IoT-järjestelmien kyberuhat älykaupungeissa

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Helmikuu 2025
Jenni Alarakkola

TURUN YLIOPISTO
Tietotekniikan laitos

Jenni Alarakkola: IoT-järjestelmien kyberuhat älykaupungeissa

TkK-tutkielma, 22 s.
Tietotekniikka
Helmikuu 2025

Älykaupungit hyödyntävät IoT-järjestelmiä tiedonkeruuseen ja palveluiden kehittämiseen. Jatkuva tiedonkeruu mahdollistaa palveluiden parantamisen, mutta samalla se altistaa kaupunkien järjestelmät kyberturvallisuusuhille. Tämä tutkielma on kirjallisuuskatsaus älykaupunkien IoT-järjestelmiin liittyvistä kyberturvallisuusriskeistä sekä keinoista haavoittuvuuksien tunnistamiseen ja ehkäisemiseen. Katsaus perustuu viime vuosina julkaistuihin tieteellisiin tutkimuksiin, jotka käsittelevät IoT-järjestelmien turvallisuutta ja älykaupunkien kyberturvallisuusratkaisuja.
Älykaupunkien turvallisuus edellyttää monitasoista lähestymistapaa, jossa yhdistyvät teknologiset ratkaisut, lainsäädäntö ja asukkaiden tietoisuuden lisääminen. Tehokas haavoittuvuuksien hallinta edistää kaupunkien kestävää kehitystä. Älykaupunkien on panostettava vahvasti kyberturvallisuuteen, jotta asukkaiden tiedot ja kriittiset infrastruktuurit voidaan suojata.

Asiasanat: älykaupunki, riskienhallinta, kyberturvallisuus, IoT, esineiden internet, haavoittuvuudet

Sisällys

Kuvat

Taulukot

Termistö

4IR The Fourth Industrial Revolution, teollisuus 4.0

AI Artificial intelligence, tekoäly

DDoS A distributed denial-of-service attack, hajautettu palvelunestohyökkäys

DNS Domain Name System, nimipalvelin

DoS denial-of-service attack, palvelunestohyökkäys

GPS Global Positioning System, satelliittipaikannusjärjestelmä

HTTP Hypertext Transfer Protocol, HTTP-protokolla

ICT Information and communications technology, Informaatiotekniikka

IoT Internet of Things, Esineiden internet

LPWAN Low-Power Wide Area Network, LPWAN verkkoteknologia

M2M Machine-to-Machine, langaton verkkotekniikka

MAC Media Access Control, verkkolaitteen yksilöivä osoite

MITM Man-in-the-middle attack, väliintulohyökkäys

MQTT Message Queuing Telemetry Transport, MQTT-protokolla

NFC Near-field communication, lähitunnistusteknologia

OSI Open Systems Interconnection model, OSI-malli

OWASP Open Worldwide Application Security Project, OWASP-järjestö

PAN Personal Area Network, henkilökohtainen verkko, likiverkko

RFID Radio-frequency identification, radiotaajuinen etätunnistus

SSL/TLS Secure Sockets Layer / Transport Layer Security, SSL- ja TLS-salausprotokolla

URL Uniform Resource Locator, verkko-osoite

WLAN Wireless local area network, langaton lähiverkko

1 Johdanto

Kaupungistuminen on pitkään jatkunut kiihtyvä globaali ilmiö, sillä yhä useampi ihminen valitsee asuinpaikakseen kaupungin. Amerikkalaisen organisaation, Population Reference Bureaun tutkimuksen [1] mukaan vuonna 2023 57 % maailman väestöstä asui kaupungeissa, ja vuoteen 2050 mennessä määrän odotetaan olevan jopa 70 %. Väestönkasvu lisää painetta kaupunkien palveluille ja infrastruktuurille samalla, kun teknologian kehitys avaa uusia mahdollisuuksia resurssien tehokkaaseen hyödyntämiseen ja kaupunkien kehittämiseen.

Älykaupunki on tehokkaasti johdettu ja asukkaiden tarpeisiin keskittyvä kokonaisuus, jossa erilaiset teknologiat, tekoäly (engl. *Artificial Intelligence*, AI), dataanalytiikka ja esineiden internet (engl. *Internet of Things*, IoT) auttavat parantamaan palveluita ja tekemään kaupungista turvallisemman [2]. Älykaupungit houkuttelevat niin asukkaita kuin yrityksiäkin, sillä teknologiset ratkaisut tarjoavat tehokkaita palveluita, kuten älykkään liikenteen ja hallinnon.

Vaikka älykaupunki on suhteellisen uusi käsite, sen juuret ulottuvat kaupunkikehityksen ja teknologian integroimisen varhaisiin vaiheisiin. Jo 1960- ja 1970-luvuilla pyrittiin käyttämään tietokoneita ja dataa kaupunkien suunnittelussa, mikä loi perustan nykyisille älykaupungeille. 1980- ja 1990-luvuilla tietokoneiden ja internetin yleistyminen mahdollisti datapohjaisen kaupunkisuunnittelun ja -hallinnon kehittämisen. Tietojärjestelmiä, tietoverkkotekniikkaa ja telekommunikaatiojärjestelmiä

alettiin hyödyntää kaupunkipalveluissa. Lopulta 2000-luvulla painopiste siirtyi digitaalisiin palveluihin, sähköiseen hallintoon ja verkkopalvelujen kehittämiseen.

Älykaupungit alkoivat saada enemmän huomiota 2000-luvun lopulla, jolloin niitä alettiin kehittämään eri puolilla maailmaa. [3] Älykaupunkien toteutus on kuvattu useissa eri malleissa, kuten Euroopan komission rahoittamassa ”The Smart Cities and Communities lighthouse projects” -ohjelmassa. Ohjelmaan kuuluu yhteensä 99 projektia, joiden tavoitteena on edistää älykaupunkien kehittämistä Euroopassa ja toimia esimerkkinä muille kaupungeille maailmalla. [4]

Älykaupunki hyödyntää dataa, sensoriteknologiaa ja analytiikkaa niin päätöksenteossa kuin kaupungin infrastruktuurin ja julkisten palveluiden kehittämisessä. Älykaupungin perusta ovat sen asukkaat, joiden tietoja hyödyntämällä kaupungit voivat parantaa palvelujaan. Sen vuoksi tietojen keräämisessä, tallentamisessa ja käsittelyssä on tärkeää huomioida IoT-järjestelmien haavoittuvuudet.

Tässä tutkielmassa tarkastellaan IoT-järjestelmiin pohjautuvien älykaupunkien kyberturvallisuusriskejä, haavoittuvuuksien tunnistamista ja sitä, kuinka näitä haavoittuvuuksia voidaan ehkäistä. Tavoitteena on selvittää, miten jatkuva tiedonkeruu, joka on yhä yleisempää älykaupunkien ympäristössä, vaikuttaa niiden järjestelmien turvallisuuteen, sekä millaisia toimenpiteitä voidaan toteuttaa haavoittuvuuksien minimoimiseksi. Tutkielmassa pyritään vastaamaan seuraavaan tutkimuskysymykseen:

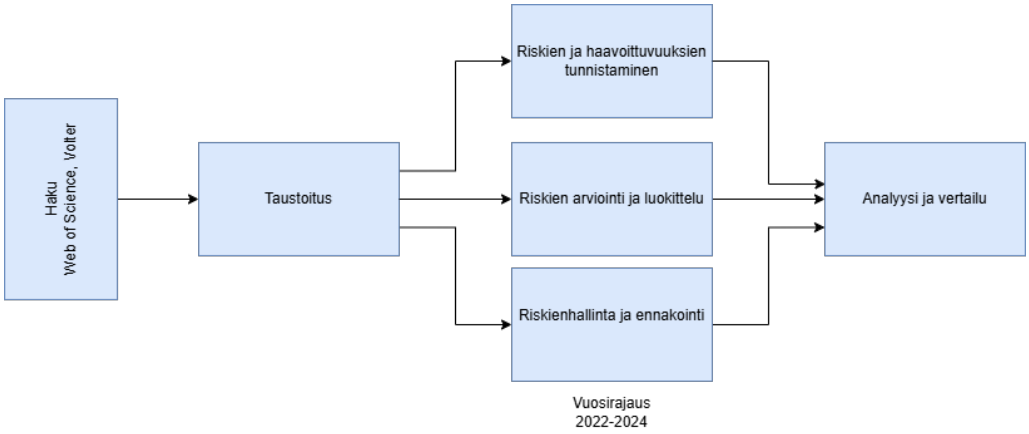
TK1 Miten älykaupunkien IoT-järjestelmien haavoittuvuuksia voidaan ehkäistä?

