

Janette Tukonen

LOHKOKETJUTEKNOLOGIAN ROOLI TERVEYSVAKUUTUSPETOSTEN TUNNISTAMISESSA JA EHKÄISYSSÄ

Johtamisen ja talouden tiedekunta

Kandidaatintutkielma

Joulukuu 2024

Ohjaaja: Jarna Pasanen

TIIVISTELMÄ

Janette Tukonen: Lohkoketjuteknologian rooli terveystakuutuspetosten tunnistamisessa ja ehkäisyssä

Kandidaatintutkielma

Tampereen yliopisto

Kauppatieteiden tutkinto-ohjelma

Joulukuu 2024

Vakuutuspetokset ovat merkittävä ongelma vakuutusosalalla, sillä ne aiheuttavat taloudellisia menetyksiä ja lisäävät vakuutusyhtiöiden hallinnollisia kustannuksia, mikä puolestaan nostaa rehellisten asiakkaiden vakuutusmaksuja. Terveystakuutusten kohdalla petokset voivat ilmetä esimerkiksi perusteettomina korvaushakemuksina tai tarpeettomina lääketieteellisinä toimenpiteinä. Koska terveydenhuolto käsittelee suuria määriä arkaluonteista tietoa, ala on erityisen altis vilpilliselle toiminnalle. Teknologian kehitys, erityisesti lohkoketjuteknologia, tarjoaa kuitenkin uusia mahdollisuuksia vähentää petollista toimintaa ja sen haitallisia seurauksia. Lohkoketjuteknologia voi luoda turvallisempia ja läpinäkyvämpiä järjestelmiä, jotka vähentävät väärinkäytöksiä ja tehostavat petosten havaitsemista.

Tutkimuksen tavoitteena oli selvittää, miten lohkoketjuteknologiaa voidaan hyödyntää terveystakuutuspetosten torjunnassa. Tutkimus keskittyi kahteen keskeiseen tutkimuskysymykseen: 1. Miten lohkoketjuteknologia voi edistää terveystakuutuspetosten tunnistamista ja ehkäisemistä? ja 2. Mitä tietoja teknologia hyödyntää petosten tunnistamisessa? Näiden avulla pyrittiin hahmottamaan, kuinka teknologia voisi edistää vakuutusalan prosesseja ja petosten ehkäisyä. Tutkimusmenetelmäksi valittiin systemaattinen kirjallisuuskatsaus ja tutkimus toteutettiin kvalitatiivisena tutkimuksena. Kirjallisuuskatsaukseen valittiin kansainvälistä vertaisarvioitua tutkimuskirjallisuutta, ja aineiston analyysi tehtiin aineistolähtöisellä sisällönanalyysillä.

Tutkimusten tulosten mukaan lohkoketjuteknologia voi vähentää petoksia erityisesti parantamalla tiedon turvallisuutta ja läpinäkyvyyttä. Tiedon muuttumattomuus estää vilpillisten tietojen muokkaamisen, ja hajautettu rakenne mahdollistaa tehokkaamman tiedon jakamisen eri toimijoiden välillä. Näin vakuutusyhtiöt voivat paremmin havaita epäilyttävää toimintaa ja vähentää petosriskiä. Teknologian tarjoama luotettava tietojärjestelmä auttaa varmistamaan, että tiedot säilyvät tarkkoina ja oikeellisinä. Lohkoketjuteknologia toimii myös alustana monelle muulle vakuutuspetostorjunnassa hyödynnetylle teknologialle ja mahdollistaa niiden tietoturvallisen käytön ja kehittämisen.

Toisen tutkimuskysymyksen osalta tulokset osoittivat, että lohkoketjuteknologia ja sen alustalla toimivat muut teknologiat hyödyntävät monia erilaisia tietoja, kuten vakuutusnottajan potilashistoriatietoja, maksuhistoriaa tai vahinkotapahtumaan liittyviä tietoja esimerkiksi annetusta hoidosta, tutkimustuloksista tai korvausvaatimuksen suuruudesta ja sisällöstä. Erityisesti epänormaalit käyttäytymismallit tai muut epätavalliset yhdistelmät tiedoissa olivat merkittävimpiä indikaattoreita petosten havaitsemisessa. Tutkimuksen tulosten perusteella voidaan todeta, että erityisesti tietojen varmistaminen eri osapuolilta ehkäisee petosten toteutumista.

Yhteenvetona voidaan todeta, että lohkoketjuteknologialla on potentiaalia parantaa vakuutusalan toimintaa ja vähentää terveystakuutuspetoksia. Se ei ainoastaan lisää tiedon luotettavuutta ja läpinäkyvyyttä, vaan tarjoaa myös mahdollisuuden tehokkaampaan petosten tunnistamiseen. Vaikka teknologian käyttöönotto vaatii edelleen kehitystyötä ja yhteistyötä eri toimijoiden välillä, sen mahdollisuudet ovat lupaavat niin taloudellisesti kuin yhteiskunnallisesti.

Avainsanat: terveystakuutus, vakuutuspetos, vakuutuspetostorjunta, lohkoketjuteknologia

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

- Ei
 Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot:

Chat GPT 4o
Microsoft Copilot
Scopus AI

Käyttötarkoitus:

Tutkimuksen suunnittelussa tekoälyä käytettiin ideoinnin tukena sekä lähteiden etsimiseen. Tekoälyä on käytetty yleiseen kielenhuoltoon, sanojen synonyymien etsimiseen ja aineiston kääntämiseen läpi koko tutkielman.

Osiot, joissa tekoälyä on käytetty:

Tekoälyä on käytetty kaikissa osioissa kielenhuollon tukena ja englannin kielen kääntämisessä.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

KUVIOLUETTELO

Kuvio 1. Teoreettinen viitekehys	12
---	----

TAULUKKOLUETTELO

Taulukko 1. Hakusanat ja hakusanalauseke	35
Taulukko 2. Seulontaprosessi ja sisällöllinen rajausta.....	36
Taulukko 3. Kirjallisuuskatsauksen artikkelit	37
Taulukko 4. Esimerkki pelkistämisestä.....	39
Taulukko 5. Esimerkki ryhmittelystä	39
Taulukko 6. Teknologioiden ryhmittely	40
Taulukko 7. Artikkeleissa hyödynnettyjen teknologioiden ryhmittely.....	42
Taulukko 8. Käytettyjen muuttujien ryhmittely	45

SISÄLLYSLUETTELO

1	Johdanto	6
1.1	Aihealueen esittely ja merkitys.....	6
1.2	Tutkimuksen tavoite ja tutkimuskysymykset.....	8
1.3	Tutkimusmenetelmät ja aineisto	10
1.4	Teoreettinen viitekehys ja keskeiset kirjallisuuslähteet	11
1.5	Keskeiset käsitteet	13
1.6	Aiempi tutkimus aiheesta.....	14
2	Petokset vakuutusosalalla	16
2.1	Vakuutuspetokset yleisesti	16
2.2	Vakuutuspetosten tyypit.....	17
2.3	Vakuutuspetosten tunnistaminen ja ehkäisy	19
2.4	Terveysvakuutuspetokset	21
2.4.1	Lakisääteinen- ja vapaaehtoinen terveysvakuutus	21
2.4.2	Terveysvakuutuspetosten tunnusmerkit	23
3	Lohkoketjuteknologia osana petosten tunnistamisprosessia	26
3.1	Lohkoketjuteknologian periaatteet ja toiminta	26
3.2	Lohkoketjuteknologia vakuutuspetosten tunnistamisessa	27
3.3	Lohkoketjuteknologian hyödyt verrattuna perinteisiin järjestelmiin	30
3.4	Lohkoketjuteknologian haasteet vakuutusosalalla	32
4	Lohkoketjuteknologian rooli terveysvakuutuspetosten tunnistamisessa	34
4.1	Tutkimusaineiston hankinta ja esittely.....	34
4.2	Tutkimusaineiston analyysi.....	38
4.3	Lohkoketjuteknologian rooli terveysvakuutuspetosten tunnistamisessa ja ehkäisyssä ...	40
4.4	Terveysvakuutuspetosten tunnistamisessa hyödynnettävät muuttujat	44
5	Johtopäätökset	48
5.1	Vastaukset tutkimuskysymyksiin.....	48
5.2	Tutkimuksen arviointi ja jatkotutkimusehdotukset	53
	Lähdeluettelo	55
	Kirjallisuuslähteet	55
	Verkkolähteet.....	61
	Oikeudelliset lähteet.....	63

1 JOHDANTO

1.1 Aihealueen esittely ja merkitys

Nykyteknologia luo uudenlaiset puitteet petoksille, mutta myös niiden tunnistamiselle. Kehittyvien teknologioiden myötä esimerkiksi tekoälyllä luodut väärennetyt dokumentit mahdollistavat yhä kehittyneempiä petoksia, joita ihmissilmällä voi olla vaikea havaita (PwC, 2023). Vakuutusala on erityisen altis petoksille, koska informaation epäsymmetria tekee vakuuttamisesta pitkälti sopimusosapuolten väliseen luottamukseen perustuvaa. Vakuutusyhtiöiden on voitava luottaa vakuutusnottajien vilpittömyyteen ja kyettävä arvioimaan riskin hinta annettujen tietojen perusteella. Vakuutuspetosten tunnistaminen onkin yksi vakuutusyhtiöiden keskeisimmistä tehtävistä, sillä tunnistamattomat petokset voivat aiheuttaa merkittäviä taloudellisia menetyksiä ja kasvattavat vakuutusmaksuja (Viaene & Dedene, 2004, 314–318). Tästä voidaan päätellä, että vakuutuspetokset eivät ole haitallisia ainoastaan vakuutusyhtiöille, vaan niiden vaikutukset ulottuvat yksilötasolta koko yhteiskuntaan. Vakuutuspetosten kitkeminen hyödyttääkin sekä vakuutusasiakkaita että vakuutusyhtiöitä, ja se on myös osa vakuutusyhtiöiden yhteiskuntavastuuta (Finanssiala, 2021; Insurance Europe, 2024).

Teknologian kehittyessä vakuutuspetokset ovat yhä digitaalisempia ja myös kansallisten rajojen ylittäviä, mikä tekee niiden torjunnasta entistä hankalampaa (Viaene & Dedene, 2004, 317). Insurance European (2024) vuosittaisen raportin mukaan noin 10 % Euroopan vakuutuskorvauksista liittyy petoksiin. Pelkästään Suomessa vuonna 2022 vakuutusyhtiöillä oli 2500 epäselvää vahinkoa tutkinnassa. Näiden epäselvien vahinkojen arvo oli noin 147 miljoonaa euroa (Finanssiala, 2023). Lisäksi Finanssiala ry:n tekemässä haastattelussa noin 16 % vastaajista myönsi tuntevansa jonkun vakuutuspetoksen tehneen henkilön ja 16 % vastaajista oli myös täysin tai osittain samaa mieltä siitä, että on hyväksyttävää liioitella vahingon määrää korvaushakemuksessa (Finanssiala, 2022). Vakuutuspetokset koskevat kaikkia vakuutuslajeja: henki-, omaisuus- ja terveystakuutuksia. Tässä tutkielmassa keskitytään erityisesti terveystakuutuspetoksiin.

Terveysvakuutus on viime aikoina kasvattanut suosiotaan Suomessa. Yle:n (2021) mukaan jo yli 1,2 miljoonalla suomalaisella on terveysvakuutus. Valitettavasti myös terveysvakuutuspetokset ovat kasvussa. Rahallinen menoerä terveydenhuollossa on merkittävä johtuen sektorin koosta ja sen sisällä liikkuvista rahasummista. Rahan suuri volyyymi ja isot massat arkaluontoisia henkilötietoja tekevät terveysvakuutuspetokset houkuttelevaksi rikollisille. (Duman, 2017.) Tällainen vilpillinen toiminta on taakaksi jo valmiiksi hauraalle terveydenhuoltojärjestelmälle, sillä se nostaa terveysvakuutusmaksuja ja kuormittaa vakuutusyhtiötä. Terveysvakuutuspetoksia havaitaan sekä yksilötasolla että terveydenhuollon edustajien toimesta. Yksilötasolla tehdään esimerkiksi identiteettivarkauksia, jolloin tarkoituksena on hyötyä toisen henkilön vakuutusturvasta. Toinen yksilötasolla tunnistettu petos on oirekuvan väärentäminen ja korvaukseen oikeuttavien reseptilääkkeiden myyminen. Terveydenhuollon puolesta voidaan toimia petollisesti esimerkiksi hoitoon tarpeettomien välineiden tai testien ylimääräisellä laskuttamisella (Li ym., 2022).

Petosten tunnistamiseksi olisi tärkeää tarkastella terveystietoja systemaattisesti. Terveystietojen tarkasteleminen yksilötasolla on kuitenkin huomattavan kuormittavaa ja kallista vakuutusyhtiön näkökulmasta. Tämän vuoksi teknologiaa on alettu hyödyntää petosten havaitsemisessa. Lohkoketjuteknologia on yksi uusimmista teknologioista ja sen potentiaali petosten tunnistamisessa on havaittu. Lohkoketjuteknologia perustuu pääasiassa hajautettuun vertaisverkkoon, vertaisverkon konsensukseen ja kryptografiaan (Saldamli, 2020; Treleaven et al., 2017; Murray, 2019). Lohkoketjuteknologia tarjoaa toimintaperiaatteellaan mahdollisuuden käsitellä tietoja luotettavasti ja läpinäkyvästi, mikä luo hyvän lähtökohdan datan käsittelyyn ja petosten tunnistamiseen (Saldamli, 2020). Lohkoketjuteknologia soveltuu hyvin esimerkiksi juuri arkaluontoisten terveystietojen käsittelyyn sen turvallisuuden ja eheyden vuoksi (Zhang ym., 2022).

Tämän tutkielman tavoitteena on kartoittaa lohkoketjuteknologian roolia terveysvakuutuspetosten tunnistamisessa ja ehkäisyssä. Aiheen tutkiminen on erityisen tärkeää, sillä vakuutuspetokset aiheuttavat huomattavia kustannuksia paitsi vakuutusyhtiöille, myös vilpittömille asiakkaille sekä välillisesti myös koko yhteiskunnalle. Viaenen & Dedenen (2004) mukaan vilpillisten korvausvaatimusten maksaminen tuottaa

vakuutusyhtiöille kasvavaa korvausmenoa, mikä puolestaan kasvattaa vakuutusmaksuja. Vakuutuspetosten havaitseminen kasvattaa myös tutkinnan kuluja. Tämä vilpillinen käytös rasittaa vakuutusyhtiöitä, mutta ennen kaikkea vakuutusasiakkaita, jotka joutuvat petoksien aiheuttamien kulujen vuoksi maksamaan suurempia vakuutusmaksuja. Laajemmassa mittakaavassa vakuutuspetokset vaikuttavat koko yhteiskuntaan, sillä petoksista saaduilla varoilla rahoitetaan usein myös muuta rikollista toimintaa, kuten järjestäytyntä rikollisuutta (IAIS, 2011).

Uusia ratkaisuja petosten havaitsemiseen kehitetään jatkuvasti, sillä suuri osa petoksista jää edelleen tunnistamatta (Insurance Europe, 2013). Vaikka lohkoketjuteknologia kehitettiin jo vuonna 2008 bitcoinin transaktioita varten, sen potentiaali vakuutusosalalla on tunnistettu vasta hiljattain. Integroimalla lohkoketjuteknologia vakuutuspetosten tunnistamiseen voidaan potentiaalisesti säästää merkittäviä summia sekä vakuutusasiakkailta että yhtiöiltä (Roriz & Pereira, 2019). Ajankohtainen ilmiö on sairaudenhoitokulujen väärentäminen ja hakeminen terveystakuutuksesta. Harmillisesti monet näistä petoksista jäävät kuitenkin huomaamatta ja siitä maksaa rehellinen vakuutusasiakas (Finanssiala, 2023; Hyman, 2001). Tutkielman aihe on edelleen varsin tuore ja tutkimusta on toistaiseksi vähän, mutta kiinnostus kasvaa nopeasti. On viitteitä siitä, että lohkoketjuteknologia tulee olemaan merkittävä muutostekijä vakuutusosalalla tulevaisuudessa, minkä vuoksi tätä aihetta on tarpeen tutkia tarkemmin.

1.2 Tutkimuksen tavoite ja tutkimuskysymykset

Tutkimuksen tavoitteena on kartoittaa lohkoketjuteknologian potentiaalia terveystakuutuspetosten tunnistamisessa. Tutkimuksessa pyritään luokittelemaan erilaiset terveystakuutuspetoslajit ja arvioimaan, kuinka hyvin lohkoketjuteknologia soveltuu näiden petosten havaitsemiseen. Lisäksi tavoitteena on tuottaa konkreettisia tuloksia eri teknologioiden toimivuudesta ja tehokkuudesta tässä kontekstissa.

Tutkimuskysymykset ovat seuraavat:

1. Miten lohkoketjuteknologia voi edistää terveysvakuutuspetosten tunnistamista ja ehkäisemistä?
2. Mitä tietoja lohkoketjuteknologia hyödyntää terveysvakuutuspetosten tunnistamisessa?

Ensimmäinen tutkimuskysymys lähestyy aihetta yleisemmästä näkökulmasta eli kartoittaa, millä tavoin lohkoketjuteknologialla voidaan vähentää petoksia ja niiden haitallisia seurauksia. Tutkimuksessa pyritään rajaamaan lohkoketjuteknologian käyttöönoton taloudelliset kustannukset ja teknologian integroinnin muut haasteet pois arvioinnista. Tässä tutkielmassa siis ikään kuin oletetaan, että muut tekijät eivät rajoittaisi teknologian lisäämistä vakuutuspetostutkinnan liiketoimintoon, tai ainakaan tällaisia tekijöitä ei huomioida.

Toinen tutkimuskysymys konkretisoi, miten lohkoketjuteknologiaa voidaan hyödyntää petosten tunnistamisessa, ja pyrkii selvittämään, millaisia tietoja teknologia käyttää toiminnassaan. Tutkimuksen tarkoitus ei ole keskittyä teknologiaan syvällisesti eikä perehtyä sen konkreettiseen toteutukseen, vaan tuoda esille sitä, millaiset henkilöihin tai ilmoitettuun vahinkoon liittyvät muuttujat ja tiedot otetaan huomioon terveysvakuutuspetosta tunnistettaessa.

Tutkielma tehdään yleisesti koskien terveysvakuutusta. Tutkimusta ei rajata vapaaehtoiseen tai lakisääteiseen vakuutukseen, sillä vakuutuksen lakisääteisyys riippuu kansallisen tason lainsäädännöstä, johon tutkimuksessa ei oteta kantaa. Tutkimuksen tarkoituksena ei myöskään ole analysoida terveysvakuutuksen lakisääteisyyttä tai sen muita ominaisuuksia. Tutkimus ei rajaudu maantieteelliseen alueeseen, sillä aihetta on mielekkäämpää tutkia globaalilla tasolla, koska vakuutuspetokset ovat yleinen ongelma, jota havaitaan ympäri maailmaa samankaltaisena ilmiönä. Tavoitteena on tutkia nimenomaan terveysvakuutuspetoksen yleisimpiä tunnusmerkkejä sekä petosten tunnistamista lohkoketjuteknologiaa hyödyntäen.

1.3 Tutkimusmenetelmät ja aineisto

Tämä kandidaatintutkielma tehdään kvalitatiivisena tutkimuksena. Kvalitatiivisen eli laadullisen tutkimuksen ideana on ymmärtää ja kuvata tutkittavan ilmiön teoriaa (Saaranen-Kauppinen & Puusniekka, 2009). Tutkimukseen valittiin kvalitatiivinen menetelmä, jotta tutkimuksen teknologinen luonne saa ymmärrettävämmän muodon. Kvalitatiivinen tutkimusmenetelmä tarjoaa erityisen hyödyllisiä työkaluja silloin, kun on tavoitteena syventyä ja ymmärtää ilmiöiden taustalla olevia mekanismeja ja konteksteja. Terveysvakuutuspetosten tunnistaminen lohkoketjuteknologialla on itsessään monimutkainen kokonaisuus, jossa tarvitaan sekä teknologian toiminnan että sen tuomien haasteiden tarkkaa analyysia ja syvää ymmärrystä. Kvalitatiivisella lähestymistavalla voidaan oppia tunnistamaan terveysturvakuutuspetoksen tunnuspiirteet ja ymmärtää, kuinka petoksia voidaan kitkeä konkreettisesti lohkoketjuteknologiaa hyödyntäen.

