Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Samuli Pesonen

Selvitys eri tallennusjärjestelmien sopivuudesta 3D-mittausaineistojen käsittelyyn ja tallentamiseen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

9.4.2019

Tekijä Otsikko Sivumäärä Aika	Samuli Pesonen Selvitys eri tallennusjärjestelmien sopivuudesta 3D-mittausaineistojen käsittelyyn ja tallentamiseen 41 sivua 9.4.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tietotekniikka
Ammatillinen pääaine	Tietotekniikan koulutusohjelma
Ohjaajat	Osaamisaluepäällikkö Janne Salonen

Käsiteltävän tiedon määrä on lisääntynyt nopeasti kaikkialla. Tästä johtuen tietokoneen ulkopuoliset tallennusjärjestelmät ovat nykyisin lähes välttämättömiä kaikissa organisaatioissa.

Tällä hetkellä useassakaan organisaatiossa ei ole käytössä riittävän suurta ja nopeaa tallennusjärjestelmää 3D-mittausaineistojen käsittelyyn ja arkistointiin. Suurikokoisia työtiedostoja tallennetaan muun muassa tietokoneiden paikallisille levyille ja ulkoisille kovalevyille, jotka eivät ole tarpeeksi hyviä isojen datamäärien arkistointiin. Projektien työtiedostot voivat olla kooltaan useita kymmeniä terabittejä.

Insinöörityön tarkoituksena oli selvittää näiden 3D-mittausaineistojen käsittelyyn ja arkistointiin parhaiten sopivien tallennusjärjestelmien vaihtoehtoja. Alussa tarkastellaan verkkolevypalvelimien ja pilvipalvelujen ominaisuuksia, niiden etuja, haittoja ja sopivuutta tallennusjärjestelmänä. Insinöörityön lopussa tarkastellaan tallennusjärjestelmävaihtoehtojen etuja ja haittoja. Tarkastelussa olennaisina kriteereinä olivat myös hinta ja tekniset ominaisuudet.

Osana selvitystyötä lähetettiin kahdellekymmenelle tallennusjärjestelmiä tarjoavalle yritykselle kyselyitä sähköpostitse liittyen erilaisiin tallennusjärjestelmiin. Tallennusjärjestelmistä kerättiin tietoa myös tallennusratkaisuja tarjoavien yritysten nettisivujen kautta. Selvityksen pohjalta verkkolevypalvelin tallennusjärjestelmänä olisi nykytarpeeseen sekä hinnaltaan että ominaisuuksiltaan parhaiten sopiva.

Avainsanat	tallennusjärjestelmä, verkkolevy, verkkolevypalvelin, pilvipalvelu, tietoturva

Author	Samuli Pesonen
Title	Report on the Suitability of the Different Storage Systems for Handling and Storing 3D Metering Data
Number of Pages	41 pages
Date	9 April 2019
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Information Technology
Instructors	Head of School (ICT) Janne Salonen

The amount of information to be processed has increased rapidly everywhere.
As a result, computers' external storage systems are now almost indispensable in all organizations.

At present, many organizations do not have a sufficiently large and fast storage system for processing and archiving 3D metering data. Large work files are currently stored on, inter alia, local disk drives and external hard drives, which are not good enough for archiving large amounts of data. Project work files can be several tens of terabytes in size.

The purpose of the thesis was to determine the options for the most suitable storage systems for handling and archiving these 3D measurement materials. First, the features of the webhost servers and cloud services, their advantages, disadvantages, and compatibility as a storage system were studied. Finally, the advantages and disadvantages of the storage system options were examined. Price and technical features also acted as relevant criteria for the examination.

As part of the survey, twenty storage companies were sent questionnaires via email regarding various storage systems. Information from the storage systems was also collected through the websites of companies providing storage solutions. On the basis of the survey, the network-attached storage would be the most suitable as the storage system for the current needs in terms of price and features.

Keywords	storage system, network disk, network disk server, cloud service, security

Sisällys

Lyhenteet

ATP	Advanced threat protection. Kehittyneitä haittaohjelmia tai hyökkäyksiä estävä tietoturvaratkaisu.
Botnet	Bottiverkko. Joukko tietokoneohjelmia (botteja), jotka kytkeytyvät toisiinsa tietoverkon välityksellä.
BPaaS	Business Prosess as a service. Liiketoimintaprosessi palveluna.
CaaS	Communication as a service. Viestintä palveluna.
CSA	Cloud Security Alliance. Yhdysvaltalainen organisaatio, joka pyrkii määrittelemään ja lisäämään tietoisuutta turvallisesta pilvipalveluympäristöstä.
DBaaS	Database as a Service. Tietokanta palveluna.
DoS	Denial of Service. Palvelunestohyökkäys, jolla pyritään estämään verkkosivuston käyttö.
DoS	Denial of Service. Palvelunestohyökkäys, jolla pyritään estämään verkkosivuston käyttö.
DDoS	Distributed Denial of Service. Hajautettu palvelunestohyökkäys, useista lähteistä tapahtuva palvelunestohyökkäys.
EaaS	Everything as a service. Organisaation koko IT hankitaan ulkopuolisesta palveluntuottajalta.
EGI-yhdistetty pilvi	EGI Federated Cloud. IaaS-tyyppinen pilvi, avoimien standardien ympärille akateemisista yksityisistä pilvistä ja virtualisoiduista resursseista rakennettu pilvi, jonka kehitystä ohjaavat tiedeyhteisön vaatimukset.
EOSC	Euroopan avoimen tieteen pilvipalvelu.
Ethernet	Pakettipohjainen lähiverkkoratkaisu.

FaaS	Function as a Service. Toiminto palveluna.
GDPR	General Data Protection Regulation. Euroopan unionin yleinen henkilötietoja koskeva tietosuoja-asetus.
CPU	Central Processing Unit eli CPU. Suoritin, tietokoneohjelman sisältämiä konekielisiä käskyjä suorittava tietokoneen osa.
Iaas	Infrastracture as a service. Infrastruktuuri palveluna.
IDC	International Data Corporation. Tietotekniikan ja liike-elämän tutkimus- ja konsultointipalveluja tarjoava yhdysvaltalainen yritys.
IP	Internet Protocol. TCP/IP-mallin Internet-tason protokolla, joka mahdollistaa internetiin kytkeytyneet laitteet kommunikoimaan keskenään.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.
ISO 9001	Johtamisen ja laadunhallinnan yleisstandardi.
ISO 27001	Tietoturvan hallintajärjestelmien standardi.
ISO 14001	Ympäristöasioiden hallinnan standardi.
LAN	Local Area Network. Lähiverkko, tietyllä maantieteellisellä alueella toimiva tietoliikenneverkko.
NAS	Network-attached storage tai network access storage eli verkkolevypalvelin on verkossa oleva tallennusjärjestelmä.
NIST	National Institute of Standards and Technology on yhdysvaltalainen kauppaministeriön alainen virasto, jonka tehtävänä on kehittää ja edistää mittaustekniikoita, standardeja ja tekniikkaa.

Paas	Platform as a service. Sovellusalusta palveluna.
RAID	Redundant Array of Independent Disks. Menetelmä, jolla tietokoneiden vikasietoisuutta ja nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä yhdistämällä ne yhdeksi loogiseksi levyksi.
Saas	Software as a Service. Sovellukset palveluna.
SAS	Serial Attached SCSI. Sarjamuotoinen SCSI-järjestelmä.
SCSI	Small Computer System Interface. Tietokoneen ja oheislaitteen välille tiedon välittämiseen kehitetty standardi.
SECaaS	Security as a service. Tietoturvaratkaisut palveluna.
Serverless	Käytön perustella maksettua palvelinkapasiteettia pilvipalvelussa.
SSH	Secure Shell. Salattuun etäyhteyden tietoliikenteeseen tarkoitettu protokolla.
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla, salattuun Internet-sovellusten tietoliikenteeseen tarkoitettu protokolla.

Storage as a service. Tallennustila palveluna.

TCP/IP	Transmission Control Protocol / Internet Protocol. Monen Internet-liikennöinnissä käytettävän tietoliikenneprotokollan yhdistelmä.
Tdos	Telephony Denial of Service. Puhelimiin kohdistuva palvelunestohyökkäys.
VPN	Virtual Private Network. Virtuaalinen yksityisverkko, useita verkkoja yhdistetään julkisen verkon yli.
XaaS	Anything as a Service. Organisaation koko IT hankitaan ulkopuolisesta palveluntuottajalta.

1 Johdanto

Käsiteltävän tiedon määrä on lisääntynyt nopeasti niin yrityksissä, tutkimuslaitoksissa kuin yliopistoissa. Tästä johtuen tietokoneen ulkopuoliset tallennusjärjestelmät ovat nykyisin lähes välttämättömiä kaikissa organisaatioissa. Tietokoneen omissa kovalevyissä ei yleensä kannattaisi säilyttää sellaisia tiedostoja, joita työstetään muilla koneilla, joiden käsittelyyn osallistuu muita organisaatioita tai joita siirretään eri yksiköiden välillä.

Ulkoisista tallennusjärjestelmistä voidaan käyttää esimerkiksi verkkolevyä, pilvipalvelua ja ulkoista kovalevyä. Sisäinen ja ulkoinen kovalevy monista hyvistä ominaisuuksista huolimatta ei täytä aina kaikkia nykyajan tallennustilalle asetettuja vaatimuksia. Vaikka ulkoisen kovalevyn kohdalla levyjä voi lisätä lähes rajattomasti, suurien levymäärien hallinnointi ja käsittely sekä niistä tiedon ja tiedostojen löytyminen voi muodostua haastavaksi. Tallennusmuotoina verkkolevypalvelin ja pilvipalvelu ovat usein parempia vaihtoehtoja, koska niihin tallennetut tiedot ovat samassa paikassa, helpommin käytettävissä ja siten monesti myös helpommin löydettävissä. Lisäksi tiedostojen siirtäminen ja yhteiskäyttö on niissä helppoa, eikä niiden käyttö ole aikaan ja paikkaan rajattua.

Insinöörityö tehdään Aalto-yliopiston Rakennetun ympäristön mittauksen ja mallinnuksen instituutille. Rakennetun ympäristön mittauksen ja mallinnuksen instituutti tuottaa kansainvälisen huipputason maanmittaustekniikan alan tutkimus- ja kehitystyötä rakennus- ja ympäristötekniikan aloille. Käytännössä työ pohjautuu 3D-mittauksen ja -mallinnuksen tutkimukseen ja tiedonhallintaan, jolloin työskentelyn ja tutkimuksen yhtenä tärkeänä osana ovat 3D-mittausaineistot. 3D-mittausaineistot sisältävät laserkeilauksella saatuja mittaustuloksia ja kuvia, valokuvista ja videoista leikattuja kuvia sekä pistepilviä ja eri ohjelmistojen projektitiedostoja. 3D-mittausaineistojen tallentamiseen ja käsittelyyn tarvitaan paljon tallennustilaa.

Tässä insinöörityössä on tarkoituksena selvittää näiden 3D-mittausaineistojen käsittelyyn ja arkistointiin parhaiten sopivien tallennusjärjestelmien vaihtoehtoja. Selvityksen pohjaksi tarkastellaan ensin yleisesti verkkolevyjen ja pilvipalvelujen ominaisuuksia, niiden etuja, haittoja ja sopivuutta tallennusjärjestelmänä. Selvityksen lopussa tarkastellaan tallennusjärjestelmävaihtoehtojen etuja ja haittoja instituutin kannalta.

2 Tutkimuksen tausta ja tavoitteet

2.1 Tutkimuksen taustaa

Tutkimuksen tarkoituksena on selvittää Aalto-yliopiston Rakennetun ympäristön mittauksen ja mallinnuksen instituutille erilaisia mahdollisuuksia tallennustilan kasvattamiseen ja eri tallennusmahdollisuuksien skaalautuvuuteen ja käytettävyyteen. Instituutin työ perustuu 3D-mittauksen ja -mallinnuksen tutkimukseen ja tiedonhallintaan. Käytännön työ on erityyppisten sensorien avulla sekä erilaisten tiedonkeruun ja analyysin menetelmin tehtävää kolmiulotteisten objektien, kaupunkien ja kohteiden mittausta ja mallinnusta, paikkatietoihin perustuvien palveluiden suunnittelua, verkostojen rakentamista, virtuaalimaailmojen luomista sekä tiedon, innovaatioiden ja patenttien tuottamista ja jakamista (Rakennetun ympäristön mittauksen ja mallinnuksen instituutti 2019).

3D-mittausaineistot koostuvat laserkeilauksella tehdyistä mittaustuloksista ja kuvista, etäisyyskameroilla ja stereoperiaatteella eri sijainneista otetuista valokuvista ja videoista leikatuista kuvista. Kuva- ja laserkeilausaineistot tallennetaan digitaalisessa muodossa ja mallinnetaan riippuen käyttötarkoituksesta erilaisilla 3D-ohjelmistoilla. 3D-mittaustekniikat tuottavat yksittäisten valittujen pisteiden sijaan nopeasti suuren joukon 3D-pisteitä ympäristöstä eli pistepilven. Pistepilvestä kohteet voidaan tunnistaa ja mallintaa, esimerkiksi rakennuksen seinät ikkunoineen ja ovineen, tien pinnan muoto ja katumaalaukset tai puun rungon muoto ja oksiston rakenne (Kaartinen et al. 2015). Ohjelmistojen projektitiedostot voivat koostua 3D-mittausaineiston käsittelyohjelmien erilaisista käsittelyä, mallinnusta ja tallennusta varten luoduista tiedostoista ja ohjelmistojen väliaikaistiedostoista (mm. temp-tiedostot), aineistoista tehtyjen projektien demoista ja keskeneräisistä ohjelmista. Helppokäyttöiset, nopeat ja turvasuojatut tallennusjärjestelmät ovat edellytyksenä tehokkaaseen ja häiriöttömään työskentelyyn.

