

Student name: Eliel Selmgren

Email address (prefer your @students.oamk.fi email if you have such address): t0seel00@students.oamk.fi

Save the final version of this document as PDF and submit it for peer reviews via Moodle's workshop tool before the deadline. Last course week is for peer reviews.

Week 1

Question 1: Describe with short examples: SaaS, PaaS and IaaS

Answer 1:

IaaS (Infrastructure as a service)

- IaaS-palvelussa palveluntuottaja tarjoaa infrastruktuuria palveluna asiakkaalle tyypillisesti niin, että asiakkaan käyttöön tarjotaan web-pohjainen hallintaliittymä, jonka kautta voi itse perustaa tarvittavia palvelimia sekä hallinnoida palvelimen kapasiteettia, verkkoyhteyksiä ja palomuurauksia. Tärkeä huomioitava asia on, että IaaS-mallissa palveluntuottajan vastuu ulottuu vain alustoihin, joita käytetään kapasiteetin tuottamiseen. Malli vaatii paljon osaamista ostajalta. Palvelunkäyttäjän vastuulle jäävät siis kaikki palvelimet, konfiguraatiot ja hallinnointi. IaaS-palvelut sopivat hyvin organisaatiolle, jolla on oma IT-osasto tai -porukka tai tarvittavaa osaamista muuta kautta. Palvelun käyttäjä huolehtii siis itse palvelimien tietoturvasta, palomuurauksesta sekä asennuksista ja ohjelmistoista.
- Esimerkkejä IaaS -palveluista ovat: Microsoft Azure, Google Compute Engine ja IBM SmartCloud Enterprise.

SaaS (Software as a Service)

- SaaS-palvelut tarjoavat kokonaisuudessa ohjelmiston palveluna, tästä hyvänä esimerkkinä toimii sähköpostipalvelu. SaaS-palvelussa palveluntuottaja vastaa kokonaisvaltaisesti koko ohjelmistosta. Tyypillisesti SaaS-palveluita käytetään web-selaimen kautta.
- Palvelunkäyttäjä saa automaattisesti käyttöön uudet versiot ja mm. lisenssit sisältyvät kokonaispalvelun hintaan.
- Ohjelmistot palveluna ovat vaivaton ja kustannustehokas tapa ostaa ohjelmistot valmiissa paketissa. Suurimmat kustannussäästöt saadaan vähentyneestä ylläpitotarpeesta, josta siis palveluntuottaja huolehtii automaattisesti.
- Organisaatiossa, jossa on käytössä useita eri SaaS-palveluita, saattaa muodostua ongelmaksi se, että käyttäjillä on jokaiseen palveluun eri tunnukset. Tämä on ratkaistu monessa palveluista niin, että tarjotaan ns. kertakirjautumisvaihtoehto (Single sign-on, SSO), jonka avulla voidaan hyödyntää olemassa olevia järjestelmiä, jolloin riittää, että käyttäjä kirjautuu yhteen palveluun.
- Esimerkkejä SaaS palvelusta ovat: Office 365, Google Apps collection, SAP ja Dropbox.

PaaS (Platform as a Service)

- PaaSista puhutaan kun palveluntuottaja tarjoaa palveluna sovelluspalveluita, jotka ovat paketoitu helposti käyttöön otettavaan muotoon. Sovelluspalveluita tarjotaan yleisesti ottaen ohjelmistokehityksen käyttöön/tarpeisiin. Käytännössä palvelunkäyttäjä voi tilata sopivan alustan, maksaa joustavasti käyttöön perustuen ja siirtää sovelluksensa palveluun.

- Tyypillisesti PaaS-alustassa palveluntarjoaja tarjoaa web käyttöliittymän lisäksi vaihtoehtoisia tapoja muodostaa yhteyksiä palveluihin kuten suorat yhteydet palvelimiin (FTP/SFTP, SSH), komentorivityökalut (CLI) ja API-rajapinta, jonka kautta voidaan automatisoida toimenpiteitä ja vaikkapa tuoda palvelut osaksi omaa sovellusta tai itsepalvelumallia.
- PaaS laajentaa palveluntuottajan vastuulle myös käyttöjärjestelmä- ja varusohjelmisto tasot. Palvelunkäyttäjän vastuulle jää oman sovelluksen tietoturva. Käytännössä tämä tarkoittaa sitä, että palvelunkäyttäjän tulee huolehtia itse sovellustason päivityksestä sekä tietoturvasta.
- Yksinkertaisimmillaan tämä tarkoittaa, että jos laitat PaaS-alustaan verkkosivut, jossa on alustana julkaisujärjestelmä (esimerkiksi WordPress, Drupal) huolehdi itse julkaisujärjestelmään liittyvistä päivityksistä ja tietoturvasta.
- Esimerkkejä PaaS palveluista ovat: Amazon Web Services, Google App Engine ja Heroku

Question 2: Describe with short examples: Private cloud, public cloud and hybrid cloud

Answer 2:

Public cloud

- Julkinen pilvi, joka tunnetaan myös nimellä julkinen pilvi, on palveluntarjoajan verkon kautta vapaasti ja avoimesti suuren yleisön käytettävissä. Vastaavat palveluntarjoajat, jotka tässä yhteydessä tunnetaan ensisijaisesti palveluntarjoajina, kuten Amazon, Google tai Microsoft tarjoavat pilvipalvelunsa infrastruktuuriin. Käyttäjien pääsy Internetin kautta tapahtuu yleensä ilman erityisiä rajoituksia. Julkisessa pilvipalvelussa käyttäjällä ei ole tietoa eikä määräysvaltaa siitä, missä ja miten palveluntarjoaja tarkalleen ottaen toimii. On myös tärkeää tietää, että kaikilla julkisen pilven käyttäjillä on pääsy samaan infrastruktuuripooliin. Kokoonpano sekä taattu turvallisuus ja käyttäjän käytettävissä olevat vaihtoehdot pilvipalvelussa rajoittuvat vain olennaiseen. Vastineeksi julkisen pilven käyttäjät hyötyvät massaliiketoiminnasta. Tämä johtuu siitä, että kyseinen palveluntarjoaja siirtää infrastruktuurin rahoituskustannukset suurelle määrälle käyttäjiä. Kukin henkilö maksaa alhaiset kustannukset maksuperusteisesti. Koska palvelimia on lähes rajattomasti, julkiset pilvet ovat myös erittäin luotettavia. Jos jokin komponentti vikaantuu, pilvi voi käyttää muita komponentteja hyvin lyhyessä ajassa.

Private cloud

- Yksityiset pilvet ovat yritysten tai organisaatioiden itse ylläpitämiä ja organisoimia palveluja. Usein yritykset, viranomaiset tai laitokset suosivat näitä yksityisiä pilvipalveluja tietosuojasyistä tai tietotekniikkansa turvallisuuden vuoksi, ja ne antavat pääsyn niihin vain omille työntekijöilleen. Valtuutettuja käyttäjiä voivat olla myös asiakkaat, liikekumppanit tai toimittajat. Yksityisten pilvien suunnittelu ja isännöinti voidaan tehdä sisäisesti. Tällöin tietotekniikka sijaitsee oman organisaation sisällä, ja sitä voidaan käyttää sisäisen verkon eli intranetin kautta. Myös ulkoinen hosting on mahdollista. Ulkoisesti isännöidyt eli kolmannen osapuolen isännöimät pilvet ovat yhtä yksinoikeudellisia kuin sisäiset yksityiset pilvet, ja ne tarjoavat siten turvallisuuden, joka julkisista pilvistä puuttuu. Toisaalta yksityisten pilvien kustannukset ovat korkeammat. Ulkoisen isännöinnin tarjoajat ovat erikoistuneita yrityksiä ja yhä useammin myös teleyrityksiä.

Hybrid cloud

- Jos julkiset ja yksityiset pilvet yhdistetään, puhutaan hybridipilvistä. Tässä hybridimuodossa tietyt palvelut voivat toimia internetissä julkisten palveluntarjoajien kanssa, kun taas toiset sovellukset pysyvät yrityksessä tietosuojasyistä. Haasteena on erottaa liiketoimintaprosessit tietosuojaajaratellen kriittisiin ja vähemmän kriittisiin prosesseihin. Kaikkien resurssien joustavan käytön lisäksi hybridipilven etuja ovat hyvä skaalautuvuus ja alhaisemmat kustannukset verrattuna puhtaaseen yksityiseen pilveen. Pilvipalvelun hallinnointiin liittyy kuitenkin enemmän työtä. On myös olemassa riski, että Tiedot joutua väärään pilveen on suurempi. Lisäksi hallinnointityö on hybridipilvessä suurempi.

