen erot lisäävät uhkia, erityisesti jos pahantahtoiset käyttäjät valtuutetaan laajempiin pääsyihin. Identiteetinhallinta pitää tiedot turvassa ja ilman sitä voi tapahtua esimerkiksi tietovuotoja. [15] Identiteetin- ja pääsynhallintaan liittyvät uhat voivat ulottua niin fyysisen infrastruktuurin ja verkon kuin virtualisoinninkin uhkiin.

Viimeisenä uhkaluokituksena on **dataan** liittyvät uhat, jotka viittaavat uhkiin, joiden kohteena on erityisesti data. Data voi olla kuljetuksessa tai säilössä. Useimmiten nämä uhat liittyvät tallennustiloihin tai kuljetettavaan dataan käsiksi pääsemiseen, datan muokkaamiseen, tai muuten datan hyväksikäyttöön. Yleisiä dataan liittyviä uhkia ovat käyttäjän datan säilöminen epäluotettavassa pilvitallennustilassa, data liikenteen nuuskinta, datan luvaton muokkaaminen ja dataan luvaton pääsy. [3]

4.2 Uhkien välttäminen ja tietoturvan hallinta

Aineistossa käsitellyt uhkien hallintakeinot voidaan jakaa uhkien ennaltaehkäisyyn, havainnointiin ja vastatoimenpiteisiin sekä palautumiskeinoihin. Ennaltaehkäisy tarkoittaa kaikkia uhkia ennaltaehkäiseviä ja välttäviä toimenpiteitä. Havainnointi viittaa keinoihin, joilla uhkia ja mahdollisia hyökkäyksiä pyritään seuraamaan ja tunnistamaan. Vastatoimenpiteet ovat keinoja, joiden avulla pyritään joko hidastuttamaan, rajaamaan tai pysäyttämään jo käynnissä olevaa hyökkäystä tai tietovuotoa, ja palautumiskeinoja voidaan hyödyntää näistä ennalleen palaamiseen. Näiden luokittelujen perusteella aineiston uhkien hallinta- ja ratkaisukeinot on esitetty taulukossa 4.2.

Artikkeli [7] on ainoa aineistossa, joka ei ole mukana taulukossa 4.2, sillä siinä ei käydä hallinta- tai välttämiskeinoja ollenkaan, vaan keskitytään ainoastaan uhkien tutkimiseen. Ennaltaehkäisykeinoja tuodaan aineistossa eniten esiin. Ainoat artik-

kelit, jotka eivät näitä tarkemmin käy läpi ovat [10] ja [6], sillä ne keskittyvät vain uhkien havainnointikeinoihin. Vastatoimenpiteitä ja uhkien havainnointikeinoja käydään hieman vähemmän läpi. Ennaltaehkäisyillä pyritään välttämään tarvetta suorille vastatoimenpiteille ja havainnointi on oma osansa ennaltaehkäisyä. Havainnointi on oleellista niin vastatoimenpiteiden kuin ennaltaehkäisynkin toteuttamiseen, jotta voidaan tietää millaista uhkaa yritetään hallita ja välttää.

Taulukko 4.2: Aineisto luokiteltuna uhkien hallintakeinojen perusteella

Aineisto	Ennaltaehkäisy	Uhkien havainnointi	Vastatoimenpiteet ja palautuminen
Abdullayeva (2023) [10]		x	
Abu-Alhaija et al. (2022) [20]	x		x
Aburukba et al. (2022) [1]	x	x	
Almadhoor et al. (2021) [6]		x	
Charu et al. (2024) [2]	x		x
Chatterjee et al. (2020) [18]	x	x	x
Chaudhari et al. (2023) [15]	x	x	x
Jangjou & Sohrabi (2022) [3]	x	x	x
Mikail & Pranggono (2019) [5]	x	x	
Parast et al. (2022) [8]	x		x
Sahu & Nene (2021) [19]	x		x