Tutkimus tehdään systemaattisena kirjallisuuskatsauksena. Aiheen tuoreus ja kompleksisuus tekisivät esimerkiksi haastattelu- tai kyselytutkimuksen toteuttamisesta haastavan, koska alan todellisia asiantuntijoita on etenkin Suomessa vielä verrattain vähän. Aiheesta on kuitenkin jo julkaistu korkeatasoisia tieteellisiä artikkeleita, joiden pohjalta tehty kirjallisuuskatsaus antaa mahdollisimman kattavan ja luotettavan kuvan ilmiöstä. Myös Finkin (2019) mukaan systemaattinen kirjallisuuskatsaus auttaa kartoittamaan ja syntetisoimaan olemassa olevan tiedon, mikä antaa kattavan kuvan siitä, mitä aiheesta jo tiedetään ja missä on vielä tutkimusaukkoja. Lohkoketjuteknologia ja sen soveltaminen terveysturvakuutuspetosten havaitsemiseen on suhteellisen uusi ja nopeasti kehittyvä tutkimusalue, jonka vuoksi kattava systemaattinen kirjallisuuskatsaus auttaa ymmärtämään sekä tutkimuksen nykyiset puitteet että uudet tutkimustarpeet.

Salmisen (2011) mukaan systemaattisen kirjallisuuskatsauksen täytyy noudattaa tiettyjä kriteerejä. Menetelmälle ominaista on nimensä mukaan lähteiden systemaattisuus, loogisuus ja yhteensopivuus. Systemaattinen kirjallisuuskatsaus noudattaa tarkkoja ja läpinäkyviä menetelmiä, mikä lisää tutkimuksen luotettavuutta ja validiteettia. Tämän metodin yksi parhaimmista puolista on tehokas ja johdonmukainen tapa tiivistää

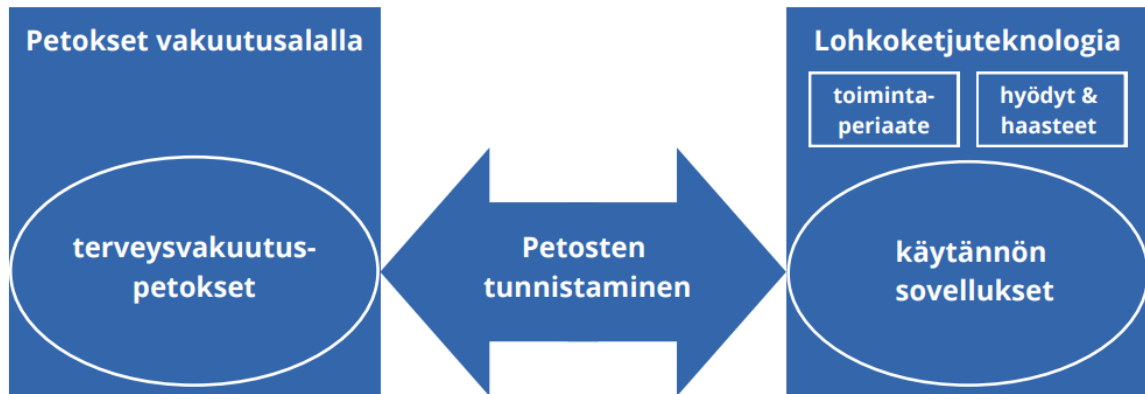
tutkimustuloksia yhteen. Tutkimustulosten vertailu ja nitominen yhteen lisää toisaalta myös tutkimusten uskottavuutta. (Salminen, 2011, 9–11.)

Systemaattisen kirjallisuuskatsauksen kriteerein tutkimukseen valikoitui lopulta kahdeksan vertaisarvioitua tieteellistä lähdeä. Tiedonhaussa käytettiin Tampereen yliopiston Andor-tietokantaa. Haku toteutettiin syyskuussa 2024. Aineistoa valitessa huomattiin kotimaisen tutkimuksen puute, joten tutkimuksessa käytettiin aineistona vain englanninkielisiä lähteitä. Aihealue on varsin uusi, joten julkaisuvuotta ei rajattu erikseen. Tutkimuksen konkreettinen toteutus, eli aineiston valinta, sisältö ja analyysimenetelmät kuvataan tarkemmin luvussa 4.

1.4 Teoreettinen viitekehys ja keskeiset kirjallisuuslähteet

Tämän tutkielman teoriapohjaa havainnollistetaan kuviossa 1 esitetyssä teoreettisessa viitekehyksessä. Viitekehyksessä kuvataan terveystieteen vakuutuspetokset vakuutuspetosten kontekstissa. Tutkielman ensimmäinen teoriapohja on vahvasti vakuutustieteellinen ja käsittelee vakuutuspetoksiin (ominaisuudet ja tyypit) sekä niiden tunnistamiseen liittyvää tietoa. Lisäksi teoriassa esitellään tarkemmin terveystieteen vakuuttamista petosten kontekstina.

Toinen teoriapohja on lohkoketjuteknologiassa. Toisessa teoriaosiossa esitelläänkin lohkoketjuteknologian käytännön sovelluksia, niiden toimintaperiaatteita, hyötyjä ja haasteita. Lohkoketjuteknologian yksi sovelluksista on sen käyttömahdollisuudet vakuutuspetosten torjunnassa tämä linkittää tutkielman kaksi teoriapohjaa yhteen. Lohkoketjuteknologian toimintaperiaate ja sen ainutlaatuiset ominaisuudet ovat syy, miksi sen ajatellaan sopivan hyvin vakuutuspetostorjuntaan.



Kuvio 1. Teoreettinen viitekehys

Tutkielman rakenne on seuraava: Johdannossa esitellään tutkielman aihe, tavoite, tutkimuskysymykset, tutkimusmenetelmät ja teoreettinen viitekehys. Ensimmäinen teorialuku (luku 2) käsittelee vakuutuspetoksia yleisellä tasolla ja sisältää alaluvun, jossa syvennytään erityisesti terveysvakuutuspetoksiin, jotka ovat tutkimuksen kannalta keskeinen aihe. Tämän lisäksi luvussa 2 käsitellään vakuutuspetosten tunnistamisprosessia. Toisessa teorialuvussa (luku 3) käsitellään yleisemmin lohkoketjuteknologian toimintaperiaatetta, sen roolia petostorjunnassa sekä teknologian hyötyjä ja haasteita.

Luku 4 muodostaa tutkielman empiirisen osuuden. Luvussa 4 käydään aluksi läpi tutkimusaineiston hankinta sekä sen esittely ja analyysi. Tämän jälkeen esitellään tutkimustulokset, jotka perustuvat systemaattiseen kirjallisuuskatsaukseen. Ensin esitellään lohkoketjuteknologian roolia terveysvakuutuspetosten tunnistamisessa ja sen jälkeen kootaan yhteen muuttujat, joita teknologia hyödyntää petosten tunnistamisessa. Luvussa 5 vastataan tutkimukselle asetettuihin tutkimuskysymyksiin sekä arvioidaan tutkimuksen onnistumista ja mahdollisia rajoitteita. Tämän lisäksi luvussa käsitellään tutkimuksen aikana esiin nousseita tutkimusaukkoja aiheeseen liittyen ja tuodaan esille jatkotutkimusehdotukset.

1.5 Keskeiset käsitteet

Tässä alaluvussa käsitellään keskeisiä käsitteitä, jotka auttavat lukijaa ymmärtämään tutkittavaa aihetta. Näiden käsitteiden määrittely luo aihepiirin kehyksen ja auttaa hahmottamaan tutkimuksen olennaisia osatekijöitä.

Vakuuttaminen perustuu riskinalaisten yksilöiden eli vakuutuksenottajien ja vahinkojen jakamiseen erikoistuneen vakuutuslaitoksen eli vakuutuksenantajan väliseen sopimukseen. Vakuuttamisen peruserä perustuu *suurten lukujen lakiin*, joka tarkoittaa riskien ja vahinkokustannuksien jakamista vakuutuksenottajien kesken. Sopimuksen tarkoitus on, että riskin toteutuessa vakuutuksenantaja korvaa vakuutuksenottajalle sattuneen vahingon. (Rantala & Kivisaari, 2020, 56–57, 80).

Terveysvakuutus on vapaaehtoinen vakuutus, joka täydentää lakisääteistä sairausvakuutusta ja tarjoaa räätälöitävissä olevan turvan, joka kattaa sairauden tai tapaturmien aiheuttamia kustannuksia. (Pohjola Vakuutus, n.d.). Suomessa kaikilla vakituisesti asuvilla on lakisääteinen sairausvakuutus, joka korvaa sairaanhoidosta aiheutuneita kustannuksia. Tämä sairausvakuutus rahoitetaan työnantajien, työntekijöiden ja valtion toimesta. (Jokela ym., 2021, 38.)

Suomen rikoslain mukaan *vakuutuspetos* tarkoittaa tekoja, joilla pyritään hankkimaan itselle tai toiselle oikeudettomasti vakuutuskorvausta, esimerkiksi sytyttämällä tuleen palovakuutettu omaisuus (RL 36:4 §). Toisaalta rikoslain 36:1 § mukaan petos on toisen erehdyttämistä taloudellisen hyödyn saamiseksi. Näin ollen myös vakuutuspetokset täyttävät usein petoksen tunnusmerkit ja ovat siten rikoslain mukaan rangaistavia.

Lohkoketjuteknologia on hajautettu järjestelmä, jossa vertaisverkon jäsenien täytyy saavuttaa yhteisymmärrys eli konsensus hyväksyäkseen lohkoihin lisättävät tiedot. Tiedot tallennetaan pääkirjaan, joka sisältää kaikki suoritettut ja vahvistetut tapahtumat. Nämä tiedot jaetaan kaikkien osapuolten paikallisiin kopioihin lohkoketjusta, mikä tekee järjestelmästä läpinäkyvän ja luotettavan. Lohkoketjuteknologia toimii täysin hajautetun vertaisverkon avulla, eikä se tarvitse kolmatta osapuolta välikädeksi. (Yli-Huumo ym., 2016.)

1.6 Aiempi tutkimus aiheesta

Tutkielman aihe liittyy terveysturvakuutuspetosten havaitsemiseen lohkoketjuteknologialla. Suomenkielistä tutkimusta aiheeseen liittyen on hyvin vähän. Yleisemmin vakuutuspetoksiin liittyvää tutkimusta on tehnyt mm. Timonen (2020) opinnäytetyössään “Tutkintaan johtaneet omaisuusvahingot Suomessa vuosina 2008–2018”, Kuusisto (2021) kandidaatintutkielmassaan “Vilppiin ja petoksiin liittyvien vahinkotapausten ratkaisut vakuutuslautakunnassa”, Saajos (2020) opinnäytetyössään “Petokset vakuutuslalla” ja Paaso (2017) maisterintutkielmassaan “Petos ja vakuutuskorvaukset”.

Lähimpänä aihetta on Jyrinsalon (2024) kandidaatintutkielma “Ajoneuvovakuutuspetosten havaitseminen teknologian avulla”, jossa tutkitaan kirjallisuuskatsauksen muodossa tietyn vakuutuslajin petosten tunnistamista teknologian avulla. Toisin kuin Jyrinsalon kandidaatintutkielmassa tässä tutkimuksessa pyritään tarkastelemaan eri vakuutuslajien petoksia ja erityisesti lohkoketjuteknologiaa hyödyntäviä menetelmiä. Aiempiin terveysturvakuutuspetoksia käsitteleviin tutkimuksiin tutustuttaessa havaittiin, että vakuutuspetoksista on olemassa runsaasti tutkimusta, mutta terveysturvakuutuspetoksiin liittyviä artikkeleita ja opinnäytetöitä on niukasti. Terveysturvakuutuspetokset eroavat myös muista vakuutuslajeista, sillä niillä on omat tyypilliset lajikohtaiset tunnuspiirteensä. Lisäksi lohkoketjuteknologian soveltaminen vakuutuspetosten havaitsemiseen on vielä tutkimaton alue suomenkielisissä tieteellisissä julkaisuissa ja opinnäytetöissä. Tämä tekee tutkimuksesta ajankohtaisen ja tarpeellisen, sillä se avaa uuden näkökulman ja laajentaa ymmärrystä lohkoketjuteknologian potentiaalista erityisesti terveysturvakuutuspetosten ehkäisyssä.

Kansainvälisesti aihetta on kuitenkin tutkittu enemmän, ja esimerkiksi englanniksi löytyy useita vertaisarvioituja tieteellisiä tutkimuksia. Yleisemmin vakuutuspetosten tunnistamisesta teknologialla löytyi paljon erilaisia tieteellisiä tutkimuksia, muun muassa: Tumminello ym. (2023) “Insurance fraud detection: A statistically validated network approach”, Gomes ym. (2021) “Insurance fraud detection with unsupervised deep learning” ja Aslam ym. (2022) “Insurance fraud detection: Evidence from artificial intelligence and machine learning”. Tutkimusta on kuitenkin tehty myös aiheeseen läheisesti liittyvistä

aiheista. Esimerkiksi McGhin ym. (2019) ovat tutkineet lohkoketjun sovelluksia terveydenhuollon kontekstissa. Tutkimuksessaan he punnitsivat lohkoketjun erilaisten soveltamisalojen tuomia mahdollisuuksia ja haasteita. Artikkelissaan he käsittelevät erityisesti älykkäitä sopimuksia, petosten tunnistamista ja identiteetin varmentamista.

Cai ja Zhu (2016) tutkivat lohkoketjuteknologiaa niin sanotuissa mainejärjestelmissä (engl. the reputation system). He keskittyivät tutkimuksessaan arviointipetoksiin (engl. *rating fraud*) ja niiden vaikutuksiin kilpailijoiden aseman heikentämisessä. Tutkimuksessa erotellaan subjektiiviset, mielipideperusteiset petokset ja objektiiviset, faktaperusteiset petokset. Tulokset osoittavat lohkoketjuteknologian olevan tehokas objektiivisten petosten tunnistamisessa. Toisaalta subjektiivisten petosten tunnistaminen on huomattavasti hankalampaa.

Tämä tutkimus eroaa aikaisemmista siinä, että tutkimuksessa käsitellään nimenomaan vakuutuspetoksia terveysvakuutuspetosten näkökulmasta ja tutkitaan lohkoketjuteknologian roolia tunnistamisprosessissa. Aiheesta löytyviä tutkimuksia on vasta vähän, eikä niitä ole saatavilla suomen kielellä. Tutkielma eroaa myös tutkimusmenetelmällisesti monista aiemmista; sen tarkoituksena on koota yhteen ja analysoida aiempia relevantteja tieteellisiä tutkimuksia aiheesta. Kirjallisuuskatsauksen vahvuutena on sen kyky tuottaa järjestelmällisesti ja kattavasti yhteenvetoa jo tutkitusta tiedosta, minkä avulla saavutetaan monipuolinen ja syvä ymmärrys aiheesta. Lisäksi katsauksen avulla voidaan tunnistaa tutkimuksen aukkoja ja tiivistää jo olemassa olevaa tietoa kadottamatta tärkeimpiä osia.

2 PETOKSET VAKUUTUSALALLA

2.1 Vakuutuspetokset yleisesti

Vakuutuspetokset ovat monimuotoisia ja niitä tehdään monista eri syistä. IAIS:n (2011) mukaan näitä petoksia tekevät vakuutuksenottajat, ammattimaiset petoksenteelijät, yhtiön henkilöstö sekä muut sidosryhmät. Vakuutuspetos voidaan määritellä tietoisesti tekaistun tai väärennetyn korvausvaatimuksen esittämisenä, korvausvaatimuksen liioitteluna tai muiden tarpeettomien osien lisäämisenä vaatimukseen. Vakuutuspetos voi olla myös muulla tavalla epärehellistä toimintaa. (Rantala & Kivisaari, 2020, 267—268.) Insurance Europen (2019) mukaan petos voi tapahtua vakuutuselinkaaren missä vaiheessa tahansa, mutta useimmiten vilppiä yritetään korvausta hakiessa.

Vakuutuspetokset ovat merkittävä ongelma ympäri maailman ja Finanssialan (2023) mukaan pelkästään Suomessa vuonna 2022 vakuutusyhtiöillä oli 2500 epäselvää vahinkoa tutkinnassa. Yhteensä näiden epäselvien vahinkojen arvo oli noin 147 miljoonaa euroa. Finanssialan (2018) mukaan ajoneuvovakuutuspetoksia, jotka liittyvät autoihin, moottoripyöriin ja veneisiin, on kappalemääräisesti eniten. Näissä vakuutettu saattaa liioitella omaisuuden arvoa tai väittää, että varkaus on tapahtunut, vaikka omaisuus on edelleen vakuutetun hallussa. Toisaalta suurimmat perusteettomat korvaussummat syntyvät henkilövahinkopetoksista. Tyypillisessä henkilövahinkopetoksessa vakuutettu voi väittää olevansa työkyvytön. Vakuutuspetokset voivat ilmetä monella eri tavalla ja eri vakuutuslajeissa, mutta niillä on yhteinen piirre: ne aiheuttavat merkittävää taloudellista haittaa niin vakuutusyhtiöille kuin asiakkaille.

Petosten taustalla olevat syyt voidaan jakaa kolmeen päätekijään: motiivi, järkiperaistaminen ja tilaisuus. Useimmiten petosten taustalla on taloudellinen motiivi, vaikka motiivit voivatkin vaihdella suuresti. Järkiperaistaminen on mielen prosessi, jossa petos oikeutetaan itselle. Monet petoksen tekijät ajattelevat, että myös muut tekevät niin tai että vakuutuspetokset ovat niin sanottuja uhrittomia rikoksia. Petoksen tekemiseen vaaditaan myös sopiva tilaisuus, jossa tekijä olettaa kiinnijäämisen riskin olevan pieni. (IAIS,

2011, 4–5.) Monille ihmisille kyseinen sopiva tilaisuus voi olla erityisen houkutteleva, vaikka heillä ei olisikaan aiempaa rikollista taustaa. Tällaisissa tilanteissa pätee osuvasti sananlasku ”*tilaisuus tekee varkaan*” (Felson & Clarke, 1998). Vakuutusyhtiöiden onkin tärkeää tunnistaa nämä tilaisuudet ja yrittää kehittää yhä parempia työkaluja petosten havaitsemiseksi ja ennaltaehkäisemiseksi.

Vaikka monet vakuutuspetoksen tekijät eivät koe petoksella olevan varsinaista uhria, rehelliset vakuutusasiakkaat ja vakuutusyhtiöt kärsivät merkittävästi petosten seurauksista (Dean, 2004; Finanssiala, 2023). Tennysonin (2008) mukaan kuluttajien keskuudessa vakuutuspetokset ovat varsin hyväksyttäviä, vaikkakin hyväksymisaste on viime vuosina laskenut. Erityisesti korvausvaatimusten liioittelua pidetään petosmuodoista hyväksyttävimpänä. On kuitenkin huomionarvoista, että tutkimuksen vastaukset muuttuivat jonkin verran, kun vakuutetuille selitettiin, miten vakuutuspetokset vaikuttavat myös heihin itseensä, esimerkiksi korkeampien vakuutusmaksujen ja omavastuiden muodossa. (Tennyson, 2008, 1995–1999). Vakuutustiedon lisääminen näyttää vähentävän petosten hyväksyttävyyttä ja sitä kautta niiden yleisyyttä. Vakuutustieto parantaa asenteita vakuutusyhtiöitä kohtaan, mikä puolestaan lisää luottamusta asiakkaan ja yhtiön välillä. Vakuutustiedon kehittäminen voi myös vahvistaa luottamusta koko vakuutusjärjestelmään ja toimia keinona vakuutuspetosten torjumisessa.

