

Konsta Suutari

IoT:n hyödyntäminen koulutusjärjestelmässä

Tietotekniikan kandidaatintutkielma

21. joulukuuta 2018

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Konsta Suutari

Yhteystiedot: `konsta.m.suutari@student.jyu.fi`

Työn nimi: IoT:n hyödyntäminen koulutusjärjestelmässä

Title in English: The application of IoT in education systems

Työ: Kandidaatintutkielma

Sivumäärä: 24+0

Tiivistelmä: Tutkielma tekee muutamia keskeisiä teemoja käsitellen arvion IoT:n nykytilasta koulutusjärjestelmässä. Tutkielma punnitsee aiemmassa tutkimuksessa havaittuja hyötyjä ja ongelmia, kun IoT:ta integroidaan koulutusjärjestelmään. IoT:n keskeisiksi hyödyntämiskohteiksi on valittu tunnistautuminen, älykäs energianhallinta ja opetus. Ongelmia tarkastellaan tietoturvan ja kustannusten näkökulmista.

Avainsanat: IoT, koulutus, interaktiivisuus, koulutusjärjestelmä

Abstract: This thesis makes a general review of the current state of IoT in education systems. Different benefits and difficulties are weighed in the context of IoT being integrated into education systems. Identification, smart energy managing and teaching, are chosen as the pivotal benefits of IoT in this thesis. Security and the costs of IoT are chosen as the common issues that are addressed.

Keywords: IoT, education, interaction, education systems

Kuviot

Kuvio 1. IoT:n neljä tasoa. Lähde: Wikimedia Commons	4
Kuvio 2. IoT:n käytön vaikutukset tietokoneen komponenttien opetuksessa	15

Sisältö

1	JOHDANTO	1
2	INTERNET OF THINGS	3
	2.1 Mistä IoT koostuu	3
	2.2 Teknologiat	4
	2.2.1 RFID	5
	2.2.2 NFC	6
	2.2.3 Muut	6
3	HAASTEET JA VAATIMUKSET KOULUTUSJÄRJESTELMÄSSÄ	8
	3.1 Tietoturva	8
	3.2 Kustannukset	9
4	SOVELLUSKOHTEET JA HYÖDYT KOULUTUSJÄRJESTELMÄSSÄ	11
	4.1 Tunnistautuminen	11
	4.2 Energianhallinta kampuksella	12
	4.3 Opetus	13
5	YHTEENVETO	16
	KIRJALLISUUTTA	18

1 Johdanto

IoT (Internet of Things), eli esineiden internet, on tämän hetken merkittävimpiä puheenaiheita tietotekniikan alalla. Esimerkiksi alan julkaisusivuston IEEEExplore:n suosituimpien hakutermien listalla se on tutkielman kirjoitushetkellä sijalla yksi. Internet of Things on käsitteenä ollut olemassa jo vuodesta 1999, kun IoT:n isänä pidetty Kevin Ashton käytti käsitettä ensimmäisen kerran esitelmänsä otsikkona. Sen suosio on kuitenkin lähtenyt kiihtyvään kasvuun vasta 2010-luvulla. Tämän kasvun on mahdollistanut mm. merkittävä kehitys langattomissa viestintäteknologioissa kuten Bluetooth, radiotaajuinen etätunnistus eli RFID ja Wi-Fi (Gubbi, Buyya, Marusic & Palaniswami 2013). Lisäksi IoT-tekniikan kaupallinen houkuttelevuus on tuonut valtavan määrän uusia tekijöitä, tutkijoita ja ideoita kentälle. Esimerkiksi IDC:n tutkijoiden tekemä hyvin kattava markkina-analyysi osoittaa, että IoT:n markkinat kasvavat jopa 7,1 triljoonaan dollariin vuoteen 2020 mennessä, kun vuonna 2013 se oli vielä 1,9 triljoonaa dollaria (Lund, Turner, MacGillivary & Morales 2014). IoT:n suosio on siis kiistaton.

Tässä kirjallisuuskatsauksessa lähdän kartoittamaan, että miten, ja millä ehdoilla tätä suurta innovaation, tutkimuksen ja rahoituksen aaltoa voitaisiin valjastaa koulutusjärjestelmän hyödyksi. Etenkin Suomessa koulutusjärjestelmä on yksi yhteiskunnan tärkeimpiä kulmakiviä, ja siksi on tärkeää aina merkittävien uusien ideoiden noustessa pinnalle punnita niiden potentiaalista hyötyarvoa, jotta järjestelmä pysyisi kilpailukykyisenä ja ajan tasalla. Tutkielmassa kirjoitan paljon erityisesti *koulutusjärjestelmästä* pelkän koulutuksen sijaan, sillä IoT:n hyötyjä punnitessa tulee ottaa huomioon myös muut kuin suorat pedagogiset hyödyt. Esimerkiksi RFID -tai NFC-siruille perustuvat kulunvalvontajärjestelmät, joilla pyritään lisäämään opetusrakennusten tehokkuutta ja turvallisuutta (Bagheri & Haghghi 2016) ovat jo omien havaintojeni mukaan melko laajamittaisessa käytössä, ja nähtävissä myös suomalaisilla kampuksilla ja kouluilla.

Toisessa luvussa aion avata syvemmin tutkielmassa käytettyjä tärkeitä käsitteitä. Avaan IoT:ta käsitteenä, ja annan esimerkkejä laitteista joista se koostuu. Lisäksi

kerron myös hieman tekniikoista jotka tekevät IoT:n mahdolliseksi. Kolmannessa luvussa haluan keskittyä haasteisiin joita tämä uusi teknologia joutuu kohtaamaan, mikäli sitä halutaan soveltaa koulutussektorille. Pyrin selvittämään löytyykö näiden ongelmien ratkomiseen varteenotettavia ratkaisuja, sekä esitän hieman omia ajatuksiani aiheesta.

