Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Žan Pižmoht

Sistem za zagotavljanje zaupanja v dobavni verigi zdravil z uporabo verige blokov

magistrsko delo

magistrski študijski program druge stopnje
računalništvo in informatika

Mentor: prof. dr. Vlado Stankovski
Somentor: doc. dr. Petar Kochovski

Ljubljana, 2025

Zahvala

Na tem mestu zapišite, komu se zahvaljujete za izdelavo magistrske naloge. V zahvali se poleg mentorja spodobi omeniti vse, ki so s svojo pomočjo prispevali k nastanku vašega izdelka.

Žan Pižmoht, 2025

Vsem rožicam tega sveta.

"The only reason for time is so that everything doesn't happen at once."

— Albert Einstein

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
CA	classification accuracy	klasifikacijska točnost
DBMS	database management system	sistem za upravljanje podatkovnih baz
SVM	support vector machine	metoda podpornih vektorjev
...	...	...

Povzetek

Naslov: Sistem za zagotavljanje zaupanja v dobavni verigi zdravil z uporabo verige blokov

V vzorcu je predstavljen postopek priprave magistrskega dela z uporabo okolja LaTeX. Vaš povzetek mora sicer vsebovati približno 100 besed, ta tukaj je odločno prekratek. Dober povzetek vključuje: (1) kratek opis obravnavanega problema, (2) kratek opis vašega pristopa za reševanje tega problema in (3) (najbolj uspešen) rezultat ali prispevek magistrske naloge.

Ključne besede

zaupanje, tehnologija veriženja blokov, dobavna veriga zdravil

Abstract

Title: Trust System in Pharmaceutical Supply Chain Using Blockchain

This sample document presents an approach to typesetting your BSc thesis using LaTeX. A proper abstract should contain around 100 words which makes this one way too short. A good abstract contains: (1) a short description of the tackled problem, (2) a short description of your approach to solving the problem, and (3) (the most successful) result or contribution in your thesis.

Keywords

trust, blockchain, pharmaceutical supply chain

Poglavje 1

Uvod

Poglavje 2

Pregled literature in ozadje

2.1 Zaupanje

Pojem zaupanja je temeljni gradnik pri zasnovi našega sistema za farmacevtsko dobavno verigo. Zaupanje je kompleksen, večdimenzionalen in interdisciplinaren koncept, ki ga obravnavajo različne vede. Obravnava se v sociologiji, psihologiji, ekonomiji, računalništvu in še ostalih vedah. Prav zaradi te raznolikosti v literaturi ne obstaja enotna definicija, temveč več pristopov, ki poudarjajo različne vidike [1, 2].

2.1.1 Definicije zaupanja

V družboslovnem kontekstu je zaupanje pogosto opredeljeno kot stanje pozitivnih pričakovanj glede dejanj druge osebe v okoliščinah, kjer obstaja določena stopnja tveganja [3]. Gambetta [4] zaupanje definira kot subjektivno verjetnost, da bo agent opravil določeno dejanje, še preden je to mogoče preveriti. Mayer, Davis in Schoorman [5] pa ga opredelijo kot pripravljenost ene stranke, da se izpostavi ranljivosti glede na dejanja druge stranke, ob pričakovanju, da bo ta delovala v skladu s pričakovanji.

V digitalnem okolju se koncept zaupanja prenaša iz družbenega v tehnični kontekst. Denning [6] trdi, da je zaupanje v sistem lastnost, ki jo je mogoče formalno določiti in jo modelirati. Sistem je torej zaupanja vreden, če mu

njegovi uporabniki zaupajo glede na opaženo skladnost z vnaprej določenimi standardi. Grandison in Sloman [2] zaupanje obravnavata kot kvalificirano prepričanje zaupnika o kompetentnosti, integriteti, varnosti in zanesljivosti zaupanja vrednega subjekta.

2.1.2 Lastnosti zaupanja

Zaupanje je po svoji naravi večdimenzionalen pojem, ki ga ni mogoče zajeti z eno samo definicijo. V literaturi se ponavlja, da zaupanje vključuje čustvene in vedenjske komponente, ki se med seboj prepletajo in vplivajo na odločanje posameznika ali sistema [7, 8]. V družbenem kontekstu gre za pripravljenost posameznika, da se izpostavi tveganju na podlagi prepričanja, da bo druga stran delovala predvidljivo in skladno s pričakovanji. V informacijskih sistemih pa to pomeni sposobnost sistema, da sprejema odločitve o sodelovanju na podlagi preteklih izkušenj in ocenjene zanesljivosti entitet.

Zaupanje obstaja le v razmerju med dvema ali več entitetami, kjer ena zaupa drugi v določeni situaciji ali kontekstu. Takšno razmerje je dinamično, saj se lahko stopnja zaupanja sčasoma povečuje ali zmanjšuje. Poleg tega je zaupanje asimetrično: dejstvo, da entiteta A zaupa entiteti B, še ne pomeni, da bo tudi B zaupala A [5].

Ena od osrednjih značilnosti zaupanja je njegova povezanost s tveganjem in negotovostjo. Zaupanje je smiselno le v okoliščinah, kjer obstaja možnost, da drugi akter ne bo ravnal skladno s pričakovanji [3]. Če bi imeli popoln nadzor ali popolno informacijo, zaupanje sploh ne bi bilo potrebno. V kontekstu varnostnih in distribucijskih sistemov zaupanje dopolnjuje formalne zaščitne mehanizme, kot so avtentikacija in šifriranje, saj omogoča oceno vedenja akterjev tam, kjer tehnični ukrepi ne zadostujejo [6].

Zaupanje je tudi subjektivno in kontekstualno. Različni akterji lahko enake vedenjske vzorce interpretirajo različno, odvisno od svojih ciljev, izkušenj, regulatornih zahtev, prepričanj itn.