2.2 Vakuutuspetosten tyypit

Vakuutuspetoksia toteutetaan vaihtelevilla motiiveilla ja yhteiskuntaryhmästä riippumatta. Erityisesti talouden taantuma ja yhteiskunnan epävarmuus näkyy vakuutuspetostilastoissa. Henkilövahinkopetoksissa näkyy erityisesti julkisen terveydenhuollon vaikeudet, ja entistä pidemmät jonot antavat ihmisille motiivin antaa vakuutusyhtiölle virheellisiä tietoja sekä pyrkiä perusteettomasti siirtymään yksityiselle puolelle vakuutuksen kautta. (Niemelä, 2024.)

Vakuutuspetoksia luokitellaan muun muassa sen mukaan, tapahtuiko vahinkotapahtuma vai ei. Mikäli vahinkotapahtuma on tapahtunut ja korvausvaatimusta liioitellaan tai vääristellään,

on kyseessä opportunistinen petos, eli petos, joka tehdään sopivan tilaisuuden tullen. Mikäli vahinkotapahtumaa ei ole käynyt, mutta korvauksia lähdetään hakemaan, on silloin kyseessä suunniteltu petos. (Tennyson, 2008, 1183.) Vakuutuspetokset voidaan jakaa vielä niin sanotusti koviksi ja pehmeiksi petoksiksi. Suunnitellut petokset ovat usein kovia petoksia, jotka ovat selkeästi rikollisia ja niistä on tarpeeksi selkää näyttöä ja rikollisia ominaisuuksia, kuten taloudellinen hyöty ja lain rikkominen. Nämä tunnusmerkit pitää vakuutuspetoksessa olla, jotta se voitaisiin viedä oikeuteen. Opportunistinen petos on usein luokiteltu pehmeäksi petokseksi, ja monesti sekin on rikollista, mutta monesti selkeää näyttöä petoksesta ei ole, jolloin pehmeät petokset muodostuvat enemmän vakuutusyhtiön hallintatehtäväksi taaten reilun korvauskäsittelyn. (Tennyson, 2008, 1183; Kilroy 2024)

Vakuutuspetokset jaetaan myös sisäisiin ja ulkoisiin petoksiin. Sisäiset petokset tehdään vakuutusyhtiön sisäpiiriläisen, kuten työntekijän, vakuutuksenvälittäjän tai johtajan, toimesta. Sisäinen vakuutuspetos voi olla esimerkiksi kavallus tai vakuutusten myyminen ilman lupaa. (Viane & Dedene, 2004, 315.) Petos voi tapahtua myös sisäisen ja ulkoisen tekijän yhteistyönä. Esimerkkinä tästä on tapaus, jossa vahinkoasiantuntija ja kauneudenhoitoalan yrittäjä tekivät yhteistyötä. Yrittäjä ilmoitti vakuutusyhtiön työntekijän ehdotuksesta keksittyjä vahinkoja, jotka vahinkoasiantuntija käsitteli itse. Saatuaan vakuutuskorvaukset, yrittäjä luovutti osan niistä vahinkoasiantuntijalle. (Kerkelä, 2024.)

Ulkoinen petos taas on useimmiten vakuutuksenottajan tai muun ulkoisen henkilön tekemä. Kyseessä voi olla esimerkiksi väärin tietojen antaminen tai tekaistujen korvausvaatimusten laatiminen. (Viaene & Dedene, 2004, 315.) Väärin tietojen antaminen rikkoo tiedonantovelvollisuutta, josta määrätään Suomen vakuutuslakissa. Vakuutuslakien 22§ mukaan tiedonantovelvollisuudella tarkoitetaan seuraavaa: ”vakuutuksenottajan ja vakuutetun tulee ennen vakuutuksen myöntämistä antaa oikeat ja täydelliset vastaukset vakuutuksenantajan esittämiin kysymyksiin, joilla voi olla merkitystä vakuutuksenantajan vastuun arvioimisen kannalta” (VakSL 22§). Tiedonantovelvollisuuden rikkominen johtaa käytännössä siihen, että vakuutusyhtiö ei kykene arvioimaan riskiä oikein, mikä voi johtaa väärinhinnoitteluun tai sellaisen riskin vakuuttamiseen, jota normaalisti ei vakuutettaisi. Näin ollen vakuutuksenottaja voi hyötyä saamalla perusteettomasti paremman vakuutuksen ehdoiltaan tai hinnaltaan. (Viaene & Dedene, 2004, 316.)

2.3 Vakuutuspetosten tunnistaminen ja ehkäisy

Vakuutuspetosten ehkäisemiseksi on ensiarvoisen tärkeää ymmärtää, miksi vakuutuspetoksia tehdään. Tämä tieto auttaa kehittämään tehokkaampia ennaltaehkäisykeinoja ja tukee vakuutusyhtiöitä tunnistamaan petokset ajoissa. Ymmärryksen pohjalta voidaan ottaa käyttöön toimivimmat menetelmät petosten havaitsemiseksi ja niiden torjumiseksi.

Vakuutuspetosten ja väärinkäytösten torjunta on osa vakuutusyhtiöiden yhteiskuntavastuuta. Vakuutusyhtiöiden tulee toiminnassaan tunnistaa, tutkia ja ilmoittaa havaitsemistaan väärinkäytöksistä ja rikoksista. Vakuutuspetoksia tutkii Suomessa poliisi ja muut viranomaiset, sen lisäksi vakuutusyhtiöillä on myös sisäinen tutkintatoiminto. (Finanssiala, 2019.) Vakuutusyhtiön tulee tutkinnassaan noudattaa hyvää vakuutustapaa, joka tarkoittaa toiminnan ammattitaitoisuutta, lainmukaista, eettisesti kestäväää, kohtuullista, tasapuolista ja oikeudenmukaista toimintaa (Luukkonen ym., 2018, 112–113).

Vakuutusyhtiöt ehkäisevät rikoksia hyödyntämällä yhteisiä rekistereitä, kuten väärinkäytös- ja vahinkorekistereitä. Näissä rekistereissä jaetaan tietoa ilmoitetuista vahingoista ja rikosepäilyistä. Väärinkäytösrekisterin merkinnät perustuvat poliisille tai syyttäjälle ilmoitettuihin rikosepäilyihin. Rekisterimerkinnät pyyhitään viimeistään viiden vuoden kuluttua merkinnästä. Näiden rekisterien avulla vakuutusyhtiöt voivat olla yhteydessä toisiinsa, ja tunnistaa mahdolliset väärinkäytökset. Väärinkäytösrekisteri on hyödyllinen vakuutuspetosten ennaltaehkäisyn kannalta, sillä sen avulla vakuutusyhtiöt voivat havaita petoksia. (HE 87/2019.) Vakuutusutkijoiden sekä väärinkäytös- ja vahinkorekisterien lisäksi on myös muita tapoja tunnistaa ja ehkäistä vakuutuspetoksia. Insurance European (2019) mukaan myös ihmisten tietoisuuden kasvattaminen, vakuutusyhtiön työntekijöiden kouluttaminen ja teknologian hyödyntäminen ovat proaktiivisia tapoja kamppailla vakuutuspetoksia vastaan. Käsittelen ensin ihmisten tietoisuuden kasvattamista.

Ihmisten tietoisuuden kasvattaminen on yksi keino ehkäistä vakuutuspetoksia (Insurance Europe, 2019, 14). Esimerkiksi vakuutusehtojen esittäminen ymmärrettävässä muodossa ei ole ainoastaan hyvä tapa lisätä vakuutuksenottajien tietoisuutta, vaan se on myös

lakisääteistä. Vakuutuslainsäädännön luvussa 2 (pykälät 4b - 9a) käsitellään vakuutuksesta annettavia tietoja. Vakuutuslainsäädännön 4b §:ssä määrätään vakuutustarpeen selvittämisestä. Tässä pykälässä pääpointtina on se, että vakuutuksenantajan on ennen vakuutuksen tarjoamista selvitettävä vakuutuksenottajan vakuutustarve ja lisäksi selvitettävä vakuutuksenottajan tietämys kyseisestä vakuutuksesta. Näin voidaan varmistaa, että vakuutuksenottaja tietää, mihin on sitoutumassa. Vakuutuslainsäädännön 5 §:ssä määrätään tiedoista ennen sopimuksen tekemistä. Tässä pykälässä määrätään, että vakuutuksenantajan on huolehdittava, että vakuutuksenottaja ymmärtää sopimuksen ehdot, vakuutusmuodot ja vakuutusmaksut. Tämä pykälä kattaa myös vakuutuksenantajan velvollisuuden selvittää vakuutuksenottajalle vakuutusturvan kattavuus ja rajoitusehdot. Lisäksi 5a §:ssä määrätään, että tiedot on toimitettava pysyvällä tavalla. (VakSL, 4b §, 5 §, 5a §.)

Vakuutusyhtiö siis kantaa vastuuta siitä, että vakuutuksenottaja tietää vakuutuksen ehdot, omat vastuunsa ja vakuutuksen rajoitukset. On myös tärkeää ottaa huomioon, että vakuutuksenottaja nimenomaan ymmärtää mihin on sitoutumassa, mihin se voi vaikuttaa ja millä tavalla (VakSL, 4b §, 5 §, 5a §). Mikäli vakuutuksen kokonaisvaltaista ymmärrettävyyttä parannettaisiin, on mahdollista, että tietämättömyydestä johtuvat petokset vähenisivät (Insurance Europe, 2019, 21; Gill & Randall, 2015, 31–35).

Toinen proaktiivinen keino kitkeä vakuutuspetoksia on vakuutusalan työntekijöiden kouluttaminen (Insurance Europe, 2019, 14). Vakuutuspetoksia tunnistetaan pääasiassa poikkeavuuksien ja ristiriitaisuuksien avulla. Esimerkiksi kun vahingon olosuhde ei täsmää vakuutuksenottajan kertomusta, vakuutuksenottaja vaatii toistuvasti korvauksia samanlaisista menetyksistä, tai vakuutuksenottaja käyttäytyy poikkeavalla tavalla, kuten aggressiivisesti tai epävarmasti. Korvauskäsittelijät, jotka työskentelevät päivittäin vakuutusrajapinnassa, ovat luonnollisesti avainasemassa vakuutuspetosten tunnistamisessa ja torjunnassa. Tämän vuoksi he ovat yksi tärkeimmistä koulutettavista ryhmistä. (Morley ym., 2006, 165–179.)

Viimeisin esiteltävä proaktiivinen vakuutuspetosten torjumiskeino on teknologian lisääminen vakuutustunnistusprosessiin. Teknologialla voidaan merkittävästi parantaa petosten

tunnistamista. Erityisesti suurien massadatojen analysointi tiedonlouhintateknologilla (engl. data-mining) edistää vakuutuspetosten tunnistamisprosessia. Nämä tiedonlouhintateknologiat pystyvät havaitsemaan muun muassa poikkeavuuksia tai muita petollisia toimintamalleja, kuten toistuvat korvausvaatimukset. Teknologian yhdistäminen henkilöstön osaamiseen voi huomattavasti parantaa tehokkuutta petostorjunnassa. (Morley ym., 2006, 167–179; Derrig, 2002, 271–278.)

Niin kuin jo aiemmin mainittu, vakuutuspetoksia ja niiden tekijöitä on monia. Sen lisäksi datan manuaalinen läpikäyminen on erittäin kuormittavaa ja kallista vakuutusyhtiöille. Teknologiset ratkaisut, kuten tekoälysovellukset ja lohkoketjuteknologia, tarjoavat potentiaalisia keinoja petosten tunnusmerkkien havaitsemiseen ja siten myös petosten tunnistamiseen. Seuraavassa teorialuvussa käsitellään lohkoketjuteknologian periaatteita ja toimintaa, sen käytännön sovelluksia petosten havaitsemisessa, hyötyjä verrattuna perinteisempiin teknologioihin sekä siihen liittyviä haasteita.

2.4 Terveysvakuutuspetokset

Tässä alaluvussa käsitellään terveysvakuutusta sekä siihen liittyviä petoksia. Kansainvälisesti käytetään yleisimmin termiä terveysvakuutus eli "health insurance" kun taas Suomessa puhutaan yleisemmin sairausvakuutuksesta eli "sickness insurance". Tässä luvussa käytetään soveltuvien osien molempia termejä, mutta niillä tarkoitetaan käytännössä samaa kokonaisuutta. Seuraavissa kappaleissa tarkastellaan sekä lakisääteistä että vapaaehtoista terveysvakuutusta ja käydään läpi yleisimpiä terveysvakuutuspetosten tunnusmerkistöjä.

2.4.1 Lakisääteinen- ja vapaaehtoinen terveysvakuutus

Ihmisten terveyden- ja sairaanhoito on järjestetty hyvin eri tavoilla eri puolilla maailmaa. Terveydenhuoltoa rahoitetaan tyypillisesti joko verotuksella tai vakuutusmaksuilla. Terveysvakuutus voi olla luonteeltaan joko lakisääteinen tai vapaaehtoinen. Monissa Keski-Euroopan ja Latinalaisen Amerikan maissa lakisääteinen terveysvakuutus on

terveydenhuollon pääasiallinen rahoitusmuoto, eli pakolliset vakuutusmaksut peritään esim. työtuloista, ja niiden maksamiseen osallistuvat yleensä sekä työnantajat että työntekijät. Maissa, joissa vakuutus on pääasiallinen terveydenhuollon rahoitusmuoto, järjestelmä kattaa yleensä koko väestön. Terveysvakuutuksen toimeenpanosta vastaa joko julkinen laitos, ryhmä itsenäisiä rahastoja tai vakuutusyhtiöitä tai ammattiryhmän, työnantajan tai maantieteellisen alueen perusteella määräytyvä sairausvakuutuskassa. Käytännössä tällöin terveydenhuollon tuottaja tuottaa tarpeellisen palvelun ja sitten laskuttaa sen vakuutetun potilaan lakisääteiseltä sairausvakuutuslaitokselta tai -kassalta. (Klavus ym., 2005.)

Vapaaehtoinen sairausvakuutus toimii yleensä lakisääteisiä terveystakuuksia ja -palveluita täydentävänä järjestelmänä. Yksityinen vapaaehtoinen vakuutus tarjoaa usein laajemman valikoiman palveluja ja nopeamman pääsyn erikoislääkäreille. (Klavus ym., 2005). Vapaaehtoisen sairausvakuutuksen avulla voidaan siis päästä hoitoon paitsi kuluitta, myös mahdollisesti nopeammin. Vapaaehtoisen sairausvakuutuksen sisältö vaihtelee eri yhtiöiden välillä, ja vakuutus on usein räätälöitävissä. (Jokela ym., 66–67; Tuorila, 2019, 20.) Yksityisen sairausvakuutuksen osuus terveydenhuollon kokonaisrahoituksesta on etenkin EU-alueella varsin pieni, ja kohdistuu usein esimerkiksi suurituloisille tai lapsiperheille. (Klavus ym., 2005.)

Yhdysvalloissa taas tilanne on päinvastainen, eli lakisääteinen sairausvakuutus (esim. yli 65-vuotiaille sekä vakavasti sairaille suunnattu Medicare ja pienituloisille suunnattu Medicaid) kärsii heikosta hoidon saatavuudesta ja laadusta. Sen lisäksi nämä lakisääteiset ohjelmat kattavat vain pienen osan väestöstä, jättäen suuren joukon vaille riittävää turvaa. (Grabowski, 2007, 579–584.) Tämän vuoksi suurin osa yhdysvaltalaisista hankkii terveystakuuksensa yksityisiltä vakuutusyhtiöiltä joko työnantajan kautta tai itsenäisesti. Yksityisten vakuutusten hinnat ja kattavuus vaihtelevat suuresti, ja ne voivat olla erittäin kalliita, erityisesti ilman työnantajan tukea. Näin ollen työnantajan tarjoamat vakuutukset ovatkin yleisin vaihtoehto, ja ne kattavat usein työntekijän lisäksi myös perheenjäsenet. (Su ym., 2019, 673; Borelli, 2024.)

Suomen terveydenhuoltopalvelut koostuvat kolmesta osasta: julkisesta perusterveydenhuollosta ja erikoissairaanhoidosta, lakisääteisen sairausvakuutuksen

tukemana toteutettavasta työterveyshuollosta ja osittain lakisääteisen sairausvakuutuksen korvaamasta yksityisestä terveydenhuollosta. Lähtökohtaisesti kaikki Suomessa asuvat kuuluvat julkisen terveydenhuollon piiriin, jonka kustannuksia kompensoidaan verovaroin. Käytännössä julkisesta terveydenhuollosta maksetaan käytön mukaan asiakasmaksuja, jotka ovat kuitenkin vain murto-osa hoidon todellisista kustannuksista. Lisäksi työntekijöillä on Suomessa mahdollisuus käyttää julkisen terveydenhuollon ohella myös työnantajan täysin kustantamaa työterveyshuoltoa, jonka kattavuus vaihtelee. Vaihtoehtoisesti yksilö voi hakea hoitoa myös yksityisiltä terveystalvelujen tuottajilta. (EU-Terveystoito, n.d.)

Lisäksi Suomessa on olemassa lakisääteinen sairausvakuutus, joka toimii julkisen terveydenhuollon rinnalla ja täydentää sen tarjoamia palveluita (Mattila, 2011, 12–14). Sairausvakuutuksesta korvataan ensinnäkin yksityisen hoidon kustannuksia (korvaukset rajattuja ja tasoltaan alhaisia), lääkekustannuksia ja matkakuluja, sekä ansionmenetystä (esim. sairauspäiväraha). (Jokela ym., 2021, 38; Kansaneläkelaitos, 2024.) Lakisääteistä turvaa voi täydentää vapaaehtoisella sairausvakuutuksella, joka kattaa useimmiten tutkimus-, hoito- ja lääkekuluja.

2.4.2 Terveystakuutuspetosten tunnusmerkit

Terveystakuutuspetokset ovat suuri haaste koko vakuutusallalle, sillä terveydenhuollon tappiot petosten vuoksi ovat kasvussa ympäri maailman. Terveystakuutuspetokset eivät ole ongelma vain vakuutusyhtiölle, vaan ne ovat merkittävä uhka myös jo valmiiksi hauraalle terveydenhuoltojärjestelmälle. Sen lisäksi terveystakuutuspetokset luonnollisesti nostavat myös vakuutusmaksuja ja vakuutuksen omavastuita. Tämä voi olla monelle yksilölle erittäin kuormittavaa ja haitallista rehellisille vakuutuksenottajille. (Li, ym., 2022, 1–4.)

Terveystakuutuspetos voi tapahtua useassa eri tilanteessa ja monen osapuolen toimesta. Terveystakuutuspetoksia tekevät potilaat, terveydenhuollon edustajat ja vakuutusyhtiön edustajat. Sen lisäksi terveystakuutuspetos voi tapahtua vakuuttamisen yhteydessä tai hoitopolun eri vaiheissa. Petosten monimuotoisuus tekee niiden tunnistamisesta haastavaa. Esimerkkinä hoitopolun vaiheessa tehtävästä petoksesta voidaan mainita terveydenhuollon

tarjoajan tekemä ylilaskuttaminen tai potilaan terveydellisten haasteiden vääristely. (Johnson & Nagarur, 2016, 250; Duman 2017, 840; Li, ym., 2022, 4.)

Tutkimuksissa on tunnistettu monia eri terveysvakuutuspetoksen variaatioita. Terveysvakuutuspetosten tekijäosapuolet voidaan Li ym. (2012) mukaan jakaa neljään kategoriaan. Nämä kategoriat ovat: yksilöt, palveluntarjoajat, palveluntarjoajien ja vakuutusnottajien välinen yhteistyö, ja petoksia tekevät rikosryhmät. Terveysvakuutuspetoksia esiintyy runsaasti. Seuraavissa kappaleissa käsitellään yleisimpiä esimerkkejä terveysvakuutuspetoksista eri tekijäosapuolten näkökulmasta.

Identiteettivarkauspetos (engl. identity fraud) on petos, jossa vakuuttamaton henkilö käyttää vakuutetun henkilön identiteettiä ja vakuutustietoja hyötyäkseen perusteettomasti toisen henkilön vakuutusturvasta. Identiteettivarkauden tekijä voi tässä yhteydessä hyötyä muun muassa saamalla väärin perustein sairauskulukorvauksia tai saadakseen terveydenhuollon hoitoa. (Li ym., 2008, 276; Rashidian ym., 2012, 2; Thornton ym., 2015, 716.) Toinen yksilöiden tekemä terveysvakuutuspetos on harhaanjohtaminen (engl. false reporting), joka tarkoittaa sitä, että vakuutettu käy lääkärillä usein kertoen keksittyjä sairauden oireita päästäkseen käsiksi reseptilääkkeisiin. Näitä reseptilääkkeitä käytetään ja myydään huumausainetarkoituksessa (Rashidian ym., 2012, 2.)