Kun valtion koulutukseen myöntämä budjetti kiristyy (Tervasmäki & Tomperi 2018), IoT-ratkaisut - kuten kaikki muut uudet innovaatiot - joutuvat kilpailemaan rahoituksesta koulutuksen fundamentaalisten perustarpeiden, kuten opettajien palkkaamisen ja koulutustilojen parannusten kanssa. Siksi tutkielman neljännessä luvussa haluan keskittyä tarkastelemaan olemassa olevan tutkimuksen tarjoamaa näyttöä IoT:n hyödyllisyydelle koulutusjärjestelmässä. Kartoitan käytössä olevia ja suunniteltuja käyttökohteita, sekä niitä tutkimalla saatuja tuloksia.

Tutkielman lopuksi kerään yhteenvedon tekemistäni havainnoista ja pohdin min-kälaisia merkittäviä tuloksia saatavilla olevat tieteelliset lähteet tarjoavat. Pyrin tekemään lähdemateriaalin perusteella johtopäätöksiä, ja vastaamaan tutkimuskysymyksiin:

1. Onko IoT:lla ja sen tuottamilla sovelluksilla paikka suomalaisessa koulutusjärjestelmässä?
2. Onko IoT-ratkaisuilla realistisia mahdollisuuksia vastata julkisen koulutusjärjestelmän asettamiin vaatimuksiin ja rajoitteisiin, vai pitääkö tekniikan vielä kehittyä pidemmälle, ennenkuin sitä voidaan hyödyntää kannattavasti ja turvallisesti?

2 Internet Of Things

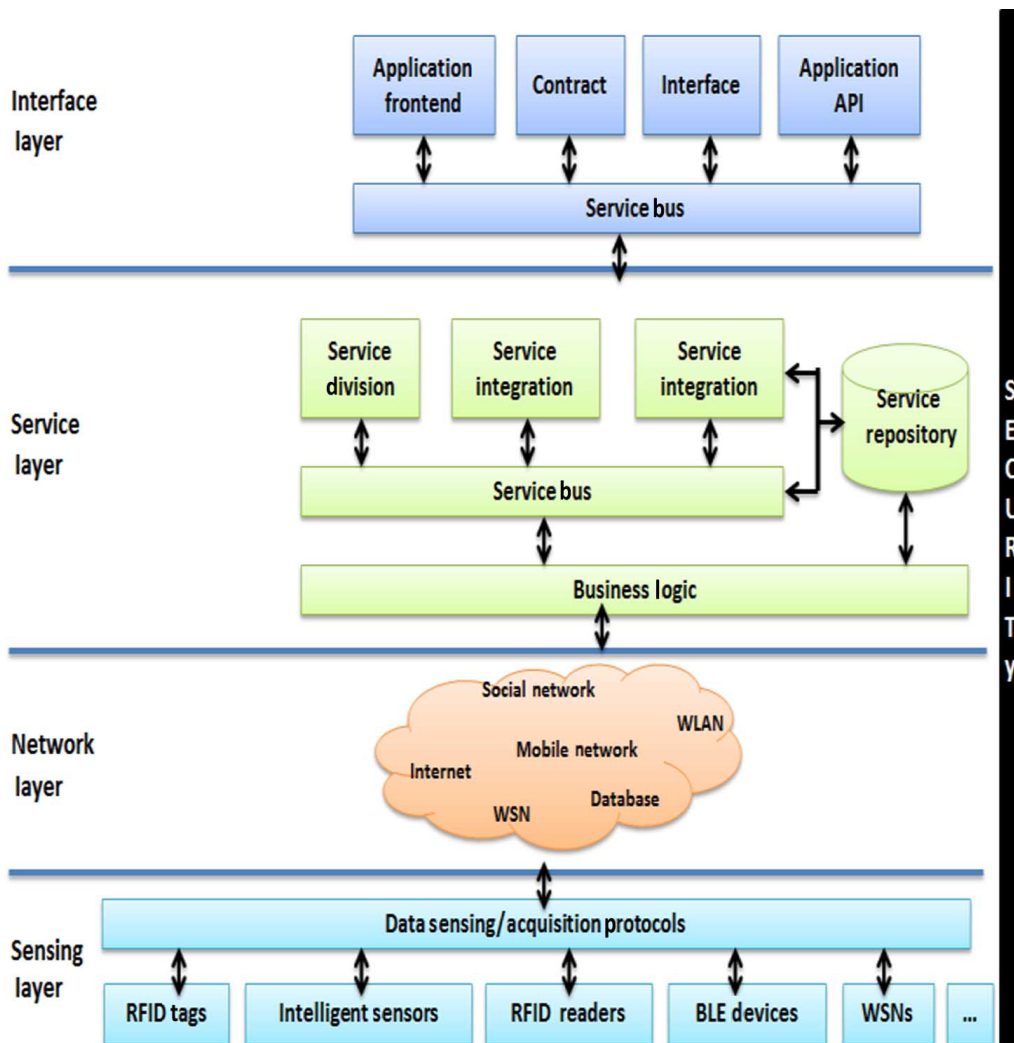
IoT ei ole yksittäinen laite tai verkko, vaan se on monimuotoinen laitteiden luoma verkostojen verkosto. Nämä laitteet voivat olla liikennevaloja, pesukoneita, jääkaappeja, tai mitä tahansa sellaista, johon on mahdollista sulauttaa laskentaa suorittava yksikkö kuten mikroprosessori. Usein nämä ns. "esineet"(engl. Things) sisältävät myös erilaisia sensoreita, tai muita toimilaitteita, jotka keräävät dataa ympäristöstään ja lähettävät sen sitten eteenpäin päätteelle, joka tekee siitä hyödyllistä informaatiota (Bagheri & Haghghi 2016).

IoT-laitteita käytetään todella moniin eri käyttötarkoituksiin, mutta erityisesti IoT-tekniikat perustuvat ympäristönsä mittaamiseen ja mitatun tiedon kommunikointiin. Kumpikaan näistä asioista ei ole uusi haaste tietotekniikan ratkottavaksi, mutta IoT pyrkii suoriutumaan näistä tehtävistä uudella tavalla; autonomisesti ja älykkäästi. Tämän kaltainen teknologia, joka ei vaadi ihmistä toimiakseen, voi muuttaa kaiken jokapäiväisessä elämässämme, mikäli se toteutetaan oikein (Shah & Yaqoob 2016). Laitteiden autonomisuus voi nousta suureksi hyödyksi erityisesti olemassaolevien koulutusjärjestelmän toimintatapojen tehostamisessa.

