03 UPORABNA INFORMATIKA

2022 ‹ ŠTEVILKA 3 ‹ LETNIK XXX ‹ ISSN 1318-1882

U P O R A B N A
I N F O R M A T I K A
2022 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XXX ISSN 1318-1882

Znanstveni prispevki

Kratki znanstveni prispevki

Strokovni prispevki

Prispevki iz konference Dnevi slovenske informatike

Informacije

U P O R A B N A
I N F O R M A T I K A

2022 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XXX ISSN 1318-1882

Ustanovitelj in izdajatelj
Slovensko društvo INFORMATIKA
Litostrojska cesta 54, 1000 Ljubljana

Predstavnik
Niko Schlamberger

Odgovorni urednik
Mirjana Kljajić Borštnar

Tehnični urednik
Slavko Žitnik

Lektoriranje angleških izvlečkov
Marvelingua (angl.)

Oblikovanje
KOFEIN DIZAJN, d. o. o.

Prelom in tisk
Boex DTP, d. o. o., Ljubljana

Naklada
110 izvodov

Naslov uredništva
Slovensko društvo INFORMATIKA
Uredništvo revije Uporabna informatika
Litostrojska cesta 54, 1000 Ljubljana
www.uporabna-informatika.si

Revija izhaja četrtletno. Cena posamezne številke je 20,00 EUR. Letna naročnina za podjetja 85,00 EUR, za vsak nadaljnji izvod 60,00 EUR, za posameznike 35,00 EUR, za študente in seniorje 15,00 EUR. V ceno je vključen DDV.

Revija Uporabna informatika je od številke 4/VII vključena v mednarodno bazo INSPEC.

Revija Uporabna informatika je pod zaporedno številko 666 vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo RS.

Revija Uporabna informatika je vključena v Digitalno knjižnico Slovenije (dLib.si).

Vabilo avtorjem

V reviji Uporabna informatika objavljamo kakovostne izvirne prispevke domačih in tujih avtorjev z najširšega področja informatike, ki se nanašajo tako na poslovanju podjetij, javno upravo, družbo in posameznika. Prispevki so lahko znanstvene, strokovne ali informativne narave, še posebno spodbujamo objavo interdisciplinarnih prispevkov. Zato vabimo avtorje, da prispevke, ki ustrezajo omenjenim usmeritvam, pošljejo uredništvu revije po elektronski pošti na naslov ui@drustvo-informatika.si.

Avtorje prosimo, da pri pripravi prispevka upoštevajo navodila, ki so objavljena na naslovu http://www.uporabna-informatika.si.

Za kakovost prispevkov skrbi mednarodni uredniški odbor. Prispevki so anonimno recenzirani, o objavi pa na podlagi recenzij samostojno odloča uredniški odbor. Recenzenti lahko zahtevajo, da avtorji besedilo spremenijo v skladu s priporočili in da popravljeni prispevek ponovno prejmejo v pregled. Sprejeti prispevki so pred izidom revije objavljeni na spletni strani revije (predobjava), še prej pa končno verzijo prispevka avtorji dobijo v pregled in potrditev. Uredništvo lahko še pred recenzijo zavrne objavo prispevka, če njegova vsebina ne ustreza vsebinski usmeritvi revije ali če prispevek ne ustreza kriterijem za objavo v reviji.

Pred objavo prispevka mora avtor podpisati izjavo o avtorstvu, s katero potrjuje originalnost prispevka in dovoljuje prenos materialnih avtorskih pravic. Avtorji prejmejo enoletno naročnino na revijo Uporabna informatika, ki vključuje avtorski izvod revije in še nadaljnje tri zaporedne številke. S svojim prispevkom v reviji Uporabna informatika boste pomagali k širjenju znanja na področju informatike. Želimo si čim več prispevkov z raznoliko in zanimivo tematiko in se jih že vnaprej veselimo

Uredništvo revije

Navodila avtorjem člankov

Članke objavljamo praviloma v slovenščini, članke tujih avtorjev pa v angleščini. Besedilo naj bo jezikovno skrbno pripravljeno. Priporočamo zmernost pri uporabi tujk in, kjer je mogoče, njihovo zamenjavo s slovenskimi izrazi. V pomoč pri iskanju slovenskih ustreznic priporočamo uporabo spletnega terminološkega slovarja Slovenskega društva Informatika, Islovar (www.islovar.org).

Znanstveni prispevek naj obsega največ 40.000 znakov, kratki znanstveni prispevek do 10.000 znakov, strokovni članki do 30.000 znakov, obvestila in poročila pa do 8.000 znakov.

Prispevek naj bo predložen v urejevalniku besedil Word (*.doc ali *.docx) v enojnem razmaku, brez posebnih znakov ali poudarjenih črk. Za ločilom na koncu stavka napravite samo en presledek, pri odstavkih ne uporabljajte zamika.

Naslovu prispevka naj sledi polno ime vsakega avtorja, ustanova, v kateri je zaposlen, naslov in elektronski naslov. Sledi naj povzetek v slovenščini v obsegu 8 do 10 vrstic in seznam od 5 do 8 ključnih besed, ki najbolje opredeljujejo vsebinski okvir prispevka. Sledi naj prevod naslova povzetka in ključnih besed v angleškem jeziku. V primeru, da oddajate prispevek v angleškem jeziku, velja obratno. Razdelki naj bodo naslovljeni in oštevilčeni z arabskimi številkami.

Slike in tabele vključite v besedilo. Opremite jih z naslovom in oštevilčite z arabskimi številkami. Na vsako sliko in tabelo se morate v besedilu prispevka sklicevati in jo pojasniti. Če v prispevku uporabljate slike ali tabele drugih avtorjev, navedite vir pod sliko oz. tabelo. Revijo tiskamo v črno-beli tehniki, zato barvne slike ali fotografije kot original niso primerne. Slikam zaslonov se v prispevku izogibajte, razen če so nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Enačbe oštevilčite v oklepajih desno od enačbe.

V besedilu se sklicujte na navedeno literaturo skladno s pravili sistema IEEE navajanja bibliografskih referenc, v besedilu to pomeni zaporedna številka navajenega vira v oglatem oklepaju (npr. [1]). Na koncu prispevka navedite samo v prispevku uporabljeno literaturo in vire v enotnem seznamu, urejeno po zaporedni številki vira, prav tako v skladu s pravili IEEE. Več o sistemu IEEE, katerega uporabo omogoča tudi urejevalnik besedil Word 2007, najdete na strani https://owl.purdue.edu/owl/research_and_citation/ieee_style/ieee_general_format.html.

Prispevku dodajte kratek življenjepis vsakega avtorja v obsegu do 8 vrstic, v katerem poudarite predvsem strokovne dosežke.

Simulacija in izboljšava prometnih tokov: primer na dveh izbranih slovenskih križiščih

Sandi Gec, Vlado Stankovski, Marko Bajec, Slavko Žitnik
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana
sandi.gec@fri.uni-lj.si, vlado.stankovski@fri.uni-lj.si, marko.bajec@fri.uni-lj.si, slavko.zitnik@fri.uni-lj.si

Izvleček

Prometna omrežja zaradi povezanosti trgov, potrošništva, potovanj, … postajajo vse bolj zasičena. Izgradnja dodatnih povezav ni vedno možna, poleg tega pa je potrebno izvesti vse možne optimizacije za večjo pretočnost prometa. Eden od pristopov zahteva vpeljavo semaforizirane logike, ki skrbi za vzpostavitev prednostne logike na posameznih križiščih oz. vozliščih. Obstoječo deterministično logiko je potrebno posodobiti s prilagodljivimi sistemi. V delu se osredotočamo na študijo primerjave semaforskih logik in sicer fiksnega programa ter naprednejšega stohastičnega polno prometno odvisnega programa ter adaptivnega programa. Analiza uspešnosti algoritmov poteka na slovenskih križiščih Šoštanj predstavljen z enim semaforiziranim križiščem in Podutik Ljubljana, ki sestoji iz štirih zaporednih semaforiziranih križišč. Ugotovitve nakazujejo, da vpeljava adaptivne logike omogoča boljšo pretočnost prometa ter posledično zmanjšuje onesnaževanje.

Ključne besede: simulacija prometa, fiksni program, polno prometno odvisni program, adaptivni program, semaforizirano križišče, semaforske faze.

Simulation and improvement of traffic flows: A use case study on two selected Slovenian crossroads

Abstract

Transportation networks are becoming increasingly congested due to markets interconnection, consumers' needs, travelling etc. Implementation of additional links is not always possible, and therefore all possible optimisations need to be taken into account to enable more fluid traffic flows. One of the options is introduce traffic light logic that takes care of prioritization at individual intersections or nodes. It is necessary to ensure flowing traffic by upgrading the existing deterministic logic of fixed networks. The paper focuses on the analysis and the comparison of traffic lights logic programmes, specifically the fixed programme, the more advanced stochastic fully traffic-dependent programme and the adaptive programme. The analysis takes place at the Slovenian intersections Šoštanj, with one traffic lights intersection, and Podutik Ljubljana, which consists of four consecutive traffic lights intersections. The findings suggest that the introduction of adaptive logic enables improved traffic flow and consequently reduces pollution.