Aalto-yliopistolla on tällä hetkellä tietojen tallentamiseen käytössä sekä verkkolevyjä että pilvipalveluja, jotka näkyvät taulukossa 1.

Taulukko 1. Aalto-yliopistossa tietojen tallentamiseen käytössä oleva vaihtoehdot (Data Storage, File Services | Aalto IT Help 2019).

Data Storage, File Services

Similar instructions

	home	work	teamwork	Teams	gDrive	OneDrive	Dropbox	IDA
quota	40 GB	~10 TB	100 TB / volume	-	-	5 TB	-	-
purpose	personal data, configuration files, student's data, confidential data	work data, project data, confidential data	project data, archive data, confidential data	public data	public data	public data	public data	object storage for archive data
eligibility	each Aalto user	each department and cost center	departments and cost centers by request	each Aalto user	each Aalto user	each Aalto user	each Aalto user (staff), apply	departments and cost centers
accessible from	Aalto network, VPN, general purpose servers	Aalto network, VPN, general purpose servers	custom within Aalto network, VPN, general purpose servers	internet	internet	internet	internet	limited custom
backup	Aalto default i.e. high data survivability	Aalto default i.e. high data survivability	custom	determined by service provider	determined by service provider	determined by service provider	determined by service provider	determined by service provider
service provider	Aalto	Aalto	Aalto	Microsoft	Google	Microsoft	Dropbox	CSC

Aalto-yliopistolla on käytössä useita pilvipalveluita. Google Drive -pilvipalvelu otettiin sekä henkilökunnan että opiskelijoiden käyttöön 2014. Dropboxin pilottivaihe aloitettiin alkuvuodesta 2018. OneDriven ja Teamsin sekä OneDriven for Businessin käyttö aloitettiin Office 365:n yhteydessä vuonna 2018. Käytössä on myös CSC:n maksuton IDA-tallennuspalvelu yliopiston tutkimusryhmille. Rakennetun ympäristön mittauksen ja mallinnuksen instituutilla, MeMolla, on tällä hetkellä käytössä AaltoIT:n tarjoamia verkkolevyjä ja ulkoisia kovalevyjä. Työasemissa on omat sisäiset datalevyt.

Tällä hetkellä ei Rakennetun ympäristön mittauksen ja mallinnuksen instituutin käytössä ole toiminnallisuudeltaan ja skaalattavuudeltaan riittävän suurta ja nopeaa tallennusjärjestelmää 3D-mittausaineistojen käsittelyyn ja arkistointiin. Suurikokoisiin työtiedostoihin

käytetään mm. tietokoneiden paikallisia levyjä ja ulkoisia kovalevyjä, jotka eivät ole tarpeeksi hyviä isojen datamäärien arkistointiin. Instituutilla jopa yksittäisenkin projektin työtiedostot voivat olla kooltaan useita kymmeniä terabittejä.

Edellä mainituista syistä on havaittu tarpeelliseksi tehdä selvitys sellaisesta tallennustilasta, jota usean käyttäjän on nopea käyttää sekä johon on mahdollista tallentaa suuriakin työtiedostoja. Uuden tallennusjärjestelmän kapasiteetin tulisi olla vähintään 100 terabittiä. Lisäksi on otettava huomioon, että tulevaisuudessa datan tallennus- ja siirtomäärät tulevat ilmeisesti kasvamaan.

2.2 Tutkimuksen tavoitteet ja tutkimusmenetelmä

Tutkimuksen tavoitteena on selvittää

- eri tallennusjärjestelmiä ja niiden ominaisuuksia
- minkälaisia tallennusjärjestelmiä tällä hetkellä on saatavilla
- tallennusjärjestelmävaihtoehtojen sopivuus Rakennetun ympäristön mittauksen ja mallinnuksen instituutille käytettävyys, tietoturva ja kustannustehokkuus huomioiden.

Tässä tutkimuksessa on tarkoitus selvittää erilaisia tallennusjärjestelmävaihtoehtoja. Selvityksestä tulee käydä ilmi, kuinka suurta datamäärää eri järjestelmät kykenevät käsittelemään ja minkälaiset tietoturvaominaisuudet järjestelmillä on. Tietoturvaratkaisujen tulee yleisestikin ottaen olla sellaisia, että data ei voi joutua ulkopuolisten käsiin. Selvityksen perusteella myös muut yksiköt voivat arvioida, millaista järjestelmää ne voisivat käyttää 3D-mittausaineistojen tallentamiseen, käsittelyyn ja arkistointiin. Selvitystä voidaan käyttää tukena hankintoja tehdessä.

Opinnäytetyö on rakenteeltaan kvalitatiivinen eli laadullinen tutkimus, jossa selvitetään eri tallennusjärjestelmävaihtoehtoja toimeksiantajan näkökulmasta edellä mainitut tavoitteet huomioiden.

Tutkimusmenetelmänä käytettiin sähköpostikyselyä. Selvitystyössä lähetettiin 20 tallennusjärjestelmiä tarjoavalle yritykselle sähköpostikysely erilaisista tallennusjärjestelmävaihtoehdoista. Kyselyyn vastasi yhteensä 11 yritystä asetettuun määräaikaan mennessä. Vastanneista yrityksistä seitsemän oli pilvipalveluihin erikoistunutta yritystä ja neljä, jotka tarjosivat verkkopalvelintallennuksen vaihtoehtoja. Osa sähköpostikyselyn saaneista eivät vastanneet kyselyyn sen vuoksi, että he tekevät ainoastaan sitovia tarjouksia loppuasiakkaille.

Tallennusjärjestelmistä kerättiin tietoa myös tallennusratkaisuja tarjoavien yritysten nettisivujen kautta.

3 Eri tallennusjärjestelmiä

3.1 Verkkolevypalvelin tallennusjärjestelmänä

Verkkolevypalvelin eli network-attached storage / network access storage (NAS) on tallentamiseen, säilyttämiseen ja jakamiseen tarkoitettu, lähiverkon tai internetin välityksellä käytettävissä oleva levytila, joka ei ole fyysisesti tietokoneessa. Verkkolevypalvelin voi sijaita organisaation omassa datakeskuksessa, yksiköissä tai ulkopuolisen palvelun-tuottajan konesaleissa sijaitsevassa varmistetussa levytilassa. Käyttäjän kannalta verkkolevyjen käyttö ei juurikaan eroa tietokoneen omista tallennusasemista. Verkkolevyä voivat käyttää useat käyttäjät samanaikaisesti riippumatta sijainnista organisaatiossa. Monen verkkolevyn kohdalla, verkkolevyn yhteydet internetiin voidaan avata ja sen tallennuskapasiteettia käyttää pilvipalvelun avulla.

Verkkolevypalvelimia käytettäessä tiedostoja voidaan kopioida oman tietokoneen ja verkkolevypalvelimen välillä tai niitä voidaan muokata suoraan verkkolevypalvelimella. Verkkolevypalveluita voi olla useita päällekkäisiä. Tällöin esimerkiksi TCP/IP-protokollaa käytettäessä kullakin palvelulla on oma IP-osoitteensa. Verkkolevyn hallinnoija voi lisätä käyttöoikeuksia oman organisaation työntekijöille eri käyttöoikeuksilla. Käyttöoikeuksia voidaan jakaa myös yhteistyökumppaneille, mikä mahdollistaa joustavan projektityös-

kentelyn tai tutkimusprojektien toteuttamisen eri yhteistyökumppanien kesken. Tietoliikenne voidaan salata SSH-tunneloinnin avulla, SSL-tekniikalla tai VPN-tekniikoilla. (Tietokehitys 2019.)

Verkkolevypalvelimiin voidaan käyttää normaaleja kiintolevyjä, mutta monesti verkkolevypalvelimissa käytetään sellaisia kiintolevyjä, joiden ominaisuudet esim. virheenkorjaavuuden suhteen ovat paremmat. Tällaisia kiintolevyjä kutsutaan verkkokiintolevyiksi, joiden tallennuskapasiteetit ovat tällä hetkellä suurimmillaan 14 TB ja jopa suuremmat.

Organisaatio voi hyödyntää verkkolevytallennusta myös sisäisen Intranet-palvelun kehittämisessä, mikä mahdollistaa sen käyttämisen useasta eri toimipisteestä tai etänä matkoilla tai kotitoimistossa. Tällöin verkkolevypalvelin muuttuu omaksi pilvipalveluksi verkon yli. Nykyisin verkkolevyjen käyttö on turvallista, koska sen kautta kulkeva tietoliikenne pystytään monen verkkolevyn kohdalla salaamaan mm. SSH-tunneloinnin, SSL-tekniikan ja/tai VPN-tekniikan avulla.

Verkkolevyt eivät ole käyttöjärjestelmäsidonnaisia eikä niiden käyttöönotto vaadi yleensä erikseen asennettavia sovelluksia, koska useissa käyttöjärjestelmissä ne ovat jo valmiina. Tosin joissakin uudemmissa käyttöjärjestelmissä tarvitaan asennettavia ohjelmistoja. Verkkolevyjä voi käyttää myös useilla mobiililaitteilla asentamalla niihin sovelluksia, jotka ovat monesti myös maksuttomia. (Tietokehitys 2019.)

Vertailtaessa verkkolevypalvelimen haittapuolia muihin tallennusjärjestelmiin yksi suurimmista haitoista on se, että verkkolevypalvelin on riippuvainen yhteydestä lähiverkkoon tai internetiin ja häiriö yhteydessä estää sen käytön.

Heikkoutena verkkolevytallennuksessa on lisäksi hyvinkin suuresta tallennuskapasiteetista huolimatta tallennustilan rajallisuus, vaikkakin verkkotallennustilaa voi useimmissa tapauksissa kasvattaa tiettyyn määrään lisäämällä uusia verkkolevyjä verkkotallennuspalvelimeen. Yhtenä heikkoutena on myös se, että verkkotallennukselle on rakennettava hyvä varmuuskopiointijärjestelmä, mikä ei tule itse verkkolevyn mukana kuten useissa pilvipalvelutallennusjärjestelmissä.

Verkkolevypalvelimen vaurioituminen tai tuhoutuminen on riski, mutta sitä voidaan vähentää hyvällä varmuuskopiointijärjestelmällä. Tietoturvan kannalta verkkolevypalvelimen joutuminen ulkopuolisten tahojen haltuun on nykyään pieni, koska useimmat organisaatiot ovat ymmärtäneet, että verkkolevypalvelinta kannattaa säilyttää turvallisessa organisaation omassa tilassa tai vuokratussa datakeskuksessa.

Hinta saattaa muodostua yhdeksi haittapuoleksi verkkolevytallennuksessa erityisesti, jos verkkolevypalvelinta käytetään joidenkin hyvin suurien datamäärien tallennukseen kuten suurien tilapäistiedostojen väliaikaisessa tallennuksessa. Koska käytettävän datan määrä tulee todennäköisesti lisääntymään nopeasti, pidemmällä tähtäimellä verkkolevytallennuksen hinta saattaa kasvaa hyvinkin suureksi verrattuna pilvipalvelutallennuksiin.

3.2 Pilvipalvelut

Tietojen tallentamisessa ja jakamisessa tapahtui 2000-luvulla teknologinen murros pilvipalveluiden (engl. cloud service) ja pilvilaskennan (engl. cloud computing) kehittyessä. (Srinivasan 2014.) Pilvipalveluissa on kyse kokonaisvaltaisesta muutoksesta kohti uudenlaisia toimintamalleja sekä nopeampaa ja kustannustehokkaampaa infrastruktuuria vapauttaen siten organisaatioiden pääomia ja henkilöstöresursseja arvoa tuottavien palveluiden kehittämiseen.

Vuonna 2011 yhdysvaltalainen, kauppaministeriön alainen National Institute of Standards and Technology (NIST) määritteli pilvipalvelun toimintamallina, joka mahdollistaa yleisen ja vapaan pääsyn konfiguroitaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan nopeasti ottaa käyttöön ja pois käytöstä (Mell & Grance 2011; Salo 2012).

Pilvipalvelu tarkoittaa yksinkertaisesti internetin kautta tapahtuvaa, joko ulkopuolisen palveluntarjoajan tai organisaation itsensä tuottamaa palvelua datan säilyttämiseen, prosessointiin ja käyttöön. Pilvilaskenta viittaa IT-palveluiden ja erityisesti datan muokkauksen ja käsittelyn hajautukseen ja ulkoistukseen. Se mahdollistaa IT-palveluiden skaalautuvuuden. Käyttäjät voivat hyödyntää tarpeidensa mukaan lähes rajatonta laskentatehoa ilman suuria investointeja ja he pääsevät dataan paikasta riippumatta internetin avulla. (Komissio 2012.)

Digitalisaation kasvattaessa datan määrää tallennustilan tarve kasvaa, jolloin pilvipalveluiden tallennus- ja laskentakapasiteetti soveltuu hyvin tällaisten datamäärien käsittelyyn ja säilyttämiseen. Palveluista veloitetaan yleensä todellisten käytettyjen resurssien mukaan. Perinteisesti organisaatiot ovat hankkineet tietotekniikkapalvelut itselleen ja hallinneet omia datakeskuksiaan. Tämä on tarkoittanut sitä, että organisaatiot ovat ostaneet tarvittavat laitteet ja sovellukset sekä palkanneet osaavan IT-asiantuntijaryhmän rakentamaan ja hallinnoimaan IT-palveluja, mikä on sitonut paljon pääomaa. Pilvipalvelujen käyttö voi monesti olla kustannustehokasta, sillä se mahdollistaa käyttäjälle tietotekiikkakustannusten vähentämisen ja uusien palvelujen kehittämisen, kun ei tarvitse investoida suuriin alku- ja käyttökustannuksiin.

