Aaro Koinsaari

Turvallisuusstrategiat IoT-ympäristöissä

Tietotekniikan kandidaatintutkielma

29. huhtikuuta 2024

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Aaro Koinsaari

Yhteystiedot: aaro.k.koinsaari@student.jyu.fi

Ohjaaja: Sanna Juutinen

Työn nimi: Turvallisuusstrategiat IoT-ympäristöissä

Title in English: Security strategies in IoT environments

Työ: Kandidaatintutkielma

Sivumäärä: 29+0

Tiivistelmä: Internet of Things (IoT) yhdistää päivittäin käyttämiämme laitteita globaaliin verkkoon mahdollistaen kommunikaation ja älykkäiden toimintojen automatisoinnin. IoT tarjoaa merkittävää potentiaalia useilla sektoreilla mutta sen laajamittainen käyttöönotto tuo mukanaan vakavia turvallisuushaasteita. Tässä tutkielmassa tarkastellaan näitä haasteita sekä keskustellaan strategioista, joilla pyritään parantamaan niitä etenkin verkkokerroksella. Tutkielma keskittyy verkkoliikenteen analysointiin, autentikointiin ja pääsynvalvontaan, lohkoketjuteknologiaan sekä reunalaskentaan. Lopuksi analysoidaan näiden menetelmien vahvuuksia ja heikkouksia yhdessä, jotta tulevaisuudessa voidaan kehittää monipuolisempia ja tehokkaampia turvallisuusratkaisuja IoT-verkkojen suojelemiseksi.

Avainsanat: kandidaatintutkielma, iot, turvallisuus, IoT-verkot

Abstract: The Internet of Things (IoT) rapidly integrates our daily devices into a global network, enabling communication and automated intelligent functions. IoT presents significant potential across various sectors but its widespread adoption introduces substantial security challenges. This paper reviews these challenges and discusses strategies to enhance IoT security, especially on the network layer. It focuses on network traffic analysis, authentication and access control, blockchain technology, and edge computing. Finally, the strengths and weaknesses of these methods are analyzed together to enhance the understanding and discussion of security solutions for protecting IoT networks in the future.

Keywords: Bachelor's thesis, iot, security, IoT networks

Sisällys

1 Johdanto

Internet of Things (IoT) on nopeasti kehittyvä teknologia, joka yhdistää ympärillämme olevia laitteita verkkoon mahdollistaen niiden välisen kommunikaation keskenään (Atzori, Iera ja Morabito 2010). Vaikka IoT tarjoaa merkittävää potentiaalia monilla elämänalueilla, kuten teollisuudessa, terveydenhuollossa tai ympäristönseurannassa (Neshenko ym. 2019), sen laajamittainen käyttöönotto tuo mukanaan myös vakavia turvallisuushaasteita. Tämä tutkielma tarkastelee IoT:n nykytilaa ja sitä, miksi IoT-laitteet ovat tunnetusti niin heikkoja suojaukseltaan, sekä käy läpi erilaisia strategioita, joilla pyritään parantamaan IoT-ympäristöjen turvallisuutta. Tähän tutkielmaan eri turvallisuusstrategiat on rajattu verkkoliikenteen analysointiin ja anomalioiden tunnistamiseen, autentikointiin ja pääsynvalvontaan, lohkoketjuteknologiaan sekä reunalaskentaan.

On tärkeää ymmärtää, että esitellyt strategiat ovat toistensa leikkaavia eivätkä ne rajoitu pelkästään verkkokerrokseen; ne tarjoavat laajempia näkökulmia ja ratkaisuja IoT-verkkojen suojaamiseen. Vaikka tässä tutkielmassa keskitytään vain kyseisiin strategioihin, on olemassa myös muita turvallisuusstrategioita, kuten fyysinen suojaus tai käyttäjien tietoisuuden lisääminen, jotka voivat olla yhtä lailla tärkeitä IoT-ympäristöjen turvallisuuden kannalta.

Strategioiden esittelyn jälkeen analysoidaan näiden vahvuuksia, heikkouksia ja niiden yhteispeliä, jotta tulevaisuudessa voidaan kehittää monipuolisempia ja tehokkaampia turvallisuusratkaisuja IoT-verkkojen suojelemiseksi.

Keskeisenä tutkimuskysymyksenä on selvittää, kuinka esitellyt turvallisuusstrategiat suojaavat IoT-verkkoja, millaisia haasteita kunkin strategian soveltamisessa kohdataan, sekä millaisia näkökulmia tulisi ottaa huomioon näiden strategioiden integroimiseksi, jotta voidaan kehittää mahdollisimman tehokas ratkaisu IoT-verkkojen turvallisuuden varmistamiseksi.

Tutkimusmenetelmänä käytetään kirjallisuuskatsausta, joka soveltuu aiheen laaja-alaiseen tarkasteluun. Tutkielmassa käydään läpi kattavasti kirjallisuutta, joka käsittelee eri turvallisuusstrategioita IoT-ympäristöille ja esittelee niiden keskeisiä tieteellisiä julkaisuja. Lisäksi IoT:n taustaa ja nykytilaa valotetaan käyttäen julkisia tilastotietoja, jotka tarjoavat kattavan kuvan IoT:n kehityksestä ja nykytilanteesta. Kirjallisuuskatsauksen avulla pyritään tarjoa-

maan syvällinen ymmärrys esitellyistä turvallisuusstrategioista ja niiden vuorovaikutuksesta keskenään, jotta voidaan luoda pohja tulevaisuuden turvallisuusratkaisujen kehittämiselle IoT-ympäristöissä.

2 Keskeiset käsitteet ja niiden ympäristö

Tässä luvussa keskitytään keskeisten käsitteiden selventämiseen, jotka ovat oleellisia ymmärtämään IoT-teknologian toimintaa ja sen tuomia haasteita. Aluksi määritellään, mitä IoT tarkoittaa ja kuinka se muuttaa perinteistä käsitystämme Internetistä muuttaen sen toisiinsa yhteydessä olevien älykkäiden objektien verkostoksi. Tarkastellaan myös IoT:n keskeisiä sovellusalueita sekä botnet-käsitettä ja DDoS-hyökkäyksiä, jotka ovat keskeisimpiä haitallisia sovellutuksia, johon IoT-laitteita voidaan käyttää. Tämän avulla pyritään luomaan kuva ja vastaamaan siihen, miksi IoT:n turvallisuuden huomiointi on kriittisen tärkeää.

2.1 Internet of Things

Esineiden Internet, eli Internet of Things (*IoT*) konseptille on vaikeaa löytää yksiselitteistä määritelmää. Atzorin, Ieran ja Morabiton mukaan IoT tarkoittaa paradigmaa, jossa ympärillämme olevat laitteet, kuten erilaiset sensorit, toimilaitteet ja puhelimet, ovat verkottuneita ja kykeneviä kommunikoimaan keskenään (Atzori, Iera ja Morabito 2010). Heidän mukaansa se, miten IoT määritellään, voi kuitenkin vaihdella riippuen kontekstista ja siitä, katsotaanko sitä nimensä mukaan esinekeskeisestä vai internetkeskeisestä näkökulmasta. Miorandi ym. (2012) mukaan IoT voidaan laajemmin käsittää innovaationa, joka syntyy arjen fyysisten objektien muuttuessa älykkäiksi teknologian avulla, ja niiden yhdistyessä osaksi globaalia kyberfyysistä infrastruktuuria. Tämä tarkoittaa, että perinteinen käsitys Internetistä, joka toimii loppukäyttäjien laitteisiin ulottuvana infrastruktuuriverkkona, väistyy toisiinsa yhdistettyjen älykkäiden esineiden kommunikoinnin tieltä (Miorandi ym. 2012). Toisin sanoen IoT muuntaa nykyisen Internetin toisiinsa yhteydessä olevien älykkäiden objektien verkostoksi, joka kerää tietoa ympäristöstään, vuorovaikuttaa fyysisen maailman kanssa ja tarjoaa monipuolisia palveluita käyttäen olemassa olevia internetstandardeja (Gubbi ym. 2013).