Tämän lisäksi tarkastellaan, kuinka IoT-järjestelmiin kohdistuneita hyökkäyksiä ja haavoittuvuuksia voidaan jälkikäteen korjata.

Tutkielma on toteutettu kirjallisuuskatsauksena tieteellisten lähteiden pohjalta. Aineisto on kerätty pääasiassa Web of Science -tietokannasta käyttäen tutkimuksen aiheeseen liittyviä hakulausekkeita. Hakulausekkeina on käytetty *"IoT"AND ("security"AND ("risk*"OR "threat*")) AND "identification"* sekä *"smart ci-*

ty"("security"AND ("risk"OR "threat*")) AND "management"*, ja ne on valittu siten, että ne kattavat tutkimuksen kannalta olennaiset avainsanat.

Aineistonhaku on rajattu ajanjaksolle 2022-2024, keskittyen kyberhaavoittuvuuksien tunnistamiseen, riskien arviointiin ja riskienhallintaan. Näiltä osa-alueilta on pyritty löytämään tuoreimpia tutkimuksia aiheesta. Vaikka aineisto on rajattu tälle aikavälille, tutkimuksia löytyi myös aikaisemmilta vuosilta, mikä viittaa siihen, että kyseistä aihetta on aktiivisesti tutkittu jo pidemmän aikaa.



Kuva 1.1: Hakumenetelmä

Luvussa 2 käsitellään älykaupungin rakennetta, IoT-järjestelmän arkkitehtuuria ja siihen liittyviä teknologioita. Tämä luku luo pohjan myöhemmille luvuille, jotta niiden sisältö on helpommin ymmärrettävissä. Luvussa 3 esitellään tutkimusaineiston tulokset, vertaillaan IoT-järjestelmän riskejä ja pyritään näin vastaamaan tutkimuskysymykseen. Luvussa 4 pohditaan työn aikana tehtyjä havaintoja. Luvun 5 yhteenveto tuo esiin keskeisimmät tulokset ja tiivistää tärkeimmät havainnot.

2 Älykaupungin määritelmä

Kaupunkien kasvaessa myös älykkäiden kaupunkiratkaisujen käyttö lisääntyy merkittävästi. IoT-laitteiden määrä kasvaa huimaa vauhtia, sillä teknologian hyödyntäminen kaupunkien hallinnossa on yleistynyt maailmanlaajuisesti [5].

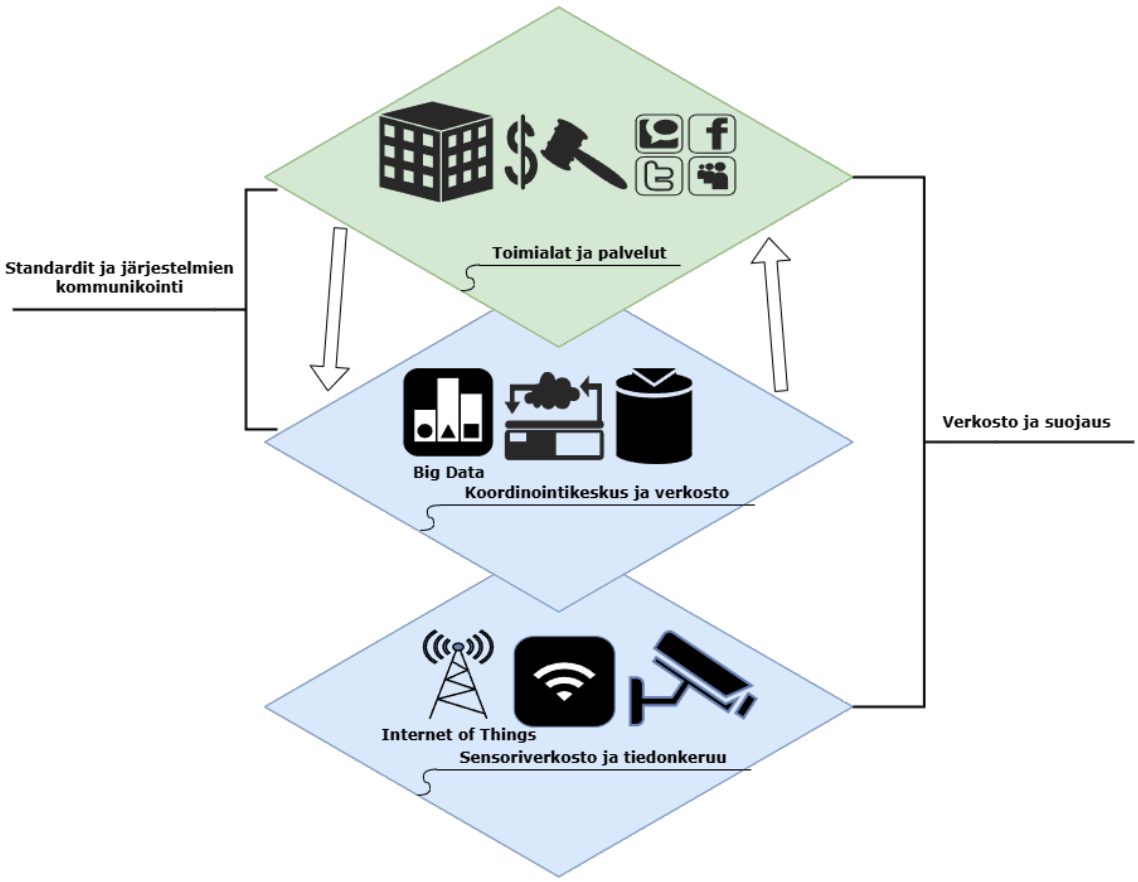
On arvioitu, että vuoteen 2025 mennessä niitä on maailmanlaajuisesti yli 20 miljardia, minkä jälkeen määrän ennustetaan lähes kaksinkertaistuvan vuoteen 2030 mennessä. [6] Tässä luvussa tarkastellaan älykaupungin rakennetta sekä sitä, kuinka älykaupungit voivat kerätä dataa hyödyntämällä IoT-laitteita ja sensoriteknologiaa. Luvun lopussa käsitellään myös IoT-järjestelmien haavoittuvuuksia kyberuhkien näkökulmasta.

2.1 Älykaupungin rakenne

Älykaupunki on laaja käsite, joka kattaa moninaisia kaupunkien kehittämishankkeita. Se toimii kattoterminä erilaisille hankkeille, joissa teknologian ja datan avulla pyritään tehostamaan kaupunkien toimintoja sekä parantamaan asukkaiden elämänlaatua. Älykaupunkien kehityksessä on suuria eroja eri valtioiden välillä, sillä niiden kehittäminen liittyy moniin eri aloihin, kuten infrastruktuuriin ja yhteiskuntasuunnitteluun. Hankkeet voivat vaihdella riippuen niiden tavoitteista, toteutustavoista ja kaupungin koosta. [7]

Älykaupunkien kehittämiseen on esitetty useita malleja, mutta niissä on havaittavissa yhteisiä piirteitä, jotka tekevät kaupungista älykkään. Kuvassa 2.1 esitetään

yksinkertaistettu malli perustuen lähteisiin [2], [3] ja [7]. Se jakaa älykaupungin komponentit kolmeen tasoon.



Kuva 2.1: Älykaupungin rakenne

Alin kerros muodostuu laajoista sensoriverkostoista, jotka kattavat koko kaupungin. Näihin verkostoihin on kytketty lukuisia erilaisia laitteita, kuten kamerat, liikennesensorit ja muut IoT-laitteet. Nämä laitteet keräävät jatkuvasti tietoa ympäristöstä, liikenteestä, ilmanlaadusta, energiankulutuksesta ja ihmisten liikkumisesta [8].

