Teemu Pöytäniemi

Tiedostojen siirto ja talletus Azure -pilvialustalla

Diplomityö

Tieto- ja säjkötekniikan tiedekunta

Tarkastaja: Kari Systa

9/202

TIIVISTELMÄ

Teemu Pöytäniemi: Tiedostojen siirto ja talletus Azure -pilvialustalla

Diplomityö

Tampereen yliopisto

Tietotekniikan tutkinto-ohjelma

9/2024

Diplomityössä tarkastellaan tiedostojen siirtämistä ja tallentamista Azure -pilvialustalla. Tiedostojen siirtämistä ja talletusta tarkastellaan kolmesta näkökulmasta: kustannukset, suorituskyky ja tietoturva. Tiedoston siirtämistä vertaillaan eri tiedostonsiirtoprotokollien avulla. Diplotyössä vertaillaan seuraavia suojaamattomia protokollia: HTTP, WebDav, WebSocket sekä FTP. Lisäksi työssä on mukana kaikkien suojaamattomien prokollien suojatut versiot sekä suojattu SFTP- protokolla. Tiedostojen talletukseen käytetään SQL-tietokantaa, NOSQL-tietokantana, Object Storagea, Block Storagea ja File Storagea. Tietoturvan teoriaosuudessa käsitellään RSA- ja TLS- salausta.

Diplotyötä varten pystytettiin testausympäristö Azureen. Azuren virtuaalikoneeseen pystytettin SFTP-, FTPS- ja WebDav -palvelimet tiedonsiirtoa varten. .NET -palvelimen pystytettiin HTTP- ja WebSocket- liikennettä varten. Angularilla tehdyn käyttöliittymän avulla pystyttiin testaamaan HTTP- ja WebSocket liikennettä selaimesta. C#- ja Python -kirjastoja käytettiin testaamaan tiedonsiirtoa eri protokollilla. Tiedostojen tallentamiseen käytettiin Postgres Tietokantaa, Cosmos- tietokantaa, Azure Blob -tietovarastoa, Azure Files- tietovarastoa sekä Azure managed disks- tietovarastoa.

Kustannusvertailussa vertaillaan Azuren talletusratkaisuiden hintoja kolmen eri talletuskoon avulla: 16GB , 245GB ja 1 TB. Talletusratkaisuiden hinnat vaihtelevat merkittävästi. Tiedostojen siirron kustannuksia vertaillaan epäsuorasti siirretyn internet- liikenteen avulla. Jokaiselle protokollalle laskettiin kuinka paljon ne kasvattavat tiedoston kokoa siirrettäessä. SFTP- prokolla kasvatti tiedoston kokoa kaikista eniten.

Tehokkuusvertailussa vertaillaan useaa eri asiaa tekemällä useita testejä. Tiedonsiirrossa huomattiin, että suojaamttomat protokollat ovat hieman nopeampia, mitä suojatut, mutta erot olivat erittäin pieniä. Tiedostojen talletuksessa huomattiin että Cosmos- tietokanta ei sovellu ollenkaan binääritiedostojen tallentamiseen. Talletusratkaisut, joita voitiin käyttää sisäverkossa, oli huomattavasti nopeampia kuin ulkoverkossa olevat talletusratkaisut.

Tietoturvavertailussa tutkittiin TLS-salausprotokollan tietoturvallisuutta tiedostonsiirrossa sekä vertailtiin tarvittavia palomuuriasetuksia eri siirtoprotokollilla. Azuren pääsynhallinnan periaatteet käytiin läpi tässä osiossa sekä Azuren talletusratkaisuissa ja pääsynhallinnassa havaitut tietoturvaongelmat. Lopuksi vielä vertailtiin pilvialustoista tehtyjä tietoturvatutkimuksia. Tutkimuksissa havaittiin että suurin syy tietoturvaongelmiin pilvialustoilla kehitetyissä sovelluksissa liittyy inhimillisiin virheisiin ja pilvialustojen tekniset tietoturvaongelmat ovat erittäin harvinaisia.

abstract

Teemu Pöytäniemi: File transfer and file storages on the Azure cloud platform

Master thesis

Tampere University

Master of engineering, information technology

9/2024

The thesis examines file transfer and file storage on the Azure cloud platform. File transfer and file storage are examined from three perspectives: cost, performance and security. File transfer is compared using different file transfer protocols. The thesis compares the following non-secure protocols: HTTP, WebDav, WebSocket and FTP. In addition, secure versions of all non-secure protocols are included, as well as the secure SFTP protocol. SQL database, NOSQL database, Object Storage, Block Storage and File Storage are used to store the files. The theoretical part of the information security section deals with RSA and TLS encryption.

For the thesis, a testing environment was set up in Azure. SFTP, FTPS and WebDav servers were set up on the Azure virtual machine for data transfer. A .NET server was set up for HTTP and WebSocket traffic. Angular front-end was used to test HTTP and WebSocket traffic from the browser. C# and Python libraries were used to test data transfer using different protocols. Postgres Database, Cosmos Database, Azure Blob, Azure Files and Azure Managed Disks were used to store the files.

The cost comparison compares the prices of Azure's storage solutions using three different storage sizes: 16GB, 245GB and 1 TB. The prices of the storage solutions vary significantly. File transfer costs are compared using indirectly method by measuring transferred internet traffic. For each protocol, it was calculated how much they increase the file size when transferring. The SFTP protocol increased the file size the most.

A performance comparison compares several different things by carrying out several tests. In file transfer, it was found that the unprotected protocols were slightly faster than the protected protocols, but the differences were very small. For file storage, it was found that the Cosmos database is not at all suitable for storing binary files. The storage solutions that could be used on the internal network were significantly faster than the storage solutions on the external network.

The security comparison examined the security of the TLS encryption protocol for file transfer and compared the required firewall settings for different transfer protocols. The principles of Azure's access management were discussed in this section, as well as the security issues identified in Azure's storage and access management solutions. Finally, security studies on cloud platforms were compared. The studies found that the main cause of security problems in applications developed on cloud platforms is related to human error and that technical security problems in cloud platforms are very rare.

ALKUSANAT

Diplomityö on tehty mielenkiinnosta pilvialustoja kohtaan ja se ei liity suoraan minkään yrityksen projektiin. Ajatus työnaiheesta tuli yhdestä terveydenhuollon projektista, jossa ladataan aivokuvia pilvialustalle.

Haluan kiittää Mika Välimäkeä neuvoista ja työn ohjauksesta.

Tampereella, 3.9.2024

Teemu Pöytäniemi

Sisällysluettelo

[1. Johdanto 1](#_Toc175367990)

[2. Teoria 3](#_Toc175367991)

[2.1 Tiedostojen siirto 3](#_Toc175367992)

[2.1.1 HTTP 3](#_Toc175367993)

[2.1.2 WebDav 6](#_Toc175367994)

[2.1.3 WebSocket 7](#_Toc175367995)

[2.1.4 FTP ja FTPS 11](#_Toc175367996)

[2.1.5 SFTP 13](#_Toc175367997)

[2.2 Tiedostojen talletus 15](#_Toc175367998)

[2.2.1 SQL-tietokannat 15](#_Toc175367999)

[2.2.2 NOSQL 16](#_Toc175368000)

[2.2.3 Object Storage 16](#_Toc175368001)

[2.2.4 Block storage 19](#_Toc175368002)

[2.2.5 File storage 20](#_Toc175368003)

[2.3 Pilvialustat 22](#_Toc175368004)

[2.3.1 Microsoft Azure 22](#_Toc175368005)

[2.4 Tietoturva 23](#_Toc175368006)

[2.4.1 RSA 23](#_Toc175368007)

[2.4.2 TLS 24](#_Toc175368008)

[3. Projektin esittely 30](#_Toc175368009)

[4. TULOKSET 31](#_Toc175368010)

[4.1 Tiedostojen siirto 32](#_Toc175368011)

[4.2 Tiedostojen talletus 34](#_Toc175368012)

[5. Projektien tulokset 35](#_Toc175368013)

[5.1 Kustannusvertailu 35](#_Toc175368014)

[5.1.1 Pilvialustojen talletusratkaisujen kustannukset 35](#_Toc175368015)

[5.1.2 Tiedostojen siirron kustannukset 41](#_Toc175368016)

[5.2 Tehokkuusvertailu 43](#_Toc175368017)

[5.3 Tietoturvavertailu 50](#_Toc175368018)

[6. yhteenveto 56](#_Toc175368019)

[Lähteet 58](#_Toc175368020)

LYHENTEET JA MERKINNÄT

ADD engl, Azure Active Directory, Microsoftin pääsynhallintajärjestelmä

AES engl, Advanced Encryption Standard, lohkosalaus

API engl, Application Programming Interface, ohjelman rajapinta

ASCII engl, American Standard Code for Information Interchange,

merkistökoodaus

AWS engl, Amazon Web Services, pilvialusta

C# ohjelmointikieli

DH Diffie–Hellman, salausalgoritmi

DNS engl, Domain Name System, palvelu IP-osoitteiden löytämiseen

EC2 Elastic Compute Cloud, AWS:n virtuaalikonepalvelu

FCP engl, Fibre Channel Protocol, verkkoprotokolla

FTP engl, File Transfer Protocol, tiedonsiirtoprotokolla

FTPS engl, File Transfer Protocol Secure, tiedonsiirtoprotokolla

HDD engl, Hard Disk Drive, talletusratkaisu

HTTP engl, Hypertext Transfer Protocol, tiedonsiirtoprotokolla¨

HTTPS engl, Hypertext Transfer Protocol Secure, tiedonsiirtoprotokolla

IDA engl, Information Dispersal Algoritmia, talletusalgoritmi

IO engl, Input Output, sisään ja ulos menevä liikenne

IOPS engl, Input Output Operations Per Second, IO- operaatioiden määrä sekunnissa

IP engl, Internet Protocol, tiedonsiirtoprotokolla

JSON engl, JavaScript Object Notation, dataformaatti

NIST engl, National Institute of Standards and Technology, Yhdysvaltain kansallinen standardisointi- ja teknologiainstituutti

NOSQL engl, Not only SQL, tietokantamalli

PCAP engl, Packet Capture, verkkokäytäntö

QUIC engl, general-purpose transport layer network protocol,

tiedonsiirtoprotokolla

RC4 engl, Rivest Cipher 4, virtasalaus

REST engl, Representational State Transfer, rajapinta-arkkitehtuuri

RSA Rivest–Shamir–Adleman, julkisen avaimen salausjärjestelmä

SaaS engl, software as a service, sovellus joka on tarjottu palveluna

SAN engl, Storage Area Network, tietoverkko

SCSI engl, Small Computer System Interface, kommunikointiprotokolla

SFTP engl, Secure File Transfer Protocol, tiedonsiirtoprotokolla

SPA engl, Single Page Application,selainkäyttöliittymä

SSD engl, Solid State Drive, talletusratkaisu

SSH engl, Secure Shell, tietoliikenneprotokolla

SSL engl, Secure Sockets Layer, salausprotokolla

SQL engl, Structured Query Language, kyselykieli

TCP engl, Transmission Control Protocol, tiedonsiirtoprotokolla

TLS engl, Transport Layer Security, salausprotokolla

UDP engl, User Datagram Protocol, tiedonsiirtoprotokolla

URL engl. Uniform Resource Locator, verkkosivun osoite

UTF-8 engl, Unicode Transformation Format-8, merkistökoodaus

WAL engl, Write Ahead Logging, tietokantojen protokolla

WebDav engl, Web-based Distributed Authoring and Versioning,

Tiedonsiirtoprotokolla

XML engl, Extensible Markup Language, dataformaatti

XSS engl, Cross-Site Scripting, hyökkäys uhrin selaimeen

.

# Johdanto

Moderni kaupallinen pilvilaskentainfrastruktuuri sai alkunsa vuonna 2002, kun Amazon Web Services (AWS) julkaistiin. Vuonna 2006 Amazon esitteli Simple Storage Service (S3) -palvelun ja Elastic Compute Cloud (EC2) -palvelun. Nämä palvelut olivat ensimmäisiä, jotka hyödynsivät palvelinvirtualisointia ja mahdollistivat asiakkaille palvelimien vuokraamisen heidän sovellustensa infrastruktuuriksi.[1]

Vaikka pilvipalveluiden kasvu oli aluksi hidasta, viimeisten 15 vuoden aikana ne ovat laajentuneet merkittävästi. Google, Microsoft, Oracle ja IBM julkaisivat omat pilvialustansa vuosien 2010 ja 2013 välillä. Tämä auttoi tekemään pilvipalvelut yleisesti saataville, ja pilvialustojen käyttö lisääntyi merkittävästi. Nykyään pilvipalvelut ovat vallanneet suuren osan yritysmaailmasta, ja tuoreimpien tutkimusten mukaan yli 90 % yrityksistä käyttää pilvipalveluita.[2][3]

Pilvilaskenta-alustat voidaan jakaa kolmeen ryhmään: julkiseen, yksityiseen ja hybridiin. Julkiset alustat ovat yleisin pilvipalveluiden muoto. Niissä pilviresurssit (kuten palvelimet ja tallennustila) ovat kolmannen osapuolen pilvipalveluntarjoajan omistamia ja ylläpitämiä, ja ne toimitetaan internetin kautta. Microsoft Azure ja AWS ovat esimerkkejä julkisesta pilvestä. Julkisessa pilvessä samat laitteistot, tallennustilat ja verkkolaitteet jaetaan muiden organisaatioiden tai käyttäjien kanssa.[4]

Yksityinen pilvi koostuu pilvipalveluista, joita käyttää yksinomaan yksi yritys tai organisaatio. Yksityinen pilvi voi sijaita fyysisesti omassa palvelinkeskuksessa tai sitä voi isännöidä kolmannen osapuolen palveluntarjoaja. Hybridipilvi taas yhdistää paikallisen infrastruktuurin tai yksityisen pilvialustan julkiseen pilvialustaan. Hybridialustat mahdollistavat tietojen ja sovellusten liikkumisen kahden ympäristön välillä. Monet organisaatiot valitsevat hybridipilvilähestymistavan liiketoiminnan tarpeiden vuoksi, kuten säännösten ja tietosuojavaatimusten täyttämiseksi, paikan päällä tapahtuvan teknologiainvestoinnin hyödyntämiseksi tai alhaisen viiveen ongelmien ratkaisemiseksi.[4]

Tässä työssä tutkitaan pelkästään julkisen pilven alustoja, erityisesti Microsoftin Azurea. Työssä tarkastellaan tiedostojen siirtämistä ja tallentamista Azure-pilvialustalla sekä vertaillaan julkisista pilvialustoista tehtyjä tietoturvatutkimuksia. Tutkimuksissa on arvioitu, että julkisten pilvialustojen tallennusratkaisuiden liikevaihto vuonna 2023 olisi noin 99 biljoonaa Yhdysvaltain dollaria. Liikevaihdon ennuste vuodelle 2028 on 235 biljoonaa Yhdysvaltain dollaria. [5] Pilvialustojen tallennusratkaisuiden suuri kysyntä ja arviot kysynnän kasvusta olivat yksi motiivi työn tekemiselle. Työ rajoittuu pelkästään binäärimuotoisiin tiedostoihin, eikä se käsittele erikseen esimerkiksi tekstitiedostoja.

Työn teoriaosuudessa tiedostojen siirrosta esitellään kaikki yleisesti käytetyt protokollat, joiden avulla tiedostoja voidaan siirtää pilvialustalle. Tiedostojen tallennuksen osuudessa esitellään pääarkkitehtuurit, joita julkiset pilvialustat tarjoavat tallennusratkaisuille. Tietoturvaosuudessa käsitellään Rivest–Shamir–Adleman (RSA) -salausjärjestelmää sekä Transport Layer Security (TLS) -salausprotokollaa.

Työn tutkimusosassa käsitellään tiedostojen siirtoa ja tallennusta kolmesta eri näkökulmasta: kustannukset, suorituskyky ja tietoturva. Tutkimusta varten Azure-pilvialustalle kehitettiin tarvittavat palvelut tutkittavien asioiden testausta varten. Azureen luotiin tiedonsiirtoprotokollille vaadittavat palvelimet, jotka integroitiin käytettäviin tallennusratkaisuihin. Tiedostojen siirrossa asiakasohjelmana käytetään selaimessa toimivaa käyttöliittymää sekä ohjelmointikielien kirjastoja. Tiedostojen siirron ja tallennuksen suorituskykyä mitataan useilla erilaisilla suorituskykytesteillä. Tallennusratkaisuiden kustannuksia vertaillaan kolmen eri tallennuskokonaisuuden avulla. Työssä pohditaan, millaisia käyttötapauksia varten eri tallennusratkaisut on kehitetty, jotta niiden käyttäminen olisi mahdollisimman kustannustehokasta.

Tiedostojen siirron kustannuksia vertaillaan epäsuorasti siirretyn internetliikenteen määrän perusteella. Internetliikennettä tutkitaan WireShark-nimisen avoimen lähdekoodin pakettianalysaattorin avulla. Tietoturvaosuudessa esitellään suojaamattomien tiedonsiirtoprotokollien ongelmat ja tutkitaan TLS-salausprotokollan turvallisuutta. TLS-salausprotokollaa käytetään suojaamaan salaamattomia tiedonsiirtoprotokollia. Tässä osuudessa esitellään myös Azuren pääsynhallintamekanismit sekä tarkastellaan Azuren palveluiden tietoturvahaavoittuvuuksia. Lopuksi vertaillaan muutamia tutkimuksia, jotka käsittelevät julkisille pilvialustoille kehitettyjen sovellusten tietoturvaa.

# Teoria

## Tiedostojen siirto

Tässä luvussa käsitellään protokollia, joiden avulla tiedostoja voidaan siirtää pilvialustoille. Ensimmäisessä alaluvussa tarkastellaan selainten tarjoamia lataustapoja, minkä jälkeen siirrytään protokolliin, joita erilliset asiakasohjelmat käyttävät.