IoT:n hyödyistä ja sen potentiaalista nykypäivänä ja tulevaisuudessa ei ole epäilystä, sillä se tuo innovatiivisia ja tärkeitä ratkaisuja ongelmiin monella eri sektorilla. Konkreettisina esimerkkeinä tästä voidaan antaa Neshenko ym. (2019) mukaan ratkaisuja, jotka esimerkiksi vähentävät onnettomuusriskiä älykkäiden ajoneuvojen ja itsenäisesti toimivien teollisuuslait-

teistojen avulla; lisäävät vanhusten ja vammaisten itsenäisyyttä mahdollistamalla reaaliaikaisen hälytyksen terveydellisissä hätätilanteissa; valvovat ympäristön saastumista ja kemiallisia vuotoja tehtaissa, sekä edistävät luonnonvarojen kestävää käyttöä älykkäiden mittauslaitteiden avulla.

IoT:n tarjoamien hyötyjen ohella on kuitenkin syntynyt vakavia turvallisuusriskejä, kun liiketoiminnan voitontavoittelu ja nopea tuotteiden markkinoille tuonti yhdessä puutteellisen lainsäädännön kanssa on johtanut vakavaan turvallisuusnäkökulmien laiminlyöntiin (Neshenko ym. 2019). Laitteiden heikon suojauksen syitä käsitellään tarkemmin kappaleessa 3.

IoT-markkinoiden odotetaan kasvavan yli 15 miljardista laitteesta vuonna 2015 yli 75 miljardiin vuoteen 2025 mennessä (Butun, Österberg ja Song 2019). Samaan aikaan hajautettujen palvelunestohyökkäysten (*DDoS*) volyymi on kasvanut räjähdysmäisesti 2007-2016 välisenä aikana kohoten etenkin vuodesta 2012 lähtien (ks. Mahjabin ym. 2017). Tämä korostaa IoT-laitteiden ja verkon suojausprotokollien ja -mekanismien kehityksen välttämättömyyttä, sillä jokainen näistä miljardeista laitteista muodostaa potentiaalisen riskin joutua osaksi botnet-verkostoa ja sitä kautta DDoS-hyökkäysten välineiksi (ks. kappale 2.2). Tämän vuoksi IoT:n turvallisuuspuutteet eivät ole uhka pelkästään yksittäisen verkon tietoturvalle vaan koko Internetille. Toinen syy tietoturvan ja suojauksen kehittämisen tarpeelle on IoT-laitteiden käyttökohteet etenkin kriittisen infrastruktuurin kohteissa, kuten terveydenhuollossa. Islam ym. (2015) korostavat, että IoT tarjoaa erittäin lupaavia mahdollisuuksia terveydenhuollon alalla tehden siitä yhden IoT-ympäristön keskeisimmistä sovelluskohteista.

2.2 DDoS-hyökkäykset ja botnet-verkostot

Palvelunestohyökkäyksessä (*Denial-of-Service, DoS*) pyritään estämään legitiimin käyttäjän pääsy johonkin palveluun, ja niiden käyttö on vuosien ajan ollut luonteeltaan hajautettua (Zargar, Joshi ja Tipper 2013). Tällöin voidaan puhua hajautetusta palvelunestohyökkäyksestä (*Distributed Denial-of-Service, DDoS*), jossa palveluihin pääsy pyritään estämään käyttämällä hyödyksi monia eri lähteitä, jotka lähettävät haluttuun kohteeseen valtavia määriä liikennettä (Mirkovic ja Reiher 2004). Tämän tarkoituksena on ylikuormittaa järjestelmän resursseja tai aiheuttaa toimintahäiriöitä, mikä tekee palveluista saavuttamattomia oikeille

käyttäjille. Hyökkäysketjun toteutus alkaa usein värväämällä ja kaappaamalla eri laitteita (agenttilaitteita) tietoturva-aukkojen kautta. Nämä laitteet tartutetaan hyökkäyskoodilla, jota sitten käytetään lisäämään hyökkäyksen voimaa tai rekrytoimaan lisää agentteja, jolloin väärinkäytettyjen pakettien lähettäminen sekoittaa kohdejärjestelmän toimintaa. (Mirkovic ja Reiher 2004)

DDoS-pohjaiset hyökkäykset toteutetaan nykyään yleensä botnet-verkostojen kautta (Zargar, Joshi ja Tipper 2013). Botnet viittaa haittaohjelman saaneisiin, jo saastuneiden laitteiden verkkoon, joita etenkin IoT:n kontekstissa käytetään laukaisemaan DDoS-hyökkäyksiä (Salim, Rathore ja Park 2020).

3 IoT-laitteiden turvallisuushaasteet

IoT:n heikko turvallisuus on ollut jo vuosien ajan yksi keskeisistä teemoista, joka on esillä alan akateemisessa keskustelussa (esim. Alaba ym. 2017; Mosenia ja Jha 2017; Neshenko ym. 2019; Atzori, Iera ja Morabito 2010; Miorandi ym. 2012). Syy tähän juontuu useista keskeisistä tekijöistä, joita Neshenko ym. (2019) tuovat artikkelissaan esille. Yksi niistä on puute yhtenäisestä ja systemaattisesta turvallisuusvisiosta IoT-ympäristössä, sillä standardoituja turvallisuusratkaisuja ei ole laajalti vielä implementoitu (Neshenko ym. 2019). Toisaalta IoT-laitteiden heterogeenisuus ja niiden rajoitetut resurssit, kuten laskentateho, muisti ja verkon kaistanleveys rajoittavat kehittyneempien turvallisuusprotokollien käyttöönottoa (Vishwakarma ja Jain 2020; Alaba ym. 2017; Chaabouni ym. 2019). Heterogeenisyys, eli laitteiden ja standardien moninaisuus, sekä IoT:n ja perinteisten laitteiden verkkoinfrastruktuurin erot vaikuttavat Vishwakarman ja Jainin mukaan siihen, miksi myös IoT:n avulla toteutetut DDoS-hyökkäykset ovat hieman monipuolisempia ja hienostuneempia (Vishwakarma ja Jain 2020). Myös Sharma, Pandey ja Khatri (2017) huomauttavat, että IoT-laitteiden ainutlaatuinen kyky kommunikoida laitteelta toiselle (*M2M*) lisää verkoston monimutkaisuutta, mikä asettaa vaatimuksia uudentyyppisille turvallisuusratkaisuille. Neshenko ym. (2019) tutkimuksen mukaan IoT-laitteiden moninaisuuden ja niiden käyttämien protokollien erityispiirteiden vuoksi turvallisuusratkaisujen skaalautuminen onkin osoittautunut haastavaksi ja siksi monet nykyiset suojausmetodit ovat vielä alkuvaiheessa eivätkä ne kattavasti torju laajaa kirjoa hyökkäyksiä. Liiketoiminnan voitontavoittelu, pyrkimys nopeaan markkinoille tuloon sekä sääntelyn puute ovat johtaneet myös siihen, että valmistajat ovat jättäneet laitteiden turvallisuuspuolen huomiotta ja markkinoille on päässyt yhä enemmän heikosti suojattuja IoT-laitteita (Neshenko ym. 2019).

IoT-laitteiden turvallisuushaasteiden taustalla olevat tekijät voidaan täten lajitella karkeasti neljään eri päätekijään: laitteiden heterogeenisuus, laitteiden rajalliset resurssit, yhtenäisten ja standardoitujen turvallisuusprotokollien puute sekä heikko sääntely. Tiivistetysti IoT-laitteiden heterogeenisuus ja niiden rajalliset resurssit ovat keskeisiä ongelmia kehittyneiden turvallisuusratkaisujen käyttöönotossa. Eri laitteiden vaihtelevat käyttötarkoitukset ja kapasiteetit sekä niiden heikko yhteentoimivuus luovat haasteita yhtenäisten turvallisuusproto-

kollien toteuttamiselle. Tämän lisäksi IoT-laitteiden nopea lisääntyminen on johtanut turvallisuuskehityksen viivästymiseen, mikä on osin seurausta valmistajien paineista pitää kustannukset alhaisina ja sääntelyn puutteesta, mikä on johtanut puutteelliseen laitesuojaukseen.