3.2.1 Pilvipalvelumallit

Pilvipalvelut jaotellaan yleisimmin hierarkkisesti ominaisuuksiensa perusteella kolmeen ryhmään, jotka ovat SaaS (Software as a Service) ohjelmisto palveluna, PaaS (Platform as a Service) sovellusalusta palveluna ja IaaS (Infrastructure as a Service) infrastruktuuripalveluna. Näiden voidaan katsoa muodostavan kolmion (kuva 1), jonka pohjana on infrastruktuuri. Keskitason muodostavat sovellusalustat ja ylätasolla ovat ohjelmistot.

Kuva 1. Pilvipalvelumallien hierarkkisuus (Mukaellen Sheehan 2008 ja Haikumind 2011).

IaaS – Infrastruktuuri palveluna

IaaS-mallissa infrastruktuuri palveluna on pilvipalvelujen kivijalka. IaaS-mallissa infrastruktuurin kehittämisen ja hallinnan sijaan palvelunkäyttäjä ostaa palveluntuottajalta infrastruktuuriresursseja palveluna käyttöönsä, jolloin organisaation tietotekniikkainfrastruktuuri siirto-, tallennus- ja tiedonkäsittelypalveluineen sijaitsevat ulkopuolisessa virtuaalisessa datakeskuksessa. Palvelu antaa myös mahdollisuuden ottaa käyttöön lisää kapasiteettia tarpeen mukaan. Käyttäjä asentaa käyttöjärjestelmät ja ohjelmistot, hallinnoi palvelimia, verkkoyhteyksiä ja huolehtii palvelimien tietoturvasta ja palomuurauksesta. IaaS-palvelussa palveluntuottaja on vastuussa vain tuottamiensa resurssien toiminnasta ja tietoturvasta. IaaS-palvelussa palvelunkäyttäjällä on suurin toimintavapaus, mutta myös suurin vastuu verrattuna muihin pilvipalvelumalleihin. (Kavis 2014; Salo 2012.)

Organisaatiot voivat myös itse hallita ja käyttää infrastruktuuriresurssejaan IaaS-mallin mukaisesti, jolloin on kyseessä yksityinen pilvi (ks. s.10).

IaaS-palvelun etu tutkimuslaitoksen tai yrityksen kannalta on, ettei investoida kalliisiin tietokonesaleihin ja niiden ylläpitoon ja päivittämiseen vaan keskitytään varsinaisen tutkimuksen tai yritystoiminnan kehittämiseen. Tällöin maksetaan tallennus ja laskentakapasiteetin käytöstä. Etuna on myös resurssien joustavuus kulloisenkin tarpeen mukaan. Palvelunkäyttäjä ostaa laitteet ja resurssit palveluna palveluntuottajalta. (Salo 2012.) Palveluntuottaja vastaa infrastruktuurin toimivuudesta, turvallisuudesta ja saatavuudesta. Asiakkaalla on koko ajan käytössä ajantasainen uusi tekniikka. Tietokonesalien yhteiskäyttö on myös ympäristöystävällistä, kun jokaisen toimijan ei tarvitse investoida kalliiseen tietotekniikan infraan. Asiakkaalla säilyy myös hallinta omien sovellutusten kehittämiseen ja dataan.

Jotkut asiakkaat kokevat ongelmana sen, ettei heillä ole mahdollisuutta fyysisesti tai muutoin kontrolloida tietokonesalien toimintaa, vaan he joutuvat luottamaan palveluntuottajan antamiin turvallisuuslupauksiin mm. siitä, kuinka turvallinen datakeskus on hakkereiden tai fyysisen murtautumisen suhteen.

Mahdollisia toiminnan keskeytymistä tai häiriöitä aiheuttavia uhkia ovat luonnonmullistusten kuten tulvien tai myrskyjen aiheuttamat katkokset sähkönsaantiin tai konesalien tuhoutuminen esimerkiksi maanjäristysten seurauksena. Viime vuosina Suomi ja Ruotsi ovat saaneet useita suurten kansainvälisten pilvipalvelujen konesali-investointeja. Suomen etuna on toimiva infrastruktuuri ja viileä sää, jotka ovat merkityksellisiä suurten konesalien toiminnalle. Pohjoismaissa ei myöskään ole juurikaan tulvia tai maanjäristyksiä.

Suosituimmat IaaS-pilvipalvelujen tarjoajat vuonna 2019 olivat Amazon AWS, Microsoft Azure ja Google Cloud (ZDNET 2019). Muita kansainvälisiä IaaS-palveluja tarjoavia yrityksiä ovat mm. HP, IBM, Fujitsu sekä RackSpace, GoGrid ja CloudSigma. Suomalaisia IaaS-palvelujen tuottajia ovat mm. QX Enterprise Cloud, Elisan eCloud ja INcloud 9 -pilvipalvelu.

PaaS – Sovellusalusta palveluna

PaaS-mallissa palveluntuottaja tarjoaa käyttäjälle sovellusalustoja, esim. käyttöjärjestelmiä ja apuohjelmia sovelluksien kehittämiseen, testaamiseen ja käyttöön. Näin ei tarvitse huolehtia infrastruktuurista. Myös eri toimintoja on saatavilla moduuleina ja ohjelmointirajapintoina (Salo 2012), jolloin sovelluskehityksestä tulee yksinkertaisempaa ja skaalautuvampaa. Käyttäjä voi tuoda sovellusalustoille myös omia sovelluksiaan, mikä nopeuttaa ohjelmistokehitystä (Kavis 2014).

PaaS-palvelun etuja ovat nopeus, kustannustehokkuus ja monesti sovellusalustan tietoturva sekä lisäksi joustava kapasiteetin käyttö. Käyttäjän vastuulla on oman sovelluksen tietoturva ja päivitykset. Sen sijaan palveluntuottaja vastaa sovellusalustasta. PaaS-palveluja käyttämällä organisaation vastuu järjestelmien ylläpidosta vähenee, mikä säästää henkilöstökuluja. (Kavis 2014.) PaaS tarjoaa käyttäjälle/organisaatiolle mahdollisuuden kehittää omia sovellutuksia kustannustehokkaasti, nopeasti ja tietoturvallisesti (Salo 2012).

Ongelmana on olematon kontrolli toiminnan pohjana olevaan infrastruktuuriin ja paikoin alustalle ominaiset ratkaisut, joita on vaikea siirtää toiselle alustalle. Esimerkiksi alustalla saatetaan käyttää ohjelmointikieltä, joka on hyvin erilainen verrattuna muiden palveluntuottajien alustojen ohjelmointikieliin. Riskinä onkin juuttuminen yhden palveluntarjoajan

asiakkaaksi. Myös riippuvuus yhdestä alustan tarjoajasta on riski, jos palveluntarjoaja lopettaa toiminnan tai menee konkurssiin.

PaaS-palvelujen tuottajia ovat mm. Microsoft Azure, Google App Engine, Amazon AWS, IBM:n Red Hat OpenShift, SAP, Oracle, Salesforce, Bungee Connect, WorkXpress ja OrangeScape.

SaaS – Sovellukset palveluna

SaaS-mallille on eniten kysyntää ja myös palveluntuottajia. Saas on helppo tapa hankkia sovelluksia palveluna omien sovellusten hallinnoinnin sijaan. Palvelunkäyttäjän ei tarvitse huolehtia sovellusten ylläpidosta, päivityksistä, uusista versioista tai lisensseistä, vaan ne hoitaa palveluntuottaja. Saas-palveluiden etuna on, että organisaation ei tarvitse sitoa pääomaa ohjelmistoihin eikä tarvitse huolehtia niiden hallinnoinnista. Heikkouksina on, että Saas-sovelluksia ei voida monestikaan räätälöidä käyttäjän toiveiden mukaan, palveluntuottaja myös omistaa ne ja myös hallitsee niitä. Lisäksi Saas-sovellusten toiminta on täysin riippuvainen internetin toiminnasta. (Kavis 2014; Salo 2012.)

Jokaisessa keskisuuressa ja suuressa yrityksessä ja organisaatiossa on useita SaaS -tyyppisiä sovellutuksia käytössä. Näitä ovat esimerkiksi henkilöstöhallinnon ohjelmat, toiminnanohjausjärjestelmät (esim. ERP) sekä asiakkuuksien hallintaohjelmat (mm. CRM) ja taloushallinnon ohjelmat.

SaaS-palvelun käyttäjän kannalta on hyvä puoli se, että sovellutukset päivitetään joustavasti pilvessä ja ne ovat käyttäjälle aina ajan tasalla. Ylläpito ja päivitykset ovat palvelun tarjoajan vastuulla, jolloin asiakkaan ei tarvitse sitoa henkilöstöä näihin tehtäviin, vaan asiakas voi keskittyä oman toimintansa kehittämiseen. Myös palvelun tietoturva on palvelun tarjoajan vastuulla.

SaaS-palvelu on asiakkaan kannalta kustannustehokas. Asiakkaan ei tarvitse investoida sovellutuksen kehittämiseen, vaan hän maksaa sovellutuksen käytöstä. Ongelmana on usein sovellutuksen kytkeminen yrityksen tai organisaation toimintaan ja yhteensopivuus jo käytössä oleviin järjestelmiin. Myös henkilöstön koulutus ja motivointi uuden sovellu-

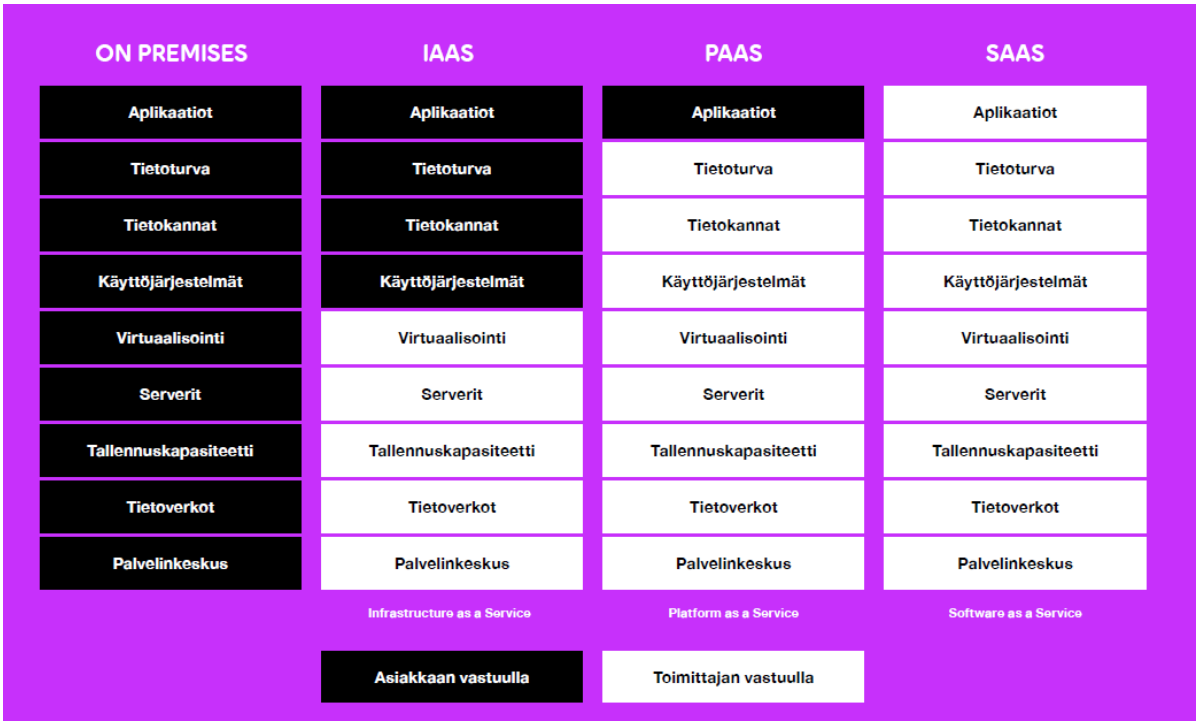
tuksen hyödyntämiseen on tärkeää, jotta sovellutuksesta saadaan sen tarjoama toiminnan tehostaminen ja hyöty esiin. Suurissakin yrityksissä on ollut ongelmia esim. toiminnan ohjausjärjestelmän käyttöönotossa (esim. Oriola).

SaaS-palvelun huonona puolena voidaan nähdä se, että palvelua käyttävä organisaatio käyttää samoja sovelluksia kuin kilpailija, mikä voi vaikeuttaa kilpailuetujen luomista (Ranger 2018). Lisäksi tietototurvallisuus on myös riski SaaS-palvelun käytössä.

Organisaatioiden tulee huomioida SaaS-palveluita käyttäessään se, että järjestelmästä saatava tiedon kerääminen ja analysointi on noussut monille SaaS-palvelun tarjoajalle ansaintalogiikan keskiöön. Viime vuosina on paljastunut esim. Facebookin keräämien tietojen myyminen ja hyödyntäminen kyseenalaisilla tavoilla. GDPR (Euroopan Unionin tietosuoja-asetus) asettaa onneksi palvelujen tarjoajille lisäpaineita yksityisyyden ja tietosuojan turvaamiseen. Viime aikoina tietosuojan turvaamiseen on kiinnitetty lisää huomiota. Yhtenä vaihtoehtona on tärkeiden salassa pidettävien tietojen pitäminen yrityksen tai organisaation omilla palvelimilla.

Kansainvälisiä SaaS-palveluja tuottavia yrityksiä ovat esimerkiksi Microsoft, Google, Salesforce, Oracle, IBM, SAP, Adobe, Amazon.com ja Cisco. Vuonna 2019 globaalisia SaaS-palveluiden markkinoita on hallinnut Salesforce (ZDNET 2019). Suomalaisia SaaS-palveluita tarjoavia yrityksiä on lukuisia.

Kuva 2 selventää IaaS-, PaaS- ja SaaS-palveluiden eroja ja vastuualueita suhteessa palveluntuottajiin ja käyttäjiin.