2.1.3 Atributi zaupanja

Da bi bilo zaupanje uporabno v digitalnem okolju, ga je potrebno izraziti z merljivimi atributi, ki opisujejo lastnosti ali vedenje zaupanja vrednega subjekta. Ti atributi omogočajo, da se konceptualna ideja zaupanja preslika v formalne modele. V literaturi se pojavljajo različne skupine atributov.

Klasični modeli, kot sta Mayer, Davis in Schoorman [5] ter McKnight in Chervany [7], opredeljujejo tri temeljne dimenzije zaupanja: kompetentnost, integriteto in dobrohotnost. Kompetentnost se nanaša na sposobnost entitete, da učinkovito izvede nalogo, integriteta na njeno zavezanost etičnim in profesionalnim načelom, dobrohotnost pa na odsotnost namere povzročiti škodo. Kasneje so bili tem trem dodani še predvidljivost in zanesljivost, ki poudarjata konsistentnost vedenja skozi čas.

V digitalnih in porazdeljenih okoljih so se pojavili dodatni atributi, ki izhajajo iz tehničnih vidikov zaupanja. Grandison in Sloman [2] zaupanje opišeta kot prepričanje o kompetentnosti, varnosti in verodostojnosti drugega subjekta. Denning [6] poudarja, da je zaupanja vrednost sistema mogoče ocenjevati tudi z vidika varnosti, skladnosti s pravili ter preverljivosti delovanja. Ti atributi omogočajo formalno ocenjevanje zaupanja med akterji.

V farmacevtski dobavni verigi imajo atributi zaupanja izrazito regulatorno in sledilno komponento. Uddin in sodelavci [9] poudarjajo, da so pri zagotavljanju zaupanja ključni kazalniki sledljivost, pristnost in celovitost podatkov. Kayhan in sodelavci [10] izpostavljajo še pomen transparentnosti, nespremenljivosti in izvorne sledljivosti (angl. *provenance*), ki jih omogoča tehnologija veriženja blokov.

Predstavljeni atributi ne predstavljajo univerzalne množice meril, temveč zbirko značilnosti, ki jih lahko posamezen akter uporabi pri lastni presoji zaupanja. V sistemu, ki je predstavljen v tej nalogi, se atributi uporabljajo predvsem kot podatkovne lastnosti (angl. *data properties*) v ontologiji. Te omogočajo, da akterji formalno zapišejo svoje kriterije za ocenjevanje drugih entitet. S tem v sistemu omogočamo standardizirano predstavitev vhodnih metrik, ki jih posamezni akterji uporabljajo pri svojem algoritmu za

izračunavanje zaupanja.

2.2 Upravljanje zaupanja v razpršenih sistemih

Huaizhi Li in Mukesh Singhal v članku *Trust Management in Distributed Systems* [11] opredelita upravljanje zaupanja kot proces zbiranja informacij, potrebnih za vzpostavitev zaupanja med entitetami, ter dinamičnega spremljanja in prilagajanja obstoječih razmerij zaupanja. Avtorja poudarjata, da v razpršenih okoljih kot so internet, sistemi enakovrednih entitet (angl. `peer-to-peer`) in mobilna omrežja ad hoc pogosto sodelujejo entitete, ki se med seboj ne poznajo. Zato zaupanje postane ključni mehanizem za zmanjšanje tveganja in zagotavljanje sodelovanja. Namen sistema za upravljanje zaupanja je ohranjati ažurne in skladne informacije o zaupanju med akterji v omrežju.

2.2.1 Dokazni modeli zaupanja

Dokazni modeli temeljijo na preverljivih dokazih, kot so digitalna potrdila, javni ključi ali kriptografski podpisi. Ti pristopi zagotavljajo preverjanje identitete in integritete entitet, ne pa tudi njihove dejanske zanesljivosti. Najpogostejša primera sta hierarhični sistem X.509 [12] in decentralizirani sistem PGP [13], kjer se zaupanje posreduje prek verige certifikatov oziroma prek subjektivnih ocen uporabnikov. Tak model se uporablja predvsem pri inicializaciji zaupanja in zagotavlja osnovno preverjanje pristnosti brez ocenjevanja vedenja.

2.2.2 Priporočilni modeli zaupanja

Priporočilni modeli gradijo zaupanje na osnovi izkušenj in posredovanih ocen drugih entitet. Vsaka entiteta ocenjuje druge glede na pretekle interakcije, te ocene pa se lahko delijo naprej kot priporočila. Model uporablja pogojno

tranzitivnost zaupanja – entiteta A lahko zaupa entiteti C, če A zaupa B kot priporočitelju in lahko ovrednoti njegovo oceno.

Pri tem se uporablja zvezna vrednost zaupanja tv_T med 0 in 1, izračunana iz vrednosti priporočil po poti $A \to B \to C \to D$. Za končno vrednost se uporabi zmnožek delnih zaupanj na poti:

$$tv_T = \prod_{i=1}^{n} \frac{rtv(i)}{4} \times tv(T)$$

kjer $rtv(i)$ predstavlja stopnjo zaupanja v posameznega posrednika, $tv(T)$ pa končno vrednost zaupanja v ciljno entiteto. Če obstaja več poti med akterjema, se končna vrednost določi kot povprečje rezultatov posameznih poti.

2.2.3 Porazdeljeno ocenjevanje zaupanja

V omrežjih enakovrednih akterjev (angl. *peer-to-peer*) se zaupanje ocenjuje decentralizirano. Vsako vozlišče vodi lastno evidenco interakcij in vrednoti druge glede na uspešnost sodelovanja. Xiong in Liu predlagata metriko, ki temelji na razmerju med pozitivnimi in negativnimi interakcijami:

$$T(u,t) = \frac{\sum_{v \in P, v \neq u} S(u,v,t)\, Cr(v,t)}{\sum_{v \in P, v \neq u} I(u,v,t)}$$

kjer $S(u,v,t)$ označuje zadovoljstvo uporabnika u z v do časa t, $Cr(v,t)$ je korekcijski faktor za filtriranje povratnih informacij, $I(u,v,t)$ pa število interakcij med u in v. Rezultat $T(u,t)$ je vedno v intervalu $(0,1)$ in predstavlja trenutno stopnjo zaupanja v entiteto. Sistem lahko določi pragove C_1 in C_2, pri čemer entiteta velja za zaupanja vredno, če velja $I(u,t) > C_1$ in $T(u,t) > C_2$.