Question 3: Describe usual cloud service related privacy and security issues, worries and challenges

Answer 3: Pilvipalveluiden yksityisyys ja turvallisuus

Ongelmat

- Kyberturvallisuuden suhteen datakeskukset voivat tarjota suurempaa turvaa, mutta tietosuojan suhteen pilvipalvelut voivat olla ongelmallisia. Syynä on se, että kun arkaluonteinen tieto siirtyy pilveen, organisaatio menettää osan heidän kontrollistaan tietoon, sillä pilvi on ulkopuolinen ympäristö jota ylläpitää kolmas osapuoli. Huolimatta siitä onko pilvipalvelu IaaS, PaaS tai SaaS, asiakkaalle jää vastuu heidän tiedon ja käyttäjien pääsyn turvaamisesta.
- Ongelmana pilvipalveluissa on myös se, että tietopalvelimien paikka määrittää sen, että mikä tietosuojalaki pätee arkaluonteiseen tietoon. Se voi myös tarkoittaa, että tietopalvelimien täytyy noudattaa sen maan tietosuojalakia missä ne sijaitsevat, mutta nämä lait eivät välttämättä päde niin maihin joista data on alkujaan lähtöisin. Riippuen laista, yritykset saattavat tarvita erilisen suostumuksen rekisteröityneeltä keräysmään ulkopuolelle.
- Yhtenä esimerkkinä on, kun Amazonin Yhdysvaltojen itärannikon datakeskukseen tuli sähkökatkos ja myös varageneraattoreihin tuli vikaa. Lopputuloksena osa asiakkaiden datasta katosi ja sitä ei saatu enää takaisin. Eli pilvipalveluun tallentaminen ei tarkoita, että tietoja ei tarvitse varmuuskopioida muualle.

Huolet

- Suurimpina pilvipalveluiden turvallisuushuolina tutkimuslaitos Forrester listasi
 - Turvallisuus ja yksityisyys
 - Asetusten ja standardien mukaisuus
 - Lakeihin ja sopimuksiin liittyvät seikat.
- Julkisissa pilvissä yksityisyys ja turvallisuus on suurin huoli, sillä tuolloin tiedot ja sovellukset ovat hajautettu ympäri maailmaa ja useampi yritys/henkilö käyttää samoja palveluja.
- Yksityisen pilven huolia ovat taas esimerkiksi ulkopuolisen pilvipalvelun tarjoajan henkilökunnan pääsy tietoihin, varautuminen odottamattomiin ongelmiin ja varmuus palvelun toiminnan jatkuvuudesta.

Haasteet

- Esimerkiksi EU:n yleisellä tietosuoja-asetuksella (GDPR) tai Kalifornian yksityisyyden suojaa koskevalla lailla (CCPA) on ekstraterritoriaalisuus lausekkeet. Tämä tarkoittaa, että asetus/laki pätee huolimatta siitä, missä yritys tai palveluntuottaja sijaitsee. Eli jos yritys kerää henkilökohtaisia tietoja EU:n tai Kaliforniaan rekisteröityneeltä, datan turvatoimien täytyy noudattaa GDPR:ää tai CCPA:ta. Tämä tuottaa omia haasteita palvelun tuottajille.

- Auditoitavuus tuo myös haasteita, sillä pienellä toimijalla ei ole resursseja auditoida pilvipalvelun tarjoajaa. Heidän on siis luotettava dokumentaatioonsa tai jo aikaisemmin tehtyihin auditointeihin.
- Kiteytettynä tiedon sijainti, saatavuus ja tietoturvan sekä tietosujan tason auditointi aiheuttavat erityisiä haasteita pilvipalvelujen käyttöön

Question 4: What is “shadow IT” and why it is causing significant troubles for many organisations and enterprises? Especially cloud shadow IT. Use examples

Answer 4: Ympäriämme on nykyään lukuisia teknisiä apuvälineitä, jotka voidaan kaikki yhdistää pilvipalveluun. Kyse voi olla esimerkiksi sähköpostista, asiakirjoista, tiedostoista, musiikista, tietokoneista, tableteista, ohjelmista ja puhelimesta.

Pilvipalveluteknikka on yleistynyt, ja siitä on tullut niin helppokäyttöistä ja laadukasta, että on vaikea välttää tietojen lähettämistä pilveen. Moni on varmasti lähettänyt tietoja pilvipalveluun, vaikka lähettäminen on saattanut olla tahatonta.

Oletko esimerkiksi huomannut, että puhelimesta olevat kuvat ilmestyvät työtietokoneelle, mutta et tiedä, miten? Niin voi käydä yksinkertaisesti silloin, jos puhelin ladataan työtietokoneen kautta ja tietty valintaruutu valitaan puhelimen näytöllä. Oletko napsauttanut pilvipainiketta, joka ilmestyi PDF-asiakirjan pikavalikkoon? Arvaa, minne asiakirjasi silloin päättyy?

Useimmilla on yksityinen sähköpostitili esimerkiksi Googlen palvelussa. Jos työasiakirjan avaa tai tallentaa siellä, se tallennetaan Google Drive -pilvipalveluun. Jos ostat Applen iPhone, sinun on hankittava iCloud-tili puhelimen käyttämiseksi. Kaikki kuvasi kopioidaan automaattisesti pilveen, jos tallennustila ei ole täynnä. Jos otat kuvan työasiakirjasta, kuva tallennetaan sekä puhelimeesi että Applen palveluun. Mitä enemmän varjo-IT:tä syntyy, sitä enemmän syntyy dataa eri paikkoihin. Tästä syntyy useita haittoja, **tietoturvan huolehtiminen** vaikeutuu tiedon levitessä ja **tietoa myös hukkuu**. Työntekijät erilaisissa rooleissa toimivat osittaisen tiedon varassa ja tämä **heikentää tehokkuutta** sekä vaikeuttaa työn tekemistä.

Joissakin tapauksissa voi itse asiassa olla parempi valita pilvipalveluiden tarjoaja kuin vähemmän hyvä tietoturvaratkaisu omassa yrityksessä. Se johtuu siitä, että ammattimaisten pilvipalveluiden tarjoajien on noudatettava tiettyjä säännöstöjä, muuten niitä ei pidetä vakavasti otettavana vaihtoehtona markkinoilla.

Week 2

Question 1: Describe what is serverless architecture?

Answer 1: Serverless on järjestelmäarkkitehtuurimalli, jonka keskeisenä tavoitteena on siirtää palvelimien hallinnan, niiden provisioinnin sekä skaalautumisen suunnittelun aiheuttama operatiivinen kuorma ohjelmiston tuottajalta (pilvipalvelun käyttäjältä) palveluntarjoajalle. Järjestelmä ei näydy serverless-mallissa kehittäjälle enää kokoelmana palvelimia ja näillä suoritettavia monoliittisia ohjelmistoja. Sen sijaan puhutaan tapahtumista (event) ja näitä käsittelevistä tilattomista funktioista (FaaS, Function as a Service tai fPaaS, Function Platform as a Service), joita suoritetaan tarvittaessa, tapahtumiin reagoiden. Kyseessä on siis abstraktiotason nosto tilanteeseen, jossa järjestelmä rakentuu koodista palvelimien sijaan. Tästä seuraa, että kehittäjät voivat siirtää resurssejaan infrastruktuurin hallinnasta ohjelmiston liiketoimintalogiikan kehittämiseen

Lähestymistapa tuo mukanaan kehittäjäkokemuksen suoraviivaistamisen lisäksi muitakin etuja. Jatkuvasti suorituksessa olevat palvelinsovellukset on mallissa korvattu lyhytkestoisilla funktiosuorituksilla, ja käyttäjää laskutetaan vain tämän funktiokutsun vaatiman prosessointiajan mukaan. Tyhjäkäynnistä ei siis aiheudu kustannuksia, sillä sitä ei mallin määritelmän mukaan synny. Tämän lisäksi perinteisiin palvelinratkaisuihin verrattuna serverlessalustojen hinnoittelu on myös merkittävästi hienojakoisempaa. Siinä missä konesalista vuokrattu fyysinen tai virtuaal

Question 2: Compare application containers to microservices

Answer 2: Ensinnäkin kontteja ja mikropalveluita voidaan käyttää yhdessä tai erikseen. Sovellus voi olla monoliittisena palveluratkaisuna, jossa kaikki tarvittava sisältyy yhteen suoritettavaan funktioon; on myös mahdollista, että tämä suurempi palvelu on itse asiassa kokoelma mikropalveluita ilman konttia näkyvissä. Säiliöt voivat itsessään sisältää mikropalveluita – ja mikropalvelu voi sisältää kontin, joka helpottaa ydintoimintoa, jota ei voida enää vähentää.

Toiseksi jokaisessa toteutuksessa on etuja ja haittoja. Mikropalvelut tarjoavat entistä laajennettavissa olevia ja skaalautuvia ratkaisuja, koska jokainen palvelu voi liikkua ketterästi eri segmenttien ja alustojen välillä. Tämä tarkoittaa myös sitä, että mikropalvelut voivat olla erittäin kevyitä muihin ratkaisuihin verrattuna, koska jokainen uusi mikropalvelu on vain osa suurempaa massaa sen sijaan, että se vaatisi kokonaan uuden kokonaisuuden luomista omilla resursseillaan.