Myös palveluntarjoajat eli terveydenhuollon edustajat tekevät vakuutuspetoksia. Palveluntarjoajien yleisimpiin petoksiin lukeutuu muun muassa ylikoodaus (engl. up-coding). Ylikoodaus tarkoittaa sitä, että palveluntarjoajat saattavat laskuttaa kalliimmista hoidoista kuin mitä on todellisuudessa suoritettu, tai jopa laskuttaa hoidoista, joita ei ole lainkaan tehty. (Li ym., 2008, 276; Rashidian ym., 2012, 2; Thornton ym., 2015, 716.) Toinen yleinen palveluntarjoajien petos on ylilaskutus (engl. overcharging). Ylilaskutus tässä yhteydessä tarkoittaa sitä, että palveluntarjoaja teettää turhia vastaanottokäyntejä, testejä ja toimenpiteitä mitä olisi tarve, maksimoidakseen korvauksen vakuutuksesta. (Li ym., 2008, 276; Thornton ym., 2015, 717.) Viimeisimpänä tästä kategoriasta on erikseen laskuttaminen (engl. unbundling), tämä tarkoittaa sitä, että palveluntarjoaja laskuttaa hoidoista tai tarvikkeista erikseen, vaikka yhdessä tarjottuna se loisi kustannussäästöjä. Palveluntarjoaja

tekee näin maksimoidakseen korvauksen vakuutuksesta. (Li ym., 2008, 276; Thornton ym., 2015, 716; Rashidian ym., 2012, 2.)

Yhteistyö palveluntarjoajien ja vakuutusnottajien välillä tarkoittaa terveystietojen vaihtamisen kontekstissa esimerkiksi lääkkeiden, välineiden ja tarvikkeiden vaihtamista (engl. drug, equipment, and supply replacement). Käytännössä siis terveydenhuollon palveluntarjoaja tekee yhteistyötä vakuutetun kanssa. Tarkoituksena on vaihtaa ei-korvattavia tuotteita korvattaviin tuotteisiin väärentämällä reseptejä ja laskutusta. (Li ym., 2008, 276; Rashidian ym., 2012, 2.) Toinen esimerkki yhteistyöpetoksesta näiden kahden tekijäosapuolen välillä on perusteeton sairaalahoito (engl. false hospitalization). Kyseisessä petoksessa palveluntarjoaja, eli tässä tapauksessa sairaala, hoitaa vakuutuksen ottanutta potilasta, joka ei täytä sairaalahoidon vaatimuksia. Vaihtoehtoisesti sairaala voi esittää korvausvaatimuksen sairaalahoidosta useammalle vakuutetulle potilaalle kuin mitä on todellisuudessa hoidettu. (Thornton ym., 2015, 717.)

Viimeisimpänä tekijäosapuolista käsitellään petoksia tekevät rikosryhmät (engl. fraud gangs). Tällaiselle ryhmälle on tyypillistä muun muassa yhteistyö apteekkien, lääkärin ja vakuutusnottajien kanssa. Yksi yleisimmistä rikosryhmät tekemistä petoksista on reseptilääkkeiden myynti (engl. drug selling). Tämä toteutetaan käyttämällä vakuutusnottajien vakuutuskortteja reseptilääkkeiden hankkimiseksi. (Thornton ym., 2015, 716.) Toinen hyvin yleinen petos rikosryhmille on lääkärin lausuntojen ja terveystietojen väärentäminen. Väärentämällä lausuntoja rikolliset pääsevät käsiksi perusteettomiin terveystietojen korvauksiin. (Li ym., 2008, 276.) Viimeisimpänä esimerkkinä rikosryhmän tekemistä petoksista on reseptipetos (engl. prescription fraud). Reseptipetoksessa rikosryhmät tekevät tiivistä yhteistyötä apteekkien kanssa päästäkseen toisten ihmisten terveystietojen kortteihin käsiksi ja hyötyäkseen tästä taloudellisesti. (Li ym., 2022, 4.)

Terveydenhuollossa käsitellään suuria määriä monimutkaista terveystietoa ja arkaluontoisia henkilötietoja, mikä tekee petosten tunnistamisesta haastavaa. Siksi teknologiaa, kuten tekoälyä, koneoppimista ja lohkoketjuja, hyödynnetään yhä enemmän terveystietojen petosten havaitsemiseen (Mohammed ym., 2023).

3 LOHKOKETJUTEKNOLOGIA OSANA PETOSTEN TUNNISTAMISPROSESSIA

3.1 Lohkoketjuteknologian periaatteet ja toiminta

Lohkoketjuteknologia on tapa tallentaa ja jakaa tietoa turvallisesti ilman tarvetta kolmannelle osapuolelle, kuten pankille. Tämä uusi teknologia tarjoaa mahdollisuuksia monille eri toimialoille. Lohkoketjuteknologia toiminta nojaa kolmeen periaatteeseen: hajautettuun vertaisverkkoon, vertaisverkon konsensukseen ja kryptografiaan. (Treleaven ym., 2017.)

Tämä teknologia toimii hajautetussa vertaisverkossa ilman kolmannen osapuolen keskitettyä valvontaa. Hajautettu verkko koostuu lohkoketjun osapuolista, joissa jokaisella osapuolella eli solmulla (engl. node) on oma kopio lohkoketjuun tallennetuista tiedoista. Tämä hajautettu järjestelmä pitää kirjaa kaikista tehdyistä muutoksista. Lohkoketjuteknologia käyttää hajautettua vertaisverkkoa varmistaakseen tiedon eheyden ja turvallisuuden. Tämän menetelmän ansiosta lohkoketjun manipulointi on vaikeampaa, koska tieto on hajautettu useisiin palvelimiin sen sijaan, että se säilytettäisiin yhdessä paikassa. (Nakamoto 2008; Murray, 2019.)

Lohkoketjuteknologian toiminta perustuu siihen, että vertaisverkon osapuolet ovat samaa mieltä lohkoketjuun lisättävistä tiedoista. Tätä vertaisverkon konsensusta kutsutaan konsensusalgoritmiksi (engl. consensus algorithm). Lohkoketjuteknologiassa käytetään erilaisia konsensusmekanismeja, joilla taataan, että kaikki solmut ovat samaa mieltä lohkoketjuun lisättävästä tiedosta. Kysesen mekanismin tavoitteet ovat: tiedon eheyden varmistaminen, tiedon muuttumattomuus, tiedon luotettavuus, haitallisten osapuolien estäminen ja hajautetun verkon luottamuksen ylläpito. Konsensusmekanismit ovat algoritmeja, joista monet toimivat samankaltaisella periaatteella. Tunnetuimmat algoritmit ovat Proof of Work (PoW) ja Proof of Stake (PoS). Kun lohkoketjuun lisätään uutta tietoa, käynnistyy ketjussa käytettävä algoritmi. Tieto lisätään lohkoon, kun ensimmäinen solmuista saa ratkaistua vaikean matemaattisen ongelman. Ongelman ratkaissut solmu saa lisätä tiedot lohkoon ja ansaitsee tästä palkkion. (Swan, 2015; Murray, 2019.)

Lohkoketju hyödyntää myös kryptografiaa (engl. cryptography), jota hyödynnetään tietojen suojaamiseen. Jokainen lohko sisältää hajautusarvon (engl. hash), joka toimii linkkinä edelliseen lohkoon, muodostaen näin ketjun, jossa lohkot ovat kytkeytyneet toisiinsa. Tämän rakenteen ansiosta tietojen muuttaminen on erittäin hankalaa, sillä yhden lohkon muokkaaminen edellyttää kaikkien sitä seuraavien lohkojen muuttamista. Tämä ominaisuus varmistaa tiedon eheyden ja estää manipuloinnin. (Nakamoto, 2008; Murray, 2019.)

Lohkoketjuteknologian keskeiset edut ovat siis tiedon muuttumattomuus, hajautettu rakenne ja läpinäkyvyys. Nämä ominaisuudet tekevät siitä merkittävän työkalun vakuutusalan petosten ehkäisyssä. Vakuutusallalla on perinteisesti ollut epäröintiä uusien teknologioiden käyttöönotossa, mutta lohkoketjuteknologia on herättänyt kasvavaa kiinnostusta erityisesti petosten havaitsemisen kannalta. Teknologiaa on verrattu merkittäviin keksintöihin, vaikka sen laajamittaisessa käyttöönotossa on edelleen haasteita, kuten energiatehokkuuden, skaalautuvuuden ja sääntelyn puutteet (Kar & Navin, 2021).

3.2 Lohkoketjuteknologia vakuutuspetosten tunnistamisessa

Tässä alaluvussa kuvataan lyhyesti ja teoriapohjaisesti lohkoketjuteknologian roolia vakuutuspetosten tunnistamisessa. Laajempi kartoitus teknologian käytännön mahdollisuuksista erityisesti terveysvakuutuspetosten kontekstissa on tehty kirjallisuuskatsauksen muodossa luvussa 4. Lohkoketjuteknologian kehitys on tuonut uusia mahdollisuuksia useille toimialoille ja sen soveltaminen petosten tunnistamisessa on yksi merkittävimmistä. Lohkoketjuteknologia tarjoaa läpinäkyvyyttä, turvallisuutta, muuttumattomuutta ja luotettavan tavan tallentaa tietoja. Lohkoketjuteknologian avulla voidaan hyödyntää myös muita keskeisiä teknologioita. (Treleaven ym., 2017, 15–16.)

Lohkoketjuteknologian hajautetun vertaisverkon tilikirjoihin tallennetun digitaalisen jäljen avulla voidaan varmistaa tapahtumien kulku, sekä niiden turvallisuus ja aitous. (Ali, 2019; Saldamli, 2020.) Näiden ominaisuuksien vuoksi se sopii hyvin väärinkäytön tunnistamiseen ja on siten houkutteleva ratkaisu erityisesti vakuutusallalla petosten tunnistamiseen. Lohkoketjuteknologian on yksinkertaisuudessaan tietokantarakenne, jonka sisälle voidaan

rakentaa erilaisia ohjelmia, jotka suorittavat automaattisesti ennalta määritettyjä ehtoja (Ali, 2019; Saldamli, 2020). Kuten jo todettu, lohkoketjuun voidaan integroida myös muita teknologioita, kuten älykkäitä sopimuksia, esineiden internetiä sekä tekoälysovelluksia, kuten koneoppimista ja syväoppimista. Näitä teknologioita esitellään seuraavaksi.

Älykkäät sopimukset ovat lohkoketjualustalla toimivia ohjelmia, jotka hyödyntävät lohkoketjun tarjoamaa turvallisuutta ja muuttumattomuutta. Älykkäät sopimukset ovat lohkoketjuteknologiaan perustuvia ongelmia, jotka voivat automatisoida prosesseja, kuten korvaushakemusten vilpillisyyden arviointia ja maksun suorittamista (Luu ym., 2016, 256; Macrinici ym., 2019, 2338.) Toinen teknologia, jota hyödynnetään lohkoketjuteknologian kanssa, on esineiden internet (Reyna ym., 2018). Esineiden internet viittaa laitteisiin ja antureihin, jotka ovat kytketty keskenään ja internetiin. Tämän avulla ne voivat jakaa ja käsitellä tietoa yhdessä. Esineiden internetin tavoitteena on usein luoda älykkäitä sovelluksia, jotka helpottavat esimerkiksi arkea. Näitä laitteita yhdistää pilvipalvelu, jossa tietoa tallennetaan ja analysoidaan. (Gubbi ym., 2013, 1647.)

Lohkoketjualustalla voidaan hyödyntää myös koneoppimista, joka on tekoälypohjainen teknologia ja perustuu algoritmeihin, jotka analysoivat suuria määriä tietoja. Tämän avulla voidaan kehittää ennustemalleja petosten havaitsemiseen. Ennustemallit voidaan esimerkiksi kouluttaa erottamaan petolliset ja ei-petolliset vaatimukset (Jordan & Mitchell, 2015; Ali, 2017). Lisäksi koneoppimisen sovelluksia ovat muun muassa luottokorttipetosten havaitseminen, kuvantunnistus ja luonnollisen kielen prosessointi (Jordan & Mitchell, 2015). Nämä ominaisuudet säästävät aikaa, tehostavat korvauspäätöksiä, mutta myös auttavat vakuutusyhtiöitä tunnistamaan toistuvia vilpillisiä kaavoja ja siten ennakoimaan petoksia.

Toinen tekoälypohjainen teknologia, jota hyödynnetään lohkoketjualustalla, on syväoppiminen. Syväoppiminen on koneoppimisen osa-alue, jossa käsitellään suuria määriä tietoja käyttämällä syviä, kerroksittaisia hermoverkkoja. Tiedon käsittely etenee vaiheittain, jolloin jokainen kerros oppii tunnistamaan yhä monimutkaisempia piirteitä datasta. Näitä piirteitä ovat muun muassa kuvien värit, muodot ja esineet. Syväoppiminen on erityisen hyödyllinen suurien tietomäärien kanssa, kuten kuvan tunnistuksessa, puheen ymmärtämisessä ja tekstin kääntämisessä. Tämä teknologia on hyvin käytännöllinen, sillä

syväoppimisen mallit oppivat itsenäisesti yhtäläisyyksiä ja piirteitä, jotka ovat tärkeitä annetun tehtävän ratkaisemiseksi. (LeCun ym., 2015.)

Lohkoketjuteknologia voisi mahdollistaa eri vakuutusyhtiöiden välisen tiedon jakamisen ja näin auttaa estämään petoksia, kuten kaksoiskorvauksia. Esimerkiksi vakuutusyhtiö A voisi pyytää asiakkaalta tarvittavat tiedot, kuten auton rekisterinumeron, auton tiedot ja asiakkaan iän. Jos asiakas yrittäisi hakea korvausta samasta vahingosta myös toiselta yhtiöltä (kaksoiskorvaus, engl. double dipping), lohkaketjuun tallennettu tieto voisi varoittaa yhtiöitä päällekkäisistä hakemuksista, mikä estäisi petosyrityksen jo ennen korvauskäsittelyn aloittamista. (Roriz & Pereira, 2019.)

Kaksoiskorvausongelmaa havaitaan myös terveystakuutuksen kontekstissa. Eli vakuutusasiakas yrittää hakea korvausta kahdelta eri taholta saadakseen korvauksen samasta vakuutustapahtumasta useammin kuin on oikeutettu. (Saldamli ym., 2017.) Tästä päätellen tämänlainen käytös toistuu vahinkolajista riippumatta.

Vakuutuksenottajat voivat usein esittää väärää tai harhaanjohtavaa tietoa vakuutusyhtiöille pyrkiessään saamaan perusteettomia korvauksia ja saadakseen taloudellista etua. Tällaiset petokset aiheuttavat merkittäviä taloudellisia tappioita vakuutusyhtiöille, ja niiden tehokas tunnistaminen ja ehkäiseminen edellyttää järjestelmän kehittämistä, jossa prosessin kaikki vaiheet ovat läpinäkyviä ja luotettavasti jäljitettävissä. Lohkoketjuteknologia tarjoaa alustan, jolle rakentaa läpinäkyvä ja luotettava järjestelmä petosten tunnistamiseksi.

Muun muassa Al-Quayed ym. (2023) tutkimuksessa esitellään malli, jossa petosten tunnistaminen tapahtuu kolmessa kerroksessa: ennustekerroksessa tekoäly ja koneoppiminen luokittelevat petolliset tiedot erikseen, turvakerroksessa lohkoketjuteknologia suojaa tiedot ja estää näin manipuloinnin, ja käsittelykerroksessa varmistetaan älykkäiden sopimusten avulla, että kaikki osapuolet saavat aidot ja luotettavat tiedot. Toisaalta Ashfaq ym. (2022) tutkimuksessa näitä samankaltaisia kerroksia oli kaksi. Heidän versiossaan järjestelmä koostuu lohkoketjuserroksesta ja koneoppimiserroksesta. Lohkoketjuserrokseen tallennetaan tapahtumien tiedot ja koneoppimiserroksessa havaitaan ja luokitellaan tapahtumat aitoihin ja vilpillisiin.

Edellisistä päätellen lohkoketjuteknologia tarjoaa merkittävän mahdollisuuden tehostaa vakuutuspetosten tunnistamista ja ehkäisemistä. Eri teknologioiden yhdistäminen lohkoketjuteknologiaan mahdollistaa petosten tehokkaan luokittelun ja ehkäisyn. Näiden teknologioiden hyödyntäminen yhdessä voi paitsi vähentää taloudellisia tappioita, mutta myös parantaa vakuutusjärjestelmien kokonaisvaltaista toimivuutta ja luotettavuutta.

3.3 Lohkoketjuteknologian hyödyt verrattuna perinteisiin järjestelmiin

Tässä alaluvussa käsitellään lohkoketjuteknologian roolia vakuutuspetostorjunnassa ja peilataan sitä nykyisiin niin sanottuihin perinteisempiin järjestelmiin. Tutkimuksessa esiteltävät perinteiset järjestelmät sisältävät myös teknologiaa sisältävät ratkaisut, jotka ovat olleet laajemmin ja pidempään käytössä kuin lohkoketjuteknologia. Hilal ym. (2022) mukaan vakuutuspetosten tunnistaminen oli pitkään manuaalista työtä, joka on nykyisiin järjestelmiin verrattuna varsin tehotonta ja resursseja tuhlaavaa. Varsinkin petosten havaitseminen ennakkoon on haastavaa pelkästään ihmisresurssein. Tämän vuoksi vakuutusyhtiöt ovatkin integroineet nykyaikaista teknologiaa vakuutuspetostorjunnan tueksi.

Vakuutusyhtiöille on taloudellista tunnistaa vakuutuspetokset mahdollisimman aikaisessa vaiheessa (Kajwang, 2022, 62; Hilal ym., 2022, 6–7). Vilpillisen toiminnan tunnistamista voidaan helpottaa rakentamalla ennustemalleja datan avulla. Nykyaikaista teknologiaa hyödyntämällä vakuutusyhtiöt voivat ottaa vakuutuspetostorjuntaan mukaan historia- ja reaaliaikaista dataa (Kajwang, 2022, 62; Hilal ym., 2022, 4–6). Vakuutusyhtiöt voivat hyödyntää data-analyysissa esimerkiksi palkkatietoja, aikaisempia korvaustietoja, oikeudenkäyntikuluja, demografisia tietoja, säättietoja, yhtiön muistiinpanoja ja äänitallenteita. (Kajwang, 2022, 62.)

Vakuutuspetostorjunnassa hyödynnetään paljon koneoppimisalgoritmeja, kuten päätöspuita. Koneoppiminen on erittäin toimiva menetelmä tunnistamaan vilpilliset korvaushakemukset ja havaitsemaan petollisia toimintatapoja. Koneoppimisen yksi isoimmista ongelmista on tietojen yksityisyyden sekä tietoturvan varmistaminen. Asiakkaat kokevat tietoturvan puutteellisuuden ongelmaksi, minkä vuoksi monet eivät tämän vuoksi

halua antaa lupaa arkaluontoisten tietojansa automaatiokäsittelyyn vakuutusyhtiössä. Koneoppimisjärjestelmiä voidaan suojata homomorfisella salauksella (engl. homomorphic encryption), joka mahdollistaa datan käsittelyn ilman tietojen purkamista. Tämä parantaa tietoturvaa ja lisää asiakkaiden yksityisyyttä mahdollistaen samalla petosten ennustussmallien rakentamisen ja petosten paremman tunnistamisen. Homomorfinen salaus on tehokas lisäämään tietojen käsittelyn turvallisuutta, mutta se lisää huomattavasti kustannuksia ja tiedonsiirtomäärää. Salattujen tietojen käsittely ja siirtäminen on huomattavasti hitaampaa. (Canillas ym., 2018, 25–30.)