IoT-laitteiden resurssirajoitteet voivat siis tehdä verkkokerroksen suojaamisesta käytännöllisemmän lähestymistavan turvallisuuden parantamiseen erityisesti kun otetaan huomioon laitteiden tehon paranemisen mahdollisuus. Kuitenkin, jos laitekehitys ei sisällä riittäviä turvatoimia, kasvaa riski vakavien turvallisuusuhkien, kuten DDoS-hyökkäysten, esiintymiselle, mikä voi uhata koko Internetin infrastruktuuria. On tärkeää, että valmistajat tunnistavat tarpeen implementoida kattavia turvallisuusratkaisuja jo laitekehityksen alkuvaiheissa, mikä voi edellyttää uusien markkinainsentiivien tai tiukemman sääntelyn käyttöönottoa. Toisaalta on myös tärkeää, että loppukäyttäjät ymmärtävät ja aktiivisesti ylläpitävät laitteidensa turvallisuutta esimerkiksi säännöllisten päivitysten avulla.

3.1 Botnet ja IoT: DDoS-hyökkäysten uusi eturintama

Kuten aiemmin todettiin, IoT-laitteet ovat useasti osana botnet-verkostoa, jonka kautta massiiviset DDoS-hyökkäykset toteutetaan. IoT-laitteiden määrän sekä botnet-verkostoihin yhdistettyjen IoT-laitteiden ja sitä kautta DDoS-hyökkäysten määrän välillä voidaan havaita selkeä korrelaatio. Abu Rajab ym. (2006) havaitsivat tutkimuksessaan, että 27 % kaikista haitallisista yhteysyrityksistä heidän hajautetussa verkossaan voitiin suoraan yhdistää botnet-verkostojen levittämään toimintaan. Heidän havaintojensa mukaan botnet-liikenteen todellinen osuus on kuitenkin merkittävästi suurempi kuin mitä tämä luku antaa ymmärtää (Abu Rajab ym. 2006). On syytä huomioida, että tämä tutkimus tehtiin jo lähes 20 vuotta sitten. Botnettiin liitettyjen IoT-laitteiden määrä nousi noin 200 000:sta vuonna 2022 noin miljoonaan laitteeseen vuonna 2023, mikä muodostaa yli 40 % kaikesta DDoS-liikenteestä tänä päivänä (Nokia Corporation 2023). StationX:n mukaan on ollut 807 % kasvu tehdyissä DDoS-hyökkäyksissä vuosien 2013 ja 2022 välillä (Smith 2024). Samaan aikaan Statistan tietojen mukaan IoT-laitteiden määrä oli kasvanut vuoden 2019 8,6 miljardista 15,14 miljardiin vuoteen 2023 mennessä (Statista 2024).

IoT-laitteiden massiivinen kasvu tarjoaa siis täydellisen hyödyntämiskentän kyberrikollisille,

etenkin hajautetuille palvelunestohyökkäyksille, mikä selittää myös botnet-verkkojen määrän ja sitä kautta DDoS-hyökkäysten määrän jatkuvaa kasvua. Suureneva määrä hajautettuja, usein heikosti suojattuja laitteita muodostaa laajan pohjan, josta botnet-verkostot voivat rekrytoida uusia kaapattuja laitteita suorittamaan massiivisia palvelunestohyökkäyksiä. IoT on tämän vuoksi keskeisessä roolissa DDoS-hyökkäysten määrän ja tehokkuuden kasvussa, ja siksi on tärkeää keskittyä itse laitteiden tai niiden käyttämän verkon suojaamiseen.

4 IoT-verkkojen turvallisuusstrategiat

Tässä luvussa esitellään tutkielmaan valitut IoT-verkkojen turvallisuusstrategiat. Kappaleessa 4.1 tarkastellaan verkkoliikenteen analysointia ja anomalioiden tunnistamista, kappaleessa 4.2 käsitellään autentikointia ja pääsynvalvontaa, ja seuraavissa lohkoketjuteknologiaa sekä reunalaskentaa. Ensimmäiset kaksi ovat yleisiä turvallisuustekniikoita verkkoympäristöissä, mutta niiden soveltaminen IoT-verkkojen kontekstissa vaatii erityistä huomiota. Lohkoketjuteknologia ja reunalaskenta sen sijaan ovat uudempia ja hieman erilaisia lähestymistapoja IoT:n turvallisuuden kannalta, mutta molemmat ovat olleet merkittävästi esillä nykykirjallisuudessa IoT:n turvallisuuteen liittyen.

4.1 Verkkoliikenteen analysointi ja anomalioiden tunnistaminen

Verkkoliikenteen analysoinnilla tarkoitetaan Alqudahin ja Yaseenin mukaan prosessia, jossa verkkokommunikaation kuviot tunnistetaan, kirjataan ja tutkitaan mahdollisten turvallisuusuhkien havaitsemiseksi ja niihin vastaamiseksi, vaikka itse viestit olisivatkin salattuja (Alqudah ja Yaseen 2020). Tähän liittyvät anomaliat, eli poikkeavuudet, jotka ovat epätavallisia mutta huomattavia muutoksia verkossa ja jotka voivat levitä useiden linkkien yli. Anomaliat eivät välttämättä tarkoita pelkästään haitallista liikennettä, vaan ne voivat myös viitata esimerkiksi reitittimen virheelliseen konfigurointiin. Yhtenä anomaliana verkossa voi kuitenkin olla esimerkiksi palvelunestohyökkäysliikenne. (Lakhina, Crovella ja Diot 2004) Anomalioiden tunnistuksen (*Anomaly Detection*) tehtävänä on tunnistaa datasta malleja, jotka eivät vastaa odotettua käyttäytymistä (Doshi, Apthorpe ja Feamster 2018). Anomalioiden tunnistaminen voidaan siis ajatella osaksi verkkoliikenteen analysointimenetelmiä, vaikka kirjallisuudessa näitä termejä saatetaan käyttää hieman päällekkäin.

Verkkoliikenteen anomalioiden tarkastelu on tärkeää, koska ne voivat ruuhkauttaa verkkoa ja kuormittaa reitittimien resursseja tai vaikuttaa loppukäyttäjään (Lakhina, Crovella ja Diot 2004). Näin ollen erityisesti IoT-ympäristössä, jossa laitteiden moninaisuus ja lukumäärä ovat suuret, valppaus verkon epätavallisen liikenteen suhteen voi olla ensiarvoisen tärkeää, sillä se auttaa koko verkon suojaamisessa ja mahdollisten tietoturvaloukkausten ehkäisemi-

sessä tunnistamalla ja estämällä esimerkiksi mahdollisen botnet- tai DDoS-liikenteen.

4.1.1 Haasteet anomalioiden tunnistamisessa IoT-verkkoliikenteessä

Verkkoliikenteen analysointi ja anomalioiden tunnistaminen eivät siis ole luonteeltaan ennaltaehkäiseviä strategioita IoT-verkkojen suojaamiseen. Ne voidaan ymmärtää ennemmänkin reaktiivisina ratkaisuina, jotka vaativat, että uhka on jo verkossa tai että IoT-laitetta käytetään jo osana DDoS-hyökkäystä.

Anomaliapohjaisilla tunkeutumisen havaitsemisjärjestelmillä (*Intrusion Detection Systems, IDS*) esiintyy García-Teodoro ym. (2009) mukaan merkittäviä haasteita, kuten alhainen havaitsemistehokkuus, joka johtuu usein korkeasta väärien hälytysten määrästä. Tämä ongelma liittyy tutkimusten puutteeseen tunkeutumistapahtumien luonteesta ja se edellyttää uusien, tarkkojen prosessointimenetelmien ja parempien verkkojärjestelmien mallinnustapojen kehittämistä. Lisäksi haasteita aiheuttaa alhainen läpäisykyky ja korkeat kustannukset, jotka johtuvat nykyisten laajakaistatekniikoiden suurista datanopeuksista. Muita ongelmia ovat sopivien mittareiden ja arviointimenetelmien puute, järjestelmien puolustuskyvyn heikkous hyökkäyksiltä sekä salatun datan analysoinnin haasteet. (García-Teodoro ym. 2009)

IoT-ympäristössä nämä haasteet voivat korostua. Ongelmaksi voi nousta edelleen laitteiden heterogeenisyys ja suuri määrä, mitkä voivat tehdä verkosta haastavan hallita ja suojata. Tämä voisi tarkoittaa myös väärien hälytysten määrän kasvamista, jos laitteita on monenlaisia monilta eri valmistajilta ja ne eivät ole täysin yhteensopivia. Tämä korostaa siis standardoitujen protokollien ja sääntelyn kehittämistä IoT-verkoille ja -laitteille. Anomalioiden tunnistaminen voi olla kriittistä etenkin, jos IoT-laitteita käytetään osana botnettiä.