2.1 Mistä IoT koostuu

Kuten tämän luvun aloituskappaleessa jo totesin, IoT koostuu hyvin monimuotoisesta joukosta laitteita. Vuonna 2016 IoT käsitti jopa 6.4 miljardia laitetta, ja määrän uskotaan kasvavan 25 miljardiin vuoteen 2020 mennessä (Van Der Meulen 2015). Tähän joukkoon mahtuu luonnollisesti laitteita tuhansilta eri valmistajilta käyttäen tuhansia eri teknologioita.

Laitteilla on kuitenkin joitain yhdistäviä piirteitä. Tietokoneet jotka yhdistävät esineen IoT:hen ovat usein pienikokoisia, joka mahdollistaa niiden integroimisen lähes kaikkiin päivittäin kohtaamiimme esineisiin (Gomez, Huete, Hoyos, Perez & Grigori 2013). Tämä pieni koko osoittautuu monesti myös suureksi ongelmakohdaksi, sillä siitä johtuen laitteisiin ei usein mahdu paljoa laskentatehoa, joka taas puoles-



Kuvio 1. IoT:n neljä tasoa. Lähde: Wikimedia Commons

taan pakottaa kompromisseihin esimerkiksi tietoturvassa (Zhang, Cho, Wang, Hsu, Chen & Shieh 2014). Näistä kirjoitan lisää erityisesti koulutusjärjestelmän kontekstissa luvussa 3. Tavanomainen IoT-järjestelmä rakentuu neljäkerroksisen arkkitehtuurin päälle. Kuvio 1 havainnollistaa näitä IoT:n neljää yleisesti tunnistettua kerrosta, niiden funktioita, sekä teknologioita joita kukin taso hyödyntää toimiessaan.

2.2 Teknologiat

IoT:n suosion suureen kasvuun viime vuosina ovat johtaneet tällä vuosikymmenellä saavutetut merkittävät kehitysaskleet teknologioissa, joita IoT usein hyödyntää.

Erityisesti langattomat teknologiat kuten RFID, NFC, Bluetooth ja Wi-Fi ovat ottaneet suuria kehitysaskelia, ja avanneet uusia mahdollisuuksia IoT-sovelluksille. Tämä näkyy myös valtioiden ja koulutuslaitosten kasvaneena kiinnostuksena IoT:ta kohtaan, ja IoT-pohjaisia ratkaisuja onkin jo otettu käyttöön monella koulutusjärjestelmän osa-alueella. IoT harvoin hyödyntää vain yhtä edellä mainituista teknologioista, vaan se yhdistää useita teknologioita yhdeksi toimivaksi ratkaisuksi (Shah & Yaqoob 2016). Siksi toimivia ratkaisuja etsiessä kenttää on tarkasteltava hyvin laajakatseisesti.

2.2.1 RFID

Radio Frequency Identificationia (RFID) pidetään yhtenä merkittävimmistä IoT:n mahdollistajista. Valtaosa olemassa olevista IoT-laitteista hyödyntää RFID:tä jollain tavalla (Atzori, Iera, & Morabito 2010). Tyypillisessä RFID-sovelluksessa luetaan radioaaltoja, jotka kulkevat tunnistesirun, eli "tagin" ja lukijan välillä. Siru pitää sisällään dataa Electronic Product Coden (EPC) muodossa, joka on ohjelmoitu siruun jonkin RFID-verkkoa hallinnoivan keskuksen, eli "Auto-ID Centerin" toimesta. (Lee & Lee 2015). Lukijat on sitten mahdollista ohjelmoida lukemaan näitä siruja ja reagoimaan niihin halutulla tavalla. Esimerkiksi koulurakennuksen ovet voidaan varustaa tällaisilla lukijoilla, ja käyttää RFID-siruja ovien avaimina. Tätä esimerkkiä käsittelen lisää luvussa 4.

RFID-tunnisteita on passiivisia, semipassiivisia ja aktiivisia. Passiiviset tunnisteet eivät sisällä minkäänlaista virtalähdettä, vaan saavat virtansa käyttämiensä radioaaltojen elektromagneettisesta energiasta. Semipassiiviset tunnisteet sisältävät virtalähteen (esim. jonkinlainen patteri), mutta käyttävät silti radioaalloista saatavaa energiaa hyödykseen. Aktiiviset tunnisteet taas toimivat täysin oman virtalähteen energialla. Aktiiviset tunnisteet mahdollistavat monipuolisemman kommunikation tunnisteiden ja lukijan välillä, mutta ne ovat kalliimpia kuin passiiviset tunnisteet. (Lee & Lee 2015) Aktiiviset tunnisteet vaativat myös virtalähteiden kulumisesta aiheutuvaa ylläpitoa.

2.2.2 NFC

Near Field Communication (NFC) on toimintatavaltaan hyvin lähellä RFID:tä, ja sitä pidetäänkin ikään kuin yhtenä RFID:n alalajina. NFC-kommunikaatio tapahtuu myös radioaaltojen avulla, ja myös NFC:n tapauksessa laitteet voivat olla aktiivisia tai passiivisia. Merkittävin ero näiden teknologioiden välillä on kuitenkin laitteiden kyky toimia sekä lukijana, että tunnisteena. Tämä mahdollistaa ”peer-to-peer”-tyyppisen tiedonjaon laitteiden välillä, jossa tieto voi liikkua molempiin suuntiin. NFC-verkko toimii RFID:n tavoin vain lyhyillä etäisyyksillä, ja sen tiedonsiirtonopeus on hyvin hidas. Tästä johtuen NFC:tä käytetään usein esimerkiksi vain kommunikaation avaajana tai aloittajana, kun lopullinen massiivisempi tiedonsiirto tapahtuu jonkin toisen kommunikaatioteknologian, kuten Wi-Fi:n, välityksellä. (Cavoukian 2012)

Esimerkiksi koulukirjan sivuille voitaisiin integroida passiivisia NFC-tunnisteita, jotka lukija voi lukea omalla älypuhelimellaan. Tunniste voisi sisältää esimerkiksi osoitteen verkkosivulle, jonka puhelin sitten avaa selaimessaan ja lataa itse sivun sisällön käyttäen esimerkiksi Wi-Fi -tai 3G-yhteyttä. Uskon että juuri tällaiset sovellustavat voivat osoittautua hyvinkin toteutettaviksi, sillä valtaosalta oppilaista jo peruskoulutasolla löytyy taskustaan älypuhelin jolla on kyky toimia sekä NFC-lukijana että tunnisteena.