Kuva 2. Pilvipalvelumallien hierarkkisuus (Sheehan 2008 ja Haikumind 2011).

Palveluarkkitehtuurin jako näihin kolmeen edellä mainittuun palvelumalliin on yleisin, ja useimmat pilvipalvelujen tarjoajat käyttävät näitä markkinoinnissaan. Pilvipalvelujärjestelmä kehittyy kuitenkin nopeasti ja siihen on lisätty tekniikoita kuten Serverless (tarkoittaa käytön perustella maksettua palvelinkapasiteettia pilvipalvelussa). Miyachin mukaan (2018) IaaS-PaaS-SaaS-palvelumallien kehitysprosessin seuraus on Anything as a Service (XaaS), jolloin kaikki tietotekniikka hankitaan ulkopuolisesta palveluntuottajalta pilvipalveluna – voidaan kutsua myös Everything as a Service (EaaS). (Salo 2012.) Pilvipalvelujen tarjoajat pystyvät nykyisin tarjoamaan useita erilaisia tekniikoita pilvipalveluina, koska Internetyhteydet ovat tulleet luotettavimmiksi ja nopeammiksi, ja koska palvelimien virtualisoinnin ja Serverlessin kehittyminen tehostaa palvelualustojen ja näin ollen palveluiden nopeaa saatavuutta. XaaS mahdollistaa nopean reagoinnin markkinoiden muutoksiin. (Miyachi 2018.)

Muita palvelumalleja ovat mm. BPaaS (Business Prosess as a Service) -liiketoimintaprosessi palveluna, (Storage as a Service) -tallennustila palveluna, SECaaS (Security as a Service) -tietoturvaratkaisut palveluna, CaaS (Communication as a Service) -viestintä

palveluna, DBaaS (Database as a Service) -tietokanta palveluna ja FaaS (Function as a Service) -toiminto palveluna. (Salo 2012.)

NIST määrittelee IaaS-, PaaS-, SaaS-pilvipalvelumallit kolmelle eri tasolle (Salo 2012; Miyachi 2018). Nykypäivän IT-teknologioita ja kaupallisten tarjoajien valikoimia paremmin kuvaavan vuorovaikutteisen pilvipalvelumallin Miyachi (2018) päivitti Johan den Haanin (2013) mallin pohjalta (kuva 3). Siinä on otettu mukaan Serverless ja virtualisointi sekä verkkojen ja tallennuksen ohjelmistopohjainen ohjaus peruspalveluina.

6	SaaS		Applications		*End User*
5	App Services	Apps in the Cloud	Communications and Social Media Apps	Data as a Service	*Any User*
4	Built-up PaaS	Business as a Process	Social Media PaaS	Data Analytics	*Rapid Developers*
3.5		Serverless Computing			*Speed Developers*
3	PaaS				*Developers*
2	Foundational PaaS	Application Containers	Routing, Messaging, Orchestration	Object Storage	*DevOps*
1	Software Defined	Virtual Machines	Software Defined Networks (SDN)	Software Defined Storage	*Infrastructure Engineers*
0	Hardware	Servicers	Switches, Routers	Storage	
		Compute	***Communicate***	***Store***	

Kuva 3. Miyachin päivittämä pilvipalvelumalli pohjautuen Johan Den Haanin malliin (Miyachi 2018).

Miyachin malli kuvaa paremmin sitä, mitä tällä hetkellä IT-pilvessä tapahtuu. Silti NISTin määritelmään perustuvan IaaS-PaaS-SaaS mallin avulla on helpompi aloittaa pilvipalvelujen käyttö (Miyachi 2018).

3.2.2 Pilvipalveluiden tyypit

Pilvipalveluja voidaan ottaa käyttöön useilla tavoin. Käyttöönottotavat riippuvat siitä, onko palveluympäristö kokonaan organisaation omassa käytössä vai onko se jaettu eri palvelunkäyttäjien kanssa. NIST (National Institute of Standards and Technology) on

määritellyt käyttöönottotapojen perusteella pilvipalvelut yksityiseen pilveen (Private cloud), yhteisöpilveen (Community cloud), julkiseen pilveen (Public cloud) ja hybridipilveen (Hybrid cloud). (Mell & Grance 2011.)

Yksityinen pilvi

Yksityinen pilvi on nimensä mukaan yksityinen, yhden organisaation tai käyttäjäryhmän käyttöön rakennettu infrastruktuuri, joka muodostaa oman suljetun verkon. Yksityisessä pilvessä palvelut sovitetaan käyttäjäorganisaation mukaisesti ja palvelin-, verkko-, tallennus- ja muu laitteisto on vain organisaation käytössä. Organisaatio vastaa palvelujen ylläpidosta, päivityksistä ja hallinnoinnista sekä tietoturvan tasosta. Yksityinen pilvi mahdollistaa siten suuren kontrollin ja turvallisuustason. Kustannuksiltaan yksityinen pilvi on huomattavasti kalliimpi kuin julkinen pilvi. Yksityinen pilvi onkin sopiva silloin, kun käyttäjäorganisaatiolla on normaalia tiukemmat vaatimukset tietoturvan tasosta. Isot organisaatiot hyötyvät suhteessa kustannuksiin yksityisen pilven eduista. (Heino 2010; Salo 2011; Srinivasan 2014.)

Julkinen pilvi

Julkinen pilvi on useiden organisaatioiden käytössä samanaikaisesti julkisen verkon kautta. Palvelunkäyttäjä tarvitsee vain internetyhteyden ja päätelaitteen ja mahdollisesti liikenteen salaamista varten esimerkiksi VPN-laitteen. Ero julkisen pilven ja yksityisen pilven kohdalla on myös resurssien omistuksessa. Palveluntuottaja omistaa ja hallinnoi pilven infrastruktuuria ja sovelluksia datakeskuksessaan. Julkisen pilven palvelut ovat kaikkien ulottuvilla ja niitä voidaan ostaa tarpeen mukaan aika- ja paikkariippumattomasti. Palvelunkäyttäjä maksaa ainoastaan niistä palveluista, joita se käyttää. Julkinen pilvi on kustannustehokas erityisesti pienissä organisaatioissa. Julkinen pilvi onkin tunnetuin pilvipalvelutyypeistä. (Heino 2010; Salo 2011; Srinivasan 2014.)

Hybridipilvi

Hybridipilvi on pilviympäristö, jossa tietoliikenneyhteyksien välityksellä yhdistetään sekä julkinen pilvi että yksityinen pilvi ja mahdollisesti paikallinen ympäristö. Pilvipalvelujen

välinen erityinen verkostoituminen voi mahdollistaa tehokkaamman infrastruktuurin, kuten esimerkiksi organisaation kannalta tärkeät ja salassa pidettävät ohjelmistot ovat yksityisessä pilvessä tai omassa konesalissa ja toimintaa tukevat sovellukset saadaan julkisesta pilvestä. Hybridipilvellä voidaan saavuttaa yksityisen ja julkisen pilven edut sekä kustannustehokkuus. Tietojen ja sovellusten helppo käyttöönotto ja siirrettävyys ovat hybridipilven etuja käyttäjälle. Hybridipilven tarkoituksena on myös yhdistää yksityisen ja julkisen pilven etuja, kuten yksityisen pilven tietoturvaa ja julkisen skaalautuvuutta. (Salo 2011; Srinivasan 2014; Varghese & Buyya 2018.)

Yhteisöllinen pilvi

Yhteisöllinen pilvi on useiden eri organisaatioiden jakama infrastruktuuri, jossa yhdistyvät organisaatioiden kiinnostuksen kohteet, tavoitteet ja vaatimukset pilvipalvelulle. Sitä hallinnoi joko käyttäjäorganisaatiot yhdessä, pilvipalvelun tuottaja tai niiden yhdistelmä. Etuna yhteisöllisen pilven käytölle ovat julkiseen pilveen verrattuna parempi tietoturva sekä kustannussäästöt yksityiseen pilveen verrattuna, kun kustannukset jakautuvat kaikille käyttäjäorganisaation jäsenille. (Mell & Grance 2011; Varghese & Buyya 2018.)

Multipilvi

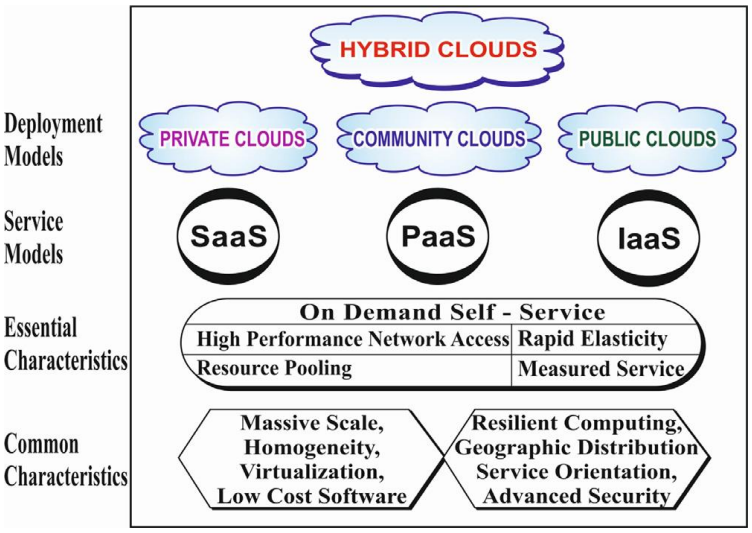
Usean pilven yhdistämisessä on kyse palveluntuottajien voimavarojen hyödyntämisestä. Monen palveluntuottajan mallit yleistyvät yritysten pilvi-infrassa (Pervilä 2017), mutta on myös esteitä. Esimerkiksi yhteisten sovellusliittymien, jotka on tehty helpottamaan multipilveä, on otettava huomioon palveluntuottajien erilaiset resurssit. Myös erilaiset sovellukset, hinnoittelu ja laskutusmallit vaikeuttavat multipilvien kehittämistä. (Varghese & Buyya 2018.) Multipilvet ovat kuitenkin tulossa, kuten IDC:n Euroopan pilvi-infran johtaja Giorgio Nebuloni sanoo:

> Erilaisten pilviympäristöjen yhdistely hybridien avulla ei enää riitä vuonna 2018 yhden suuren palvelutarjoajan käytöstä puhumattakaan. Varsinkin kaikkein innovatiivisimpien yritysten bisnesjohtajat sekä it-pomot ja sovelluskehittäjät tukeutuvat yhtä lailla monipilven eli monen toimittajan malliin.
>
> ”Näin vältetään yrityksen lukkiutuminen vain yhden palvelutarjoajan asiakkaaksi, mikä on tärkeää varsinkin teknologioiden ostoista vastaaville IT-osastoille", Nebuloni perustelee kantaansa. (Pervilä 2017).

Muita pilvipalvelutyyppejä ovat esimerkiksi yhdistetty pilvi (Federated Cloud), mikropilvet (Microcloud and cloudlet), Ad hoc -pilvi (Ad hoc cloud) ja heterogeeninen pilvi (Heterogeneous cloud). (Varghese & Buyya 2018.) Yhdistetyllä pilvellä on useita etuja, sillä pilvipalvelujen tuottajat ovat yhden sateenvarjon alla yhdistetyssä pilvessä. Esimerkkinä on EU:n EGI-yhdistetty pilvi, jossa yli 20 pilvipalvelujen tuottajaa ja 300 datakeskusta on yhdistetty.

Vaihtoehdoksi paljon sähköä kuluttaville suurille tietokeskuksille on kehitetty matalampien kustannusten vaihtoehtoja, edullisia, pienitehoisia mikropilviä lähemmäksi käyttäjiä. Mikropilvet voivat vähentää sovellusten viiveitä käyttäjälaitteiden ja datakeskusten välillä. (Varghese & Buyya 2018.)

Kuva 4 havainnollistaa pilvipalvelumallien ja pilvipalveluiden käyttöönottotapojen ominaispiirteitä.



Kuva 4. NIST:n määrittelemien pilvipalveluiden viitekehys (Subramanian & Jeyaraj 2018).

3.3 Verkkolevy- ja pilvipalvelujärjestelmien vertailua

Organisaation suunnitellessa tallennusjärjestelmäänsä tulee kiinnittää huomiota tallennusjärjestelmän niihin ominaisuuksiin, jotka ovat organisaation kannalta kriittisiä. Verkkolevytallennuksessa ja tallennuksessa pilvipalveluihin on erilaisia heikkouksia ja vahvuuksia, mutta osa toisen heikkouksista on toisen vahvuuksia.

Verkkolevyjen vahvuuksista puhuttaessa usein todetaan, että verkkolevytallennusjärjestelmät ovat organisaation itsensä hallinnassa ja siksi turvallisia sekä vian sattuessa helposti korjattavissa. Heikkouksia sen sijaan on levytilan kasvattaminen ja varmuuskopiointi.

Pilvipalvelujen kohdalla vahvuuksia ovat tallennustilan kasvattaminen sujuvasti lähes kuinka suureksi tahansa ja myös varmuuskopiointi. Suurimpina heikkouksina nähdään, että niitä ei organisaatio itse pysty hallitsemaan, vikojen selvitys on riippuvainen palveluntuottajasta, vikojen korjaaminen kestää kauan ja tietoturvallisuudesta ei ole varmuutta.

Omistajuus ja hallinta

Omistajuuden ja tallennuspalvelujen hallinnan suhteen pilvipalvelu- ja verkkolevytallennuksessa on huomattavia eroja. Käyttäjä omistaa yleensä verkkolevyt ja siten myös hallinnoi ja ylläpitää niitä. Pilvipalveluissa palveluntuottaja omistaa tallennuskapasiteetin ja siten myös vastaa ylläpidosta, päivityksistä ja hallinnoinnista pitäen palvelut ajan tasalla käyttäjää varten.