4.2 Autentikointi ja pääsynvalvonta

Romanin, Zhoun ja Lopezin mukaan tukimusyhteisössä on todettu, että autentikointi on yksi tärkeimpiä ominaisuuksia IoT:n turvallisuuden parantamiseksi, sillä ilman sitä ei voida varmistaa virtaavan datan luotettavuutta (Roman, Zhou ja Lopez 2013). Tähän liittyy myös valtuutus (*authorization*), joka viittaa pääsynvalvontaan (*access control*), sillä ei ole suotuisaa antaa kaikille samantasoista pääsyä IoT-laitteisiin tai -verkkoon (Roman, Zhou ja Lopez

2013). Autentikoinnin ja pääsynvalvonnan voidaan siis ajatella kulkevan käsi kädessä, kun suunnitellaan turvallista IoT-arkkitehtuuria.

Pääsynvalvonta tarkoittaa Sicari ym. (2015) mukaan sitä, miten lupia resurssien käyttöön jaetaan eri tekijöille IoT-verkoissa. Roman, Zhou ja Lopez (2013) huomauttavat, että on arvioitava sitä, otetaanko pääsynvalvonta käyttöön hajautetusti laitetasolla vai keskitetymmin erillisessä paikassa. Kuten autentikoinnissa, keskitetyssä IoT-arkkitehtuurissa, jossa pääsynvalvonta toteutetaan erillisesti, on helpompi hallita pääsynvalvontalogiikkaa, koska silloin resurssiheikkojen IoT-laitteiden ei tarvitse itse implementoida monimutkaista pääsynvalvontaa. Toisaalta tämä tarkoittaa että pääsynvalvonnan hoitavaan erilliseen entiteettiin on oltava vankka luottamus. (Roman, Zhou ja Lopez 2013)

4.2.1 Haasteet autentikoinnissa ja pääsynvalvonnassa IoT-laitteille

IoT:ssa autentikoinnin ja pääsynhallinnan haasteet liittyvät pääasiassa kahteen keskeiseen kysymykseen: nykyisten pääsynhallintateknologioiden soveltuvuuteen ja uusien, IoT:n erityisvaatimuksiin suunniteltujen mekanismien kehittämiseen. Nykyiset turvallisuusstandardit ja pääsynhallintaratkaisut eivät ole suunniteltu IoT:n kaltaisiin ympäristöihin, joissa laitteet ovat resurssirajoitteisia ja tarve on suuri skaalautuvuudelle, keveydelle ja kattavalle turvallisuudelle. Tämän seurauksena on tarpeen joko mukauttaa olemassa olevia ratkaisuja tai kehittää kokonaan uusia, IoT:n vaatimuksiin vastaavia pääsynhallintatekniikoita. (Ouaddah ym. 2017)

Toisaalta keskustelu keskittyy myös pääsynhallinnan hallintamalliin: onko keskitetty, hajautettu tai hybridi lähestymistapa tehokkain tapa hallita pääsynhallintaa skaalautuvassa IoT-arkkitehtuurissa? Keskittyneessä mallissa turvallisuustehtävät ulkoistetaan palvelimille, mikä helpottaa pääsynhallintapolitiikkojen hallintaa, mutta samalla luo haavoittuvuuksia, kuten yksittäisen vikapisteen ja riippuvuuden yhdestä luotettavasta tahosta. Hajautetussa mallissa turvallisuus ja pääsynhallinta pyritään integroimaan suoraan IoT-laitteisiin, mikä parantaa tietosuojaa ja käyttäjien hallintaa omista laitteistaan, mutta tuo haasteita turvallisuusmekanismien ylläpitoon ja hallintaan, etenkin kun kyseessä ovat resursseiltaan rajalliset laitteet. (Ouaddah ym. 2017)

Näin ollen IoT:n autentikoinnin ja pääsynhallinnan kehittäminen vaatii tasapainon löytämistä näiden kahden lähestymistavan välillä, ottaen huomioon sekä tekniset haasteet että käytännön toteutettavuuden (Ouaddah ym. 2017).

4.3 Lohkoketjuteknologian hyödyntäminen

Khanin ja Salahin mukaan teollisuuden ja tiedeyhteisön ennusteet osoittavat, että lohkoketjuteknologialla (*blockchain*) tulee olemaan merkittävä rooli IoT-laitteiden hallinnassa, valvonnassa ja niiden suojaamisessa (Khan ja Salah 2018). Lohkoketjuteknologian potentiaali IoT:n suojaamisessa piilee sen hajautetussa ja läpinäkyvässä luonteessa. Christidiksen ja Devetsikiotiksen mukaan lohkoketjuteknologia perustuu ideaan hajautetusta tietorakenteesta, joka koostuu toisiinsa linkitetyistä lohkoista (Christidis ja Devetsikiotis 2016). Lohkot sisältävät aikaleimattuja transaktiotietueita ja ovat yhdistetty toisiinsa kryptografisilla hash-tunnuksilla, jotka pohjautuvat aina niitä edeltävän lohkon hash-tunnukseen. Tämä luo teknologian nimensä mukaisesti lohkojen välisen "ketjun". Tässä järjestelmässä verkoston laitteet, eli solmut, tallentavat ja jakavat lohkoketjun, joka koostuu transtaktioista. Nämä transtaktioit vahvistetaan käyttäen turvallisuusavaimia, jotka takaavat, kuka on transtaktion takana. Kun transaktio hyväksytään, se lisätään lohkoketjuun, jonka kaikki solmut voivat tarkistaa. Tämä jatkuva hyväksyntäprosessi rakentaa turvallisen ja avoimen järjestelmän, jossa kaikki tiedot ovat kaikkien solmujen saatavilla ilman, että tarvitaan keskitettyä hallintaa. (Christidis ja Devetsikiotis 2016)

IoT:n kontekstissa lohkoketjuteknologian käyttö tuo mukanaan merkittäviä etuja, jotka vahvistavat laitteiden turvallisuutta ja parantavat niiden hallinnointia. Se tarjoaa ensinnäkin hajautetun tavan varmistaa laitteiden ja niiden välisen kommunikaation aitouden ja turvallisuuden. Tämän ansiosta jokainen laite voi toimia itsenäisesti ilman tarvetta keskitetylle valvonnalle, mikä tekee järjestelmästä läpinäkyvämmän ja turvallisemman. (Khan ja Salah 2018) Tämä on kustannustehokkaampi ratkaisu kuin nykyiset keskitetyt mallit, osittain myös sen takia, että valmistajat voivat sijoittaa laiteohjelmistopäivitysten hash-arvot verkkoon, minkä jälkeen laitteet voivat hakea päivitykset hajautetun tiedostonjakelujärjestelmän kautta. Tällöin valmistajan ei tarvitse jatkuvasti jaella päivitystiedostoja, ja laitteet voivat jopa jakaa päivityksiä keskenään, mikä tekee prosessista tehokkaan ja itsenäisen. (Christidis ja Devetsi-

kiotis 2016) Myös älykkäiden sopimusten (*smart contracts*) avulla lohkoketju mahdollistaa monimutkaisten todentamis- ja valtuutusprosessien yksinkertaistamisen. Nämä sopimukset automatisoivat pääsynhallinnan ja käyttöoikeudet, mikä tekee perinteisiin menetelmiin verrattuna turvallisuudesta vahvemman ja hallinnasta vähemmän monimutkaista. Lisäksi, koska jokaisella IoT-laitteella on oma ainutlaatuinen tunniste ja avainpari lohkoketjussa, perinteisen avainhallinnan tarve poistuu, mikä vähentää turvallisuusriskejä ja yksinkertaistaa laitteiden välisiä turvallisia yhteyksiä. (Khan ja Salah 2018)

4.3.1 Esimerkkejä lohkoketjuteknologian mahdollisuuksista IoT:ssa

Lohkoketjuteknologian integroiminen IoT:iin antaa mielenkiintoisen näkökulman siitä, miten tulevaisuuden digitaaliset ekosysteemit voivat kehittyä ja miltä ne saattavat tulla näyttämään. Teknologian hajautetun luonteen ansiosta IoT:n kyky toimia itsenäisesti voi tuoda hyvinkin kehittyneitä ratkaisuja eri ymäristöihin.