2.2.3 Muut

IoT koostuu myös lukuisista muista teknologioista. Esimerkiksi yleisesti tunnetummat Wi-Fi ja Bluetooth ovat usein keskeisessä osassa IoT-laitteiden kommunikaatiota. Lisäksi IoT:n käyttämistä kommunikaatioteknologioista käytävässä keskustelussa käytetään paljon käsitteitä kuten WSN, WSAN, UID ja WISP, mutta niiden toiminnan syvempi analysoiminen ei ole olennaista tämän tutkielman kannalta. Pidän kuitenkin RFID:n ja NFC:n käsitteitä hieman tärkeämpinä, sillä ne ovat ylivoimaisesti suosituimpia teknologioita IoT-ratkaisuista puhuttaessa (Atzori ym. 2010).

On tärkeää tiedostaa myös, että IoT:n sovellusmahdollisuuksia ja ongelmia määrit-

telee lisäksi muut teknologiat ja sovellukset, kuin tässä luvussa käsitellyt kommunikaatioteknologiat. Esimerkiksi datan muuttaminen tiedoksi sen lopullisessa määränpäässä, kuten palvelimella tai pilvessä, vaatii omat teknologiset ja ohjelmalliset ratkaisunsa. Rajoitun tässä kirjallisuuskatsauksessa kuitenkin tarkkailemaan IoT:ta ja sen näkyvyyttä "kentällä", joten en koe, että näiden tekijöiden tarkkaileminen on tässä tutkielmassa tärkeää. Kuitenkin myös näiden tässä tutkielmassa käsittelemättömien kerroksien tutkiminen on elintärkeää teknologian kehitykselle.

3 Haasteet ja vaatimukset koulutusjärjestelmässä

Kuten mikä tahansa uusi teknologia, myös IoT joutuu kohtaamaan oman kirjonsa haasteita ja ongelmakohtia sen siirtyessä teoriasta käytäntöön. IoT:ta käsittelevässä tutkimuksessa nousee joitain IoT:n kaikille sovellusalueille ylettäviä ongelmia. Esimerkiksi tutkijapari Lee & Lee (2015) nostavat esiin viisi keskeistä haastetta jotka tulevat vastaa IoT-kehityksessä:

1. Suurten datamäärien hallinnointi.
2. Tiedonlouhinnan haasteet. ts. Kuinka tehdä raa'asta datasta jotain hyödyllistä?
3. Yksityisyyden haasteet. Käyttäjän yksityisyyden suojaaminen usein epätuoteliasta sovelluksen kehittäjälle.
4. Tietoturva haasteet.
5. Laitteiden määrän ja nopeasti kehittyvien tuotteiden aiheuttama kaoottisuus.

Tutkielma käsittelee seuraavaksi lyhyesti kahta ongelmaa jotka esiintyvät erityisen voimakkaasti koulutusjärjestelmässä; Tietoturva ja kustannukset. Esimerkiksi tietoturvan merkitys korostuu paljon kun puhutaan julkisesta palvelusta kuten koulutus. Koulutusjärjestelmän IoT-sovellukset voivat esittää myös joitain uusia ongelmia, jotka eivät esiinny muissa ympäristöissä, tai ne esiintyvät jossain eri muodossa.

3.1 Tietoturva

Tietoturva on haaste, joka nousee usein esiin IoT:ta käsittelevissä tutkimuksissa (esim. Mukherjee 2015; Bagheri & Haghghi 2016; Gubbi ym. 2013). Tutkijoiden huoli näiden järjestelmien tietoturvasta voi olla hyvinkin aiheellista, sillä esimerkiksi Hewlett Packard (2014):in tekemän tutkimuksen mukaan jopa 70% IoT-laitteista sisältää haavoittuvuuksia. Haavoittuvuuksia sisältävistä laitteista löydettiin keskimäärin 25 haavoittuvuutta laitetta kohden. Kouluympäristössä tällaiset haavoittuvuudet voivat altistaa esimerkiksi opiskelijoiden tai oppilaiden henkilökohtaiset tiedot hyökkääjälle.

Tietoturva haasteet ovat erityinen haaste julkisille palveluille kuten terveydenhuololle ja koulutukselle, sillä lain noudattaminen esimerkiksi yksityisyyttä koskevissa asioissa on ehdottomana prioriteettina näitä palveluita suunniteltaessa. Esimerkiksi riski alaikäisen oppilaan puhelimesta kerätyn tiedon vuotamisesta julkisuuteen tietomurron seurauksena on riski, joka saattaisi olla hyväksyttävä yksityisen yrityksen sovelluksessa kuten mobiilipelissä, mutta julkisen peruspalvelun kontekstissa hyvinkin kriittinen. Jos tämän tyyppiselle tietovuodolle olisi huomionarvoinen mahdollisuus julkisen koulujärjestelmän käyttämässä sovelluksessa, uskon että sen käyttöönotto herättäisi hyvin vakavia kysymyksiä sovelluksen käytön eettisyydestä. Myös hiljattain voimaan astuneen GDPR:n noudattaminen vaatii paljon tietohallinnollisia järjestelyitä kaikilta IoT-palveluilta (Castelluccia, Cunche, Le Métayer & Morel 2018), mutta erityisesti julkisten elimien on noudatettava näitä säädöksiä hyvinkin tarkasti.

3.2 Kustannukset

IoT:n integroimisesta opetusinfrastruktuuriin syntyy luonnollisesti uusia kustannuksia, jotka koulutusjärjestelmän on oikeutettava. Koulutusjärjestelmän on kokeiltava uusia innovaatioita ja pysyttävä ajan tasalla, mutta samalla on taattava tarpeeksi opettajia ja laadukkaat tilat laadukkaasti opetuksen takaamiseksi. Jotta IoT:lla on realistisia mahdollisuuksia päästä koulutusmarkkinoille, on siis keksittävä ratkaisuja, jotka eivät ole vain tehokkaita tarkoitettussa tehtävässään, vaan myös kustannettavuudeltaan.