Pilvipalveluihin siirryttäessä kontrollin määrä dataan nähden vähenee ja samalla niiden muokattavuus. Salo (2010) listaa kuusi kohtaa, joissa kontrollin määrä on suurin kohdassa ja yksi ja pienin kohdassa kuusi.

1. itse kehitetty sovellus omalla alustalla (oma palvelinkeskus)
2. ostettu sovellus omalla alustalla (oma palvelinkeskus)
3. itse kehitetty sovellus ulkoistetulla palveluntuottajan alustalla (perinteinen hosting)
4. ostettu sovellus ulkoistetulla palveluntarjoajan alustalla (perinteinen hosting)
5. itse kehitetty sovellus pilvialustalla (PaaS, IaaS)
6. ostettu sovellus pilvialustalla (SaaS)

Resurssien hallinnan menettäminen käyttäjältä palveluntuottajalle herättää monissa epäilyksiä. Se kasvattaa toiminta- ja turvallisuusriskejä.

Tallennuskapasiteetti

Verkkolevyissä tallennustilaa ei voi rajattomasti kasvattaa, tai ainakin sen kasvattaminen vaatii seurantaa ja uusien verkkolevyjen hankintaa, mikä taas kasvattaa kustannuksia.

Pilvipalveluissa tallennuskapasiteetti on ainakin näennäisesti rajatonta, sillä palvelujen-tuottajien resurssit ovat suuria ja näyttäytyvät käyttäjien silmissä loputtomilta.

Laskentateho, nopeus ja ketteryys

Pilvipalveluissa käyttäjä ostaa palvelua tarpeen mukaan, joten resursseja on mahdollista ottaa käyttöön miltei loputtomasti. Kun monet toiminnot voidaan tehdä pilvessä, toiminta nopeutuu. Verkkolevyjen kohdalla laskentatehon määrä riippuu tallennustilan määrästä ja verkkolevypalvelimen komponenttien ominaisuuksista, esimerkiksi muistin määrästä. Pilvipalvelutallennusjärjestelmät ovat verkkolevytallennukseen verrattuna nopeampia käyttää.

Pilvipalveluja käyttäessä organisaatiot voivat liikkua nopeammin projekteissa ja testata käsitteitä ilman pitkäaikaisia hankintoja ja suuria ennakkokustannuksia, koska ne maksavat vain kuluttamansa resurssit. Tämä liike-elämän ketteryyden mainitsema käsite mainitaan usein tärkeänä etuna. Mahdollisuus kokeilla uusia palveluita ilman perinteistä IT-hankintaa nopeasti ja vaivatta mahdollistaa uusien sovellusten käyttöönoton nopeammin. (Ranger 2018.)

Kustannukset

Pilvipalvelujen käyttäjät maksavat yleensä todellisen käytön mukaan, jolloin ei tarvitse investoida suuriin alkukustannuksiin ja kiinteisiin kuluihin, joita tarvitaan kehittyneen tietoteknisen laitteiston ja sovellusten hankintaan ja käyttöön.

Pilvipalvelut eivät ole välttämättä halvempia kuin muut tietojenkäsittelymuodot. Omien laitteiden ja ohjelmistojen ostaminen saattaa olla edullisempaa ostaa pitkällä aikavälillä

erityisesti, jos sovelluksella on säännöllinen ja ennakoitavissa oleva käyttö. Vaikka uuden pilvisovelluksen käyttäminen saattaa olla helppoa, olemassa olevien tietojen tai sovellusten siirtäminen pilveen voi olla paljon monimutkaisempaa ja kalliimpaa. Äskettäin ilmestyneessä raportissa huomattava osa kokeneista pilvipalvelujen käyttäjistä ajatteli, että siirtokustannukset ylittävät lopulta IaaS:n tuomat pitkän aikavälin säästöt. (Ranger 2018.)

Lukkiutuminen pilvipalveluissa

Pilvipalveluiden kohdalla riskinä voi olla myös lukkiutuminen yhteen palveluntuottajaan. Käyttäjälle voi olla vaikeaa ja joskus jopa mahdotonta vaihtaa palveluntuottajaa, jos esimerkiksi on rakennettu infrastruktuuri yhden palveluntuottajan kanssa tai on investoinut suuria summia palveluihin. Joskus lukkiutuminen yhteen toimittajaan saattaa tuoda etuja muun muassa määräalennusten suhteen tai että palvelujen hankkiminen palveluntarjoajalta varmistaa niiden sujuvamman yhdentymisen sekä paremman turvallisuuden. (Tynan 2017.) Tämänkaltaisia ongelmia ei verkkolevytallennusjärjestelmissä yleensä ole.

3.4 Turvallisuus eri tallennusjärjestelmissä

3.4.1 Verkkotallennuspalvelun turvallisuus

Verkkolevytallennusjärjestelmässä turvallisuus riippuu siitä, miten verkkotallennus on järjestetty. Jos verkkolevyt sijaitsevat organisaation omassa datakeskuksessa tai yksiköissä, vastuu tietoturvasta on omalla vastuulla. Jos verkkotallennus on ulkopuolisen palveluntuottajan konesaleissa sijaitsevassa varmistetussa levytilassa, vastuu on ulkopuolisella palveluntarjoajalla, mutta osittain myös omalla organisaatiolla. Kussakin tapauksessa on suojauduttava ulkopuolisten tietomurtoihin, jolloin vaarana on tietojen häviäminen tai että ne myydään tai vuodetaan kilpailijalle. Haitalliset sisäpiiriläiset ovat myös riski. Organisaatiossa voi olla käyttöoikeudet omaavia henkilöitä, jotka haluavat väärinkäyttää mahdollisuuttaan päästä organisaation järjestelmiin, tietoverkkoihin ja dataan haitaten esimerkiksi organisaation palveluiden saatavuutta ja luotettavuutta. Myös hakkerit voivat hävittää hyökkäyksen kohteena olevalta palvelimelta dataa tai palvelun-

tuottajan työntekijän virhe aiheuttaa tiedon häviämisen. Hakkerit voivat tehdä palvelunestohyökkäyksiä, joilla kuormittavat kohteen palvelinta, kunnes palvelun toiminta hidastuu tai lakkaa ja estävät palvelunkäyttäjien pääsyn dataan ja sovelluksiin. Myös tulvat, maanjäristykset tai myrskyt ja niiden aiheuttamat tulipalot voivat olla syynä tiedon häviämisen. Suomessa riski on kuitenkin suhteellisen pieni. Kummassakin tapauksessa on huolehdittava, että tallennus on yhdistetty riittävään varmuuskopiointijärjestelmään ja verkkolevyt on säilytetty hyvin turvasuojatussa datakeskuksessa. Myös verkkoyhteys verkkotallennusjärjestelmään on suojattava hyvin. (Salo 2012; Rousku 2014.)

3.4.2 Pilvipalvelujen turvallisuus

Pilvipalveluiden käyttö on nykyisin arkipäivää niin yrityksille, yliopistoille, valtion ja kuntien hallinnolle kuin myös yksityishenkilöille. Tällöin on syntynyt virheellinen käsitys, että myös tieturva voidaan ulkoistaa pilvipalveluihin. Käytännössä tietosuojaan pilvipalvelussa liittyvät samat riskit kuin, jos tieto tallennetaan perinteisillä tavoin muualle. Pilvessä olevat tiedot tallennetaan edelleen datakeskukseen. Tällöin hakkerit pääsevät näihin tietoihin käyttäen samoja menetelmiä, joita ne ovat aina käyttäneet. Pilvipalvelujen käytön yleistyessä monet organisaatiot ovat huolissaan niiden turvallisuudesta, vaikkakin turvallisuusrikkomukset ovat harvinaisia. (Ranger 2018.)

Selvittääkseen, mitkä ovat suurimmat turvallisuusuhkat pilvipalveluissa, Cloud Security Alliance (CSA) -työryhmä suoritti alan asiantuntijoiden joukossa tutkimuksen pilvipalvelujen suurimmista turvallisuuskysymyksistä. CSA Top Threats -työryhmä esitti tutkimuksen tulokset vuoden 2016 loppuraportissan. Tässä raportin viimeisimmässä versiossa asiantuntijat määrittelivät seuraavat 12 kriittistä ongelmaa pilvipalvelun turvallisuuteen (luokitellaan jäljempänä vakavuuden mukaan tutkimuksen tulosten perusteella). (Cloud Security Alliance 2016). Samat turvallisuusuhat Cloud Security Alliance määritteli myös vuodelle 2018 (Cloud Security Alliance 2017):

Tietosuojan murtaminen

Tietosuojan murtaminen määritellään tapahtumaksi,

> jossa arkaluonteisia, suojattuja tai luottamuksellisia tietoja luovuttaa, vakoilee, varastaa tai käyttää henkilö, joka ei ole siihen valtuutettu. Tietosuojan murtaminen

> voi olla kohdennetun hyökkäyksen ensisijainen tavoite tai se voi johtua vain inhimillisestä virheestä, sovellusten haavoittuvuuksista tai huonosta turvallisuuskäytännöstä. Tietosuoja voi sisältää kaikenlaisia tietoja, joita ei ollut tarkoitettu julkiseen julkaisuun, mukaan lukien, mutta ei rajoittuen, henkilökohtaiset terveystiedot, taloudelliset tiedot, henkilökohtaiset tiedot, liikesalaisuudet ja henkinen omaisuus. (INSUREtrust 2018.)

Murtautujia voivat olla esimerkiksi ulkomaiset ja kotimaiset kilpailijat, taloudellista hyötyä tavoittelevat rikolliset tai aktivistit, jotka jostain syystä haluavat haitata tai vaikeuttaa yrityksen tai organisaation toimintaa. Myös luvaton sisäpiiriläinen, joka saa tietoa pilvistä, voi olla murtautuja. (Cloud Security Alliance 2017.)

Vaikka pilvipalvelut yleensä tarjoavat hyvän suojan asiakkaidensa tallentamalle tiedolle, ovat lopulta asiakkaat vastuussa tietojen suojaamisesta pilvessä. Paras suoja tietomurtoja vastaan on tehokas turvaohjelma, monivaiheinen todennus ja salaus sekä monikertainen varmuuskopiointi.

Riittämätön henkilöllisyyden, tunnistetietojen ja käyttöoikeuksien hallinta

Laittomat toimijat naamioituneina operaattoreiksi tai kehittäjiksi voivat lukea tai poistaa tietoja, antaa ohjaustasoa tai hallintotoimintoja koskevia ohjeita, tunkeutua kauttakulkua koskeviin tietoihin tai vapauttaa haittaohjelmia, jotka näyttävät olevan peräisin laillisesta lähteestä. Tämän seurauksena riittämättömät henkilöllisyyden, tunnistetietojen tai salasanojen ja salausavainten käytön hallinta voivat mahdollistaa tietojen luvattoman käytön ja aiheuttaa suurta vahinkoa organisaatioille tai loppukäyttäjille. (Cloud Security Alliance 2017.)

Epävarmat liitännät ja sovellusliittymät

Pilvipalvelun tarjoajat paljastavat joukon ohjelmiston käyttöliittymiä tai sovellusohjelmointirajapintoja, joita asiakkaat käyttävät. Näiden rajapintojen avulla toteutetaan kaikki palvelut, hallinta, järjestäminen ja seuranta. Yleisten pilvipalvelujen turvallisuus ja saatavuus ovat riippuvaisia näiden perusliittymien turvallisuudesta. Nämä rajapinnat on suunniteltava siten, että ne suojaavat sekä vahingossa tapahtuvia että haitallisia yrityksiä kiertää turvallisuuskäytäntöjä. (Cloud Security Alliance 2017.)

Järjestelmän haavoittuvuudet

Hyökkääjät ja hakkerit käyttävät hyväkseen järjestelmässä olevia virheitä, joiden kautta ne voivat tunkeutua tietokonejärjestelmään varastaakseen tietoja, ottaakseen järjestelmän kontrollin haltuunsa tai häiritäkseen pilvipalveluntoimintaa. (Cloud Security Alliance 2017.)

Asiakastilin tilin ja palvelun kaappaaminen

Tilin tai palvelun kaappaaminen ei ole uusi asia. Hyökkäysmenetelmät, kuten tietojen kalastelu, petokset ja ohjelmistojen haavoittuvuuksien hyödyntäminen ovat olleet käytössä ja pitkään. Tietoturvan kannalta pilvipalvelun käyttö tuo asiakkaan oman tietoturvariskin lisäksi myös palveluntarjoajan tietoturvariskin. Jos hyökkääjä pääsee käyttämään käyttäjän käyttöoikeustietoja, he voivat vakoilla hänen toimintojaan ja tapahtumia, manipuloida tietoja, palauttaa väärennetyt tiedot ja ohjata hänen asiakkaitaan laittomiin sivustoihin. (INSUREtrust 2018; Cloud Security Alliance 2017.)

> Salon mukaan identiteettihallinta on yksi pilvipalveluiden suurimmista haasteista. Asiakkaan on voitava luottaa palveluntarjoajan kykyyn turvata asiakastietojen koskemattomuus ja yhteyksien tietoturvallisuus (Salo 2012).

Haitalliset sisäpiiriläiset

Organisaatiossa voi olla käyttöoikeudet omaavia henkilöitä, jotka haluavat väärinkäyttää mahdollisuuttaan päästä organisaation järjestelmiin, tietoverkkoihin ja dataan haitaten esimerkiksi organisaation palveluiden saatavuutta ja luotettavuutta. Omien työntekijöiden osalta asiakas voi tehdä valvontaa, mutta pilvipalvelun tarjoajan osalta joutuu luottamaan, että palvelun tarjoaja hoitaa tämän puolen riskinhallintaa hyvin. (Cloud Security Alliance 2017.)