Mikropalveluissa on kuitenkin joitain haittoja. Erityisesti mikropalveluverkoista voi tulla hyvin monimutkaisia. Koska jokainen mikropalvelu on olennaisesti osa suurempaa palveluekosysteemiä, jokainen yksittäinen mikropalvelu on rakennettava ja suunniteltava monimutkaisen kontekstuaalisen järjestelmän sisällä.

Säiliöillä sen sijaan on suurin etu siinä, että rakenne on erilainen. Koska kaikki on rakennettu omaan konttiinsa ja kaikki tarvittavat resurssit on niputettu toimintoon, kaikki voidaan rakentaa omaksi erilliseksi muotokseen ja virtauksensa. Tämä on valtava etu kehityksen yksinkertaisuuden kannalta, koska sinun tarvitsee huolehtia vain itse säiliöstä.






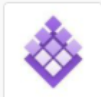


Valitettavasti tämä tarkoittaa myös suurta tehottomuutta. Useat konttijärjestelmät tarkoittavat päällekkäisiä resursseja, päällekkäisiä toimintoja ja joissakin tapauksissa täysin päällekkäisiä palveluita. Tämä tarkoittaa, että laajennettavuutta ja joustavuutta myönnetään huomattavasti vähemmän resurssien suhteen, vaikka kehitettäisiinkin jonkin verran laajennettavuutta ja joustavuutta kehitysmalleissa.

Question 3: Describe shortly what is Kubernetes and what alternatives are there?

Answer 3: Kubernetes on avoimen lähdekoodin orkestrointijärjestelmä Docker-säiliöille. Se käsittelee aikataulutuksen laskentaklusterin solmuille ja hallitsee aktiivisesti työkuormia varmistaakseen, että niiden tila vastaa käyttäjien ilmoittamia aikomuksia.

Tässä vaihtoehtoisia järjestelmiä Kubernetesille:

TOP ALTERNATIVES TO KUBERNETES

























	Docker Swarm Swarm serves the standard Docker API, so any tool which already communicates ...		Nomad Nomad is a cluster manager, designed for both long lived services and short ...
	OpenStack OpenStack is a cloud operating system that controls large pools of compute, ...		Rancher Rancher is an open source container management platform that includes full distributions ...
	Docker Compose With Compose, you define a multi-container application in a single file, then ...		DC/OS Unlike traditional operating systems, DC/OS spans multiple machines within a ...
	Apache Mesos Apache Mesos is a cluster manager that simplifies the complexity of running ...		Docker The Docker Platform is the industry-leading container platform for continuous, ...

Question 4: When and why some organisations use (cloud) VDI/DaaS (here DaaS = Desktop as a Service) solutions? List some DaaS providers and offerings

Answer 4: Desktop as a service eli DaaS on pilvipalveluratkaisu, joka toimittaa virtuaaliset sovellukset ja työpöydät turvallisesti pilvestä mihin tahansa laitteeseen. Tämä hallitun työpöydän virtualisointiratkaisu, jota käytetään turvallisten SaaS- ja vanhojen sovellusten sekä täydellisten Windows-pohjaisten virtuaalisten työasemien tarjoamiseen ja toimittaa ne työntekijöillesi. Ennustettavan jako-tilausmallin avulla DaaS helpottaa skaalatausta tarpeen mukaan. Sitä on helppo hallita ja se yksinkertaistaa monia työpöytäratkaisujen IT-järjestelmänvalvojatehtäviä.

Miksi DaaS? Työntekijät odottavat pääsevänsä työhönsä mistä tahansa millä tahansa laitteella. Yritykset etsivät edullista, yksinkertaista ratkaisua työnsä suorittamiseen tarvittavien sovellusten ja pöytätietokoneiden turvalliseen toimittamiseen. Perinteisiä PC-ympäristöjä rasittavat IT-hallinnan haasteet, jotka vaihtelevat yksinkertaisista työntekijöiden salasanan nollauksista monimutkaisiin tietoturvakorjauksiin ja -päivityksiin. Nämä eivät ainoastaan vie IT-järjestelmänvalvojille arvokasta aikaa, vaan voivat myös vaikuttaa käyttökokemukseen ja rajoittaa tuottavuutta. Vaikka monet asiakkaat ovat siirtymässä virtualisointiin, prosessi vaatii usein pääomasijoituksia ja erityisiä IT-taitoja. Vastauksena monet organisaatiot etsivät yksinkertaistettua ratkaisua, joka toimii operatiivisen kulurakenteen puitteissa. DaaS voi olla vartenotettava vaihtoehto asiakkaille, jotka pitävät VDI:n keskittämisestä, turvallisuudesta ja hallinnasta, mutta ovat kiinnostuneita siitä, että ammattimaisen organisaation yksinkertaisuus suorittaa työpöydän perushallinta heidän puolestaan.

Tässä muutama DaaS palveluntuottaja:

	NetSuite The World's Leading, Most Deployed Cloud ERP Solution See more details >	 4.1 READ REVIEWS	VISIT WEBSITE
	monday.com Project Management Made Easy See more details >	 4.6 READ REVIEWS	VISIT WEBSITE
	Jira Project & Issue Tracking Software - See why we're #1! See more details >	 4.4 READ REVIEWS	VISIT WEBSITE
	CAFLOW Business management system for small and mid-size companies. See more details >	 5.0 READ REVIEWS	VISIT WEBSITE
	Scoro All-in-one work management software. See more details >	 4.6 READ REVIEWS	VISIT WEBSITE
	Bitrix24 100% free CRM, collaboration and communication tool suite See more details >	 4.0 READ REVIEWS	VISIT WEBSITE
	Odoo Full Suite of Integrated Business Apps See more details >	 4.2 READ REVIEWS	VISIT WEBSITE
	Smartsheet An online work execution platform for any size organization. See more details >	 4.5 READ REVIEWS	VISIT WEBSITE
	Mindbody Health & Wellness Business Management Software See more details >	 4.0 READ REVIEWS	VISIT WEBSITE
	ClickUp Project management, task tracking, & professional goal tools See more details >	 4.7 READ REVIEWS	VISIT WEBSITE
	todo.vu Productivity suite for freelancers & SMBs See more details >	 4.4 READ REVIEWS	VISIT WEBSITE
	Exercise.com Fitness business software for gyms and fitness professionals See more details >	 4.8 READ REVIEWS	VISIT WEBSITE

Week 3

Question 1: Describe reasons why so many (most?) companies are using cloud based email and calendar services?

Answer 1:

Kun yritys käyttää pilvipohjaista sähköpostijärjestelmää, yrityssähköposti sijaitsee ulkopuolisessa, erittäin suojatussa paikassa, mikä tekee siitä turvallisemman kuin jos ne olisivat paikan päällä. Pilvipohjainen sähköpostipalveluntarjoaja, kuten Microsoft, voi käyttää paljon enemmän resursseja toimitilojensa turvaamiseen kuin useimmat muut organisaatiot.

Question 2: Your thoughts about when to maintain your own web server and when to use SaaS/PaaS/IaaS to provide web services?

Answer 2:

Startup-yritykset ja pienet yritykset voivat mieluummin käyttää **SaaS/PaaS/IaaS** välttääkseen aikaa ja rahaa laitteiston ja ohjelmiston ostamiseen ja luomiseen. Suuremmat yritykset saattavat haluta säilyttää sovelluksensa ja infrastruktuurinsa täydellisen hallinnan, mutta ne haluavat ostaa vain sen, mitä he todella kuluttavat tai tarvitsevat.

Question 3: Select and describe 2-3 well-known Amazon S3 data leak incidents. What went wrong? List some automated S3 bucket search engines and attack tools

Answer 3:

- Henkilötietoja noin 198 miljoonasta amerikkalaisesta äänestäjästä:
The Lowdown: Republikaanipuolueen tukema suurdatayritys Deep Root Analytics vaaransi henkilökohtaiset tiedot ja äänestäjien profiloititiedot tallentamalla ne laajalle avoimelle S3-palvelimelle. Tiedon aarrearkku yhdisti julkisesti saatavilla olevat äänestäjätiedot ylimääräisiin markkinatutkimustietoihin saadakseen matriiseja yksittäisistä äänestäjistä heidän äänestyskäyttäytymisensä todennäköisyydestä tulevilla vaaleilla.
- Henkilökohtaisia tunnistetietoja 6 miljoonasta ihmisestä ja arkaluonteisia yritystietoja IT-järjestelmistä, mukaan lukien kirjautumistiedot:
Huonosti suojatut S3-järjestelmät pursuivat Verizonin takaosaan ei kerran vaan kaksi kertaa viime vuonna parilla korkean profiilin datan valotuksella. Ensimmäinen oli 6 miljoonan asiakastietueen vuoto, kun Verizon-kumppanin Nice Systemsin työntekijä asetti asiakaspalvelupuheluiden lokitiedot julkisesti saatavilla olevalle S3-palvelimelle. Ennen kuin kukaan ehti antaa Verizonille epäilyksen kumppanin toimista, muutama kuukausi myöhemmin toinen S3-tapaus iski vielä lähemmäs kotia. Tällä kertaa Verizonin insinööri loi epäluotettavan ja epävarman S3-tilin, joka sisälsi joukon omaa teknistä tietoa. Se sisälsi tiedot yrityksen väliohjelmistosta, sisäisestä viestinnästä, tuotantolokeista, palvelinarkkitehtuurista ja kirjautumistiedoista.
- Pentagonin online-tiedonkeruutapojen yksityiskohtien paljastumiset:
Tietoa paljastui teratavujen verran vakoiluarkistosta, ansioluettelo tiedustelutehtäviin, mukaanlukien turvallisuus selvitykset ja toimintahistoria, vultuustiedot ja metatiedot viraston sisäisestä tiedustelutietojen jakamisalustasta. Vuodot tapahtuivat huonosti konfiguroitujen S3 ämpäreiden vuoksi.