IoT:sta syntyvät kustannukset ovat monien tekijöiden summa. Tyypilliseen järjestelmään kuuluu esimerkiksi sensoreita, prosessointiyksiköitä, kommunikaatiojärjestelmiä, tiedon varastointiyksiköitä ja tiedon esittämiseen tarvittavia ohjelmia (Velasquez, Medina, Castro, Acosta & Mendez 2017). Tällaisen järjestelmän käyttöönottokustannukset voivat olla suuret, kun siihen liittyvät esimerkiksi palvelimien ja ohjelmistojen hankintaan liittyvät kulut. Kuitenkin alun kustannusten jälkeen järjestelmä voi olla hyvinkin tehokkaasti skaalautuva, sillä sen käyttäjämäärän kasvattaminen vaatii parhaassa tapauksessa vain uusien tunnisteen hankkimista. Yleisesti

käytetyn passiivisen RFID-tunnisteen hinta on ollut vuonna 2014 hieman alle euron (Yewon 2014), ja teknologian nopea kehitys tekee niistä jatkuvasti halvempia.

IoT:n hyödyntämisestä koulutusjärjestelmässä on hyvin vähän tutkimuksia, ja vielä vähemmän sen kustannettavuudesta kyseisellä sektorilla. IoT on kuitenkin osoittanut useissa tutkimuksissa olevansa hyvin kustannustehokas teknologia kun sitä hyödynnetään oikein (esim. Sinha, Wei & Wang 2017; Mercer & Leech 2018). Yksi tapa vastata tähän haasteeseen on myös IoT-järjestelmät, joiden funktio on luonteeltaan ekonominen, ja joiden rahallinen hyöty on suoraan nähtävissä. Tästä esimerkkinä luvussa 4 käsiteltävät energianhallintajärjestelmät. IoT saattaa siis hyvin usein olla jopa varallisuutta lisäävä teknologia, sillä suurimassa osassa sovelluksia pyritään juurikin vähentämään kustannuksia ja kasvattamaan tehokkuutta järjestelmässä johon se integroituu. Esimerkiksi tutkijaryhmä Abuarqoub, Abusaimah, Hammoudeh, Uliyan, Abu-Hashem, Murad & Al-Fayez (2017) listaa IoT:n hyötyjä analysoidessa ensimmäisenä tehokkuuden lisäämisen ja kustannusten pienentämisen.

4 Sovelluskohteet ja hyödyt koulutusjärjestelmässä

IoT:lla, kuten millä tahansa uudella teknologialla on lukuisia potentiaalisia sovelluskohteita koulutusjärjestelmässä. IoT:n mukautuvainen ja monimuotoinen luonne voi kuitenkin tuottaa tavallistakin enemmän hyödyllisiä sovelluksia. Tässä luvussa käsittelen joitain aiemmassa tutkimuksessa löydettyjä hyötyjä IoT:n käytölle koulutusjärjestelmässä ja pohdin niiden realistista käyttömahdollisuutta Suomessa.

4.1 Tunnistautuminen

RFID- ja NFC-pohjaisesta tunnistautumisesta, joka on jo laajalti käytössä muilla aloilla, voi olla merkittäviä hyötyjä koulujen ja kampusten henkilökunnalle. IoT-tunnistautumisen perustuva kulunvalvonta on kenties kaikkein yleisin IoT:n käyttökohde Suomalaisessakin koulutusjärjestelmässä jo nyt. Useat vierailemani koulut (esimerkiksi Jyväskylän normaalikoulu) käyttävät kulunvalvontaan RFID-tunnistautumista. Näin koulun lukitut luokahuoneet ja muut ovet voidaan avata RFID-tunnisteen avulla, ja avaimen katoamistapauksessa tunniste voidaan deaktivoida. Perinteisellä avainjärjestelmällä avaimen katoaminen voi pakottaa koulun vaihtamaan useita lukkoja luvattoman kulun estämiseksi, aiheuttaen näin suuria lisäkustannuksia.

IoT-pohjaista tunnistautumista voidaan käyttää myös lisäämään tehokasta opetusai-
kaa korkeakouluympäristössä. Esimerkiksi Arulogun, Fakolajo & Olaniyi (2013) kirjoittavat havainneensa oppilaiden vähäisen motivaation saapua kuuntelemaan luentoja paikan päälle, ja tästä aiheutuvan huolen oppilaiden ja opettajien välisen interaktiivisen suhteen rikkoutumisesta. Koska oppilaiden läsnäolon valvominen pakottaa luennoitsijan kuluttamaan arvokasta luentoaikaa läsnäolijoiden tarkistamiseen, kirjaamiseen tai testaamiseen, se voitaisiin mielummin hoitaa automaattisen IoT-järjestelmän avulla. Tutkijaryhmä esittääkin artikkelissaan oman sovelluksensa, jossa oppilas voi kirjata itsensä läsnäolevaksi vain näyttämällä nopeasti RFID-tunnistettaan lukijalle huoneeseen saapuessa. Tällainen järjestelmä tekee mahdolliseksi myös oppilaalle seurata omaa osallistumisprosenttiaan, ilman kurssin pitäjälle

aiheutuvaa lisätyötä.

Tunnistautumisen hyödyt eivät kuitenkaan rajoitu vain koulutusorganisaation hyödyiksi, vaan myös opiskelijoiden elämää voidaan helpottaa autonomisilla IoT-järjestelmillä. Esimerkiksi Koreassa Sookmyungin yliopistossa on kehitetty ja otettu käyttöön ”Smart Sookmyung”-sovellus, jolla on mahdollista seurata kampuksen pääkirjaston pöytien varaustilannetta (Yewon 2014). Kun opiskelija saapuu rakennukseen, hän voi tunnistautua mobiililaitteesta löytyvän NFC-tunnisteen avulla, tarkistaa kirjastossa vapaana olevat pöydät, sekä varata itselleen pöydän. Sovellusta voidaan käyttää myös aiemmin mainittuun läsnäolon valvontaan.