Kehittyneet pysyvät uhkat (ATP)

Kehittyneitä pysyviä uhkia ovat haittaohjelmat, jotka tunkeutuvat tietojärjestelmään ilman, että järjestelmän käyttäjä huomaa sitä. Saatuaan jalansijaa kohdeyhtiöiden tietotekniikkainfrastruktuurissa, ne varastavat tietoja ja intellektuaalista omaisuutta. APT:tä

vastaan suojautuessa on tärkeää päivittää tietoturvajärjestelmät ja kouluttaa IT-henkilöstö tunnistamaan APT:n menetelmät. Myös muun henkilöstön pitää ymmärtää, ettei tuntemattomia tiedostoja kannata avata. (Cloud Security Alliance 2017.)

Tiedon menetys

Tiedon menetyksen syynä voi olla hakkerin hyökkäyksen aiheuttama tiedon häviäminen, Syynä voi olla myös oman henkilöstön tai palveluntarjoajan työntekijän virhe, mikä aiheuttaa tiedon menetyksen. Myös luonnon katastrofit, kuten maanjäristys, myrsky, tulipalo tai tulva voivat aiheuttaa tietojen tuhoutumisen. (Cloud Security Alliance 2017.)

Tiedon merkitys yritysten ja organisaatioiden toiminnalle on tullut entistä tärkeämmäksi. Siitä syystä toiminnan kannalta kriittisen tiedon varmuuskopiointi päivittäin ja tiedon tallennus useassa paikassa on tietoturvan kannalta tärkeää. On myös tärkeää varmistaa pilvipalvelun tarjoajan kanssa varmuuskopioinnin ja muu tiedon tallentamisen turvallisuus. (Cloud Security Alliance 2017.)

Riittämätön due diligence

Kun organisaatio suunnittelee pilvipalvelujen ja siihen liittyvän teknologian hyödyntämistä, on tärkeää, että due diligence -prosessi suoritetaan huolellisesti. Se tarkoittaa, että selvitetään huolellisesti uuden teknologian tai pilvipalvelun hankkimiseen liittyvät kaupalliset, taloudelliset, tekniset, lailliset ja sopimuksen noudattamisen riskit. Riskit realisoituvat, jos esim. pilvipalvelun tarjoaja menee konkurssiin tai ei pysty teknisesti toteuttamaan sopimuksessa luvattua palvelua. (Cloud Security Alliance 2017.)

Pilvipalvelujen väärinkäyttö ja turha käyttö

Hakkerit ja muut haitalliset toimijat voivat käyttää hyväkseen huonosti suojattujen pilvipalvelujen resursseja toteuttaakseen käyttäjiä, organisaatioita tai muita pilvipalvelujen tarjoajia vastaan kohdistuvia hyökkäyksiä. Esimerkkejä väärinkäytöstä ovat palvelunestohyökkäyksen (DDoS) käynnistäminen, roskapostit sähköpostin kautta, salasanojen ja salausavainten urkinta, digitaalisiin valuuttoihin kohdistuvat hyökkäykset, haittaohjel-

mien ja laittomien sisältöjen ylläpito. Pilvipalvelun tarjoajasta peräisin olevat tai suunnatut DDoS-hyökkäykset voivat johtaa saatavuuden puutteeseen, liiketoiminnan häiriöihin ja muiden samaan pilvialustaan sijoitettujen sivustojen tulojen menetykseen. Vilpillinen maksuvälineiden käyttö voi johtaa siihen, että kustannukset kohdistuvat myös ulkopuolisiin viattomiin osapuoliin, kuten taloudellisiin palveluntarjoajiin ja lopulta asiakkaisiin. (Cloud Security Alliance 2017.)

Palvelunestohyökkäys

Palvelunestohyökkäyksellä (Denial of Service, DoS) pyritään estämään verkkosivuston tai palvelun toiminta. Tällöin verkkosivustolle voidaan esimerkiksi kohdistaa niin paljon häiriöliikennettä, että se ei pysty palvelemaan asiakkaitaan. Jos hyökkäys toteutetaan useasta lähteestä, esimerkiksi käyttäen hyväksi kaapatuista tietokoneista koostuvaa botnettia, kutsutaan sitä DDoS:ksi (Distributed Denial of Service). Vastaavasti puhelimiin kohdistettua hyökkäystä kutsutaan TDoS (Telephony Denial of Service). (Cloud Security Alliance 2017.)

Jaetun teknologian haavoittuvuudet

Pilvipalvelujen tarjoajat toimittavat palveluitaan skaalattavasti jakamalla infrastruktuureja (IaaS), alustoja (PaaS) tai sovelluksia (SaaS). Pilvipalvelujen jaettu teknologia aiheuttaa sen, että esimerkiksi SaaS:ssa havaittu turvallisuusongelma voi haitata kaikkea kyseisen palveluntarjoajan pilvessä liikkuvaa dataa ja siellä toimivia muita sovelluksia. (Cloud Security Alliance 2017; INSUREtrust 2018.)

Erilaiset turvallisuusriskit uhkaavat monella tavoin pilvipalveluita ja niihin uhkiin on pyrittävä varautumaan suojaamalla mahdollisimman vahvasti pilvipalveluissa olevat tiedot sekä pyrittävä hankkimaan pilvipalveluita turvallisilta palveluntuottajilta. Vastuu tietojen suojaamisesta pilvessä ei ole palveluntarjoajalla, vaan päävastuu on pilvipalveluja käyttävällä asiakkaalla (Violino 2018).

3.5 Yhteenveto verkkolevy- ja pilvipalveluntallennusjärjestelmien ominaisuuksista

Taulukossa 2 esitetään yhteenveto verkkolevy- ja pilvipalveluntallennusjärjestelmien ominaisuuksista. Pilvipalvelutallennusjärjestelmän ominaisuudet riippuvat paljolti siitä, minkälainen pilvipalvelumalli on siellä sisällä.

Taulukko 2. Verkkolevy- ja pilvipalvelujärjestelmien ominaisuuksia

	Verkkolevypalvelin-pohjainen tallennusjärjestelmä	**Pilvipalvelupohjainen tallennusjärjestelmä**		
Ominaisuudet		Saas	Paas	Iaas
Tietoturvallisuus	Hyvä	Riskialtis	Mahdollinen riski	Mahdollinen riski
Tallennuskapasiteetti	Riippuu verkkolevyjen määrästä	Joustava, näennäisesti rajaton	Joustava, näennäisesti rajaton	Joustava, näennäisesti rajaton
Omistajuus	Käyttäjällä	Palveluntuottajalla	Suurimaksi osin palveluntarjoojalla	Osin palveluntuottajalla
Hallinta	Käyttäjällä	Palveluntuottajalla	Suurimaksi osin palveluntuottajalla	Osin palveluntuottajalla
Laskentateho	Riippuu komponenteista	Nopea	Nopea	Nopea
Nopeus	Riippuu komponenteista	Hyvä	Hyvä	Hyvä
Huolto	Käyttäjällä yleensä	Palveluntuottajalla	Osin palveluntuottajalla	Osin palveluntuottajalla
Hinta	Komponenteista ja kovalevyistä	Hinta määräytyy käytön mukaan	Hinta määräytyy käytön mukaan	Hinta määräytyy käytön mukaan

4 Tallennusvaihtoehdot selvityksen pohjalta

4.1 Verkkolevypalvelintallennuksen vaihtoehdot

Verkkolevytallennukseen voi hankkia lisää tilaa yrityksen tai organisaation oman konesalin tallennustilasta ja laskentatehosta tai hankkimalla yksikön omaan käyttöön lisää tallennustilaa ja laskentatehoa. Oman konesalin tai yksikön tallennustilan hankkimista puoltaa tietoturvan suojaaminen, toiminnan tai tutkimuksen kannalta kriittisen tiedon säilyttäminen omissa käsissä ja myös tietosuojaan liittyvät viranomaismääräykset ja GDPR:n asettamat vaatimukset.

Organisaation konesalin käyttöä tukee se, että konesalin toiminnasta ja turvallisuudesta huolehti sitä varten koulutettu ja palkattu henkilöstö, ja myös tilat täyttävät tallennusten säilyttämiselle asetetut varmuuskopiointi- ja tietosuojavaatimukset. Oman yksikön hallussa olevan tallennustilan hoitamiseen tarvitaan asianmukaiset tilat turvallisuusvaatimuksineen ja käyttöoikeuksiin, kulkulupiin, varmuuskopiointiin ja tietosuojautumiseen vaadittavat toimenpiteet sekä vastuuhenkilöt. Myös verkkoyhteyksien varmistaminen on tärkeää yksikön ja tallennustilan säilytyspaikan välillä.

Varsinkin sellaiset sovellukset, jotka nojautuvat raskaasti toisiin, vain talon sisällä käytettäviin sovelluksiin tai tietokantoihin jätetään usein talon oman IT-osaston ja kyseisten yksiköiden hoitoon.

Selvityksessä tuli esille seuraavia verkkolevypalvelimen etuja tallennusjärjestelmänä:

Omat laitteet

Verkkolevytallennusjärjestelmässä organisaatio hankkii yleensä omat laitteet, jolloin se voi hallita ja huoltaa laitteita itse.

Laitteet sijaitsevat organisaation itse hallitsemassa tilassa, jolloin niitä pääsee käyttämään ja huoltamaan tarpeen mukaan henkilöt, joilla on käyttöoikeus.

Tietoturva

Tietoturva on organisaation omalla vastuulla. Jos tietoturva on rakennettu hyvin, oma verkkolevypalvelin antaa hyvän tietoturvan datalle ulkopuolisilta, kuten kilpailijoilta, taloudellista hyötyä tavoittelevilta tai keneltä tahansa muilta, jotka jostain syystä haluavat haitata tai vaikeuttaa yrityksen tai organisaation toimintaa. On myös suojauduttava sisältä päin tulevilta uhilta, kuten työntekijöiltä, joiden ei tule päästä verkkolevypalvelimelle. Hakkereilta suojautumiseen on varauduttava päivittämällä ja uusimalla turvajärjestelmiä.

Tietoturvan kannalta on myös tärkeää, että verkkoyhteys suojataan hyvin. Verkkolevypalvelin tulee sijoittaa tulipalolta, vesivahingoilta ja muilta onnettomuuksilta turvasuojattuun tilaan, jonne on pääsy vain tietyillä, verkkolevypalvelimen käyttöön ja huoltoon määrätyillä henkilöillä.

Edullinen käyttää alkuinvestoinnin jälkeen

Hankittaessa oman verkkolevytallennusjärjestelmän, alkuinvestoinnit ovat melko suuret, mutta sen jälkeen itse käyttökustannukset ovat melko edulliset. Käyttökustannuksia arvioitaessa on otettava huomioon, että verkkolevypalvelimen ylläpitoon ja huoltoon tarvitaan henkilöstöä, mikä nostaa sen käyttökustannuksia.

Verkkolevypalvelin tallennusjärjestelmänä -kyselyn tuloksia

Rakennetun ympäristön mittauksen ja mallinnuksen instituutilla työskennellään erilaisten tutkimusprojektien parissa, minkä vuoksi pitää pystyä ilman suurta aikaviivettä ottamaan tiedostoja tallennusjärjestelmästä, säilyttää sovelluksia ja tallentaa erilaisia tiedostoja, kuvaa ja videota. Yksittäisen projektin työtiedostot voivat olla kooltaan useita kymmeniä terabittejä. Nopeuden ja sujuvuuden lisäksi hyvä tietoturva on välttämätön valintakriteeri tallennusjärjestelmälle. Tallennustilaa tarvitaan 3D-mittausaineistojen käsittelyyn ja arkistointiin. 3D-mittausaineistot koostuvat kuvista, videoista, pistepilvistä ja eri ohjelmistojen projektitiedostoista. Tallennustilaa tarvitaan vähintään 100 terabittiä.

Tietojen tallentamisen lisäksi tietojen varmistus ja palautusmahdollisuus ovat välttämättömiä, samoin kuin se, että tiedot pysyvät Suomessa.

Päätelaite on yleensä Windows 10, mutta työskentelyssä voidaan käyttää myös muitakin käyttöjärjestelmiä kuten Linuxia. Tällä hetkellä olevia tallennusjärjestelmiä ei korvata, vaan halutaan lisää tallennustilaa.

Sähköpostilla lähetettiin kysely 20 verkkolevypalvelinratkaisuja ja pilvipalveluja tarjoaville yrityksille. Vastauksia, jotka koskivat verkkolevypalvelinta tallennusjärjestelmäratkai-

suna, tuli neljältä yritykseltä. Tämän lisäksi olen selvittänyt laitevalmistajien ja verkkokauppojen sivuilta mahdollisia eri verkkolevypalvelinvalmistajien vaihtoehtoja verkkolevypalvelimeksi.

Yrityksiltä kysyttiin, mitä vaihtoehtoja eri yrityksillä on tarjottavana toimeksiantajan ehdoilla. Toimeksiantaja haluaa verrata erityisesti verkkolevypalvelin- ja pilvipalvelutallennuksen välillä ja haluaa sen vuoksi tietää tallennusvaihtoehtojen hyvät ja huonot puolet. Erityisesti he ovat kiinnostuneita verkkolevypalvelintallennusvaihtoehdosta. Myös hinta on tärkeä valintakriteeri.

Verkkolevypalvelimia vertailtaessa otettiin huomioon seuraavat ominaisuudet:

- Muistin määrä: minimi 32 GB, suositeltava määrä 64 GB.
- Tallennuskapasiteetti: vähintään 100 TB.
- Kovalevytyyppi: käykö kaikki kiintolevytyypit vai ainoastaan SAS.
- Tallennuksen hallinta: onko palvelimella RAID-ominaisuus eli voiko tallennustilan vikasietoisuutta ja/tai nopeutta lisätä.
- Pilvipalvelu: onko laitteessa sisäänrakennettu valmius pilvipalveluun.
- Lähiverkkoliitäntä ja sen ominaisuudet: mitkä ovat laitteen Ethernet-standardit ja millaiset tiedonsiirtoprotokollat ja -nopeudet laitteessa on.
- Suoritin: se, minkä tasoinen suoritin kyseisessä laitteessa on, vaikuttaa verkkolevypalvelimen tehoon.
- Asennustyyppi: onko verkkolevypalvelin telineasennettava eli ns. räkkityyppinen.
- Käyttöjärjestelmä: onko järjestelmässä oma käyttöliittymä vai pitääkö se asentaa siihen.
- Järjestelmävaatimukset: minkä laitteiden ja käyttöjärjestelmien kanssa se on/ei ole yhteensopiva.