Takšni sistemi so učinkoviti pri akumuliranju ocen, vendar občutljivi za napačne ali zlonamerne povratne informacije. Zato številne rešitve uvajajo uteževanje priporočil glede na zanesljivost virov ali časovno starost podatkov.

2.2.4 Dinamično posodabljanje zaupanja

Ker se vedenje akterjev sčasoma spreminja, se mora zaupanje prilagajati novim podatkom. Posodobitev vrednosti se pogosto izvede z amortizacijskimi ali diskontnimi faktorji, ki dajejo večjo težo nedavnim interakcijam. Primer takega mehanizma je izračun nove vrednosti zaupanja po zaključeni interakciji:

$$T_{\text{new}} = \frac{r + N\, T_{\text{old}}\, e^{-\beta \Delta t}}{1 + N\, e^{-\beta \Delta t}}$$

kjer T_{old} predstavlja prejšnjo vrednost zaupanja, r novo oceno po transakciji, N število izvedenih interakcij, β faktor dušenja, Δt pa čas od zadnje posodobitve. Na ta način sistem zagotavlja, da nove izkušnje hitreje vplivajo na oceno, stare pa postopoma izgubijo težo.

2.2.5 Povezava z našo rešitvijo

Predstavljeni modeli zaupanja predstavljajo osnovo za delovanje razvitega sistema. Vsak akter v dobavni verigi lahko uporabi svoj način izračuna zaupanja, ki temelji na dokazih, priporočilih ali dinamičnih metrikah. Sistem ne vsiljuje enotnega algoritma, temveč omogoča, da akter sam oblikuje pravila na podlagi podatkov iz ontologije. Rezultati teh izračunov se shranjujejo v verigo blokov, ki deluje kot skupen in trajen zapis ocen. S tem smo združili različne pristope v enoten sistem, kjer je zaupanje merljivo in preverljivo.

2.3 Farmacevtske dobavne verige

2.3.1 Značilnosti in pomen sledljivosti

Farmacevtska dobavna veriga je ena najbolj reguliranih in kompleksnih industrijskih verig. Vključuje proizvajalce, distributerje, prevoznike, lekarne, regulatorne agencije in končne uporabnike [14]. Zaradi velikega števila vmesnih akterjev in globalnega obsega poslovanja je nadzor nad izvorom in kakovostjo zdravil zahtevna naloga.

Sledenje zdravilom omogoča identifikacijo posamezne serije skozi celoten življenjski cikel izdelka, od proizvodnje do izdaje pacientu [10]. Natančno beleženje gibanja zdravil preprečuje vstop ponaredkov v sistem in omogoča hitro ukrepanje ob odpoklicih ali neskladjih. Sledljivost je zato neposredno povezana z varnostjo pacientov in zaupnostjo zdravstvenega sistema [15].

Za zagotavljanje sledljivosti so regulatorji uvedli stroge predpise. Evropska unija je sprejela Direktivo o ponarejenih zdravilih (2011/62/EU) [16] in Delegirano uredbo (EU) 2016/161 [17], ki zahtevata enolično označevanje embalaže z dvodimenzionalno kodo in uporabo evropskega sistema EMVS. V ZDA podobno vlogo opravlja zakon DSCSA, ki uvaja popolnoma digitalno sledenje zdravil do leta 2025 [18].

Ti ukrepi predstavljajo pomembne korake k večji sledljivosti, vendar še vedno temeljijo na centraliziranih bazah podatkov, kjer posamezni akterji nimajo popolnega vpogleda v celotno verigo.

2.3.2 Izzivi in tveganja

Kljub regulacijam farmacevtske dobavne verige ostajajo izpostavljene številnim tveganjem. Največji problem predstavljajo ponarejena in neustrezna zdravila, katerih število v zadnjih letih narašča. Po podatkih Svetovne zdravstvene organizacije je bilo med letoma 2017 in 2021 zabeleženih 877 incidentov ponarejenih ali neustreznih medicinskih izdelkov, kar pomeni povprečno letno rast za 36 % [19]. Ti izdelki so bili zaznani v vseh regijah sveta, tudi v državah z razvitimi regulativnimi sistemi. Ponarejena zdravila so lahko neučinkovita ali nevarna, njihova prisotnost pa neposredno ogroža zdravje pacientov in zmanjšuje zaupanje javnosti v zdravstvene sisteme.

Drugo tveganje izhaja iz razdrobljenosti informacijskih sistemov. Podatki o serijah, skladiščih in pošiljkah se pogosto hranijo v ločenih bazah, ki med seboj niso povezane [9]. To povzroča zamude, napake in oteženo preverjanje izvora zdravila. Centralizirane rešitve, kot je EMVS, sicer izboljšajo preverjanje avtentičnosti, vendar ne rešujejo težave zaupanja med različnimi organizacijami, ki podatke ustvarjajo in posredujejo.

Poleg ponarejanja in pomanjkljive sledljivosti se pojavljajo tudi tveganja, povezana z motnjami v dobavi zdravil. V kriznih obdobjih, kot so pandemije ali politične napetosti, se zaradi pomanjkanja podatkov o zalogah in zanesljivosti partnerjev pogosto pojavijo nepričakovane prekinitve dobav. Takšni dogodki razkrivajo, kako pomembno je zaupanje med organizacijami in pravočasna izmenjava podatkov.

Kljub tehnološkim in pravnim izboljšavam obstoječi modeli še vedno ne zagotavljajo celovitega vpogleda v dogajanje znotraj verige. Potrebne so rešitve, ki združujejo varno upravljanje podatkov, decentralizirano preverjanje in semantično usklajevanje informacij med akterji.