### HTTP

Hypertext Transfer Protocol (HTTP) on World Wide Webin (WWW) perusta, ja sitä käytetään verkkosivujen lataamiseen hypertekstilinkkien avulla. Hyperteksti on tekstiä, joka näytetään tietokoneen näytöllä tai muussa elektronisessa laitteessa, ja jossa on viittauksia hyperlinkeillä muihin teksteihin, joihin lukija pääsee välittömästi käsiksi. WWW käyttää Hypertext Markup Language (HTML) -tiedostoja määrittämään hypertekstitiedostojen rakenteen ja muotoilun. HTML on standardoitu merkintäkieli asiakirjoille, jotka on suunniteltu näytettäväksi verkkoselaimessa.[6]

HTTP on asiakas-palvelin-protokolla, jossa asiakasohjelma tekee palvelimelle pyynnön, johon palvelin vastaa. HTTP:n yleisin asikasohjelma on verkkoselain, muita yleisiä asikasohjelmia ovat mobiili- ja työpöytäsovellukset. Asiakasohjelma lähettää HTTP-pyynnön palvelimelle, joka vastaa siihen HTTP-vastauksella. HTTP-vastaus sisältää pyydetyt tiedot tai resurssit, kuten verkkosivun, kuvan tai videon. HTTP on tilaton protokolla, mikä tarkoittaa, että jokainen pyyntö ja vastaus ovat itsenäisiä, eivätkä ole riippuvaisia aiemmista pyynnöistä tai vastauksista.[7]

HTTP-pyynnöt koostuvat seuraavista osista: metodi, polku, versio, otsikot ja runko. Metodi määrittää toiminnon, jonka asiakas haluaa suorittaa. Yleisimmät metodit ovat GET ja POST. GET-metodin avulla asiakas pystyy noutamaan tiedostoja palvelimelta, ja POST-metodin avulla asiakas voi lähettää dataa palvelimelle. Muita yleisiä metodeja ovat DELETE, PUT, PATCH, OPTIONS ja HEAD. Polku määrittää halutun resurssin sijainnin palvelimella, ja sen määrittämisessä käytetään Uniform Resource Locator (URL) -osoitteita. Otsikot ovat avain-arvo-pareja tekstimuodossa, joiden avulla asiakas ja palvelin voivat välittää lisätietoja pyyntöjen ja vastausten mukana. Pyynnön runko sisältää tiedot, jotka asiakas lähettää palvelimelle, kuten kirjautumistiedot tai palvelimelle siirrettävän tiedoston. Versio ilmaisee pyynnössä käytetyn HTTP-protokollan version.[8]

HTTP-vastaukset sisältävät tilakoodin, tilaviestin, version, otsikot ja rungon. Tilakoodi on kolminumeroinen luku, joka kertoo, onko tietty HTTP-pyyntö suoritettu onnistuneesti. Tilakoodit voidaan ryhmitellä viiteen kategoriaan pyynnön onnistumisen perusteella: informatiiviset vastaukset, onnistuneet vastaukset, uudelleenohjausviestit, asiakasvirheet ja palvelinvirheet. Tilaviesti on lyhyt tekstikuvaus tilakoodista. Versio, otsikot ja runko toimivat samalla tavalla kuin HTTP-pyynnössä.[8][9]

HTTP-protokollasta on julkaistu useita versioita: HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2 ja HTTP/3. HTTP-protokolla sai alkunsa 1980-luvun lopulla, ja ensimmäinen internet-palvelin kehitettiin CERNissä vuonna 1990. Vuonna 1991 julkaistiin ensimmäinen virallinen dokumentoitu HTTP-versio, nimeltään HTTP/0.9. Se tuki vain GET-pyyntöä, jonka avulla asiakkaat pystyivät noutamaan HTML-asiakirjoja palvelimelta, mutta ei muita tiedostomuotoja.[10][11]

HTTP/1.0 julkaistiin vuonna 1996, ja se käyttää yksinkertaista pyyntö-vastausmallia, jossa asiakas lähettää pyynnön palvelimelle ja palvelin vastaa asiakkaalle. Protokolla tukee GET-, POST- ja HEAD-pyyntöjä, ja siihen lisättiin otsikot sekä tilakoodit. Otsikoiden avulla protokolla mahdollistaa muidenkin tiedostotyyppien siirron kuin pelkkien HTML-dokumenttien. Pyyntö- ja vastausviestit lähetetään verkon yli tekstimuodossa, jossa otsikko ja teksti erotetaan tyhjällä rivillä. Jokaiselle pyynnölle luodaan oma TCP-yhteys, joka katkaistaan vastauksen saavuttua.[11][12]

HTTP/1.1 julkaistiin vuonna 1997, ja siitä julkaistiin päivitetty versio vuonna 1999. HTTP/1.1 tukee pysyviä yhteyksiä, joiden avulla useita pyyntöjä ja vastauksia voidaan lähettää peräkkäin saman TCP-yhteyden kautta. Tämä vähentää uusien yhteyksien luomistarvetta jokaiselle pyynnölle ja parantaa protokollan suorituskykyä. Yksi HTTP/1.1:n merkittävistä ominaisuuksista on HTTP-putkitus, jonka avulla useita HTTP-pyyntöjä voidaan lähettää saman TCP-yhteyden kautta ilman, että pyyntöjen vastauksia tarvitsee odottaa. Tämä parantaa huomattavasti HTML-sivujen latausaikoja, erityisesti korkean viiveen yhteyksissä. Palvelimen täytyy kuitenkin lähettää vastaukset samassa järjestyksessä kuin pyynnöt vastaanotetaan.[11][12]

HTTP/1.1:n suurin suorituskykyongelma on head-of-line (HOL) -esto. Se tapahtuu, kun useampi pyyntö on menossa samaan kohteeseen, mutta jonon kärjessä oleva pyyntö, joka ei voi noutaa vaadittua resurssia, estää kaikki sen takana olevat pyynnöt. HOL-esto ilmenee myös HTTP-putkessa, koska putkessa lähetettyihin pyyntöihin täytyy vastata samassa järjestyksessä. Rinnakkaisten TCP-yhteyksien lisääminen voi helpottaa ongelmaa, mutta samanaikaisten TCP-yhteyksien määrä asiakkaan ja palvelimen välillä on rajallinen, ja jokainen uusi yhteys vaatii merkittäviä resursseja.[10][11][12]

HTTP/2 on päivitetty versio HTTP/1.1-protokollasta, joka otettiin käyttöön vuonna 2015. Se on suunniteltu korjaamaan joitakin HTTP/1.1:n rajoituksia ja suorituskykyongelmia sekä parantamaan verkkoviestinnän nopeutta ja tehokkuutta. Yksi merkittävimmistä eroista HTTP/1.1:n ja HTTP/2:n välillä on binäärikehystyskerros. HTTP/1.1 käsittelee kaikki pyynnöt ja vastaukset tekstimuodossa, kun taas HTTP/2 käyttää binäärikehystyskerrosta viestien kapselointiin binäärimuotoon säilyttäen silti HTTP-semantiikan. Viestien muuntaminen binäärimuotoon mahdollistaa HTTP/2:n käyttämät uudet tiedonsiirtotavat, joita ei ole saatavilla HTTP/1.1.[10][11]

HTTP/2:n binäärinen kehystyskerros koodaa pyynnöt ja vastaukset sekä pilkkoo ne pienemmiksi tietopaketeiksi, mikä lisää huomattavasti tiedonsiirron nopeutta. Toisin kuin HTTP/1.1, joka tarvitsee useita TCP-yhteyksiä HOL-eston vaikutuksen vähentämiseksi, HTTP/2 muodostaa yhden yhteyden kahden palvelimen välille, jossa on useita tietovirtoja. Jokainen tietovirta koostuu useista pyyntö- ja vastausviesteistä, jotka puolestaan jakaantuvat pienempiin yksiköihin, joita kutsutaan kehyksiksi. Yhteys koostuu joukosta binäärikoodattuja kehyksiä, joista jokainen on merkitty tiettyyn tietovirtaan. Tietovirran tunnisteet mahdollistavat kehysten lomittamisen siirron aikana ja niiden kokoamisen uudelleen toisessa päässä. Lomitetut pyynnöt ja vastaukset voivat toimia rinnakkain estämättä niiden takana olevia viestejä. Tätä prosessia kutsutaan multipleksaukseksi, ja se ratkaisee HTTP/1.1:n HOL-eston.[10][11]

Yksi mahdollinen ongelma on, että useat tietovirrat voivat olla riippuvaisia tietyn tietovirran valmistumisesta ja joutuvat odottamaan sen valmistumista. Ongelman ratkaisemiseksi käytetään tietovirtojen priorisointia, jonka avulla tietovirralle voidaan määrittää prioriteetti ja riippuvuussuhde muihin tietovirtoihin. Palvelin käyttää näitä tietoja luodakseen riippuvuuspuun, jonka avulla se voi määrittää, missä järjestyksessä tietovirtojen kehykset lähetetään.[10][11]

HTTP:n uusin versio, HTTP/3, on Googlen kehittämä, ja se julkaistiin vuonna 2015. Suurin muutos verrattuna HTTP/2:een on taustalla olevan siirtokerroksen verkkoprotokollan TCP:n vaihtaminen Quick UDP Internet Connections (QUIC) -protokollaan. QUIC on Googlen vuonna 2012 kehittämä protokolla, joka käyttää siirtokerroksessa UDP:ta TCP:n sijaan. QUIC on multipleksoitu viestintäalgoritmi, joka kehitettiin tehokkaammaksi kuin HTTP/2:n käyttämä multipleksaus.[13][14]

Vaikka HTTP/2 poistaa HOL-eston HTTP-protokollasta, TCP-protokollassa on oma HOL-esto. Jos TCP hukkaa paketin yhdessä HTTP/2:n luomassa tietovirrassa, kaikkien muiden tietovirtojen kehysten siirtäminen samassa TCP-yhteydessä keskeytyy, kunnes hukatut paketit on lähetetty uudelleen. QUIC puolestaan jakaa tietovirran datan pienempiin osiin, joita kutsutaan kehyksiksi. Kehykset lähetetään UDP-paketteina, ja ne sisältävät tietovirran tunnuksen ja järjestysnumeron. Vastaanottaja voi järjestää ne uudelleen, jos ne vastaanotetaan eri järjestyksessä kuin ne lähetettiin. Jos paketti katoaa, QUIC lähettää sen uudelleen aikakatkaisun jälkeen. Logiikka on sama kuin TCP:llä HTTP/2-protokollassa, mutta QUIC:n toiminta ei vaikuta yhteyden muihin tietovirtoihin.[13][14]

### WebDav

Web Distributed Authoring and Versioning (WebDAV) on HTTP/1.1:n laajennus. WebDAV-protokolla esiteltiin alun perin vuonna 1996, ja se standardoitiin ensimmäistä kertaa vuonna 1999. Protokollan nykyinen versio on vuodelta 2007. WebDAV mahdollistaa HTTP-palvelimen toimimisen tiedostopalvelimena, mahdollistaen useamman asiakkaan työskentelyn saman tiedoston parissa samanaikaisesti. WebDAV laajentaa HTTP-otsikoiden ja -metodien standardijoukkoa. WebDAV:n avulla voi luoda, siirtää, muokata, poistaa ja kopioida tiedostoja ja kansioita.[15][16][17]

WebDAV-palvelimet mahdollistavat tiedostojen versioiden seurannan, ja ne on jaettu kahteen luokkaan versioiden seurannan perusteella: luokka 1 ja luokka 2. Luokan 1 WebDAV-palvelimet tarjoavat perushallintaominaisuuksia, kuten mahdollisuuden luoda, kopioida, siirtää tai poistaa tiedostoja ja kansioita. Monet asiakasohjelmat pitävät luokan 1 WebDAV-palvelimia vain lukuoikeuksilla, koska ne eivät voi suojata tiedostoja samanaikaisilta muutoksilta. Luokan 2 WebDAV-palvelimet voivat lukita tiedostoja ja sallivat niiden samanaikaisen muokkauksen.[15][16][17]

WebDAV lisää seuraavat HTTP-metodit HTTP/1.1-standardiin: PROPFIND, PROPPATCH, COPY, MOVE, MKCOL, LOCK ja UNLOCK. WebDAV hyödyntää myös PUT- ja DELETE-metodeja, jotka kuuluvat jo HTTP-standardiin. Protokolla viittaa tiedostoihin ja kansioihin resursseina. PROPFIND-metodilla voi hakea tietoja resursseista, ja PROPPATCH-metodi mahdollistaa niiden muokkaamisen. LOCK-metodi lukitsee valitun resurssin niin, että muut käyttäjät eivät voi tehdä siihen muutoksia, ja UNLOCK-metodi purkaa lukituksen. COPY-metodi kopioi resurssin palvelimella, ja MOVE-metodi siirtää sen. Resurssin voi ladata palvelimelle PUT-metodilla, poistaa DELETE-metodilla ja ladata GET-metodilla.[17]

Kuva 1 esittää esimerkkitapauksen asiakkaan ja palvelimen välisestä liikenteestä, jossa asiakas ensin lukitsee tiedoston, muokkaa sitä ja lopuksi purkaa lukituksen.A screenshot of a computer

Description automatically generated

Kuva 1 Esimerkki WebDav -latauksesta

### WebSocket

WebSocket-protokolla luo kaksisuuntaisen reaaliaikaisen yhteyden asiakkaan ja palvelimen välille. Tämä mahdollistaa sen, että palvelin voi lähettää dataa asiakkaalle ilman asiakkaan erillistä pyyntöä. WebSocket on tilallinen protokolla, mikä tarkoittaa, että asiakkaan ja palvelimen välinen yhteys pysyy aktiivisena, kunnes jompikumpi osapuoli lopettaa sen. Kun asiakas tai palvelin sulkee yhteyden, yhteys katkeaa molemmista päistä. WebSocket toimii TCP:n yli toimivana siirtokerrosprotokollana. Vaikka WebSocket muistuttaa TCP-protokollaa, ne eroavat toisistaan, eikä WebSocketilla voi muodostaa yhteyttä TCP-palvelimeen. WebSocketin pääasiallinen asiakasohjelma on selain, mutta myös muilla asiakasohjelmilla voidaan luoda yhteys palvelimeen. WebSocket API on selaimen ohjelmointirajapinta, joka mahdollistaa yhteyden muodostamisen selaimesta WebSocket-palvelimeen JavaScript-ohjelmointikielen avulla.[18][19]

Kuva 2 esittää WebSocketin arkkitehtuurin korkealla tasolla. Aluksi kättelyvaiheessa käytetään HTTP-protokollaa, minkä jälkeen siirrytään WebSocket-protokollaan.



Kuva 2 webSocket-protokolla

Asiakas aloittaa kättelyprotokollan lähettämällä HTTP GET -pyynnön palvelimelle. Pyynnössä tulee olla mukana tietyt HTTP-otsikot, jotta palvelin hyväksyy pyynnön. Upgrade- ja Connection-otsikoiden arvoilla kerrotaan palvelimelle, että yhteys halutaan vaihtaa WebSocket-protokollaan. WebSocketin version tulee olla 13, joka on nykyinen versio WebSocket-standardista. Pyynnössä on myös mukana Sec-WebSocket-Key-otsikko, jonka arvo on satunnainen 16-tavuinen merkkijono, joka on base64-koodattu. Tämän merkkijonon generoinnin tulee olla kryptografisesti satunnainen, eikä sen arvoa pitäisi pystyä arvaamaan. Jos palvelin hyväksyy kättelyn, HTTP-vastauskoodi on 101.[19]

Kun kättely on onnistuneesti suoritettu, siirrytään WebSocket-protokollaan. Kuva 3 esittää protokollassa siirtyviä kehyksiä, joiden avulla data kulkee. Kehyksen lohkoilla on seuraavat merkitykset alkaen ensimmäisestä bitistä:

* FIN: Tämä yksi bitti ilmaisee, onko kehys viestin viimeinen osa vai onko tulossa lisää kehyksiä.
* RSV1, RSV2, RSV3: Nämä kolme bittiä on varattu tulevia laajennuksia varten. Niiden tulee olla nollia, ellei jokin laajennus ole asettanut niitä muuksi.
* Opcode: 4-bittinen kenttä, joka ilmoittaa kehyksen tyypin, kuten tekstin, binääridatan tai ohjausviestin.
* Mask: Tämä yksi bitti ilmaisee, onko viesti naamioitu vai ei. Asiakkaan lähettämät viestit tulee aina olla naamioitu.
* Datan-pituus: Tämä kenttä ilmaisee datan pituuden
* Naamiointiavain: Jos Mask-bitti on asetettu, tämä 32-bittinen arvo sisältää maskin, joka käytetään datan naamioimiseen.
* Siirrettävä data: Tämä lohko sisältää itse siirrettävän datan, kuten tekstin tai binääridatan.



Kuva 3: WebSocket kehys

Kun asiakas lähettää kehyksen palvelimelle, MASK-bittillä täytyy olla arvo 1, ja 32-bittinen naamiointiavain tulee olla määriteltynä. Tämän avaimen on oltava jokaiselle kehykselle erilainen, ja sen tulee olla luotu kryptografisesti vahvalla algoritmilla, jotta tulevia arvoja ei voida ennustaa aiempien perusteella. Datan naamiointi tapahtuu 8 bitin lohkoissa, ja prosessissa käytetään jakojäännös- ja XOR-operaatioita.[19]

Datan naamioimisen tarkoituksena on tehdä WebSocket-liikenteestä erottuvaa ja arvaamatonta verrattuna HTTP-liikenteeseen. Ilman tätä verkkoinfrastruktuurilaitteet, jotka eivät ole päivitetty käsittelemään WebSocket-liikennettä, saattaisivat virheellisesti luulla sitä normaaliksi HTTP-liikenteeksi. Tämä voisi avata tietoturva-aukkoja. Naamioimalla data voidaan estää tällaisten laitteiden mahdollisesti aiheuttamat riskit. Vaikka hyökkääjä pystyisi hallitsemaan sekä asiakas- että palvelinpuolen koodia, hän ei pysty manipuloimaan kehyksen arvoja, koska naamiointi tekee niistä satunnaisia ja siten vaikeasti ennustettavia. Tämä parantaa verkkoyhteyden tietoturvaa huomattavasti.[20]

4-bittisellä Opcode-koodilla pystytään merkitsemään kehyksen tyyppi. Kehys voi olla datan siirtoon tarkoitettu kehys tai hallintakehys. Jos kehys on hallintakehys, sillä on sovittu hallintakoodi Opcode-lohkossa ja mahdollisesti siirrettävää dataa. Mahdollisia komentoja ovat close, ping ja pong. Close-komento aloittaa yhteyden sulkemisprosessin, ja se voi sisältää datakentässä viestin, miksi yhteys halutaan sulkea. Kun close-komento on vastaanotettu, siihen vastataan lähettämällä kehys, jonka komento on myös close. Close-vastausta voi viivästyttää ja jatkaa datan lähettämistä, mutta silloin ei ole takuita siitä, että close-komennon lähettänyt osapuoli pitää yhteyden auki. Ping-komennon tarkoitus on tarkistaa, että yhteyden toinen pää vastaanottaa edelleen liikennettä. Kun ping-komento on vastaanotettu, siihen vastataan lähettämällä pong-komento.[19][20]

Jos kehys on datan siirtokehys, Opcode-koodilla hallitaan siirrettävän datan formaattia. Mahdollisia vaihtoehtoja ovat binääri ja teksti. Tekstin käyttämä merkistö on UTF-8. Opcoden avulla voidaan pilkkoa lähetettävä data useampaan kehykseen, jolloin kaikkien kehysten datan formaatin on oltava sama kuin ensimmäisen kehyksen. Ensimmäinen kehys määrittää Opcode-arvolla siirrettävän datan tyypin, ja seuraavien kehysten Opcode määrittää, että ne ovat jatkoa edelliselle kehykselle. Datan viimeisen kehyksen FIN-bitin arvo on 1, mikä kertoo, että kyseessä on datan viimeinen kehys.[19][20]

Opcode-koodissa on varattuja komentoja lisäosia varten, joita ei ole määritelty WebSocket-protokollassa. Asiakas voi pyytää lisäosan käyttöä kättelyvaiheessa lisäämällä Sec-WebSocket-Extensions-otsikon pyyntöön. Jos serveri hyväksyy lisäosien käytön, se lisää saman Sec-WebSocket-Extensions-otsikon vastaukseen, johon se listaa hyväksytyt lisäosat.[19][20]

### FTP ja FTPS

File Transfer Protocol (FTP) on tiedostojen siirtoon käytetty protokolla. Protokolla toimii TCP/IP-yhteyden päällä, ja se koostuu asiakkaasta ja palvelimesta. Kuvassa 2 on esitetty FTP-protokollan arkkitehtuuri korkealla tasolla. Sekä asiakas että palvelin tarvitsevat ohjelmat, jotka toteuttavat protokollan. Asiakkaan ohjelma voi olla graafinen käyttöliittymä tai se voi toimia komentoriviltä.[21]



Kuva 4 FTP- protokolla

Protokolla käyttää kahta rinnakkaista TCP-yhteyttä: hallintayhteyttä ja datayhteyttä. Hallintayhteydellä lähetetään kaikki komennot, jotka liittyvät käyttäjien hallintaan ja tiedonsiirtoon, ja se on toteutettu Telnet-protokollalla. Telnet on vanha sanomamuotoinen protokolla, joka toimii TCP-protokollan päällä. Telnetillä pystyy muodostamaan yhteyden etätietokoneelle, ja sitä on aikoinaan käytetty muun muassa sähköpostien lähetykseen. Telnet ei salaa sanomiaan, minkä vuoksi protokolla on tietoturvaltaan heikko. Telnetin käytöstä on luovuttu moderneissa järjestelmissä, ja se on korvattu turvallisemmilla protokollilla, kuten SSH:lla. Hallintayhteydellä määritellään datayhteyden ominaisuudet ja sillä avataan haluttu datayhteys.[21]

Datayhteydellä siirretään tiedostot. Yhdellä aktiivisella yhteydellä voidaan siirtää vain yhtä tiedostoa samanaikaisesti. Datayhteys siirtää datan aina 8-bittisinä tavuina, joita kutsutaan siirtotavun kooksi. FTP tukee muutamia eri tiedonsiirtotyyppejä, joilla se pystyy esittämään siirrettävän datan. Oletustyyppi on ASCII, jota kaikkien FTP-toteutusten täytyy tukea. ASCII on tekstin merkistö, jossa jokainen merkki esitetään 7-bittisenä numerona. Tiedosto lähetetään 8-bittisenä NVT ASCII:na, jossa eniten merkitsevä bitti on nolla ja sen perässä on 7-bittinen ASCII-koodi.Vaihtoehtoinen tiedonsiirtotyyppi tekstitiedostoille on EBCDIC. Se on 8-bittinen merkistö, jota käytetään pääasiassa IBM:n suurtietokoneissa. ASCII- ja EBCDIC-tyypit voivat ottaa myös toisen vapaaehtoisen parametrin, joka määrittää tekstin pystysuuntaista asettelua ja sitä käytetään tekstin tulostuksen muotoiluun.[21]