Erityisesti tietojen siirtäminen organisaatiosta toiseen nähdään myös uhkana tietovuotojen ja luottamuksen puutteen vuoksi. Tämä vaikeuttaa tietojen tarkempaa tutkimista sekä uusien menetelmien kehittämistä. Tähän ongelmaan lohkoketjuteknologia tarjoaa ratkaisua. Lohkoketjuteknologia tarjoaa luotettavan alustan, mikä mahdollistaa tietojen turvallisen tallennuksen ja analysoinnin. Esimerkiksi identiteetti voidaan suojata kryptografisella menetelmillä, joka parantaa huomattavasti asiakkaiden tietosuojaa. Lohkoketjuteknologia on alustana joustava, sillä koneoppimismallit, tekoäly, automaatio ja älysovimukset voidaan integroida lohkoketjuteknologian tarjoaman luotettavan ympäristön sisälle. (Pranto ym., 2022.) Tämä tarjoaa menetelmille mahdollisuuden toimia ja kehittyä suojatussa ympäristössä.

Näin ollen lohkoketjuteknologia tarjoaa merkittäviä etuja organisaatioille. Ensinnäkin se parantaa tietoturvaa ja luotettavuutta, sillä kryptografiset menetelmät suojaavat ja parantavat asiakkaiden tietosuojaa. Toiseksi lohkoketjuteknologia voi vähentää taloudellisia kustannuksia samaan aikaan tarjoamalla tehokkaan ja turvallisen tavan tallentaa ja analysoida tietoja. Kolmanneksi se on joustava alusta, johon voidaan integroida monia jo käytettyjä teknologioita ja mahdollistaa vanhojen sekä uusien menetelmien kehittämisen suojatussa ympäristössä.

3.4 Lohkoketjuteknologian haasteet vakuutusallalla

Niin kuin moni muukin teknologia, myös lohkoketjuteknologian käyttöönotto kohtaa haasteita. Isoimpia ongelmia ovat skaalautuvuuden vaikeus, lainsäädännölliset haasteet, korkea energiankulutus, yhteensopivuushaasteet nykyisten järjestelmien kanssa ja korkeat kustannukset. (Niranjanamurthy ym., 2019, 12–13.)

Vakuutusala on tunnistettu yhdeksi nopeimmin kasvavista toimialoista. Tämä johtuu osaksi siitä, että vakuutustuotteita on yhä enemmän ja ihmisillä on yhä enemmän vakuuttamistarpeita. Tämän vuoksi vakuutusyhtiöiden tulisi laajentaa toimintaansa. (Raikwar, 2018, 1.) Lohkoketjuteknologian yksi haasteista on huono skaalautumiskyky. Lohkoketjuteknologian luonteen vuoksi se on hitaampi kuin keskitetyt tietokannat. Tämä johtuu siitä, että kun uusi tieto lisätään, lohkoketjussa suoritetaan samat tehtävät kuin keskitetyssä tietokannassa, jonka lisäksi lohkoketjussa suoritetaan kolme muutakin tehtävää, eli konsensuksen saavuttaminen, tiedon lisäämisen vaatima laskentatehtävä ja kryptografisen suojauksen lisääminen. Näiden tehtävien suorittaminen ja vahvistaminen on monimutkaista ja voi aiheuttaa pullonkaulan käsittelyyn. (Niranjanamurthy ym., 2019, 12–13; Bhutta ym., 2021, 7–8.)

Toinen suuri haaste lohkoketjuteknologian käyttöönotolle on sitä koskeva sääntely, tai oikeastaan sen puute tai vaihtelevuus. Lohkoketjuteknologian käyttöä ei ole monessa maassa selkeästi säännelty, mikä luo epävarmuutta vakuutusyhtiöille, jotka pohtivat teknologian integroimista yhtiöön. (Niranjanamurthy ym., 2019, 12–13.) Lohkoketjuteknologian laajamittainen hyödyntäminen edellyttää lainsäädännön kehittämistä, sillä sääntelyn puute voi aiheuttaa merkittäviä oikeudellisia ongelmia. Toisaalta liian tiukka sääntely voi rajoittaa innovaatioiden kehitystä ja käyttöönottoa. Lisäksi vakuutukset voivat olla globaaleja, joka voi johtaa monimutkaisuuteen tai säädöseroihin maiden välillä. (Rahkola, 2019, 60.)

Lohkoketjuteknologian suuri energiankulutus muodostuu lohkojen lisäyksistä, mikä vaatii merkittävän määrän tietokoneen tehoa (Niranjanamurthy ym., 2019, 13). Korkea energiankulutus liitetään erityisesti Proof-of-Work (PoW)-konsensusalgoritmiin. PoW-

konsensusalgoritmin toimintaperiaate perustuu siihen, että vertaisverkon osapuolet kilpailevat ratkaistakseen vaativia matemaattisia pulmia, varmistaakseen tietojen lisäykset lohkoihin ja saadaksesen palkkion tehtävän ratkaisusta. Tämä uuden lohkon luomisprosessi tarvitsee merkittävän määrän laskentatehoa ja näin myös energiaa. (Sedlmeir ym., 2020, 600–604.) Esimerkiksi bitcoin, joka perustuu täysin lohkoketjuteknologiaan, kulutti vuosina 2020 ja 2021 arviolta noin 125 TWh energiaa vuodessa. Tämä määrä vastaa pienten maiden vuosittaista sähkönkulutusta. (Sedlmeir ym., 2020, 603; Tomatsu & Han, 2023, 92.) Energiankulutus ei kuitenkaan johdu tehottomista algoritmeista, vaan lohkoketjuteknologian turvallisuusmekanismista, joka on suunniteltu kuluttamaan paljon energiaa. Suuri energiankulutus ehkäisee hyökkäyksiä, koska hyökkääjän tulisi hallita 25–50 % kokonaislaskentatehosta, jotta hän voisi päästä käsiksi järjestelmään. Tunnetuista algoritmeista Proof-of-Work (PoW), Proof-of-Authority (PoA) ja Proof-of-Stake (PoS), tämä edellä lyhyesti esitelty PoW on energiankulutuksen kannalta kuluttavin. (Sedlmeir ym., 2020, 601.)

Vakuutusyhtiöt hyödyntävät liiketoiminnassaan järjestelmiä, joiden yhteensopivuus lohkoketjuteknologian kanssa nähdään myös ongelmana. Lohkoketjuteknologia ja sen sovellukset tarjoavat ratkaisuja, joita varten yhtiön täytyisi tehdä merkittäviä muutoksia jo olemassa oleviin järjestelmiin tai ne täytyisi kokonaan korvata uusilla lohkoketjuteknologian kanssa sopivilla. (Niranjanamurthy ym., 2019, 13.) Tämä vaatii yhtiöltä paljon resursseja, suunnittelua ja riskiarviointia. Näiden haasteiden lisäksi Linin ja Liaon (2017) mukaan nykyisen järjestelmän muuttaminen soveltuvammaksi on merkittävän kallista sekä rahallisesti että ajallisesti. Mainittujen haasteiden lisäksi lohkoketjuteknologia on suhteellisen tuore keksintö ja sen integrointi vaatisi alan asiantuntijoiden apua. (Lin & Liao, 2017, 459–461.) Nimenomaan korkeat rahalliset investoinnit voivat olla integraation esteenä, vaikkakin lohkoketjuteknologia voisi tarjota säästöjä pitkällä aikavälillä (Niranjanamurthy ym., 2019, 13).

4 LOHKOKETJUTEKNOLOGIAN ROOLI TERVEYSVAKUUTUSPETOSTEN TUNNISTAMISESSA

4.1 Tutkimusaineiston hankinta ja esittely

Tutkielman empiirinen osuus toteutetaan systemaattisena kirjallisuuskatsauksena. Tässä alaluvussa esitellään, miten kirjallisuuskatsaus on tehty ja miten tutkimusaineisto on haettu. Kirjallisuuskatsaus toteutettiin Finkin (2019, 6–7) mallia hyödyntäen. Finkin malli etenee seuraavanlaisesti.

1. Tutkimuskysymyksen asettaminen
2. Tietokannan ja kirjallisuuden valinta
3. Hakusanojen valinta
4. Käytännön seulan asettaminen
5. Sisällöllisen rajauksen tekeminen
6. Katsauksen suorittaminen
7. Synteesin tekeminen tuloksista

Finkin mallin (2019, 6–7) mukaan tutkimukselle määriteltiin ensin tutkimuskysymykset. Tämän vaiheen jälkeen siirryttiin seuraavassa järjestyksessä tietokannan, kirjallisuuden, hakusanojen ja hakusanalausekkeen valintaan. Tutkimuksessa päädyttiin käyttämään Tampereen yliopiston Andor-tietokantaa, sillä se osoittautui laajaksi korkealaatuisten tieteellisten artikkelien valikoimaksi. Tutkielman aiheen tuoreuden vuoksi oli tärkeää löytää tietokanta, jossa on paljon erityisesti laadukkaita kansainvälisiä artikkeleita. Näitä löytyi Andorista, mikä oli yksi tärkeimmistä syistä käyttää kyseistä tietokantaa tässä tutkielmassa. Aineiston hankinnan rajaaminen tiettyyn tietokantaan parantaa tutkimuksen läpinäkyvyyttä ja selkeyttää tutkimusprosessia. Nämä ominaisuudet ovat kirjallisuuskatsauksen asianmukaisen toteutuksen kannalta tärkeitä, sillä tutkimus on oltava myöhemmin toistettavissa (Fink, 2019, 6).

Hakusanojen valinnassa hyödynnettiin aihealueeseen liittyvää kirjallisuutta. Hakusanojen ja hakusanalausekkeen määrittelyssä keskityttiin tutkimuksen kannalta relevantteihin käsitteisiin. Hakulauseketta rajattiin sopivammaksi operaattorilla AND ja operaattoria OR käyttämällä saatiin laajennettua hakusanaa synonyymeja käyttämällä. Käytetyt käsitteet ja hakusanalauseke löytyy alla olevasta taulukosta 1.

Hakusanat	Hakusanalauseke
health, medical, fraud, fraudulent, insurance, blockchain	(health OR medical) AND (fraud OR fraudulent) AND insurance AND blockchain

Taulukko 1. Hakusanat ja hakusanalauseke

Tätä hakulauseketta käyttäen tietokannasta löytyi yhteensä 221 osumaa. Hakulausekkeen määrittelyä seurasi seuraava vaihe, eli käytännön seulojen asettaminen ja sisällöllinen rajaus. Finkin (2019, 7) mukaan käytännön seulojen asettamisella on merkittävä tehtävä epärelevanttien hakutuloksien karsimisessa ja hakusanalausekkeen kohdentamisessa. Käytännön seuloja ovat esimerkiksi julkaisuvuosi, artikkelin kieli ja tyyppi. (Fink, 2019, 7.) Tässä kirjallisuuskatsauksessa käytännön seulaksi asetettiin vertaisarvioidut artikkelit, minkä jälkeen hakutuloksia jäi jäljelle 35 kappaletta. Vuosirajausta harkittiin, mutta se todettiin tarpeettomaksi, sillä kaikki tutkimus aiheeseen liittyen on varsin uutta. Vanhin julkaisu, joka valittiin aineistoksi, oli vuodelta 2021. Kielirajausta harkittiin myös, mutta englanninkielisiä hakusanoja käyttäessä, hakutuloksista tuli vain englanninkielisiä artikkeleita. Tämän vuoksi itse seulaa kieleen liittyen ei tarvinnut asettaa.

Sisällöllinen rajaus prosessin vaihe, jossa saatuja hakutuloksia arvioidaan tieteelliseen tutkimuksen sopivaksi (Fink, 2019, 7). Tässä kirjallisuuskatsauksessa ei tehty varsinaista rajausta artikkeleissa käytettyjen menetelmien suhteen, mutta rajaus tehtiin enemmänkin sisällöllisesti lukemalla tiivistelmiä ja arvioimalla hakutulosten otsikoita. Näin katsaukseen soveltuvien artikkeleiden määrä putosi kahteentoista. Tämän avulla varmistuttiin

hakutulosten tieteellisestä laadusta ja sopivuudesta toteutettavaan tutkimukseen. Tässä prosessin vaiheessa oli tärkeää, että artikkeli käsitteli terveysvakuutuspetosten tunnistamista joko lohkoketjuteknologialla tai sen yhdistelmällä jonkin toisen teknologian kanssa. Rajaus laajennettiin koskemaan lohkoketjuteknologian yhdistelmiä muiden teknologioiden kanssa, koska useimmat petosten torjuntaan kehitetyt sovellukset edellyttävät lohkoketjuteknologian alustaa varmistaa tietojen turvallisuuden ja eheyden. Lopulta jäljellä olevat artikkelit seulottiin vielä sillä perusteella, kuinka hyvin ne soveltuivat asetettuihin tutkimuskysymyksiin ja lopullinen kirjallisuuskatsauksen aineisto muodostuu kahdeksasta tieteellisestä artikkelista. Edellä esitellyt prosessin vaiheet ovat tiivistetysti kuvattuna taulukossa 2.

Rajaustyyppi	Rajaus	Osumat
Tietokanta	Tampereen yliopiston Andor	
Hakusanalauseke	health AND (fraud OR fraudulent) AND insurance AND blockchain	221
Kirjallisuuden tyyppi	Vertaisarvioidut artikkelit	35
Sisällöllinen rajaus	Soveltuvuus tiivistelmän ja otsikon perusteella	12
Lopullinen rajaus	Soveltuvuus tutkimuskysymysten kannalta	8

Taulukko 2. Seulontaprosessi ja sisällöllinen rajaus

Taulukossa 3 esitellään kaikki valitut artikkelit kirjoittajineen, otsikoineen, julkaisukanavineen ja julkiasuvuosineen. Taulukon ensimmäisessä sarakkeessa on artikkelin tunnistenumero, jonka avulla kirjallisuuteen viitataan seuraavissa alaluvuissa.

Tunniste	Kirjoittajat	Otsikko	Julkaisukanava	Vuosi
1	Krishna, C., Kumar, D. & Dharmender S.K.	MedBlockSure: Blockchain-based insurance system	Cognitive Computation and Systems	2024
2	Mahapatra, S. & Sinha, D.	Smart h-Chain: A blockchain based healthcare framework with insurance fraud detection	Transactions on Emerging Telecommunications Technologies	2024
3	Zhang, G., Zhang, X., Bilal, M., Dou, W., Xu, X. & Rodrigues, J.	Identifying fraud in medical insurance based on blockchain and deep learning	Future Generation Computer Systems	2022
4	Kapadiya, K., Patel, U., Gupta, R., Alshehri, M.D., Tanwar, S., Sharma, G. & Bokoro, P.N	Blockchain and AI-empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects	IEEE Open Access Journals	2022
5	Ismail, L. & Zeadally, S.	Healthcare Insurance Frauds: Taxonomy and Blockchain-Based Detection Framework (Block-HI)	IEEE: IT Professional	2021
6	Jena, S.K., Kumar, B., Mohanty, B., Singhal, A. & Barik, R.C	An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry	Decision Analytics Journal	2024
7	El-Samad, W., Adda, M. & Atieh, M.	AI -Driven Data Aggregation Level Smart Contracts for Blockchain Healthcare Insurance Claims Adjudication	Procedia Computer Science	2024
8	Amponsah, A., Acheampong A., Adebayo F. & Weyori, B.A.	A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology	Decision Analytics Journal	2022

Taulukko 3. Kirjallisuuskatsauksen artikkelit

4.2 Tutkimusaineiston analyysi

Finkin mallin mukaan toteutettavan systemaattisen kirjallisuuskatsauksen viimeisin vaihe on itse synteessin tekeminen (Fink, 2019, 7). Tässä tutkimuksessa aineistoa käsitellään aineistolähtöisen sisällönanalyysin avulla, joka etenee kolmivaiheisen prosessin mukaisesti. Aineistolähtöinen sisällönanalyysi mahdollistaa laajan aineiston tiivistämisen ja jäsentämisen. Sen lisäksi tiivistetty ja jäsennetty aineisto parantaa tulkittavuutta ja selkeyttä. Tämän avulla voidaan tehokkaasti arvioida myös tutkimusten johdonmukaisuutta. Kolmivaiheinen prosessi koostuu pelkistämisestä, ryhmittelystä ja käsitteellistämisestä. (Miles & Huberman, 1994, 10; Tuomi & Sarajärvi, 2018, 90–91.)

Pelkistämisen prosessissa etsitään aineistosta ilmaisuja, jotka ovat relevantteja tutkimukselle. Tämän jälkeen aineistosta löytyneestä alkuperäisilmauksesta muodostetaan pelkistettyjä ilmauksia. (Tuomi & Sarajärvi, 2018, 90–92.) Seuraava vaihe tästä on ryhmittely. Ryhmittelyssä aineistosta poimituista alkuperäisilmauksista etsitään samankaltaisuuksia tai eroavaisuuksia. Tällä tavoin samankaltaiset pelkistetyt ilmaukset saadaan yhdisteltyä luokiksi. (Tuomi & Sarajärvi, 2018, 91–92.) Seuraavaksi tutkimuksessa havainnollistetaan näitä vaiheita käytännön esimerkein.

Ensimmäistä tutkimuskysymystä varten aineistosta etsittiin kohdat, jossa mainittiin lohkoketjuteknologian toimintaperiaatteesta tai vaikutuksesta vakuutuspetostorjuntaan. Tämän jälkeen näistä kohdista poimittiin ydinajatus ja pelkistettiin se ytimekkääksi ilmaisuksi. Toista tutkimuskysymystä varten aineistosta haettiin kohtia, joissa mainittiin tiedot, joita lohkoketjuteknologia tai sen yhdistelmäteknologiat hyödyntävät vakuutuspetosten torjunnassa. Taulukossa 4 esitellään lohkoketjuteknologian keskeisten ominaisuuksien ja sen vakuutuspetostorjuntaan luomien etujen pelkistämisen prosessia.

Tunniste	Alkuperäinen ilmaus	Pelkistetty ilmaus
3	Blockchain technology [12] is a mode to manage the generation, access, and use of trusted data through transparency and trust rules. A blockchain is typically managed by a peer-to-peer (P2P) network, the data stored on blockchain are unchangeable, non-forgable, and traceable.	Tietojen jäljitettävyyys Tietojen muuttumattomuus Tietojen turvallisuus Tietojen hajautettu luonne

Taulukko 4. Esimerkki pelkistämisestä

Ryhmittelyprosessin kuvaamisessa esimerkkinä käytetään toista tutkimuskysymystä. Toinen tutkimuskysymys käsittelee terveystakuutuspetoksissa tunnistamisessa hyödynnettäviä muuttujia. Kyseiselle kysymykselle tehtiin edellä esitetty pelkistämisen prosessi ja pelkistetyt ilmaukset listattiin alaluokkiin, joista saatiin muodostettua kolme pääluokkaa. Yhtä näistä alaluokista havainnollistetaan taulukossa 5.

Pääluokka	Pelkistetyt ilmaisut
Vakuutustapahtumaan liittyvä	Tiedot annetusta hoidosta
	Tutkimusten tulokset
	Korvausvaatimuksen suuruus
	Korvausvaatimuksen sisältö
	Maantieteellinen sijainti

Taulukko 5. Esimerkki ryhmittelystä

4.3 Lohkoketjuteknologian rooli terveysturvakuutuspetosten tunnistamisessa ja ehkäisyssä

Alla olevassa taulukossa 6 ryhmitellään lohkoketjuteknologian roolia terveysturvakuutuspetosten tunnistamisessa ja ehkäisyssä. Lohkoketjuteknologian ominaisuudet auttavat varsinkin petosten ehkäisyssä. Se tarjoaa myös alustan muille taulukossa esitellyille teknologioille. Näitä ominaisuuksia ja teknologioita käydään läpi tässä alaluvussa.

Lohkoketju- teknologia	Ominaisuudet	Läpinäkyvä ja turvallinen tietojen tallentaminen
		Hajautettu vertaisverkko
		Tiedon muuttumattomuus
		Reaaliaikainen tiedonsiirto
	Muiden teknologioiden hyödyntämisen mahdollistaja	Älykkäät sopimukset
		Koneoppiminen
		Syväoppiminen
		Esineiden internet

Taulukko 6. Teknologioiden ryhmittely

Tässä alaluvussa esitellään lohkoketjuteknologian keskeisimmät keinot ja ominaisuudet, joita hyödynnetään terveysturvakuutuspetosten tunnistamisessa ja ehkäisyssä. Ensinnäkin aineistosta tehtiin havainto, että lohkoketjuteknologian toimintaperiaatteet itsessään ovat terveysturvakuutuspetosten torjunnassa tärkeässä roolissa. Kyseinen havainto tehtiin sen perusteella, että jokaisessa kahdeksassa hyödynnetyssä artikkelissa korostettiin lohkoketjuteknologian luomaa turvallista, hajautettua ja muuttumatonta ympäristöä. [1,2,3,4,5,6,7,8].