Toimeksiantajan käyttötarkoitukseen sopivat laitteet löytyvät seuraavilta laitevalmistajilta: QNAP:lta, Synologylta, Delliltä ja HPE:ltä.

Toimeksiantajan kriteerit täyttävien verkkolevypalvelinvaihtoehtojen hinnat vaihtelivat 9.400 €:n - 37.400 €:n välillä. Koska insinöörityön tekijä pyysi hinnat omissa nimissään insinöörityötä varten, ovat hinnat korkeammat kuin jos kysely olisi tehty toimeksiantajan

nimissä. Kilpailutuksessa suurasiakkaat pystyvät kilpailuttamaan tehokkaammin ja saavat edullisemmat hinnat.

Omissa tiloissa sijaitsevien verkkolevypalvelimien hintaa verrattaessa pilvipalvelun hintoihin tulee ottaa huomioon lisäkustannukset, jotka syntyvät verkkolevypalvelimien säilytyksestä, huoltamisesta ja turvajärjestelyistä. Myös mahdolliset tiedostojen siirtonopeuden parantamiseen liittyvät kaapeloinnit voivat aiheuttaa lisäkustannuksia.

Halvin verkkolevypalvelinvaihtoehto sisältää 140 TB verkkotallennustilaa. Turvallisuus on parempi, jos käytetään kahta palvelinta, joissa kummassakin tallennustila on vähintään 100 TB ja toinen toimii varmuustallennukseen varattuna tallennustilana. Halvin tämän kriteerin täyttävä verkkolevypalvelinvaihtoehto oli 18.700 €. Turvallisuutta lisää myös, jos palvelimet sijaitsevat fyysisesti eri tilassa, jolloin mahdollisen tulipalon tai muun vahingon sattuessa molemmat eivät tuhoudu.

Rakennetun ympäristön mittauksen ja mallinnuksen instituutin tämänhetkisen tallennustarpeen huomioon ottaen oma verkkolevypalvelin on edullisempi ratkaisu kuin yksityisen pilvipalvelun hankkiminen.

4.2 Pilvipalvelutallennuksen vaihtoehdot

Pilvipalvelutallennusten tarjoajia on paljon aina globaaleista jättiyrityksistä pieniin kotimaisiin pilvipalveluyrityksiin. Ostajan tai palvelun tilaajan on vaikea verrata ja arvioida eri vaihtoehtoja. Oheisessa luettelossa on esitetty tärkeimpiä kriteereistä, joita tulisi arvioida palveluntarjoajia valittaessa:

- Missä konesali sijaitsee (Suomessa, Euroopassa vai muualla)?
- Onko sähkönjakelu kahdennettu, varmistettu ja, että varavoimaa on riittävästi sähkökatkon varalta?
- Konesalin kulunvalvonta ja turvallisuus on riittävän tiukka?
- Miten ja millaisella laitteistolla konesalin paloturvallisuus on järjestetty?
- Tarjoaako yritys palveluja omista konesaleistaan vai ostaako se ne alihankintana? Missä yrityksen arvokas data ja järjestelmät sijaitsevat? Kun konesalit ovat

palveluntarjoajalla itsellään, on toiminta pitkäjänteistä ja suunnitelmallista ja kontrolli asiakkaalle myydyistä palveluista omissa käsissä.

- Miten konesalin jäähdytys on järjestetty ja onko jäähdytyskapasiteetti riittävä?
- Pystyykö palveluntarjoaja vähintään kahdentamaan koko konesaliympäristönsä kattaen myös tietoliikenneyhteydet? Onko konesalien välinen etäisyys vähintään 10 km.
- Täyttääkö yrityksen toiminta viranomaisten salassa pidettävää tietoa varten kehitetyn viranomaisten auditointityökalun (Katakri) vaatimukset? Katakria viranomainen voi käyttää arvioidessaan kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa.

  Katakri määrittää kohteen turvallisuuden tason arvioimiseksi ja auditoimiseksi tarvittavat kriteerit. Kriteeristöön sisältyy fyysinen, hallinnollinen ja toiminnallinen turvallisuus.
- Onko pilvipalveluyritys hankkinut laatusertifikaatin (esimerkiksi ISO 9001, ISO 27001, ISO 14001) (Suomen Standardisoimisliitto SFS ry 2019)? Laatusertifikaatin hankinta osoittaa, että yrityksen toimintatavat ja prosessit täyttävät sertifioijan asettamat laatuvaatimukset. Näiden standardien vaatimukset voidaan integroida osaksi organisaation johtamisjärjestelmää.

Yksityinen pilvipalvelu tallennusvaihtoehtona

Yksityinen pilvipalvelu voi olla verkkolevypalvelinta parempi ratkaisu tilanteissa, kun tarvitaan erittäin suurta ja kasvavaa datamäärän tallennustilaa, tavallista korkeampaa tietoturvaa ja muusta verkkoliikenteestä riippumatonta ja häiriötöntä tiedonsiirtokapasiteettia. Yksityistä pilvipalvelua mietittäessä suunnittelun tulee lähteä yrityksen/tutkimuslaitoksen nykyisistä ja tulevaisuuden tarpeista ja niihin räätälöidystä palveluympäristöstä. Tyypillisin syy yksityisen pilven käytölle verrattuna julkiseen pilvipalveluun on huoli tietoturvariskeistä. Yksityiset pilvipalvelut on suunniteltava tiukkojen tietoturvavaatimusten edellyttämällä tavalla. Jos sovellutusten ja ohjelmistojen käyttöehdot edellyttävät palveluiden suorittamisen jaetuista palveluympäristöistä erotettuina, yksityinen pilvipalvelu on silloin ainoa vaihtoehto. Myös lainsäädäntö voi rajoittaa tiedon ja tietojenkäsittelyn luovuttamista ulkopuolisten palveluntarjoajien haltuun. Yksityinen pilvipalvelu voi myös tarkoittaa palvelimien ja/tai palvelinsalien ulkoistamista siten, että pilvipalvelu on vain pal-

velun tilaajan hallussa. Ulkopuolisen palveluntarjoajan vastuulle kuuluu tyypillisesti verkkoyhteydet, tallennustila, palvelimet ja niiden ylläpito. Tärkeä kriteeri on myös, että verkkosali sijaitsee lähellä (Suomessa) ja että konesalien välimatka on vähintään 10 km. Yksityinen pilvipalvelu eroaa omassa konesalissa säilytettävästä tallennustilasta siinä, että infrastruktuurista huolehtii ulkopuolinen palveluntarjoaja, joka vastaa verkkoyhteyksistä, tallennustilasta, palvelimista ja niiden ylläpidosta sekä turvallisuudesta ja varmuuskopioinnista ts. infrastruktuuri ostetaan palveluna (IaaS).

Selvityksen perusteella yksityisen pilvipalvelun edut ja haitat tallennusjärjestelmänä ovat:

Tallennustila lähes rajaton

Pilvipalvelussa ei tarvitse huolehtia tallennustilan määrästä, sillä sitä voidaan kasvattaa hyvinkin suureksi.

Tietoturva hyvä

Yksityisen pilvipalvelun tietoturva on hyvä erityisesti silloin, jos konesalit sijaitsevat Suomessa.

Maksu käytön mukaan

Pilvipalvelutallennuksesta maksetaan käytön mukaan, joten alkuinvestoinnit eivät ole suuret. Yksityisen pilvipalvelun etuna on, että hallintaportaalin avulla voidaan säädellä konesalin kapasiteettia ja tarkkailla käyttöastetta, palvelutasoraportteja sekä kustannustietoja. Suorituskyvyn niin vaatiessa voidaan esimerkiksi lisätä kapasiteettia kuukauden ruuhkaviikolle ja vähentää sitä muille viikoille. Päiväkohtaiseen kapasiteettiin perustuva laskutus on joustava ja antaa mahdollisuuden säästöön. Kuitenkin selvityksen perusteella pilvipalvelun käyttö tulisi tämän työn toimeksiantajalle huomattavasti kalliimmaksi kuin verkkolevypalvelin tallennusjärjestelmäratkaisuna, kun otetaan huomioon heidän ehtonsa.

Muut pilvipalveluvaihtoehdot

Hybridipilvi sekä yhteisöllinen ja julkinen pilvi soveltuvat tämän opinnäytetyön toimeksiantajan asettamilla ehdoilla huonommin toimeksiantajan tarpeisiin.

Hybridipilvessä yhdistetään pilvipalvelun ja sen ulkopuolella olevan tiedon arkistoinnit. Yritys tai muu organisaatio voi säilyttää toiminnan kannalta kriittisen, tärkeän tai viranomaismääräysten takia osan tiedoista omassa konesalissa ja osan toiminnan kannalta ei niin kriittistä tietoa pilvipalvelun tarjoajan konesalissa tai palvelualustalla. Hybridipilven etu on siinä, että voidaan hyödyntää eri pilvipalvelujen tarjoajien alustoja tai palveluja ja samalla säilyttää oman toiminnan kannalta tärkeä ja kriittinen tieto omassa hallinnassa. Insinöörityön toimeksiantaja haluaa säilyttää erillään nykyiset tallennusratkaisut ja uusi tallennusjärjestelmä tulee jo olemassa olevien lisäksi, joten hybridipilvi ei tule kyseeseen tallennusjärjestelmävaihtoehtona.

Yhteisöllinen pilvi on kyllä käyttökelpoinen ratkaisu esim. kansainväliselle tutkija- tai tuotekehitysryhmälle, jotka tekevät yhteistyötä tutkimus- tai tuotekehityshankkeessa. Hallinnointi ja laitteistot voivat olla tällöin ulkopuolisen palveluntarjoajan vastuulla, jolloin palvelun ostajat eivät tarvitse sijoittaa infrastruktuuriin vaan voivat keskittyä itse toimintaan.

Julkisessa pilvessä asiakas ostaa palvelut pilvipalvelujen tarjoajalta maksua vastaan. Tällöin vastuu konesaleista, laitteistoista, tietoturvasta, ohjelmistoista ja palvelualustoista on palvelun tarjoajalla. Tässä on myös etuna, ettei asiakkaan tarvitse investoida ohjelmistoihin ja infrastruktuuriin, vaan voi keskittyä oman liike- tai tutkimustoimintansa kehittämiseen. Sekä yhteisöllisen että julkisen pilven kohdalla ei voida olla varmoja, mihin data on tallennettu ja missä konesalit sijaitsevat, joten tietojen vuodon epävarmuus on olemassa. Tietoturvan kohdalla pilvipalveluissakin on huomioitava, että tietoturvasta pääasiassa huolehtii palvelun käyttäjä.

Pilvipalvelujen hankinta sisältää yleensä seuraavat vaiheet:

Tarjousvaihe

Määritellään ja kartoitetaan tarvittava pilvipalvelu ja lähetetään tarjouspyynnöt. Tarjousten perusteella valittujen palveluntarjoajien kanssa käydään yhdessä läpi asiakkaan tarvitsema palvelupaketti. Tämän jälkeen järjestetään yleensä tapaamien tai workshop, jossa palveluntarjoaja esittelee tarjouksen ja tehdään tarvittavat tarkennukset. Koska asiakkaan kannalta on hyödyllistä kilpailuttaa pilvipalvelut, tarjoukset kannattaa pyytää usealta palveluntarjoajalta. Tällöin tarjousvaiheessa on tärkeää varata riittävät ja asiantuntevat henkilöresurssit käsittelemään ja neuvottelemaan tarjouksista.

Sopimus

Sopimusneuvotteluissa määritellään tarkkaan, mitä palveluita ja laitteita pilvipalvelu sisältää, mitkä ovat sen tarjoamat tallennus- ym. resurssit ja miten ne hinnoitellaan sekä mikä on aikataulu palvelujen käyttöönotolle.

Käyttöönotto

Käyttöönotto suoritetaan sopimuksessa määritellyssä aikataulussa sisältäen sopimuksen mukaiset palvelut ja mahdolliset palvelun käyttöönottoon liittyvät koulutukset/valmennukset.

Koska pilvipalveluissa on kyse jatkuvasta palvelusta, tehdään tarvittaessa palveluun tarvittavat muutokset esimerkiksi tallennustilan lisäämisen tai uusien palveluiden tarpeen mukaisesti. Tärkeä on myös palveluiden käytön raportoinnin, kehittämisen ja seurannan valvominen sisältäen myös palvelun kustannusten seuraamisen.

Pilvipalvelutarjoukset sisältävät yleensä seuraavat palvelut ja laitteet:

- Tietoliikenneyhteys: Palvelujen kannalta on tärkeää turvallinen ja katkeamaton tietoliikenneyhteys.
- Palomuuri: Hakkereiden ja muiden ulkoisten tunkeutujien hyökkäyksiltä suojaava palomuuri on tärkeä. Tietoturvan kannalta on myös tärkeä riittävän tehokas virustorjunta.