Image-tyyppi on tarkoitettu binääritiedostojen lähettämiseen. Tiedosto luetaan biteiksi ja bitit lähetetään 8-bittisinä tavuina. Lähetyksen loppuun saatetaan tarvita täytettä, jos tiedoston bitit eivät ole jaollisia kahdeksalla. Täyte on pelkästään nollia, ja asiakkaan ja palvelimen täytyy sopia, kuinka täyte tunnistetaan oikeasta datasta. Local-tyyppi on image-tyypin laajennos, ja sen avulla voidaan muuttaa lähetettävän datan loogisen tavun kokoa annetulla parametrilla.[21]

FTP tukee kolmea eri tiedostonvälitysrakennetta. Tiedostorakenne, tallennerakenne ja sivurakenne: Tiedostorakenteessa tiedostolla ei oleteta olevan mitään sisäistä rakennetta, vaan tiedosto lähetetään binäärimuodossa. Tallennerakenteessa tiedoston oletetaan koostuvan toistuvista pienemmistä osista. Sivurakenteessa tiedoston oletetaan koostuvan sivuista, jotka ovat indeksoitu. Tätä rakennetta käytetään epäjatkuvien tiedostotyyppien kanssa jotka voivat sisältää useampia sisäisiä tiedostoja jotka tunnistetaan tiedostossa olevalla otsikkodatalla.[21]

Datan siirtämisen aloittaminen edellyttää datayhteyden muodostamista sekä siirtoparametrien sopimista. Ensin asiakkaan on avattava datayhteyden portti kuuntelua varten ja lähetettävä pyyntösanoma hallintayhteydellä. Tämä sanoma sisältää tiedon siitä, mihin suuntaan dataa ollaan siirtämässä. Palvelin vastaa pyyntöön ottamalla yhteyden asiakkaan datayhteyden porttiin. Seuraavaksi sovitaan tiedoston siirtotapa. FTP tukee kolmea siirtotapaa: stream, block ja compressed.[21]

Stream-tilassa tiedostot siirretään jatkuvana virtana. Jos tiedoston rakenne on tiedostomuotoinen, tiedoston päättyminen merkitään sulkemalla datayhteys. Tallennerakenteessa käytetään kaksitavuista hallintakoodia osoittamaan osien tai koko tiedoston päättymistä.[21]

Block-siirrossa data jaetaan lohkoihin, ja jokaisella lohkolla on 3-tavuinen otsikko, joka sisältää tiedot lohkon pituudesta ja tyypistä. Lohkon tyypin avulla voidaan määritellä, onko kyseessä tiedoston viimeinen lohko, tallenteen viimeinen lohko vai uudelleenkäynnistysmerkki.[21]

Compressed-siirrossa käytetään yksinkertaista pakkausalgoritmia, nimeltään run-length encoding, joka lähettää dataa lohkoina samalla tavalla kuin block-siirrossa. Pakkaus vähentää siirrettävän datan määrää, mutta yleensä tiedostot pakataan tehokkaammilla algoritmeilla jo niiden luontivaiheessa tai verkkotasolla, esimerkiksi modeemien toimesta.[21]

FTP-protokolla ei sisällä sisäänrakennettua tapaa tarkistaa siirrettävän datan eheyttä, vaan se luottaa TCP-protokollaan tässä tehtävässä. FTP tukee kuitenkin tiedostonsiirron jatkamista, jos lataus keskeytyy. Latauksen jatkaminen on mahdollista vain, jos siirtotapana on block tai compressed. Jatkaminen merkitään lohkon otsikkoon varatulla koodilla, joka osoittaa, mistä tiedoston lataus jatkuu.[21]

FTP-protokolla ei salaa kumpaakaan käyttämäänsä yhteyttä, joten sitä pidetään nykyään tietoturvattomana. FTPS (FTP Secure) on FTP-protokollan turvallisempi lisäosa, joka käyttää SSL- tai TLS-suojausprotokollaa. Suojauksen käyttöönotto voidaan toteuttaa kahdella eri tavalla: implisiittisesti ja eksplisiittisesti. Implisiittinen tapa edellyttää suojausta heti yhteyden muodostamisvaiheessa. Tämä rikkoo yhteensopivuuden pelkästään FTP-protokollaa tukevien asiakasohjelmien ja palvelimien kanssa, jotka eivät tue implisiittistä suojausta. Eksplisiittisessä suojauksessa asiakas pyytää erikseen suojattua yhteyttä. Tämä mahdollistaa sen, että palvelin voi tukea sekä FTP- että FTPS-asiakkaita. Eksplisiittisessä suojauksessa voidaan lisäksi määritellä, mitkä yhteydet suojataan, kun taas implisiittisessä suojauksessa molemmat kanavat (hallinta- ja datayhteys) ovat suojattuja. Esimerkiksi, jos siirrettävä data on jo valmiiksi salattu, voidaan suojata vain hallintayhteys, kun taas datayhteyttä ei välttämättä tarvitse suojata.[21][22]

### SFTP

Secure File Transfer Protocol (SFTP) on tiedostonsiirto- ja tiedostonhallintaprotokolla, joka koostuu palvelimesta ja asiakasohjelmasta. SFTP toimii suojatun kanavan kautta, ja se suunniteltiin SSH-2-protokollan laajennukseksi. SFTP ei suojaa liikennettä itsessään, vaan se luottaa alapuolella olevan kanavan, kuten SSH:n, suojaukseen. SFTP-yhteyden avulla voidaan siirtää tiedostoja sekä suorittaa tiedostonhallintaan liittyviä toimintoja. Vaikka SFTP suunniteltiin alun perin SSH-2-protokollan laajennukseksi, sitä voidaan käyttää myös muiden protokollien, kuten SSH-1:n, kanssa. SSH-1-protokollan käyttö aiheuttaa kuitenkin rajoituksia asiakasohjelmalle, sillä sen on tiedettävä SFTP-palvelimen binääritiedostojen tarkka sijainti palvelimella.[23][24]

SFTP-protokollasta on julkaistu useita versioita, joista nykyisin käytetyin on versio 3, joka julkaistiin vuonna 2001. Tämän jälkeen on julkaistu versiot 4, 5 ja 6, mutta ne eivät ole saaneet laajaa tukea. Useat SFTP-palvelimien kehittäjät ovat ilmoittaneet, että heillä ei ole aikomusta tukea uusimpia versioita tulevaisuudessa.[23][24]

SFTP-protokolla lähettää paketit verkon yli muodossa, jossa paketin alussa on tavun kokoinen tila komennolle, ja sen jälkeen seuraa siirrettävä data. Kuvassa 5 on esitetty SFTP-protokollan arkkitehtuuri, jossa näkyvät pakettien komentojen nimet. Asiakasohjelma lähettää aluksi SSH\_FXP\_INIT-komennon, jonka mukana on haluttu protokollan versio. Palvelin vastaa SSH\_FXP\_VERSION-komennolla, joka sisältää palvelimen tukemat versiot. Asiakasohjelman ja palvelimen on tuettava samaa protokollaversiota, jotta yhteys voidaan muodostaa.[24]

Tiedostojen käsittely tapahtuu niille tarkoitetuilla komennoilla. Esimerkiksi SSH\_FXP\_OPEN-komento avaa tiedoston tai luo uuden tyhjän tiedoston. Palvelin vastaa SSH\_FXP\_OPEN-kyselyyn SSH\_FXP\_HANDLE-komennolla, jos tiedoston avaaminen onnistuu. SSH\_FXP\_HANDLE palauttaa datana ID:n, jonka avulla asiakasohjelma voi käyttää tiedostoa. Asiakas voi tämän jälkeen lukea tiedoston sisällön SSH\_FXP\_READ-lukukomennolla.[24]

Diagram

Description automatically generated

Kuva 5 SFTP-protokolla

## Tiedostojen talletus

Tässä luvussa käsitellään eri talletusrartkaisuita, joita pilvialustat yleisesti tarjoavat.

### SQL-tietokannat

SQL-tietokannat ovat relaatiotietokantoja, joissa tieto on tallennettuna tauluihin, jotka koostuvat riveistä ja sarakkeista. Taulut perustuvat relaatiomalliin, joka pohjautuu predikaattilogiikkaan. Taulu esittää tiettyyn aiheeseen liittyviä tietoja, sarakkeet kuvaavat kokonaisuuden eri ominaisuuksia, ja rivit edustavat kyseisen asian yksittäisiä ilmentymiä. Taulujen riveillä on uniikki tunniste, eli ID, joka voi koostua yhdestä tai useammasta sarakkeen arvosta. Taulujen välille voidaan luoda yhteyksiä avainten avulla. Avaimet toimivat viitteinä toisten taulujen arvoihin, mahdollistaen tietojen yhdistämisen ja viittaamisen eri taulujen välillä.[25]

Tietokannan käyttöä mahdollistavat tietokannan hallintajärjestelmät (DBMS, Database Management Systems). Ne mahdollistavat käyttäjien pääsyn tietokantaan sekä sen päivittämisen ja muokkaamisen. Tietokannan hallintajärjestelmiä on sekä maksullisia että avoimen lähdekoodin ilmaisia vaihtoehtoja. Suosituimmilla avoimen lähdekoodin hallintajärjestelmillä on hyvin samankaltainen pääarkkitehtuuri, vaikka niiden toteutuksissa saattaa olla pieniä eroavaisuuksia.[25]

Kuva 6 esittää Postgres-tietokannan arkkitehtuuria. Postgres on yksi suosituimmista avoimen lähdekoodin tietokannoista, ja se julkaistiin vuonna 1995. Postgres toimii asiakas-palvelin-mallilla, jossa asiakasohjelma ottaa yhteyden hallintajärjestelmään. Postgres luo jokaiselle asiakasyhteydelle oman palvelinprosessin. Kaikilla palvelinprosesseilla on pääsy jaettuun muistiin, joka sijaitsee RAM-muistissa. Tietokantakyselyt kohdistuvat jaettuun muistiin, joka sisältää kopion levyllä olevasta datasta. Jaettu muisti on huomattavasti nopeampi kuin levyltä lukeminen, joten lukuoperaatiot tehdään suoraan jaettuun muistiin.[26][27]

Kirjoitusoperaatiot käsitellään ensin Write-Ahead Log (WAL) -logissa. Muutokset tehdään ensin jaettuun muistiin, ja sen jälkeen WAL-kirjoittaja kirjoittaa muutokset levylle säännöllisenä taustaprosessina. Checkpointer- ja writer-prosessit päivittävät muutokset jaetusta muistista levylle sen jälkeen, kun muutokset on kirjattu WAL-tiedostoon. Levylle kirjoittaminen tapahtuu taustalla pienissä erissä, koska I/O-operaatiot ovat raskaita ja aikaa vieviä. Jaetussa muistissa säilytetään myös poistettujen rivien sekä muutettujen rivien vanhoja versioita, koska muut prosessit saattavat tarvita näitä arvoja. Autovacuum-prosessi poistaa vanhentuneet rivit jaetusta muistista.[26][27]

Diagram

Description automatically generated

Kuva 6 Postgresin arkkitehtuuri

### NoSQL

NoSQL tarjoaa mahdollisuuden tallentaa dataa muussa muodossa kuin relaatiomallin tauluina. Ensimmäiset NoSQL-tietokannat kehitettiin jo 1960-luvulla, mutta termi NoSQL syntyi vasta 2000-luvun alussa. NoSQL-tietokannoille ei ole yhtä yksiselitteistä määritelmää, vaan ne jaetaan neljään pääkategoriaan: asiakirjatietokannat, avain-arvo-tietokannat, sarakepohjaiset tietokannat ja graafitietokannat.. [28]

Asiakirjatietokannat tallentavat datan dokumentteina. Yleisimmin käytetyt dokumenttiformaatit ovat JSON, BSON ja XML. Tietokannan dokumentit voivat olla sisäkkäisiä, ja tiettyjä elementtejä dokumentin sisällä voidaan indeksoida nopeamman haun mahdollistamiseksi. Asiakirjatietokannat käyttävät kokoelmia, joihin tallennetaan yleensä asiakirjoja, joilla on samankaltainen sisältö. Tämä vastaa sitä, miten SQL-tietokannat tallentavat dataa tauluihin. Asiakirjatietokannoissa on joustavat skeemat, mikä tarkoittaa, että kaikissa kokoelman asiakirjoissa ei tarvitse olla samoja kenttiä. Skeemavalidoinnin avulla kentille voidaan luoda sääntöjä, kuten sallitut tietotyypit ja arvoalueet, ja näin varmistaa, että asiakirjojen kentät noudattavat haluttua rakennetta. Asiakirjatietokannoissa on käytössä API tai kyselykieli, joiden avulla voidaan suorittaa operaatioita tietokantaan. [28][29]

Avain-arvo-tietokannat ovat tietokantatyyppejä, joissa data tallennetaan avain-arvo-muodossa, ja ne on optimoitu nopeaan tietojen lukemiseen ja kirjoittamiseen. Tietoja haetaan yksilöllisen avaimen avulla, ja arvot voivat sisältää minkä tahansa tietotyypin. Yksi yleinen käyttötapaus avain-arvo-tietokannoille on datan tallentaminen välimuistiin, joko muistiin tai levylle. [30]

Sarakepohjaiset tietokannat tallentavat datan tauluihin samalla tavalla kuin SQL-tietokannat. Ero näiden tietokantojen välillä syntyy siitä, miten data tallennetaan levylle. Sarakepohjaisissa tietokannoissa data tallennetaan sarakkeittain, kun taas SQL-tietokannoissa data tallennetaan riveittäin. Kuva 7 esittää SQL-tietokantojen ja sarakepohjaisten tietokantojen tapaa tallentaa taulujen data levylle.[30]

A screenshot of a computer

Description automatically generated

Kuva 7 SQL-tietokantojen ja sarakepohjaisten tietokantojen taulujen tallentamisen erot

SQL-tietokannat tallentavat yhden rivin tiedot muistiin samaan paikkaan ja ovat optimoituja rivien nopeaan lukemiseen ja kirjoittamiseen. Sarakepohjaiset tietokannat järjestävät tiedot sarakkeittain ja pitävät kaikki tiettyyn sarakkeeseen liittyvät tiedot muistissa vierekkäin. Ne ovat optimoituja sarakkeiden tehokkaaseen lukemiseen. Sarakepohjaiset tietokannat ovat erityisen hyödyllisiä analyyttisissä kyselyissä, joissa skannataan tai aggregoidaan suuria tietokokonaisuuksia, mutta tarvitaan vain muutamia sarakkeita. Koska vain tarvittavat sarakkeet luetaan tallennustilasta, I/O-operaatioihin kuluva aika on huomattavasti pienempi kuin SQL-tietokannoissa. Vaikka sarakepohjaiset tietokannat soveltuvat erinomaisesti analytiikkaan, niiden kirjoitustapa vaikeuttaa tietojen päivittämistä. Uuden rivin lisääminen tietokantaan vaatii useita kirjoitusoperaatioita, koska jokaisen sarakkeen arvo täytyy kirjoittaa levylle erilliseen paikkaan.[30]

Graafitietokannat tallentavat tiedot solmuina ja reitteinä. Solmut tallentavat tyypillisesti tietoja kohteista, ja reitit tallentavat tietoja solmujen välisistä suhteista. Ne soveltuvat erityisen hyvin monimutkaisiin ja vahvasti kytkeytyneisiin tietoihin, joissa suhteet tai niiden riippuvuudet eivät ole yksinkertaisia. Graafitietokantojen taustalla oleva tallennusmekanismi voi vaihdella. Yleisesti graafitietokannat käyttävät muita tietokantoja tallennusratkaisunaan, ja suosituimmat näistä ovat SQL-tietokannat, asiakirjatietokannat ja avain-arvo-tietokannat. [30]

### Object Storage

Object Storage tarjoaa tallennusratkaisun rakenteettomalle datalle. Tiedostojen tyypillä ja koolla ei ole merkitystä, vaan kaikki tiedostot tallennetaan yhteen ämpäriin. Ämpärissä tiedostoilla ei ole kansiorakennetta, vaan jokaisella tiedostolla on uniikki tunniste (ID). Ämpäriin pääsee käsiksi HTTP REST -rajapinnan kautta, joka mahdollistaa tiedostojen hallinnan. Jokainen Object Storage -palvelua toteuttava taho voi luoda oman REST-rajapintansa, mutta käytännössä lähes kaikki noudattavat Amazon AWS S3 -ämpärin rajapintaa. S3 oli ensimmäinen Object Storage -ratkaisu pilvialustoilla, ja sen hyvin dokumentoitu rajapinta teki siitä erittäin suositun. Tämän seurauksena muut pilvialustat alkoivat tarjota samaa rajapintaa. Object Storage tarjoaa erittäin hyvän skaalautuvuuden, sillä ämpärin kokoa voidaan kasvattaa jopa exatavujen suuruiseksi. Lisäksi Object Storage on kustannustehokas ratkaisu, koska laskutus perustuu ainoastaan käytetyn tallennustilan määrään. Toisin kuin perinteisissä levytallennusratkaisuissa, käyttäjää ei veloiteta ylimääräisestä varalla olevasta tallennustilasta.[31]

Nykyään jokaisella suurella pilvialustalla on oma versio Object Storagesta, ja niiden sisäiset toteutukset voivat vaihdella. Seuraavaksi on esitelty IBM:n Object Storage -toteutus, jonka arkkitehtuuri on esitetty kuvassa 8.

. 