Question 4: What would a mid-size company store to the Amazon Glacier? What not? Why? What other large cloud backup or mass storage providers are there?

Answer 4: Amazon Glacier on hyvä paikka tietojen arkistointiin ja pitkäaikaiseen tallennukseen. Se on ensisijaisesti suunniteltu staattisen datan arkistointiin, jota ei muuteta tai jota ei käytetä pitkiin aikoihin (kuukausista vuosikymmeniin). Glacieriin arkistoidut tiedot pysyvät muuttumattomia sillä niitä ei voi muokata, siirtää tai kopioidaan. Eli ne voi ainoastaan ladata ja poistaa. Näiden syiden vuoksi Glacierin käyttö ei sovellu aktiivisen tiedon tallentamiseen, jota joudutaan muokkaamaan usein.

Glacierista tiedon hakuprosessi on hyvin hidasta ja monimutkaista joka on myös yksi syy miksi Glacier ei toimi, jos tarvitsee päästä nopeasti tietoihin käsiksi jotka sinne on tallentanut. Kun Glacieriin laittaa palautuspyynnön, viive vastaukseen on 3-5 tuntia ja vasta tämän jäkeen arkistot on ladattavissa. Myös jokainen palautuspyyntö maksaa ja maksu perustuu palautettavan tiedon kokoon.

Vaihtoehtona Amazon Glacierille on esimerkiksi Google Cloud Storage, Azure Archive Storage ja Blackblaze.

Week 4

Question 1: Your thoughts why small, mobile and portable devices, benefit greatly from cloud services**Answer 1:**

Pilvipalveluiden avulla tietoihin jotka ovat tallennettu pilveen pääsee helposti ja nopeasti käsiksi mistä vain. Varsinkin puhelin on nykyään lähes jokaisella melkein aina mukana. Puhelimen avulla on helppo tallentaa tärkeitä tietoja/tiedostoja ja nämä voi kätevästi puhelimesta varmuuskopioida pilveen. Kadonnut kannettava tietokone tai älypuhelin voi olla henkilölle erittäin vakava ongelma, jos tärkeä tieto katoaa. Pilvipalveluissa tieto on aina laitteen lisäksi pilvessä ja siksi tieto on helppo palauttaa, vaikka laitteet katoaisivat. Lisäksi kadonnut laite voidaan tyhjentää etänä, jolloin data ei joudu väariin käsiin.

Question 2: Study MQTT and CoAP protocols for M2M/IoT communications. What to use and when? Locate some services or cloud data broker and analysis provides supporting either or both**Answer 2:**

- MQTT on avoimeen lähdekoodiin perustuva erittäin kevyt viestiprotokolla. Protokolla pyrkii minimoimaan sitä käyttävien laitteiden resurssivaatimukset sekä käytettävän kaistanleveyden tiedonsiirrossa. Tästä syystä se soveltuu erinomaisesti IoT:n tarpeisiin esimerkiksi mobiililaitteisiin joissa mm. akun kesto on ensiarvoisen tärkeää. Protokolla itsessään ei tue salausta vaan tietoyhteyden salaus on hoidettava erikseen esimerkiksi TLS/SSL:llä. Lähetetty data voidaan myös kryptata lähetettävän laitteen päässä mutta tämäkin on tehtävä protokollan ulkopuolisilla sovelluksilla. MQTT on laajasti käytössä IoT sovelluksissa, tunnetuimpia ovat Facebook Messenger sekä Amazonin IoT palvelut joissa kommunikaatio perustuu MQTT protokollaan.
- CoAP on veistintäprotokolla joka on suunniteltu toimimaan hyvin yksinkertaisissa laitteissa sallien niiden keskustella verkon yli. Protokolla on suunniteltu erityisesti kiinteistöautiomaation ja sähköön kulutuksen valvontaan. Protokollana CoAP käyttää pohjana REST palveluita ja on yhteensopiva käytännössä kaikkien tunnettujen datamallien kanssa kuten XML, JSON jne. CoAP tarjoaa sisäänrakennettuna erittäin vahvan, RSA-pohjaisen suojauksen kommunikaatiolle mikä tekee siitä soveltuvan myös vahvempaa tietoturvaa vaativiin sovelluksiin.

Huolimatta protokollien erilaisuudesta, perusvaatimukset niiden tietoturvan suhteen ovat varsin yhteneviä.

Question 3: Describe few open source chatbot projects, frameworks and examples. List chatbot use cases where you could use chatbots either as user or provider (or both)**Answer 3:**

- Microsoft Bot Framework (MBF) – tarjoaa skaalautuvia, integroituja yhteyksiä ja kehityspalveluja tarjoavia yritysliikennepalveluja. Se auttaa kehittäjiä luomaan älykkäitä botteja, joita voidaan käyttää useilla alustoilla. Bottia voidaan käyttää 141 maassa, koska se tarjoaa pilvipohjaista palvelua ja on monikielinen. Kehitystuokalu on järjestetty Microsoft Bot Builder SDK:n kanssa, johon .NET- ja Node.js kehittäjät pääsevät. Microsoftin lähestymistapa on ensisijaisesti koodipohjainen ja suunnattu nimenomaan kehittäjille. MBF antaa kehittäjän täysin hallita chatbotin rakennuskokemusta. Kehitysympäristössä on suuri määrä työkaluja jotka auttavat chatbotin tekemisessä. MBF:ää ei voida pitää täysin avoimen lähdekoodin ohjelmajana, sillä NLU-mootori Luis jota se käyttää, on patentoitu ohjelmisto. Kohdeympäristönä ovat: verkkosivusto, sovellus, Cortana, Microsoft Teams, Skype, Facebook Messenger ja Slack.

- Rasa – Rasa on johtava avoimen lähdekoodin kehys kontekstuaalisten chatbottien rakentamiseen. Kuten tiedämme, saatavilla on monia tekoälypohjaisia chatbot-kehysiä, mutta useimmat niistä tarjoavat perustoimintoja, kuten vastaamisen staattisiin usein kysyttyihin kysymyksiin tai joihinkin ennalta määritettyihin peruskyselyihin. Rasa-kehys tarjoaa enemmän kuin järkevää, eli kontekstuaaliset chatbotit, jotka tekevät robotista kehittyneemmän ja antavat tunteen ihmisen vuorovaikutuksesta.
Rasassa on kaksi pääkomponenttia Rasa NLU ja Rasa Core, Rasa NLU vastaa luonnollisesta kielen ymmärtämisestä ja Rasa core auttaa luomaan älykkäitä, keskustelua edistäviä kontekstuaalisia chatbotteja. Seuraavassa on joitain Rasa-kehysen tärkeimmistä eduista: avoimen lähdekoodin bottien kehysympäristö joka on keskittynyt tarinalliseen lähestymistapaan chatbottien rakentamisessa. Rasa on keskittynyt tekoälyyn ja rakentamaan sellaisen kehysympäristön joka sallii kehittäjien jatkuvasti parannella heidän tekoälyapulaistaan. Rasa ei ole itse määritellyt visuaalista kulkua eikä tavoitteita alustan sisällä vaan antaa kehittäjille mahdollisuuden itse luoda tarinoita (koulutus esimerkkejä), joiden tarkoituksena on kouluttaa bottia. Rasan standardi NLU-moottori on täysin avointa lähdekoodia. Rasa X:ssä on erilaisia työkaluja joiden avulla kehittäjät voivat tarkastella keskusteluja ja parantaa avustajaa. Jokainen chatbot alusta tarvitsee tietyn verran koulutusdataa, mutta Rasa toimii parhaiten, kun siihen asetetaan suuri määrä koulutusdataa, yleensä asiakaspalvelun chat-logien muodossa. Asiakaspalvelu chat logit jäsennellään, järjestetään ja luokitellaan ja lopuksi niitä käytetään NLU-moottorin kouluttamiseen. Yksi mahdollinen ongelma tarinallisessa lähestymistavassa on se, että voi olla vaikea ennustaa, mitä botti aikoo tietyllä hetkellä sanoa, sillä kukaan ei pysty vaikuttamaan taustalla olevaan logiikkaan. Tätä riskiä yritetään pienentää suurella harjoittelumäärällä.
- BotKit – Microsoftin ostama avoimen lähdekoodin alusta. Botkit on enemmän visuaalisen keskustelun rakentaja, jossa keskitytään enemmän käyttäjän käytettävissä oleviin käyttöliittymiä toimintoihin. Visuaalisen keskustelun rakentaja auttaa chatbottien kehittämisessä ja sen avulla käyttäjät, joilla ei ole paljon koodauskokemusta pystyvät myös osallistumaan chatbotin luontiin. Myös BotKit on koodikeskeinen alusta ja kehittäjien on helppo käyttää sitä. Botkit on yksi osa laajempaa sarjaa kehittäjätyökaluja ja SDK:ita, jotka kattavat MBF:n. Bot Framework SDK tarjoaa perustan, jolle BotKit on rakennettu. Myös BotKit käyttää NLU-moottori Luis:ta, mutta se voidaan tarvittaessa integroida muihin NLU-moottoreihin. BotKit on saatavilla useilla eri ohjelmointikielillä. BotKit:ssä on paljon erilaisia laajennuksia eri chat-alustoille, kuten Webex, Slack, Facebook Messenger ja Google Hangout.