Kirjallisuudessa on esitetty esimerkiksi kotitalouksien energiankulutukseen liittyvää skenaariota, jossa älykodin IoT-laitteet hallinnoivat itse omaa energiankulutustaan kommunikoimalla suoraan toistensa ja energiantoimittajien kanssa, minkä tavoitteena olisi optimoida energian käyttöä ja kustannuksia reaaliajassa. Tämä voisi tarkoittaa älykkäitä sopimuksia, jotka automatisoivat energian ostamisen, myymisen tai vaihdon perustuen reaaliaikaisiin tarpeisiin ja markkinahintoihin. (ks. Afzal ym. 2020; Yang ja Wang 2021)

Toinen käyttökohde, jonka Christidis ja Devetsikiotis (2016) tuovat myös esille, voisi olla esimerkiksi toimitusketjujen hallinnasssa, mikä varmistaisi tuotteiden läpinäkyvyyden ja seurattavuuden toimittajilta kuluttajille. Esimerkiksi ruokateollisuudessa tuotteiden eettinen ja kestävä tuottaminen voitaisiin varmistaa IoT-sensoreilla, jotka seuraavat tuotteiden koko toimituksen ajan tiettyjä parametreja, kuten lämpötilaa ja kosteutta, ja tallentavat havainnot suoraan lohkoketjuun, jolloin loppuasiakas voi nähdä tuotteiden olosuhteet koko toimitusketjun ajalta ja varmistaa niiden tuoreuden (ks. Christidis ja Devetsikiotis 2016).

4.3.2 Lohkoketjun haasteet ja heikkoudet

Kappaleessa 4.3.1 esitetyt ratkaisut kohtaavat omat käytännön haasteensa. Kodin älykäs energiankulutusratkaisu voisi tarkoittaa merkittäviä investointeja ja infrastruktuurin muutoksia verkko-operaattoreiden ja energiantoimittajien näkökulmasta. Toimitusketjuissa saattaisi tulla vastaan skaalautuvuusongelmat, kun laitteiden verkko laajenee. Suuret määrät IoT:n generoimaa dataa uskoisi johtavan transaktioiden viiveisiin ja lisäämään kustannuksia.

Ennen kaikkea jokaisella, sekä uudella ja innovatiivisellä että jo olemassa olevalla lohkoketjuteknologiaa IoT:ssa hyödyntävällä ratkaisulla korostuu tietoturvan ja suojauksen tarve haitallisia toimijoita vastaan. Kodin energiaopitmoinnissa halutaan pitää henkilökohtaiset transaktiot suojassa. Toimitusketjuissa on kriittisen tärkeää, että itse IoT-laitteita ja -sensoreita, jotka lähettävät dataa lohkoketjuun, ei päästäisi manipuloimaan. Lohkoketjun haavoittuvuudet IoT:ssä liittyvät enemmänkin datan eheyteen. Vaikka lohkoketju pystyy takaamaan ketjussa olevan datan muuttumattomuuden, alkuperäisesti vääristynyt data pysyy korruptoituneena lohkoketjussa, mikä voi johtua esimerkiksi laitevaurioista, ympäristövaikutuksista tai vandalismista (Reyna ym. 2018). Lisäksi käyttäjän yksityinen avain (*private key*), jonka käyttäjä itse muodostaa ja säilyttää ja joka toimii identiteetti- ja turvallisuustodisteena, voi altistua hyökkäyksille, jos avaimen tuottamisprosessi ei tuota riittävää satunnaisuutta (Li ym. 2020).

Vaikka lohkoketjuteknologiaan liittyy muitakin turvallisuusaukkoja, suurin osa niistä liittyy ensisijaisesti Bitcoinin kaltaisten kryptovaluuttojen transaktioihin ja varojen siirtoihin, koska tämä on edelleen teknologian laajimmin käytetty sovellusalue (Li ym. 2020).

4.4 Reunalaskennan hyödyntäminen

Reunalaskenta (*Edge computing*) on teknologia, joka mahdollistaa laskennan suorittamisen verkon reunalla. Tässä kontekstissa "reuna"käsittää kaikki laskenta- ja verkkoresurssit, jotka sijaitsevat datalähteiden ja pilvidatakeskusten välillä. Esimerkiksi älypuhelin voi toimia reunana ihmiskehon sensorien ja pilven välillä, ja älykodin keskitin kodin laitteiden ja pilven välillä. Reunalaskennan idea on, että laskenta tapahtuu mahdollisimman lähellä datalähteitä. Reunalaskenta nähdään osittain samankaltaisena kuin sumulaskenta (*fog computing*), mutta

reunalaskenta keskittyy enemmän laitteiden puoleen, kun taas sumulaskenta painottaa enemmän infrastruktuuria. Reunalaskennan odotetaan vaikuttavan yhteiskuntaan yhtä laajasti kuin pilvilaskenta. (Shi ym. 2016)

Reunalaskentaa hyödynnetään IoT:ssa parantamalla datan käsittelyn nopeutta ja tehokkuutta suoraan datan syntypaikalla. Tämä on tärkeää erityisesti tilanteissa, joissa nopea reagointi on välttämätöntä, kuten älyautojen ja terveysseurantalaitteiden kohdalla. Koska IoT-laitteet tuottavat jatkuvasti suuria määriä dataa, reunalaskenta vähentää tarvetta siirtää kaikkea dataa pilvipalveluihin, mikä parantaa sekä viestinnän nopeutta että vähentää verkon kuormitusta. Lisäksi reunalaskenta parantaa tietoturvaa ja yksityisyydensuojaa, koska arkaluonteiset tiedot voidaan käsitellä paikallisesti eikä niitä tarvitse lähettää keskitettyihin pilvipalveluihin. Energiatehokkuuden parantuminen on myös merkittävä hyöty, sillä reunalaskenta mahdollistaa laskentatehtävien siirtämisen pois energiankulutukseltaan suurista pilvipalvelimista, mikä säästää laitteiden akkua ja pidentää niiden käyttöikää. Näiden etujen ansiosta reunalaskennan rooli IoT:ssa korostuu, ja sen odotetaan muovaavan teknologian käyttöä samalla tavalla kuin pilvilaskennan aikaisemmat innovaatiot. (Shi ym. 2016)

Lin ym. (2017) esittelevät reunalaskennan käytännön sovelluksia IoT:ssa, joita ovat muun muassa älykkäät sähköverkot, älyliikenne ja älykaupungit. Älykkäissä sähköverkoissa reunalaskenta mahdollistaa energian tehokkaamman käytön ja varastoinnin, optimoiden energiankulutusta ja -jakelua reaaliaikaisesti. Älyliikenteessä reunalaskenta parantaa ajoneuvojen välistä kommunikaatiota ja datan käsittelyä, mikä tehostaa liikenneturvallisuutta ja -sujuvuutta. Älykaupungeissa reunalaskenta tukee eri alapalveluiden, kuten ympäristönvalvonnan ja jätehuollon datan tehokasta käsittelyä edistäen resurssien optimointia ja palveluiden laatua. Kaikissa näissä sovelluksissa reunalaskenta vähentää viiveitä, parantaa tietoturvaa ja lisää yksityisyyden suojaa, koska dataa käsitellään lähellä sen alkuperää vähentäen näin sen altistumista ulkopuolisille hyökkäyksille. (Lin ym. 2017)