2.3.3 Regulativni okvir in trenutne rešitve

Evropska zakonodaja temelji na Direktivi o ponarejenih zdravilih (2011/62/EU) [16] ter Delegirani uredbi (EU) 2016/161 [17]. Skupaj uvajata obvezne varnostne elemente na embalaži, dvodimenzionalno kodo ter sistem EMVS (European Medicines Verification System). EMVS omogoča preverjanje serijske številke ob izdaji zdravila, pri čemer nacionalni sistemi NMVS sodelujejo prek skupnega evropskega vozlišča. Sistem učinkovito zazna poskuse ponarejanja v zadnji fazi distribucije, ne omogoča pa vpogleda v celotno zgodovino serije, saj temelji na centralizirani arhitekturi [10].

V ZDA sledljivost ureja zakon DSCSA (Drug Supply Chain Security Act), ki je del zakona DQSA iz leta 2013 [18]. DSCSA uvaja elektronsko izmenjavo treh vrst podatkov: transakcijske informacije, zgodovine transakcij in izjave o skladnosti. Sistem zahteva popolnoma interoperabilno sledljivost do leta 2025. Kljub napredku ameriški model ostaja pretežno centraliziran, podatki pa se prenašajo predvsem med neposrednimi poslovnimi partnerji [9].

Na mednarodni ravni Svetovna zdravstvena organizacija (WHO) pripravlja smernice za dobre distribucijske prakse in spremlja pojav ponarejenih in neustreznih izdelkov.

Za izpolnjevanje regulativnih zahtev podjetja uporabljajo različne informacijske platforme, med katerimi so najpogostejše centralizirane rešitve, kot

so EMVS, TraceLink in SAP ATTP. Te rešitve izboljšujejo sledljivost serij in avtomatizirajo poročanje regulatorjem, vendar ne omogočajo skupnega vpogleda v podatke ali preverjanja zanesljivosti akterjev po celotni verigi [10]. Podatkovni tokovi ostajajo razdrobljeni, zanašajo pa se tudi na zaupanja vredne posrednike.

V zadnjem desetletju se pojavljajo projekti, ki preučujejo uporabo tehnologije veriženja blokov v farmacevtskih dobavnih verigah. Projekta MediLedger v ZDA in PharmaLedger v Evropi uporabljata porazdeljene zapise za izboljšanje integritete in sledljivosti podatkov [9]. Takšni pristopi dokazujejo, da blockchain omogoča nespremenljivost zapisov in enostavnejše preverjanje informacij, vendar večinoma rešujejo le problem integritete podatkov.

Kljub temu večina rešitev ostaja usmerjena v zaupanje v podatke, medtem ko je upravljanje zaupanja med posameznimi organizacijami pogosto implicitno, vezano na statične pravice dostopa ali vnaprej dogovorjene pogodbeno–pravne odnose. Manj je pristopov, kjer bi lahko vsak akter izrecno definiral svoje kriterije zaupanja in iz njih izpeljal odločitve o sodelovanju. Prav v tej vrzeli se umešča sistem, predstavljen v tej nalogi, ki kombinira semantični model dobavne verige, subjektivne politike zaupanja in zapis rezultatov v verigo blokov.

2.4 Tehnologija veriženja blokov v dobavnih verigah

Tehnologija veriženja blokov je bila prvič predstavljena leta 2008 v sklopu kriptovalute Bitcoin [20]. Osnovna ideja je zasnova podatkovne strukture, ki povezuje zapise v verigo blokov. Vsak blok vsebuje podatke, kriptografski povzetek prejšnjega bloka in časovno oznako. Takšna vezava med bloki preprečuje naknadne spremembe podatkov, saj bi sprememba v enem bloku povzročila neujemanje celotne verige [21].

Veriga blokov deluje v porazdeljenem omrežju, kjer vsako vozlišče hrani kopijo celotne verige. Soglasje o pravilnem zaporedju blokov se doseže s

konsenznim mehanizmom. V javnih verigah se pogosto uporabljata Proof of Work ali Proof of Stake, medtem ko dovoljena omrežja uporabljajo lažje mehanizme, ki temeljijo na znanih udeležencih. Zaradi porazdeljene narave sistem ne potrebuje centralne avtoritete, kar omogoča zanesljivo beleženje podatkov v okolju z različnimi deležniki.

Poleg javnih omrežij, kot je Ethereum, so v praksi pogosta dovoljena omrežja, kjer je dostop omejen na pooblaščene organizacije. Primer takšnega sistema je Hyperledger Fabric [22]. Ta pristop omogoča višjo prepustnost, večjo zasebnost podatkov in nadzor nad identitetami v omrežju. V dobavnih verigah so takšne lastnosti ključne, saj morajo podjetja varovati poslovne podatke, hkrati pa zagotavljati zanesljivo izmenjavo informacij.

Verige blokov omogočajo nespremenljiv zapis dogodkov, preverljivo zgodovino podatkov in enoten pogled na transakcije, kar so pomembne zahteve farmacevtskih dobavnih verig.

2.4.1 Pametne pogodbe

Pametne pogodbe predstavljajo enega ključnih konceptov sodobnih verig blokov. Gre za programe, ki se shranijo in izvajajo neposredno v verigi blokov ter se sprožijo, ko so izpolnjeni določeni pogoji. Ethereum je prvi uvedel splošno platformo za izvajanje pametnih pogodb prek navideznega stroja EVM (Ethereum Virtual Machine), ki omogoča deterministično izvajanje kode na vseh vozliščih omrežja [23].