Kuva 8 IBM Object Storage

Manager tarjoaa toiminnot admin-käyttäjille ja mahdollistaa järjestelmän valvonnan sekä hallinnan. Accesser tarjoaa REST-rajapinnan käyttäjille ja vastaa datan salauksesta tallennuksen yhteydessä sekä salauksen purkamisesta lukuvaiheessa. Slicestor on vastuussa tiedostosiivujen tallentamisesta, jotka se saa Accesserilta. Slicestoreiden ryhmää kutsutaan laitekokonaisuudeksi, ja laitekokonaisuuksien ryhmää puolestaan varastointialtaaksi. Ämpärit sijaitsevat sisäisessä arkkitehtuurissa varastointialtaassa. Yksi varastointiallas voi sisältää useita ämpäreitä, ja jokainen ämpäri koostuu Slicstoreista, jotka kuuluvat eri laitekokonaisuuksiin.[32]

Datan tallentamiseen käytetään Information Dispersal Algorithm (IDA) -algoritmia. Algoritmin perusidea on seuraava: tallennettava tiedosto pilkotaan paloiksi, ja palojen lukumäärää kutsutaan algoritmin leveydeksi. Kaikkia näitä paloja ei kuitenkaan tarvita tiedoston lukemiseen tai kirjoittamiseen kokonaisuudessaan, vaan pienempi määrä riittää. Lukukynnysarvo määrittää, kuinka monta palaa tarvitaan alkuperäisen datan lukemiseksi, ja kirjoituskynnysarvo määrittää, kuinka monta palaa on kirjoitettava, jotta kirjoitusoperaatio voidaan merkitä suoritetuksi. Kirjoituskynnysarvo on aina suurempi kuin lukukynnysarvo.[32]

Kuvassa 9 on esitetty tiedoston kirjoitusprosessi. Prosessi alkaa Accesser-palvelusta, joka pilkkoo yli 4 MiB:nkokoiset tiedostot neljäksi erilliseksi siivuksi. Siivut viedään yksitellen loppuprosessin läpi, kun taas pienet tiedostot viedään kokonaisina. Seuraavaksi dataan lisätään tiivistefunktion avulla tarkistusarvo eheyden varmistamiseksi, ja tarvittaessa data salataan lohkosalauksella. Data viipaloidaan ensin lukukynnysarvon määrittämän määrän mukaisesti viipaleiksi, ja näistä viipaleista luodaan algoritmin leveyden verran paloja. Kirjoitusoperaation onnistumiseksi tulee algoritmin kirjoituskynnysarvon mukainen määrä paloja kirjoittaa, jotta operaatio voidaan merkitä suoritetuksi. Nämä palat lähetetään Slicestor-palvelimelle tallennettavaksi. Kun kirjoitusoperaatio on onnistuneesti suoritettu, puuttuvat palaset kirjoitetaan loppuun taustaprosessina. Lukuprosessi toimii käänteisesti kirjoitusprosessiin nähden. Slicestor-palvelimelta luetaan lukukynnysarvon mukainen määrä siivuja, ja näistä siivuista rekonstruoidaan alkuperäinen tiedosto.[32]



Kuva 9 Tiedoston kirjoitusprosessi

### Block storage

Block storage tallentaa datan vakiokokoisina paloina, jotka se tallentaa yksilöllisen tunnisteen avulla. Tavallinen tietokoneen kiintolevy toimii käyttöjärjestelmässä Block storagen kanssa identtisesti tiedostoja tallentaessa. Block storage toteutetaan pilvialustoissa tallennusalueverkkojen (SAN) avulla, jotka ovat yleisimpiä varastointiverkkoarkkitehtuureja. SAN yhdistää useita tallennuslaitteita yhdeksi verkoksi, johon tallennustilaa käyttävät laitteet myös liittyvät.[33]

SAN mahdollistaa verkon luomisen useilla eri protokollilla, mutta kaikki nämä protokollat käyttävät Small Computer System Interface (SCSI) -protokollaa. SCSI on vanha, vuonna 1986 standardoitu protokolla, joka määrittää tiedonsiirtoväylän sekä sen, miten siihen kytketyt laitteet kommunikoivat keskenään. Monet tietokonearkkitehtuurit sisältävät erillisen I/O-väylän, jonka avulla suoritin (CPU) kommunikoi I/O-laitteiden kanssa. Tämä väylä toteuttaa SCSI-protokollan. SCSI-väylällä voidaan yhdistää useita tallennuslaitteita ja palvelimia, mutta sen skaalautuvuus on erittäin rajallinen. Verkkoon voidaan liittää vain rajallinen määrä laitteita, ja kaapelien maksimipituus on lyhyt. Versiosta riippuen verkkoon voidaan liittää 8–16 laitetta, ja laitteiden välinen etäisyys voi olla enintään noin 20 metriä. Koska SCSI-väylät eivät ole tehokkaita tallennusalueverkkojen (SAN) luomiseen, ne on korvattu paremmilla ja skaalautuvammilla väylillä.[34]

Valokuituverkot käyttävät valokuituja tiedonsiirtoon, ja Fibre Channel Protocol (FCP) on näiden verkkojen käyttämä protokolla. Valokuituverkot vastaanottavat SCSI-komentoja, muuntavat ne FCP-protokollan komennoiksi tiedonsiirron ajaksi ja muuttavat ne takaisin SCSI-komennoiksi, kun siirto on suoritettu. Tätä varten käyttöjärjestelmään on asennettava oma laiteajuri. Tallennustilaa käyttävät laitteet ja tallennuslaitteet kytketään samaan valokuituverkkoon, jolloin tiedonsiirrot eivät kuormita normaalia internetyhteyttä. Tämä protokolla on yleisimmin käytetty ja nopein ratkaisu, koska valokuituverkko on erittäin tehokas tiedostojen siirtoon. Haittapuolena on verkon korkea hinta ja sen ylläpitämiseen tarvittava erityisosaaminen. [35]

Toiseksi yleisin protokolla on iSCSI, joka käyttää internetyhteyttä valokuituverkon sijasta. iSCSI on huomattavasti edullisempi kuin valokuituverkot, mutta myös hitaampi. iSCSI siirtää SCSI-komennot TCP-protokollan avulla verkossa. iSCSI on myös tehottomampi tapa siirtää dataa, koska TCP-paketeissa on huomattavasti enemmän ylimääräistä dataa verrattuna FCP-protokollaan. Muita TCP:tä käyttäviä SAN-protokollia ovat iFCP ja FCIP, mutta ne ovat huomattavasti vähemmän käytettyjä kuin iSCSI. [34]

Pilvipalveluiden tarjoamat Block storage -ratkaisut on lähes poikkeuksetta toteutettu iSCSI-protokollan avulla, ja ne voidaan liittää virtuaalikoneisiin tavallisina hakemistoina. Block storageen tallennettu data ei ole sidottu virtuaalikoneen elinkaareen, eli data säilyy, vaikka virtuaalikone, johon Block storage oli liitetty, poistettaisiin.

### File storage

File storage tallentaa datan hierarkkisessa rakenteessa käyttäen tiedostoja ja kansioita. File storage mahdollistaa levyn käytön useille yhtäaikaisille käyttäjille, ja sen toteutus perustuu samoihin teknologioihin kuin tavallinen verkkolevy. Yleisin teknologia on Network Attached Storage (NAS), joka on esitetty kuvassa 10. NAS käyttää sisäisesti samoja teknologioita kuin SAN, mutta lisää oman protokollakerroksen hallitsemaan tiedostoja. NAS-palvelin avaa IP-osoitteen, johon asiakkaat voivat ottaa yhteyden LAN-verkosta. Tiedostot liikkuvat samassa verkossa, missä muukin internetliikenne tapahtuu, ja tiedostojen siirto voi kuormittaa muuta internetliikennettä. NAS edellyttää asiakkailta erillistä asiakasohjelmaa, joka on käyttöjärjestelmästä riippuvainen. Yleisin asiakasjärjestelmän protokolla on Network File System (NFS)..[36]



Kuva 10 NAS-arkkitehtuuri

## Pilvialustat

Tässä kappaleessa käsitellään projektissä läytettävät julkisen pilven palvelut.

### Microsoft Azure

Microsoft Azure on Microsoftin ylläpitämä pilvipalvelu, joka julkistettiin Microsoftin Professional Developers Conferencessa (PDC) lokakuussa 2008. Virallisesti se julkaistiin helmikuussa 2010 nimellä Windows Azure vaihtoehtona silloisille tunnetuille Amazonin ja Googlen pilvialustoille. Azuren ensimmäinen versio tarjosi hyvin rajoitetun joukon palveluita, kuten pilvipalvelun ASP.NET-verkkosovellusten kehittämiseen ja käyttämiseen, Azure Blob -tietovaraston, Azure SQL -pilvitietokannan ja Azure Service Busin. Vuonna 2014 alustan nimi muutettiin nykyiseksi Microsoft Azureksi. Azuren kehitystarina alkoi jo vuonna 2005, kun Microsoft osti Groove Networksin, ja tämän jälkeen Microsoftin kehittäjät aloittivat pilvikäyttöjärjestelmän kehittämisen. Azurea koodattiin aluksi koodinimellä Red Dog, ja se oli tuolloin Windows NT:n laajennus, joka oli suunniteltu toimimaan pilvessä.[37]

Azure tarjoaa ohjelmistoa palveluna (SaaS), alustaa palveluna (PaaS) ja infrastruktuuria palveluna (IaaS). Se tukee monia erilaisia ohjelmointikieliä, työkaluja ja kehyksiä, mukaan lukien sekä Microsoftin omat että kolmannen osapuolen ohjelmistot ja järjestelmät.[37]

Azure, kuten muutkin pilvialustat, perustuu virtualisointiteknologiaan. Tietojenkäsittelyssä virtualisointi tarkoittaa virtuaalisen version luomista jostakin tietokoneen osasta, kuten virtuaalisista tietokonelaitteistoista, tallennuslaitteista ja tietokoneverkkoresursseista. Suurin osa tietokonelaitteistoista voidaan virtualisoida ohjelmiston avulla. Tietokonelaitteisto koostuu yksinkertaisesti joukosta ohjeita, jotka on pysyvästi tai puolipysyvästi koodattu piihin. Virtualisointikerrokset toimivat siltana ohjelmiston ja laitteiston ohjeiden välillä. Ne mahdollistavat sen, että virtualisoitu laitteisto voidaan suorittaa ohjelmistossa samalla tavalla kuin fyysinen laitteisto.[38]

Pohjimmiltaan pilvialustat koostuvat joukosta fyysisiä palvelimia yhdessä tai useammassa datakeskuksessa. Nämä datankeskukset tarjoavat virtualisoituja laitteistoja asiakkaille. Jokaisessa datankeskuksessa on kokoelma palvelimia, jotka on järjestetty palvelintelineisiin. Jokainen palvelinteline sisältää useita palvelinkortteja sekä verkkokytkimen, jotka tarjoavat verkkoyhteyden. Lisäksi telineissä on virranjakeluyksikkö (PDU), joka huolehtii sähkönjakelusta. Palvelintelineet voidaan myös ryhmitellä suuremmiksi yksiköiksi, joita kutsutaan klustereiksi. Nämä telineet tai klusterit suorittavat virtualisoituja laitteistoja käyttäjille.[38]

Joissakin palvelimissa ajetaan kuitenkin pilvihallintaohjelmistoa, joka tunnetaan kuituohjaimena. Kuituohjain on hajautettu sovellus, jolla on useita tehtäviä, kuten palveluiden allokointi, palvelimien ja niiden suorittamien palveluiden kunnon valvonta sekä palvelimien korjaaminen, jos ne kaatuvat. Kuituohjaimet ovat yhteydessä pilviorkesteriohjelmistoon, joka huolehtii palvelimista, rajapinnoista ja sisäisistä tietokannoista, joita Azure tarvitsee toimiakseen.[38]

Pilviorkesteriohjelmisto käsittelee muun muassa käyttäjien hallintakäyttöliittymän kautta tekemiä pyyntöjä, joilla varataan Azure-resursseja ja -palveluita. Käyttöliittymä tarkistaa ensin, onko käyttäjällä oikeudet pyydettyjen resurssien varaamiseen. Jos oikeudet ovat kunnossa, käyttöliittymä tarkistaa tietokannasta palvelintelineen, jolla on riittävä kapasiteetti. Sen jälkeen käyttöliittymä kehottaa kuituohjainta varaamaan resurssin käyttäjälle.[38]

## Tietoturva

Tässä kappaleessa käsitellään tietoturvaan liittyviä protokollia

### RSA

Rivest–Shamir–Adleman (RSA) on julkisen avaimen salausjärjestelmä ja yksi vanhimmista yleisesti käytetyistä salausmenetelmistä. RSA salaa tai allekirjoittaa tiedot kahdella eri avaimella: julkisella ja yksityisellä avaimella. Julkinen avain on kaikkien käytettävissä, kun taas yksityinen avain pidetään salassa. Julkisella avaimella salattujen tietojen salaus voidaan purkaa vain yksityisellä avaimella.[39]

Allekirjoittamisessa käytetään yksityistä avainta allekirjoituksen luomiseen, ja kuka tahansa voi vahvistaa allekirjoituksen aitouden julkisen avaimen avulla. Kahden avaimen käytön vuoksi julkisen avaimen salaus tunnetaan myös epäsymmetrisenä salauksena, koska salaus ja salauksen purku tapahtuvat eri avaimilla. Toisin kuin epäsymmetrisessä salauksessa, symmetrisessä salauksessa samaa avainta käytetään sekä salauksen luomiseen että purkamiseen.[39]

Nimi RSA tulee Ron Rivestin, Adi Shamirin ja Leonard Adlemanin sukunimistä, jotka julkaisivat algoritmin vuonna 1977. RSA:n turvallisuus perustuu siihen, kuinka vaikeaa on käytännössä jakaa kahden suuren alkuluvun tulo tekijöihinsä. RSA-salauksen murtaminen tunnetaan RSA-ongelmana. Tätä ongelmaa ei ole onnistuttu ratkaisemaan, jos käytössä on riittävän suuri avain. RSA on kuitenkin suhteellisen hidas algoritmi, minkä vuoksi sitä ei yleensä käytetä suoraan tietojen salaamiseen, vaan sen avulla salataan jaettuja avaimia, joita käytetään symmetrisessä salauksessa.[39]

RSA:n perusperiaate on, että on suhteellisen helppoa löytää kolme erittäin suurta positiivista kokonaislukua , ja , niin että kaikille kokonaisluvuille , jotka täyttävät ehdon , pätee seuraava yhtälö:

Kun annetaan vain ja , on erittäin vaikea löytää . Kaavassa Kokonaisluvut ja muodostavat julkisen avaimen, on yksityinen avain ja on viesti. Koska ja d voidaan vaihtaa kaavassa päikseen, mahdollistaa se viestien allekirjoittamisen ja allekirjoituksen tarkistamisen samaa algoritmia käyttäen. julkinen avain muodostetaan kahden satunnaisen suuren alkuluvun tulona, ja sen pituus määrittää julkisen avaimen pituuden. on positiivinen satunnainen kokonaisluku, jonka arvon valintaväli määritetään Carmichaelin funktion avulla. Yksityinen avain saadaan myös laskettua Carmichael funktion ja julkisen avaimen avulla. Viesti saadaan salattua laskemalla seuraava salakirjoitus käyttäen julkista avainta ja kaavalla.

Salattu viesti voidaan myöhemmin purkaa käyttämällä yksityistä avainta , jolloin alkuperäinen viesti saadaan takaisin kaavalla: [39][40]

### TLS

TLS on julkisen avaimen salausmenetelmä, joka on luotu vanhentuneen SSL-protokollan päivitettynä versiona. SSL:n ensimmäistä versiota ei koskaan julkaistu tietoturvaongelmien takia, mutta ensimmäinen julkaistu versio, SSL 2.0, julkaistiin vuonna 1995. SSL 2.0:ssa havaittiin pian tietoturvaongelmia, jotka korjattiin seuraavana vuonna julkaistussa SSL 3.0 -versiossa. TLS 1.0 julkaistiin vuonna 1999, eikä siinä ollut merkittäviä eroja SSL 3.0 -versioon verrattuna. Vuonna 2006 julkaistu TLS 1.1 toi lisää tietoturvaparannuksia. TLS 1.2 julkaistiin vuonna 2008, ja nykyinen uusin versio, TLS 1.3, julkaistiin vuonna 2018. Uudemmat versiot ovat parantaneet tietoturvaa poistamalla protokollasta vanhentuneita ja murtuneita salausalgoritmeja sekä pakottamalla käyttämään vahvempia avaimia salausalgoritmeissa.[41]

TLS käyttää X.509-sertifikaattistandardin varmenteita viestintäkumppanin todentamiseen. Kun asiakas ottaa yhteyden palvelimeen, palvelin lähettää varmenteen asiakkaalle. Tärkeitä tietoja varmenteessa ovat verkkotunnuksen nimi, jolle varmenne on myönnetty, varmenneviranomainen (CA), joka on myöntänyt varmenteen ja allekirjoittanut sen, varmenteen voimassaoloaika sekä palvelimen julkinen avain. [42][43]

CA on kolmannen osapuolen palvelu, joka tallentaa, allekirjoittaa ja myöntää digitaalisia varmenteita. Molemmat osapuolet, sekä asiakas että palvelin, luottavat CA:han. Asiakkaalla on luotettujen varmenneviranomaisten lista ja niiden julkiset avaimet. Asiakas pystyy vahvistamaan palvelimen varmenteen oikeellisuuden tarkistamalla CA:n tekemän allekirjoituksen, joka on luotu CA:n yksityisellä avaimella. [42][43]

Ennen varmenteen allekirjoittamista varmenneviranomaisen on varmistettava, että palvelin todella omistaa verkkotunnuksen, jolle varmenne on pyydetty. Tämä todentaminen voidaan suorittaa esimerkiksi DNS-tietueiden avulla. CA:n tekemän allekirjoituksen avulla asiakas voi luottaa palvelimen identiteettiin. Varmenteen voi myös allekirjoittaa omalla yksityisellä avaimella, jolloin puhutaan itseallekirjoitetuista varmenteista. Tällöin asiakas ei voi varmistaa palvelimen aitoutta varmenneviranomaisten kautta, vaan luottamus täytyy todentaa toisella tavalla. [42][43]

TLS-kättely on prosessi, joka käynnistää TLS:ää käyttävän viestintäistunnon. TLS-kättelyn aikana kaksi kommunikoivaa osapuolta vaihtavat viestejä vahvistaakseen toisensa, sopiakseen käytettävistä salausalgoritmeista ja sopiakseen istuntoavaimista. TLS-versioissa ennen versiota 1.3 prosessi etenee seuraavasti:

Ensimmäiseksi asiakas lähettää viestin palvelimelle, jossa se ilmoittaa tukemansa TLS-versiot ja salausalgoritmit. Lisäksi asiakas lähettää satunnaisesti generoidun numeron. Palvelin vastaa valitsemalla korkeimman TLS-version, jota molemmat osapuolet tukevat, sekä yhteisesti tukeman salauksen. Palvelin lähettää myös oman satunnaisesti generoidun numeron sekä SSL-sertifikaatin asiakkaalle, jonka avulla asiakas voi varmistaa sertifikaatin aitouden.[44]

Kun sertifikaatin aitous on varmistettu, asiakkaalla on useita tapoja jakaa symmetriseen salaukseen käytettävä avain palvelimen kanssa. Yksinkertaisin tapa on RSA-kättely, jossa asiakas lähettää palvelimelle avaimen salattuna palvelimen julkisella avaimella. Ainoastaan palvelin pystyy purkamaan tämän salauksen yksityisellä avaimellaan.[44]

Monimutkaisempi tapa avaimen vaihtoon on käyttää Diffie–Hellman-avaintenvaihtoprotokollaa (DH). DH-protokollassa avainta ei lähetetä salattuna toiselle osapuolelle, vaan molemmat osapuolet laskevat yhteisen salaisuuden julkisia arvoja käyttäen. DH-protokollassa valitaan alkuluku ja sen generaattori , jotka jaetaan julkisesti osapuolten välillä. Molemmat osapuolet valitsevat itselleen salaisen luvun ja laskevat siitä julkisen luvun kaavalla:

Osapuolet jakavat julkiset luvut toisilleen ja laskevat yhteisen salaisuuden kaavalla:

jossa on toisen osapuolen julkaisema julkinen luku ja on oma salainen luku.[44][45][46]

TLS 1.3 yksinkertaistaa kättelyprosessia merkittävästi ja parantaa tietoturvaa poistamalla protokollasta epäturvallisia algoritmeja. Yhteisen salaisuuden jakamisessa TLS 1.3 vaatii eteenpäin turvattavuutta. Tämä tarkoittaa, että vaikka palvelimen yksityinen avain paljastuisi tulevaisuudessa, sillä ei voida purkaa aiempia salauksia. Tämän vuoksi aiemmin mainittu RSA-kättely ei ole enää mahdollista, ja Diffie-Hellman-protokollassa (DH) vaaditaan, että jokaiselle yhteydelle käytetään aina uusia julkisia parametrejä. [44]

Asiakas lähettää ensimmäisessä viestissään satunnaisesti generoidun numeron, tukemansa symmetriset salausalgoritmit sekä valitsee menetelmän yhteisen salaisuuden jakamiseen ja laskee siihen tarvittavat julkiset arvot. Tässä vaiheessa asiakas ei voi tietää varmasti, tukeeko palvelin valittua menetelmää, mutta koska vaihtoehtoja on vähemmän kuin aikaisemmissa versioissa, on todennäköistä, että palvelin tukee asiakkaan valintaa. [44]

Palvelin vastaa tähän viestiin valitulla symmetrisellä salausalgoritmilla, omalla satunnaisluvullaan sekä menetelmällä yhteisen salaisuuden jakamiseen, johon se on laskenut omat julkiset arvonsa. Palvelin pystyy tässä vaiheessa laskemaan yhteisen salaisuuden ja on valmis aloittamaan symmetrisen salauksen käytön. Palvelimen viesti toimii samalla kuittauksena aloittaa salattu yhteys. [44]

Asiakas laskee jaetun salaisuuden palvelimen vastauksen perusteella ja on valmis käyttämään symmetristä salausta. Asiakas varmistaa vielä palvelimen varmenteen aitouden ja lähettää kuittausviestin palvelimelle. Kättely on nyt suoritettu, ja yhteys jatkuu symmetrisellä salauksella. [44]

TLS 1.3 tukee myös nopeampaa TLS-kättelyn versiota, joka ei vaadi lainkaan edestakaisia viestejä. Jos asiakas ja palvelin ovat aiemmin muodostaneet yhteyden, ne voivat luoda toisen jaetun salaisuuden ensimmäisen yhteyden aikana käytettäväksi seuraavaa yhteyttä varten. Palvelin lähettää asiakkaalle myös istuntolipun yhteyden aikana. Seuraavan yhteyden alkaessa asiakas voi käyttää istuntolippua ja yhteyden jatkamista varten luotua salaisuutta, jolloin TLS-salaus voidaan pystyttää ilman perinteistä kättelyvaihetta..[44]

Symmetrisessä salauksessa käytetään joko lohko- tai virtasalausalgoritmia. Lohkosalausalgoritmi ottaa vakiokokoisen lohkon dataa ja salaa sen salatekstiksi. Virtasalauksessa jokainen salattavan tekstin bitti salataan yksitellen salausnumerovirran vastaavalla bitillä, jotta saadaan salatekstivirran bitti. Lohkosalausta voidaan käyttää virtasalauksen tapaan, jos hyödynnetään alustusvektoreita: alustusvektori salataan lohkosalauksella, ja salattu alustusvektori yhdistetään salattavaan tekstiin. TLS-protokollan symmetrisessä salauksessa käytetään lohkosalausta virtasalauksen kaltaisesti. Salauksen lisäksi algoritmin täytyy pystyä todentamaan salatun datan aitous eli varmistaa, ettei kukaan ole muokannut dataa siirron aikana. Tällaisia salausjärjestelmiä, jotka pystyvät sekä salaamaan datan että todentamaan sen aitouden, kutsutaan todennetuksi salaukseksi (AE). Yleisin AE-algoritmi on Galois/Counter Mode (GCM), jota TLS-protokolla käyttää. TLS 1.3 mahdollistaa myös toisen AE-algoritmin, Counter with CBC-MAC (CCM), jota aiemmat TLS-versiot eivät tukeneet.[47][48][49]

TLS 1.2 ja sitä aikaisemmat versiot käyttävät useita eri lohko- ja virtasalausalgoritmeja, mutta TLS 1.3 versiossa käytetään vain yhtä lohkosalausta (AES) ja yhtä virtasalausta (ChaCha20). AES (Advanced Encryption Standard), joka tunnetaan myös alkuperäisellä nimellään Rijndael, on Yhdysvaltain kansallisen standardisointi- ja teknologiainstituutin (NIST) vuonna 2008 vahvistama spesifikaatio lohkosalaukseen. AES on nykyään yksi käytetyimmistä lohkosalausalgoritmeista, ja siitä on olemassa variaatiot 128-, 192- ja 256-bittisille avaimille.[50][44]

Kuvassa 11 on esitetty lohkokaavio AES-GCM -todennetun salauksen järjestelmästä, jota sekä TLS 1.3 että TLS 1.2 käyttävät.