4.4.1 Reunalaskennan haasteet IoT:ssa

Shi ym. (2016) mukaan reunalaskennan heikkoudet liittyvät pääasiassa sen monimutkaisuuteen ja heterogeenisuuteen verrattuna perinteiseen pilvilaskentaan. Ensinnäkin ohjelmoita-

vuus reunalaskennassa kohtaa haasteita, koska reunasolmut voivat olla erilaisia ja niiden suoritusympäristöt vaihtelevat. Tämä tekee sovellusten kehittämisestä vaikeampaa, sillä ohjelmoijan on otettava huomioon laitteiston erilaisuudet ja sopeutettava koodi toimimaan eri alustoilla. Myös nimeäminen reunalaskennassa on haastavaa, koska laitteiden suuri määrä ja niiden liikkuvuus vaativat joustavampia ja dynaamisempia nimeämismenetelmiä kuin perinteisissä verkostoissa. Olemassa olevat nimeämismekanismit, kuten DNS, eivät ole riittävän joustavia palvelemaan dynaamista ja heterogeenistä reunaverkkoa. (Shi ym. 2016)

Lisäksi reunalaskennassa datan abstraktio ja palvelunhallinta ovat monimutkaisia prosesseja, joissa tietojen yhdenmukaistaminen ja palveluiden eristäminen tuovat esiin teknisiä haasteita. Tiedon abstraktioon liittyen on vaikeaa päättää, kuinka paljon raakadataa tulisi suodattaa, mikä voi vaikuttaa palveluiden kykyyn oppia ja tehdä päätöksiä tehokkaasti. Palvelunhallinnassa taas haasteita tuovat sovellusten keskinäinen eristäminen ja järjestelmän luotettavuus, jossa yhden sovelluksen toimintahäiriö ei saisi kaataa koko järjestelmää. (Shi ym. 2016)

Vaikka reunalaskennan hyödyntäminen IoT:ssa on lupaavaa, se näyttäisi vaativan vielä lisätutkimuksia ja kehitystyötä. Haasteiden, kuten laitteiden yhteensopivuuden, nimeämisen ja datan käsittelyn monimutkaisuuden voittaminen edellyttää alan toimijoiden laajaa yhteistyötä ja uusien, yhtenäisten ratkaisujen kehittämistä. Tämä mahdollistaisi reunalaskennan tehokkaamman ja luotettavamman käytön IoT-ympäristöissä.

5 Vertaileva analyysi eri turvallisuusstrategioiden välillä

Kuten aiemmin mainittiin verkkoliikenteen analysointi ja anomalioiden tunnistaminen ovat luonteeltaan enemmänkin reaktiivisia turvallisuusratkaisuja IoT:n suojaamisessa. Kyky tunnistaa poikkeuksia verkossa on kuitenkin arvokasta, sillä se voi estää laajempien turvallisuusongelmien syntymisen. Toisaalta, jos laitteiden data ja toiminta on jo alunperin vääristynyt, menetelmä ei kykene korjaamaan alkuperäistä ongelmaa. Tämä korostaa tarvetta IoT-laitteiden ja -verkon alkuperäisen eheyden säilyttämiseen.

Tähän ratkaisuna voi olla lohkoketjuteknologia, joka tarjoaa mahdollisuuksia nimenomaan datan eheyden varmistamiseksi ja säilyttämiseksi. Hajautetun luonteensa ansiosta lohkoketju mahdollistaa tietojen muuttumattomuuden ja läpinäkyvyyden, mikä voi olla keskeistä IoT:n suojaamiselta esimerkiksi botnettejä vastaan. Lohkoketju voisi myös mahdollistaa laitteiden itsenäisen toiminnan ilman keskitettyä valvontaa sen läpinäkyvän luonteensa vuoksi, mikä lisäisi järjestelmän turvallisuutta ja kustannustehokkuutta, kuten kappaleessa 4.3 on käsitelty. Tämä voisi poistaa osittain tarpeen keskitetylle pääsynvalvontamekanismille, kuten kappaleessa 4.2 esitettiin.

Toisaalta alkuperäisesti vääristyneen datan pysyminen korruptoituneena lohkoketjussa korostaa tarvetta IoT-laitteiden ja -sensorien tarkkaan testaukseen ja valvontaan. Lohkoketjusta voidaan todeta, että se tarjoaa vahvan perustan IoT:n turvallisuuden parantamiselle, mutta sen tehokas hyödyntäminen edellyttää jatkuvaa huomiota datan eheyteen ja laitteiden turvallisuuteen liittyviin haasteisiin.

Mielenkiintoisimman strategian voisi toteuttaa reunalaskennan ja lohkoketjun yhdistäminen. Kuten kappaleessa 4.3.1 todettiin, lohkoketjuteknologian hyödyntämisen ongelmana IoT:ssa on sen resurssivaativuus sekä jo vääristyneen datan korjaaminen. Reunalaskenta mahdollistaa datan käsittelyn suoraan sen syntypaikalla, mikä voisi vähentää tarvetta keskitetyille ratkaisuille lohkoketjudatan validoimisessa. Tämä voisi tehostaa luotettavuutta ja tehokkuutta, jos validointi tapahtuu paikallisesti. Toisaalta, voisiko reunalaskennalla toteuttaa myös autentikoinnin ja laitteiden identiteetin hallinnan?

On selvää, että autentikointi kuitenkin on keskeinen osa turvallista IoT-verkkoa, ja sen voi-

daan ajatella olevan ennaltaehkäisevä lähetymistapa, jolla minimoidaan tietomurtojen riskiä. Tämä yhdistettynä reaktiivisiin tekniikoihin, kuten anomalioiden tunnistamiseen, voi antaa hyvän pohjan suojaukselle sekä proaktiivisella että reaktiivisella tasolla IoT-ympäristöissä. Tehokas autentikointi on myös mahdollista saavuttaa resurssirajoitteisessa ympäristössä, kuten Ye ym. (2014) esittelemässä tutkimuksessa todettiin.

Tarkastellessa jokaista neljää eri suojausstrategiaa ja ottaen huomioon niiden vahvuudet ja heikkoudet voidaan todeta, että kattavan turvallisuusratkaisun kehittäminen IoT:lle vaatii näiden menetelmien yhdistämistä ja tasapainottamista niiden vahvuuksien ja heikkouksien mukaisesti. Jokaisella strategialla on oma roolinsa kokonaisvaltaisessa turvallisuusjärjestelmässä. Vaikka verkkoliikenteen analysointi ja anomalioiden tunnistaminen ovat luonteeltaan reaktiivisia, ne vaikuttavat olevan välttämättömiä nopeisiin uhkiin reagoimisessa ja mahdollisten vahinkojen rajoittamisessa. Lohkoketjuteknologia voi tarjota proaktiivisen lähestymistavan, joka varmistaa datan eheyden ja läpinäkyvyyden, mikä vähentää siten tarvetta jälkikäteisiin korjauksiin ja lisää järjestelmän luotettavuutta. Sen hajautettu ja läpinäkyvä luonne voivat poistaa osittain tarpeen erilliselle keskitetylle pääsynvalvontamekanismille. Autentikointi puolestaan muodostaa ensimmäisen puolustuslinjan, joka estää luvattomien laitteiden pääsyn verkkoon ja minimoisi siten mahdollisten hyökkäysten riskiä alusta alkaen. Kaikilla näillä tulee kuitenkin eteen yhteinen ongelma: IoT-laitteiden resurssirajoitteet.

Resurssirajoitteen voisi ratkaista osittain reunalaskennalla, jossa salaustoimenpiteet tai muut tarvittavat datan käsittelyt voitaisiin toteuttaa. Laitteiden heterogeenisyys on myös yksi keskeinen tekijä jokaisessa strategiassa. Voitaisiinko reunalaskentaa suorittaa esimerkiksi vain resursseiltaan vahvimmissa IoT-laitteissa, jotta heikommat laitteet voivat keskittyä niiden spesifiin tehtävään?