Kuten näistä esimerkeistä tulee esille, uskon että IoT:n tunnistautumismahdollisuudet luovat erityisesti mahdollisuuksia tehostaa olemassa olevia järjestelmiä, ja luoda enemmän ajan käyttöä opettamiseen ja opiskeluun ylimääräisten järjestelykysymysten ratkomisen sijasta. Pidän tässä mainittujen tunnistautumisjärjestelmien toteuttamista myös ekonomisesti realistisina, sillä RFID ja siihen perustuva NFC ovat tyypillisesti hyvin kustannustehokkaita teknologioita (Arulogun ym. 2013).

4.2 Energianhallinta kampuksella

IoT:n suosion kasvun myötä siihen perustuvat älykkäät energianhallintajärjestelmät ovat herättäneet suurta kansainvälistä kiinnostusta (Suwon & Seongcheol 2016). Nämä ns. ”Smart Grid”-järjestelmät tuottavat käyttäjilleen älykkäitä keinoja hallita energiaa kustannustehokkaammin ja säästäväisemmin. Smart Gridit perustuvat usein erilaisiin sensoriverkkoihin, jotka mittaavat laajemmin ja tarkemmin jokaisen yksittäisen kuluttajan energiantarvetta, ja muokkautuu sitten käyttäytymään näiden tarpeiden mukaisesti. Pidän todennäköisenä, että älykäs energianhallinta nousee tärkeäksi osaksi julkisten järjestelmien kompetenssia mitatessa, kun ilmastomuutoksen rooli mediassa ja yleisessä keskustelussa kasvaa.

Jotta suomalaiset korkeakoulut pysyisivät kilpailukykyisenä kansainvälisillä koulutusmarkkinoilla, on sen otettava vakavasti huomioon kohderyhmänsä intressit ja asenteet ympäristöä koskeviin asioihin kuten energianhallintaan. Rieki (2015)

tekemässä tutkimuksessa ympäristöasenteista nähdään, että 1986-1995 syntyneistä suomalaisista 30,5% pitää ilmastonmuutosta äärimmäisen vaarallisena, 32,8% Hyvin vaarallisena ja 20,9% Melko vaarallisena. Siis 84,2% yliopistojen tärkeimmästä kohderyhmästä pitää ilmastonmuutosta jonkin asteisena uhkana. Tutkimus osoitti tämän olevan myös kasvava trendi kaikissa ikäryhmissä. On siis syytä olettaa että koulutuslaitokset, jotka pystyvät vastaamaan tähän huoleen järkevillä energiaratkaisuilla, on tulevaisuudessa selkeä etu opiskelijoista kilpaillessa.

Smart Grid-teknologiat ovat vasta aikaisessa kehitysvaiheessa, ja Suwon & Seongcheol (2016) osoittaaakin tutkimuksessaan, että Smart Grid-järjestelmien on kehitettävä vielä, jotta ne ovat tarpeeksi kannattavia laajemmille markkinoille. Sama tutkimus osoittaa myös, että tällaisen älykkään järjestelmän käyttöönotto valtiollisella tasolla tarvitsee taakseen yleisen hyväksynnän kansalta, joka voi osoittautua haasteelliseksi, sillä järjestelmän tarvitsee toimiakseen kerätä dataa massiiviselta määrältä ihmisiä. Vaaditaan siis vielä paljon yhteisiä pelisääntöjä esimerkiksi valtion ja järjestelmää hallinnoivien yritysten välille, jotta järjestelmä voidaan harkita laajempaan käyttöön. Tästä huolimatta pidän aiheellisena olettamuksena, että koulutusjärjestelmien on syytä varautua ympäristöasenteiden kasvavaan merkitykseen kohderyhmänsä päätöksenteossa.

4.3 Opetus

Tähän asti tässä luvussa ollaan käsitelty lähinnä koulutusjärjestelmän hallinnollisiin ja infrastruktuurillisiin asioihin. IoT:sta voi kuitenkin olla merkittävää hyötyä myös varsinaisessa opetustilanteessa, ja sillä voidaan tässä luvussa käsiteltävän Gomez ym. (2013) tutkimuksen mukaan parantaa oppimistuloksia ainakin korkeakoulutasolla. Peruskoulutason opetuksessa IoT:n hyödyistä on vielä hyvin vähän tutkittua näyttöä, ja siksi pitäydyn tässä luvussa vain korkeakoulutasolla havaituissa hyödyissä.

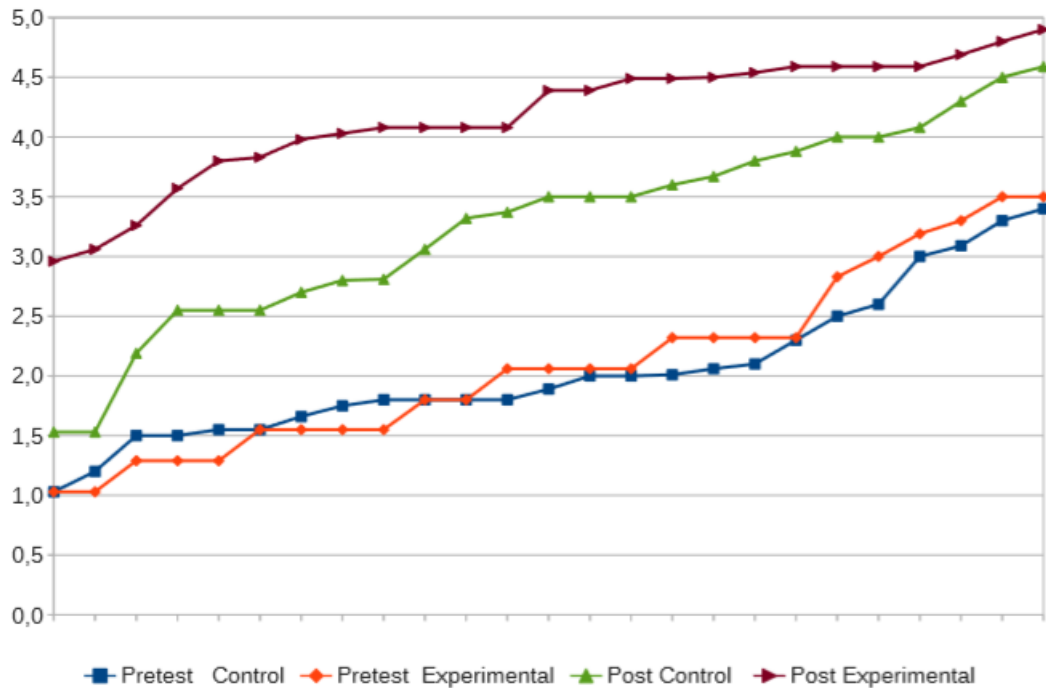
Esimerkki IoT:n hyödyistä opetuksen tukena on tutkijaryhmä Gomez ym. (2013) julkaisema tutkimus, jonka tulokset näyttävät lupaavilta. Gomez ym. (2013) esittävät