A diagram of a computer program

Description automatically generated

Kuva 11 AES-GCM

Lohkokaavion yläosassa lasketaan salattu data AES-algoritmilla, ja alaosassa lasketaan varmenne salatusta datasta, jonka avulla voidaan todentaa, että dataa ei ole muokattu siirron aikana. Salauksessa käytetään alustusvektoria (IV), johon lisätään lohkonumero, ja tämä summa salataan AES-algoritmin avulla. Varmenne lasketaan Galois'n kuntien avulla, ja siihen luodaan avain AES-salauksessa käytetyn avaimen pohjalta. Varmenteen laskemiseen käytetään salattua dataa, alustusvektoria sekä mahdollista ylimääräistä dataa. AES-GCM mahdollistaa myös ylimääräisen salaamattoman datan lähettämisen salatun datan kanssa ja pystyy todentamaan tämän aitouden ottamalla sen mukaan varmenteen laskentaan. Tämä on merkitty kaavioon nimellä AAD (Additional Authenticated Data).. [47][50]

Kuva 12 esittää F5 Labsin tekemän The 2021 TLS Telemetry Report -tutkimuksen tuloksia TLS:n käytetyimmistä salausalgoritmeista. Tutkimuksessa on mukana miljoona käytetyintä nettisivustoa. Salausalgoritmit on esitetty muodossa yhteisen salaisuuden jakaminen – symmetrinen salaus – MAC. Tutkimuksen mukaan neljä yleisintä algoritmia käyttävät kaikki symmetriseen salaukseen AES-GCM-algoritmia, joka esiteltiin edellisessä kappaleessa. Kun neljän suosituimman algoritmin käyttöprosentit lasketaan yhteen, havaitaan, että AES-GCM suojaa 93,2 % kaikista TLS-yhteyksistä. Lisäksi kuvasta käy ilmi, että yhteisen salaisuuden jakamiseen käytetään DH-protokollan monimutkaisempaa elliptisiin käyriin perustuvaa versiota, joka on merkitty kuvaan lyhenteellä ECDHE (Elliptic Curve Diffie-Hellman Ephemeral).[51]

A screenshot of a computer

Description automatically generated

Kuva 12 Suosituimmat TLS-salausalgoritmit vuonna 2021

# Testausympäristö

Työssä esitellään useampi pienempi testausprojekti, jotka voidaan jakaa karkeasti kahteen osioon: tiedostojen siirtoon sekä tiedostojen talletukseen. Kokonaisjärjestelmän arkkitehtuuri on esitetty kuvassa 13, joka kattaa sekä tiedostojen siirron että talletuksen. Järjestelmän luomiseen on käytetty Azure-pilvipalvelua ja testejä ajetaan Azuren ulkopuolella paikallisella tietokoneella. Azuressa on käytössä virtuaalikone, jossa pyörii testaukseen vaadittavia palvelimia. Käyttöliittymä on toteutettu Angular ohjelmointikehyksen avulla, ja se on toteutettu Single Page Application (SPA) arkkitehtuurilla. Nginx-palvelinta käytetään SPA-käyttöliittymän jakamiseen internettiin. Virtuaalikoneella on myös asennettu vsftp-palvelin, joka on FTP palvelin, joka mahdollistaa myös FTPS-yhteyden. WebDav palvelin on toteutettu Apache -palvelimen avulla OpenSSH-palvelinta käytetään SFTP-yhteyden luomiseen. Virtuaalikoneeseen on liitetty Bock ja File storaget, ja ne on sidottu osaksi virtuaalikoneen tiedostojärjestelmää. Blob storageen ja Dynamo-tietokantaan pääsee käsiksi julkisen HTTP rajapinnan kautta. Dynamo-tietokanta on Azuren toteuttama NoSQL-tietokanta, jossa data on tallennettuna JSON-dokumentteina. Virtuaalikoneeen kanssa samassa virtuaalisessa sisäverkossa on myös Postgres SQL-palvelin. Virtaalikone kommunikoi SQL palvelimen kanssa C# ohjelmoiintikielellä toteutetun asiakasohjelman avulla.

Diagram

Description automatically generated

Kuva 13 Testiohjelman kokonaisarkkitehtuuri

## Tiedostojen siirto

Tiedostojen siirtoon liittyvät projektit ovat jaoteltu useampaan pienempään projektiin eri tiedostonsiirtotapojen perusteella. FTP-, FTPS- ja SFTP-siirrot muodostavat yhden projektin ja selaimella toimivat protokollat muodostavat oman projektin.

FTP, FTPS ja SFTP siirrot ovat toteutettu kahdella eri ohjelmointikielen kirjastolla. Käytetyt ohjelmointikielet ovat Python sekä C#. Python-ohjelmointikielelllä on FTP- ja FTPS-kirjastot totetettuna standardikirjastona, eikä siihen ei tarvita kolmannen osapuolen kirjastoja. SFTP-yhteys on luotu Paramiko -kirjastolla, joka on kolmannen osapuolen ilmaisen lähdekoodin kirjasto. C#-koodissa on läytetty kolmannen osapuolen Nuget -paketteja yhteyksien luomiseen. FluentFTP -kirjastoa on käytetty FTP- ja FTPS-yhteyksien luomiseen ja SSH.NET-kirjastoa SFTP-yhteyteen. Projektissa on ladattu erikokoisia tiedostoja käyttäen kumpaakin ohjelmointikieltä. Tiedostojen koot ovat olleet kilotavun ja 10 megatavun välissä. Saman kokoinen tiedosto on ladattu viiteen kertaan ja jokaisen latauksen latausaika on kirjattu muistiin. Näistä latausajoista on laskettu keskiarvo kullekin tiedostokoolle ja keskiarvoja on käytetty tulosten käsittelemiseen

Selaimella toimivia protokollia eli HTTP- ja WebSocket-prokollia on testattu selainpohjaisen käyttöliittymän avulla sekä C# ohjelmointikielen avulla. Kuvassa 9 on näyttökuva käyttöliittymän HTTP-latauksesta

Graphical user interface, text, application

Description automatically generated

Kuva 14 HTTP-latausnäkymä

Käyttöliittymällä pystyy valitsemaan eri asetuksia käytettäviin protokolliin. HTTP-latauksessa tiedostoa ei lueta kokonaan selaimeen muistiin, vaan se luetaan palasina. Jos tiedostoa ei palotelttaisi, koko tiedosto pitäisi lukea selaimen käyttämään RAM- muistiin ja se rajoittaisi merkittävästi lähetettävän tiedoston maksimikokoa. Tiedoston paloittelemisen avulla lähetettävällä tiedostolla ei ole maksimikokoa rajoittavaa tekijää. Käyttöliittymässä on valittavana 5kB-, 50kB- ja 500kB -kokoiset palaset. Kukin palanen läheteään omana POST-pyyntönä palvelimellle ja viimeisen palasen jälkeen palvelin kokoaa palaset yhteen ja muodostaa kokonaisen tiedoston palvelimella. Toinen valittava ominaisuus on lähetettävän palasen koodaus. Kaikissa koodauksissa tiedoston palanen luetaan selaimen File API:n avulla ArrayBuffer-tyyppisenä selaimen muistiin. Arraybuffer on datan esitys kahdeksan bittisenä numeroina taulukkotietorakenteessa. Data voidaan siirtää käyttäen eri koodauksia siirrossa. Base64 -koodauksessa binäärinen data muunnetaan merkkijonoksi. Base64 koodisto käyttää 64 -merkkistä aakkostoa, johon binääridata muunnetaan. Number array-valinta lähettää binäärisen datan merkkijonona ilman koodausta. Tämä vaihtoehto kasvattaa huomattavasti siirrettävän tiedoston kokoa, koska jokaisen tavun jokainen numero esitetään UTF -8 merkkinä siirron aikana. Base64 ja Number array siirtävät datan json-formaattina, jonka merkistö on UTF-8. Form-data formaatti siirtää datan binäärimuodossa ja dataa ei tarvitse lähettää merkkijonona.

WebSocket-protokollalla on mahdollista valita siirrettävän datan formaatti. Valittavana on merkkijono sekä binääri. Merkkijono käyttää UTF-merkistöä siirrettävän datan koodauksena ja binääri käyttää binääriformaattia tiedonsiirtoon.

Käyttöliittymää ohjataan testeissä Selenium -kirjastolla, jolla pystyy automatisoimaan selaimen käyttöä. Seleniumin avulla selainta ohjataan toistamaan aina samat valinnat. Kun tiedosto on ladattu onnistuneesti selaimeen tulee latausaika näkyviin, jonka Selenium poimii talteen.

## Tiedostojen talletus

Tiedostojen talletukseen on toteutettu .NET-palvelin joka suorittaa talletusoperaatiot, sekä Python ja C# ohjelmat, jotka tekevät pyynnön .NET-palvelimelle ja muodostaa tuloksista csv-tiedoston sekä kuvaajan.

# Projektien tulokset

Projektien tulokset ovat jaettu suorituskyvyn, kustannusten sekä tietoturvan mukaan. Kustannusvertailussa otetaan kantaa talletusratkaisujen kustannuksiin Azure-pilvipalvelussa ja vertaillaan eri talletusratkaisujen kustannuksia. Lisäksi tiedonsiirron kustannuksia vertaillaan epäsuorasti käytetyn internet kaistan avulla. Tehokkuusvertailussa vertaillaan talletus- sekä lataustapojen suorituskykyä ajallisessa näkökulmassa. Tietoturvavertailussa vertaillaan käytettyjen ratkaisujen tietoturvaa ja vertaillaan tutkimuksia pilvialustoja käyttävien sovullestun tietoturvasta.

## Kustannusvertailu

Kustannusvertailu on jaettu kahteen osaan: Pilvialustojen talletusratkaisuihin ja tiedostojen siirtoon. Tiedostojen siirron kustannuksia mitataan epäsuorasti kuinka paljon siirrettävän tiedoston koko kasvaa siirron aikana eri protokollilla. Siirrettävän datan määrä voi vaikuttaa internetyhteyden hintaan sekä pilvipalvelut laskuttavat virtuaalikoneille tulevasta ja lähtevästä datasta.

Tutkimus tehtiin käyttämällä WireShark-ohjelmistoa, joka avoimen lähdekoodin pakettianalysaattori. Wireshark on monialustainen, ja se käyttää Packet Capturea (PCAP) pakettien sieppaamiseen.

### Pilvialustojen talletusratkaisujen kustannukset

Tässä osiossa vertailtaan Azuren tarjoamien talletusratkaisujen hintoja. Azure Cosmos on NOSQL -tietokanta sekä vektoritietokanta, joka tallentaa dokumentteja JSON-muodossa. Dokumentit indeksoidaan, ja niitä on mahdollista hakea ja muokata kyselyillä. Azure Cosmos laskuttaa kolmesta eri käyttötyypistä: laskenta, tallennustila ja kaistanleveys. Azure tarjoaa ilmaiset 25 GB talletustilaa jokaiselle Azuren tilille. Laskennan laskutus tapahtuu pyyntöyksikköjen (RU) avulla. RU on tietokannan operaatioihin vaadittavan laskennan, muistin ja IO:n abstrakti mitta. eri tietokantaoperaatiot kuluttavat pyyntöyksikköjä tietyn välin sisällä. Tietyn operaation vaadittavaan pyyntöyksikköjen määrään vaikuttaa useampi tekijä, esimerkiksi kirjoitettavan/luettavan asian koko. Indeksien käyttäminen kasvattaa vaadittavien Pyyntöyksikköjen määrää. Vaadittavien pyyntöyksikköjen määrä on deterministinen, eli sama operaatio, samalla tietokannalla vaatii aina saman verran pyyntöyksikköjä. Azure Cosmos DB laskuttaa pyyntöyksiköillä sekunnissa mitattuna (RU/s), tai pelkästään käytetyistä pyyntöyksiköistä. Laskutus riippuu tietokannan valitusta skaalautuvuusmallista. Palveliton malli laskuttaa pelkästään käytetyistä pyyntöyksiköistä 0.235 € miljoonasta käytetystä pyyntöyksiköstä. Kiinteäsuorituskyky-mallissa tietokantaan kiinnitetään kiinteä RU/s-arvo, ja siitä veloitetaan 0.0075 € tunnilta sataa RU/s -yksikköä kohden. Automaattisessa skaalaus- mallissa tietokannan RU/s arvo skaalautuu automaattisesti kuorman mukana 10% -100% välillä annetusta maksimi RU/s-arvosta. Tunnin maksimi RU/s-arvosta veloitetaan 0.008 € tunnilta sataa RU/s yksikköä kohden. Talletustila maksaa 0.235 euroa kuukaudessa giga tavulta. Kaistanleveydestä joutuu maksamaan pelkästään tietokannasta ulos siirtyvästä datasta. Ensimmäiset 5 GB on ilmaista, jonka jälkeen hinta on 0.05 € giga tavulta.[52][53]

Azure tarjoaa täysin ylläpidetyn SQL-tietokannan, ja varmistaa sen saatavuuden ja suorituskyvyn. Tietokannoissa maksaa laskenta ja talletustila. laskentaan on tarjolla kaksi eri mallia: virtuaaliytimeen (vCore) ja Tietokantatapahtumayksikköön (DTU) perustuva ostomalli. Virtuaaliytimeen (vCore) perustuva malli tarjoaa valinnan varattujen tai palvelimettomien laskentamallien välillä. Varartun laskentamallin avulla voi valita tarkan määrän virtuaaliytimiä, jotka on aina varattu laskentaa varten. Palvelimettomassa laskentamallissa virtuaaliytimiä voidaan automaattisesti skaalata konfiguroitavalla laskenta-alueella. Palvelimeton laskentamalli sulkee automaattisesti tietokannan epäaktiivisina aikoina, jolloin tietokantaan ei ole yhtään istuntoa avattuna. Suljetusta ajasta laskennasta ei laskuteta olleenkaan, ja tietokanta käynnistyy udelleen kun uusi istunto luodaan. Virtuaaliytimiä on tarjolla eri arkkitehtuurilla ja niillä on hieman eri hinnat. Virtuaaliytimen määrä on valittavissa 2 ja 128 väliltä, ja yhden virtuaaliytimen hinta pienenee hieman kun valitaan suurempi määrä ytimiä. Yhden ytimen hinta kuukaudessa on 100-120 euroa. Palvelimeton malli laskuttaa ytimestä sekuntihintaa ja varattu malli puolestaan minuuttihintaa. Tietokantatapahtumayksikkö (DTU) edustaa suorittimen, muistin, lukujen ja kirjoitusten abstraktia mittaa. DTU-pohjaisessa ostomallissa on mahdollista valita laskentatehon määrä, joka ilmoitetaan käytettävissä olevilla tietokantatapahtumayksiköillä. Valittuun laskentatehoon on kiinnitetty kiinteä määrä mukana olevaa tallennustilaa, kiinteä säilytysaika varmuuskopioille ja kiinteä hinta. Lisämuistia on mahdollista ostaa hintaan kuuluvan muistin lisäksi. Laskentatehoa voidaan lisätä tietokannan luomisen jälkeen lisäämällä tietokantatapahtumayksikköjä ja se aiheuttaa vain lyhyen katkoksen tietokannan käyttämiseen. DTU-pohjaisen laskentatehon voi muuttaa virtuaaliytimen tehoon suhteella 100 DTU-yksikköä vastaa yhtä virtuaaliydintä. Laskentateho on valittavissa 5-400 DTU-yksikön välistä ja käytettävissä oleva talletustila vaihtelee 2 GB-4 TB välissä. Hinta taas vaihtelee 4.5 ja 14515 euron välillä. Virtuaaliytimeen perustuva malli laskuttaa talletustilasta 0.232 euroa kuukaudessa giga tavulta. Tietokantatapahtumayksikköön perustuvassa mallissa hintaan sisältyy tietty määrä levytilaa ja lisälevytila maksaa 0.16 euroa kuukaudessa giga tavulta. [54][55][56]

Azure Blob Storage on Microsoftin Object Storage, ja se on suunniteltu rakenteettoman datan tallentamiseen. Azure Blob Storage tarjoaa HTTP-rajapinnan, jonka avulla tiedostoja pystytään muokkaamaan. Useille ohjelmistokielille on tehty valmiit asiakaskirjastot sekä CLI-työkaluja. Blob Storage laskuttaa talletustilasta sekä operaatioista. Talletustilan ja operaatioiden hinta määräytyy valitun palvelumallin mukaan. Valittavia malleja on viisi: korkealuokkainen, kuuma, lämmin, kylmä ja arkisto. Tallennuksen gigatavujen hinnat nousevat arkistosta kohti korkealuokkaista jokaisella askeleella. Puolestaan operaatiot halpenevat arkistosta kohti korkealuokkaista jokaisella askeleella. Korkealuokkaisella mallilla on pienin latenssi ja latenssi kasvaa kohti arkistoa. korkealuokkaisenmallin talletus tila maksaa 0.13869 € giga tavulta ja on melkein kymmenen kertaa kalliimpi kuin seuraava kuumamalli. Hinnat halpenevat edelleen kohti arkistoa mentäessä ja arkisto maksaa 0.00092 € giga tavulta. korkealuokkainen malli tarjoa halvimmat luku- ja kirjoitusoperaatiot. korkealuokkaisen kirjoitusoperaatioiden hinta on 0.0211 € kymmentä tuhatta operaatiota kohden ja on noin kuusi kertaa halvempi kuin arkistomallin hinta. Lukuoperaatioiden hinta puolestaan muuttuu huomattavasti enemmän mallien välillä. korkealuokkaisen hinta on 0.0017 € kymmentä tuhatta operaatiota kohden. Kylmän mallin hinta on noin 100 kertainen korkealuokkaiseen nähden ja arkiston noin 4000 kertaa kalliimpi.[57][58]

Azure Files on Microsoftin File Storage-palvelu. Palvelu mahdollistaa tiedostojen yhtäaikaisen käyttämisen eri käyttöjärjestelmien välillä. Valittavia palvelumalleja on neljä: korkealuokkaien, Tapahtuma optimoitu, kuuma, viileä. Korkealuokkaien tarjoaa pienimmän latenssin ja latenssi kasvaa kohti kylmää mallia. Korkealuokkaisella talletustila maksaa eniten ja se halpenee mentäessä kohti kylmää. Korkealuokkaisen hinta on 0.1480 € varatulta giga tavulta ja kylmän mallin hinta on noin 10 kertaa halvempi. Luku- ja kirjoitusoperaatiot ovat korkealuokkaisessa ilmaisia, mutta muissa malleissa maksullisia. Tapahtuma optimoidussa on halvimmat Luku- ja kirjoitusoperaatiot ja hinnat kasvavat kun siirrytään kylmää mallia kohti. Kylmän mallin Luku- ja kirjoitusoperaatioiden hinnat ovat keskimäärin noin kymmenen kertaa kalliimmat kuin Tapahtuma optimoidun. [59]