Keywords: Traffic simulation, fixed programme, full traffic dependent programme, adaptive programme, traffic light intersection, traffic light phases

1 UVOD

Slovenija je iz urbanističnega vidika ena redkih držav, kjer večji del prebivalstva živi v manjših mestih in vaseh, pri čemer imamo le peščico večjih mest. Pretežni del prebivalstva si za zagotovitev hitrega prehoda najpogosteje izbere lasten avtomobilski prevoz. Posledica takšnega trenda je število registriranih vozil, kar se odraža v večji prometni obremenitvi ter onesnaževanju[1], zastojih, zmanjšani pretočnosti vozil, zamudah javnega cestnega prometa ter tovornega prometa in druge cestne dogodke. V našem delu se osredotočamo na optimizacijo semaforske logike,

[1] http://kazalci.arso.gov.si/sl/content/lastnistvo-osebnih-avtomobilov-2 (Dostopano dne: 18. julij 2022).

s katero želimo doseči večjo pretočnost prometa ter posledično nižjo onesnaževanje okolja. Za namene povečanja pretočnosti vozil je smotrna vpeljava rešitev pametnega prometa, predvsem na nivoju semaforske logike. Ker je neposredna vpeljava rešitev na infrastrukturi tvegana in cenovno draga, je smiselno proučiti rezultate posodobitve prometnih tokov semaforskih križišč na podlagi realnih podatkov. V te namene je bila izvedena študija, ki se osredotoča na analitiko prometnih tokov na dveh različnih scenarijih, in sicer samostojno semaforizirano križišče ter nabor medsebojno odvisnih križišč. Analitika poleg numeričnih rezultatov omogoča tudi prilagajanje parametrov posameznega scenarija ter vizualizacijo prometnega poteka.

V tem prispevku obravnavamo prometna omrežja, ki so predstavljena s tremi osnovnimi elementi, in sicer: (a) cestišča, (b) semaforizirana križišča in (c) vozila. V prometna omrežja se dodajajo vozila, ki vozijo po vnaprej določeni poti na eno, dvo ali večpasovnih cestiščih, pri čemer je najbolj obremenjen del križišč semaforiziran. Cilj našega dela je definicija adaptivne logike semaforiziranih križišč z namenom izboljšanja pretočnosti v primerjavi s **fiksno semaforsko logiko**.

Vodenje prometa v samostojnih izoliranih križiščih je potrebno analizirati ločeno od tistih za mrežno oz. arterijsko vodenje prometa, v conah in s sekvenco semaforiziranih križišč. Slednje se v osnovi nanaša na prometna omrežja z dvema ali več semaforiziranih križišč na isti cesti, kjer je potrebno upoštevati soodvisno semaforsko logiko. Na izoliranih križiščih je bistveno več prostora za prilagajanje dolžine trajanj posameznih prikaznih luči (t.i. »splitov«), zamenjave vrstnega reda ter preskakovanja celotne sekvence faz, ker na teh križiščih ni potrebno upoštevati koordinacije, kot je to nujno v conah. V našem delu obravnavamo obe vrsti omrežij - samostojno izolirano omrežje v Šoštanju in več soodvisnih semaforiziranih križišč na prometnem omrežju Ljubljana-Podutik.

Delo se osredotoča na optimizacijo prometnih tokov z vidika definicije logike oziroma algoritmov semaforiziranih križišč. Vmesni algoritmi med fiksnimi in adaptivnimi so polno prometno odvisni. Ti so nadgradnje fiksnih algoritmov z vnaprej določenimi dolžinami posameznih faz, splitov in ciklov, kjer ima vsak split minimalno in maksimalno dolžino trajanja, ta pa je odvisen od količine prometa beleženega na podlagi induktivnih zank ali detektorjev, postavljenih na vseh vhodnih poteh pred semaforjem. Najbolj napredni **adaptivni algoritmi** za kontrolo semaforjev ne potrebujejo vnaprejšnje definicije fiksnih prometnih programov, saj se dolžina cikla, »spliti« in zaporedje faz dinamično izračuna, in sicer z namenom, da se v križiščih poveča pretočnost prometa. Podatke za izračune podobno kot pri polno prometno odvisnih algoritmih pridobivamo iz detektorjev. V nadaljevanju so predstavljeni algoritmi in študije, ki nakazujejo, da se adaptivna kontrola obnese boljše od polno prometno odvisne.

V nadaljevanju najprej analiziramo sorodna dela. V poglavju kasneje opredelimo algoritme, ki se v našem delu uporabljajo ter orišemo našo rešitev, vključno z arhitekturo. Evalvacija ter rezultati simulacije z diskusijo so predstavljeni v četrtem poglavju. V zaključnem poglavju podamo sklepne ugotovitve in nadaljne možnosti za razvoj.

2 SORODNO DELO

Težnja k optimizaciji prometnih tokov sega v čase druge polovice prejšnjega stoletja, ko so se začela množično graditi prometna omrežja in povečano proizvodnjo vozil. V nadaljevanju se osredotočamo na sorodna dela in sicer:

- Pregled trendov raziskav mehke logike prometnih tokov skozi čas, ki razvoj pogojuje tudi z razvojem senzorske in druge tehnološke opreme,
- razvoja algoritmov adaptivne logike ter način delovanja in
- analizo računalniških orodij za simulacijo prometnih tokov vključno z izdelavo prometnega toka, definicije semaforske logike in simulacijskih entitet (npr. vozila, pešci itd.).

2.1 Pregled raziskav mehke logike prometnih tokov

Prvi znani poskus uporabe mehke logike pri upravljanju prometne signalizacije sta leta 1977 izvedla Pappis in Madani. Predlagala sta teoretično simulacijsko študijo mehkega upravljalnika v izoliranem semaforiziranem križišču dveh enosmernih cest z dvema voziščema in enakim prometnim pretokom (Pappis in Madani, 1997). Njuno delo se uvršča v povoje aplikativne predstavitve mehke logike. Avtorja sta primerjala svojo mehko metodo s prilagodljivim sistemom upravljanja signalizacije, ki minimizira zamude z optimalno dolžino cikla. Mehka logika je bila

vsaj tako dobra kot primerjalni prilagodljiv sistem.

V devetdesetih letih prejšnjega stoletja so se začele vrstiti raziskave in študije uporabe mehke logike pri upravljanju prometne signalizacije. Sodobne mehke sisteme v prometnem inženirstvu je predstavil Teodorovic, ki se med drugim osredotoča tudi na prilagodljivo upravljanje prometne signalizacije (Teodorovic, 1999). Preučevanje mehke logike so predstavili avtorji, ki so preučevali mehke algoritme v izoliranih križiščih (Kim, 1997). Avtorji so dolžino zelenega signala prilagodili razmeram prometa ob koncu vsake faze. Favilla in sod. so leta 1993 predstavili dve različni metodi ostrenja in kriterije pri sprejemanju odločitev (Favilla in sod., 1993). Trabia in sod. so leta 1999 predstavili mehki sistem upravljanja prometne signalizacije za izolirano križišče, ki je temeljil na dvonivojski proceduri, ki je odločala o podaljšanju ali prekinitvi faze (Trabia in sod., 1999). V prvi fazi je sistem ocenil intenzivnost prometa, nato pa rezultat upošteval v drugi fazi, kjer se odloča o prekinitvi ali podaljšku. Sistem je vračal boljše rezultate, predvsem za manjše zakasnitve vozil in enak delež ustavljanja kot v primeru metode na zaznavo vozil. Sayers in sod. so se ukvarjali z mehkim upravljanjem prometne signalizacije z vidika več ciljev in tudi z ozirom na to, kje naj bi se upravljalni sistem uporabljal (Sayers in sod., 1998). Uporabili so genetski algoritem (MOGA) kot optimizacijsko tehnologijo. Wei in sod. so predstavili pristop za zmanjševanje zamud in kontrolo faz - koncept »glavna nujna faza« in »manjša nujna faza« skupaj z vsemi pravili mehke logike (Wei in sod., 2001). Pristop algoritma mehke logike z agenti, ki imajo sposobnost odločanja, je leta 2003 predstavil Kosonen (Kosonen, 2003). Avtorja Akiyama in Okushima sta leta 2006 predlagala pristop kako v algoritmu spreminjata tok prihodov vozil s spremenljivkami za optimizacijo lingvističnih spremenljivk v definiciji modela mehke logike (Akiyama in Okushima, 2006). Avtorja sta pripravila napredni adaptivni algoritem, ki je dodatna funkcionalnost prometnemu informacijskemu sistemu za prometne tokove na hitrih vpadnicah na Japonskem. Drugačen pristop, in sicer z uporabo Mamdani metode za optimizacijo in skrajševanjem povprečnih časov ter zmanjševanje dolžine kolon so pripravili Hu in sod., kjer so leta 2007 definirali algoritem z mehko logiko za določanje dolžine zelenega časa. Evalvacijo so izvedli za 5-krako križišče s 14 pasovi, ki vključujejo 6 zavijalnih pasov in dva prehoda za pešce (Hu in sod., 2007). Algoritem uporablja prometne podatke iz detektorjev v križišču. Avtorja Zhang in Ye sta predstavita metodologijo za napoved prometnih tokov v križišču z uporabo dvojnega detektorja (Zhang in Ye, 2008). Metoda se je izkazala za bolj natančno in robustno, saj so bile napovedi natančne za različne prometne tokove.

2.2 Algoritmi semaforske logike prometnih tokov

Adaptivna kontrola temelji na analizi napovedi prihajajočega prometnega toka, za kar obstajata dve vrsti napovedi. Prva napoved meri podatke v realnem času na detektorjih, druga pa iz historičnih podatkov napove gibanje prometnega toka. Z analizo podatkov v realnem času lahko nastavljamo cikel med odvijanjem in se sproti odločamo o podaljševanju ali zaključevanju posamezne faze. Z optimizacijo na nivoju cikla med samim izvajanjem se zelo dobro prilagajamo hipnim nihanjem v prometu. Za optimizacije, ki potekajo vsakih 30 do 60 sekund, se lahko uporablja podatke v realnem času.

COP algoritem (Sen in Head, 1997) iz sistema RHODES (Mirchandani in Fei-Yue Wang, 2005) optimizira vrstni red in trajanje faz vsakih 30 do 40 sekund, in sicer odvisno od lokacije detektorjev. RHODES razdeli potovanje od oddaljenega detektorja do črte stop na dva dela, in sicer od oddaljenega detektorja do bližnjega ter od bližnjega detektorja do stop črte. Bližnji detektorji so definirani precej daleč, in sicer okvirno 100 m od stop črte, da ima krmilnik dovolj časa da se odzove na podatke iz detektorjev. Ker je detektor precej oddaljen, se ocenjuje trajanje poti in hitrosti od tega detektorja do črte stop, saj pri gostem prometnem toku prihaja do nabiranja kolon.