Parhaan lopputuloksen saavuttamiseksi on siis mietittävä näitä kaikkia strategioita ja niiden jonkinlaista, tasapainoitettua hybridiratkaisua. Verkkoliikenteen analysointi ja autentikointi ovat kulmakivinä turvallisen IoT-verkon luomiselle, mutta niiden toimivuuden ja datan eheyden varmistamisessa on syytä hyödyntää lohkoketjuteknologiaa, joka taas hyötyisi reunalaskennasta resurssien käytön minimoimiseksi.

6 Yhteenveto

Tässä tutkielmassa on tarkasteltu Internet of Things (*IoT*) -teknologian turvallisuushaasteita ja erilaisia strategioita näiden haasteiden voittamiseksi. Tutkielma osoittaa, että IoT:n laajamittainen käyttöönotto tuo mukanaan monimutkaisia turvallisuusongelmia, jotka edellyttävät kattavia ja monikerroksisia turvallisuusstrategioita.

Erityisesti on keskitytty neljään keskeiseen turvallisuusstrategiaan: verkkoliikenteen analysointiin ja anomalioiden tunnistamiseen, autentikointiin ja pääsynvalvontaan, lohkoketjuteknologiaan sekä reunalaskentaan. Näistä strategioista jokaisella on omat vahvuutensa ja heikkoutensa, mutta vain yhdessä ne voivat tarjota vahvan perustan IoT-ympäristöjen suojelemiseksi. Verkkoliikenteen analysointi auttaa tunnistamaan potentiaaliset uhkat reaaliajassa, kun taas autentikointi ja pääsynvalvonta toimivat ensilinjan puolustuksena estäen luvattomat pääsyt ja datavuodot. Lohkoketjuteknologia tarjoaa tietojen muuttumattomuuden ja läpinäkyvyyden, mikä on erityisen arvokasta datan eheyden varmistamisessa, sekä voi poistaa osittain tarpeen keskitetylle pääsynvalvontamekanismille IoT-verkoissa. Reunalaskenta puolestaan mahdollistaa datan käsittelyn lähellä sen syntypaikkaa, mikä nopeuttaa prosesseja ja vähentää verkon kuormitusta ratkaisten osittain IoT-laitteiden resurssirajoitteen ongelman.

Tutkielma osoittaa, että yksittäisen turvallisuusstrategian sijaan parhaat tulokset saadaan yhdistämällä näitä strategioita. Tällainen monikerroksinen lähestymistapa mahdollistaa laajemman suojan ja vähentää yksittäisten strategioiden heikkouksien vaikutusta.

Tutkielman heikkouksina voidaan mainita, että käytännön sovellusten ja ehdotettujen ratkaisujen välillä on vielä tutkimus- ja kehityskuilu, mikä voi vaikuttaa tulosten soveltuvuuteen todellisissa IoT-ympäristöissä. Myöskään vertailevassa analyysissä ei suoritettu empiiristä tutkimusta, vaan tarkastelu perustui kirjallisuuslähteisiin ja teoreettisiin pohdintoihin. Käytännön tasolla myös IoT-laitteiden heterogeenisuuden ja jatkuvasti muuttuvien teknologioiden vuoksi voi olla haastavaa ylläpitää turvallisuusratkaisujen ajantasaisuutta ja tehokkuutta.

Jatkotutkimuksena olisi syytä tutkia tarkemmin, kuinka näitä eri turvallisuusstrategioita voidaan integroida yhteen saumattomasti ja tehokkaasti. On myös tarpeen kehittää uusia metodeja, jotka voivat automaattisesti mukautua ja reagoida IoT-ympäristöjen nopeisiin muutok-

siin turvallisuusuhkien hallitsemiseksi. Lisäksi on tärkeää tutkia tarkemmin reunalaskennan ja lohkoketjuteknologian yhdistämisen potentiaalia ja kehittää kestävämpiä ratkaisuja, jotka voisivat minimoida energiankulutusta ja parantaa datan käsittelyn tehokkuutta.

Lähteet

Abu Rajab, Moheeb, Jay Zarfoss, Fabian Monrose ja Andreas Terzis. 2006. “A multifaceted approach to understanding the botnet phenomenon”. Teoksessa *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement,* 41–52.

Afzal, Muhammad, Qi Huang, Waqas Amin, Khalid Umer, Asif Raza ja Muhammad Naeem. 2020. “Blockchain enabled distributed demand side management in community energy system with smart homes”. Cited by: 113; All Open Access, Gold Open Access, *IEEE Access* 8:37428–37439. https://doi.org/10.1109/ACCESS.2020.2975233. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081121656&doi=10.1109%2fACCESS.2020.2975233&partnerID=40&md5=09a025a952fa233f88e44e1870d6ee0a.

Alaba, Fadele Ayotunde, Mazliza Othman, Ibrahim Abaker Targio Hashem ja Faiz Alotaibi. 2017. “Internet of Things security: A survey”. *Journal of Network and Computer Applications* 88:10–28.

Alqudah, Nour ja Qussai Yaseen. 2020. “Machine Learning for Traffic Analysis: A Review”. The 11th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40) / Affiliated Workshops, *Procedia Computer Science* 170:911–916. ISSN: 1877-0509. https://doi.org/https://doi.org/10.1016/j.procs.2020.03.111. https://www.sciencedirect.com/science/article/pii/S1877050920305494.

Atzori, Luigi, Antonio Iera ja Giacomo Morabito. 2010. “The Internet of Things: A survey”. Cited by: 11081, *Computer Networks* 54 (15): 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010. https://www.scopus.com/inward/record.uri?eid=2-s2.0-77956877124&doi=10.1016%2fj.comnet.2010.05.010&partnerID=40&md5=14b4f3bf4d13ee412acf573a91a817de.

Butun, Ismail, Patrik Österberg ja Houbing Song. 2019. “Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures”. *IEEE Communications Surveys & Tutorials* 22 (1): 616–644.

Chaabouni, Nadia, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac ja Parvez Faruki. 2019. “Network Intrusion Detection for IoT Security Based on Learning Techniques”. Cited by: 523, *IEEE Communications Surveys and Tutorials* 21 (3): 2671–2701. https://doi.org/10.1109/COMST.2019.2896380. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071375386&doi=10.1109%2fCOMST.2019.2896380&partnerID=40&md5=e9ea7cfb11ea97f02f5eac0314769a65.

Christidis, Konstantinos ja Michael Devetsikiotis. 2016. “Blockchains and Smart Contracts for the Internet of Things”. Cited by: 2947; All Open Access, Gold Open Access, *IEEE Access* 4:2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84979828304&doi=10.1109%2fACCESS.2016.2566339&partnerID=40&md5=6e954454a54dc6453ba8b670d4f6d41e.

Doshi, Rohan, Noah Apthorpe ja Nick Feamster. 2018. “Machine learning DDoS detection for consumer internet of things devices”, 29–35. Cited by: 492; All Open Access, Bronze Open Access, Green Open Access. https://doi.org/10.1109/SPW.2018.00013. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85052194137&doi=10.1109%2fSPW.2018.00013&partnerID=40&md5=be036fa134b7cf21034b73fbb0567e23.

García-Teodoro, P., J. Díaz-Verdejo, G. Maciá-Fernández ja E. Vázquez. 2009. “Anomaly-based network intrusion detection: Techniques, systems and challenges”. Cited by: 1305, *Computers and Security* 28 (1-2): 18–28. https://doi.org/10.1016/j.cose.2008.08.003. https://www.scopus.com/inward/record.uri?eid=2-s2.0-57849130705&doi=10.1016%2fj.cose.2008.08.003&partnerID=40&md5=2dfaec9d30db1e45b36bb8d578429fcb.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic ja Marimuthu Palaniswami. 2013. “Internet of Things (IoT): A vision, architectural elements, and future directions”. Cited by: 8618; All Open Access, Green Open Access, *Future Generation Computer Systems* 29 (7): 1645–1660. https://doi.org/10.1016/j.future.2013.01.010. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84876943063&doi=10.1016%2fj.future.2013.01.010&partnerID=40&md5=b9f84477e4bfc7ed42bf27de7ee14537.