Question 4: Search and describe examples of CAP theorem in cloud services context

Answer 4: CAP-teoreema soveltaa samanlaista logiikkaa hajautetuissa järjestelmissä, nimittäin, että hajautettu järjestelmä voi tarjota vain kaksi kolmesta halutusta ominaisuudesta: Riistattomuus, Saatavuus ja Osittamistoleranssi:

- Ristiriidattomuus (Consistency) tarkoittaa, että kaikilla palvelimilla on sama data samaan aikaan siten, että datan käyttäjä saa saman vastauksen riippumatta siitä miltä palvelimelta vastaus annetaan. Järjestelmä ei kuitenkaan pysty välittömästi tallentamaan data muutoksia kaikille palvelimille. Tämän vuoksi tavoitteena on, että datan muutosten tallentaminen tehdään riittävän nopeasti jolloin viivettä on lähes mahdotonta huomata.
- Saatavuus (Availability) tarkoittaa, että jokaiseen käyttäjän tekemään pyyntöön (datan lukemiseen tai muokkaamiseen) tulee saada järjestelmältä vastaus vaikka toiminto epäonnistuisi.
- Osittamistoleranssi (Partition tolerance) tarkoittaa, että järjestelmä jatkaa toimintaansa huolimatta siitä, että yksittäinen palvelin ei olisikaan toiminnassa tai saavutettavissa. Palvelimen ongelmat voivat johtua esimerkiksi verkkoyhteysvirheestä tai serverin kaatumisesta

Week 5

Question 1: Describe pros and cons of cloud WAFs

Answer 1:

WAF on sovellusten palomuuuri, joka koskee erityisesti verkkosovelluksia. Se otetaan käyttöön verkkosovellusten edessä ja se analysoi kaksisuuntaista verkkopohjaista (HTTP) liikennettä sekä havaitsee ja estää kaiken haitallisen liikenteen.

Pilvipohjaisen WAF:t ovat edullinen vaihtoehto ja ne on helppo ottaa käyttöön. Käyttäjät maksavat kuukausittain tai vuosittain turvallisuudesta palveluna. Pilvipohjaiset WAF:t voi myös tarjota ratkaisun, jota päivitetään jatkuvasti uusimpien uhkien estämiseksi ilman käyttäjälle aiheutuvaa lisätöitä tai kustannuksia. Pilvipohjainen WAF on yös helposti vaihdettavissa uuteen/toiseen.

Haittapuolet:

- Käyttäjän siirtämä vastuu kolmannelle osapuolelle, joten jotkin WAF:n ominaisuudet voivat olla heille musta laatikko.
- Luotettavuus: pilvipohjaisen WAF:n on ohjattava tehokkaasti kaikki liikenne verkkosovellukseen. Kun WAF:n suorituskyky on heikko, niin myös verkkosovelluksen suorituskyky on heikko.
- Pilvipohjaisella WAF-toimittajalla on monia asiakkaita, jotka käyttävät samaa palvelua. Jos toimittajien palvelimet ovat ylikuormitettuja tai alhaalla, tietoturva voi kärsiä.

Hyödyt:

- Pilvipohjaisessa WAF:lla pystyy hallitsemaan käyttöoikeuksia suoraan ja yksittäisen liikennevirran pystyy estämään tiettyyn sovellukseen ilman, että se vaikuttaa sisäisiin käyttäjiin.
- Ennaltaehkäisee evästemyrkytyksiä/istuntokaappauksia
 - Kyberrikollinen manipuloi tai väärentää evästettä ohittaakseen turvallisuuden tai päästäkseen palvelimelle varastaakseen tietoja. Tällaisia hyökkäyksiä käytetään, kun käyttäjän on kirjaututtava sisään tilille ja kyberrikollinen sieppaa evästeen poimiakseen siitä tallennettuja tietoja, kuten automaattisesti täytettyjä henkilökohtaisia tietoja.
 - WAF:t pystyvät estämään edellämainitun tapahtuman suojaamalla ja salamalla henkilökohtaisia tunnistetietoja sekä tunnistamalla manipuloituja tai väärennetyjä evästeitä pääsemästä palvelimelle.
- Estää SQL-injektion (Structured Query Language injection)
 - Tarkoittaa sitä, kun kyberrikollinen muuttaa sovelluksen tekemiä kyselyitä, jotka voivat antaa kyberrikolliselle pääsyn tärkeisiin henkilökohtaisiin tai taloudellisiin tietoihin.
 - WAF kykenee estämään edellämainitun suorittamalla sääntöjä, jotka edellyttävät SQL-injektoiden täyttävän tiettyjä ehtoja, ja jos ehdot eivät täyty, se estää käyttäjältä pääsyn verkkosovellukseen
- Estää cross-site scripting (XSS)
 - Evästemyrkytyksen tavoin XSS on eräänlainen injektio, johon liittyy haitallisia komentosarjoja. Kyberrikollinen lähettää haitallista koodia verkkosovelluksen kautta suoraan toiselle loppukäyttäjälle yrittääkseen päästä selaimen tallennettuihin evästeisiin tai muihin arkaluontoihin tietoihin joita verkkosovellus käyttää.
 - WAF voi auttaa estämään edellämainitun konfiguroiduilla käytännöillä, jotka tarkistavat ja valvovat näitä pyyntöjä ja estää ne, kun turvallisuusehdot eivät täyty.

- Estää hajautetun palveluestohyökkäyksen (Distributed Denial of Services, DDoS)
 - Hyökkäys koskee useita laitteita, jotka ovat saaneet tartunnan haittaohjelmasta, joka on vallannut verkkosovelluksen aiheuttamalla epätavallisen määrän liikennettä. Tästä aiheutuu noraalin liikenteen palveluneston, joka aiheuttaa suorituskykyongelmia ja heikentää suojauskerroksia.
 - WAF pystyy tunnistamaan ja estämään tämän tyyppisen epätavallisen toiminnan avainindikaattoreiden perusteella, kuten korkea liikenteen määrä tietystä IP-osoiteesta, epätavalliset liikennöinnit tai tietyn sivun suuri liikenne.

Question 2: Search and describe some already implemented systems, how blockchains are being used by corporations

Answer 2: Lohkoketjuteknologiaa käytetään jäljentämään ja tellentamaan tuotteiden logistiikka- tai tuotantoketjuja. Tällaisia yrityksiä ovat esimerkiksi ShipChain ja Provenance. Logistiikka- ja tuotantoketjujen lisäksi lohkoketjuteknologia helpottaa välillistä toimintaa eli ylimääräisen paperityön jäädessä vähemmäksi tehottomuutta saadaan pienemmäksi. Lohkoketjuteknologian poistaessa välikäsiä myös kustannukset pienentyvät. Tästä voi myös aiheutua uutta liiketoimintaa, joka ei olisi mahdollista välikäsiä kanssa. Lohkoketjuteknologiaa käytetään myös rahoitusallalla, jossa lohkoketjuteknologian avulla pyritään kehittämään järjestelmää, jossa asunto-osakekirjat voitaisiin säilyttää lohkoketjussa. Myös sosiaali- ja terveydenhuollossa pyritään käyttämään lohkoketjuteknologiaa mm. Tietojen käsittelyyn ja turvaamiseen, maksuliikenteeseen ja sähköisiin sosiaali ja terveystietoihin. Esimerkiksi Medileader, joka on lääketieteellisyydelle suunnattu yksityinen lohkoketjuteknologia. Sen tarkoituksena on valvoa lääkkeiden toimitusketjua ja sitä kautta taata, että lääkkeiden hinnat ovat aina säädeltyjä. Dentocoin on hammasallalle suunnattu sovellus, jossa käyttäjiä palkitaan heidän tuottamastaan tiedosta liittuen palvelun laatuun ja arviointiin. Microsoft tarjoaa lohkoketjuteknologiaa ratkaisuja, eli pilvipohjaisia kehitysympäristöjä lohkoketjujen kehittäjille. Saksalainen energiayhtiö RWE on lanseerannut lohkoketjuja hyödyntävän sähköautojen latausverkon. Tarkoituksena on laajentaa verkon toimintaa myös muualle Eurooppaan. Volkswagen-konserni on perustanut oman IOTA-kryptovaluutta hyödyntävän lohkoketjuprojektin. Lohkoketjuteknologian mahdollisuuksia nähdään esimerkiksi huoltotoiminnassa ja itseajavissa autoissa.