Lohkoketjuteknologian tärkeimmät ominaisuudet ovat läpinäkyvä ja turvallinen tietojen tallentaminen, hajautettu vertaisverkko ja muuttumaton kirjanpito. Tietojen muuttumattomuus ja jäljitettävyyys esiintyvät jokaisessa artikkelissa oleellisina tekijöinä

terveysvakuutuspetosten tunnistamisessa. Lohkoketjuteknologia on monessa artikkelissa esitelty hajautettuna pääkirjajärjestelmänä, joka tallentaa ja säilyttää tietoja useissa solmuissa ilman kolmannen osapuolen tarvetta. Tietojen tallentaminen hajautettuun ja muuttumattomaan lohkoketjuun tekee tietojen manipuloinnista haastavaa sekä vähentää petosten mahdollisuuksia. Tämä johtuu siitä, että lohkoketju toimii hajautetun vertaisverkon varassa, ja jokainen lohkoketjuun lisättävä tieto vaatii lohkoketjun osapuolien suostumuksen. Kun tieto tallennetaan lohkoketjuun, se salataan kryptografisella suojauksella, mikä tekee tiedosta muuttumatonta. Mikäli tietoa halutaan muokata, tarvitaan jälleen kerran koko vertaisverkon suostumus. Lisäksi tieto tiedon muuttamisesta jää pysyvästi lohkoketjuun. Nämä ominaisuudet lisäävät lohkoketjuteknologian luottamusta ja turvallisuutta. Edellä mainitut ominaisuudet helpottavat manipulaation huomaamista huomattavasti. [1,2,3,4,5,6,7,8.] Esimerkiksi, jos korvauskäsittelijä yrittää jälkikäteen muokata vakuutusnottajan hoitotietoja tai vaatimuksen yksityiskohtia, lohkoketjuun jää pysyvä jälki muutoksesta, mikä helpottaa petoksen havaitsemista ja ehkäisyä.

Lohkoketjuteknologia tarjoaa lohkoketjun osallisille sidosryhmille suojatun alustan, jossa tiedot välittyvät osapuolelta toiselle reaaliajassa. Tietojen tallentaminen samaan järjestelmään mahdollistaa datan analysoinnin samaan aikaan. Tämä nopeuttaa terveysvakuutuspetosten tunnistamista ja mahdollistaa reaaliaikaisen vakuutuspetostorjunnan. Reaaliaikainen tietojen tallentaminen yhteiseen lohkoketjujärjestelmään tehostaa korvaushakemusten tarkastusprosessia. [1,4,6,7.] Oletetaan, että potilas käy lääkärissä ja saa tietyn diagnoosin. Lääkäri tallentaa diagnoosin ja hoitosuunnitelman lohkoketjujärjestelmään. Näin useat osapuolet, kuten sairaala, lääkäri, potilas ja vakuutusyhtiö, voivat tarkastella tätä tallennettua tietoa reaaliaikaisesti. Lohkoketju takaa, että tiedot ovat muuttumattomia ja jäljitettävissä, mikä estää niiden vääristelyn myöhemmin. Toisaalta jos jokin osapuoli on syöttänyt virheellisiä tai epäilyttäviä tietoja, tämä näkyy heti ja korvausprosessi voidaan pysäyttää ennen kuin korvausmaksuja maksetaan. [1,4,6,7.] Reaaliaikainen tieto mahdollistaa esimerkiksi lääkärishoppailun havaitsemisen heti ja voi estää tulevien käyntien korvauksien maksun. Lääkärishoppailulla tarkoitetaan useilla lääkäreillä käymistä, saadakseen useita korvauksia samasta vaivasta.

Lohkoketjuteknologian ominaisuudet ovat edistäviä tekijöitä terveysvakuutuspetosten tunnistamisessa, mutta monesti lohkoketjuteknologia on alustana välttämätön muiden teknologioiden tietoturvalliseen hyödyntämiseen. Lähes jokaisessa artikkelissa käytettiin lohkoketjuteknologian lisäksi jotain toista tai useampaa teknologiaa yhdessä [1,3,4,5,6,7,8]. Näiden teknologioiden hyödyntäminen ja kehittäminen edellyttää useimmiten turvallista alustaa, jonka lohkoketjuteknologia tarjoaa. Artikkeleissa nousi erityisesti muutama kategoria eniten esille. Lohkoketjuteknologiapohjaisia älykkäitä sopimuksia käytettiin jokaisessa artikkelissa. Lisäksi tekoälyä ja sen sovelluksia, kuten koneoppimista ja syväoppimista, käytettiin monissa artikkeleissa usein integroituna älykkäisiin sopimuksiin. Näiden lisäksi esineiden internetiä käytettiin muutamassa artikkelissa. Taulukossa 7 esitellään eri artikkeleissa hyödynnettyjä teknologioita.

Pääluokka	Teknologia	1	2	3	4	5	6	7	8
Lohkoketjuteknologia	Lohkoketjuteknologia	x	x	x	x	x	x	x	x
	Älykkäät sopimukset	x	x	x	x	x	x	x	x
Tekoäly	Koneoppiminen				x		x	x	x
	Syväoppiminen			x					
Muut teknologia	Esineiden internet				x		x		

Taulukko 7. Artikkeleissa hyödynnettyjen teknologioiden ryhmittely

Kuten jo teoriaosuudessa on kuvattu, älykkäät sopimukset suorittavat automaattisesti tehtäviä ennalta määritettyjen ehtojen mukaan. Terveysvakuutuskontekstissa tällaisia tehtäviä voivat olla muun muassa potilastietojen varmistaminen [1,2,8] ja lääkärinlausuntojen [2] tarkistaminen. Lisäksi älykkäät sopimukset voivat maksaa korvauksia [1,2,3,4,6,7], luoda korvauspäätöksiä [3,4,6,7,8] ja valvoa osapuolien pääsyä tietoihin [3]. Tapahtuman sisällön perusteella älykkäät sopimukset voivat määrittää, ketkä osapuolet ovat vastuussa sen aitouden vahvistamisesta. Esimerkiksi hoitokertomuksiin liittyvissä tapauksissa ne voivat edellyttää sekä potilaan että lääkärin hyväksyntää.

Tällainen älykkäisiin sopimuksiin pohjautuva prosessi auttaa torjumaan esimerkiksi laskutuspetoksia, koska se varmistaa, että tapahtuma perustuu todellisiin hoitotilanteisiin ja niiden dokumentaatioon. Lisäksi älykkäät sopimukset voivat vastaavalla logiikalla havaita muun muassa lääkärihoppailun (engl. doctor shopping), provisiopohjaiset petokset (engl. commission-based frauds), potilaiden itselle ohjaamisen (engl. self-referral) ja järjestelmän harhauttamisen (engl. ping-pong the system). Lääkärihoppailulla tarkoitetaan sitä, että potilas hakeutuu useiden lääkäreiden vastaanotoille saadakseen useita lääkärintodistuksia, reseptejä tai hoitosuunnitelmia. Näiden avulla hän voi hakea enemmän vakuutuskorvauksia kuin hänelle kuuluisi. Provisiopohjaiset petokset taas liittyvät tilanteisiin, joissa provisiopalkkainen osapuoli manipuloi tietoja saadakseen itselleen taloudellista hyötyä tai muita etuja. Potilaiden itselle ohjaaminen on toimintaa, jossa terveydenhuollon edustaja ohjaa potilaan tiettyyn hoitopaikkaan, josta ohjaaja voi itse hyötyä taloudellisesti. Tässä yhteydessä ei ole kyse potilaan hyödyn maksimoimisesta, vaan ohjaajan taloudellisesta hyödystä. Lisäksi järjestelmää voidaan yrittää harhauttaa esimerkiksi väärennettyjen lääkärintodistusten tai muiden tekaistujen tietojen luomisella. [5.]

Artikkelissa 5 käsiteltiin terveysvakuutuspetosten tunnistamista älykkäiden sopimusten avulla. Järjestelmän vertaisverkon osapuolia ovat muun muassa sairaalat, lääketieteen asiantuntijat, potilaat, diagnostiikkakeskukset, lääketieteellisten tarvikkeiden tarjoajat, farmasiayritykset ja farmaseutit. Vertaisverkon osapuolet olivat kaikki osa korvausvaateen vahvistusprosessia, mikä mahdollisti petosten havaitsemisen nopeammin ja tarkemmin, sillä kaikki osapuolet voivat tarkistaa ja todentaa tiedot reaaliajassa. Tämä vähentää inhimillisiä virheitä ja parantaa prosessin kokonaisvaltaista läpinäkyvyyttä. Järjestelmä auttoi sekä vähentämään väärinkäytöksistä aiheutuvia taloudellisia menetyksiä että parantamaan potilasturvallisuutta estämällä petosten mahdollisuuden, jotka voisivat vaarantaa potilaan hoidon laadun. [5.] Älykkäät sopimukset toimivat usein myös toisten teknologioiden rinnalla ja hyödyntävät niiden tuottamaa dataa ennalta määritettyjen ehtojen mukaisesti. Esimerkiksi syväoppimisen [3], koneoppimisen [4,6,7,8] ja esineiden internetin [4,6] rinnalla hyödynnettiin älykkäitä sopimuksia.

Lohkoketjuteknologioiden lisäksi tekoäly nousi aineistossa keskeiseksi teknologiaksi, jota hyödynnetään terveysvakuutuspetoksissa. Tekoälyyn kuuluvaa koneoppimista

hyödynnetään muun muassa korvausvaatimusten aitouden arvioinnissa. Aitouden arviointi on kytketty älykkääseen sopimukseen, joka siirtää vaatimuksen ihmiselle käsiteltäväksi tai vaihtoehtoisesti käsittelee vaatimuksen myönteisenä, mikäli vaatimus todetaan aidoksi [4,7,8]. Tämä voi tarkoittaa muun muassa vaatimuksen maksamista [4,7] tai korvauspäätöksen lähettämistä [8]. Lohkoketjualustalla toimivan koneoppimisen avulla voidaan saatujen tietojen avulla luoda turvallisesti terveystietojen ennustemalleja [4]. Artikkelissa 3 hyödynnettiin syväoppimista potilaskertomusten diagnoosien määrittelyyn avuksi. Jos potilaskertomuksen diagnoosi ja siihen merkitty ICD-10-koodi tunnistetaan loogiseksi, älykäs sopimus aktivoituu ja maksaa korvauksen suoraan. Muussa tapauksessa potilaskertomus tarkistetaan manuaalisesti. [3.]

Artikkeleissa 4 ja 6 hyödynnettiin esineiden internetiä. Esineiden internetiä hyödyntävät laitteet keräävät reaaliaikaista terveystietoa, kuten askelmäärää ja sydämen sykettä. Vakuutusyhtiö voi hyödyntää näitä tietoja muun muassa riskiarvioinnissa ja vakuutushinnoittelussa. Lisäksi vakuutusyhtiö voi luoda malleja vakuutusnottajan käytöksestä, jolloin epä johdonmukaisuudet voidaan havaita helpommin. Vakuutusnottaja, joka jakaa laitteidensa reaaliaikaisen datan vakuutusyhtiölle, voi aktiivisesti liikkumalla nauttia muun muassa edullisimmista vakuutusmaksuista. Näiden tietojen hyödyntämiseksi vaaditaan kuitenkin tiettyä tasoa tietosuojaa, jota lohkoketjuteknologia tarjoaa [4,6].

4.4 Terveystietojen tunnistamisessa hyödynnettävät muuttujat

Tässä alaluvussa esitellään tietoja, joita teknologiat hyödyntävät terveystietojen tunnistamisessa. Monissa artikkeleissa on tarkasteltu tiedon mahdollisia käyttömekanismeja yleisellä tasolla, mutta niissä ei ole täsmennetty, miten tai mihin terveystietokategoriassa tiettyä tietoa konkreettisesti hyödynnetään. Artikkeleissa teknologiat havaitsivat ja analysoivat tietoja vakuutus sopimuksista, korvaushakemuksista, lääkärinlausunnoista, laskuista tai muusta vakuutusyhtiön saatavilla olevista tiedoista. Tiedot liittyivät usein vakuutusnottajaan, kuten aiempaan maksuhistoriaan ja potilastietoihin. Lisäksi artikkeleissa käytettiin usein myös vakuutus tapahtumaan liittyviä

tietoja, kuten annetun hoidon tietoja, tutkimusten tuloksia sekä korvausvaatimuksen sisältöä ja suuruutta.

Kaiken kaikkiaan kirjallisuuskatsaukseen valikoituneissa artikkeleissa esiintyi hyvin monia erilaisia muuttujia, joita hyödynnettiin terveysvakuutuspetosten tunnistamisessa. Alla olevaan taulukkoon 8 on ryhmitelty artikkeleissa useimmin esiintyneitä muuttujia. Taulukkoon valittiin muuttujat, jotka mainittiin vähintään kahdessa artikkelissa. Tällä tavalla pystyttiin rajaamaan muuttujien määrää ja keskittymään useimmiten hyödynnettäviin muuttujiin. Muuttujat kategorisoitiin pääluokittain. Viimeisessä taulukon sarakkeessa näkyy, kuinka monta kertaa kyseinen muuttuja esiintyi artikkeleissa.

Pääluokka	Muuttuja	Esiintyminen
Vakuutustapahtumaan liittyvä	Tiedot annetusta hoidosta	8
	Tutkimusten tulokset	5
	Korvausvaatimuksen suuruus	5
	Korvausvaatimuksen sisältö	4
	Maantieteellinen sijainti	2
Vakuutuksenottajaan liittyvä	Vakuutuksenottajan maksuhistoria	6
	Vakuutuksenottajan aiemmat potilastiedot	4
	Vakuutuksenottajan henkilötiedot	2
	Terveyssovellusten ja -laitteiden data	2
Vakuutukseen liittyvä	Vakuutuksen turva	3

Taulukko 8. Käytettyjen muuttujien ryhmittely

Vakuutustapahtumaan liittyvät muuttujat olivat terveysvakuutuspetosten tunnistamisessa eniten hyödynnettyjä teknologioiden toimesta. Eniten hyödynnetty muuttuja oli tiedot annetusta hoidosta, sillä se mainittiin jokaisessa artikkelissa. Toinen monessa artikkelissa mainittu muuttuja oli tutkimusten tulokset. Artikkelissa 3 esiteltiin konkreettinen menetelmä,

jossa tiedot annetusta hoidosta ja tutkimusten tuloksista olivat erittäin keskeisessä roolissa. Tässä tutkimuksessa keskityttiin hoitolaitosten liioiteltuihin diagnooseihin, joita voidaan tunnistaa lohkoketjuteknologian ja syväoppimisen avulla. Joissakin maissa hoitolaitos laskuttaa diagnoosikoodin perusteella, joka voi motivoida lääkäriä tai hoitolaitosta merkkamaan potilaan vaivaan nähden vakavamman diagnoosikoodin. Tutkimuksessa rakennettiin malli, joka analysoi vakuutusnottajan eli potilaan vaivan ja vertaa sitä potilaan valitusten perusteella lääkärin antamaan ICD-10-diagnoosikoodiin. Jos malli havaitsee merkittävän poikkeaman, tiedot annetusta hoidosta tarkastetaan manuaalisesti. [3.]

Annetun hoidon tietojen lisäksi muita keskeisiä muuttujia olivat korvausvaatimuksen suuruus ja sisältö. Artikkelissa 5 lohkoketjuteknologiaan rakennettu älysovimus luokittelee vaatimuksen sisällön perusteella tapahtuman todellisuuden vahvistajat. Esimerkiksi annetun hoidon vahvistaa potilas ja lääkäri. Vahvistettua tietoa verrataan korvausvaatimuksen suuruuteen ja vakuutusyhtiöltä laskutettuihin palveluihin tai välineisiin. [5.] Teknologian avulla voidaan verrata korvausvaatimuksia laskutettujen palveluiden sisältöön ja laajuuteen, mikä helpottaa epäloogisuuksien, kuten tarpeettomien tai kokonaan suorittamatta jääneiden hoitojen tunnistamista. [3,4,5.]

Artikkeleissa esiteltiin myös useita vakuutusnottajaan liittyviä muuttujia, joista yleisimpiä olivat potilashistoria ja maksuhistoria. Vaikka näitä muuttujia mainittiin valituissa artikkeleissa, niiden konkreettista käyttöä ei juurikaan avattu tarkemmin. Useissa artikkeleissa kuitenkin korostettiin, että näiden muuttujien seuranta hyödynnetään lohkoketjujärjestelmissä. Eri osapuolia, kuten hoitolaitoksia, potilaita tai apteekkeja, pyydetään joko täydentämään tietoja [2, 6] tai sekä täydentämään että vahvistamaan tietoja [1, 3, 5]. Tällä käytännöllä pyritään lisäämään tietojen luotettavuutta ja vähentämään terveysvakuutuspetoksia.

Artikkeleissa 1,2,3 ja 7 esiteltiin vakuutusnottajan potilashistoria teknologian hyödyntämänä muuttujana [1,2,3,7]. Artikkelissa 7 tuotiin esille, että hyödyntämällä korvausvaatimuksen määrää, vakuutusturvan sisältöä sekä vakuutusnottajan henkilötietoja ja potilashistoriaa voidaan merkittävästi parantaa terveysvakuutuspetosten ennustemallien tehokkuutta [7]. Lohkoketjuteknologia-alustalla jokainen maksutapahtuma kirjataan muuttumattomaan pääkirjaan, mikä tekee niistä läpinäkyviä ja jäljitettäviä. Jos

petollista toimintaa havaitaan, maksutapahtuman suorittajat ja vastaanottajat voidaan helpommin jäljittää. [3,4,5,6,7,8.] Artikkelissa 6 tarkastellaan maksutapahtumia ja niiden muutoksia reaaliajassa. Esimerkiksi lisääntyneet epäonnistuneet maksutapahtumat tai yllättävät muutokset niiden volyymissa voivat viestiä epäilyttävästä toiminnasta. Näiden huomaaminen ajoissa on tärkeää, jotta voidaan reagoida uhkiin ja varmistua, että järjestelmä pysyy luotettavana. [6.]

Artikkeleissa 4 ja 6 esineiden internetiä käytettiin antamaan reaaliaikaista ja tarkkaa dataa esimerkiksi älyvaatteista ja -laitteista [4,6]. Artikkeleissa käytettiin älylaitteiden tarjoamaa tietoa käyttäjän terveydentilasta, kuten sykkeestä, kalorinkulutuksesta ja aktiivisuuden tasosta. Näitä muuttujia hyödynnettiin esimerkiksi epänormaalien käyttäytymismallien tunnistamiseen ja reaaliaikaiseen analyysiin. Lisäksi älylaitteet tarjoavat maantieteellistä sijaintitietoa, jonka avulla voidaan tunnistaa petollista toimintaa, jos korvausvaatimuksen tiedot poikkeavat älylaitteiden keräämistä tiedoista. Vakuutusentottajat voivat olla valmiita jakamaan älylaitteidensa tietoja vapaaehtoisesti turvalliselle lohkoketjualustalle, sillä luotettavan tietojen säilytyksen varmistaminen on monille erityisen tärkeää. Motivaatiota lisää myös se, että terveysdatan avulla olisi mahdollista kustomoida ja alentaa vakuutusmaksuja tai omavastuita, jos käyttäjä liikkuu aktiivisesti ja huolehtii terveydestään. Tällä tavalla sekä vakuutusyhtiö että asiakas voisivat hyötyä tästä muutoksesta parhaalla mahdollisella tavalla. [4,6.]