mallin jossa IoT teknologioita, tarkemmin NFC:tä ja QR-koodia käytetään tietokoneen komponenttien opetteluun korkeakoulutason kurssilla. Tutkijaryhmä järjesti kurssin kahdelle eri ryhmälle. Kontrolliryhmälle komponentteja opetettiin perinteisillä luennointimenetelmillä, ja testiryhmälle sovellettiin interaktiivista IoT opetustapaa. Molempien kurssien ryhmät koostuivat opiskelijoista, joilla oli vain vähän kokemusta tai ymmärrystä tietokoneen rakenteesta tai komponenteista. Molempien ryhmien taitotasoa mitattiin ennen opetusta ja sen jälkeen.

Testiryhmän opetus tapahtui laboratoriossa, jossa tietokoneen komponentit olivat aseteltuna pöydille ympäri huonetta. Jokainen komponentti varustettiin joko QR-koodilla tai NFC-tunnisteella. Kun oppilas saapuu luokkaan, hän skannaa tunnisteen joka rekisteröi harjoituksen aloitetuksi ja antaa oppilaalle tehtäviä, jotka hänen on suoritettava. Oppilas voi sitten kulkea ympäri harjoitustilaa tehden tehtäviä. Kun oppilas skannaa komponentista löytyvän NFC-tunnisteen tai QR-koodin, hänen puhelimensa ohjaa hänet verkkosivulle, joka sisältää tietoa kyseisestä komponentista. Tämän menetelmän tarkoituksena on kannustaa oppilasta aktiiviseen tiedonhakuun, ja tehdä tiedosta sellaista, että se on helposti jokaisen oppilaan saatavilla.

Kuvio 1 näyttää, että molempien ryhmien keskimääräinen taitotaso oli hyvin samanlainen ennen opetusta (sininen ja oranssi käyrä). Opetuksen jälkeen voidaan kuitenkin huomata, että testiryhmän (ruskea käyrä) keskimääräinen taso on selvästi kontrolliryhmää (vihreä käyrä) korkeampi. On tärkeää huomioida, että erityisesti heikosti pärjävien opiskelijoiden osuus pieneni merkittävästi, ja huonoin arvosana loppu-testistä oli 3, kun kontrolliryhmässä se oli 1,5. Tutkijaryhmä osoittaa analyysissään ryhmien välisen eron olevan merkittävä 95% varmuustasolla, kun analyysiin käytettiin W-testiä.

Tutkimuksen osoittamat hyödyt voivat selittyä oppilaiden aktiivisemmalla osallistumisella, keskittymiskyvyn paremmalla säilymisellä, ja avunsaannin helpottumisella oppimistilanteessa. Erityisesti oppilaat jotka pärjäävät tavallisesti heikommin, voivat sosiaalisen paineen alla pelätä avun kysymistä jonkin jäädessä epäselväksi, joka taas puolestaan kasvattaa oppilaan epävarmuutta ja tekee harjoittelun luovut-



Kuvio 2. IoT:n käytön vaikutukset tietokoneen komponenttien opetuksessa

tamisesta todennäköisempää (Akey 2006). Tätä voidaan ehkäistä integroimalla oppilaan henkilökohtainen mobiililaite opetukseen, jolta avun kysymisen kynnyks on luonnollisesti pienempi, kuin esimerkiksi hyvin pärjävältä kaverilta tai opettajalta.

5 Yhteenveto

Tässä tutkielmassa käsittelin kirjallisuuskatsauksen muodossa IoT:ta, ja sen tuomia uusia mahdollisuuksia ja haasteita. IoT on uusi ja valtava tekniikan ala, jonka kasvu jatkuu edelleen. Siksi yhdessä tutkielmassa onkin mahdotonta ottaa huomioon kaikki sen tuomat mahdollisuudet edes yhdestä — tässä tapauksessa koulutusjärjestelmän — näkökulmasta. Tutkielman tarkoituksena oli kuitenkin tuoda lukijan tietoisuuteen joitain esimerkkitapauksia, joita olemassa oleva tutkimus käsittelee. Tällä tutkimuksen tasolla on erittäin vaikeaa asettaa käsiteltyjä mahdollisuuksia ja haasteita minkäänlaiseen tärkeysjärjestykseen, sen selvittäminen jää tulevaisuuden tutkimusten tehtäväksi.

Tutkielma tuo esille lukuisia teknologioita ja periaatteita, joiden pohjalle IoT rakentuu, sekä antaa ideoita siitä, miten nämä tekijät vaikuttavat sen integrointiin koulutusjärjestelmässä. IoT:n merkittäviksi haasteiksi todettiin sen edelleen hyvin heikko tietoturva, sekä koulutusjärjestelmälle aiheutuvat lisäkustannukset. Nämä ovat aiheita jotka tulevat esiin hyvin usein mediassa ja tutkimuksessa, kun keskustellaan uuden tekniikan lisäämisestä koulutusjärjestelmään, ja siksi ne olivat luonnollisia valintoja tutkielman käsiteltäviksi. Olemassaolevaa tutkimusta analysoimalla voidaankin tehdä johtopäätös, että IoT saattaa olla vielä liian nuori teknologia laajamittaiseen käyttöön julkisella sektorilla. IoT ei kovinkaan useasti pysty vielä vastaamaan koulutusalan asettamiin turvallisuusvaatimuksiin, ja siksi on otettava vielä merkittäviä kehitysaskelita turvallisemman teknologian suuntaan.