Pametne pogodbe omogočajo avtomatizacijo pravil in procesov, pri čemer ni potrebno zaupati enemu samemu posredniku. Njihovo delovanje je predvidljivo, saj se vedno izvršijo natančno tako, kot je določeno v kodi. Zaradi teh lastnosti se pogosto uporabljajo v scenarijih, kjer je treba uveljaviti dogovorjena pravila med neodvisnimi akterji. V dobavnih verigah se uporabljajo za potrjevanje dogodkov, registracijo premikov blaga ter preverjanje skladnosti podatkov.

V modelih, ki temeljijo na verigi blokov, pametne pogodbe služijo tudi kot enotna plast poslovne logike. S tem omogočajo, da vsi akterji delujejo

na osnovi istega sklopa pravil. To je posebej pomembno v okoljih, kjer se morajo organizacije dogovarjati o interpretaciji podatkov ali izvajanju procesov. Pametne pogodbe z nespremenljivo kodo zagotovijo, da se pravila ne spreminjajo brez soglasja deležnikov.

V predstavljenem sistemu ima pametna pogodba osrednjo vlogo, saj hrani rezultate ocenjevanja zaupanja in omogoča preverjanje vzpostavljenih razmerij med akterji. Pogodba vsebuje funkcije za zapisovanje rezultatov, njihovo posodabljanje in preverjanje stanja zaupanja. S tem tvori register zaupanja, ki je dostopen vsem udeležencem verige.

2.4.2 Oraklji in zunanje zaupne storitve

Pametne pogodbe delujejo znotraj verige blokov in nimajo neposrednega dostopa do zunanjih podatkov. Ta omejitev je posledica zasnove verig blokov, ki morajo zagotoviti deterministično in ponovljivo izvajanje kode. Zaradi tega pametna pogodba ne more sama pošiljati zahtev v zunanje sisteme ali zbirati podatkov iz okolja. Težava je znana kot orakeljski problem [21].

Oraklji predstavljajo mehanizem, ki omogoča prenos podatkov iz zunanjega sveta v pametno pogodbo. So posredniki, ki sprejemajo zunanje informacije, jih po potrebi obdelajo in nato posredujejo v verigo blokov. Najbolj razširjeni pristopi vključujejo decentralizirana orakljska omrežja, kot je Chainlink, kjer več neodvisnih vozlišč poda svoje rezultate, pametna pogodba pa izračuna skupno vrednost [**?**]. Tak pristop zmanjša tveganje posameznih napak in omogoča večjo zanesljivost.

Oraklji se razlikujejo glede na stopnjo zaupanja in način validacije podatkov. V dovoljenih omrežjih so oraklji pogosto del infrastrukture sodelujočih organizacij. Podatki so podpisani, vsak posrednik pa je znan in preverljiv. To omogoča večjo varnost in jasen nadzor nad tem, kdo posreduje podatke v sistem. V primerjavi z javnimi omrežji je takšen model bolj primeren za poslovna okolja, kjer morajo organizacije upoštevati pogodbe, regulatorne zahteve in politike zasebnosti.

V predstavljenem sistemu delujejo oraklji kot most med sklepnim meha-

nizmom in pametno pogodbo. Vsak akter izvede lokalni izračun zaupanja na podlagi ontologije in lastnih pravil. Rezultat ocenjevanja se nato pošlje v verigo blokov kot podpisana transakcija. Pametna pogodba prejme več neodvisnih ocen in na tej osnovi določi končni status zaupanja med akterji. Tak pristop omogoča, da odločitev ne temelji na enem samem viru, temveč na več porazdeljenih izračunih, ki odražajo različne perspektive v verigi.

2.5 Semantični splet in ontološke metode

2.5.1 RDF, OWL in orodja za ontologijo

2.5.2 Ontologija zaupanja

2.6 Ontologija zaupanja

2.6.1 Koncepti in odnosi

2.6.2 SWRL pravila

2.6.3 Mehanizem razumevanja (angl. Reasoning Mechanism)

2.7 Analiza vrzeli in prispevek te naloge

Poglavje 3

Implementacija sistema

3.1 Arhitektura sistema

Arhitektura sistema za upravljanje zaupanja v farmacevtski dobavni verigi je sestavljena iz več plasti. Te omogočajo kombinacijo semantičnih podatkov, subjektivne ocene zaupanja in decentraliziranega shranjevanja rezultatov v verigo blokov. Z delitvijo sistema na plasti omogočamo modularnost, večjo preglednost in lažjo implementacijo nadaljnjih razširitev.

Arhitekturo razdelimo na tri plasti, katere bodo podrobneje opisane v naslednjih podpoglavjih:

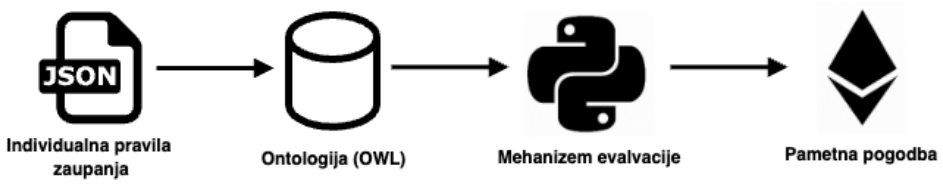
1. **Plast znanja**
   V tej plasti se nahajajo vse ontološke definicije, primerki akterjev in njihove lastnosti. Sem spada tudi konceptualna zasnova lastnosti zaupanja, kot so licence, temperaturne nepravilnosti, točnost dostave ipd.

2. **Mehanizem za sklepanje zaupanja**
   Ta plast vključuje sistem za izvajanje ocenjevanja zaupanja. Združuje podatke iz ontologije in pravil zaupanja ter izvede sklepanje za vsak par entitet. Rezultat je preslikava razmerja zaupanja med akterji, ki je pripravljena za zapis v verigo blokov.

3. **Graf zaupanja na verigi blokov**

Zadnja plast predstavlja pametno pogodbo, ki beleži razmerja zaupanja med entitetami. Shranjevanje rezultatov v verigo blokov omogoča transparentnost, trajnost in decentralizirano preverljivost zaupanja.