Ennaltaehkäisy on oleellista uhkien hallitsemisessa, sillä sen avulla voidaan varautua erilaisiin uhkiin sekä tehdä hyökkääjälle mahdollisimman hankalaksi asemoida hyökkäystä. Ennaltaehkäisylle yleistä ovat vahvat datan salaukset ja erilaiset säännökset, joita noudattamalla ylläpidetään tiettyjä salauskäytänteitä. [18], [19] Näiden lisäksi on seuraavia ennaltaehkäisy keinoja: *Vahva tunnistautuminen ja valtuutukset*, jotka vaikeuttavat hyökkääjien mahdollisuuksia esiintyä nimettömänä ja päästä käsiksi vääriin tietoihin. [18] *Tarkat konfigurointi säännöt*, jotka pitävät järjestelmän konfiguroinnit ja asetukset hyvällä tasolla vähentäen haavoittuvuuksien hyväksikäyttöä. *Vankka avaintenhallinta*, joka ehkäisee hyökkääjien pääsyä palveli-

mille ja tietoihin. [19] *Datavuotojen estäminen*, eli kuljetuksessa olevan datan suojaaminen tekoälyä ja salaustekniikoita hyödyntäen. *Palomuurit ja ohjelmistopäivitykset*, jotka suojelevat hyökkääjiltä ja paikkaavat haavoittuvuuksia, estäen niiden hyödyntämisen hyökkäyksissä. Lisäksi vielä *uhkien havainnointi*. [18], [19]

Uhkien havainnointi on oleellista uhkien ennaltaehkäisyn kannalta ja on siis täydentävä osa ennaltaehkäisytapoja. Uhkien havainnointi mahdollistaa epäilyttävien toimintojen paikantamisen ja aikaisen reagoinnin. [18] Uhkien havainnointiin käytettäviä tekniikoita ja tapoja on seuraavia: *Poikkeamien tunnistus*, eli automatisoitu havaitsemistyökaluja hyödyntävä tekniikka epäilyttävien toimintojen tunnistamiseen järjestelmän käyttäytymisen avulla. [6], [18] *Allekirjoituspohjaiset tekniikat*, jotka ovat yleisten haittaohjelmien havaitsemiseen käytettyjä tekniikoita, jotka tunnistavat haittaohjelmia ”allekirjoitusten”, eli niiden ominaisten tavujonojen perusteella. [3], [6] *Verkkopohjainen tunkeutumisen havaitsemisjärjestelmä (NIDS)*, joka on poikkeamien tunnistusta sekä allekirjoituspohjaista analyysia hyödyntävä havainnointijärjestelmä. [15] Sekä *ennakoiva tietoverkkorikostutkinta*, eli säännöllisesti, mutta satunnaistetusti toteutettava virtuaalisten kiintolevyjen rikostekninen analyysi, joka tunnistaa epäilyttäviä tilejä. [18]

Vastatoimenpiteet ja palautuminen ovat hyödyllisiä silloin kun uhka ei ole enää uhka, vaan jo käynnissä oleva tai mennyt ongelmatilanne tai tietoturvahyökkäys. Tärkeää on tietää miten järjestelmää on käytetty väärin ja palauttaa tilat ennalleen. Joitain keinoja tähän ovat haitallisen liikenteen estäminen, Virtuaalikoneiden eristäminen, hyökkääjän paikantaminen ja havainnointiprosessin suorittaminen. Hyökkääjän paikannus ja virtuaalikoneiden eristäminen mahdollistaa hyökkääjän valtuutuksien poiston ja eristämisen muusta palvelusta. Uhkien havainnointi on siis myös oleellinen osa palautumista, esimerkiksi virtuaalisten kiintolevyjen rikosteknisellä analyysillä voidaan tunnistaa hyökkääjä ja havainnointikeinoilla tarkistaa onko uhkaa vielä muualla järjestelmässä. [8], [18]

5 Pohdinta

Tässä tutkimuksessa havaittiin, että IaaS-pilvipalveluiden tietoturvauhkia on monenlaisia, eikä suurimpaan osaan uhista ole täydellisiä ja yksinkertaisia ratkaisuja. IaaS-palveluiden tietoturvan hallinta perustuu pääosin uhkien ennaltaehkäisyyn ja niihin varautumiseen, kuten voimme tuloksista nähdä. Kun uhkatilanne on jo käynnissä, ei sen perumiseen ole keinoja, voidaan ainoastaan lieventää seuraamuksia ja koittaa palautua. Nämä tulokset ovat yhdenmukaisia muiden tutkimusten kanssa, kuten [6], [18].

Aineistoon valitut artikkelit käsittelivät tutkimuskysymyksiä laajasti, vähemmän syvällisesti. Uhkien hallintakeinoja tuotiin esiin, mutta vain [6], [18], [19] keskittyivät näihin uhkia tarkemmin. Muu aineisto käsitteli uhkia enemmän ja laajemmin. Aineistovalinta rajattiin pääosin ensimmäisen tutkimuskysymyksen perusteella ja koska aineisto sisälsi paljon samantyylistä uhkien luettelemista, tämä hankaloitti syvällisempää tutkielmatyötä. Aineistovalinnassa olisi voinut valita enemmän syvällisempiä tai erilaisia artikkeleita.