5 JOHTOPÄÄTÖKSET

5.1 Vastaukset tutkimuskysymyksiin

Tutkimuksen tavoitteena oli selvittää, miten lohkoketjuteknologia voi edistää terveysvakuutuspetosten tunnistamista ja ehkäisyä sekä mitkä muuttujat ovat keskeisiä tunnistamisprosessissa. Asetetut tutkimuskysymykset olivat:

1. Miten lohkoketjuteknologia voi edistää terveysvakuutuspetosten tunnistamista ja ehkäisemistä?
2. Mitä tietoja lohkoketjuteknologia hyödyntää terveysvakuutuspetosten tunnistamisessa?

Kirjallisuuskatsauksen avulla pystyttiin vastaamaan kattavasti tutkimuskysymyksiin ja saavuttamaan syvällistä ymmärrystä siitä, miten lohkoketjuteknologiaa voidaan hyödyntää terveysvakuutuspetosten tunnistamisessa. Tulokset osoittavat, että lohkoketjuteknologian tarjoamat ominaisuudet, kuten tiedon läpinäkyvyys ja muuttumattomuus, mahdollistavat terveysvakuutuspetosten tehokkaamman havaitsemisen ja ehkäisyn. Esimerkiksi lohkoketjuteknologian avulla voidaan varmistaa, että vakuutuksenottajan ja palveluntarjoajan väliset tiedot ovat yhdenmukaiset, mikä estää esimerkiksi väärien tai liioiteltujen korvausvaatimusten esittämisen. Lohkoketjuteknologia myös tarjoaa tietoturvallisen alustan vakuutuspetostorjunnassa hyödynnettäville teknologioille.

Tulosten mukaan lohkoketjuteknologian turvallisuus, jäljitettävyys ja tietojen muuttumattomuus tekevät siitä erinomaisen työkalun vakuutuspetosten torjuntaan. Myös Zheng ym. (2017) korostavat, että lohkoketjun tietojen muuttumattomuus estää petolliset muutokset vakuutustietoihin. Esimerkkinä voidaan ajatella tilannetta, jossa vakuutuksenottaja yrittää jälkikäteen korottaa sairauskulujaan. Lohkoketjun muuttumattomuus estää tämän, sillä alkuperäinen tapahtuma on tallennettu pysyvästi lohkokon. Lisäksi lohkoketjuteknologian kolmannen osapuolen tarpeettomuus mahdollistaa vakuutusprosessien suoraviivaistamisen ja kustannusten vähentämisen. Terveystieteiden huollon

palveluntarjoajat voivat jakaa potilastiedot suoraan lohkoketjussa ilman, että tietoja tarvitsee erikseen siirtää vakuutusyhtiölle. Näin eri osapuolilla on samat tiedot hallussa reaaliajassa. Tämä parantaa järjestelmän tehokkuutta, nopeuttaa korvausten käsittelyä ja vapauttaa resursseja esimerkiksi petosten tunnistamiseen.

Tulosten mukaan lohkoketjuteknologian katsotaan olevan sopiva erityisesti opportunististen petosten tunnistamiseen. Myös Viaenen ja Dedenen (2004) tutkimuksen tulokset ovat linjassa tämän kanssa. Heidän tutkimuksensa toi esiin vakuutuspetosten jaon koviin ja pehmeisiin petoksiin. Kovat petokset liittyvät suuriin, huolellisesti suunniteltuihin petoskokonaisuuksiin, joissa voi olla useita osapuolia mukana. Kova petos voisi olla sairaalahoidon järjestäminen tekaistujen potilaiden nimissä, jolloin suuri määrä sairaalamaksuja saadaan korvattua vakuutusyhtiöltä. Pehmeät petokset puolestaan perustuvat opportunistiseen käyttäytymiseen, kuten liioiteltuihin vaatimuksiin todellisista kuluista. Pehmeä petos voi olla todellisen sairaanhoitokulun ilmoittaminen kaksinkertaisena vakuutusyhtiölle perusteettomien korvausten saamiseksi.

Viaene ja Dedenen (2004) tutkimuksen mukaan pehmeitä petoksia esiintyy huomattavasti enemmän, ja niiden yhteenlaskettu taloudellinen vaikutus on suurempi kuin kovien petosten. Tämän vuoksi erityisesti pehmeiden petosten torjuminen auttaa hillitsemään petoksista aiheutuvia vaikutuksia. Heidän tutkimuksessaan todetaan pehmeiden petosten johtuvan pääasiassa tiedon epäsymmetriasta. Tämän tutkielman mukaan lohkoketjuteknologian mahdollistama osapuolten välinen tiedon jakaminen vähentää tiedon epäsymmetriaa, mikä näin ollen tekee pehmeiden petosten toteuttamisesta vaikeampaa. Tällä tavoin lohkoketjuteknologia voi siis auttaa tunnistamaan ja ehkäisemään näitä petoksia.

Lohkoketjuteknologia tarjoaa tietoturvallisen alustan myös muille vakuutuspetostorjunnassa hyödynnettäville teknologioille. Näiden teknologioiden hyödyntäminen täydessä potentiaalissaan vaatii kuitenkin luotettavan alustan, jonka lohkoketjuteknologia tarjoaa. Tulosten mukaan eniten lohkoketjun kanssa hyödynnetty teknologia on älykkäät sopimukset. Älykkäät sopimukset ovat lohkoketjupohjainen ratkaisu, jonka avulla voidaan automatisoida terveysvakuutuspetosten tunnistamista. Tärkeimpiä toimintoja ovat potilastietojen tarkistaminen ja kategorisointi. Älykkäät sopimukset suorittavat ennalta

määritettyjen ehtojen mukaan tarkastuksia ja merkitsevät epäilyttäviä tapahtumia, mikä parantaa prosessin tehokkuutta. Älykkäiden sopimusten ohella hyödynnettiin myös muita teknologioita. Erityisesti tekoälysovellukset, kuten koneoppiminen ja syväoppiminen, olivat laajasti käytössä, ja lisäksi esineiden internetiä hyödynnettiin. Tekoälypohjaiset teknologiat olivat aineistossa keskeisessä roolissa.

Lyeonov ym. (2024) ovat tuoreessa kirjallisuuskatsauksessaan tarkastelleet tekoälyn, erityisesti koneoppimisen, roolia rahoitusalan rikollisuuden torjunnassa. Heidän tuloksensa tukevat tämän tutkielman havaintoja, sillä molemmat osoittavat, että tekoälypohjaiset ratkaisut pystyvät analysoimaan suuria tietomääriä ja havaitsemaan poikkeavuuksia tehokkaasti. Lisäksi tutkimuksen mukaan nämä ratkaisut ovat vähentäneet niin sanottujen väärin hälytysten määrää ja parantaneet petosten tunnistamisen tarkkuutta. Tässä tutkielmassa saatujen tulosten mukaan tekoälysovellukset analysoivat muun muassa potilastietoja ja havaitsevat niistä poikkeamia, kuten epätavallisen korkeita lääkäri- tai lääkekuluja. Lohkoketjuteknologia takaa näiden tietojen eheyden, mikä lisää analyysin luotettavuutta. Myös nämä havainnot ovat linjassa Lyeonov ym. (2024) tulosten kanssa.

Lisäksi esineiden internetin osalta tulokset ovat hyvin samankaltaisia Lyeonov ym. (2024) kanssa. He nostavat esiin esineiden internetin yhdistämisen näihin teknologioihin, mikä avaa uusia mahdollisuuksia reaaliaikaiseen datan hallintaan ja analysointiin. Tämä ei ole tärkeää vain vakuutuspetosten tunnistamisessa, vaan myös uusien vakuutus tuotteiden kehittämisessä. Esineiden internetiä hyödyntävät laitteet, kuten älykellot, keräävät tietoja, kuten sykettä ja sijaintia, jotka tallennetaan lohkoketjuun. Näitä tietoja voidaan hyödyntää vakuutuspetosten havaitsemiseen vertaamalla niitä ilmoitettuihin tapahtumiin. Esimerkiksi loukkaantumisloukituksen yhteydessä kyseiset laitteet voivat varmistaa, onko käyttäjän fyysinen aktiivisuus todella laskenut tai onko sijainti paikkansapitävä, vähentäen väärin korvausvaatimusten riskiä.

Nämä edellä mainitut tutkimukset tukevat saatuja tuloksia, jotka korostavat teknologioiden, kuten lohkoketjuteknologian, tekoälyn ja esineiden internetin, roolia vakuutuspetosten torjunnassa ja ehkäisyssä. Ne vahvistavat myös reaaliaikaisen datan käsittelyn tärkeyttä ja osoittavat, että teknologioiden integrointi parantaa sekä tehokkuutta että tarkkuutta.

Yhdistettynä kehittyneet teknologiat tarjoavat merkittäviä etuja terveysturvakuutuspetosten torjunnassa. Näiden teknologioiden avulla voidaan parantaa tiedonhallinnan turvallisuutta, vähentää kustannuksia ja nopeuttaa prosesseja, mikä luo luotettavampia ja tehokkaampia ratkaisuja vakuutuslalle.

Toinen tutkimuskysymys käsitteli erityisesti sitä, millaisia muuttujia seurataan ja käytetään petosten tunnistamisprosessissa. Tuloksista ilmeni, että teknologiat hyödyntävät laajasti erilaisia tietoja. Vakuutuksenottajaan liittyviä tietoja, kuten potilashistoriatietoja ja maksuhistoriaa käytettiin paljon. Kuitenkin annetun hoidon tietoja, tutkimustuloksia ja korvausvaatimuksien sisältöä sekä suuruutta tarkkailtiin tulosten mukaan eniten.

Tulokset eivät sinänsä ole yllättäviä, sillä nämä tiedot ovat helposti saatavilla ja analysoitavissa. Erityisesti korvausvaatimukseen liittyvien tietojen tarkkailu on tärkeässä roolissa, sillä vakuutuspetokset tapahtuvat yleisimmin juuri korvausta hakiessa. Sen lisäksi hoitolaitosten tuottamien raporttien, kuten lääkärinlausuntojen ja tutkimustulosten, tarkkailu yhdessä laskujen kanssa ei yllätä, sillä tällä tavoin poikkeavuuksia voidaan huomata tehokkaammin teknologiaa hyödyntäen. Monissa artikkeleissa käsiteltiin käytettäviä muuttujia, mutta tarkempaa tietoa siitä, miten näitä tietoja hyödynnetään eri terveysturvakuutusten petoskategorioissa, tarvitaan vielä merkittävästi lisää.

Kuitenkin muuttujat, joita eri tutkimuksissa käytettiin, ovat samankaltaisia kuin tässä tutkimuksessa todettiin. Li ym. (2008) tutkimuksessa tutkittiin terveydenhuollon petosten tunnistamista tilastollisin menetelmin. Tässä tutkimuksessa käytettiin muun muassa korvausvaatimusten analyysia, jossa yksittäisiä vaatimuksia verrattiin tavanomaisiin hoitopolkuihin ja tunnistettiin epäsäännöllisyyksiä, kuten hoidollisesti tarpeettomia toimenpiteitä tai liiallista laskutusta. Lisäksi analysoitiin toistuvia ja epätyypillisiä hoitoja sekä palveluiden ajallisia epäkohonmukaisuuksia. Tutkimuksessa hyödynnettiin myös potilaaseen eli vakuutuksenottajaan liittyviä tietoja, kuten demografisia tietoja ja maksuhistoriaa. Myös Obodoekwen ja van der Haarin (2018) tutkimuksessa esiteltiin osittain samoja ja lisäksi samankaltaisia muuttujia. Muun muassa lääkärin kirjoittamia ICD-10-koodeja ja hoitopolkuja vertailtiin tyypillisiin vastaaviin. Annettu hoito, joka ei täyttänyt perinteisiä lääketieteellisiä standardeja, merkittiin korvauskäsittelijän manuaalista

tarkastusta varten. Myös laskutettuja palveluja analysoitiin, esimerkiksi ylihinnoittelun tai tarpeettomien palveluiden tunnistamiseksi. Tutkimuksessa analysoitiin myös vakuutusurva ja vakuutusopimuksen ehtoja suhteessa korvausvaatimukseen. Tässäkin tutkimuksessa otettiin huomioon vakuutuksenottajan maksuhistoria. Aiempien tutkimusten tulokset käytetyistä muuttujista vastasivat tämän kandidaatintutkielman tuloksia.

Tulosten perusteella voidaan myös todeta, että petosten havaitseminen vaatii usein monenlaista tietoa vilpillisen toiminnan tunnistamiseksi. Tällainen tieto voi olla aikaisempaa historiatietoa, jota verrataan uuteen tietoon. Vaihtoehtoisesti voidaan tarkastella kahta samaan asiaan liittyvää tietoa ja vertailla niiden eroavaisuuksia, joiden perusteella voidaan tunnistaa mahdollisia petosmalleja. Tämänkaltaisten vertailujen tekeminen on kuitenkin huomattavan hidasta ihmisten toimesta verrattuna uusiin teknologioihin. Lohkoketjuteknologian tarjoama alusta, jossa kaikki tarvittavat tiedot ovat parhaimmillaan helposti saatavilla, parantaa petostorjunnan tehokkuutta ja takaa tietojen luotettavan säilytyksen.

Aiempia tutkimuksia täysin samasta aiheesta on varsin vähän. Tutkimuksen tulokset ovat kuitenkin pitkälti vastaavanlaisia verrattuna aiempiin tutkimustuloksiin ja teoriaan. Lohkoketjuteknologian hyödyntäminen vakuutuspetostorjunnassa on korostunut terveydenhuoltosektorilla, sillä kyseinen sektori säilyttää massiivisia määriä arkaluonteista tietoa. Sen vuoksi myös lohkaketjuteknologiaa on alettu soveltamaan terveystakuutusten käsittelyyn ja petosten tunnistamiseksi.

Myös muilla sektoreilla tietoturva on nähty merkittävänä haasteena, johon lohkaketjuteknologia tarjoaa potentiaalisia ratkaisuja. Mateen ym. (2023) tarkastelevat tutkimuksessaan lohkaketju- ja pilvipohjaista ratkaisua autovakuutusten hallintaan, erityisesti tehokkuuden parantamisen ja vakuutuspetosten ehkäisyn näkökulmasta. Tutkimuksen keskeisiä teemoja ovat tietojen turvallinen tallennus, vakuutuspetosten tunnistaminen, tietoturvan parantaminen sekä korvauskäsittelyn automatisointi. Mateen ym. (2023) saavuttivat pitkälti samoja johtopäätöksiä kuin tämä tutkimus: tiedon turvallinen jakaminen ja jäljitettävyyys korostuivat keskeisinä elementteinä vakuutuspetosten torjunnassa.

Park ja Ryun (2019) tutkimuksessa tutkittiin lohkoketjuteknologian roolia terveysvakuutuksessa tietojen jakamisen ja vakuutuspetosten ehkäisyn näkökulmasta. Heidän tutkimuksessaan nousi ilmi erityisesti lohkoketjuteknologian avulla saavutettava informaation symmetria osapuolten välille. Heidän tutkimuksessaan nousi esille muun muassa tietojen muuttumattomuus ja vaatimusten käsittely reaaliajassa mikä ehkäisee mahdollisten välikäsien luomaa manipulaatoriskiä. Myös Norta ym. (2019) tutkimuksessa korostettiin informaation epäsymmetriaa ongelmana, johon ratkaisuna esitettiin lohkoketjuteknologiaa sen pysyvän luonteen vuoksi.

5.2 Tutkimuksen arviointi ja jatkotutkimusehdotukset

Tutkimuksen luotettavuutta ja onnistumista voidaan arvioida validiteetin ja reliabiliteetin avulla (Saaranen-Kauppinen & Puusniekka, 2009, s. 25–26). Reliabiliteetin eli toistettavuuden osalta tutkimus on toteutettu huolellisesti. Tutkimuksessa käytetyn aineiston keruu- ja analyysiprosessi on kuvattu tarkasti, mikä parantaa tutkimuksen läpinäkyvyyttä ja toistettavuutta. Aineistohakuprosessissa käytetyt rajaukset, kuten tietokantojen ja hakusanojen valinta, on dokumentoitu asianmukaisesti. Lisäksi asetettujen käytännön seulojen valinnat on perusteltu tutkimuksessa. Koska tutkimuksen aihe on uusi ja aihetta käsitteleviä artikkeleita on rajallinen määrä, tämä voi osaltaan heikentää tutkimuksen reliabiliteettia. Kirjallisuuskatsaukseen valittiin tämän vuoksi ainoastaan kahdeksan artikkelia, jotta aineiston laadusta ei tarvitsisi tinkiä.

Validiteetin eli pätevyyden kannalta on keskeistä, että tutkimukseen valitut artikkelit vastaavat mahdollisimman hyvin asetettua tutkimusasetelmaa ja tutkimuskysymyksiä, mikä tuki tutkimuksen tavoitteiden saavuttamista. Valitut artikkelit käsitelivät tutkimuksen aihetta varsin rajatusti, mutta tämän ansiosta tutkimuskysymyksiin saatiin selkeitä ja kohdennettuja vastauksia. Kuitenkin tutkimuksen tekninen luonne näkyi monissa artikkeleissa. Osa artikkeleista keskittyi tutkimuksen kannalta tarpeettoman paljon teknisiin yksityiskohtiin, kuten algoritmeihin ja käytännön järjestelmän toteutukseen. Tämä haaste tunnistettiin jo tutkimuksen suunnitteluvaiheessa, minkä vuoksi artikkeleita valittiin tiivistelmien ja otsikoiden perusteella siten, että tutkimuksen kannalta epäolennaisiin teknisiin toteutuksiin

keskittyvät aineistot rajattiin tarkasti katsauksen ulkopuolelle. Lisäksi aineiston englanninkielisyys tuo mukanaan riskin ymmärrysvirheet, mutta tätä riskiä on pyritty vähentämään tarkastelemalla käännöksiä huolellisesti sekä hyödyntämällä teknisiä apuvälineitä ja kriittistä arviointia. Haasteiden ennakointi ja niiden järjestelmällinen huomioiminen tutkimusprosessissa vahvistaa tutkimuksen validiteettia, sillä mahdollisten ongelmien vaikutus johtopäätöksiin on näin onnistuttu minimoimaan.

Tutkimusta suunniteltaessa tehtiin aiheeseen liittyviä hakuja, ja kirjallisuuskatsauksen toteutusvaiheessa, muutama kuukausi myöhemmin ilmeni, että aiheesta oli julkaistu uusi artikkeli. Tämä korostaa tutkimusaiheen ajankohtaisuutta. Aihe on melko uusi, mikä käy ilmi myös siitä, että aihetta käsitteleviä tutkimuksia on rajallinen määrä. Vaikka aihetta ei ole juurikaan tutkittu Suomessa, kansainvälisesti vastaavia tutkimuksia on kuitenkin saatavilla. Ilmiön uutuus sekä saatavilla olevan aiemman tutkimuksen rajallinen määrä voi kuitenkin rajoittaa tutkimuksen syvyyttä ja laajuutta. Lisäksi ajankohtaisen aiheen tutkiminen tarkoittaa, että tutkimusympäristö muuttuu nopeasti, mikä voi vaikuttaa tutkimuksen relevanssiin ja tulosten yleistettävyyteen.

Teknologian kehityksen myötä myös petosyritykset kehittyvät, mikä tekee vakuutuspetosten torjuntamenetelmien tutkimisesta ja kehittamisestä entistä tärkeämpää. Aiheen ajankohtaisuus ja merkitys yhdistettynä suomenkielisen tutkimuksen vähäisyyteen korostavat tarvetta lisätä alan tutkimusta Suomessa. Aihe tarjoaa runsaasti mahdollisuuksia jatkotutkimukselle, erityisesti lohkoketjuteknologian ja Suomen lainsäädännön yhteensovittamisen näkökulmasta. Esimerkiksi lohkoketjun muuttumattomuuden ja EU:n yleisen tietosuojasetuksen GDPR:n (2016/679) ”oikeus tulla unohdetuksi” (engl. right to be forgotten) liittyvien vaatimusten yhteensovittaminen on tärkeä tutkimuskohde. Lisäksi jatkotutkimuksessa voitaisiin tarkastella, miten lohkoketjun sääntelyn vähäisyys vaikuttaa lohkoketjun käyttöönottoon vakuutuslalla Suomessa.