Na sliki 3.1 je prikazan arhitekturni pregled sistema.



Slika 3.1: Večplastna arhitektura sistema za upravljanje zaupanja

3.1.1 Plast znanja

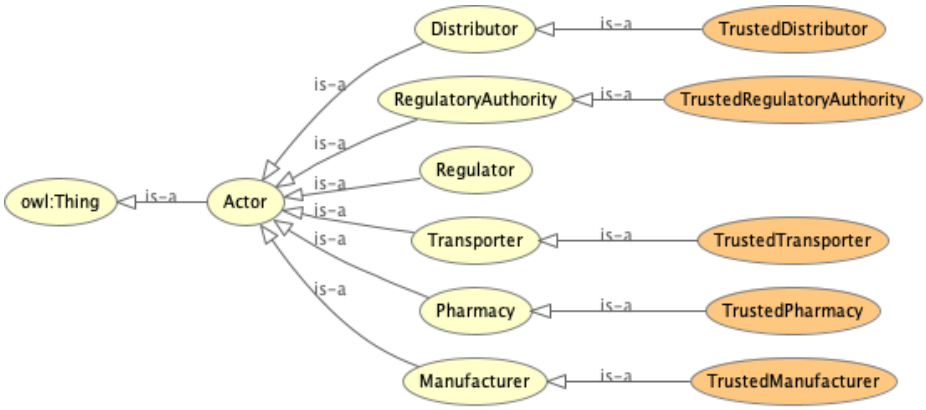
Plast znanja (angl. Knowledge Layer) definira semantično strukturo akterjev, njihove značilnosti in nabor pravil za individualno ocenjevanje zaupanja. V osnovi jo sestavljata dve ključni komponenti: ontologija in pravila zaupanja posameznih akterjev.

Ontologija Ontologija v jeziku OWL predstavlja formalno definiran model, ki vključuje vse vrste entitet, ki sodelujejo v farmacevtski dobavni verigi (npr. *Proizvajalec*, *Lekarna*, *Prevoznik*, *Regulator*). Vsaka vrsta entitete ima lahko specifične lastnosti, ki jih sistem uporablja pri sklepanju o zaupanju, kot so na primer:

- `hasDeliveryPunctuality` - točnost dostave,
- `hasTempViolationRate` - stopnja temperaturnih odstopanj,
- `hasLicense` - podatek o veljavni licenci,
- `hasGMP` - skladnost s proizvodnimi standardi GMP [24],
- `hasAuditScore` - rezultat presoje kakovosti.

Ontologija je zapisana v formatu RDF [25] zasnovan na označevalnem jeziku XML [26], ki omogoča enostavno obdelavo s knjižnico `rdflib` [27] v programskem jeziku Python. Na ta način lahko sklepanje temelji na aktualnih podatkih, zapisanih v ontološkem grafu, brez potrebe po relacijski bazi ali ročnem povezovanju.

Na sliki 3.2 vidimo vse akterje v ontologiji predstavljene v programu Protege.



Slika 3.2: Akterji ontologije v programu Protege

V ontologiji so definirani tudi posamezni primerki entitet (npr. *Pfizer*, *DHL*, *MediPlus*), skupaj z njihovimi lastnostmi. To omogoča sistemu, da na podlagi resničnih podatkov izvede evalvacijo zaupanja.

Pravila zaupanja posameznih akterjev Vsaka entiteta v sistemu lahko definira svoja lastna pravila zaupanja, ki opisujejo pogoje, pod katerimi določena entiteta zaupa drugi. Ta pravila so zapisana v berljivi in strukturirani obliki JSON, kar omogoča enostavno vključevanje v mehanizem sklepanja.

Primer politike pravil zaupanja za entiteto *Pfizer* je prikazan v spodnjem zapisu v formatu JSON:

```
{
  "actor": "http://example.org/trust#Pfizer",
  "trusts": {
    "Transporter": {
      "hasDeliveryPunctuality": { "gte": 0.9 },
      "hasTempViolationRate": { "lte": 0.05 }
    }
  }
}
```

Zapis pove, da entiteta *Pfizer* zaupa samo tistim prevoznikom, ki dosegajo vsaj 90 % pravočasnih dostav (`hasDeliveryPunctuality` $\geq$ `0.9`) in katerih delež temperaturnih odstopanj pri transportu zdravil ne presega 5 % (`hasTempViolationRate` $\leq$ `0.05`). Na ta način se pravila zaupanja natančno preslikajo v merljive pogoje, ki temeljijo na lastnostih, definiranih v ontologiji.

Mehanizem sklepanja nato uporabi ta pravila za vsako entiteto, s katero obravnavani akter vzpostavi zaupanje ter preveri, ali so pogoji izpolnjeni.

Ker so pravila zapisana v JSON obliki, je možno preprosto razviti uporabniški vmesnik, kjer lahko predstavnik podjetja (npr. administrator lekarne ali regulatorja) preko obrazca določil svoje kriterije za zaupanje. Vmesnik bi generiral JSON strukturo na podlagi definiranih lastnosti v ontologiji. To nam omogoča visoko stopnjo prilagodljivosti in enostavne uporabe brez tehničnega predznanja.

JSON pravila služijo kot most med semantičnim modelom in subjektivno presojo vsakega akterja. Tako omogočamo personalizirano ocenjevanje zaupanja.

3.1.2 Mehanizem za sklepanje zaupanja (angl. Trust Resolution Engine)

Mehanizem za sklepanje zaupanja predstavlja osrednjo logično plast sistema, kjer se združujejo podatki iz ontologije in pravila zaupanja posameznih akterjev. Tukaj se izvede proces ocenjevanja, ki določi, ali določena entiteta zaupa drugi glede na pogoje, zapisane v pravilih zaupanja posameznega akterja.