Kerätty data toimii pohjana muille kerroksille, ja se analysoidaan keskimmäisessä tiedonkäsittelykerroksessa. Tähän kerrokseen kuuluvat tiedonhallintajärjestelmät ja datavarastot massadatalle (engl. *big data*). Data on peräisin useista lähteistä, kuten IoT-laitteiden sensoreista ja sosiaalisen median alustoilta. Analysoinnin avulla

voidaan tunnistaa erilaisia suuntauksia ja poikkeamia, jotka ovat hyödyllisiä päätöksenteossa. Vaikka suuria datamääriä hyödyntämällä voidaan tehdä merkittäviä parannuksia monilla aloilla, keskitetty datanhallinta voi johtaa yksityisyyden suojan heikkenemiseen. [5]

Analyysin tuloksia hyödynnetään ylimmässä kerroksessa, joka kattaa kaupungin asukkaiden, yritysten ja hallinnon älykkäät palvelut. Älykaupunkien kehittämisessä keskeistä on älykäs hallinto, jossa digitaaliset teknologiat mahdollistavat tehokkaamman ja läpinäkyvämmän päätöksenteon sekä palveluiden tuottamisen kaupunkilaisille. Kaupunki voi käyttää esimerkiksi sensoreita keräämään tietoa liikenteestä liikennevalojen optimoimiseen, tai dataa analysoimaan ja parantamaan palveluiden käyttöä. Kansalaisille voidaan myös tarjota mahdollisuus osallistua päätöksentekoon verkossa. [3] Suurin osa näistä osa-alueista voidaan toteuttaa itsenäisinä yksikköinä, jolloin kaupunki voidaan muuttaa vaiheittain älykkääksi.

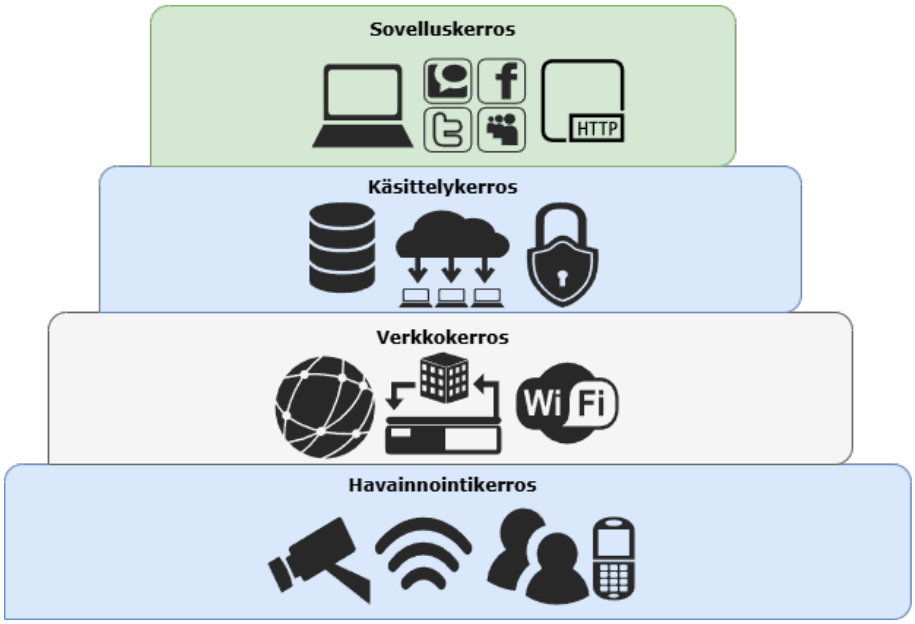
Älykäs hallinto edistää demokraattisten prosessien ja avoimuuden parantamista digitaalisella aikakaudella. Sen suurin haaste on hankkia oikeaa tietoa ja pitää se turvassa. Eri tahot, kuten kansalaiset, yritykset ja viranomaiset, osallistuvat yhdessä yhteisten päätösten tekemiseen. Tavoitteena on luoda kestävä yhteiskunta, jossa tiedolla ja teknologialla on suuri merkitys.

2.2 IoT-järjestelmä ja sensorit

Älykkäät kaupunkipalvelut perustuvat neljännen teollisen vallankumouksen (4IR) teknologioihin, joihin kuuluvat IoT, data-analytiikka, pilvilaskenta, AI ja koneoppiminen. Automaation ja tehokkuuden ansiosta kaupungit toimivat sujuvammin ja tarjoavat asukkailleen parempia palveluja. [9] Älykaupungit hyödyntävät tyypillisesti informaatio- ja viestintäteknologioita (ICT) tiedon jakamiseen sekä datan keräämiseen monista lähteistä, kuten sensoreista, verkkolaitteista, tai muista ulkoisista lähteistä. Pilvipalvelut tarjoavat joustavan ympäristön suurten datamäärien hal-

linnalle ja analysoinnille. Data-ohjatut mallit, jotka hyödyntävät massadataa, ovat keskeisiä älykaupunkien kasvun haasteissa. Näiden mallien avulla ne voivat tarjota personoituja palveluja sekä ennakoida ja ehkäistä kyberuhkia.

4IR:n myötä kehittyneet teknologiat ovat mahdollistaneet älykaupunkien, monimuotoisten kokonaisuuksien, syntymisen. IoT-arkkitehtuurit luovat perustan älykaupunkien teknologioiden integroimiselle. IoT-arkkitehtuurilla tarkoitetaan sitä, miten erilaiset laitteet ja järjestelmät kommunikoivat keskenään. [10, s. 31] Ne perustuvat usein OSI-mallin yksinkertaistettuun versioon, jota kuva 2.2 esittää. Tässä mallissa IoT-kehys on jaettu neljään kerrokseen: Sovelluskerros, käsittelykerros, verkkokerros ja havainnointikerros.



Kuva 2.2: IoT-arkkitehtuurin OSI-malli

Sovelluskerros vastaa käyttäjän vuorovaikutuksesta järjestelmän kanssa, kun taas tiedonsiirto ja viestintä toimivat verkkoprotokollien kautta. Nimipalvelin (engl. *Domain Name System*, DNS) on Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia numerollisiksi IP-osoitteiksi, joita laitteet tarvitsevat verkkoon yhdistämiseksi. HTTP-protokolla on jo pitkään toiminut internetin kautta välittyvässä tiedonsiirrossa. Se toimii perustana verkkopalveluille, mutta ei ole aina optimaali-

nen ratkaisu IoT-sovelluksiin, jotka vaativat usein kevyempiä ja tehokkaampia ratkaisuja. MQTT-protokolla on kevyt ja tehokas protokolla, jota käytetään usein reaaliaikaisen tiedonsiirron tarpeisiin. [10, s. 33]

Käsittelykerrokseen kuuluvat palvelualustat, sovellusohjelmointirajapinnat, tietovarastot, tietojenkäsittelyalgoritmit ja väliohjelmistot (engl. *middleware*), jotka toimivat siltana sovellusten, palveluiden ja käyttöjärjestelmien välillä. Väliohjelmisto huolehtii siitä, että data tallennetaan oikein, vaikka siihen lisättäisiin uusia laitteita. Ilman väliohjelmistoa IoT-laitteet eivät pystyisi kommunikoimaan keskenään. [10, s. 33]

Verkkokerros, joka koostuu langattomista, optisista ja puhelinverkoista, vastaa tiedon siirtämisestä eri laitteiden välillä. IoT-järjestelmissä verkkoportaalit toimivat keskeisinä välikäsinä, jotka mahdollistavat datan keräämisen antureilta, sen siirtämisen ja käsittelyn edelleen ohjausjärjestelmille. IoT-laitteet hyödyntävät langattoman tekniikan standardeja, jotka varmistavat eri valmistajien laitteiden kommunikoinnin keskenään. M2M-protokollat toimivat standardeina, joiden avulla ominaisuuksiltaan erilaiset, heterogeeniset IoT-laitteet voivat kommunikoida verkkoportaalien kautta. [10, s. 32]

Tiedonsiirtojärjestelmät voidaan jakaa sekä lähietäisyyden että laajemman alueen verkkoihin. Lähiviestintäprotokollat, kuten Bluetooth, radiotaajuinen etätunnistus (engl. *Radio-frequency identification*, RFID) ja lähitunnistus (engl. *Near-field communication*, NFC) ovat optimoitu pienitehoiseen ja lyhyen kantaman tiedonsiirtoon. Henkilökohtaiset alueverkot (engl. *Personal Area Network*, PAN) ovat matalatehoisia langattomia verkkoja, jotka perustuvat teknologioihin kuten Bluetooth. Näitä teknologioita käytetään usein älykkäissä ympäristöissä henkilökohtaisten laitteiden yhdistämiseen. Ne mahdollistavat lyhyen kantaman tiedonsiirron eri laitteiden, kuten älypuhelimien ja kannettavien tietokoneiden välillä. Laajempien alueiden langattomiin verkkoihin kuuluvat esimerkiksi Wi-Fi, 4G, 5G ja LoRaWAN.