Monet artikkelit, kuten [8], [10], [15], [20], luettelivat monta erilaista uhkaa IaaS-palveluille ja pilvipalveluiden eri kerroksille, mutta koska uhkia käytiin läpi niin monta, ei niitä kaikkia pystynyt tässä tutkielmassa yksitellen mainitsemaan. Tämä saattaa vaikuttaa tutkielman kokonaiskuvaan. Aineiston rajaus tehtiin myös vuodesta 2019 alkaen, joten aikaisempaa tutkimusaineistoa aiheesta ei käyty läpi. Tä-

män lisäksi tutkielman aihe on nopeasti kehittyvä, joten pilvipalveluiden uhat ja hallintatavat voivat muuttua, jolloin tämän tutkimuksen tulokset voivat vanheta.

Eniten aineistossa käytiin läpi uhkia, jotka perustuvat tietoturvahyökkäyksiin ja näille hyökkäyksille altistaviin seikkoihin. Näiden lisäksi mainittiin myös uhkia käyttäjävirheisiin ja pilvipalvelun suunnittelua koskeviin virheisiin, joiden kautta tietojen luottamuksellisuus, eheys tai saatavuus voi vaurioitua. Aineiston näkökannat olivat pääosin hyökkäysmuotoiset uhat ja hyökkäyksiä mahdollistavat uhat, eli keskittyminen oli siis tietoturvahyökkäyksissä, joka saattoi vaikuttaa tähänkin työhön. Tärkeää on muistaa, että tutkimus toteutettiin laajana katsauksena IaaS-pilvipalveluista, eikä ole siis välttämättä suoraan verrannollinen kaikkiin yksittäisiin IaaS-palveluihin.

Kuten tässä tutkimuksessa todettiin, IaaS-pilvipalveluilla on paljon hyötyjä kuten joustavuutta ja kustannustehokkuutta. Näiden hyötyjen lisäksi myös tietoturvallisuuden merkitys on suurempi, koska palveluiden inftrastruktuuri sijaitsee eri osoitteessa ja tietoturvalla on jaettu vastuu. Tulkitsemalla tätä työtä voikin sanoa, että IaaS-pilvipalveluiden tietoturvauhat ja niiden hallinnan hankaluus keskittyvät nimenomaan pilven olomuotoon; verkkoyhteyksillä toimivaan palvelunjakoon, moniasiakasympäristöön ja tietoturvan jaettuun vastuuseen, jotka luovat helpommin erilaisia haavoittuvuuksia. Nämä, sekä se että nämä uhka-alueet ovat jatkuvassa kehityksessä, altistavat palvelut monille erilaisille uhille.

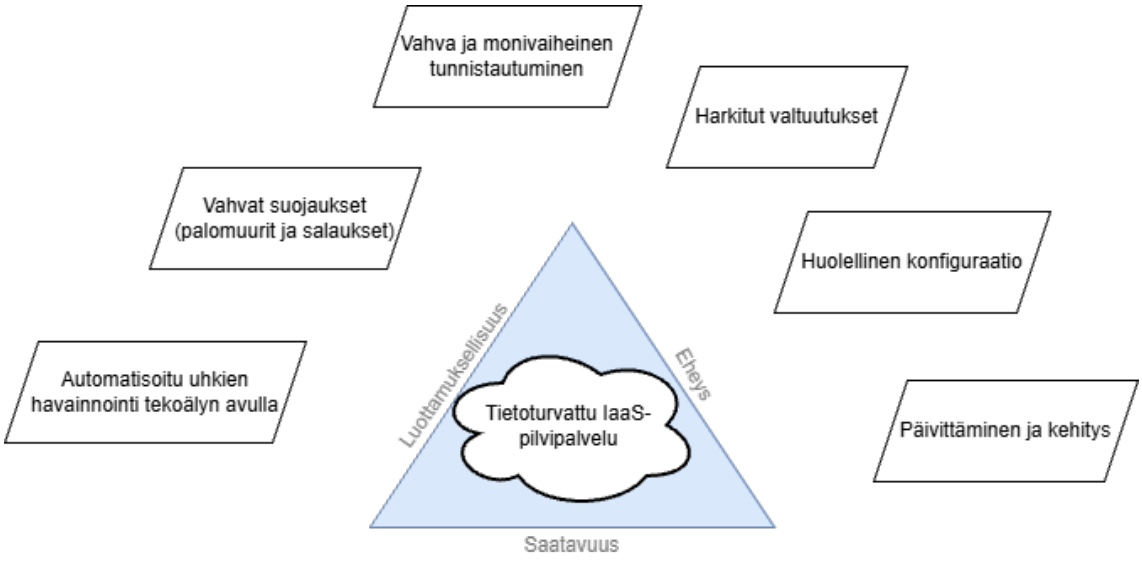
Tuloksissa mainittuja uhkia liittyy IaaS-palveluiden eri alueisiin ja osiin. Uhat eivät kuitenkaan täysin johdu itse pilvipalveluista, vaan suurinosa uhista mahdollistetaan konfigurointi virheillä ja heikolla ennaltaehkäisyllä. Nämä haavoittuvuudet johtuvat suurelta osin heikosta suunnittelusta ja uupuvista käytänteistä, kuten myös tulkitsee [19].