Delovanje mehanizma Python modul, razvit za potrebe sistema, izvaja naslednje korake:

1. Naloži ontologijo (OWL/RDF) in iz nje izlušči podatke o vseh akterjih ter njihovih lastnostih.

2. Prebere pravila zaupanja vsakega akterja, ki so zapisana v JSON formatu.

3. Za vsak par (ocenjevalec in tisti, ki je ocenjen) preveri, ali vrednosti atributov ocenjenega akterja ustrezajo pravilom ocenjevalca.

4. Rezultate ocenjevanja shrani v zbirko rezultatov (CSV datoteka) in jih pripravi za zapis v verigo blokov.

Primer ocenjevanja Če ima npr. akter *Pfizer* pravilo, da zaupa le prevoznikom z vsaj 90 % točnih dostav in manj kot 5 % temperaturnih nepravilnostih, bo mehanizem preveril te pogoje za vsakega prevoznika, zapisanega v ontologiji. Rezultat ocenjevanja je binarna vrednost (`true/false`), ki pove, ali akter izpolnjuje kriterije zaupanja.

3.1.3 Graf zaupanja na verigi blokov (angl. Blockchain Trust Registry)

Zadnja plast arhitekture je namenjena trajnemu in preverljivemu beleženju rezultatov ocenjevanja zaupanja. To dosežemo z uporabo pametne pogodbe na verigi blokov, ki deluje kot decentraliziran register zaupanja (angl. *trust registry*).

Struktura pametne pogodbe Pametna pogodba vsebuje podatkovno strukturo, ki beleži relacije zaupanja med akterji v obliki:

$$(akter1, akter2) \mapsto status\_zaupanja$$

kjer je `status_zaupanja` logična vrednost (`true/false`), ki označuje, ali akter 1 zaupa akterju 2.

Funkcionalnosti Pametna pogodba omogoča naslednje osnovne funkcije:

- `setTrustStatus()` — zapis oziroma posodobitev rezultata zaupanja na verigi blokov.

- `isTrusted()` — preverjanje, ali določen akter zaupa drugemu.
- `event TrustUpdated` — beleženje dogodkov o spremembi zaupanja za transparentnost in enostavno spremljanje.

3.2 Orodja in razvojno okolje

3.3 Ontologija in orodja za sklepanje

3.3.1 Ontologija zaupanja

Ontologija zaupanja je osnovni gradnik sistema, saj omogoča formaliziran opis vseh akterjev v farmacevtski dobavni verigi ter njihovih lastnosti. Zasnovana je v jeziku OWL. Glavni namen ontologije je, da lahko vse akterje opišemo na enoten način in jih obogatimo s podatki, ki so pomembni za ocenjevanje zaupanja.

Razredi akterjev

V ontologiji so definirani osnovni razredi, ki predstavljajo tipe akterjev. To so proizvajalec, distributer, lekarna, prevoznik in regulator. Vsi ti razredi so podrazredi splošnega razreda `Actor`, kar pomeni, da jih lahko obravnavamo skupaj, ko govorimo o celotni verigi. Vsak tip akterja ima svoje značilne lastnosti. Na primer, proizvajalci imajo lastnost `hasGMP`, ki pove, ali imajo veljavno GMP skladnost, prevozniki imajo lastnosti `hasDeliveryPunctuality` in `hasTempViolationRate`, lekarne pa lastnost `hasPrescriptionComplianceRate`.

Lastnosti zaupanja

Lastnosti opisujejo merljive kriterije, ki se uporabljajo pri presoji zaupanja. Nekaj primerov: `hasGMP` opisuje ali je proizvajalec skladen z dobrimi proizvodnimi praksami, `hasAuditScore` predstavlja oceno presoje kakovosti, `hasLicense` označuje, ali ima akter veljavno licenco, `hasDeliveryPunctuality`

izraža delež pravočasnih dostav, `hasTempViolationRate` pove, kolikšen delež transportov je imel temperaturna odstopanja, `hasPrescriptionComplianceRate` opisuje skladnost lekarne pri izdaji zdravil na recept, `hasIssuedCertifications` je število certifikatov, ki jih je regulator izdal, `hasJurisdictionLevel` pa določa raven pristojnosti regulatorja (npr. lokalna, nacionalna, globalna).

Razredi zaupanja

Za vsak tip akterja so v ontologiji definirani tudi posebni razredi, ki predstavljajo zaupanja vredne entitete. To so na primer `TrustedManufacturer`, `TrustedDistributor`, `TrustedPharmacy`, itn. Ti razredi so definirani z ekvivalenčnimi pogoji, kar pomeni, da reasoner lahko samodejno uvrsti entiteto v določen zaupanja vreden razred, če so pogoji izpolnjeni. Na primer, proizvajalec, ki ima GMP certifikat in dovolj visoko oceno presoje kakovosti, bo klasificiran kot `TrustedManufacturer`. Podobno velja za druge tipe akterjev.

Primerki akterjev

V ontologijo so dodani tudi konkretni primerki, ki predstavljajo dejanske akterje v sistemu. Tako imamo na primer proizvajalca Pfizer in Novartis, prevoznika DHL, lekarno MediPlus, distributerja EuroLogistics ter regulatorja EMA. Vsak od teh primerkov ima določene lastnosti, kot so na primer ocena presoje, točnost dostave ali število izdanih certifikatov. Te vrednosti se potem uporabijo pri sklepanju o zaupanju.

3.3.2 Primer toka podatkov in logike

Za ponazoritev delovanja si oglejmo primer, kjer proizvajalec Pfizer ocenjuje prevoznika DHL:

1. **Ontologija (OWL)**: v ontologiji so zabeležene lastnosti prevoznika DHL, npr. `hasDeliveryPunctuality = 0.95` in `hasTempViolationRate = 0.02`.

2. **Pravila zaupanja**: Pfizerjeva politika zaupanja za razred *Transporter* zahteva `hasDeliveryPunctuality` $\geq$ `0.90` in `hasTempViolationRate` $\leq$ `0.05`.