Question 3: List and describe shortly different open source or commercial internet networking (peer-to-peer) solutions where multiple hosts can share the host network connection(s) and other resources

Answer 3:

- ANts P2P: avoimen lähdekoodin anonyymi vertaisverkko-ohjelma joka on tehty Java-kielellä. ANts P2P kryptaa kaiken lähetetyn tai vastaanotetun liikenteen muilta ja välittää liikenteen osapuolten välillä verkossa tehdäkseen peräisin olevien IP-osoitteiden määrittämisen vaikeammaksi. ANts P2P antaa käyttäjien tarjota web-palvelimia anonyymisti eli näihin palvelimiin pääsee ainoastaan ANts P2P-verkon sisältä. ANts P2P ei välitä verkkopalvelinliikennettä ulos antaen käyttäjiä pääsemästä tavallisiin Internet-palveluihin.
- Freenet: keskuspalvelimeton hajautettu tietovarasto joka käyttää vertaisverkkotekniikkaa. Freenetin tarkoituksena on tarjota sähköinen sananvapaus vahvan anonyymiteetin avulla. Freenetin käyttäjät voi julkaista ja pyytää materiaalia anonyymisti ja pyydetyn datan yksilöintiin ja paikallistamiseen Freenet käyttää avainpohjaista reititystä ja hajautettuja tiivisteitä.
- Napster: Ensimmäinen laajasti käytetty vertaisverkko-ohjelma. Ohjelmisto oli helppokäyttöinen ja se oli tarkoitettu digitaalisten musiikkitiedostojen jakamiseen. Alkuperäinen Napster suljettiin

kesällä 2001 reilun puolentoista vuoden olemassa olon jälkeen. Nykyään Napster toimii samantyyppisenä maksullisena musiikkipalveluna kuin Spotify.

- GUNet: Pääosin C-kielellä kirjoitettu vertaisverkolle oleva keskukseton runkojärjestelmä ja se tarjoaa linkkitason salauksen sekä palvelut muiden verkon solmujen löytämiseen ja resurssien jakoon. GUNet on anonymisoiva, sensuuria ehkäisevä tiedostonjakopalvelu ja sen käyttäjät pystyy anonymisti julkaisemaan ja hakeman kaikenlaista tietoa. GAP-protokollaa käytetään pyyntöjen ja vastausten reititykseen.

Question 4: List and describe (with tiny examples) some commonly used data formatting standards, markup languages and syntaxes used to store or request data via cloud service APIs

Answer 4:

- JSON (JavaScript Object Notation): Asiakaspuolen komentosarjojen käsittelyssä oleva formaatti. JSON on usein nopeampi ratkaisu verrattuna muihin vaihtoehtoihin kuten XML:lle. JSON ei ole yhtä tehokas tai laajasti käytetty kuin muut vaihtoehdot, mutta sen tuki moniin ominaisuuksiin tekee siitä hyvän kilpailijan verrattuna muihin. JSON tuntee eron numeron, merkkijonon ja booleanin välillä ja tämä ominaisuus puuttuu XML:stä. Toisaalta XML pystyy käsittelemään sekoitettua sisältöä paremmin kuin JSON varsinkin silloin, kun kyseessä on sekasolmutaulukot jotka vaativat yksityiskohtaisia lausekkeita.
- XML (EXtensible Markup Language): Käytetään formaattina tiedonvälitykseen järjestelmien välillä ja tiedostomuotona dokumenttien tallentamiseen. XML on rakenteellinen kuvauskieli joka auttaa jäsentämään laajoja tietomassoja selkeämmin.
- YAML: Ei ole merkintäkieli vaan suora datamuoto. JSON ollessa kevyt ja sen ominaisuuksien ollessa suppeita ja XML:n ollessa monipuolinen, mutta usein vaikeakäyttöinen, YAML on helppolukuinen, kevyt ja JSON sekä XML:n välillä oleva muoto. Vaikka YAML on luokiteltu suoraksi datamuodoksi, sillä sitä käytetään jäsentämään kokoonpano asetuksia ja relaatiokyselyitä, YAML:ää käytetään monissa järjestelmissä perustietokantana.
- RSS (Rish Site Summary): Yleisin käytetty syötetietomuoto. Vakiintanut paikkansa syötemenetelmäksi WordPressin ja muiden blogialustojen toimesta. RSS on yksinkertainen formaatti käyttää, mutta sulkee pois hyvin muodostetut XML-merkinnät suosien pelkkää tekstiä ja pakotettua HTML-koodia.

Extra bundle A

Describe these terms and concept

- **Bare metal server** – Fyysinen tietokonepalvelin, jota käyttää vain yksi kuluttaja tai vuokralainen.[1] Jokainen vuokrattava palvelin on erillinen fyysinen laitteisto, joka on toimiva palvelin yksinään. Ne eivät ole virtuaalisia palvelimia, jotka toimivat useissa jaetuissa laitteistoissa.
- **Cloud broker** - kokonaisuus, joka hallinnoi pilvipalvelujen käyttöä, suorituskykyä ja toimitusta sekä neuvottelee suhteista pilvipalvelujen tarjoajien ja pilvikäyttäjien välillä. Pilvipalveluiden kehittyessä pilvipalvelujen integrointi voi olla liian monimutkaista, jotta pilvikuluttajat voivat hallita niitä yksin.
- **Microservice(s)** – Mikropalvelut, tunnetaan myös nimellä mikropalveluarkkitehtuuri – on arkkitehtoninen tyyli, joka jäsentää sovelluksen kokoelmaksi palveluita, jotka ovat Erittäin huollettavissa ja testattavissa, Löyhästi kytketty, Itsenäisesti käyttöön otettavissa, Järjestetty liiketoimintakykyjen ympärille, Pienen tiimin omistuksessa
- **Elastic computing** – pilvipalvelun käsite, nopeasti laajentaa tai vähentää tietokoneen prosessointi-, muisti- ja tallennusresursseja vastaamaan muuttuviin vaatimuksiin huolehtimatta kapasiteetin suunnittelusta ja suunnittelusta huippukäyttöä varten.
- **Cloud federation** – useiden ulkoisten ja sisäisten pilvipalveluiden käyttöönotto ja hallinta vastaamaan liiketoiminnan tarpeita. Se on monikansallinen pilvijärjestelmä, joka integroi yksityiset, yhteisölliset ja julkiset pilvet skaalautuviin laskenta-alustoihin.
- **AWS Lambda** – palvelimeton laskentapalvelu, joka suorittaa koodisi vastauksena tapahtumiin ja hallitsee automaattisesti taustalla olevia laskentaresursseja puolestasi. Näihin tapahtumiin voi sisältyä muutoksia tilassa tai päivitys, kuten käyttäjä sijoittaa tuotteen ostoskoriin verkkokauppasivustolla.
- **FaaS** – pilvilaskentapalvelu, jonka avulla voit suorittaa koodia vastauksena tapahtumiin ilman monimutkaista infrastruktuuria, joka tyypillisesti liittyy mikropalvelusovellusten rakentamiseen ja käynnistämiseen.
- **DaaS** – Desktop as a service eli DaaS on pilvipalveluratkaisu, joka toimittaa virtuaaliset sovellukset ja työpöydät turvallisesti pilvestä mihin tahansa laitteeseen. Tämä hallitun työpöydän virtualisointiratkaisu, jota käytetään turvallisten SaaS- ja vanhojen sovellusten sekä täydellisten Windows-pohjaisten virtuaalisten työasemien tarjoamiseen ja toimittaa ne työntekijöillesi. Ennustettavan jako-tilausmallin avulla DaaS helpottaa skaalatausta tarpeen mukaan. Sitä on helppo hallita ja se yksinkertaistaa monia työpöytäratkaisujen IT-järjestelmänvalvojatehtäviä.
- **SSO** – todennusmalli, jonka avulla käyttäjä voi kirjautua sisään yhdellä tunnukseksi mihin tahansa useista toisiinsa liittyvistä, mutta itsenäisistä ohjelmistojärjestelmistä.
- **Managed DNS** – asiakas ei itse hallitse DNS -servereitä vaan ostaa palvelun palveluntarjoalta, esimerkiksi Amazon Route 53, Cloud DNS tai Cloudflare. Palveluntarjoaja pystyy tarjoamaan paljon joustavamman yhteyden palvelimille. Palveluntarjoaja pystyy ohjaamaan resurssiansa puolesta liikenteen dynaamisesti ja tätä kautta he lyhentävät DNS latausaikaa. Palveluntarjoajat voivat myös tarjota turvallisuuspalveluita, esimerkiksi web-sovelluksen palomuurin.
- **Origin server** – tarkoituksena on käsitellä ja vastata Internet -asiakkailta saapuvia internet pyyntöjä. Origin server -käsitettä käytetään yleensä reunapalvelimen tai välimuistipalvelimen käsitteiden kanssa. Origin server on siis tietokone, jossa on käynnissä yksi tai useampi ohjelma, jotka ovat suunniteltu kuuntelemaan ja prosessoimaan tulevia pyyntöjä tai liikennettä.
- **Google Firebase** – sovellusalusta, joka on tarkoitettu mobiili (iOS ja Android) ja web -sovellusten luontiin. Firebase tarjoaa työkalut seuranta analytiikkaan, sovellusten kaatumisen raportointiin ja