Azure Managed Disks on Microsoftin Block storage, jota voidaan käyttää virtuaalikoneiden kanssa. Levyvaihtoehtoja on neljä: Ultra Disk, korkealuokkaien SSD, SSD ja HDD. Ultra Diskin latenssi on kaikista pienin ja se on uuden generation SSD- levy. Korkealuokkaisen SSD:n ja SSD:n välillä on pieni suorituskyky- ja hintaero. Levyille on ilmoitettu kuinka monta kirjoitus/luku- operaatiota voidaan suorittaa sekunnissa (IOPS) sekä nopeus, jolla data voidaan siirtää ulos tai sisään, ilmoitettuna MB sekunnissa (MB/s). Azure tarjoaa mahdollisuuden parantaa levyn IOPS- ja MB/s-suorituskykyä hetkellisesti. Tätä kutsutaan purskeeksi, ja maksimi yhtäkestoinen aika sille on 30 minuuttia. Purskeen käyttö kuluttaa krediittejä, ja kun kaikki krediitit on käytetty purske loppuu. Kun levyä käytetään alle sen IOPS- ja MB/s-suorituskyvyn krediittejä kerääntyy uutta pursketta varten. Pienillä alle 128 GB levyillä korkealuokkisen SSD:n suorituskyky on huonompi kuin tavallisen SSD:n, mutta purske on paljon tehokkaampi. Mitä suurempi levyn koko sitä tehokkaampi korkealuokkainen SSD on verrattuna vastaavan kokoiseen tavalliseen SSD-levyyn. Korkealuokkaisen SSD levyn hinta on noin 2 kertaa suurempi kuin vastaavan kokoisen SSD-levyn. Korkealuokkainen SSD levy laskuttaa vielä erikseen IO operaatioista 0.001850 € jokaista 10,000 operaatiota kohden tunnissa. IO-operaatioilla on maksimi hinta kuukaudessa ja se on noin levyn talletuskapasiteetin hinta. HDD-levyn hinta on noin puolet vastaavan kokoiseen SSD-levyyn nähden. HDD-levyn IOPS-suorituskyky on melkein sama kuin vastaavan kokoisen SSD-levyn, mutta siirrettävän datan määrä on huomattavasti pienempi. Ultra diskin laskutus toimii pikkaisen eri tavalla, siinä käyttäjä voi valita vapaasti halutun IOPS- ja MB/s-suorituskyvyn ja levyn talletuskoon. Jokaisesta valitusta komponentista laskutetaan erikseen ja levyn kustannukseksi tulee näiden summa.[60]

Eri talletusratkaisujen hintoja vertaillaan kolmella eri talletuskoolla: 16 GB, 256 GB ja 1 TB. Talletusratkaisujen pelkästään talletustilasta laskuttaama hinta kuukaudessa on esitetty taulukossa 1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 16 GB | 256 GB | 1 TB |
| Managed Disks/ korkealuokkainen SSD | 2.22€ | 31.96€ | 113.61€ |
| Managed Disks/ SSD | 1.11€ | 17.76€ | 71.01€ |
| Managed Disks/ HDD | 0.70€ | 10.48€ | 37.87€ |
| Files/ korkealuokkainen | 2.37€ | 37.89€ | 148€ |
| Files/ tapahtuma optimoitu | 0.88€ | 14.2€ | 55.5€ |
| Files/ viileä | 0.22€ | 3.55€ | 13.9€ |
| Blob Storage/ korkealuokkainen | 2.22€ | 35.50€ | 138.69€ |
| Blob Storage/ kuuma | 0.27€ | 4.28€ | 16.7€ |
| Blob Storage/ arkisto | 0.01€ | 0.24€ | 0.92€ |
| Cosmos | 3.71€ | 59.40€ | 232€ |
| SQL | 3.71€ | 59.40€ | 232€ |

Taulukosta 1 näkee että tietokantojen (Cosmos ja SQL) hinnat ovat samat ja selvästi muita ratkaisuja kalliimmat. Kaikkien muiden talleyusratkaisuiden kalliimpien ratkaisuiden hinnat ovat keskenään lähellä toisiaan. Halvempien ratkaisuiden hinnat eroavat toisistaan enemmän. Kaikista halvin ratkaisu on Blob Storagen arkisto. Sen hinta verrattuna halvimpiin Managed Disksiin tai Files palveluihin on useita kymmeniä kertoja halvempi. Blob Storagen arkiston IO-operaatiot puolestaan ovat kymmeniä kertoja kalliimmat kuin minkään muun talletusratkaisun, eli se sopii parhaiten tiedostoille, joita ei tarvitse juuri olleenkaan muokata tai lukea.

Talletusratkaisuiden IO-kuormasta syntyviä kustannuksia, on paljon vaikeampi vertailla keskenään, koska talletusratkaisuilla on käytössä eri mittoja operaatioiden vaadittavan suorituskyvyn mittaamiseen. Taulukossa 2 on esitetty eri talletusratkaisuiden hinta miljoonalle lukuoperaatiolle ja miljoonalle kirjoitusoperaatiolle. Joillekkin talleyusratkaisulle on jouduttu arvioimaan hinta, koska talletusratkaisu ei suoraan ilmoita hintaa yksittäisille operaatiolle. Arvioidun hinnan edessä on käytetty tilde-merkkiä(~).

|  |  |  |
| --- | --- | --- |
|  | Miljoona lukuoperaatiota | Miljoona kirjoitusoperaatiota |
| Managed Disks/ korkealuokkainen SSD | 0€ | 0€ |
| Managed Disks/ SSD | 0.19€ | 0.19€ |
| Managed Disks/ HDD | 0€ | 0€ |
| Files/ korkealuokkainen | 0€ | 0€ |
| Files/ tapahtuma optimoitu | 0.14€ | 1.39€ |
| Files/ viileä | 1.21€ | 12.02€ |
| Blob Storage/ korkealuokkainen | 0.17€ | 2.11€ |
| Blob Storage/ Kuuma | 0.47€ | 6.01€ |
| Blob Storage/ arkisto | 600.0€ | 12.02€ |
| Cosmos | 0.23€ | ~0.50€ |
| SQL | ~0.34€ | ~0.70€ |

Cosmos-tietokannan lukuoperaatioiden hinnan voi laskea suoraan, koska jokainen lukuoperaatio käyttää aina vain yhden RU-resurssin. Kirjoitus- operaatio voi käyttää eri määrän RU-resursseja riippuen tietokannan koosta ja kirjoitettavan tiedoston koosta. Taulukossa on arvioita että kirjoitus-operaatio käyttäisi keskimäärin 2 RU-resurssia. SQL- tietokannan IO-operaatoiden hinta on vieläkin vaikemapi arvioida, koska vastaava laskennan abstraktimitta DTU-yksikkö laskutetaan eri tavalla. DTU- yksiköistä laskutetaan käytettävistä yksiköistä kuukaudessa. Taulukun hinta on arvioitu 5 DTU-yksikön tietokannalla arvioiden että yksi lukuoperaatio vie yhden yksikön ja operaatio käyttää yksikköä sekunnin ajan. Näin viiden yksikön tietokannalla pystyttäisiin suorittamaan noin 13 miljoonaa lukuoperaatiota kuukaudessa. Kuukauden hinta on jaettu 13, josta on saatu miljoonan lukuoperaation hinta. Kirjoitusoperaatioiden on arvioitu käyttävän resursseja tuplasti ja näin ollaan päädytty taulukon hintaan. Nämä hinnat edustavat minimihintaa, ja edellyttyvät että tietokannasta käytettäisiin 100% teholla. Todelliset hinnat tulisivat näin ollen olemaan kalliimpia, riippuen tietokannan käyttöasteesta.

Kun vertailee taulukkoa 1 ja taulukkoa 2 niin huomaa selkeästi logiikan kylmien ja kuumien talletusratkaisuiden välillä. Kuumat ratkaisut ovat IO-suorituskyvyltään tehokkaita ja talletustila kustantaa enemmän, mutta IO-operaatiot ovat halpoja. Kylmät ratkaisut ovat päin vastoin erittäin halpoja talletustilaltaan, mutta IO-operaatiot ovat erittäin kalliita ja latenssi erittäin suuri. Kun halutaan optimoida talletusratkaisun hintaa, täytyy miettiä useampia asioita, jotka vaikuttaa hintaa. Kuinka paljon IO-operaatioita suoritetaan ja onko pieni latenssi ja hyvä suorituskyky kriittinen ominaisuus. Jos IO-operaatioita on paljon, mutta nopeus ei ole kriittinen tekiä, optimaalisin hintaratkaisu löytyy lämpimän päädyn ratkaisuista. Jos IO-operaatioita ei ole paljon ja nopeus ei ole kriittinen tekijä, kannattaa valita kylmämalli. Taulukoista erottuu selvimmin Blob Storagen arkisto- malli. Sen talletustilakustannukset ovat selvästi muita ratkaisuja halvemmat, mutta lukuoperaatiot ovat puolestaan luokkaa tuhat kertaa kalliimmat kuin minkään muun ratkaisun. Tietokantojen(Cosmos ja SQL) kustannukset ovat kalliimmat kuumilla ratkaisuilla, mutta ne mahdollistavat monimutkaisten kyselyjen tekemisen ja rinnakkaisen käytön turvallisesti.

### Tiedostojen siirron kustannukset

Tiedostojen siirron kustannuksia vertaillaan epäsuorasti: kuinka paljon eri siirtoprotokollat kasvattavat tiedoston kokoa siirrettäessä. Siirrettävän datan kasvu aiheuttaa lisää kustannuksia verkkoliikenteen kasvaessa. Pilvialustat velottavat virtuaalikoneen tulevasta ja lähtevästä datasta.

Tutkimuksessa käytettiin WireShark nimistä ohjelmistoa. Se on avoimen lähdekoodin pakettianalysaattori, jonka avulla voidaan tutkia verkkoliikennettä. Wireshark on monialustainen ohjelmisto ja se käyttää PCAP:ia (Packet Capture) pakettien sieppaamiseen. PCAP on verkkokäytäntö, joka kopioi verkossa kulkevia datapaketteja niiden liikkuessa verkon poikki ja tallentaa syntyneet kopiot analysointia varten. Wireshark tarjoaa käyttöliittymän kaapattujen pakettien analysointiin, jonka avulla projektin tietoliikennettä on tutkittu.

Projektissa tutkittiin tietoliikennettä tiedostoa siirtäessä molempiin suuntiin: palvelimelle ja palvelimelta kulkevaa liikennettä. Molempiin suuntiin kulkenut data laskettiin yhteen ja vertailu tehtiin tällä summatulla arvolla. Vertailussa on mukana kaikki projektissa käytetyt protokollat, ja niitä on käytetty C#-kirjastoilla. Vertailu tehtiin kahdella erikokoisella tiedostolla. Tiedostojen koot olivat 1M tavua sekä 200M tavua. Kuvassa X on esitetty vertailu 1 M tavun tiedostolla sekä kuvassa Y on esitetty vertaiulu 200M tiedostolla. Tiedoston kasvu on kuvissa ilmoitettu prosenttiaalisena kasvuna verrattuna alkuperäiseen tiedostoon.

A graph of different colored bars

Description automatically generated

A graph of different colored bars

Description automatically generated

1 M tiedosto kasvaa hieman enemmän siirtäessä kuin suurempi 200 M tiedosto kaikilla muilla protokollilla, paitsi FTP:llä jolla se pysyy melkein samana. 1MB tiedoston kasvuprosentti on 3.7 - 6.7 % välillä ja 200 M tiedoston 4.0 - 4.7 % välillä. SFTP kasvaa eniten kummallakin tiedostokoolla. FTP kasvaa vähiten pienemmällä tiedostolla ja WebSocket puolestaan isommalla tiedostolla. Salatut protokollat kasvavat kaikista eniten isommolla tiedostolla ja pienemmällä tiedostolla SFTP ja HTTPS kasvavat eniten, mutta FTPS kasvaa vähemmän kuin salaamattomat HTTP tai WebSocket. Pienellä tiedostolla kasvuun vaikuttaa enemmän esimerkiksi protokollan yhteydenavaus ja käyttäjänhallinan prosessit. Esimerkiksi HTTP protokollaa kasvattaa HTTP-pyynnön vastaus. Pienemmällä tiedostokoolla tämä vastaus on noin 1% tiedoston koosta.

## Tehokkuusvertailu

Kuva 12 esittää FTP-, FTPS- sekä SFTP-latausten latausaikojen tulokset Python- ja C#-kirjastoilla toteutettuna. Kuvasta nähdään että SFTP on selvästi FTPtä ja FTPStä hitaampi molemmilla ohjelmointikielillä suurimmilla tiedostoilla. Pienellä tiedostokoolla SFTP ei ole hitaampi kuin FTP tai FTPS, mutta ero kasvaa voimakkaasti kun tiedoston koko kasvaa. Python koodissa SFTP:n suorituskyky on selvästi huonompi, kuin mitä C#-koodilla on, mutta FTP- ja FTPS-latausten kohdalla ohjelmointiielellä ei ole merkitystä. FTP ja FTPS suorituskyvyt eroavat toisistaan vain vähän. Pienillä tiedostoilla FTP on hieman nopeampi koska aloitusprosessi on lyhyempi, koska yhteyttä ei salata.

Chart, line chart

Description automatically generated

Kuva 15 FTP, FTPS ja SFTP latausten tulokset

Kuva 13 esittää HTTP latauksien latausajat. Latausten pyynnön koko on esitetty x-akselilla ja latausaika on esitetty y-akselilla. Pylväiden väri puolestaan merkitsee eri pyynnön koodausta. Kuvaajasta näkee selvästi että pyynnön koon suurentuessa latausaika pienenee erittäin voimakkaasti kaikilla koodauksilla. Pienempi pyynnön koko aiheittaa useampia pyyntöjä palvelimelle, joka hidastaa latausta merkittävästi. 5 kB:n kokosilla pyynnöillä hitain koodaus on base64, vaikka teoriassa array on kaikista hitain koska se kasvattaa eniten siirrettävän datan kokoa.

Chart, bar chart

Description automatically generated

Kuva 16 HTTP-latausten latausajat

Kuva 14 esittä HTTP-latausten lähetettävän datan määrää suhteessa tiedoston kokoon. Lähetettävä data on mitattu Wireshark-ohjelmalla jota käytetään verkkojen analyysiin. Siirrettävässä datassa on mukana kaikki TCP-tasolla siirtnyt data, joten se katttaa siirretävän tiedosotn sekä HTTP-pyyntöön tarvittavan datan. Kun käytetään pientä 5kb kokoista pyyntöä lähetettävän datan määrä kasvaa reilusti kaikilla koodauksilla. Teoriassa form-data on kaikista tehokkain tapa lähettää dataa ja data siirtyy binäärimuodossa. Form-data kasvattaa lähetettävän datan määrää vain muutamalla prosentilla kun lähetettävän pyynnön koko on suuri. Base64 koodaus kasvattaa lähetettävän tiedoston kokoa noin 33% kun käytetään suurta pyyntöä. Array koodaus kasvattaa siirrettävän datan 100% suuremmaksi mitä alkuperäinen tiedosto, jonka takia se ehdottomasti huonoin tapa siirtää tiedostoja HTTP-protokollan avulla. Ainoastaan 500 kB on nähtävissä selkeasti teoreettinen tulos että form-data on nopein jonka jälkeen base64 koodaus on noin 33% hitaampi sekä array useampi kertoja hitaampi.

Chart, bar chart

Description automatically generated

Kuva 17 HTTP -latausten tiedoston kasvu lähettäessä

Kuva 15 esittää Webocket-latauksen tulokset. Websocket-yhteys luotiin .NET:n SignalR-kirjaston avulla. SignalR-kirjasto on osa .NET joten sitä ei tarvitse erikseen asentaa palvelimelle, mutta selaimeen se tarvitsi asentaa npm-pakettina. Signal käyttää konepellin alla selaimen Websocket API:a, mutta se luo korkeamman tason rajapinnan, mahdollistaen palvelinpään funktioiden kutsumisen käyttöliittymästä websocket-yhteyden avulla. Binääriviestintää varten SignalR kirjastoon joutuu asentamaan lisäosan Nuget paketin nimeltään MessagePack sekä käyttöliittymään saman nimisen npm-paketin. Lataus suoritettiin sekä merkkijono viestinä että binäärinä ja testissä käytettiin kolmea erikokoista tiedostoa. Latausten ajat olivat hyvin samanlaiset riippumatta käytettiinkö merkkijono- vai binääriformaattia. Pienimmillä tiedostoilla merkkijono oli hitusen nopeampi, mutta suuremmalla tiedostolla binääri oli hieman nopeampi. Teoriassa binääriformaatti pitäisi olla nopeampi, koska siirrettävä data on pienempi.

Chart

Description automatically generated

Kuva 18 Websocket-lataus

**Error! Reference source not found.** esittää siirrettävän datan suuruutta verrattuna alkuperäiseen tiedostoon. Siirrettävä data on mitattu TCP -tasolla, samaan tapaan kuin HTTP -pyyntöjen siirrettävän datan suuruutta vertailtaessa. String -formaatilla lähetettäessä siirrettävä data on kaksinkertainen alkuperäiseen tiedsotoon nähden ja binary -formattissa siirrettävä data 11% suurempi mitä alkuperäinen tiedosto.

Chart

Description automatically generated

Kuva 19 Websocket -latauksen siirrettävän datan kasvu

Kuva 17 esittää tiedostojen talletusnopeuksia eri talletusratkaisuilla. Kuvan y-akseli on logaritminen ja siitä erottuu selvästi etttä Disk ja File Storage ovat huomattavasti nopeimpia talletusratkaisuja. Tähän vaikuttavia tekijöitä on sisäverkon verkkoliikenne ja ne eivät vaadi mitään kirjautumismekanismia. SQL-talletus on seuraavaksi nopein. Siinä data siirretään TCP-yhteydellä sisäverkossa, mutta SQL-kyselyt tarvitsevat kirjautumis- ja datan eheysprosessit jotka hidastavat tiedostojen tallettamista. Blob Storage sekä Cosmos käyttävät julkisen verkon HTTP API:a tiedostojen tallentamiseen ja ovat siksi ehdottomasti hitaimpia talletuspaikkoja. Blob Storage mahdollistaa binääritiedostojen tallentamisen binäärimuodossa, mutta Cosmos käyttää pelkästään json-dokumenttejä ja tiedostojen koko kasvaa merkittävästi kun on tallennettuna tekstinä. Cosmoksen json-dokumentin maksimikoko on 2MB joten Cosmoksen suorituskykyä ei voitu testata 10 MB tiedostoilla.