Islam, S.M. Riazul, Daehan Kwak, Md. Humaun Kabir, Mahmud Hossain ja Kyung-Sup Kwak. 2015. “The internet of things for health care: A comprehensive survey”. Cited by: 2078; All Open Access, Gold Open Access, *IEEE Access* 3:678–708. https://doi.org/10.1109/ACCESS.2015.2437951. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84946921719&doi=10.1109%2fACCESS.2015.2437951&partnerID=40&md5=85e7f115a480c904319b4bab77795dd9.

Khan, Minhaj Ahmad ja Khaled Salah. 2018. “IoT security: Review, blockchain solutions, and open challenges”. Cited by: 1728, *Future Generation Computer Systems* 82:395–411. https://doi.org/10.1016/j.future.2017.11.022. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85035321551&doi=10.1016%2fj.future.2017.11.022&partnerID=40&md5=2519e8016e9b2f360ee4fecfafc5daba.

Lakhina, Anukool, Mark Crovella ja Christophe Diot. 2004. “Diagnosing network-wide traffic anomalies”, 34:219–230. 4. Cited by: 677. https://doi.org/10.1145/1030194.1015492. https://www.scopus.com/inward/record.uri?eid=2-s2.0-21844451952&doi=10.1145%2f1030194.1015492&partnerID=40&md5=1c57cee7aa6632c707c1562f626331a2.

Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo ja Qiaoyan Wen. 2020. “A survey on the security of blockchain systems”. Cited by: 882; All Open Access, Green Open Access, *Future Generation Computer Systems* 107:841–853. https://doi.org/10.1016/j.future.2017.08.020. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85029448653&doi=10.1016%2fj.future.2017.08.020&partnerID=40&md5=4e2c01f565dc53e37b106f1344da2b9e.

Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang ja Wei Zhao. 2017. “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications”. Cited by: 1977; All Open Access, Bronze Open Access, *IEEE Internet of Things Journal* 4 (5): 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85026378512&doi=10.1109%2fJIOT.2017.2683200&partnerID=40&md5=b923a2cb9171a7da22e0ab1452d7615d.

Mahjabin, Tasnuva, Yang Xiao, Guang Sun ja Wangdong Jiang. 2017. “A survey of distributed denial-of-service attack, prevention, and mitigation techniques”. Cited by: 205; All Open Access, Gold Open Access, *International Journal of Distributed Sensor Networks* 13 (12). https://doi.org/10.1177/1550147717741463. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85039848492&doi=10.1177%2f1550147717741463&partnerID=40&md5=ad4856fca05c5eb03b11e014985b594e.

Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini ja Imrich Chlamtac. 2012. “Internet of things: Vision, applications and research challenges”. Cited by: 2772; All Open Access, Green Open Access, *Ad Hoc Networks* 10 (7): 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84861997111&doi=10.1016%2fj.adhoc.2012.02.016&partnerID=40&md5=da7c2449c16b65f4df13c44a53973a2f.

Mirkovic, Jelena ja Peter Reiher. 2004. “A taxonomy of DDoS attack and DDoS defense mechanisms”. *ACM SIGCOMM Computer Communication Review* 34 (2): 39–53.

Mosenia, Arsalan ja Niraj K. Jha. 2017. “A comprehensive study of security of internet-of-things”. Cited by: 468; All Open Access, Bronze Open Access, *IEEE Transactions on Emerging Topics in Computing* 5 (4): 586–602. https://doi.org/10.1109/TETC.2016.2606384. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85021191411&doi=10.1109%2fTETC.2016.2606384&partnerID=40&md5=dda6543ddc4da7fdb33497787b9348d6.

Neshenko, Nataliia, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum ja Nasir Ghani. 2019. “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations”. *IEEE Communications Surveys & Tutorials* 21 (3): 2702–2733.

Nokia Corporation. 2023. “Nokia Threat Intelligence Report finds malicious IoT botnet activity has sharply increased”. Viitattu: 2024-04-24, kesäkuu. https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/.

Ouaddah, Aafaf, Hajar Mousannif, Anas Abou Elkalam ja Abdellah Ait Ouahman. 2017. “Access control in the Internet of Things: Big challenges and new opportunities”. Cited by: 346, *Computer Networks* 112:237–262. https://doi.org/10.1016/j.comnet.2016.11.007. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84998813174&doi=10.1016%2fj.comnet.2016.11.007&partnerID=40&md5=cc44fd02787a04c8d0a428bbc823b270.

Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler ja Manuel Díaz. 2018. “On blockchain and its integration with IoT. Challenges and opportunities”. Cited by: 1269; All Open Access, Hybrid Gold Open Access, *Future Generation Computer Systems* 88:173–190. https://doi.org/10.1016/j.future.2018.05.046. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048498829&doi=10.1016%2fj.future.2018.05.046&partnerID=40&md5=833d32e08e0077a7156041d4ed88e04f.

Roman, Rodrigo, Jianying Zhou ja Javier Lopez. 2013. “On the features and challenges of security and privacy in distributed internet of things”. Cited by: 944, *Computer Networks* 57 (10): 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84879225866&doi=10.1016%2fj.comnet.2012.12.018&partnerID=40&md5=e9aa4afb7a40923b86ee7e0788743c94.

Salim, Mikail Mohammed, Shailendra Rathore ja Jong Hyuk Park. 2020. “Distributed denial of service attacks and its defenses in IoT: a survey”. *The Journal of Supercomputing* 76:5320–5363.

Sharma, Rahul, Nitin Pandey ja Sunil Kumar Khatri. 2017. “Analysis of IoT security at network layer”. Teoksessa *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO),* 585–590. IEEE.

Shi, Weisong, Jie Cao, Quan Zhang, Youhuizi Li ja Lanyu Xu. 2016. “Edge Computing: Vision and Challenges”. Cited by: 5219, *IEEE Internet of Things Journal* 3 (5): 637–646. https://doi.org/10.1109/JIOT.2016.2579198. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84987842183&doi=10.1109%2fJIOT.2016.2579198&partnerID=40&md5=a975bcadfcbc0402da6444a53205ecde.

Sicari, S., A. Rizzardi, L.A. Grieco ja A. Coen-Porisini. 2015. “Security, privacy and trust in Internet of things: The road ahead”. Cited by: 1410, *Computer Networks* 76:146–164. https://doi.org/10.1016/j.comnet.2014.11.008. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84919372488&doi=10.1016%2fj.comnet.2014.11.008&partnerID=40&md5=0689622723f21be160a42d9b32c189af.

Smith, Gary. 2024. “DDoS Statistics”. Viitattu: 2024-04-24, huhtikuu. https://www.stationx.net/ddos-statistics/.

Statista. 2024. “IoT Connected Devices Worldwide”. Viitattu: 2024-04-24, huhtikuu. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Vishwakarma, Ruchi ja Ankit Kumar Jain. 2020. “A survey of DDoS attacking techniques and defence mechanisms in the IoT network”. *Telecommunication systems* 73 (1): 3–25.

Yang, Qing ja Hao Wang. 2021. “Privacy-Preserving Transactive Energy Management for IoT-Aided Smart Homes via Blockchain”. Cited by: 84; All Open Access, Green Open Access, *IEEE Internet of Things Journal* 8 (14): 11463–11475. https://doi.org/10.1109/JIOT.2021.3051323. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099592613&doi=10.1109%2fJIOT.2021.3051323&partnerID=40&md5=348590416d32a173e13fd71f1338251b.

Ye, Ning, Yan Zhu, Ru-Chuan Wang, Reza Malekian ja Qiao-Min Lin. 2014. “An efficient authentication and access control scheme for perception layer of internet of things”. Cited by: 174; All Open Access, Green Open Access, *Applied Mathematics and Information Sciences* 8 (4): 1617–1624. https://doi.org/10.12785/amis/080416. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84894059526&doi=10.12785%2famis%2f080416&partnerID=40&md5=54d7fcfaafcdc22628584df5ebd34097.

Zargar, Saman Taghavi, James Joshi ja David Tipper. 2013. “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks”. Cited by: 961; All Open Access, Green Open Access, *IEEE Communications Surveys and Tutorials* 15 (4): 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84888391622&doi=10.1109%2fSURV.2013.031413.00127&partnerID=40&md5=8dceebd8b85985172fccb236c366e10b.