korjaamiseen, markkinoinnin ja tuotekokelun luomiseen. Firebase tarjoaa monia palveluita, kuten esimerkiksi: analysoinnin, todennuksen, reaaliaikaisen tietokannan, testilaboratorion.

- **LAMP** – kokoelma avoimen lähdekoodin ohjelmia, jotka yhdessä muodostavat WWW-palvelimen, jonka avulla voidaan palvella dynaamisia verkkosivuja asiakasohjelmille. Dynaamiset verkkosivut käyttävät jollain ohjelmointikielellä tehtyjä ohjeita, joita suorittamalla palvelin tuottaa HTML-sivun vastauksena HTTP-pyyntöön.
- **Mashup service** – tarkoittaa tiedostoa tai sovellusta, joka yhdistelee useita erilaisia digitaalisia tiedostomuotoja tai lähteitä, kuten karttoja, musiikkia, valokuvia, videoita ja animaatioita. Käsite on alun perin lähtöisin musiikista, jossa sillä on tarkoitettu eri kappaleiden samplattuja yhdistelmiä. Mashupin ideana on luoda uutta tietoa yhdistelemällä ja rinnastamalla olemassa olevia tietoja toisiinsa.
- **Middleware** – ohjelmistokomponentti, joka toimii osien tai sovelluksien välisenä rajapintana tai palveluna. Käytännössä termiä käytetään myös laajemmin eri toiminnallisuuksien toteuttavista ohjelmakomponenteista. Termiä sanotaan käytettävän järjestelmäohjelman ja sovellusohjelman tai kahden sovellusohjelman välillä toimivasta ohjelmasta.
- **Ubiquitous computing** – jokapaikan tietotekniikka, on huomaamattomasti toimivaa ja ympäristöönsä suolaautuvaa kaikkialla olevaa tietotekniikkaa. Se ei häiristee käyttäjäänsä eikä keskeytä hänen muuta toimintaansa. Se toimii ihmisten ja yritysten arkitoimissa kaikkialla ja koko ajan. Arjen esitneet ja koneet viestivät langattomasti keskenään sekä säätävät toimintaansa itsenäisesti. Esimerkiksi äly-kodin valot, ilmastointi turvallisuus ja viihde ovat automatisoitu.
- **SLA** – Service Level Agreement (palvelutasosopimus), asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. Sopimusta mitataan erityyppisillä mittareilla ja palvelutason alittamisesta seuraa yhteisesti sovittu sanktio. Tarkasti laadittu sopimus tarjoaa myös keinot ongelmien korjaamiseksi. Sopimuksen piiriin voi kuulua esimerkiksi logistiikan ostaminen yrityksen ulkopuolelta, tai se voidaan määritellä yhtiön sisäisten kustannusyksiköiden välillekin.
- **TCO** – Total cost of ownership, taloudellinen arvio, jonka avulla ostajat ja omistajat määrittelevät tuotteen tai palvelun välittömät ja välilliset kustannukset. Kokonaiskustannusten osalta ostajien tulisi vaihtoehtoisten järjestelmien välillä tehdessään ottaa huomioon paitsi ostohinta myös pitkäaikainen hinta. Järjestelmällä, jolla on alhaisemmat kokonaiskustannukset, on korkeampi arvo pitkällä aikavälillä.
- **Vendor lock-in** – toimittajaloukku, tilanne, johon varomaton tietojärjestelmän ostaja joutuu valittuaan järjestelmälle toimittajan: kaikki muutostyöt on pakko ostaa samalta toimittajalta, ja tämä voi rahastaa niillä lähes miten haluaa. Myös huono laatu ja hitaus ongelmien korjaamisessa kulkevat yleensä käsi kädessä toimittajaloukun kanssa.
- **Utility computing** – malli missä laskentakapasiteetti jota tarjotaan tilauksesta maksettavan laskutusmenetelmän avulla. Se on laskennallinen liiketoimintamalli, jossa palveluntarjoaja omistaa, hallinnoi ja hallinnoi laskentainfrastruktuuria ja resursseja, ja tilaajat käyttävät sitä tarvittaessa vuokrauksen tai mitatun perusteella. Tämä on yksi suosituimmista IT-palvelumalleista pääasiassa sen tarjoaman joustavuuden ja taloudellisuuden vuoksi. Kuluttajalla on lähes rajoittamaton tarjonta laskentaratkaisuja Internetin tai virtuaalisen yksityisen verkon välityksellä, ja ne voidaan hankkia ja käyttää aina tarvittaessa. Taustainfrastruktuurin sekä laskennallisten resurssien hallintaa ja toimitusta hallinnoi palveluntarjoaja.
- **Fog computing (fogging)** – arkkitehtuurimalli jossa data, käsittely ja sovellukset ovat keskittyneet laitteisiin verkon reunalla sen sijaan, että ne olisivat lähes kokonaan pilvessä. Tämä tarkoittaa, että tietoja voidaan käsitellä paikallisesti älylaitteilla sen sijaan, että ne lähetettäisiin pilveen käsittelemään varten. Tällöin Fogging vähentää palveluviitettä ja parantaa QoS:ää, mikä johtaa parempaan

käyttökokemukseen. Fogging on yksi tapa käsitellä jatkuvasti kasvavien Internet-laitteiden määrää, joita joskus kutsutaan esineiden Internetiksi (IoT)

- **Network Slicing** – verkkoarkkitehtuuri, joka mahdollistaa virtualisoitujen ja itsenäisten loogisten verkkojen multipleksoinnin samassa fyysisessä verkkoinfrastruktuurissa. Jokainen verkkolohko on eristetty päästä päähän -verkko, joka on räätälöity täyttämään tietyn sovelluksen vaatimat erilaiset vaatimukset
- **Websocket** – jatkuva yhteys asiakkaan ja palvelimen välillä. WebSockets tarjoaa kaksisuuntaisen, kaksisuuntaisen tietoliikennekanavan, joka toimii HTTP:n yli yhden TCP/IP-pistokeyhteyden kautta. WebSocket-protokollan ytimessä helpottaa viestien välittämistä asiakkaan ja palvelimen välillä.

Extra bundle B

Research and answer all these questions. Few word answers are now enough. Use examples.