Vahvoilla tietoturvakäytänteillä voidaan pyrkiä maksimoimaan ja parantamaan IaaS-palveluiden tietoturvaa. Kuten tutkielma osoittaa, tietoturvan hallintaan ei ole

yksiselitteistä ratkaisua, vaan se on prosessi jota kehitetään koko ajan. Hyvä tietoturvan hallinta vaatii ainakin jatkuvaa uhkien valvontaa, ennaltaehkäisyä, automatisoituja tekniikoita näiden helpottamiseksi, vahvoja salauksia sekä tunnistautumista ja harkittuja valtuutuksia.

IaaS-pilvipalveluiden kehitys on nopeaa ja varsinkin tekoälyllä tulee luultavasti olemaan vielä suuri rooli siihen liittyvissä tietoturvauhissa ja niiden hallinnassa. Osa artikkeleista mainitsi koneoppimisen tietoturvauhkien havainnoinnissa, mutta tekoälyllä ei suurempaa roolia tässä aineistossa ollut. Uskon parin vuoden sisällä tämän muuttuvan paljon ja tekoälyn vaikuttavan sekä uhkatyyppeihin että niiden hallintakeinoihin huomattavammin. Tekoäly tulee oletettavasti olemaan johtava tekijä uhkien hallinnassa.

Lopuksi vielä pohdintaa siitä millainen täydellisesti turvattu IaaS-palvelu olisi ja mitä se vaatisi (kuva 5.1). CIA-kolmion periaatteet tulisi ainakin täyttyä: Luottamuksellisuus, eheys ja saatavuus.



Kuva 5.1: Tietoturvattu IaaS-pilvipalvelu

Tällainen malli sisältäisi jatkuvaa uhkien havainnointia eri automatisoitujen tekniikoiden ja tekoälyn avulla. Lisäksi Palvelun suunnittelun täytyisi olla huolellista ja

paljon käytänteitä tulisi ottaa käyttöön. Käytänteet sisältäisivät sääntöjä vahvoihin suojauksiin (esim. palomuurit ja salaukset), vahvaan tunnistautumiseen ja valtuutuksiin, huolelliseen konfiguraatioon, sekä jatkuvaan automatisoituun päivittämiseen ja kehittymiseen liittyen. Näiden täydellinen onnistuminen on erittäin hankalaa, jonka takia hyvien palautumiskeinojen ja uhkiin reagointikeinojen suunnittelu on myös tärkeää.

6 Yhteenveto

Pilvipalvelut ovat jatkuvassa kehityksessä ja sen myötä on myös niiden tietoturva. Tietoturvauhat ja niiden hallintakeinot kehittyvät koko ajan enemmän, uusien uhkien kehittyessä tarvitaan uusia hallintakeinoja, ja uusien hallintakeinojen myötä esiintyy uusia uhkia. Moniin tietoturvauhkiin on kehitetty monia erilaisia hallintakeinoja, mutta mikään näistä ei yksin ole täydellinen, vaan täytyy yhdistellä ja soveltaa eri hallintakeinoja. Pilvipalveuiden tietoturvan takaamiseksi on uhkien ajoittainen tutkiminen ja uusien hallintakeinojen kehittäminen tärkeää.

Tässä tutkielmassa käsiteltiin pilvipalveluiden tietoturvaa kirjallisuuskatsauksena. Keskityttiin erityisesti IaaS-pilvipalvelumalliin ja näihin palveluihin koskeviin tietoturvakysymyksiin. IaaS-pilvipalveluiden tietoturvauhkia ja tietoturvan hallintaa tutkittiin yleisellä tasolla, joitain esimerkkejä antaen. Tutkimuskysymyksiin vastattiin aineiston ja oman pohdinnan myötä.