Chart, line chart

Description automatically generated

Kuva 20 Tiedostojen talletusnopeuksia

Yksi tutkimuksista on vertailla tiedostojen tallentamista SQL-kantaan binäärisenä blob tyyppina. Toinen mahdollinen vaihtoehto on tallentaa SQL-tietokantaan tiedoston tiedostopolku ja tallentaa tiedosto kovalevylle tietokannan sijaan. Kuva 18 esittää tutkimuksen tulokset. Tutkimuksessa vertailtiin tiedostojen lukua, kirjoitusta, poistoa sekä tiedosto infon lukua tietokannasta. Tutkimuksessa käytettiin 2 tietokanta taulua jotka ovat muuten identtiset, mutta toisessa tiedosto on tallennettuna tietokantaan ja toisessa linkin avulla tiedostojärjestelmään. Tiedostoinfo on tallennettuna samalla rivillä tiedoston tai sen linkin kanssa ja tyypiltään se on varchar. Tuloksista nähdään selvästi että tiedoston luku selvästi nopempi koska erillistä levylukuoperaatiota ei tarvitse tehdä tietokanta kyselyn jälkeen. Infon luku on hieman nopeampi taulussa jossa on linkki, johtuen että rivien indeksointi on hieman nopeampaa RAM-muistissa koska rivien koko on pienempi. Kirjoitus- ja poistonopeudet ovat lähes samat riippumatta tallennustavasta. Toinen huomioita asia tiedostojen tallentamisessa levyjärjestelmään on tietokannan eheys. Kun tiedostot tallennetaan tietokantaan niin tietokanta pysyy eheänä tiedostojen suhteen. Levylle tallennettaessa eheys saattaa rikkoontua koska tietokantaoperaatio ja levyoperaatio eivät ole saman tietokantatransaktion sisällä

Chart, bar chart

Description automatically generated

Kuva 21 Tiedostojen tallentaminen SQL-tietokantaan ja kovalevylle

## Tietoturvavertailu

### Suojaamattomat protokollat

Tietoturvavertailussa vertaillaan eri talletustapojen sekä tiedonsiirtoprotokollien tietoturvallisuutta. Käsitellyistä tiedonsiirtotavoista suojaamattomia protokollia ovat HTTP, FTP, WebSocket ja WebDav. Niiden käyttöä ei suositella nykyään olleenkaan, vaan niiden tilalla pitäisi käyttää suojattuja versioita HTTPS, FTPS WebsocketS ja WebDavS. Kaikki suojaamattomat protokollat eivät salaa tiedonsiirtoa palvelimen ja asiakkaan välillä. Tämän takia kuka tahansa joka pääsee verkkoliikenteeseen käsiksi voi siepata ja lukea sen. Lisäksi suojaamattomat protokollat eivät tarjoa mitään todennusta, mikä tekee niistä haavoittuvia välimieshyökkäyksille (MITM). MITM-hyökkäys on yleinen termi, jossa tekijä päsee kuuntelemaan ja muokkaamaan kahden käyttäjän välistä keskustelua. Tarkoituksena on salakuunnella keskustelua tai esiintyä toisena osapuolena muokkaamalla keskustelua. Tällöin se vaikuttaa tavalliselta tiedonvaihdolta hyökkäyksen kohteeksi joutuneille ja ne uskovat kommunikoivan suoraan keskenään, vaikka hyökkääjä on asettunut kahden käyttäjän väliin.[61][62]

HTTP-protokollassa on lisäksi haavoittuvuuksia, joita ei pystytä torjumaan TLS- salauksella. BREACH haavoittuvuus johtuu HTTPP-protokollan pakkausalgoritmista. HTTP-pakkaus suoritetaan tavallisesti deflate-algoritmin avulla. Kun dataa pakataan tällä algoritmilla, kaikki toistuvat tavusekvenssit havaitaan, eikä niitä toisteta pakatussa datassa. Sen sijaan toistuva tavusekvenssi tallennetaan vain kerran, samoin kuin osoittimet, jotka osoittavat mistä sama sekvenssi löytyy uudelleen. Tämä vähentää lähetettävien tavujen määrää. Pakatun datan pituus on kuitenkin näkyvissä myös salattuna, ja tämä on yksi peruselementeistä, joka tekee BREACH-hyökkäyksen mahdolliseksi. Jotta sovellus olisi haavoittuvainen BREACH-hyökkäykselle, palvelimen HTTP-pakkaus täytyy olla kytkettynä päälle. hyökkääjällä tulee olla keino tarkastella uhrin liikennettä ja lisäksi hyökkääjällä on oltava mahdollisuus lähettää HTTP-pyyntöjä haavoittuvaan palvelimeen. Hyökkäys toimii lähettämällä pyyntöjä palvelimelle saadakseen tietoja pakatusta ja salatusta vastauksesta. Vastauksen otsikoita ei pakata, joten tällä hyökkäyksellä niitä ei pystytä kaappaamaan. Esimerkiksi evästeet siirretään otsikoissa, mutta CSRF-avaimet ovat saatavilla tällä hyökkäyksellä. Esimerkiksi CSRF-avaimen varastamiseksi hyökkääjän tulee tietää missä muodossa CSRF-avain lähetään HTTP- pyynnöissä ja vastauksissa. esimerkiksi voidaan käyttää CSRF avaimelle muotoa token=123456789. Hyökkääjä aloittaa ensimmäisen numeron arvaamisen ja lähettää palvelimelle pyyntöjä joissa on pelkästään mukana arvattavan CSRF- avaimen ensimmäinen numero. Hyökkääjä lähettää kaikki mahdolliset numerot palvelimelle. Palvelimen vastauksista lyhin on se missä numero on arvattu oikein. Tämä prosessi toistetaan jokaiselle numerolle erikseen kunnes koko CSRF- avain on saatu muodostettua. Hyökkäykseltä pystyy suojautumaan laittamalla palvelimen HTTP-pakkauksen pois päältä.[63]

### TLS

Kaikkien protollien suojaamiseen käytetään samaa TLS-salausprotokollaa, joten ne ovat kaikki haavoittuvia TLS-protokollan tietoturvaongelmille. Vanhoissa SSL/TLS versioissa on useita tiedossa olevia haavoittuvuuksia alle on esitelty muutama yleisesti tiedossa oleva hyökkäys protokollia vastaan.

RC4-hyökkäys tapahtuu symmetristä salausta vastaan. RC4 on symmetrinen virtasalausalgoritmi, joka julkistettiin vuonna 1987. RC4 on ollut mahdollinen symmetrinen salaus jo ensimmäisessä SSL 2.0 versiossa ja se poistettiin TLS 1.3 versiosta. Toisin kuin nykyaikaisessa virtasalauksessa, RC4 ei ota erillistä satunnaista alustusvektoria avaimen rinnalla. Tämä tarkoittaa, että jos yhtä pitkäaikaista avainta käytetään useiden virtojen turvalliseen salaamiseen, alustusvektorin ja pitkän aikavälin avain on yhdistetään RC4:n salausavaimen luomiseksi. Ensimmäiset haavoittuvuudet RC4 algoritmista löydettiin vuonna 2001 ja 2005. Haavoittuvuudet mahdollistivat löytämään käytetyn salausavaimen suuresta määrästä samalla avaimella salattuja viestejä, jos avain ja alustusvektori oli vain liitetty toisiinsa salausavaimen luomisessa. Huolimatta RC4:n tietoturvaa rikkovista hyökkäyksistä, RC4:ään perustuvia SSL- ja TLS-salausohjelmistoja pidettiin edelleen turvallisina ennen vuotta 2013 sen perusteella, miten niitä käytettiin SSL:ssä ja TLS:ssä. Vuonna 2011 RC4 suositeltiin BEAST-hyökkäyksen kiertäjäksi. Vuonna 2013 julkistetut uudet hyökkäysmuodot osoittivat lopullisesti TLS:n RC4:n rikkomisen toteutettavuuden. Hyökkäys vaatii 2^34 salattua viestiä RC4:n murtamiseen ​​TLS:ssä ja SSL:ssä. Hyökkäyksestä julkaistiin vuonna 2015 uusi versio, joka vaatii enää 2^26 viestiä salauksen murtamiseen.[64]

BEAST on selainhaavoittuvuus, joka julkaistiin vuonna 2011 ja se koskee SSL 3.0:aa ja TLS 1.0:aa. Hyökkääjä voi purkaa kahden osapuolen välillä vaihdetun tiedon salauksen hyödyntämällä haavoittuvuutta lohkosalauksen ketjuttamisen CBC (Cipher Block Chaining) toteutuksessa. Tämä on asiakaspuolen hyökkäys, joka on välimieshyökkäys. Hyökkääjä lisää paketteja TLS-virtaan. Tämän avulla he voivat arvata muokatun viestin kanssa käytetyn alustusvektorin ja siten purkaa salauksen. Jotta BEAST-hyökkäys onnistuisi, hyökkääjällä on oltava jonkinlainen hallinta uhrin selaimessa. Selainten modernit versiot estävät BEAST- hyökkäyksen. RC4 virtasalaus on immuuni BEAST-hyökkäykselle. Siksi RC4:ää käytettiin laajalti keinona lieventää BEAST-hyökkäystä palvelinpuolella ennen kuin se todettiin murretuksi vuonna 2013.[65]

POODLE on SSL 3.0 haavoittuvuus, joka johtuu BEAST:in tavoin lohkosalauksen ketjuttamisen CBC (Cipher Block Chaining) toteutuksesta. POODLE on välimieshyökkäys ja edellyttää, että hyökkääjän JavaScript-koodi ajetaan uhrin selaimessa. POODLE haavoittuvuus johtuu lohkosalausalgoritmien täytetarpeesta. Salattavan datan pitää olla lohkosalausalgoritmeissa lohkokoon monikerta, muuten viimeinen lohko pitää täyttää täytteellä loppuun. Jos data on täsmälleen lohkokoon monikerta, silloin viimeinen lähetettävä lohko on pelkästään täytettä. Palvelin hylkää pyynnön jos täyte on viallinen pyynnössä. POODLE hyökkäys perustuu siihen että hyökkääjä pääsee muokkaamaan lähetettävän pyynnön kokoa ja tietää siten pyynnön täytteen. Täytettävä sisältävä lohko on viimeisenä ja hyökkääjä vaihtaa viimeisen lohkon ja murrettavan lohkon paikkaa ja lähettää pyynnön useaan kertaan palvelimelle muuttaen pyynnön kokoa jokaisella pyynnöllä. Jos palvelin hyväksyy pyynnön, niin murrettavan lohkon bitit vastaavat täytelohkon täytettä vastaavia bittejä. Hyödyntämällä tätä haavoittuvuutta hyökkääjä saa murrettua SSL:n salauksesta lohkoja. Käyttäjän evästeiden varastaminen on yksi esimerkki onnistuneesta POODLE- hyökkäyksestä. Esimerkiksi 16 bittisen evästeen varastamiseen tarvitaan maksimissaan 4096 pyyntöä, jos hyökkääjä tietää tarkalleen missä kohtaa pyyntöä evästeet lähetetään. [66][67]

DROWN on SSL 2.0 version haavoittuvuus, joka johtuu protokollan liian heikosta symmetrisestä salauksesta. Hyökkääjän on ensiksi kuunneltava useita satoja SSL-yhteyksiä uhrin ja palvelimen välillä. Yhteyksien tarvitsee jakaa jaettusalaus RSA-kättelyllä. Hyökkääjä lähettää palvelimelle muokattuja versioita uhrin salatuista RSA-kättelyistä. Tapa jolla palvelin vastaa kuhunkin näistä muokatuista kättelyistä riippuu siitä muodostuuko salatusta viestistä oikean muotoinen viesti salauksen purkamisen jälkeen. Salaus käyttää vain 40 bittistä avainta RSA-salauksessa joten hyökkääjä pystyy vertaamaan palvelimen vastausta kaikkiin mahdollisiin vastauksiin joita on 2^40 kappaletta. Tällä tavalla hyökkääjä pystyy päätteleen oliko muokattu versio salatusta kättelystä oikein muodostettu vai ei.[68]

Tiedossa olevat TLS-haavoittuvuudet koskevat pääasiassa vanhentuneita TLS-versioita, joiden käyttämistä ei enää suositella. RC4- salauksen haavoittuvuus koskee myös turvallista TLS 1.2 versiota. Kuva 20 esittää Acunetix Web Application Vulnerability Report- tutkimuksen tuloksia vuodelta 2020. Tutkimuksen on tehnyt Invicti niminen tietoturvayhtiö ja siinä on testattu 5000 palvelimen tietoturvaa. Tutkimukseksen perusteella palvelimet sallivat edelleen TLS-yhteyden muodostamisen protokollan vanhoilla versioilla. POODLE-hyökkäys edellytttää SSL 3.0 versiota ja DROWN puolestaan vanhempaa SSL 2.0 versiota. Silti palvelimista 3.9% oli haavoittuvia POODLE-hyökkäykselle ja 0.7% oli haavoittuvia DROWN-hyökkäykselle. BREACH- hyökkäys johtuu HTTP-protokollan pakkausalgoritmista ja sille oli haavoittuvia 3.9% palvelimista. 7.7% palvelimista salli symmetriseksi salaukseksi käyttää murrettua RC4- algoritmia. RC4-algoritmia on mahdollista käyttää kaikissa muissa versioissa paitsi TLS 1.3 versiossa. Sen käyttö pitäisi erikseen kieltää TLS-palvelimen asetustiedostossa, jotta haavoittuvuudelta vältyttäisiin. Lisäksi 30.7 % palvelimista salli TLS 1.0 version käyttämisen joka on haavoittuvainen muun muassa BEAST- hyökkäykselle. [69]

A pie chart with different colored sections

Description automatically generated

Kuva 22 Vuoden 2020 AWAVR- tutkimuksessa löydetyt TLS/SSL- haavoittuvuudet

Kuva 21 esittää F5 Labsin tekemän The 2021 TLS Telemetry Report- tutkimuksen tuloksia HTTPS- palvelimien tukemista SSL/TLS- versioista. Tutkimuksessa on käytetty miljoona suosittua HTTPS-sivustoa. Tutkimuksesta huomataan että SSL 3.0- version käyttämisen mahdollistaa noin muutama prosentti tutkituista palvelimista. Nämä palvelimet ovat todennäköisesti haavoittuvia POODLE-hyökkäykselle. TLS 1.0 tuki on noin 50% palvelimista, mikä on huomattavasti suurempi luku mitä Acunetix Web Application Vulnerability Report- tutkimukseksessa saatu 30.9% on. TLS 1.1 on muutaman prosentin tuetumpi versio mitä TLS 1.0-versio. Ehdottomasti tuetuin versio on TLS 1.2, joka saavuttaa melkein 100% tuen. Uusin versio 1.3 saavutti noin 60% tuen tutkimuksessa. Vaikka F5 Labsin tekemä tutkimus ei suoraan paljasta tietoturvahaavoittuvuuksia TLS- prokollassa, niin se antaa hyvän kuvan kuinka laajasti protokollan vanhentuneet tietoturvaongelmia sisältäviä versioita käytetään jotka mahdollistavat TLS-protokollaan kohdistettuja hyökkäyksiä. [70]

A graph of different colored lines

Description automatically generated

Kuva 23 Suosituimpien HTTPS- palvelimien tukemat TLS- versiot vuonna 2021

Kun vertaillaan FTPS- ja SFTP-protokollia tietoturvan näkökulmasta, oleellisen asia on käytettävien porttien määrä. SFTP käyttää vain yhtä porttia tiedonsiirtoon, mutta FTPS tarvitsee kaksi. Lisäksi jokainen rinnakkainen yhteys tarvitsee oman porttinsa. Tämän takia FTPS -palvelimelle määritellään usein sallittujen porttien joukko palomuuriin. Palomuurit voidaan katsoa putkena, jotka määrittelevät sallitun ja kielletyn verkkotoiminnan yksityisessä verkossa. Palomuurit luovat tarkastuspisteitä verkkoliikenteen ohjaamiseksi, jolloin ne tarkistavat ohjelmoitujen parametrien perusteella verkkoliikennettä, ja toimivat niiden mukaisesti. Mitä vähemmän portteja on avattu, sitä vähemmän järjestelmässä on haavoittuvia kohtia. Jos käytössä on palomuuri, niin se pitää konffiguroida hyväksymään kaikki FTPS-palvelimen käyttämät portit, mikä lisää uhkia. Lisäksi salaus kiinnitetään FTPS -protokollaan TLS- tai SSL-tekniikoilla FTP-protokollan päälle. Tämän ulkoisen salauksen seurauksena palomuuriratkaisut eivät pysty havaitsemaan, mitä porttia käytetään ja miksi. Yksiporttiset SFTP-asetukset ovat ihanteellisia käytettäväksi palomuurin rinnalla. Se muodostaa yhden yhdistetyn yhteyden asiakkaan ja palvelimen välille. Palomuuri voi tarkkailla tämän yhteyden poikkeavuuksia, epäilyttäviä merkkejä ja muita uhkamerkkejä.[71]

### Microsoft Azure

Azure käyttää roolipohjaista pääsynhallintaa (Azure RBAC) Azure-resurssien käyttöoikeuksien hallintaan. Rooleja voidaan antaa käyttäjille, ryhmille, sovelluskäyttäjille tai hallituille identiteeteille. Käyttöoikeudet resursseihin on sidottu rooleihin. Azure tarjoaa valmiiksi määriteltyjä rooleja ja käyttäjät voivat luoda uusia itse määriteltyjä rooleja. Rooleille on määritettävä laajuus. Laajuus on joukko resursseja, joita käyttöoikeus koskee. Azuressa laajuuden voi määrittää neljällä tasolla laajasta kapeaan: hallintaryhmä, tilaus, resurssiryhmä ja resurssi. Kuva 22 esittää Azuren laajuuksien hierarkian.

A diagram of a group

Description automatically generated

Kuva 24 Azuren roolien laajuus

Alimpana hierarkiassa on yksittäinen resurssi, joka tarkoittaa jotakin Azuren tarjoamaa palvelua. Sen yläpuolella on resurssiryhmä, jonka avulla resursseja voidaan ryhmitellä. Jokaisen resurssin on kuuluttava yhteen ryhmään ja ryhmässä voi olla useampia resursseja. Resurssiryhmän yläpuolella on tilaus, johon voi kuulua useampi resurssiryhmä. Kun käyttäjätili luodaan Azureen, käyttäjätili sisältää yhden tilauksen. Tilauksen sisältämistä resursseista muodostetaan lasku ja statistiikkaa kuluista ja käytettyistä palveluista. Käyttäjä tiliin voidaan luoda lisää tilejä, joille kaikille muodostuu oma laskunsa. Useat tilit voidaan vielä yhdistää toisiinsa hallintaryhmän avulla. [72][73][74]

Kaikki käyttäjät, joilla on käyttöoikeus resurssiin voi käyttää resurssia omien Microsoft läyttäjätunnusten avulla, joko selaimessa toimivan Azure Portalin avulla tai CLI- työkalun kautta. Molemaat työkalut tarvitsevat käyttäjän käyttäjänimen ja salasanan. Kehitettävissä sovelluksissa käyttäjänimen ja salasanan käyttäminen ei ole suotavaa, koska oman salasanan suojaaminen muilta kehittäjiltä tai ylläpitäjiltä on erittäin haastavaa. Lisäksi käyttäjällä on yleensä laajemmat käyttöoikeudet resursseihin mitä kehitettävä sovellus vaatisi. Tätä käyttötapausta varten pääsynhallinnassa on sovelluskäyttäjät ja hallitut identiteetit. Sovelluskäyttäjät liittyvät Microsoftin laajempaan pääsynhallintajärjestelmään Microsoft Entra ID:hen. Microsoft Entra ID kattaa muitakin Microsoftin palveluita, kuten Office 365 ja OneDrive, joihin sen avulla voi antaa pääsyoikeudet. Sillä on oma selainpohjainen hallintapaneeli, jonka avulla voidaan antaa pääsyoikeuksia eri Microsoftin palveluihin. Sovelluskäyttäjille voidaan antaa Azuren roolien avulla käyttöoikeudet eri Azururen palveluihin. Hallitut identiteetit ovat sovelluskäyttäjien erikoistapauksia ja ne toimivat samalla tavalla. Erona on vain että hallitut identiteetit ovat olemassa vain Azuren sisällä ja niillä voidaan antaa käyttöoikeusia vain Azuren resursseihin. Sovelluskäyttäjät ja hallitut identiteetit mahdollistavat kirjautumisen sertifikaatin tai pitkän satunnaisgeneroidun salasanan avulla. Niille voidaan antaa juuri sovelluksen tarvittavat käyttöoikeudet ja käyttöoikeusia voidaaan muokata aina tarvittaessa. [75][76][77][78]

Azure tarjoaa mahdollisuutta hallita yksittäisen talletusratkaisun pääsynhallintaa 512- bittisen käyttöavaimen avulla. Käyttöavaimia on kaksi, jotka mahdollistavat sekä kirjoitus että lukuoperaatiot sekä kaksi avainta jotka mahdollistavat pelkät lukuoperaatiot. Käyttöavaimet ovat käytössä seuraavissa talletusratkaisuissa: Cosmos, File Share ja Blob Storage. Käyttöavaimen avulla talletusratkaisua voidaan käyttää sen julkisen päätepisteen tai ohjelmistokielien SDK- työkalujen avulla molemmat lukuoikeuden antavat avaimet mahdollistavat samallaiset lukuoidet talletusratkaisuun. Samalla tavalla kaksi kirjoitus ja lukuoikeutta antavaa avainta antaa samat oikeudet. Kaksi kumpaakin avainta mahdollistaa avainten kierrättämisen. Kierrättämisellä tarkoitetaan toisen avaimen päivittämistä uuteen avaimeen. Jos sovelluksella on käytössä molemmat avaimet, niin se pystyy toimimaan normaalisti käyttämällä toista vanhempaa vielä voimassa olevaa avainta. Kierrättämisellä pyritään parantamaan tietoturvaa ja Microsoft suosittelee säännöllistä avainten kierrättämistä. Avainten avulla voidaan luoda jaettuja käyttöoikeusallekirjoituksia (SAS). Jaettu käyttöoikeusallekirjoitus on URI, joka myöntää rajoitetut käyttöoikeudet talletusratkaisuun. Jaettuun käyttöoikeusallekirjoitukseen voidaan määrittää mitä operaatioita sen avulla voidaan suorittaa sekä voimassaoloaika. Jaetun käyttöoikeusallekirjoitus sopii tilanteihin joissa halutaan antaa pääsy vain tiettyihin tallennustilien resursseihin tietyn ajan. [79][80][81]