OPAC strategija (Gartner, 1990) temelji na obdelavi podatkov zadnjih 50 do 100 sekund. Prihodi vozil se merijo na oddaljenih detektorjih. Algoritem mora izračunati predviden čas potovanja od oddaljenega detektorja do stop črte. Na podoben način tudi OPAC definira potovalne čase potovanj od bolj k manj oddaljenim detektorjem, tako da tudi pri tej metodologij ostajajo problemi z nastajanjem kolon in oceno njihove dolžine.

PODE (Passive Opposition Differential Evolution) (Cheng, 2017) je strategija s hibridno funkcijo, t.j. funkcija definirana z večimi podfunkcijami, ki optimira dolžine signalov v kratkih časovnih intervalih. Kot ostali algoritmi, tudi PODE za vhodne podatke jemlje število prihodov vozil in kolone na črti stop. Poseb-

nost sistema je, da ima funkcionalnost spremenljivega intervala optimizacije in samoprilagodljivega mehanizma. Optimizacija lahko poteka le na nekaj sekund lahko pa poteka le vsake pol minute. Če je potrebno, se na začetku vsakega intervala popravi napaka ocene trajanja faz v trenutnem ciklu. Vse mogoče kombinacije dolžine in vrstnega reda faz se analizirajo za vsak interval, t.j. če imamo 8 faz in dolžino intervala 15 sekund, pomeni to 120 različnih kombinacij za analizo. Po primerjavi vseh 120 izračunov indeksov za vse kombinacije se izbere najboljša. Cilj algoritma je minimizacija zamud vozil za celotno križišče.

ACS-LITE (Zhanbo in sod. 2018) je reaktivni adaptivni sistem (sistem na osnovi povratne informacije zanke pri procesiranju podatkov) za nadzorovanje prometa. Za spremembo »splitov« uporablja podatek o zasedenosti detektorjev na stop črti. Zasedenost detektorjev se primerja z dolžino pripadajoče zelene faze, da se analizira koliko zelene faze je bilo porabljeno, oziroma za koliko časa bi se lahko skrajšala. Analiza računa povprečje v 3 do 5 ciklih. Po dobljenem rezultatu se »spliti« spremenijo. Cilj algoritma je doseči enakomerno stopnjo nasičenosti priključkov v križišču. Spreminjanje »splitov« se v ACS-LITE izvaja lokalno na vsakem krmilniku posebej in neodvisno. Vsaka optimizacija »splita« se najprej vrši po 3 končanih ciklih in 5 minutah. »Split« in zamik se spreminja v majhnih korakih, t.j. v časovnih intervalih 2 do 5 sekund. Zaključevanje faz pred maksimalno zeleno in preskakovanje faz deluje normalno v opisanem algoritmu.

Če povzamemo, potrebujemo za dobro adaptivno kontrolo na izoliranih križiščih naslednje:

- Podatke za optimizacijo, ki se pridobivajo v realnem času na podlagi podatkov s postavljenih detektorjev. Uporaba historičnih podatkov ni zaželena.
- Model napovedi prihoda na črto stop, ki mora biti zanesljiv za redek, gost in nasičen prometni tok ter mora pokrivati tudi pojavljanje zastojev.
- Adaptivni sistem, ki mora vsebovati samo prilagodljivi mehanizem za spremljanje podatkov in prilagajanje dejanskemu stanju.
- V našem delu primerjamo tri krovne pristope algoritmov in njihovo empirično delovanje na dveh različnih prometnih omrežjih z različnimi metrikami.

2.3 Orodja za simulacijo

Pri pripravi simulacije prometnih tokov smo se osredotočili na pregled odprtokodnih rešitev, ki omogočajo učinkovito simulacijo. Kot najbolj ustrezna kandidata smo identificirali orodji SUMO in Aimsun, ki sta dve izmed pogramskih orodij za izdelavo simulacij prometa. V Tabeli 1 prikazujemo njuno primerjavo.

3 SISTEM SIMULACIJE PROMETNIH TOKOV

V tem poglavju povzamemo algoritme aplicirane na izbranih prometnih omrežjih. Čeprav se širom sveta še vedno uporabljajo standardni fiksni programi, se zaradi preobremenjenosti omrežij pojavljajo potrebe po novih adaptivnih pristopih, ki merijo vozila neposredno pred semaforiziranimi križišči ali globalen pristop meritve na večjem območju prometnega omrežja in primerno ukrepanje. V našem primeru se osredotočamo na lokalni pristop, saj so omrežja dovolj zgoščena ter se njihova komunikacija podatkov razprostira do največ štirih semaforiziranih križišč.

V nadaljevanju so povzeti trije algoritmi za katere imamo razpoložljive vhodne podatke semaforske logike ter na voljo podrobne opise prihodov vozil glede na čas v omrežje.

3.1 Algoritmi

V tem razdelku so navedene le ključne lastnosti treh glavnih algoritmov. Podrobnosti algoritmov so poslovna skrivnost industrijskega partnerja projekta.

3.1.1 Fiksni program

Fiksni program lahko opredelimo kot časovno togo krmiljenje semaforjev. »Spliti« oz. podaljševanja zelenih faz so v vseh ciklih enaki, ne glede na nihanja v prometu. Cikel, zamik in split so definirani na podlagi historičnih podatkov in praviloma opredeljujejo obdobja kot so jutranji in popoldanski časi prometnih konic, nočni, vikend in ostale režimi. Z urnikom je definirana izbira prometnega programa glede na čas v dnevu oz. tednu. Takšno krmiljenje je primerno za cone, kjer so prometne obremenitve zelo predvidljive in so odstopanja majhna. Detekcija pri takšnem vodenju ni potrebna, zato se podatki na indukcijskih zankah ne uporabljajo.

Tabela 1: **Analiza funkcionalnosti med orodji SUMO in Aimsun**
Glede na preprostotst uvoza omrežij in naborom funkcionalnosti, širokim naborom metrik in možnostjo brezplačne odprtokodne uporabe, smo se odločili za orodje SUMO.

Funkcionalnost	Orodja	
	SUMO[1]	Aimsun[2]
Uvoz omrežij	NETCOVERT (skripta za uvoz in avtomatsko prilagoditev cestnih omrežij v okolje SUMO) in druga neuradna orodja.	Neposredno z aplikacijo, omogoča naprednejše možnosti in podpira integracijo z OpenStreetMap[4].
Modeliranje povpraševanja	Matrično, povpraševanje glede na aktivnosti (angl., Activity based demand) kot so dnevne poti na delo, v mesto, šole ter dogodki, naključne poti, računanje poti na podlagi uteži v omrežju. Različne funkcije za računanje uteži. Podpira razrede in tipe vozil.	Podobno kot SUMO, z nekaterimi dodatnimi funkcijami za računanje uteži povezav. Lažje generiranje prometa z isto aplikacijo.
Nadzor semaforske logike	Podpira običajno nastavljanje semaforjev. Vpliv detektorjev na semaforje in tudi programsko vodene semaforje (angl., actuated traffic lights).	Enako kot SUMO. Sistem se upravlja preko grafičnega uporabniškega vmesnika. Podpira tudi grupiranje vozlišč s semaforji, torej nastavljanje pravil za več vozlišč naenkrat. Podpira kontrolerje, ki nadzorujejo dinamiko v enem križišču (detektorji na cestah, pešci, programi za nadzor semaforjev)
Javni prevoz	Javni promet so vozila s primernim razredom. Za ustvarjanje linij je potrebno specificirati poti. Ni urnikov, oz. jih je potrebno drugače implementirati.	Zelo natančno ustvarjanje in urejanje javnega prevoza, z linijami in urniki.
Izjemni dogodki	SUMO nima posebne sekcije, ki bi se ukvarjala dogodki. Vse kar ima Aimsun, bi se dalo sicer implementirati.	Ima možnost nastavljanja množic pravil, ki določajo način kako naj se spremeni dinamika v omrežju (podprte so že nesreče, zaprtje pasov, sprememba namembnosti pasov, prisilno obračanje).
Upravljanje modelov omrežja	SUMO nima posebnih orodij za to.	Aimsun ima različne urejevalnike omrežja, prometa, javnega prometa. Pravzaprav gre za nastavljanje parametrov omrežja in prometa, da kasneje lepše delujejo kot celota. Omogoča izvajanje poskusov in ustvarjanje scenarijev.
Izbira poti	SUMO ima kar nekaj algoritmov za izbiro optimalne poti na podlagi uteži v omrežju. To je izvedeno z dodatnimi orodjem DUAROUTER (skripta za nastavljanje zahtev in omejitev pri usmerjanju prometa).	Aimsun ima vsaj na prvi pogled izredno obširno podprto usmerjanje. Vsebuje ogromno funkcij. V dokumentaciji je to zbrano pod t.i. razdelkom Dynamic Traffic Assignment.
Obnašanje voznikov	/	Ponuja precej modelov za simulacijo obnašanja voznikov na cesti, kot je npr. varnostna razdalja, spreminjanje voznih pasov, prilagajanje hitrosti glede na ostale voznike in druge.
Analiza podatkov in vizualizacija	Vsebuje orodja za vizualizacijo podatkov, ki so razširitve Python knjižnice Matplotlib. Množica podatkov, ki jih lahko pridobimo iz simulacije in statistika, je kar obsežna.	Zelo močno podprta vizualizacija in pridobitev in analiza podatkov. Sicer je precej podobno kot pri orodju SUMO.
Storitve	Del funkcionalnosti dostopen preko knjižnice Traffic Control Interface (TRACI), ki omogoča neposredno programsko upravljanje s simulacijo.	Vse funkcionalnosti dostopne preko storitve.