- **What to consider and compare when choosing a VPS server provider and VPS server features?**
 - Virtuaalipalvelimen fyysinen sijainti, esimerkiksi jos virtuaalipalvelimelle aikoo laittaa pystyyn nettisivuja, on palvelimen hyvä olla mahdollisimman lähellä loppukäyttäjää, jotta sivujen latausaika pysyy pienenä
 - RAM-muistin määrä, jos aikoo virtuaalipalvelimessa pyörittää nettisivujen lisäksi esim. sähköpostin välitystä ja sähköpostin roskapostisuodatusta, tarvitsee RAM-muistia olla tarpeeksi.
 - Kovalevyn koko ja millainen kovalevy on. Esim. SSD-kovalevy on huomattavasti nopeampi, kuin perinteinen HDD.
 - Prosessori, mitä enemmän ytimiä, sitä nopeammin tieto kulkee.
 - Yhteysnopeus ja liikenneoitiraja, jos odottaa nettisivuilleen paljon vierailijoita, se tarkoittaa myös paljon tiedonsiirtoa.
 - Käyttöjärjestelmä, käyttöjärjestelmän vaihtaminen myöhemmässä vaiheessa on vaikeata, ns. turvallista on valita 64-bittinen.
 - Palvelun hinta, hintaa katsoessa hinta on hyvä suhteuttaa ylläoleviin seikkoihin sekä mistä muista asioista hinta koostuu
- **The benefits, risks and challenges of hybrid cloud computing**
 - Hyödyt
 - Jos kapasiteettitarpeet vaihtelevat, tai jos tarvitsee nopeasti uutta kapasiteettia on hybridipilvi hyvä ratkaisu.
 - Varmuuskopiot, pilvessä on tarjolla suhteessa halpaa säilytystilaa datalle, jota tarvitaan harvoin.
 - Pilvi varastokonesalina on yksi vaihtoehto
 - Pilvipalveluun sisältyy paljon erilaisia palveluita, joita on helppo ja nopea ottaa käyttöön.
 - Riskit
 - Tietovuoto/Puutteita turvatarkistuksessa, esimerkiksi inhimillisen virheen, vaarantuneen päätepisteen (esim. kadonnut älypuhelin) tai jos pilvihallinnan sovellusliittymiä ei ole otettu käyttöön ja suojattu oikein.
 - Huonosti laadittu SLA, voi johtaa esim. ylihinnotteluun.
 - Haasteet
 - Valmiuden puute tiedonsiirtoon, hybridipilvipalveluun siirtyminen toistesta pilvestä tai tietoverkosta on aikaa vievää ja haastavaa.
 - Taito- ja asiantuntemuksen puutteet, asiakas luottaa usein liikaa palveluntarjoajaan hybridiympäristön hallinnassa. Liiallinen riippuvuus ulkoistettuun apuun johtaa tehottomaan päätöksentekoon, mahdollisiin vaaroihin ja harvempiin liiketoimintamahdollisuuksiin.
 - Yhteensopivuusongelmat, useat infrastruktuurit ja teknologiapinot yhdessä arkkitehtuurissa voivat helposti johtaa työkalujen ja prosessien yhteensopimattomuuteen.

- **Why HTTP/2 (and HTTP/3) will/may speed-up many web based cloud services? What is the current HTTP/2 adaptation rate now?**
 - HTTP/2 nopeuttaa liikennettä siirtäen kaikki tiedot binäärimuodossa HTTP/1.1:n tekstimuotoon verrattuna.
 - Samassa yhteydessä voidaan siirtää useita eri tiedostoja.
 - HTTP/3 mahdollistaa vielä nopeamman ja turvallisemman tiedonsiirron hyödyntäen Quick UDP Internet Connection (QUIC)-protokollaa. HTTP/2:n heikkouden ollessa, että virhetilanteissa kaikkien samaa yhteyttä käytettävien sisältöjen siirtäminen epäonnistuu.
- **What is (5G) mobile edge computing? How it may change IoT and mobile device use?**
 - MEC (mobile edge computing) -arkkitehtuurissa prosessointikapasiteettia viedään lähemmäksi paikkaa, jossa kerättyä ja analysoitua dataa hyödynnetään. Suurta nopeutta vaativa koneiden ja laitteiden välinen viestintä voi tapahtua MEC-serverin avulla, joka toimii tiedon välivarastona tarjoten nopeaa, paikallista prosessointikykyä.
 - MEC nopeuttaa mobiililaitteiden sovelluksia. Esim. jos monet käyttäjät lataavat samaa videota, kaikkien ei tarvitse ladata sitä kauimpana olevista palvelimista.
 - Tekoäly voi esimerkiksi oppia datamäärän vaihteluita sekä käyttäjien liikkeitä, ja auttaa palvelimia varautumaan niihin jakamalla laskentakuormaa ja lataamalla sisältöä etukäteen. Näin verkot ei tukkeudu isojen käyttäjä- ja datamäärän alla, vaan sovellukset toimivat jouhevasti.

Extra bundle C

Research and answer all these questions. Few word answers are now enough. Use examples.

- **List and describe shortly 3-5 cloud based firewall and SIEM solutions**
 - CloudFlare WAF
 - Tarkkailee säännöllisesti Internetiä mahdollisten hyökkäysten ja haavoittuvuuksien varalta.
 - Verkkosovellusten palomuuuri otetaan automaattisesti käyttöön kaikesta sellaisesta, jota pidetään uhkana suurimmalle osalle asiakkaita.
 - Päivitetään jatkuvasti ja tämän kautta varmistetaan, että CloudFlaren suojaus on aina ajantasainen.
 - Suuren asiakaskunnan vuoksi CloudFlare pystyy luottamaan kollektiiviseen älykkyyteen uhkien poistamisessa.
 - Eli kun yksi asiakas luo uuden säännön palomuurille, CloudFlare tarkistaa tarvitseeko saman säännön ottaa käyttöön muillekin asiakkaille.
 - SolarWinds Security Event Manager (SEM)
 - Tarjoaa pääsyn lokitietoihin rikosteknisiä ja vianetsintä tarkoitusta varten sekä työkaluja, jotka auttavat hallitsemaan lokitietoja.
 - Hyödyntää kerättyjä lokeja, analysoi ne reaaliajassa ja ilmoittaa ongelmasta ennen kuin ongelma aiheuttaa lisävauriota.
 - SolarWinds tarjoaa myös laitteiden etähallintatyökaluja.
 - Splunk Enterprise Security (ES)
 - Antaa tietoa järjestelmässä liikkuvasta datasta ja kertoo, jos on syntymässä mahdollisia ongelmatilanteita.
 - Kerää tietoa reaaliaikaisesti ja tallentavasti.
 - Pystyy indeksoimaan kaiken tiedon, riippumatta tiedon lähteestä, muodosta tai käyttötarkoituksesta.
 - AWS WAF
 - Käyttäjät voivat itse luoda räätälöidyt säännöt jotka ovat suunniteltu estämään yleiset hyökkäysmallit, kuten sivustojen väliset komentosarjat.
 - AWS:ssä on täysin varusteltu ohjelmointirajapinta jonka avulla käyttäjät voivat automatisoida kaikkien käytössä olevien sääntöjen luomisen, käyttöönoton ja ylläpdon.
 - Sophos Firewall
 - Sophos Firewall suojaa sovellukset ja on langaton yhdyskäytävänä.
 - Erikseen lisättävä Sophos 'iView', joka tarjoaa keskitetyn raportoinnin useiden palomuurien välillä.
 - Käyttäjät pystyvät hallinnoimaan palomuuriasetuksia ja apuohjelmien kojelautaan. Apuohjelmien kojelaudassa pystyy tarkastelemaan verkkoa, käyttäjiä ja sovelluksia.
 - Datadog Cloud SIEM
 - Tarjoaa vakaan uhkien havaitsemisen dynaamisiin, pilvitason ympäristöihin.
 - Datadog Cloud SIEM:n avulla pystyy analysoimaan toiminta- ja suojauslokeja reaaliajassa, riippumatta siitä kuinka paljon analysoitavaa on sekä hyödyntämään valikoituja, valmiita integraatioita ja sääntöjä uhkien havaitsemiseen.
 - Yksityiskohtaisten havaintotietojen hyödyntäminen joka auttaa nopeuttamaan tietoturvatutkimuksia yhdellä alustalla.

- **Companies using Software Defined Networking (or cloud networking solutions like Maraki) benefit from cloud services. Why? List some SDN vendors and products**
 - Tietoturva- ja käytäntötietojen jakaminen johdonmukaisesti koko yrityksessä.
 - Pilvipalvelun avulla SDN:stä saa herkemmän ja sen käyttäminen on halvempaa.
 - Resurssien siirtäminen yrityksiin on nopeampaa ja läpinäkyvämpää
- **List and describe few recent (or possible) software supply chain security incidents and issues where application source code is fetched from the cloud service during the build process**
 - SolarWinds Orion Platform -hallintatyökaluun lisätty takaovi. Takaovi onnistuttiin levittämään tuhansiin organisaatioihin. Takaovea on voitu käyttää organisaation palveluihin tunkeutumiseen ja sillä mahdollistettiin haitallisen sisällön lisääminen.
 - Asusin palvelimen kaapanneet murtautujat onnistuivat syöttämään haittaohjelmia sadoille tuhansille tietokoneilla. Kohteena olivat tietyt tietokoneet ja niihin asennettiin erityisiä räätälöityjä haittaohjelmia.
 - Alex Brisman tunkeutui mm. Applen ja Microsoftin järjestelmiin ujuttamalla niihin omia ohjelmistopaketteja. Brisman käytti murtautumisessa hyväkseen virhetilanteita laajasti käytettyjen ohjelmointikielten pakettihallinnassa. Brisman selvitti mahdollisimman monien sisäisten pakettien nimiä ja loi omat pakettinsa identtisin nimin asianmukaisiin julkisiin pakettivarastoihin.
- **“If the cloud product is free. Then you are the product” -Explain the logic and meaning. Note: This phrase and logic is somewhat controversial**
 - Jos yritys antaa jotakin ilmaiseksi, silloin yritys saa rahaa jollain muulla keinolla ja se on usein myymällä tietoja käyttäjältä. Myytävät tiedot voivat olla henkilökohtaisia tietoja tai yritys voi käyttää tehokkaamaa mainontaa, jotta käyttäjä hankkisi maksullisen palvelun.