Ensimmäiseen tutkimuskysymykseen vastattiin luvussa 4.1. Tutkimuksen tulokset osoittavat, että IaaS-pilvipalveluiden uhat kohdistuvat pääasiassa palveluiden moniasiakkuuteen, jaettuun vastuumalliin ja palveluiden tarjoamiseen verkon välityksellä. Verkkoon, virtualisointiin ja pääsynhallintaan liittyviä uhkia on tuotu esiin suurimmassa osassa aineistoa ja näiden alueiden uhat pyörivät noiden ominaisuuksien ympärillä. Nämä ominaisuudet ovat niitä, mitkä erottavat pilvipalvelut muista palveluista ja tekevät niistä erityisiä. Kuitenkin ne altistavat pilvipalvelut uusille ja jatkuvasti lisääntymässä oleville uhkatyypeille, joiden perässä voi olla vaikea pysyä.

Toinen tutkimuskysymys sai vastauksen luvussa 4.2. Tutkimustulosten perusteella uhkien hallintatavat keskittyvät enimmäkseen ennaltaehkäisyyn. Hallintatavat luokiteltiin ennaltaehkäisyyn, havainnointiin ja vastatoimenpiteisiin sekä palautumiskeinoihin. Kuten tulokset näyttävät, ennaltaehkäisyllä pyritään välttymään vastatoimenpiteiden ja palautuskeinojen tarpeelta, ja uhkien havainnointi voidaan luokitella erilliseksi osaksi ennaltaehkäisyä.

Tutkimuksessa huomattiin, että IaaS-pilvipalvelut tuovat paljon hyötyjä organisaatioille ja niiden tulevaisuus näyttää kirkkaalta. Niiden turvallinen käyttö vaatii kuitenkin vahvaa tietoturvan hallintaa ja tietoturvakäytänteitä sekä uhkien valvontaa. IaaS-pilvipalvelut tulevat kehittymään vielä paljon enemmän tulevaisuudessa, mutta niin tulevat myös muut tekniikat. Koska nämä ovat jatkuvassa kehityksessä, uusia tietoturvauhkia ilmenee ja muuttuu koko ajan näiden kehitysten myötä. Siksi on erityisen tärkeää, että tietoturvan hallintaa IaaS-palveluissa ylläpidetään jatkuvasti ja kehitetään aina mahdollisuuksien mukaan.

Jatkotutkimuksissa voidaan hyödyntää tässäkin tutkimuksessa saatuja tuloksia, mutta pilvipalveluiden jatkuvan kehityksen takia on näitä tuloksia käytettäessä oltava kriittinen ja huomioida myös muuttuvat tekniikat. IaaS-pilvipalveluiden uhat saattavat esimerkiksi tekoälyn avustuksella kehittyä hallintatapojen ympäri ja uusia uhkia voi ilmentyä eri alueille. Pilvipalveluiden uhkien hallintatapoja tutkiessa on muistettava palveluiden jaettu vastuumalli sekä kehittyvät tekniikat.

Lähdeluettelo

[1] R. Aburukba, Y. Kaddoura ja M. Hiba, "Cloud Computing Infrastructure Security: Challenges and Solutions", *2022 International Symposium on Networks, Computers and Communications, ISNCC 2022*, 2022. DOI: 10.1109/ISNCC55209.2022.9851812.

[2] Charu, S. Mathur ja A. S. Sengar, "Evaluating Current Cloud Security Challenges and IAAS Optimization", *Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2024*, s. 951–956, 2024. DOI: 10.1109/IC3I61595.2024.10828722.

[3] M. Jangjou ja M. K. Sohrabi, "A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing", *Archives of Computational Methods in Engineering*, vol. 29, s. 3587–3608, 6 lokakuu 2022, ISSN: 18861784. DOI: 10.1007/S11831-022-09708-9.

[4] P. Kopacz ja M. M. Chowdhury, "Cloud Computing Security and Future", *2022 IEEE World AI IoT Congress, AIIoT 2022*, s. 264–269, 2022. DOI: 10.1109/AIIOT54504.2022.9817186.

[5] A. Mikail ja B. Pranggono, "Securing infrastructure-as-a-service public clouds using security onion", *Applied System Innovation*, vol. 2, s. 1–17, 1 maaliskuu 2019, ISSN: 25715577. DOI: 10.3390/ASI2010006.