3.1.2 Polno prometno odvisni program

Značilnost tega prometnega programa je ta, da se krmiljenje izvaja na podlagi dodatne senzorike, ki je integrirano v prometno omrežje. Detektorji oz. induktivne zanke so nameščeni na vseh smereh za vse faze. Prav tako je obvezna najava pešcev v primerih, ko s tem podatkom razpolagamo. »Spliti« na nekoordiniranih fazah se izvedejo tako, da se preveri pretočnost križišča v zadnjih treh fazah ter izračuna dve možnosti:

- podaljševanje zelene faze ali
- skrajševanje zelene faze.

[2] https://www.eclipse.org/sumo/ (Dostopano dne: 18. julij 2022).
[3] https://www.aimsun.com (Dostopano dne: 18. julij 2022).
[4] https://www.openstreetmap.org (Dostopano dne: 18. julij 2022).

Z detekcijo na koordinirani fazi lahko pri manjših obremenitvah definiramo čas od dejanskega konca zelene faze do predefiniranega maksimalnega splita drugim fazam. Prometne programe umestimo v čas izvajanja z urnikom, podobno kot v sorodnih pristopih (Gartner, 1990).

Pri polno prometno odvisnih programih kjer imamo na voljo več semaforiziranih križišč, lahko opredelimo tudi njihove prioritete. Na primeru prometnega omrežja Podutik imamo na voljo 4 križišča, pri katerih je najbolj obremenjeno križišče Š-32 (prikazano na Sliki 8), saj se čez to križišče zapelje največ vozil in je posledičnost obremenjenost najvišja. Na podlagi primarnega križišča, ki ga tudi imenujemo dominantno, se »spliti« zelenih faz ostalih sekundarnih križišč lahko računajo na dva načina: (a) glede na dominantno križišče ali (b) neodvisno od dominantnega križišča. V našem primeru računamo »splite« vseh križišč neodvisno od dominantnega križišča.

3.1.3 Adaptivni program

Glavna naloga adaptivnih sistemov in algoritmov za krmiljenje prometa je z dobro analizo in interpretacijo vhodnih - detektorskih podatkov ponuditi primerno izbiro, prilagoditev obstoječega, oz. definicijo novega prometnega programa za zagotavljanje čim manjših zamud in čimvečje pretočnosti v križiščih. Za to je nujno potrebno vzpostaviti kompleksen sistem detektorjev, zmogljiv krmilnik za obdelavo in arhiviranje realnočasovnih podatkov podobno kot pri algoritmih adaptivne logike sorodnega dela ACS-LITE (Zhanbo in sod. 2018). Med križišči v koordinaciji mora obstajati zanesljiva dovolj zmogljiva povezava za prenos podatkov in sinhronizacijo med križišči. Večina adaptivnih sistemov uporablja modele za generiranje prometa v simulatorju, za distribucijo prihodov vozil, prihodov vozil v kolonah, oceno zamud in stoječih kolon. Spreminjanje cikla, splita in zamika je rezultat analiz, ki lahko služijo pri minimiziranju zamud, stopnje ustavitev vozil ter maksimizaciji zelenega vala pri križiščih v koordinaciji.

Efektivnost adaptivne strategije je odvisna tudi od parametrov, ki določajo dolžino kolone, zamude pri speljevanju in praznjenje vozil iz križišča. Zadnja parametra sta lahko odvisna od časa v dnevu, geometrije križišča, vzdolžnih naklonov, vremena in drugih dejavnikov. Večina obstoječih adaptivnih sistemov ne vsebuje samo prilagodljivih mehanizmov, ker so zgornji parametri modelirani kot statične spremenljivke.

Adaptivno krmiljenje prometa, ko na potek signalnega programa vplivajo vsi v križišče usmerjeno tokovi s sosednjih križišč, krmilimo preko nadzornega sistema, na način, da se poleg prometa na zeleni smeri hkratno analizira tudi promet na rdeči smeri. Tako se lahko »split« optimizira in prilagaja na osnovi podatkov v realnem času. Primer definicije adaptivne semaforske logike prometnega omrežja Podutik je prikazan na Sliki 1, kjer signalne glave opredeljujejo vse razpoložljive signalizacije udeležencev v prometu (vozila, pešci, kolesarji, semaforji za zavijanja in drugo). Za vsako signalno glavo je opredeljen fiksni ali prilagodljiv čas v sekundah posameznih faz semaforja, ki so navedeni v legendi na dnu slike.

Glavne funkcionalnosti na nivoju mikrokontrole pri fazni organizaciji so:

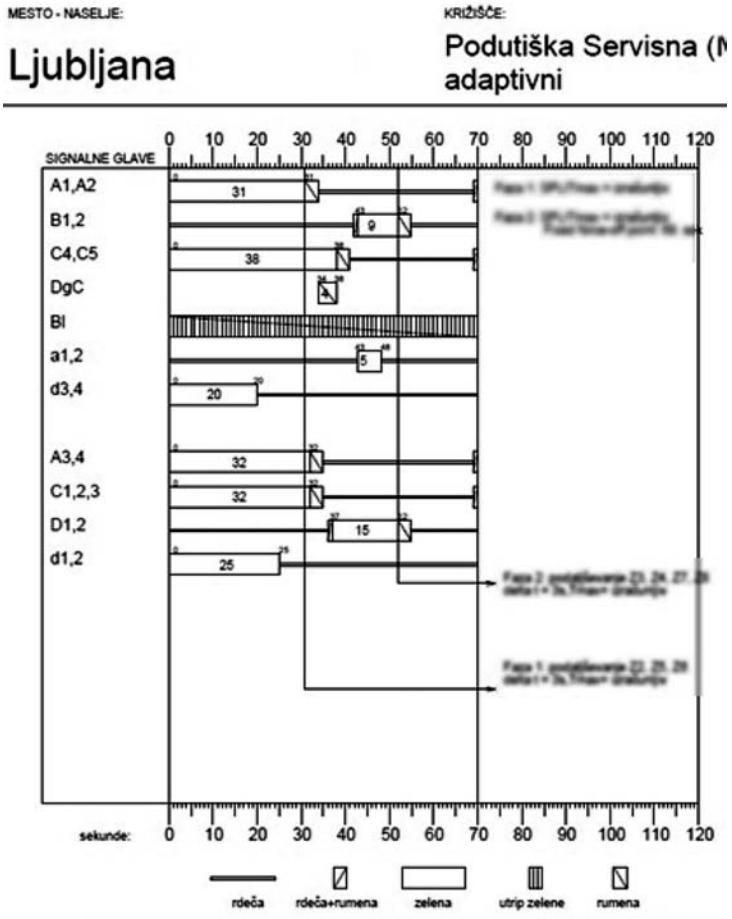
- minimalna zelena (angl., phase minimum green),
- zadrževanje faze (angl., phase rest), ki ga potrebujemo za mirovna stanja,
- podaljševanje faze (angl., phase extension), potrebujemo za podaljševanje minimalne začetne zelene,
- skrajševanje faze (angl., phase (early) cut-off), potrebujemo pri signalnih grupah z daljšimi vmesnimi časi (npr., pešci), vpeljavi prioritetnih voženj, spremembi prometnega programa križiščem v coni in prilagajanjem zamika,
- preskok faze (angl., skip-phase), uporabimo, če za preskočeno fazo ni najave na detektorjih in
- fiksiran najkasnejši možen zaključek faze (angl., phase fixed force-off), potrebujemo, da določimo kateri fazi se prerazporedi neporabljeni zeleni čas predhodne faze.

3.2 Opis rešitve

3.2.1 Funkcionalne zahteve

Simulacijsko okolje temelji na odprtokodnem orodju SUMO. V fazi zasnove sistema je bilo potrebno preučiti funkcionalne in nefunkcionalne zahteve, ki so opredeljene kot:

1. Visoka stopnja skalabilnosti sistema, za kar je potrebno ustrezno programsko ogrodje (angl., framework), ki omogoča podporo in možnost dodajanja različnih programskih paketov ter funkcionalnosti (npr. protokoli, podpora branju Microsoft Excel dokumentov).
2. Osnovna komunikacija naj bo kar se da standardna, zato temelji na standardnem protokolu REST (angl., Representational State Transfer).



Slika 1: **Primer adaptivne semaforske logike prometnega omrežja Podutik. Deli, ki predstavljajo poslovno skrivnost so zamegljeni.**

3. Osnovna interakcija sistema za (končnega) uporabnika naj bo omogočena preko spletnega (angl., Web) grafičnega uporabniškega vmesnika, ki omogoča interakcijo z osnovnimi funkcionalnostmi sistema preko protokola REST.
4. Sistem naj bo interoperabilen in prenosljiv, saj so pričakovane povezljivosti preko zunanjih sistemov.
5. Posamezne komponente naj bodo neodvisno razvite ter naj jih bo mogoče tudi neodvisno poganjati na različnih infrastrukturah.
6. Odzivnost simulacije naj omogoča vsaj 8-kratno hitrost simulacije glede na dejansko trajanje. Če celovit scenarij traja 24ur, naj bo torej maksimalno trajanje simulacije 3 ure.