Wi-Fi perustuu IEEE 802.11 -standardiin, jota langattomat paikallisverkot (engl. *Wireless local area network*, WLAN) käyttävät kodeissa ja julkisissa tiloissa. [10, s.32] LoRaWAN on LPWAN verkkoteknologian laajakaistaverkko (engl. *Low- Power Wide Area Network*, LPWAN). Se on keskeisessä roolissa IoT-sovelluksissa, joissa vaaditaan suuria laitemääriä, mutta joissa datamäärät ovat pieniä ja energiankulutus on minimoitava. [11]

Havainnointikerros on IoT-järjestelmän fyysinen taso, joka on suoraan vuorovaikutuksessa ympäristön kanssa. Sensoriteknologian avulla ympäristöstä voidaan kerätä tietoa fysikaalisista suureista, kuten lämpötilasta, nopeudesta, etäisyyksistä, sijainnista, melusta ja valaistustasosta. Kamerat, liiketunnistimet, anturit ja muut sensorit muodostavat yhdessä IoT-järjestelmän perustan, keräten jatkuvasti dataa älykaupungeissa. Ne lähettävät keräämänsä tiedot langattomien verkkojen kautta käsittelykerroksessa toimivaan keskitettyyn järjestelmään, jossa kerätty data analysoidaan. Näin saadaan reaaliaikainen kuva kaupungin tilasta, jota voidaan hyödyntää muun muassa päätöksenteossa, liikenteenohjauksessa, valvonnassa ja turvallisuusjärjestelmissä. [10, s. 31]

Ympäristön lisäksi tietoa voidaan hankkia myös puettavista laitteista, kuten älypuhelimista, aktiivisuusrannekkeista ja älykelloista. Puettavien laitteiden sensorit keräävät jatkuvasti dataa käyttäjänsä liikkeistä ja fyysisestä kunnosta, kun taas GPS-seurannan (engl. *Global Positioning System, GPS* kautta saadaan tarkkaa tietoa sijainnista. Älykaupungit pystyvät kokoamaan arvokasta tietoa asukkaidensa liikkumisesta ja toiminnasta yhdistämällä puettavien laitteiden sensoridataa esimerkiksi paikkatietoihin. [10, s. 10] Näin voidaan parantaa kaupunkipalveluita, mutta samalla herää kysymys siitä, miten henkilökohtaista dataa ja ihmisten yksityisyyttä voidaan suojella.

2.3 Tietoturvariskit

Idea älykaupungeista on lähtöisin kaupungistumisesta [10, s. 9]. Kaupungistuminen lisää IoT-laitteiden määrää huomattavasti, luoden monitasoisen laitekannan, joka kattaa niin yritykset, julkiset palvelut kuin kotitaloudetkin. IoT-laitteiden käyttö on laajentunut teollisuuteen ja kuluttajatuotteisiin, mikä on vauhdittanut markkinoiden kasvua [12, s. 2]. Vuoteen 2033 mennessä Kiinassa on arvioitu olevan yli 12 miljardia yhdistettyä IoT-laitetta, mikä on huomattavasti enemmän kuin Euroopassa ja Pohjois-Amerikassa, joissa odotetaan olevan noin 8,5 miljardia laitetta [13]. Laitekannan kasvaessa kyberhyökkäykset lisääntyvät, ja nopean tuotekehityksen sekä kustannuspaineiden vuoksi tietoturva jää usein toissijaiseksi.

IoT-laitteiden kehitys useiden valmistajien välillä on luonut hyvin hajanaisen laitekannan. Käyttöjärjestelmien, ohjelmistojen ja laitteistojen hajanaisuuden vuoksi niille on vaikea taata yhtenäistä turvallisuustasoa. [14, s. 6] Hajautunut omistajuus lisää nollapäivähyökkäyksiä (engl. *A zero-day attack*), eli hyökkäyksiä, joissa hyödynnetään ohjelmiston tai järjestelmän tuntemattomia haavoittuvuuksia ennen kuin valmistaja ehtii julkaista korjauksen. [14, s. 4] Tällä hetkellä ei ole olemassa selkeitä standardeja ja säännöksiä, jotka ohjaisivat yrityksiä uusien IoT-teknologioiden käyttöönotossa. Ongelmat liittyvät IoT:n nopeaan kehitykseen sekä lainsäädännön hitaaseen etenemiseen, mikä hankaloittaa hallitusten sekä kansainvälisten instituutioiden kykyä standardisoida ja valvoa alan säädöksiä. [14, s. 6] Ilman asianmukaista riskienarviointia kyberhyökkäykset voivat johtaa kalliisiin seurauksiin.

Potentiaalisten turvallisuusriskien ymmärtäminen kerroksittain voidaan hahmottaa kuvasta 2.2 sivulla 7. Sovelluskerroksen turvallisuus riippuu laitteiston ominaisuuksista ja käytetystä ohjelmistosta. Haittaohjelmat ja virukset voivat muuttaa sovellusten toimintaa, mikä voi johtaa laitteen toimintahäiriöön tai tietojen, kuten salasanojen vuotamiseen. Brute force -hyökkäyksessä (engl. *Brute force attack*) hyökkääjä yrittää arvata käyttäjän salasanan toistuvasti. Onnistuessaan hyökkääjä

voi saada pääsyn käyttäjän tiliin tai jopa koko laitteeseen. Joissakin sovelluksissa riittämätön muistin käytön tarkistus altistaa puskurin ylivuotohyökkäyksille, joiden avulla hyökkääjä voi varastaa tietoja tai ohittaa todennuksen IoT-laitteissa. [15, s. 11]

Käsittelykerroksessa laitteiden välisten, eli väliintulohyökkäysten (engl. *Man-in-the-middle attack*, MITM) uhka on yleinen. Hyökkääjä voi sijoittautua kahden IoT-laitteen väliseen yhteyteen ja tarkkailla tai muokata niiden välistä liikennettä, mikä voi johtaa tietojen vuotamiseen. Lisäksi monet IoT-laitteet edellyttävät tarkan ajan synkronointia. Hyökkääjät voivat hyödyntää tätä riippuvuutta estääkseen laitteiden osallistumisen sovellukseen häiritsemällä aikasynkronointia. Toinen käsittelykerroksen hyökkäyskohde ovat protokollat. Alentamalla protokollaversiota hyökkääjät voivat hyödyntää vanhemmissa versioissa olevia tietoturva-aukkoja. Palvelunestohyökkäyksessä (engl. *A denial-of-service attack*, DoS) MQTT-protokolla ylikuormitetaan lähettämällä runsaasti yhteyspyyntöjä, mikä estää laitteiden välisen kommunikaation. Hyökkäyksen vakavuus riippuu ylikuormituksen kestosta. [15, s. 11]