[6] L. Almadhoor, A. A. bd El-Aziz ja H. Hamdi, "Detecting Malware Infection on Infrastructure Hosted in IaaS Cloud using Cloud Visibility and Forensics",

International Journal of Advanced Computer Science and Applications, vol. 12, s. 919–934, 6 2021, ISSN: 21565570. DOI: 10.14569/IJACSA.2021.01206106.

[7] T. L. Mokgetse ja R. Sridaran, "A Comparative Study of underlying Threats of Cloud Deployment Service Models", s. 1218–1222, 2019.

[8] F. K. Parast, C. Sindhav, S. Nikam, H. I. Yekta, K. B. Kent ja S. Hakak, "Cloud computing security: A survey of service-based models", *Computers and Security*, vol. 114, maaliskuu 2022, ISSN: 01674048. DOI: 10.1016/J.COSE.2021.102580.

[9] M. Lane, A. Shrestha ja O. Ali, "Managing the risks of data security and privacy in the cloud: a shared responsibility between the cloud service provider and the client organisation", *Bright Internet Global Summit 2017*, 2017.

[10] F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems", *Results in Control and Optimization*, vol. 12, syyskuu 2023, ISSN: 26667207. DOI: 10.1016/J.RICO.2023.100268.

[11] P. Chavan, P. Patil, G. Kulkarni, R. Sutar ja S. Belsare, "IaaS cloud security", *Proceedings - 2013 International Conference on Machine Intelligence Research and Advancement, ICMIRA 2013*, s. 549–553, lokakuu 2014. DOI: 10.1109/ICMIRA.2013.115.

[12] F. Qazi, "Application Programming Interface (API) Security in Cloud Applications", *EAI Endorsed Transactions on Cloud Systems*, vol. 7, e1–e1, 23 lokakuu 2023, ISSN: 2410-6895. DOI: 10.4108/EETCS.V7I23.3011.

[13] H. Abusaimeh, "Virtual Machine Escape in Cloud Computing Services", *International Journal of Advanced Computer Science and Applications*, vol. 11, s. 327–331, 7 heinäkuu 2020, ISSN: 2156-5570. DOI: 10.14569/IJACSA.2020.0110743.

[14] S. Saraf. ”4 Cloud Deployment Models: Choose The Best Options”, viitattu 7. kesäkuuta 2026. url: https://absolute.co.in/cloud-deployment-models/.

[15] A. R. Chaudhari, B. N. Gohil ja U. P. Rao, ”A review on cloud security issues and solutions”, *Journal of Computer Security*, vol. 31, s. 365–391, 4 2023, ISSN: 0926227X. DOI: 10.3233/JCS-210140.

[16] M. Lata ja V. Kumar, ”Cyber security techniques in cloud environment: comparative analysis of public, private and hybrid cloud”, *EDPACS*, vol. 70, s. 1–21, 3 maaliskuu 2025, ISSN: 19361009. DOI: 10.1080/07366981.2025.2449743.

[17] S. Mohanty, M. Ganguly ja P. K. Pattnaik, ”CIA triad for achieving accountability in cloud computing environment”, *International Journal of Computer Science and Mobile Applications*, vol. 6, nro 3, s. 38–43, 2018.

[18] M. Chatterjee, P. Datta, F. Abri, A. S. Namin ja K. S. Jones, ”Abuse of the Cloud as an Attack Platform”, *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, s. 1091–1092, heinäkuu 2020. DOI: 10.1109/COMPSAC48688.2020.0-125.

[19] I. K. Sahu ja M. J. Nene, ”Model for IaaS Security Model: MISP Framework”, *2021 International Conference on Intelligent Technologies, CONIT 2021*, kesäkuu 2021. DOI: 10.1109/CONIT51480.2021.9498375.

[20] M. Abu-Alhaija, N. M. Turab ja A. R. Hamza, ”Extensive study of cloud computing technologies, threats and solutions prospective”, *Computer Systems Science and Engineering*, vol. 41, s. 225–240, 1 2022, ISSN: 02676192. DOI: 10.32604/CSSE.2022.019547.

[21] G. Somani, M. S. Gaur, D. Sanghi, M. Conti ja R. Buyya, ”DDoS attacks in cloud computing: Issues, taxonomy, and future directions”, *Computer Commu-*

nications, vol. 107, s. 30–48, heinäkuu 2017, ISSN: 0140-3664. DOI: 10.1016/J.COMCOM.2017.03.010.