Tähän astinen tutkimus osoittaa myös, että IoT:n avulla voidaan saavuttaa merkittäviä hyötyjä koulutussektorilla. Autonomiset, älykkäät ja kustannustehokkaat tunnistautumisjärjestelmät mahdollistavat turvallisemman ja käyttäjäystävällisemmän koulutusinfrastruktuurin. Älykkäät energianhallintajärjestelmät herättävät potentiaalisten korkeakouluopiskelijoiden mielenkiinnon, ja säästävät samalla ympäristöä ja koulutuksen budjettia.

Gomez ym. (2013) tekemä tutkimus osoitti myös, että IoT:n hyödyntämisestä ope-

tuskäytössä voidaan nähdä positiivisia signaaleja. Varsinainen opetus osoittautui kuitenkin lähteitä analysoidessa merkittävästi vähiten tutkituksi osa-alueeksi, ja se kaipaa ehdottomasti lisää tutkimusta. Erityisesti suomalaisessa koulutusjärjestelmässä tai peruskoulutason opetuksessa IoT:ta ei olla tutkittu juuri lainkaan. Tutkielman toivotaan herättävän lukijan mielenkiintoa tutkia näitä asioita enemmän, sillä lisätutkimus voi johtaa merkittäviin kehityksiin tulevaisuuden luokkahuoneissa.

Kirjallisuutta

- Abuarqoub, A., Abusaimah, H., Hammoudeh, M., Uliyan, D., Abu-Hashem, M. A., Murad, S., & Al-Fayez, F. 2017. *A Survey on Internet of Thing Enabled Smart Campus Applications*. In Proceedings of the International Conference on Future Networks and Distributed Systems. ACM.
- Akey, T. M. 2006. *School Context, Student Attitudes and Behavior, and Academic Achievement: An Exploratory Analysis*. MDRC.
- Arulogun, O. T., Olatunbosun, A., Fakolujo, O. A., Olaniyi, O. M. 2013. *RFID-based students attendance management system*. International Journal of Scientific & Engineering Research, 4(2), s. 1–9.
- Atzori, L., Iera, A., Morabito, G. 2010. *The Internet of Things: A survey* Computer Networks. Volume 54, Issue 15, s. 2787–2805
- Azamat, Z., Zhulduz, S., Rassim S., Zhazira K. 2017. *IoT smart campus review and implementation of IoT applications into education process of university*. International Conference on Electronics, Computer and Computation (ICECCO), 13
- Bagheri, M., Haghighi Mohaved, S. 2016. *The Effect of the Internet of Things (IoT) on Education Business Model*. International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). IEEE Computer Society, 12, s. 435–441
- Castellucia, C., Cunche, M., Le Métayer, D., Morel, V. 2018. *Enhancing Transparency and Consent in the IoT* 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) s. 116–119
- Cavoukian, A. 2012. *Near Field Communications* issa.org
- Gomez, J., Huete, J., Hoyos, O., Perez, L., Grigori, D. 2013. *Interaction System based on Internet of Things as Support for Education*. Procedia Computer Science. Volume 21, s. 132–139.
- Gubbi, J., Buyya, R., Marusic, J., Palaniswami, M. 2013. *Internet of Things (IoT): A vision, architectural elements, and future directions*. Future Generation Computer Systems. Volume 29, Issue 7, s. 1645–1660
- Hewlett Packard. 2014. *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack* <https://www8.hp.com/us/en/hp-news/press->

release.html?id=1744676#.VOTykPnF-ok

- Lee, I., Lee, K. 2015. *The Internet of Things (IoT): Applications, investments, and challenges for enterprises*. Business Horizons. Volume 58, Issue 4, s. 431–440
- Lund, D., Turner, V., MacGillivray, C., Morales, M. 2014. *Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand*. International Data Corporation.
- Mercer, C., & Leech, D. 2018. *Cost-Effective Wireless Microcontroller for Internet Connectivity of Open-Source Chemical Devices*.
- Mukherjee, A. 2015. *Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints* Proceedings of the IEEE. Volume 103, Issue 10, s. 1747–1761
- Riekkilä, E. 2015. *Suomalaisten ilmastonmuutosta koskevat asenteet ja niissä tapahtunut muutos vuosina 2000 ja 2010* Jyväskylän Yliopisto, Pro Gradu tutkielma
- Shah, S. H., Yaqoob, I. 2016. *A Survey: Internet of Things (IOT) Technologies, Applications and Challenges*. 2016 IEEE Smart Energy Grid Engineering (SEGE), s. 381–385
- Sinha, R. S., Wei, Y., & Hwang, S. H. 2017. *A survey on LPWA technology: LoRa and NB-IoT*. Ict Express, 3(1), s. 14–21.
- Suwon, K., Seongcheol, K. 2016. *A multi-criteria approach toward discovering killer IoT application in Korea*. Technological Forecasting and Social Change. 102, s. 143–155
- Tervasmäki, T., Tomperi, T. 2018 *Koulutuspolitiikan arvovalinnat ja suunta satavuotiaassa Suomessa*. niin&näin, 2/18.
- Van Der Meulen, R. 2015. *Gartner says 6.4 billion connected 'things' will be in use in 2016, up 30 percent from 2015*. <http://www.gartner.com/newsroom/id/3165317>
- Velasquez, N., Medina, C., Castro, D., Acosta, J. C., & Mendez, D. 2017. *Design and development of an IoT system prototype for outdoor tracking*. In Proceedings of the International Conference on Future Networks and Distributed Systems. ACM.
- Yewon, K. 2014. *S Korea's KT explores Internet of Things on campus* <https://asia.nikkei.com/Business/S-Korea-s-KT-explores-Internet-of-Things-on-campus>
- Zhang, Z., Cho, M., Wang, C., Hsu, C., Chen, C., Shieh, S. 2014. *IoT Security: Ongoing*

Challenges and Research Opportunities 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. s. 230–234.