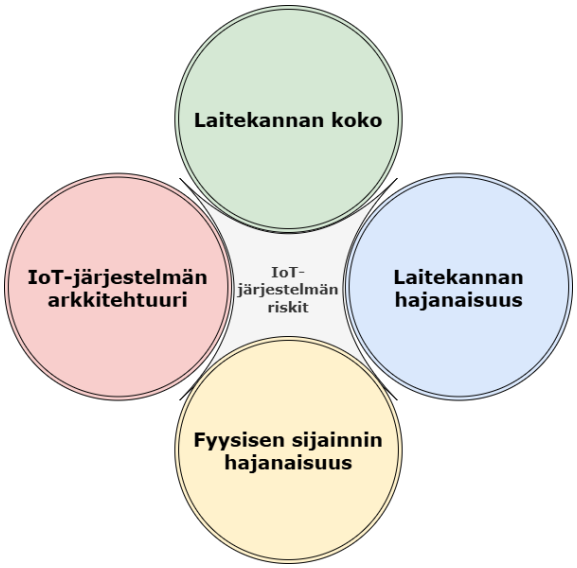
Verkkokerros kattaa langalliset, langattomat ja matkapuhelinpalvelut. Useat reitityshyökkäykset kohdistuvat tähän kerrokseen. Laitteen tunnisteen, eli MAC-osoitteen (engl. *Media Access Control*) paljastaminen voi altistaa IoT-laitteen muille hyökkäyksille. Hyökkääjä voi käyttää MITM-hyökkäystä luomalla valeidentiteettejä verkkoon, muokaten tietoliikennettä tai rikkoa verkon eheyden. Reitityspolun hyökkäys voi aiheuttaa laajamittaisia palvelukatkoksia, kun hyökkääjä manipuloi reititintä mahdollistaen DoS:ää laajemman, hajautetun palvelunestohyökkäyksen (engl. *distributed denial-of-service attack*, DDoS). [15, s. 12]

IoT-laitteiden fyysinen sijainti on hajautunut maailmanlaajuisesti, ja yksittäinen käyttäjä voi olla yhteydessä useisiin eri verkkoihin kytkettyihin laitteisiin. IoT-järjestelmien toimintaympäristö ylittää usein maantieteelliset rajat, mikä edellyttää monikansallisten kyberuhkien torjunnan kehittämistä. [14, s. 6]

2.4 Älykaupunki-määritelmän yhteenveto

Älykaupungin verkoston turvallisuus on kriittinen, sillä hyökkäys yhteen kohteeseen voi uhata koko järjestelmän toimintaa, minkä kuva 2.1 osoittaa sivulla 5. Kaupungistumisen ja kasvavan palvelutarpeen myötä IoT-järjestelmät ovat yhä alttiimpia kyberhyökkäyksille ja tietovuodoille erityisesti teollisuusmaissa kuten Euroopassa, Yhdysvalloissa ja Aasiassa [9].

Kuvassa 2.3 on esitetty tiivistetysti luvussa 2.3 käsittelyt neljä keskeistä osa-aluetta, jotka luovat turvallisuusriskejä ja haavoittuvuuksia älykaupunkien IoT-järjestelmille. IoT-laitteiden suojaus nojaa usein yleisesti käytettyihin turvallisuus-protokolliin, jotka eivät kuitenkaan aina ole riittäviä niiden suojaamiseksi. [12, s. 6] Lisäksi yritykset, jotka painottavat taloudellisia hyötyjä, pyrkivät vähentämään valmistuskustannuksia, mikä puolestaan saattaa heikentää IoT-laitteiden turvallisuutta. [15, s. 10].



Kuva 2.3: IoT-järjestelmän turvallisuusriskit

3 Älykaupungin kyberturvallisuus

Teknologia ja ihmiskeskeisyys yhdistyvät älykaupungeissa, jotka pyrkivät ratkaisemaan kaupunkien kasvusta aiheutuvia haasteita painottaen teknologisia edistysaskeleita. Älykaupungin riskien arvioinnissa on tärkeää tarkastella sekä yksittäisiä järjestelmiä että niiden vuorovaikutuksia. Vaikka yksittäisten haavoittuvuuksien tunnistaminen on helpompaa, IoT-järjestelmien riskien kokonaisvaltainen arviointi on välttämätöntä. [16, s. 1] Tässä luvussa käsitellään IoT-järjestelmän kyberturvallisuusriskejä älykaupungissa, haavoittuvuuksien tunnistamista sekä keinoja, joilla näitä haavoittuvuuksia voidaan vähentää.

3.1 Riskien ja haavoittuvuuksien tunnistaminen

Älykkaupunkien riskien ja haavoittuvuuksien luokittelu voidaan jakaa kahteen pääluokkaan: tekniset riskit ja muut kuin tekniset riskit. Tekniset riskit liittyvät teknologian käyttöönottoon ja sen haasteisiin, kuten kyberturvallisuuteen, yhteentoimivuuteen, tiedon hallintaan sekä datan laatuun ja eheyteen. [16, s. 6]

Riskien luokittelu taulukossa 3.1 pohjautuu [17, s. 14] esittämään arvioon. Korkeimman riskiarvion saivat IoT-hallintaan liittyvät riskit, jotka koskevat muun muassa IoT-verkkojen, julkisen internetin hallinnan, käyttäjien turvallisuuden, kaupunkien valvonnan sekä verkko-oppimisen toteuttamista. Erityistä huolta aiheuttavat myös teknologian eettinen käyttö, älykotien yhteydet, 5G-yhteyksien riskit, ympäristön seuranta, automaattinen tunnistus ja käyttäjien turvallisuus. [17, s. 12]

Taulukko 3.1: Älykaupungin IoT-järjestelmän riskit [17]

Riskit	**Huomioitavat osa-alueet**	**IoT-järjestelmän riskit**
IoT:n hallinta	IoT-verkko, julkinen verkko, käyttäjien turvallisuus, valvonta, käyttöetiikka, älykodit	IoT-järjestelmän arkkitehtuuri, laitekannan hajanaisuus
Kyberturvallisuuden hallinta	Fyysiset järjestelmät, kyberpuolustus, haavoittuvuudet, koulutus, tunkeutumisen havainnointi	IoT-järjestelmän arkkitehtuuri
Digitaalinen tiedonhallinta	Kaupungin uudistaminen, kaupungin kestävyys, liiketoiminta, kyberturvallisuus	IoT-järjestelmän arkkitehtuuri
Väestötiheyden hallinta	IoT-verkko, kaupunkiliikenne, väestövirrat, katastrofivalvonta	IoT-järjestelmän arkkitehtuuri, laitekannan koko
Langattomien sensoreiden hallinta	Kyberturvallisuus	IoT-järjestelmän arkkitehtuuri, laitekannan hajanaisuus, fyysisen sijainnin hajanaisuus
Seuravaan sukupolven IoT	Verkon hallinta	IoT-järjestelmän arkkitehtuuri

Riskien ja haavoittuvuuksien tunnistamiseen on kehitetty useita menetelmiä. Tunkeutumistestaus, eli hyökkäyksen simulointi älykaupungin infrastruktuuriin, on suunniteltu tunnistamaan haavoittuvuuksia, joita hakkerit voivat hyödyntää. Se auttaa arvioimaan turvatoimien tehokkuutta ja löytämään alueita, jotka vaativat parannusta. [18, s. 7]

Uhkamallintaminen tarkoittaa mahdollisten kyberuhkien ja niiden vaikutusten mallintamista infrastruktuuriin ja laitteisiin. Kyberuhkien potentiaalisten seurausten analysointi ja mallintaminen on äärimmäisen tärkeää, sillä se auttaa tunnistamaan haavoittuvuuksia ja kehittämään tehokkaita turvatoimia. [18, s. 7]

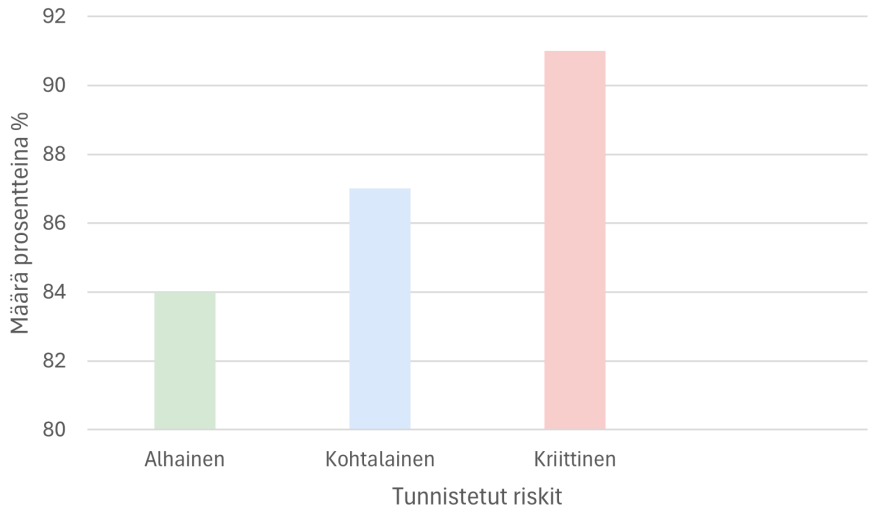
Haavoittuvuuksien skannaus tarkoittaa älykaupungin arkkitehtuurin ja laitteiden tarkastamista tunnettuja haavoittuvuuksia ja virheellisiä asetuksia vastaan. Sen avulla varmistetaan, että laitteet ovat ajan tasalla uusimpien asetusten ja turvakorjausten osalta. [18, s. 7]