3.2.2 Arhitektura rešitve

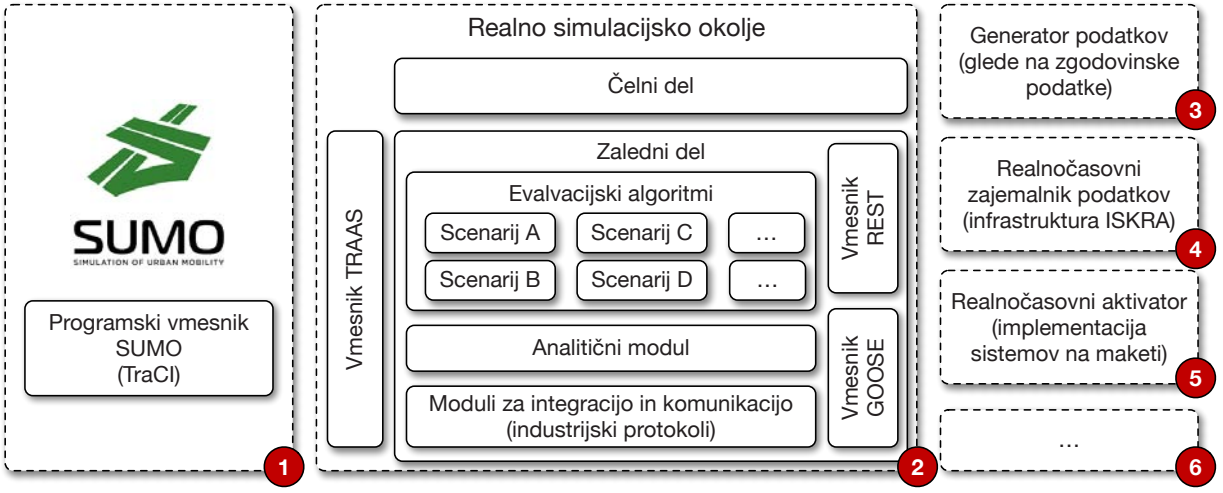
Celoten sistem je zasnovan modularno na podlagi osnovnih funkcionalnih zahtev projekta, ki so zajete v komponento za simulacijsko okolje ter izbrano okolje simulatorja SUMO. V teku projekta so se pojavile nove želje po integraciji, zato smo omogočili dodatne protokole (npr. OpenIEC61850 Goose in MQTT) ter preko vmesnikov omogočili povezljivost s komponentami za generiranje podatkov. Komponente za realnočasovno komunikacijo z našim sistemom so bile tudi neposredno integrirane s testno infrastrukturo podjetja ISKRA. Zasnova arhitekture je predstavljena na Sliki 2.

Glavna komponenta realnega simulacijskega okolja je sestavljena iz zalednega sistema, ki temelji na programskem jeziku Java in vsebuje modul z vsemi tremi simulacijskimi algoritmi, opisanimi v prejšnjem poglavju. Algoritmi komunicirajo s SUMO orodjem preko protokola SOAP (angl. Simple Object Access Protocol) z uporabo Java knjižnice TraaS, ki neposredno komunicira z vtičnikom SUMO. Takšen način komunikacije omogoča interakcijo v obe smeri in sicer:

- podatki s simulacije SUMO se lahko pošiljajo v naš zaledni sistem (npr. informacije o stanju indukcijskih zankah) ter
- zaledni sistem lahko spreminja lastnosti med izvajanjem simulacije (npr. logika semaforskih križišč).

Zaledni sistem omogoča HTTP REST protokol komunikacije, ki čelnem delu oz. spletnemu grafičnemu uporabniškemu vmesniku omogoča pripravo parametrov ter pregledovanje metrik simulacije že med samim izvajanjem. Poleg tega na željo konzorcijskega partnerja ISKRA, zaledni sistem podpira tudi protokol OpenIEC61850 Goose, ki omogoča izjemno hitro komunikacijo med strojno opremo na realnemu prometnemu omrežju (v primeru, da se komponento za simulacijo vozil priklopi na realno omrežje).

Grafični uporabniški vmesnik je bil razvit z namenom upravljanja funkcionalnosti, ki niso podprte v orodju SUMO ter predstavitvi trenda simulacije v realnem času z izrisom rezultatov metrik v grafični obliki, ter prikazu ostalih pomembnih podatkov (npr. stanja induktivnih zank). Za namene predstavitve rezultatov je pripravljena tudi stran, ki grafično ponazori vse razpoložljive metrike zaključenih simulacij.



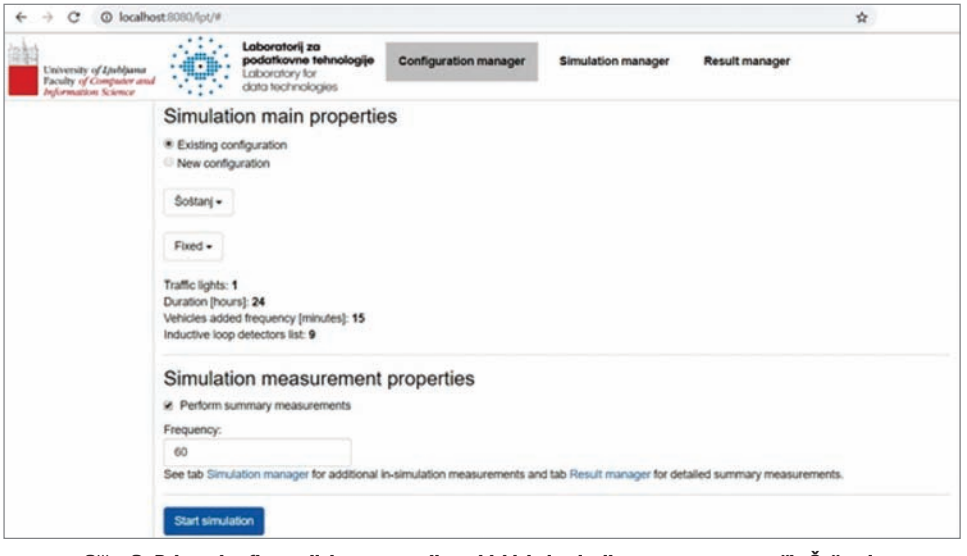
Slika 2: **Prikaz razvitega sistema za evalvacijo. Sistem sestoji iz (1) simulatorja prometa SUMO, (2) ogrodja za izvedbo simulacij, komunikacijo in analizo, (3) generatorja podatkov, (4) zajemalnika iz realnih sistemov in (5) sistema za proženje akcij. Možna je vključitev poljubnega dodatnega sistema s komunikacijo preko protokolov REST/GOOSE (6).**

3.2.3 Spletni uporabniški grafični vmesnik

Spletni grafični uporabniški vmesnik je bil razvit z namenom poenostavljenega upravljanja simulacije, njeno interakcijo v realnem času in intuitiven grafični ter numerični pregled rezultatov simulacije. Vmesnik je osnovan na podlagi treh zaslonskih form, ki so dostopne preko zavihkov, in sicer:

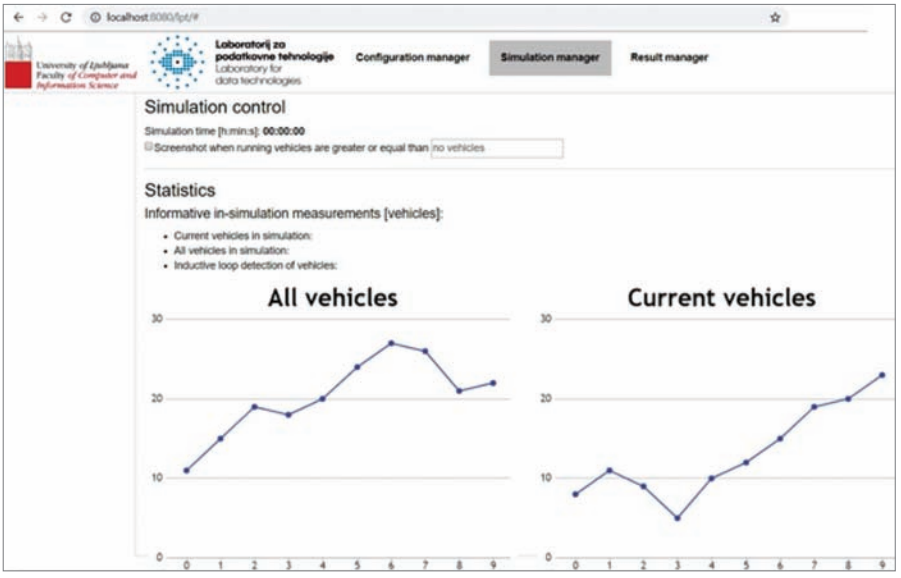
- konfiguracijski vmesnik (angl., configuration manager),
- simulacijski vmesnik (angl., simulation manager) in
- vmesnik rezultatov (angl., result manager).

Konfiguracijski vmesnik je namenjen pripravi parametrov želene konfiguracije in njenemu zagon. V osnovi vmesnik omogoča izbiro obstoječe konfiguracije, kjer se ob izbiri prikažejo osnovne lastnosti konfiguracije na podlagi XML metapodatkov konfiguracije ter vhodnih podatkov o vozilih. Te osnovne lastnosti opišejo število semaforiziranih križišč v simulaciji, trajanje simulacije, periodo dodajanja vozil (npr. na vsakih 15 minut) in število vseh induktivnih zank v konfiguraciji. Pred zagonom lahko opredelimo tudi dodatne parametre, kot je npr. način shranjevanja končnih rezultatov simulacije po zaključku ali definiramo periodo beleženja podatkov. Primer konfiguracijskega vmesnika prikazuje Slika 3.



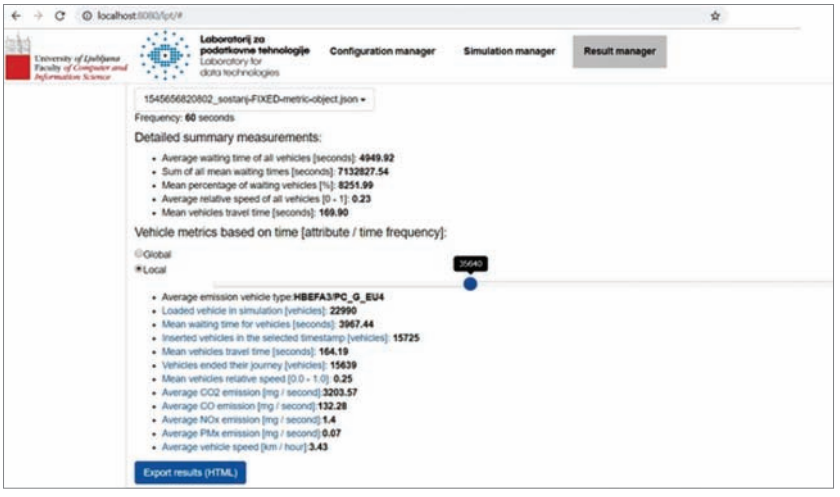
Slika 3: **Primer konfiguracijskega vmesnika pri izbiri simulacije prometnega omrežja Šoštanj.**

Simulacijski vmesnik služi uporabniku kot orodje za grafični pregled metrik tekom izvajanja simulacije. Poudarek je pri metrikah, ki se nanašajo na vozila, kot so npr. globalen prikaz števila vozil v simulaciji ali lokalni prikaz za krajše časovno obdobje (npr. v zadnjih 15 minutah). Za lažjo analizo kritičnih obremenitev nam vmesnik omogoča tudi določitev praga nad katerim se shrani zaslonska maska prometnega omrežja, ko je ta prag presežen. Na tak način nam simulator omogoča prikaz stanja ob visokih obremenitvah prometa med izvajanjem in tudi globalnih maksimumov števila vozil v prometnem omrežju. Primer simulacijskega vmesnika prikazuje Slika 4.