LÄHDELUETTELO

Kirjallisuuslähteet

- Amponsah, A. A., Adekoya, F., & Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology. *Decision Analytics Journal*, 4(1), 100122. <https://doi.org/10.1016/j.dajour.2022.100122>
- Al-Quayed, F., Humayun, M., & Tahir, S. (2023). Towards a secure technology-driven architecture for smart health insurance systems: An empirical study. *Healthcare (Basel)*, 11(16), 2257. <https://doi.org/10.3390/healthcare11162257>
- Ali, D. (2019). Blockchain for insurance and claims fraud detection. In *2019 International Conference on Biomedical Innovations and Applications*. IEEE. <https://doi.org/10.1109/BIA48344.2019.8967456>
- Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. *Sensors*, 22(19), 7162. <https://doi.org/10.3390/s22197162>
- Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022). Insurance fraud detection: Evidence from artificial intelligence and machine learning. *Research in International Business and Finance*, 62, 101744-. <https://doi.org/10.1016/j.ribaf.2022.101744>
- Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*, 9, 61048–61073. <https://doi.org/10.1109/ACCESS.2021.3073466>
- Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation*, 2(1), Article 20. <https://doi.org/10.1186/s40854-016-0039-4>
- Canillas, R., Talbi, R., Bouchenak, S., Hasan, O., Brunie, L., & Sarrat, L. (2018). Exploratory study of privacy preserving fraud detection. In *Proceedings of the 19th International Middleware Conference Industry* (pp. 25–31). Association for Computing Machinery. <https://doi.org/10.1145/3284028.3284032>
- Dean, D. H. (2004). Perceptions of the ethicality of consumer insurance claim fraud. *Journal of Business Ethics*, 54(1), 67-79. Springer Nature. <https://doi.org/10.1023/B:BUSI.0000043493.79787.e6>

- Derrig, R. A. (2002). Insurance fraud. *Journal of Risk and Insurance*, 69(3), 271–287. <https://doi.org/10.1111/1539-6975.00026>
- Duman, E. A., & Sağıroğlu, Ş. (2017). Healthcare fraud detection methods and new approaches. *Gazi University, Computer Engineering Department*. <https://doi.org/10.1109/UBMK.2017.8093544>
- El-Samad, W., Adda, M., & Atieh, M. (2024). AI-Driven Data Aggregation Level Smart Contracts for Blockchain Healthcare Insurance Claims Adjudication. *Procedia Computer Science*, 241, 63–68. <https://doi.org/10.1016/j.procs.2024.08.011>
- Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention. *Police Research Series* (98). Policing and Reducing Crime Unit.
- Fink, A. (2019). *Conducting research literature reviews: from the Internet to paper* (Fifth edition.). Sage publications.
- Gera, J., Palakayala, A. R., Rejeti, V. K. K., & Anusha, T. (2020). Blockchain technology for fraudulent practices in insurance claim process. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1068-1075). IEEE. <https://doi.org/10.1109/ICCES48766.2020.9138012>
- Gomes, C., Jin, Z., & Yang, H. (2021). Insurance fraud detection with unsupervised deep learning. *Journal of Risk and Insurance*, 88(3), 591–624. <https://doi.org/10.1111/jori.12359>
- Grabowski, D. C. (2007). Medicare and Medicaid: Conflicting incentives for long-term care. *Milbank Quarterly*, 85(4), 579–610. <https://doi.org/10.1111/j.1468-0009.2007.00502.x>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications*, 193, 116429-. <https://doi.org/10.1016/j.eswa.2021.116429>
- Hyman, D. A. (2001). Health Care Fraud and Abuse: Market Change, Social Norms, and the Trust “Reposed in the Workmen.” *The Journal of Legal Studies*, 30(S2), 531–567. <https://doi.org/10.1086/324674>
- Ismail, L., & Zeadally, S. (2021). Healthcare Insurance Frauds: Taxonomy and Blockchain-Based Detection Framework (Block-HI). *IT Professional*. doi:10.1109/MITP.2021.3071534

- Jena, S. K., Kumar, B., Mohanty, B., Singhal, A., & Barik, R. C. (2024). An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. *Decision Analytics Journal*, 10, 100411. <https://doi.org/10.1016/j.dajour.2024.100411>
- Johnson, M. E., & Nagarur, N. (2016). Multi-stage methodology to detect health insurance claim fraud. *Health Care Management Science*, 19(3), 249–260. <https://doi.org/10.1007/s10729-015-9321-1>
- Jokela, T., Poikonen, P., Ranta, K., & Westerling, T. (2021). *Vapaaehtoinen henkilövakuutus*. Jyväskylä: FINVA.
- Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science (American Association for the Advancement of Science)*, 349(6245), 255–260. <https://doi.org/10.1126/science.aaa8415>
- Jyrinsalo, H. (2024). *Ajoneuvovakuutuspetosten havaitseminen teknologian avulla*. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Kandidaatintutkielma.
- Kajwang, B. (2022). IMPLICATIONS FOR BIG DATA ANALYTICS ON CLAIMS FRAUD MANAGEMENT IN INSURANCE SECTOR. *International Journal of Technology and Systems*, 7(1), 60–71. <https://doi.org/10.47604/ijts.1592>
- Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. *IEEE Access*, 10. <https://doi.org/10.1109/ACCESS.2022.3194569>
- Kar, A. K., & Navin, L. (2021). Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telematics and Informatics*, 58, 101532. <https://doi.org/10.1016/j.tele.2020.101532>
- Klavus, J., Pekurinen, M., Järvelin, J., & Mikkola, H. (2005). Sairausvakuutus terveydenhuollon rahoitusmuotona. *Kansantaloudellinen aikakauskirja*, 101(3).
- Kuusisto, M. (2021). *Vilppiin ja petoksiin liittyvien vahinkotapausten ratkaisut vakuutuslautakunnassa*. Tampereen yliopisto. Johtamisen ja talouden tiedekunta. Kandidaatintutkielma.
- Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
- Li, J., Huang, K. Y., Jin, J., & Shi, J. (2008). A survey on statistical methods for health care fraud detection. *Health Care Management Science*, 11(3), 275–287. <https://doi.org/1007/s10729-007-9045-4>

- Li, J., Lan, Q., Zhu, E., Xu, Y., & Zhu, D. (2022). A study of health insurance fraud in China and recommendations for fraud detection and prevention. *Journal of Organizational and End User Computing*, 34(4). <https://doi.org/10.4018/JOEUC.301271>
- Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, 19(5), 653–659. [https://doi.org/10.6633/IJNS.201709.19\(5\).01](https://doi.org/10.6633/IJNS.201709.19(5).01)
- Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security: October 24-28, 2016, Vienna, Austria /*, 16–269. <https://doi.org/10.1145/2976749.2978309>
- Luukkonen, I., Mäntyniemi, L., Pekonen-Ranta, M., Raulos, V., & Santavirta, P. (2018). Vakuutuslainsäädäntö ([5. painos].). FINVA Finanssikoulutus Oy.
- Lyeonov, S., Draskovic, V., Kubaščíkova, Z., & Fenyves, V. (2024). Artificial intelligence and machine learning in combating illegal financial operations: Bibliometric analysis. *Human Technology*, 20(2), 325–360. <https://doi.org/10.14254/1795-6889.2024.20-2.5>
- Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35(8), 2337–2354. <https://doi.org/10.1016/j.tele.2018.10.004>
- Mahapatra, S., & Sinha, D. (2023). Smart h-Chain: A blockchain-based healthcare framework with insurance fraud detection. *Transactions on Emerging Telecommunications Technologies*, 35(2). <https://doi.org/10.1002/ett.4911>
- Mateen, A., Khalid, A., Lee, S. & Nam, S.Y. (2023). Challenges, issues, and recommendations for blockchain and cloud-based automotive insurance systems. *Applied Sciences*, 13(6), 3561. <https://doi.org/10.3390/app13063561>
- Mattila, Yrjö. 2011. Suuria käännekohtia vai tasaista kehitystä? Tutkimus Suomen terveydenhuollon suuntaviivoista. Sosiaali- ja terveysturvan tutkimuksia 116. Kelan tutkimusosasto.
- McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135, 62–75. <https://doi.org/10.1016/j.jnca.2019.02.027>
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2). Thousand Oaks: Sage.
- Mohammed, M. A., Boujelben, M., & Abid, M. (2023). A novel approach for fraud detection in blockchain-based healthcare networks using machine learning. *Future Internet*, 15(8), 250. <https://doi.org/10.3390/fi15080250>

- Morley, N. J., Ball, L. J., & Ormerod, T. C. (2006). How the detection of insurance fraud succeeds and fails. *Psychology, Crime & Law*, 12(2), 163–180. <https://doi.org/10.1080/10683160512331316321>
- Murray, M. (2019). Tutorial: A descriptive introduction to the blockchain. *Communications of the Association for Information Systems*, 45, Article 25. Saatavilla: <https://doi.org/10.17705/1CAIS.04525>
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin. <https://bitcoin.org/bitcoin.pdf>
- Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: Pros, cons and SWOT. *Cluster Computing*, 22(Suppl 6), 14743–14757. <https://doi.org/10.1007/s10586-018-2387-5>
- Norta, A., Rossar, R., Parve, M. & Laas-Billson, L. (2019). Achieving a high level of open market-information symmetry with decentralised insurance marketplaces on blockchains. *Advances in Intelligent Systems and Computing*, 997, 299–318. https://doi.org/10.1007/978-3-030-22871-2_22
- Obodoekwe, N., & van der Haar, D. T. (2018). A critical analysis of the application of data mining methods to detect healthcare claim fraud in the medical billing process. In M. Elhadef, A. Mellouk, M. T. Khadir, & A. Meddeb (Eds.), *Ubiquitous Networking (UNet 2018)* (pp. 320–330). Springer. https://doi.org/10.1007/978-3-030-03402-3_28
- Paaso, J. (2017). *Petos ja vakuutuskorvaukset*. Lapin yliopisto. Rikosoikeus. Maisteritutkielma.
- Park, D. & Ryu, D. (2019). Blockchain in health insurance: Sharing medical information and preventing insurance fraud. *Korean Journal of Financial Studies*, 48(4), 417–447. <https://doi.org/10.26845/KJFS.2019.08.48.4.417>
- Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive-based approach. *IEEE Access*, 10, 87115–87134. <https://doi.org/10.1109/ACCESS.2022.3198956>
- Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S., Chattopadhyay, A., & Lam, K.-Y. (2018). A blockchain framework for insurance processes. In *Proceedings of the 2018 International Conference on New Technologies, Mobility and Security* (pp. 1–4). <https://doi.org/10.1109/NTMS.2018.8328731>
- Rantala, J. & Kivisaari, E. (2020). *Vakuutusoppi*. FINVA
- Rashidian, A., Joudaki, H., & Vian, T. (2012). No evidence of the effect of the interventions to combat health care fraud and abuse: A systematic review of literature. *PLoS One*, 7(8), <https://doi.org/10.1371/journal.pone.0041988>

- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems*, 88, 173–190. <https://doi.org/10.1016/j.future.2018.05.046>
- Roriz, R., & Pereira, J. L. (2019). Avoiding insurance fraud: A blockchain-based solution for the vehicle sector. *Procedia Computer Science*, 164, 211–218. <https://doi.org/10.1016/j.procs.2019.12.174>
- Saajos, A. (2020). *Petokset vakuutuslalla*. Vaasan ammattikorkeakoulu. Oikeushallinto. Opinnäytetyö.
- Saaranen-Kauppinen, A., & Puusniekka, A. (2009). Menetelmäopetuksen tietovaranto KvaliMOTV. Kvalitatiivisten menetelmien verkko-oppikirja. Yhteiskuntatieteellisen tietoarkiston julkaisuja, 2.
- Saldamli, G. (2020). Health care insurance fraud detection using blockchain. In 2020 Seventh International Conference on Software Defined Systems (SDS). San Jose State University, San Jose, CA, USA. <https://doi.org/10.1109/SDS49854.2020.9143900>
- Salminen, A. (2011). Mikä kirjallisuuskatsaus? : Johdatus kirjallisuuskatsauksen tyypeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopisto.
- Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6), 599–608. <https://doi.org/10.1007/s12599-020-00656-x>
- Su, C. P., Asfaw, A., Tamers, S. L., & Luckhaupt, S. E. (2019). Health insurance coverage among U.S. workers: Differences by work arrangements in 2010 and 2015. *American Journal of Preventive Medicine*, 56(5), 673–679. <https://doi.org/10.1016/j.amepre.2018.12.010>
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Incorporated.
- Tennyson, S. (2008). Moral, social, and economic dimensions of insurance claims fraud. *Social Research*, 75(4), 1181. <https://doi.org/10.1353/sor.2008.0020>
- Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and describing the types of fraud in healthcare. *Procedia Computer Science*, 64, 713–720. <https://doi.org/10.1016/j.procs.2015.08.594>
- Timonen, E. (2020). *Tutkintaan johtaneet omaisuusvahingot Suomessa vuosina 2008–2018*. Jyväskylän ammattikorkeakoulu. Liiketalouden ala. Opinnäytetyö.
- Tomatsu, Y., & Han, W. (2023). Bitcoin and renewable energy mining: A survey. *Blockchains*, 1(2), 90–110. <https://doi.org/10.3390/blockchains1020007>

- Treleaven, P., Gendal Brown, R., & Yang, D. (2017). Blockchain technology in finance. *Computer*, 50(9), 14–17. <https://doi.org/10.1109/MC.2017.3571047>
- Tuomi, J., & Sarajarvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos). Tammi.
- Tumminello, M., Consiglio, A., Vassallo, P., Cesari, R., & Farabullini, F. (2022). Insurance fraud detection: A statistically validated network approach. *Journal of Risk and Insurance*, 90(2), 381–419. <https://doi.org/10.1111/jori.12415>
- Tuorila, H. (2019). Aikuisten vapaaehtoiset sairauskuluvakuutukset suomalaisilla terveystarkkinoilla. Kilpailu- ja kuluttajaviraston selvityksiä 2/2019.
- Viaene, S., & Dedene, G. (2004). Insurance Fraud: Issues and Challenges. Geneva Papers on Risk and Insurance. Issues and Practice, 29(2), 313–333. <https://doi.org/10.1111/j.1468-0440.2004.00290.x>
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., & Song, H. (2016). Where is current research on blockchain technology? A systematic review. *PLOS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- Zhang, G., Zhang, X., Bilal, M., Dou, W., Xu, X., & Rodrigues, J. J. P. C. (2022). Identifying fraud in medical insurance based on blockchain and deep learning. *Future Generation Computer Systems*, 130, 140–154. <https://doi.org/10.1016/j.future.2021.12.006>
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). IEEE. <https://doi.org/10.1109/BigDataCongress.2017.85>

Verkkolähteet

- Borrelli, L. (2024). What is private health insurance? *Forbes Advisor*. Saatavilla: <https://www.forbes.com/advisor/health-insurance/private-health-insurance/> (Viitattu: 5.11.2024)
- EU-terveydenhoito.fi. (n.d.). Mitä maksan hoidosta julkisessa terveydenhuollossa? EU-Terveystenhoito. Saatavilla: <https://www.eu-terveydenhoito.fi/hoitoon-ulkomailta-suomeen/terveydenhuoltojarjestelma-suomessa/mita-maksan-hoidosta-julkisessa-terveydenhuollossa/> (Viitattu: 11.11.2024)

- Finanssiala. (2018). Vakuutuspetoksia tehtaillaan arviolta 30 miljoonan euron edestä. Saatavilla: <https://www.finanssiala.fi/uutiset/vakuutuspetoksia-tehtaillaan-arviolta-30-miljoonan-euron-edesta/> (Viitattu: 6.10.2024)
- Finanssiala. (2021). Hyvä vakuutustapa ja vakuutustoiminnan yleiset periaatteet. Saatavilla: <https://www.finanssiala.fi/aiheet/hyva-vakuutustapa-ja-vakuutustoiminnan-yleisetperiaatteet/#3> (Viitattu: 3.10.2024)
- Finanssiala. (2022). Vakuutustutkimus 2022. Saatavilla: <https://www.finanssiala.fi/julkaisut/vakuutustutkimus-2022/> (Viitattu: 3.10.2024)
- Finanssiala. (2023). Vakuutuspetos on rikos ja rikoksella on seuraamuksia – yhtiöiden tutkinnassa viime vuonna 2 500 epäselvää vahinkoilmoitusta. Saatavilla: <https://www.finanssiala.fi/uutiset/vakuutuspetos-on-rikos-ja-rikoksella-on-seuraamuksia-yhtioiden-tutkinnassa-viime-vuonna-2-500-epaselvaa-vahinkoilmoitusta/> (Viitattu: 3.10.2024)
- Gill, M., & Randall, A. (2015). Insurance fraudsters: A study for the ABI. *Perpetuity Research & Consultancy International Ltd*. Saatavilla: www.perpetuityresearch.com (Viitattu: 11.10.2024)
- IAIS. (2011). Application paper on deterring, preventing, detecting, reporting and remedying Fraud in insurance. Saatavilla: www.iaisweb.org (Viitattu: 4.10.2024)
- Insurance Europe (2013). The impact of insurance fraud. Saatavilla: <https://www.insuranceeurope.eu/mediaitem/0bf0af82-e7ef-4439-a763-d7862859d421/The+impact+of+insurance+fraud.pdf> (Viitattu: 10.10.2024)
- Insurance Europe. (2019). Insurance fraud: Not a victimless crime. Saatavilla: <https://www.insuranceeurope.eu/publications/703/insurance-fraud-not-a-victimless-crime/> (Viitattu: 9.10.2024)
- Insurance Europe. (2024). Annual report 2023–2024. Saatavilla: <https://www.insuranceeurope.eu/publications/3112/annual-report-2023-2024> (Viitattu: 3.10.2024)
- Kansaneläkelaitos. (2024). Sairausvakuutusmaksut. Kela.fi. Saatavilla: <https://www.kela.fi/tyonantajat-sairausvakuutusmaksut> (Viitattu: 7.10.2024)
- Kerkelä, L. (2024). Kauneushoitolassa tapahtui poikkeuksellisen paljon ”vahinkoja” – Taustalta paljastui vakuutus-yhtiön työn-tekijän ja asiakkaan jättihuijaus. Helsingin Sanomat. Saatavilla: <https://www.hs.fi/suomi/art-2000010602080.html> (Viitattu: 6.10.2024)
- Kilroy, A. (2024). Insurance fraud statistics 2024. Forbes Advisor. Saatavilla: <https://www.forbes.com/advisor/insurance/fraud-statistics/> (Viitattu: 6.10.2024)

- Niemelä, P. (2024). Vakuutuspetosyrityksissä korostuvat nämä piirteet: "On tullut vastaan tilanteita, joissa vakuutus on hankittu kolaripaikalla". POP Vakuutus. Saatavilla: <https://www.popvakuutus.fi/tiedotteet-ja-media/lehdistotiedotteet/vakuutuspetosyrityksissa-korostuvat-nama-piirteet> (Viitattu: 1.10.2024)
- Pohjola Vakuutus. (n.d). Terveysvakuutus – Vakuutus sairauden ja tapaturman varalta. Saatavilla: www.op.fi (Viitattu: 20.11.2024)
- PwC. (2023). Impact of artificial intelligence on fraud and scams. PwC UK. Saatavilla: <https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf> (Viitattu: 3.10.2024)
- Rahkola, M. (2019). Katsaus lohkoketjuteknologioiden hyödyntämiseen Suomessa: Raportti tulevaisuusvaliokunnalle. *Eduskunnan tulevaisuusvaliokunnan julkaisu* 1/2019. Saatavilla: https://www.eduskunta.fi/FI/naineduskuntatoimii/julkaisut/Documents/NETTI_TUVJ_1_2019_Lohkoketjuteknologiat.pdf (Viitattu: 21.10.2024)
- Yle. (2021). Terveyskuluvakuutusten suosio kasvaa yhä- Tukija: "Suomessa on perheitä, joissa ei ole sukupolviin käyty terveystieteissä". Saatavilla: <https://yle.fi/a/3-11758911> (Viitattu: 3.10.2024)

Oikeudelliset lähteet

- HE 87/2019 Hallituksen esitys eduskunnalle sosiaaliturva- ja vakuutuslainsäädännön muuttamiseksi EU:n yleisen tietosuojasetuksen johdosta.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016). *Official Journal*, L 119, 1-88.
- Rikoslaki (39/1889)
- Vakuutuslakia (543/1994)