Kyberhyökkäyksien lisääntyminen johtuu useista tekijöistä, kuten verkottumisen kasvusta, kehittyvistä hyökkäystekniikoista, puutteellisesta tietoturvaosaamisesta ja riittämättömistä turvatoimista. Lisäksi inhimilliset virheet ovat edelleen merkittävä syy siihen, että älykaupunkien kyberuhkat jäävät usein havaitsematta. [17, s. 3]

3.2 Riskien arviointi

Riskien arviointi tarkoittaa kyberuhkien ja niiden esiintymistiheyden tunnistamista, mikä auttaa älykaupungin sidosryhmiä priorisoimaan turvatoimia ja kohdentamaan resursseja. [18] Arviointiin on esitetty useita vaihtoehtoja ja mittareita, mutta nykyiset menetelmät eivät riitä IoT-järjestelmien riskien arvioimiseen [19].

Tunnistettujen riskien esiintyminen voidaan jakaa karkeasti kuvassa 3.1 olevan kaavion mukaisesti, mikä perustuu tutkimuksessa [19] käytettyyn riskien luokitteluasteikkoon. Asteikko jakaa tunnistetut riskit kolmeen kategoriaan: alhaiseen, kohtalaiseen ja kriittiseen. Luokitteluun vaikuttaa se, mihin osaan IoT-järjestelmää hyökkäys kohdistuu ja kuinka laaja se on. Kaavion perusteella voidaan todeta, että suurin osa tunnistetuista riskeistä on luokiteltu kriittisiksi.



Kuva 3.1: Tunnistettujen riskien luokittelu. [19]

Riskien arvioinnissa voidaan käyttää skenaarioita ja uhkamalleja, jotka auttavat tunnistamaan älykaupunkien kyberuhkia. Esimerkiksi liikennevalojen ohjausjärjestelmiin kohdistuvat hyökkäykset voivat manipuloida liikennevaloja ja aiheuttaa onnettomuuksia, sillä langattomien verkkojen yleistyminen on tehnyt niistä entistä alttiimpia tällaisille hyökkäyksille. Toisaalta hyökkääjät voivat myös keskeyttää säh-

könjakelun, mikä johtaisi laajoihin sähkökatkoksiin kaupungissa. Lisäksi valvontakameroiden hyödyntäminen voi johtaa vakaviin tietoturvauhkiin. Hyökkääjät voivat päästä käsiksi henkilötietoihin ja käyttää kameroita ihmisten vakoiluun. [20] Skenaariot korostavat älykaupunkien kyberturvallisuuden merkitystä ja tarvetta kehittää kestävämpiä turvatoimia.

Älykaupunkien strategiset riskit syntyvät, kun kaupunkien kehitysohjelmien välillä ei ole yhteyttä. Sen vuoksi älykkäiden hallintojen on käsiteltävä näitä riskejä ja haasteita strategioiden laatimisessa ja toteuttamisessa. Lisäksi on tärkeää kehittää hyväksyttyjä standardeja tiedon tallentamiseen, suojaamiseen ja turvallisuuteen, jotta hallinto- ja oikeudelliset riskit voidaan minimoida. [16, s. 10]

3.3 Tunnistettujen haavoittuvuuksien vertailu

Seuraavassa taulukossa 3.2 vertaillaan IoT-arkkitehtuuriin kohdistuvia hyökkäyksiä, joiden riskejä on arvioitu luvussa 3.2 esitetyn luokittelun perusteella. Hyökkäysten vertailu perustuu [20, s. 4] esittämään taulukkoon, jossa kuvataan, kuinka eri hyökkäykset hyödyntävät IoT-järjestelmän haavoittuvuuksia. Haavoittuvuudet valittiin Application Security Projectin (OWASP) IoT Top 10 -hyökkäysten luokituksen perusteella. [1] OWASP on tietoturvaan keskittyvä vapaaehtoisjärjestö, jonka tavoitteena on edistää luotettavien sovellusten kehittämistä ja ylläpitämistä. Haavoittuvuuksia vertaillaan luvussa 2.2 kuvatun IoT-arkkitehtuurin kuvan 2.2 mukaisesti.

Sovelluskerroksen haavoittuvuudet liittyvät salasanojen murtamiseen, sillä niissä on usein heikkoja oletusasetuksia. [20, s. 3] IoT-laitteet ovat alttiita skannaushyökkäyksille (engl. *Device scanning attack*), joissa hyökkääjä skannaa IoT-laitteiden verkkoja päästäkseen järjestelmään käsiksi. Samoin verkko-osoitteen (engl. *Uniform Resource Locator*, URL) heikkouksien hyödyntäminen URL-hyökkäyksessä tai DNS-järjestelmän manipulointi voivat vaarantaa verkkoliikenteen turvallisuuden.

[1] OWASP Top Ten - `https://owasp.org/www-project-top-ten/`

Käsittelykerroksessa hyökkääjät pyrkivät hyödyntämään verkko-protokollien, kuten DNS:n, HTTP:n ja MQTT:n haavoittuvuuksia käyttäen erilaisia tekniikoita. Kyberrikolliset kohdistavat usein hyökkäyksensä juuri näihin protokolliin, sillä niissä voi olla merkittäviä heikkouksia, jotka avaavat väyliä hyökkäyksille. [20, s. 3]

Jos laite on osa laajempaa verkkoa, kuten Wi-Fi, 5G tai LoRaWAN, hyökkääjä voi vaarantaa koko verkon toiminnan verkkokerroksessa. Neljä mahdollista hyökkäystyyppiä, jotka voivat päästä koko järjestelmään käsiksi, ovat skannaushyökkäys, brute force -hyökkäys, spoofing-hyökkäys ja laiteohjelmistohyökkäykset. [20, s. 3] Väärentämishyökkäyksessä (engl. *Counterfeit attack*) RFID-tunnisteet ja älykkäät sensorit ovat alttiita väärentämiselle, koska ne välittävät tietoa langattomasti. [21, s. 21] IoT-järjestelmissä on myös riski, että hyökkääjä voisi varastaa tietoa tai esiintyä toisena henkilönä. Käyttämällä Spoofing-hyökkäystä, eli toisena henkilönä esiintymistä, hyökkääjä voisi hyödyntää IoT-järjestelmälle toteutettuja palveluja. [20, s. 3].

Laitteen fyysiset haavoittuvuudet liittyvät laitteeseen pääsyyn debug- tai boottilassa, laitteiden kuunteluun tai laitteen hallinnan kaappaamiseen. Lisäksi haitalliset laiteohjelmistot voivat vaarantaa laitteen turvallisen käytön, mikä altistaa koko järjestelmän turvallisuusriskeille. Näiden uhkien vuoksi fyysisen turvallisuuden varmistaminen on keskeinen osa IoT-laitteiden suojaamista. [18]

3.4 Riskienhallinta ja ennakointi

Riskien hallinta on toistuva prosessi, joka sisältää viisi vaihetta: riskien tunnistaminen, analysointi, arviointi, käsittely sekä seuranta ja hallinta. Uusien teknologioiden käyttöönotto älykaupungeissa on tärkeää, mutta se edellyttää myös valmiutta hallita niihin liittyviä riskejä. Älykaupunkien hallinnasta vastuussa olevat tahot, kuten älykkäät hallinnot, eivät ole vielä täysin perehtyneet uusiin teknologioihin ja niiden mahdollisiin riskeihin. [17, s. 3]

Taulukko 3.2: Tunnistetut IoT-järjestelmän kerroskohtaiset riskit. [20]