Slika 4: **Primer simulacijskega vmesnika, ki omogoča prikaz osnovnih podatkov o vozilih med izvajanjem simulacije ter možnost beleženja zaslonskih mask ob preseženem pragu – št. vozil v prometnem omrežju.**

Vmesnik rezultatov služi za pregled metrik iz zaključenih simulacij. Uporabnik izbere želeno konfiguracijo ter dobi na voljo osnovne povzetke simulacije (npr. kumulativno povprečje mirovanja vozil v simulaciji) ter možnost pregleda globalnih ter lokalnih metrik. Lokalne metrike so prikazane za celotno obdobje trajanja simulacije, v našem primeru 24ur (86.400 sekund). Lokalne metrike nam omogočajo še podrobnejši pregled metrik v izbranem trenutku glede na frekvenco vzorčenja. Primer vmesnika rezultatov fiksnega scenarija Šoštanj prikazuje Slika 5. Podrobnejši opis metrik pa je podan v naslednjem poglavju.



Slika 5: **Primer vmesnika rezultatov pri pregledu lokalnih metrik ob 9uri 54min (sekunda 35.640).**

4 EVALVACIJA IN DISKUSIJA

V tem poglavju je opisan postopek evalvacije s predstavitvijo metrik, metodologijo ter opisom testnih križišč, ki so osnova za pripravo rezultatov simulacije testnih križišč s primerjavo algoritmov. Rezultati zajemajo predvsem kvantitativne podatke razpoložljivih metrik, kjer so razvidne razlike delovanja posameznih algoritmov.

4.1 Predstavitev metrik

Simulator prometa SUMO ponuja nabor metrik, ki jih glede na vrsto vzorčenja delimo na dvoje - globalne ter podrobne. Globalne metrike nam nudijo informacije v realnem času tekom izvajanja simulacije in v povzetku simulacije. Podrobnih metrik ni mogoče pridobivati v orodju SUMO v realnem času, saj se metrike zapišejo v obliki dnevniških zapisov (angl., log), pri čemer so izračunane ob zaključku simulacije. Njihov izuračun je definiran glede na obdobje oz. periodo beleženja metrik (npr. vsakih 60 sekund).

Razpoložljive globalne metrike so:

- Trenutno število vozil v simulaciji [vozila],
- trenutno število vseh vozil umeščenih v simulacijo [vozila] in
- število zabeleženih vozil na (induktivnih) zankah v posameznem semaforskem ciklu [vozila].

Razpoložljive podrobne metrike so:

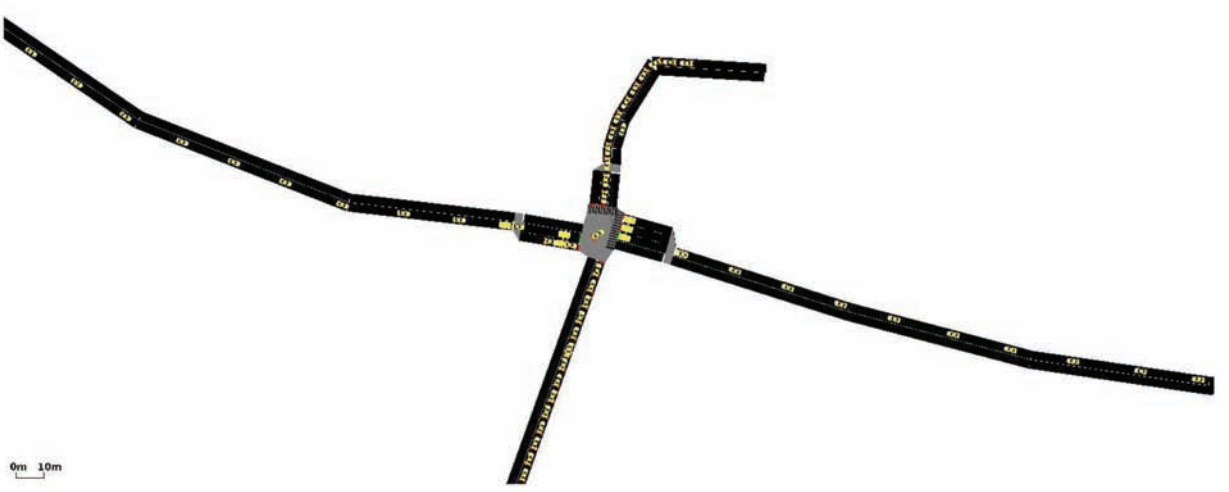
- Povprečen čas vseh vozil v mirovanju (čakanje) [sekunde],
- kumulativen seštevek časa čakanja vseh vozi [sekunde],
- razmerje vozil indikatorskih vrednosti ali je vozilo čakalo ali ne [število],
- povprečna hitrost vseh vozil čez simulacijo [km / uro],
- atributi vozil v posameznem trenutku [atribut / časovna frekvenca] kot npr.:
  - število naloženih vozil v simulaciji [vozila],
  - trenutno število vozil v simulaciji [vozila],
  - povprečen čas čakanja vozila [sekunde],
  - dodana vozila glede na predhodno časovno frekvenco [vozila],
  - povprečen čas potovanja vozila (od začetka do cilja) [sekunde],
  - število vozil z zaključenim potovanjem glede na predhodno časovno frekvenco [vozila],
  - povprečna relativna kumulativna hitrost vozil glede na omejitve [0.0 - 1.0],
- povprečen čas potovanja na posameznih cestnih odsekih [sekunde] in
- podrobne informacije individualnega vozila z možnostjo povprečiti na posamezno časovno frekvenco ali globalno:
  - CO_2 izpusti [mg / sekundo],
  - CO izpusti [mg / sekundo],
  - NOx izpusti [mg / sekundo],
  - PMx oz. izpusti trdih delcev [mg / sekundo],
  - Emisijski tip vozila (npr. EURO5, EURO6 itd.),
  - Hitrost vozila [km / uro] in
  - kategorija vozila (npr. osebni avtomobil, tovornjak, kolesar, pešec itd.).

4.2 Opis testnih križišč

Simulacija optimizacijskih algoritmov poteka na dveh različnih scenarijih oz. prometnih omrežjih. V prvem primeru gre za samostojno križišče v Šoštanju, v drugem primeru pa za prometno omrežje v Podutiku, grajeno s štirimi križišči. V nadaljevanju so povzete lastnosti obeh prometnih omrežij ter njihovo preslikavo v orodju SUMO.

4.2.1 Šoštanj

Prvi scenarij je sestavljen le iz enega semaforiziranega križišča. Značilnost križišča je povišana pretočnost križišča na podlagi cepitve prometnih pasov iz enega na dva z zahoda in cepitve iz enega prometnega pasu na tri iz vzhoda ter severa. Križišče za osnovno delovanje zadostuje pogojem opisano v vhodnih podatkih, za adaptivna algoritma pa so dodane še indukcijske zanke na vzhodu, zahodu ter jugu, skupno 8 zank. Pri gradnji križišča je bilo potrebno upoštevati ustrezne dolžine cepitev prometnih pasov in pripraviti možnosti prehoda vozil s prepovedjo polkrožnega obračanja. Prikaz scenarija v orodju SUMO je prikazan na Sliki 6.

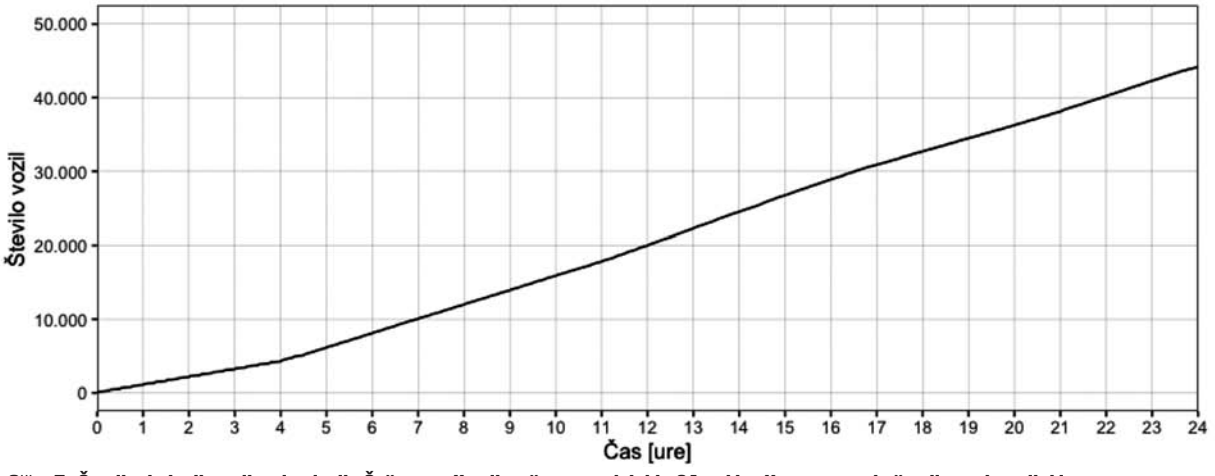


Slika 6: **Prikaz scenarija križišča v Šoštanju, ki je vozlišče na lokalni cesti ter povezuje večje kraje kot Lokovica, Šoštanj in Velenje ter premogovnik.**