Microsoft Entra ID:n aikaisempi nimi oli Azure Active Directory (ADD) ja siitä löydettiin vakava haavoittuvuus vuonna 2023. Wiz- tutkimustiimi löysi haavoittuvuuden Microsoftin omistamasta Bing- hakukoneesta. Bing- hakukoneen pääsynhallinta oli toteutettu ADD -pääsynhallinnalla. Bing hakukoneen pääsynhallinnassa oli haavoittuvuus, joka mahdollisti minkä tahansa ADD -käyttäjän kirjautumisen Bing Trivia -sivustolle. Bing Trivia -sivusto oli hallintapaneeli, jonka avulla pystyttiin muun muassa muokkaamaan Bing hakukoneen hakusivun ulkoasua. Wiz- tutkimustiimi onnistui lisäämään Bing-hakukoneeseen JavaScript koodia. Hyökkäystä kutsutaan Cross Site Scripting (XSS), kun hyökkääjä onnistuu samaan haitallista JavaScript koodia ajoon uhrin selaimeen. XSS- hyökkäyksellä onnistuttiin varastamaan Bing käyttäjien Office 365 -tileihin kirjautumistunnuksia. Myös muihin pienempiin Microsoftin sisäisiin palveluihin pääsi kirjautumaan millä tahansa ADD- tunnuksella.[82]

Azuren talletusratkaisuista on löytynyt myös vakava tietoturvahaavoittuvuus vuonna 2021, joka sai nimekseen ChaosDB. Haavoittuvuus koskee Cosmos tietokantaa ja sen löysi Wiz- tutkimustiimi. ChaosDB- haavoittuvuus mahdollisti rajoittamattoman pääsyn useiden tuhansien Azure -asiakkaiden Cosmos tietokantoihin. Haavoittuvuus johtui Jupiter Notebook -ominaisuuden virheellisestä konfiguraatiosta Cosmos tietokantaan. Jupyter Notebook on interaktiivinen verkkosovellus laskennallisten asiakirjojen luomiseen ja jakamiseen. Jupiter Notebook- ominaisuus mahdollistaa Cosmos tietokannan datan visualisoinnin. Hyödyntämällä Cosmos tietokannan Jupyter Notebook -ominaisuuden haavoittuvuuksien ketjua, hyökkääjä voi tiedustella tietoja kohde Cosmos tietokannan Jupyter Notebookista. Näin tehdessään hyökkääjä saa joukon tunnistetietoja, jotka liittyvät kohde Cosmos tietokannan tiliin sekä Jupyter Notebook -laskentaan. Näiden tunnistetietojen joukossa on myös Cosmos tietokannan käyttöavaimet, joiden avulla hyökkääjä pääsee käsiksi Cosmos tietokantaan. ChaosDB haavoittuvuus mahdollisti hyökkääjien nostamaan käyttöoikeuksiaan joka mahdollisti pääsyn Cosmos tietokannan sisäisiin salaisuuksiin ja varmentetihin. Näiden salaisuuksien avulla hyökkääjät pääsivät käsiksi muiden Cosmos tietokantojen käyttöavaimiin. Haavoittuvuuus koski kaikkia Cosmos tietokantoja, joissa oli Jupyter Notebook -ominaisuus päällekytkettynä. Jupyter Notebook -ominaisuus oli päällekytkettynä uusissa Cosmos tietokannoissa, ja käyttäjän piti erikseen laittaa ominaisuus pois päältä halutessaan tietokantaa luotaessa. Wiz- tutkimustiimi ilmoitti haavoittuvuudesta Microsoftille ja Microsodt korjasi ChaosDB -haavoittuvuuden kahden päivän kuluessa. Microsoft on ilmoittanut että sillä ei ole viitteitä että jokin muu taho kuin Wiz- tutkimustiimi olisi päässyt ChaosDB- haavoittuvuuden ansiosta käsiksi muiden käyttäjien Cosmos tietokantoihin. Microsoft kuitenkin suositteli kaikkia asiakkaitansa kierrättämään Cosmos tietokannan käyttöavaimensa.[83][84]

Azure tarjoaa osalle talletusratkaisuista lisäpalveluna erillistä tietoturvapalvelua. Microsoft Defender for Storage on Azuren tietoturvakerros, joka havaitsee mahdolliset uhat talletusratkaisuissa. Se auttaa estämään seuraavia vakavia tietoturvaongelmia: haitalliset tiedostojen lataukset, arkaluonteisten tietojen vuotaminen ja tietojen korruptio. Sitä on mahdollista käyttää Blob Storage-, Azure Files- ja Azure Data Lake Storage – talletusratkaisuiden kanssa. Microsoft Defender for Storage sisältää seuraavat toiminnalisuudet: toiminnan seurannan, arkaluonteisten tietojen uhkien havaitsemisen ja Haittaohjelmien tarkistuksen. Toiminnan seurantaan Defender for Storage analysoi jatkuvasti suojattujen talletusratkaisuiden dataa ja ohjaustason lokeja, kun se on käytössä. Palvelu käyttää Microsoft Threat Intelligenceä tunnistaaksesi epäilyttävät asiat, kuten haitalliset IP-osoitteet, Tor-poistumissolmut ja mahdollisesti vaaralliset sovellukset. Se myös rakentaa tietomalleja ja käyttää tilastollisia- ja koneoppimismenetelmiä havaitakseen perustoiminnan poikkeavuuksia, jotka voivat viitata haitalliseen toimintaan. Palvelu luo tietoturvavaroituksia epäilyttävistä toiminnoista. Haittaohjelmien tarkistus Defender for Storagessa auttaa suojaamaan tallennustilejä haitalliselta sisällöltä suorittamalla täyden haittaohjelmatarkistuksen ladatulle sisällölle lähes reaaliajassa käyttämällä Microsoft Defender Antivirus -ominaisuuksia. Arkaluonteisten tietojen uhkien havaitseminen mahdollistapalvelun tuottamien tietoturvavaroituksien priorisoinnin tietojen arkaluonteisuuden avulla. Defender for Storagen hinta on 10€ kuukaudessa jokaista talletusratkaisun tiliä kohden.[85]

### Pilvialustojen turvallisuustutkimukset

Vaikka pilvialustojen palveluiden tietoturvaongelmat ovat erittäin harvinaisia niin pilvialustoille kehitettyjen sovellusten tietoturvaongelmat ovat yleisiä. Snyk tietoturvayhtiön vuonna 2022 tekemässä tutkimuksessa The State of Cloud Security Report 2022 tutkittiin pilvialustoille kehitettyjen sovellusten tietoturvahaasteita. Tutkimukseen osallistui tietoturva-asiantuntijoita sekä pilvikehittäjiä. Kuva 23 esittää tutkimukseen osallistuneiden koetut vakavat tietoturvaongelmat pilvialustoille kehitetyissa sovelluksissa. Yleisin ongelma oli järjestelmän seisokkki, joka oli johtunut virheellisestä konfiguroinnista. Tietomurrot ja tietovuodot olivat myös erittäin yleisiä, vastaajista noin 26% oli kokonut tietovuodon ja 33% oli kokenut tietomurron.[86]

A graph with blue and white text

Description automatically generated

Kuva 25 Snykin tutkimukseen vastanneiden kokemat pilviturvallisuusongelmat

Samassa tutkimuksessa myös kysyttiin tietoturvaongelmien aiheuttajaa. Vastaajat saivat valita useampia teknisiä vaihtoehtoja, jotka olivat aiheuttaneet pilvialustoilla tietoturvaongelmia. Kuva 24 esittää tutkimuksen tuloksia teknisistä ongelmista, jotka olivat aiheuttaneet tietoturvahäiriöitä. Tutkimuksen mukaan eniten tietoturvaongelmia aiheutti turvattomasti säilytetyt varmuuskopiot, jotka olivat olleet mukana 23 % tapahtuneista tietoturvaongelmista. Ongelman aiheuttajat voidaan ryhmittää muutamaan pääryhmään. Tietoturvakriittisten asioiden turvaton säilyttäminen kuten varmuuskopiot ja API avaimet. Puutteelliset valvontamentelmät, esimerkiksi puutteelliset lokitiedot. Pääsynhallinnan virheelliset asetukset, sisältäen ryhmät sekä Object Storagen. Turvattomat yhteydet sekä tietovarastot(virtuaalikoneiden yhteydet, tiedonsiirto ja tietovarastot).[86]

A graph with blue and white text

Description automatically generated

Kuva 26 Tietoturvaongelmien aiheuttajat Snykin tutkimuksessa

Samassa tutkimuksessa myös kysyttiin syitä, jotka olivat aiheuttaneet tietoturvaongelmia. Kuva 25 esittää syitä, jotka ovat aiheuttaneet tietoturvaongelmia kutkimuksen mukaan.

A graph with blue and white text

Description automatically generated

Kuva 27 Tietoturvaongelmien aiheutumisien syyt Snykin tutkimuksen mukaan

Tietämyksen puute tietoturvasta ja nopea ympäristön muuttuminen oli yleisimmät syyt, jotka oli johtanut tietoturvaongelmiin. Molemmat syyt todennäköisesti lisääntyvät tutkimuksen mukaan tulevaisuudessa kun yhä useammat tiimit ottavat käyttöön jatkuvan käyttöönottomenetelmän ja sen tuomat tietoturvahaasteet. Suurin osa syistä johtuu pelkästään ihmisten toiminnasta, eikä liity käytettyyn pilviteknologiaan. Inhimillisen tekijän vaikutusta tietoturvaongelmiin on tukittu IBM:n vuonna 2024 julkaisemassa tutkimuksessa 2024 Data Breach Investigations Report. IBM:n tutkimus käsittelee vuosina 2022-2023 tapahtuneita tietomurtoja ja se käsittää myös pilvialostojen ulkopuolisia tietomurtoja. Kuva 26 esittää IBM:n tutkimuksen tietomurtojen avaintekijöitä. Inhimillinen tekijä oli yleisin avaintekijä ja se oli mukana 68% tehdyissä tietomurroissa. Muut tekijät tutkimuksessa oli teknisiä, mutta niiden yleisyys oli maksimissaan puolet inhimillisestä tekijästä.[86][87]

A graph with blue bars

Description automatically generated with medium confidence

Kuva 28 Avaintekijät tietomurroissa IBM:n tekemässä tutkimuksessa

Yksi IBM:n tutkimuksen inhimillisistä tekijöistä on tietojenkalastelu. Tietojenkalastelu tarkoittaa yritystä varastaa arkaluonteisia tietoja, tyypillisesti käyttäjätunnuksia, salasanoja tai pankkitunnuksia. Tietojenkalastelu tehdään yleensä sähköpostin tai tekstiviestien avulla. Tutkimuksessa vuonna 2023 vastaajista 20% ilmoitti saaneensa tietojenkalasteluviestejä ja 11% vastaajista oli avannut viestin. Tietojenkalastelun määrä on kasvanut tutkimuksen mukaan tasaisesti vuodesta 2016 asti, jolloitutkimuksessa alettiin pitää ensimmäistä kertaa kirjaa tietojenkalasteluviesteistä. Kuva 27 esittää IBM:n tutkimuksessa käytettyjä menetelmiä tietomurroissa. Yleisin mentelmä on käyttäjätunnukset, joka pitää sisällään virheellisen pääsynhallinnan sekä turvattoman tavan säilyttää käyttäjätunnuksia. Tietojenkalastelu on tutkimuksen mukaan toisista yleisin tietomurtojen aiheuttaja haavoittuvuuksien hyväksikäytön kanssa. [87]

A graph with numbers and text

Description automatically generated

Kuva 29 Tietomurroissa käytetyt menetelmät IBM:n tutkimuksessa

# yhteenveto

# Lähteet

1. https://www.dataversity.net/brief-history-cloud-computing/, viitattu 3.9.2024

1. <https://www.dataversity.net/how-the-cloud-has-evolved-over-the-past-10-years/>, viitattu 3.9.2024

1. <https://www.cloudzero.com/blog/cloud-computing-statistics/>, viitattu 3.9.2024

1. <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds>, viitattu 3.9.2024

1. <https://www.marketsandmarkets.com/Market-Reports/cloud-storage-market-902.html>, viitattu 3.9.2024

1. <https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/>, viitattu 4.9.2024

1. <https://httpwg.org/specs/rfc9110.html>, viitattu 4.9.2024

1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>, viitattu 4.9.2024

1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Status>, viitattu 4.9.2024

1. <https://www.javacodegeeks.com/2023/03/http-1-1-vs-http-2-vs-http-3-key-differences.html>, viitattu 4.9.2024

1. <https://ably.com/topic/http-2-vs-http-3>, viitattu 4.9.2024

1. <https://www.w3.org/Protocols/HTTP/1.0/spec>, viitattu 4.9.2024

1. <https://www.rfc-editor.org/rfc/rfc9114.txt>, viitattu 4.9.2024

1. <https://http.dev/3>, viitattu 4.9.2024

1. <https://www.cloudwards.net/what-is-webdav/>, viitattu 4.9.2024

1. <https://datatracker.ietf.org/doc/html/rfc4918>, viitattu 4.9.2024

1. <http://www.webdav.org/specs/rfc3744.html>, viitattu 4.9.2024

1. <https://developer.mozilla.org/en-US/docs/Web/API/WebSocket>, viitattu 5.9.2024

1. <https://datatracker.ietf.org/doc/html/rfc6455>, viitattu 5.9.2024

1. <https://http.dev/ws>, viitattu 5.9.2024

1. <https://tools.ietf.org/html/rfc959>, viitattu 5.9.2024

1. <https://www.rfc-editor.org/rfc/rfc4217.txt>, viitattu 5.9.2024

1. <https://www.ssh.com/academy/ssh/sftp-ssh-file-transfer-protocol>, viitattu 5.9.2024

1. <https://datatracker.ietf.org/doc/html/draft-ietf-secsh-filexfer-02>, viitattu 5.9.2024

1. <https://www.ibm.com/docs/en/ssw_ibm_i_71/sqlp/rbafy.pdf>, viitattu 5.9.2024

1. <https://www.postgresql.org/docs/current/routine-vacuuming.html>, viitattu 5.9.2024

1. <https://en.wikibooks.org/wiki/PostgreSQL/Architecture>, viitattu 5.9.2024

1. <https://www.mongodb.com/resources/basics/databases/document-databases>, viitattu 6.9.2024

1. <https://www.mongodb.com/resources/basics/databases/types>, viitattu 6.9.2024

1. <https://www.mongodb.com/resources/basics/databases/nosql-explained>, viitattu 6.9.2024

1. <https://www.ibm.com/topics/object-storage>, viitattu 6.9.2024

1. <https://www.redbooks.ibm.com/redpieces/pdfs/redp5537.pdf>, viitattu 6.9.2024

1. <https://www.snia.org/education/what-is-scsi>, viitattu 6.9.2024

1. <https://datatracker.ietf.org/doc/html/rfc3347>, viitattu 6.9.2024

1. <https://datatracker.ietf.org/doc/html/rfc4172>, viitattu 6.9.2024

1. <https://datatracker.ietf.org/doc/html/rfc4707>, viitattu 7.9.2024

1. <https://apix-drive.com/en/blog/reviews/microsoft-azure-review>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/what-is-azure>, viitattu 7.9.2024

1. <https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm>, viitattu 7.9.2024

1. <https://math.asu.edu/sites/default/files/rsa_0.pdf>, viitattu 7.9.2024

1. <https://kinsta.com/knowledgebase/tls-vs-ssl/>, viitattu 7.9.2024

1. <https://aws.amazon.com/what-is/ssl-certificate/>, viitattu 7.9.2024

1. <https://www.ssl.com/article/ssl-tls-self-signed-certificates/>, viitattu 7.9.2024

1. <https://www.thesslstore.com/blog/tls-1-3-handshake-tls-1-2/>, viitattu 7.9.2024

1. <https://www.upguard.com/blog/diffie-hellman>, viitattu 7.9.2024

1. <https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/> , viitattu 7.9.2024

1. <https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf>, viitattu 7.9.2024

1. <https://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.nrf52832.ps.v1.1%2Fccm.html>, viitattu 7.9.2024

1. <https://datatracker.ietf.org/doc/html/rfc8446>, viitattu 7.9.2024

1. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>, viitattu 7.9.2024

1. <https://www.f5.com/labs/articles/threat-intelligence/the-2021-tls-telemetry-report>, viitattu 7.9.2024

1. <https://azure.microsoft.com/en-us/pricing/details/cosmos-db/autoscale-provisioned/>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/cosmos-db/request-units>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/azure-sql/database/dtu-benchmark?view=azuresql>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/azure-sql/database/resource-limits-dtu-single-databases?view=azuresql>, viitattu 7.9.2024

1. <https://azure.microsoft.com/en-us/pricing/details/azure-sql-database/single/>, viitattu 7.9.2024

1. <https://azure.microsoft.com/en-us/products/storage/blobs/> , viitattu 7.9.2024

1. <https://azure.microsoft.com/en-us/pricing/details/storage/blobs/>, viitattu 7.9.2024

1. <https://azure.microsoft.com/en-us/pricing/details/storage/files/>, viitattu 7.9.2024

1. <https://azure.microsoft.com/en-us/pricing/details/managed-disks/> <https://learn.microsoft.com/en-us/azure/virtual-machines/disk-bursting>, viitattu 7.9.2024

1. <https://www.ibm.com/think/topics/man-in-the-middle>, viitattu 7.9.2024

1. <https://gcore.com/learning/http-vs-https-security-comparison/>, viitattu 7.9.2024

1. <https://www.acunetix.com/blog/articles/breach-attack/>, viitattu 7.9.2024

1. <https://beaglesecurity.com/blog/vulnerability/the-rc4-algorithm-in-transport-layer-security-and-secure-sockets-layer.html>, viitattu 7.9.2024

1. <https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/>, viitattu 7.9.2024

1. <https://www.acunetix.com/blog/web-security-zone/what-is-poodle-attack/>, viitattu 7.9.2024

1. <https://www.acunetix.com/blog/articles/poodle-gives-final-bite-puts-sslv3-rest/>, viitattu 7.9.2024

1. <https://drownattack.com/>, viitattu 7.9.2024

1. <https://www.acunetix.com/white-papers/acunetix-web-application-vulnerability-report-2020/>, viitattu 7.9.2024

1. <https://www.f5.com/labs/articles/threat-intelligence/the-2021-tls-telemetry-report>, viitattu 7.9.2024

1. <https://www.spiceworks.com/tech/networking/articles/sftp-vs-ftps/>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/entra/identity-platform/howto-create-service-principal-portal>, viitattu 7.9.2024

1. <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id>, viitattu 7.9.2024

1. [https://learn.microsoft.com/fi-fi/azure/storage/common/storage-account-keys-manage?tabs=azure-portal#regenerate-access-keys](https://learn.microsoft.com/fi-fi/azure/storage/common/storage-account-keys-manage?tabs=azure-portal" \l "regenerate-access-keys), viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data?tabs=using-primary-key>, viitattu 7.9.2024

1. <https://learn.microsoft.com/fi-fi/azure/storage/common/storage-account-keys-manage?tabs=azure-portal>, viitattu 7.9.2024

1. <https://www.wiz.io/blog/azure-active-directory-bing-misconfiguration>, viitattu 7.9.2024

1. <https://securityaffairs.com/124510/hacking/chaosdb-flaw-technical-details.html>, viitattu 7.9.2024

1. <https://chaosdb.wiz.io/>, viitattu 7.9.2024

1. <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction>, viitattu 7.9.2024

1. <https://go.snyk.io/rs/677-THP-415/images/cloud-security-report-22.pdf>, viitattu 7.9.2024

1. <https://www.verizon.com/business/resources/T4d/reports/2024-dbir-data-breach-investigations-report.pdf>, viitattu 7.9.2024

|  |
| --- |
|  |