- Kytkin (engl. Network switch) on laite, joka yhdistää pakettikytkentäisen paikallisverkon osia. Kytkimillä korvataan yleensä moniporttitoistin, eli keskitin (engl. hub), koska se välittää liikennettä tehokkaammin.
- Sähkö: Keskeytymätön ja riittävä sähkön saanti on turvattava joko aggregaateilla tai varavoimalaitoksella mahdollisten sähkönjakelussa tapahtuvien häiriöiden varalta.
- UPS (Uninterruptible Power Supply) eli keskeytymätön virransyöttö on järjestelmä tai laite, jonka tehtävä on taata tasainen virransyöttö lyhyissä katkoksissa ja syöttöjännitteen epätasaisuuksissa. UPS liitetään virtalähteen ja virtaa käyttävän laitteen (esimerkiksi tietokoneen) väliin.
- Suoritin tai prosessori (engl. Central Processing Unit eli CPU).
- Palvelin (server) ja sen ylläpito.
- Varmistukset: varmuuskopioinnin järjestäminen on oleellisen tärkeää tietoturvan kannalta.

Pilvipalvelujen hinnoittelusta

Pilvipalveluissa on kyse laajan palvelupaketin ostamisesta sisältäen palveluntarjoajan konesalin infrastruktuurin ja tallennustilan hyödyntämisestä ja vuokraamisesta ostajan käyttöön. Palveluntarjoajat odottavat perusteellista tarjousten valmistelua. Tästä syystä tarjousten valmistelu ja saaminen vaatii laajemman asiantuntijajoukon osallistumista ja laajempaa valmisteluprosessia tarjousten valmisteluun ja käsittelyyn kuin insinöörityön tekijällä on ollut mahdollista tässä työssä. Hinnoitteluun vaikuttaa oleellisesti palvelun ostajan tarvitseman palvelun laajuus ja monipuolisuus. Tarjouspyynnöt tulee myös tehdä tietyn organisaation nimissä. Tästä syystä hinnoitteluesimerkit perustuvat indikatiivisiin hintoihin, joita saatiin kyselyn vastanneilta palveluntarjoajilta. Pilvipalvelut eivät myöskään toimeksiantajan toimeksiannossa ole ensimmäiseksi priorisoitu vaihtoehto.

Kyselyyn vastanneiden palveluntarjoajien edullisempien pilvipalveluvaihtoehtojen hintahaarukka on 8.500 €/kk – 12.500 €/kk välillä, mikä vuositasolla tarkoittaa 102.000 € – 150.000 €.

4.3 Euroopan avoimen tieteen pilvipalvelu (EOSC)

EU:n kaikille tutkijoille on tulossa Euroopan avoimen tieteen pilvipalvelu (EOSC), josta Euroopan komissio järjesti 12. kesäkuuta 2018 European Open Science Cloud -huippukokouksen Brysselissä. (CSC 2018.) Palvelun tarkoituksena on:

> tarjota kaikille EU:n tutkijoille turvallinen virtuaalinen toimintaympäristö, joka sisältää maksuttomia, avoimia ja saumattomia palveluita datan tallentamiseen, hallinnointiin, analysointiin, jakamiseen ja uudelleenkäyttöön tiedealojen välillä. (CSC 2018.)

> EOSC yhdistää olemassa olevat ja uudet temaattiset datainfrastruktuurit, tutkimukseen tarkoitetut pilvipalvelut sekä liittää yhteen horisontaalisia sähköisiä infrastruktuureja. Se myös kokoaa nykyisin hajallaan olevia palveluita ja ad hoc -ratkaisuja. (CSC 2018.)

Euroopan komission ehdotuksen perusteella tuli perustaa väliaikainen hallintoneuvosto pilvipalvelulle 2019 loppuun mennessä. Komissio keskustelee myös jäsenvaltioiden ja eri sidosryhmien kanssa Euroopan avoimen tieteen pilvipalvelun toteuttamisen etenemissuunnitelman laatimiseksi. Pilvipalvelu pitäisi toteutua vuoteen 2020 mennessä. (CSC 2018.)

Euroopan avoimen tieteen pilvipalvelun käytöstä tulisi yliopistotasolla tehdä päätös, jotta sen kaikki yksiköt voisivat sitä hyödyntää tutkimuksissaan ja kansainvälisessä yhteistyössä.

5 Johtopäätökset ja pohdinta

Internetin ja multimedian nopean kehityksen myötä tiedon saatavuus ja määrä on nopeasti lisääntynyt. Myös kommunikointimenetelmät ja kanavat kehittyvät nopeasti. Tämän seurauksena verkossa liikkuvan ja tallennettavan tiedon ja tiedostojen määrä ja suuruus kasvaa nopeasti. Pilvipalvelut ovat yleistyneet nopeasti 2010-luvulta alkaen ja vastaavasti pilvipalveluina tarjottavat palvelut ovat kehittyneet nopeasti. Monesti niin yritysten kuin yliopistojen ja tutkimuslaitosten tutkimus- ja tuotekehityshankkeet perustuvat kansainväliseen yhteistyöhön. Tällöin tarvitaan yhteisiä tallennus- ja työskentelyalustoja, joihin tiedostoja voidaan tallentaa ja joissa niitä voidaan yhteisesti työstää. Tällöin entistä

tärkeämmäksi tekijäksi on tullut tallennuskapasiteetin joustavuus, skaalautuvuus ja turvallisuus.

Tässä insinöörityössä selvitettiin Rakennetun ympäristön mittauksen ja mallinnuksen instituutin toimeksiannosta toiminnallisuudeltaan ja skaalattavuudeltaan riittävän suurta ja nopeaa tallennusjärjestelmää 3D-mittausaineistojen käsittelyyn ja arkistointiin. Selvityksen pohjalta tämänhetkisen tarpeen mukainen hinnaltaan edullisin vaihtoehto tallennusjärjestelmäksi on yksityinen verkkolevypalvelin. Sen etuna on, että tallennukset sijaitsevat omissa tiloissa ja ovat siten tietoturvan osalta omassa valvonnassa. Heikkoutena on, että tallennuskapasiteettia joudutaan hankkimaan maksimitarpeen mukaan, vaikka kyseessä olisi lyhytaikainen tarve.

Koska samanlaisia tarpeita on varmasti myös muilla yliopiston yksiköillä, kannattasi yliopistotasolla selvittää, mitkä ovat lähitulevaisuuden tiedontallennus- ja siirtokapasiteetin tarpeet, miten ne jaksottuvat eri ajanjaksoille ja onko kyse pitkäaikaisista tallennustarpeista vai lyhytkestoisista tallennus- ja tiedonsiirtopiikeistä. Yksityisen pilvipalvelun etuna on, että siinä maksetaan vain kunkin hetkisen tallennuskapasiteetin käytön mukaan, eikä konesalin infrastruktuuriin tarvitse sijoittaa. Tämä voi soveltua esim. projektirahoituksella tehtäviin tutkimushankkeisiin, kun tiedon tallennus- ja siirtokustannuksia voidaan ohjata projekteille. Hybridipilven etuna on, että tietosuojan kannalta tärkeät materiaalit voidaan tallentaa omassa konesalissa tai yksityisessä pilvessä ja muuten voidaan hyödyntää julkisten pilvipalveluiden alustoja ja palveluita tarpeen mukaan erillisessä pilvessä.

Mielenkiintoinen uusi EU:n tutkijoille suunnittelema hanke on Euroopan avoimen tieteen pilvipalvelu (EOSC). Hankkeen tavoitteena on kehittää kaikille EU:n tutkijoille turvallinen virtuaalinen toimintaympäristö, joka sisältää maksuttomia, avoimia ja saumattomia palveluita datan tallentamiseen, hallinnointiin, analysointiin, jakamiseen ja uudelleenkäyttöön tieteenalojen välillä. (CSC 2018.) Tavoitteena on, että se olisi tutkijoiden käytössä jo vuonna 2020.

Lähteet

Chaudhary, S., Somani, G., & Buyya, R. (Eds.). (2017). Research Advances in Cloud Computing. Springer Singapore.

Cloud Security Alliance. (2016) The treacherous 12 - Cloud Computing Top Threats in 2016. https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf. Viitattu 11.3.2019.

Cloud Security Alliance. (2017). The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights. https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf.Viitattu 13.3.2019.

CSC. (2019). Euroopan avoimen tieteen pilvipalvelu tarvitsee jäsenvaltioiden sitoutumista. https://www.csc.fi/fi/-/euroopan-avoimen-tieteen-pilvipalvelu-tarvitsee-jasenvaltioiden-sitoutumista. Viitattu 4.3.2019.

Data Storage, File Services | Aalto IT Help. (2019). Aalto-yliopisto. Verkkoaineisto. https://it.aalto.fi/instructions/data-storage-file-services. Viitattu 25.2.2019.

Den Haan, J. (2013) The cloud landscape described, categorized, and compared. The Enterprise Architect, blog; www.theenterprisearchitect.eu/blog/2013/10/12/the-cloud-landscape-described-categorized-and-compared. Viitattu 28.2.2019.

Fehling, C., Leymann, F., Retter, R., Schupeck, W., & Arbitter, P. (2014). Cloud computing patterns: fundamentals to design, build, and manage cloud applications. Springer Science & Business Media.

Giordanelli, R., & Mastroianni, C. (2010). The cloud computing paradigm: Characteristics, opportunities and research issues. Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR).

Haikumind. (2011). Cloud Computing: Acronyms (IaaS, PaaS and SaaS). Viitattu 28.2.2019 http://www.haikumind.com/cloud-computing-acronyms-iaas-paas-and-saas/

Heino, P. (2010). Pilvipalvelut. Helsinki: Talentum.

Juniper. (2018).Cloud Service Provider Reduces Impact of Global Denial-of-Service Attacks by Over 90 Percent https://junipernetworks.lookbookhq.com/c/Unified-SecurityVendor-A2?x=91-Fdh. Viitattu 2.3.2019.

Kaartinen, H., Hyyppä, J., Hyyppä, H., Ojala, T., Visala, A., Alho, P., ... & Vaaja, M. (2015). Osaamispohjainen kasvu 3D-digitalisaation, robotiikan, paikkatiedon ja kuvankäsittelyn sekä-laskennan yhdistetyssä teknologiamurroksessa (COMBAT-konsortio).

Tilannekuvaraportti 2015. https://www.aka.fi/globalassets/33stn/tilannekuvaraportit/stn2015-hankkeet/tech-kaartinen-tilannekuvaraportti_combat.pdf.Viitattu 28.3.2019.

Kavis, M. J. (2014). Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS). John Wiley & Sons.

Komissio, E. (2014). KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE. Kohti menestyvää datavetoista taloutta.

Komissio, E. (2012). KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE. Pilvipalvelujen potentiaali käyttöön Euroopassa.

Loikkanen, V., & Tyynelä, N. (2016). Pelottava vai kiehtova big data?–# Digisaatioviikko siirtyi pilvipalveluihin.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Miyachi, C. (2018). What is “Cloud”? It is time to update the NIST definition?. IEEE Cloud Computing, (3), 6-11.

Oza, N., Karppinen, K., & Savola, R. (2010, November). User Experience and Security in the Cloud--An Empirical Study in the Finnish Cloud Consortium. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 621-628). IEEE.

Pervilä, M. (2017). Monen pilvitarjoajan mallit jyräävät hybridipilven yli. Tivi. https://www.tivi.fi/CIO/monen-pilvitarjoajan-mallit-jyraavat-hybridipilven-yli-6678978. Viitattu 20.2.2019.

Priyanka, S. P. (2014). Cloud computing: Overview, issues, challenges, applications and future research direction. Industrial Science ISSN: 2347-5420.

Rakennetun ympäristön mittauksen ja mallinnuksen instituutti MeMo. (2019). Verkkoaineisto. https://www.aalto.fi/fi/rakennetun-ympariston-laitos/rakennetun-ympariston-mittauksen-ja-mallinnuksen-instituutti-memo. Viitattu 8.3.2019.

Ranger, S. (2018). What is cloud computing? Everything you need to know about the cloud, explained. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/. Viitattu 28.2.2019.

Rountree, D., & Castrillo, I. (2013). The basics of cloud computing: Understanding the fundamentals of cloud computing in theory and practice. Newnes.

Rousku, K. (2014). Kyberturvaopas–Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Ruparelia, N. B., & Ruparelia, N. (2016). Cloud computing. Mit Press.

Salo, I. (2014). Big data & pilvipalvelut. Jyväskylä: Docendo.

Salo, I. (2010). Cloud computing - palvelut verkossa. WSOYpro.

Salo, I. (2012). Hyötyä pilvipalveluista. Jyväskylä: Docendo.

Schubert, L., & Jeffery, K. (2012). Advances in clouds. Report of the Cloud Computing Expert Working Group. European Commission.

Sheehan, M. (2008). Cloud computing expo: introducing the cloud pyramid. Clod Computing Journal.

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

Srinivasan, S. (2014). Cloud computing basics. Springer. 142 s. ISBN: 9781461476993.

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

Suomen Standardisoimisliitto SFS ry. (2019). https://www.sfs.fi/. Viitattu 29.3.2019.

Tietokehitys. (2019) Verkkolevy. http://tietokehitys.fi/verkkolevy-pilvitallennus-varmuuskopiointi.html. Viitattu 5.3.2019.

TOIMI FIKSUSTI PILVESSÄ. (2019) Yritysten pilvipalvelut tutuksi Ainan oppaan avulla. (2019) http://www.aina.fi/opas-pilveen. Viitattu 1.3.2019.

Tynan, D. (2017). The 8 biggest IT management mistakes. https://www.cio.com/article/3240943/leadership-management/biggest-it-management-mistakes.html. Viitattu 1.3.2019.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. Future Generation Computer Systems, 79, 849-86.

Viestintävirasto. 2014. Pilvipalveluiden_tietoturva_organisaatioille.pdf. https://kybertur-vallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaati-oille.pdf. Viitattu 28.2.2019.

Violino, B. (2018) The dirty dozen: 12 top cloud security threats for 2018. https://www.csoonline.com/article/3043030/12-top-cloud-security-threats-for-2018.html. Viitattu 13.3.2019.

ZDNET. (2019) Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move; Salesforce dominates SaaS. https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-sa-lesforce-dominates-saas/. Viitattu 5.3.2019.