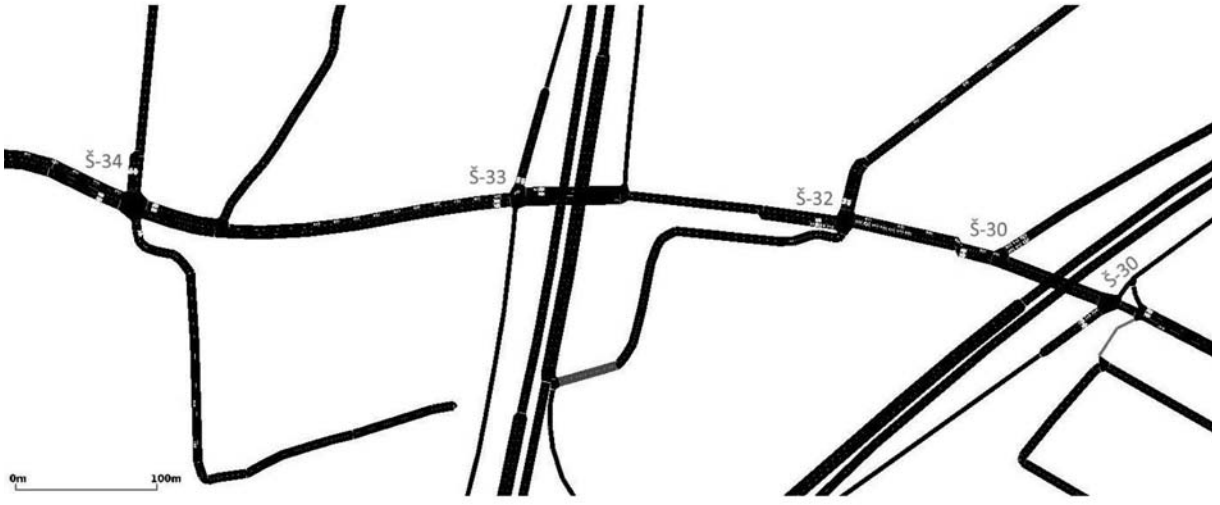
Ne glede na izbrano vrsto algoritma se vozila v simulaciji dodajajo na podlagi predhodnih meritev pridobljenimi v realnem okolju. Na podlagi meritev se določijo vozila, ki vstopajo v simulacijo s smerjo prihoda ter številom vozil, ki v simulacijo vstopajo enakomerno vsako sekundo iz posamezne smeri kot prikazuje Slika 7. Dodajanje vozil je deterministično določeno s strani podjetja Iskra d.d. na podlagi predhodnih študij obremenjenosti dotičnih omrežij in tako predstavljajo dovolj dober približek običajni prometni obremenitvi v obdobju enega dne.

4.2.2 Podutik

Drugi scenarij predstavlja prometno omrežje sestavljeno iz 4 križišč pri čemer je eno križišče deljeno na dve (Š-30). Glede na količino prevoženih vozil v križiščih je najbolj obremenjeno križišče Š-32. Takšna križišča se v notaciji algoritmov imenujejo dominantna križišča, pri čemer so vsa ostala križišča v prometnem omrežju odvisna in se temu primerno obravnavajo pri izračunih v adaptivnih algoritmih. Vsako križišče ima induktivne zanke na vseh vhodnih prometnih pasovih z izjemo križišča Š-30, ki se obravnava kot eno križišče z enim skupnim programom krmiljenja semaforjev.



Slika 7: **Število dodanih vozil v simulacijo Šoštan na X osij za časovno obdobje 24ur, kjer Y os ponazarja število vseh vozil, ki so v prometnem omrežju nastopali do določenega časa v dnevu.**



Slika 8: **Prikaz scenarija križišč v Podutiku, ki povezuje Podutik, Kamno Gorico ter ljubljansko obvoznico s Kranjem.**

Značilnost tega prometnega omrežja je prehod iz večjih hitrosti izvozov z avtoceste ljubljanske obvoznice na lokalen medkrajevni promet s temu primernimi omejitvami hitrosti. Grafična predstavitev scenarija v orodju SUMO je prikazana na Sliki 8.

Ne glede na izbrano vrsto algoritma se vozila v simulaciji dodajajo v vseh primerih enako, kar prikazuje Slika 9.

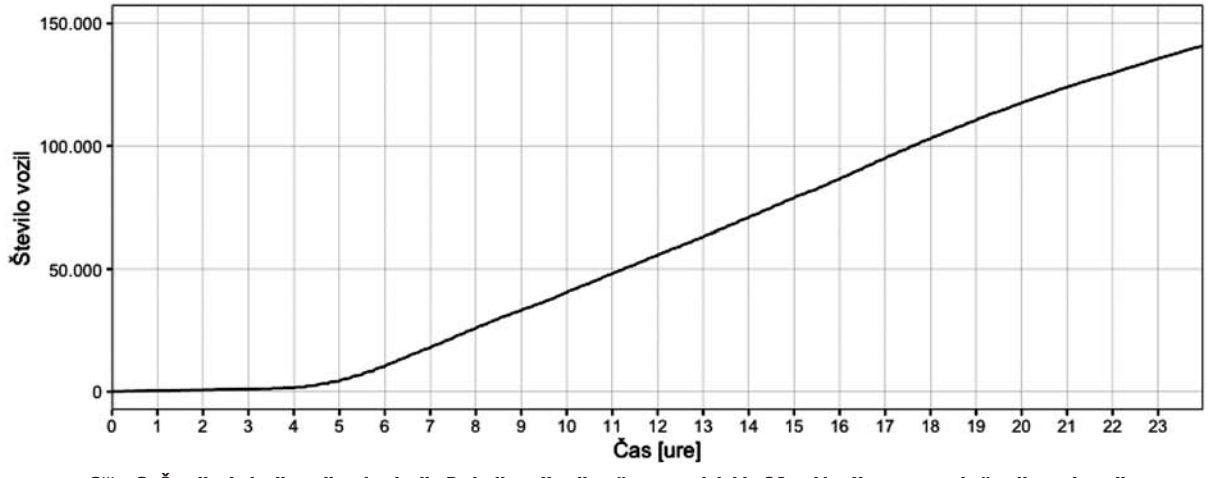
4.3 Metodologija

Metodologija se osredotoča na empirično analizo treh razpoložljivih algoritmov na predstavljenih prometnih omrežjih, pri čemer je število prihodov vozil v prometno omrežje vhodni podatek poleg topologije posameznih semaforiziranih križišč.

Pri testiranju algoritmov smo rezultate pridobili s pomočjo orodja SUMO, kjer smo beležili vse razpoložljive metrike v celotnem času simulacije celega dne. Količina razpoložljivih (surovih) rezultatov metrik vseh XML strukturiranih podatkov prometnega omrežja Šoštanj je velikostnega reda približno 10 GB. V primeru prometnega omrežja Podutik, ki je po zasnovi kompleksnejše, je količina surovih podatkov velikostnega reda 30 GB za celotno simulacijo.

4.4 Rezultati in diskusija

Pri zagonu simulacij smo z orodjem SUMO pripravili surove zabeležbe simulacij v XML obliki. Iz teh smo izločili osnovne metrike simulacij v JSON obliki za izbrano periodo vzorčenja 60 sekund, ki so pred-



Slika 9: **Število dodanih vozil v simulacijo Podutik na X osij za časovno obdobje 24ur, kjer Y os ponazarja število vseh vozil, ki so v prometnem omrežju nastopali do določenega časa v dnevu.**

stavljene v nadaljevanju. Vizualizacija rezultatov je v celoti pripravljena s spletnim grafičnim vmesnikom. Glede na to, da so simulacijski algoritmi deterministični, so bile vse simulacije zagnane le po enkrat.

4.4.1 Šoštanj

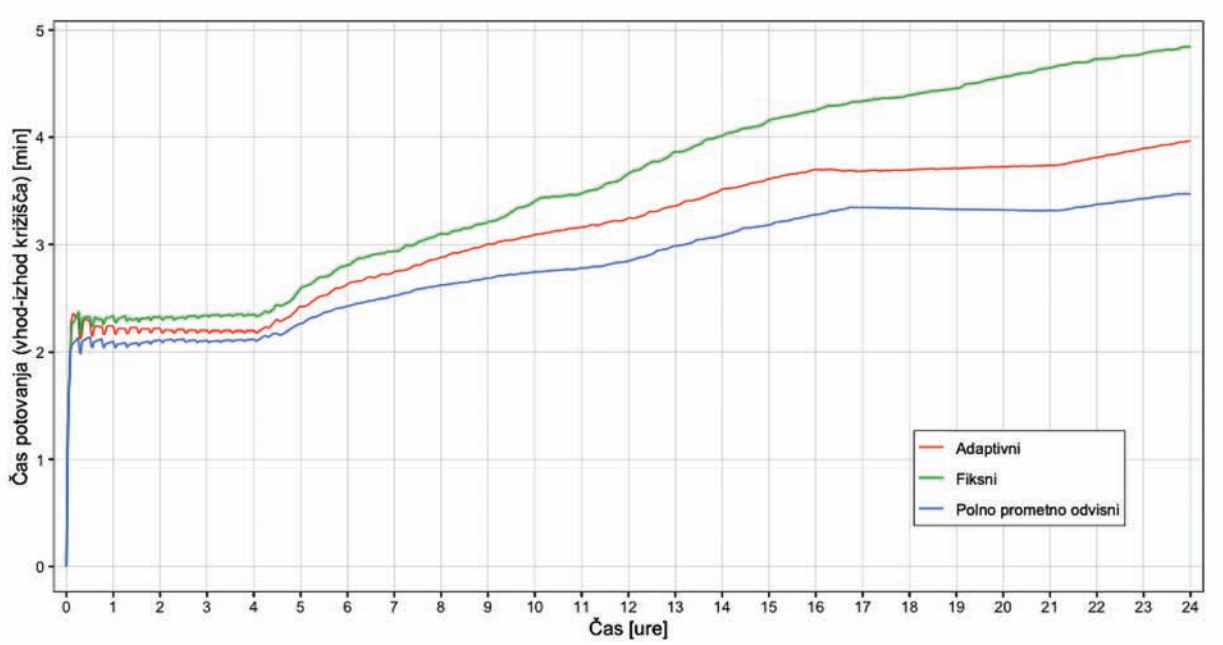
Prometno omrežje Šoštanj je sestavljeno iz enega semaforiziranega križišča, ki povezuje največja okoliška mesta in industrijo. Simulacije so bile izvedene z enakimi vhodnimi podatki dodajanja vozil - čez celotno simulacijo kumulativno približno 42.000 vozil. Osnovne časovne metrike so prikazane v Tabeli 2. Čas polno prometno odvisnega programa je najdaljši, saj očitno prihaja do zasičenja vozil, pri ostalih dveh programih pa se razlikuje glede na izbrano metriko.