Riski	Haavoittuvuus	Hyökkäys	IoT-kerros	Riskin arviointi	Riskin hallinta
Autentikointi	Salausalgoritmien toteutuksen puute. Heikko, arvattava salasana. Todennuksen ohittaminen, oletussalasanojen käyttäminen.	Brute force -hyökkäys. Toisena henkilönä esiintyminen. Laitteen skannaushyökkäys.	Sovelluskerros	Kriittinen Alhainen	Monivaiheinen tunnistautuminen. Salasanageneraattori, salasanan vahvuustesti.
Tiedonsiirtoprotokolla	HTTP:n ja DNS:n haavoittuvuudet	DoS, DDoS. URL-hyökkäys, DNS-väärennös	Sovelluskerros	Kriittinen Kohtalainen kriittinen	Järjestelmäpäivitykset, palomuurit, vahva salasana DDoS-suojaus, SSL/TLS-salauksen käyttö. Palvelimen kuormituksen tasaaminen, DNS-palvelimen suojaus.
Käyttöoikeuksien hallinta	Käyttöoikeustarkistuksen ohitus, laitteen virheellinen asetusten määritys. Metadatan manipulointi, turvaton laiteohjelmisto.	Spoofing-hyökkäys. Haitalliset laiteohjelmistot, etäohjaus, MITM-hyökkäys.	Sovelluskerros verkkokerros	kriittinen kriittinen	Ohjelmistopäivitykset, virustorjuntaohjelmistot, VPN-yhteydet
Viestintäprotokolla	MQTT-protokollan haavoittuvuudet. Tietojen vuotaminen, datan manipulointi.	Epäturvalliset palvelut, datan sieppaaminen, MQTT ei käytä datan salausta oletuksena. MITM-hyökkäys.	Käsittelykerros	Kriittinen alhainen	SSL/TLS-salauksen käyttö, Verkkosegmentointi, pääsynhallinta, vahva autentikointi, ohjelmistopäivitykset
Verkkoportaali	M2M-välinen hyökkäys, MAC-osoitteen paljastuminen. RFID- ja NFC-tunnistuksen haavoittuvuudet.	MITM-hyökkäys, väärien identiteettien käyttö. Tunnisteen tuhoaminen, DoS, Spoofing-hyökkäys, väärennöshyökkäys RFID-järjestelmään.	Verkkokerros	Kriittinen kohtalainen kriittinen	Vahva autentikointi, salausalgoritmien käyttö, digitaaliset sertifikaatit, SSL/TLS-protokollien käyttö, salausavaimien käyttö
Laitteen fyysisyys	Laitteeseen pääsy debug/boottilan kautta	DoS, kuuntelu, fyysinen manipulointi, laitteen ohjaus, haitalliset laiteohjelmistot	Havainnointikerros	Kriittinen	Ohjelmistopäivitykset, laitteen turvallinen käyttö, vahva salasana

IoT on edelleen kehittyvä teknologia, ja sen standardisointi sekä turvallisuus ovat tärkeitä kehityskohteita. Taulukossa 3.2 esitetään mahdollisia tapoja riskien ennakointiin ja hallintaan. Lisäksi tutkimuksessa [20, s. 11] on tunnistettu neljä keskeistä toimenpidettä riskien vähentämiseksi IoT-järjestelmissä: Käyttäjän tunnistaminen, eli autentikointi, tiedon salaus, verkkojen tietoturvallisuus, ja järjestelmän päivittäminen.

Autentikointi ja digitaaliset sertifikaatit ovat keskeisiä menetelmiä, jotka mahdollistavat osapuolten tunnistamisen henkilöllisyyden väärentämisestä johtuvien hyökkäysten välttämiseksi. Sertifikaatit varmentavat käyttäjän tai laitteen identiteetin. Näin voidaan tehokkaasti varmistaa tiedonsiirron luotettavuus. [21, s. 22]

Salausalgoritmien avulla suojataan tietoa luvattomalta käytöltä muuttamalla se salattuun muotoon. Salauksen ja tiedon voi purkaa ja lukea vain oikealla avaimella, mikä varmistaa tiedonsiirron luottamuksellisuuden ja eheyden. [21, s. 22]

Salausprotokollat (SSL/TLS) ovat suunniteltu suojaamaan tietoliikennettä verkkoissa takaamalla, että vain valtuutetut osapuolet voivat lukea tietoa ja että se pysyy muuttumattomana. MQTT-protokolla ei sisällä sisäänrakennettua suojausta. Sen turvallisuus riippuu siitä, miten sitä käytetään yhdessä muiden protokollien, kuten SSL/TLS-protokollien kanssa. [21, s. 23]

4 Pohdinta

Älykaupunki on monimutkainen konsepti, johon liittyy sekä hyviä mahdollisuuksia että huomattavia riskejä. Tämän tutkielman keskiössä olivat kyberhyökkäysten ja haavoittuvuuksien tunnistaminen, riskien hallinta sekä kyberuhkien ennakointi, mutta tutkielmassa käytetty aineisto ja tulokset eivät antaneet suoraa vastausta siihen, miten toimitaan, kun hyökkäys on jo tapahtunut.

Hyökkäysten jälkeinen toiminta, kuten IoT-järjestelmään tai verkkoon kohdistuneen hyökkäyksen korjaaminen ja palautuminen normaalitilaan, jää usein vähemmälle huomiolle. Toteutuneiden uhkien ja hyökkäysten vaikutukset ovat merkittäviä sekä älykaupunkien toimintaan että niiden asukkaiden yksityisyydensuojaan. Sen vuoksi älykaupunkien kehittämisessä on tulevaisuudessa huomioitava paitsi ennakoiva riskienhallinta myös tehokkaat toimenpiteet hyökkäysten aiheuttamien vahinkojen korjaamiseksi.

Älykaupungit ovat alttiita monille uhille, joista kaikkia ei ole ehditty käsitellä tässä tutkielmassa. IoT-järjestelmien ja niihin yhdistettyjen laitteiden haavoittuvuuksien lisäksi on olemassa muitakin riskejä, jotka voivat paljastaa arkaluontoista dataa tai heikentää älykaupungin toimintaa. Riskeihin kuuluvat myös sisäiset uhat, jotka voivat johtaa tietojen luvattomaan käyttöön, muokkaamiseen tai pahimmassa tapauksessa koko järjestelmän sabotoimiseen. Esimerkiksi palveluntarjoajat, jotka voivat väärinkäyttää pääsyään järjestelmiin, kuuluvat sisäisiin uhkiin. Väärinkäy-

töksiä on vaikea ennakoida, minkä vuoksi käyttöoikeuksien hallinta ja valvonta ovat tärkeitä, jotta näihin uhkiin liittyviä riskejä voidaan vähentää.

Kaupungistumisen ja kasvavan palvelutarpeen myötä IoT-järjestelmät ovat yhä alttiimpia kyberhyökkäyksille ja tietovuodoille, erityisesti teollisuusmaissa. Älykaupungit puolestaan hyödyntävät IoT-laitteiden keräämää dataa, kuten yhdistämällä sensoridataa paikkatietoihin. Se mahdollistaa kaupunkipalveluiden kehittämisen, mutta samalla nousevat esille tietoturvaan ja yksityisyydensuojaa koskevat kysymykset. Täten koko älykaupungin tasolla kerättävää tietoa on käsiteltävä suojatusti.

Massadatan määrä on kasvanut räjähdysmäisesti, sillä sitä kerätään lukuisista IoT-laitteista ja sensoreista. Laitteiden heterogeenisuuden lisäksi myös kerätyn datan laatu ja määrä vaihtelevat. IoT-palveluiden ytimessä oleville datamäärille on ominaista suuri volyymi, nopea kasvu sekä vaihtelevien tietotyyppien jatkuva lisääntyminen, joista syntyy suuria määriä jäsentämätöntä dataa IoT-laitteiden ja sovellusten kommunikoidessa keskenään. Jäsentämättömän datan hallinta aiheuttaa merkittäviä kyberturvariskejä sekä älykaupungille että älykkäälle hallinnolle. On kuitenkin tärkeää määritellä tarkasti ne erityiset toiminnalliset vaatimukset, jotka liittyvät älykaupunkien datalähteisiin ja sovelluksiin, ennen kuin ohjelmistoalustoja ja arkkitehtuureja suunnitellaan älykaupunkien tavoitteiden saavuttamiseksi.