3. **Sklepanje (Python)**: mehanizem prebere lastnosti DHL iz ontologije in jih primerja s Pfizerjevimi pogoji. Ker sta oba pogoja izpolnjena, rezultat sklepanja je `true`.

4. **Zapis v verigo blokov**: rezultat (`Pfizer` zaupa `DHL`) se zapiše v pametno pogodbo. Funkcija `isTrusted(Pfizer, DHL)` nato vrne `true`.

Na ta način sistem poveže semantične podatke, subjektivna pravila in trajne zapise rezultatov v verigi blokov v enoten potek.

3.3.3 Način posodabljanja blockchain registra

Zapis rezultatov v pametno pogodbo se lahko sproži na tri načine:

- **Ročno**: prek CLI ali uporabniškega vmesnika, primerno za prezentacije in testne scenarije.
- **Dogodkovno**: ob spremembi entitete, pravil ali metrik v ontologiji (npr. nova licenca, posodobljen audit).
- **Periodično**: v rednih intervalih (npr. dnevno), pri čemer se zapis izvrši le ob spremembi rezultata glede na prejšnje stanje.

3.4 Razvoj pametnih pogodb in oraklov

3.5 Uporabniški vmesnik in API-ji

Poglavje 4

Evalvacija

4.1 Varnostna analiza

4.2 Zmogljivost in razširljivost

4.3 Natančnost ocene zaupanja

4.4 Prednosti in omejitve

4.5 Primerjava z obstoječimi rešitvami

4.6 Pridobljena spoznanja

Poglavje 5

Zaključek in nadaljnje delo

5.1 Povzetek prispevkov

5.2 Nadaljnje raziskave

Dodatek A

Shema ontologije in SWRL pravila

Dodatek B

Izvlečki kode pametnih pogodb

Literatura

[1] S. Holtmanns, Trust modeling and management: From social trust to digital trust, in: Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global, 2008. doi:10.4018/978-1-59904-804-8.ch013.

[2] T. Grandison, M. Sloman, A survey of trust in internet applications, IEEE Communications Surveys & Tutorials 3 (4) (2000) 2–16.

[3] S. D. Boon, J. G. Holmes, The dynamics of interpersonal trust: Resolving uncertainty in the face of risk, Cooperation and Prosocial Behavior (1991) 167–182.

[4] D. Gambetta, Trust: Making and breaking cooperative relations, Basil Blackwell, 1988.

[5] R. C. Mayer, J. H. Davis, F. D. Schoorman, An integrative model of organizational trust, Academy of Management Review 20 (3) (1995) 709–734.

[6] D. E. Denning, A new paradigm for trusted systems, Proceedings of the 1993 New Security Paradigms Workshop (1993) 36–41.

[7] D. H. McKnight, N. L. Chervany, Trust and distrust definitions: One bite at a time, Trust in Cyber-societies 2246 (2001) 27–54.

[8] S. Karthik, R. Shankar, N. Arunkumar, Ontology-based trust model for pervasive computing environments, Journal of Ambient Intel-

ligence and Humanized Computing 8 (2017) 557–568. doi:10.1007/s12652-016-0442-y.

[9] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, S. Ellahham, Blockchain for drug traceability: Architectures and open challenges, Health informatics journal 27 (2) (2021) 14604582211011228.

[10] H. Kayhan, Ensuring trust in pharmaceutical supply chains by data protection by design approach to blockchains, Blockchain in Healthcare Today 5 (2022) 10–30953.

[11] H. Li, M. Singhal, Trust management in distributed systems, Computer 40 (2) (2007) 45–53. doi:10.1109/MC.2007.76.

[12] R. Housley, W. Ford, W. Polk, D. Solo, Rfc2459: Internet x. 509 public key infrastructure certificate and crl profile (1999).

[13] M. Elkins, D. Del Torto, R. Levien, T. Roessler, Mime security with openpgp, Tech. rep. (2001).

[14] S. K. Panda, S. C. Satapathy, Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers, Personal and Ubiquitous Computing 28 (1) (2024) 75–91.

[15] W. H. Organization, et al., A study on the public health and socioeconomic impact of substandard and falsified medical products: executive summary (2017).

[16] Council of European Union, Directive 2011/62/eu of the european parliament and of the council of 8 june 2011 amending directive 2001/83/ec on the community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products text with eea relevance (2011).
URL https://eur-lex.europa.eu/eli/dir/2011/62/oj/eng

[17] Council of European Union, Commission delegated regulation (eu) 2016/161 of 2 october 2015 supplementing directive 2001/83/ec of the european parliament and of the council by laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use (text with eea relevance) (2015).
URL `https://eur-lex.europa.eu/eli/reg_del/2016/161/oj/eng`

[18] U.S. Food and Drug Administration, Drug supply chain security act (dscsa) (2017).
URL `https://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/ucm382022.htm`

[19] W. H. Organization, et al., WHO global surveillance and monitoring system for substandard and falsified medical products (2017).

[20] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Available at SSRN 3440802 (2008).

[21] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, et al., Blockchain technology: Beyond bitcoin, Applied innovation 2 (6-10) (2016) 71.

[22] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the thirteenth EuroSys conference, 2018, pp. 1–15.

[23] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper 151 (2014) (2014) 1–32.

[24] J. D. Nally, Good manufacturing practices for pharmaceuticals, CRC Press, 2016.

[25] R. Cyganiak, D. Wood, M. Lanthaler, Rdf 1.2 concepts and abstract syntax, World Wide Web Consortium (W3C) Recommendation (2024). URL https://www.w3.org/TR/rdf12-concepts/

[26] D. Beckett, B. McBride, Rdf/xml syntax specification (revised), World Wide Web Consortium (W3C) Recommendation (2004). URL https://www.w3.org/TR/rdf-syntax-grammar/

[27] C. Boettiger, rdflib: A high level wrapper around the redland package for common rdf applications (2018). doi:10.5281/zenodo.1098478. URL https://doi.org/10.5281/zenodo.1098478