Viime vuosina hallitukset, kaupungit, instituutit, tutkijat ja yksityishenkilöt ovat keränneet ja jakaneet kaupunkidataa laajasti eri aloilla. Siksi on tärkeää ymmärtää älykaupungin datan luonne, mukaan lukien datan mallinnuksessa käytettävät keskeiset elementit.

5 Yhteenveto

Luvussa 3 pyrittiin vastaamaan tämän tutkielman tutkimuskysymykseen TK1: *miten älykaupunkien IoT-järjestelmien haavoittuvuuksia voidaan ehkäistä*. Luvussa 3.1 saadut tulokset osoittivat, että yksi merkittävimmistä riskeistä ovat kaupunkien epäyhtenäiset kehitysohjelmat, erityisesti hyväksyttyjen standardien puute tiedon tallentamiseen, suojaamiseen ja turvallisuuteen liittyen.

Luvussa 3.3 vertailtiin riskien ennakointiin ja hallintaan käytettäviä menetelmiä, kuten kuten autentikointia, tiedon salaustekniikoita sekä ohjelmistopäivitysten hyödyntämistä. Luvussa 3.4 esitettiin myös suosituksia haavoittuvuuksien ehkäisemiseksi. Näitä olivat vahva tunnistautuminen, salausmenetelmät, verkkojen tietoturvallisuus, ja järjestelmien säännöllinen päivittäminen.

IoT-teknologiat mahdollistavat älykaupunkien toiminnan tehostamisen, mutta niissä ei ole olemassa yhtenäisiä turvallisuusstandardeja, mikä luo merkittäviä kyberturvallisuusriskejä. Lisäksi rajalliset taloudelliset resurssit vaikeuttavat tietoturvatoimien käyttöönottoa, mikä voi estää nopean reagoinnin kyberhyökkäyksiin ja altistaa IoT-järjestelmät uhille.

Älykaupungin kyberturvallisuus edellyttää laajaa strategiaa, joka kattaa suunnitteluperiaatteet, standardit, salauksen, käyttöoikeuksien hallinnan ja uhkien ennakoinnin. Keskeistä on, että kaikki sidosryhmät, kuten älykäs hallinto ja kyberturvallisuuden asiantuntijat, tekevät yhteistyötä älykaupunkien IoT-järjestelmien ja palvelujen suojaamiseksi.

Lähdeluettelo

[1] Population Reference Bureau. ”Percent of Population Living in Urban Areas”. (2024), url: https://www.prb.org/international/indicator/urban/snapshot (viitattu 09. 11. 2024).

[2] Y. H. Kwak ja J. Lee, ”Toward Sustainable Smart City: Lessons From 20 Years of Korean Programs”, *IEEE Transactions on Engineering Management*, vol. 70, nro 2, s. 740–754, 2023. DOI: 10.1109/TEM.2021.3060956.

[3] H. Sharma ja N. Kanwal, ”Smart Cities: A Worldwide Journey into Intelligent Urbanism and State-of-the-Art Technologies”, *Scientific and Technical Information Processing*, vol. 50, nro 4, s. 328–355, joulukuu 2023, ISSN: 1934-8118. DOI: 10.3103/s0147688223040081.

[4] European Commission. ”Smart Cities and Communities”. (2024), url: https://smart-cities-marketplace.ec.europa.eu/projects-and-sites (viitattu 08. 10. 2024).

[5] S. Dowling, M. Schukat ja H. Melvin, ”Data-centric framework for adaptive smart city honeynets”, teoksessa *2017 Smart City Symposium Prague (SCSP)*, 2017, s. 1–7. DOI: 10.1109/SCSP.2017.7973836.

[6] Transforma Insights. ”Current IoT Forecast Highlights”. (2024), url: https://transformainsights.com/research/forecast/highlights (viitattu 25. 10. 2024).

[7] J. Große-Bley ja G. Kostka, ”Big Data Dreams and Reality in Shenzhen: An Investigation of Smart City Implementation in China”, *Big Data & Society*, vol. 8, nro 2, heinäkuu 2021, ISSN: 2053-9517. DOI: 10.1177/20539517211045171.

[8] A. P. Fournaris, K. Lampropoulos ja O. Koufopavlou, ”End Node Security and Trust vulnerabilities in the Smart City Infrastructure”, *MATEC Web of Conferences*, vol. 188, S. Pantelakis ja S. Koubias, toim., s. 05 005, 2018, ISSN: 2261-236X. DOI: 10.1051/matecconf/201818805005.

[9] I. H. Sarker, ”Smart City Data Science: Towards data-driven smart cities with open research issues”, *Internet of Things*, vol. 19, s. 100 528, elokuu 2022, ISSN: 2542-6605. DOI: 10.1016/j.iot.2022.100528.

[10] M. Talebkhah, A. Sali, M. Gordan, S. J. Hashim ja F. Z. Rokhani, ”Comprehensive Review on Development of Smart Cities Using Industry 4.0 Technologies”, *IEEE Access*, vol. 11, s. 91 981–92 030, 2023. DOI: 10.1109/ACCESS.2023.3302262.

[11] Digita Oy. ”LoRaWAN-teknologia”. (2024), url: https://www.digita.fi/etusivu/palvelut-yrityksille/digitan-iot-palvelut/lorawan-teknologia/ (viitattu 11. 11. 2024).

[12] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen ja B. Stiller, ”Landscape of IoT security”, *Computer Science Review*, vol. 44, s. 100 467, toukokuu 2022, ISSN: 1574-0137. DOI: 10.1016/j.cosrev.2022.100467.

[13] Transforma Insights. ”Global IoT Forecast Report 2023-2033”. (2024), url: https://transformainsights.com/research/reports/global-iot-forecast-report-2023-2033 (viitattu 23. 11. 2024).

[14] P. Radanliev, D. De Roure, C. Maple, J. R. C. Nurse, R. Nicolescu ja U. Ani, "AI security and cyber risk in IoT systems", *Frontiers in Big Data*, vol. 7, lokakuu 2024, ISSN: 2624-909X. DOI: 10.3389/fdata.2024.1402745.

[15] A. Kumar, L. Kavisankar, S. Venkatesan, M. Kumar, S. Yadav, S. K. Shukla ja R. Khondoker, "IoT device security audit tools: a comprehensive analysis and a layered architecture approach for addressing expanded security requirements", *International Journal of Information Security*, vol. 24, nro 1, marraskuu 2024, ISSN: 1615-5270. DOI: 10.1007/s10207-024-00930-z.

[16] R. A. Sharif ja S. Pokharel, "Smart City Dimensions and Associated Risks: Review of literature", *Sustainable Cities and Society*, vol. 77, s. 103 542, helmikuu 2022, ISSN: 2210-6707. DOI: 10.1016/j.scs.2021.103542.

[17] F. Ullah, S. Qayyum, M. J. Thaheem, F. Al-Turjman ja S. M. Sepasgozar, "Risk management in sustainable smart cities governance: A TOE framework", *Technological Forecasting and Social Change*, vol. 167, s. 120 743, kesäkuu 2021, ISSN: 0040-1625. DOI: 10.1016/j.techfore.2021.120743.

[18] A. Q. Raheema, "Challenges and vulnerability assessment of cybersecurity in IoT-enabled SC", *Wireless Networks*, vol. 30, nro 8, s. 6887–6900, marraskuu 2023, ISSN: 1572-8196. DOI: 10.1007/s11276-023-03493-4.

[19] M. Usman Tariq, M. Babar, M. Ahmad Jan, A. Saeed Khattak, M. Dahman Alshehri ja A. Yahya, "Security Requirement Management for Cloud-assisted and Internet of Things–enabled Smart City", *Computers, Materials & Continua*, vol. 67, nro 1, s. 625–639, 2021, ISSN: 1546-2226. DOI: 10.32604/cmc.2021.014165.

[20] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo ja I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities", *IEEE Access*, vol. 8, s. 228 922–228 941, 2020. DOI: 10.1109/ACCESS.2020.3046442.

[21] A. Nag, M. M. Hassan, A. Das, A. Sinha, N. Chand, A. Kar, V. Sharma ja A. Alkhayyat, ”Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things”, *Transactions on Emerging Telecommunications Technologies*, vol. 35, nro 4, marraskuu 2023, ISSN: 2161-3915. DOI: 10.1002/ett.4897.