Iz rezultatov simulacij prometnega omrežja Šoštanj je s Slike 10 razvidno, da fiksni program z najbolj togo logiko deluje najslabše oz. ima povprečno vozilo najdaljši potovalni čas pri večjih obremenitvah omrežja od jutranje konice naprej. Polno prometno odvisni program v tem primeru dosega najboljše rezultate, pri čemer je značilnost algoritma, da omogoča podaljšanja zelenih ciklov glede na vnaprej določen maksimum. Adaptivni program v tem primeru podaljšanja manj ugodno obravnava, saj s prevelikim podaljševanjem vozil iz vzhoda proti zahodu in obratno, obenem podaljšuje čas potovanja vozil s severa ali južne poti. Vse rezultate bi bilo mogoče dodatno izboljšati pri podaljševanju poti prometnega omrežja, saj sta severna in južna stran bistveno krajši, kar povzroča manj enakomerno hitrost vozil zaradi nenehnih pospeševanj ter zaviranj vozil. Dodatna možnost za izboljšavo bi zagotovo bila vpeljava dodatne induktivne zanke za vozila, ki vstopajo s severne strani.

Relativna hitrost se glede na čas simulacije razlikuje na posameznem programu v normirani obliki, ki je grafično povzet na Sliki 11. Fiksni program se pričakovano pretežno izkazuje kot najslabši, saj dosega najvišje vrednosti in posledično najnižjo povprečno hitrost vozil. Ostala programa se pa glede na stopnjo zasičenosti dosegata primerljive rezultate. V primerih, ko pride do izrazite spremembe v relativni hitrosti v kratkem časovnem obdobju pomeni, da prihaja do nenadnih zastojev. Ob višanju relativne hitrosti zastoji prehajajo v tekoč promet. To je najbolj izrazito v obdobju po popoldanski prometni konici po 17:00 uri, ko promet upada.

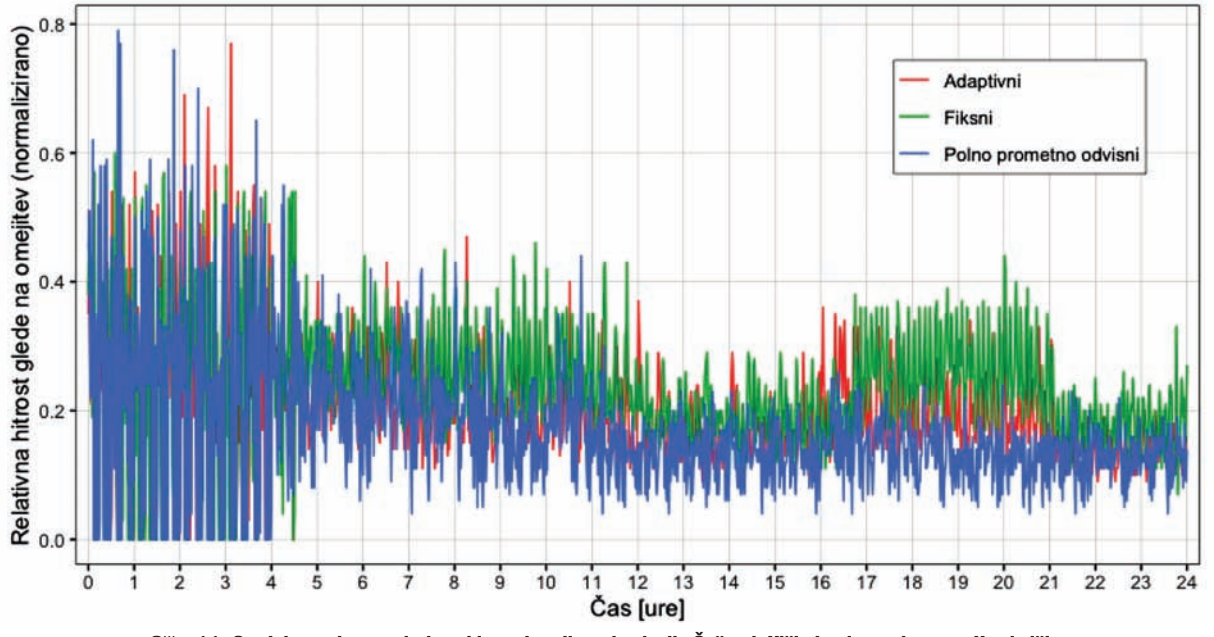
Tabela 2: **Rezultati časov trajanja vozil glede na različne prometne algoritme na prometnem omrežju Šoštanj.**

Metrike	Fiksni program	Polno prometno odvisni program	Adaptivni program
Povprečni čas čakanja vseh vozil [sekund]	6.734,82	4.949,92	5.976,91
Vsota vseh srednjih časov (mediana) v celotni simulaciji [sekund]	9.704.875,62	7.132.827,54	8.612.728,82
Srednji časi čakanja vozil [sekund]	8.190,52	8.251,99	9.447,20
Povprečna relativna hitrost vseh vozil v razponu [0-1]	0,17	0,23	0,20
Mediana potovanja vozila [sekund]	215,2	196,90 188,43	

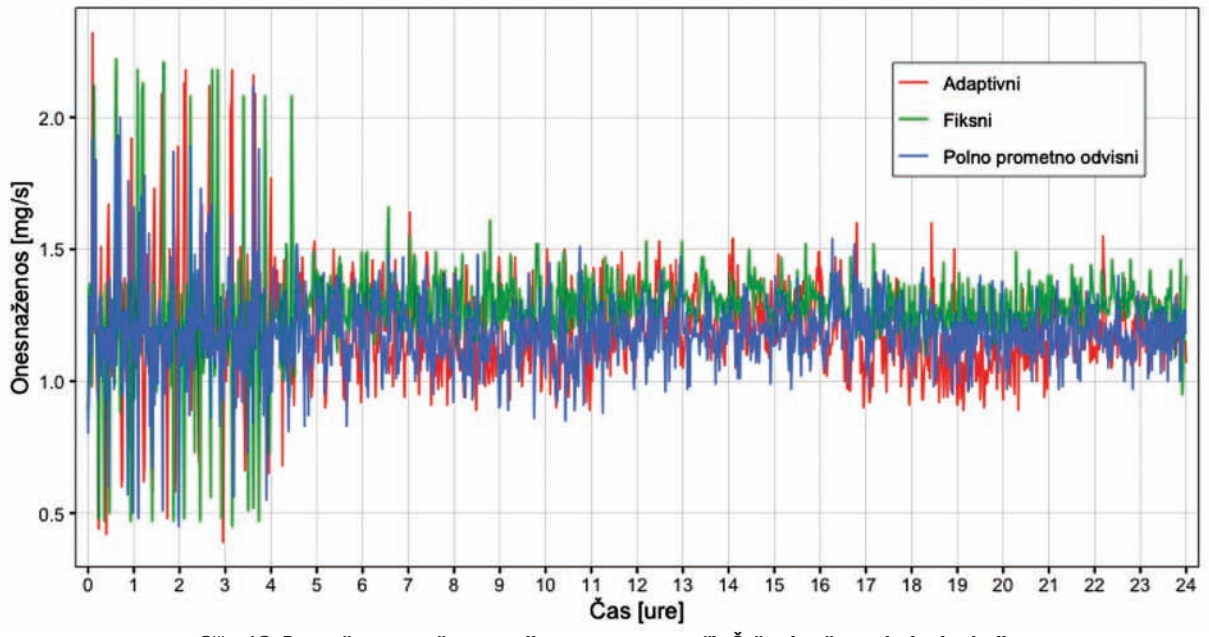


Slika 10: **Srednja vrednost časa potovanja vozil za simulacijo Šoštanj. Višja kot je vrednost na Y osi nižje so hitrosti in posledično višja so zasičenja v omrežju.**

Na Sliki 12 je predstavljena emisijska onesnaženost z delci NOx pri vseh prometnih programih, pri predpostavki, da vozila vozijo z motorji standarda Euro5, ki je najpogosteje zastopan na slovenskih cestah. Stopnja onesnaženosti je pogojena s pospeševanjem in zaviranjem vozil, kjer spremembe hitrosti terjajo višjo porabo goriva in posledično večjo onesnaženost. Rezultati nakazujejo, da fiksni program povzroča največjo onesnaženost v primerjavi z ostalima dvema programoma.



Slika 11: **Srednja vrednost relativne hitrosti vozil za simulacijo Šoštanj. Višja kot je vrednost na Y osi višje so hitrosti in posledično manjša so zasičenja v omrežju.**



Slika 12: **Povprečna onesnaženost vozil v prometnem omrežju Šoštanj za čas trajanja simulacije.**

4.4.2 Podutik

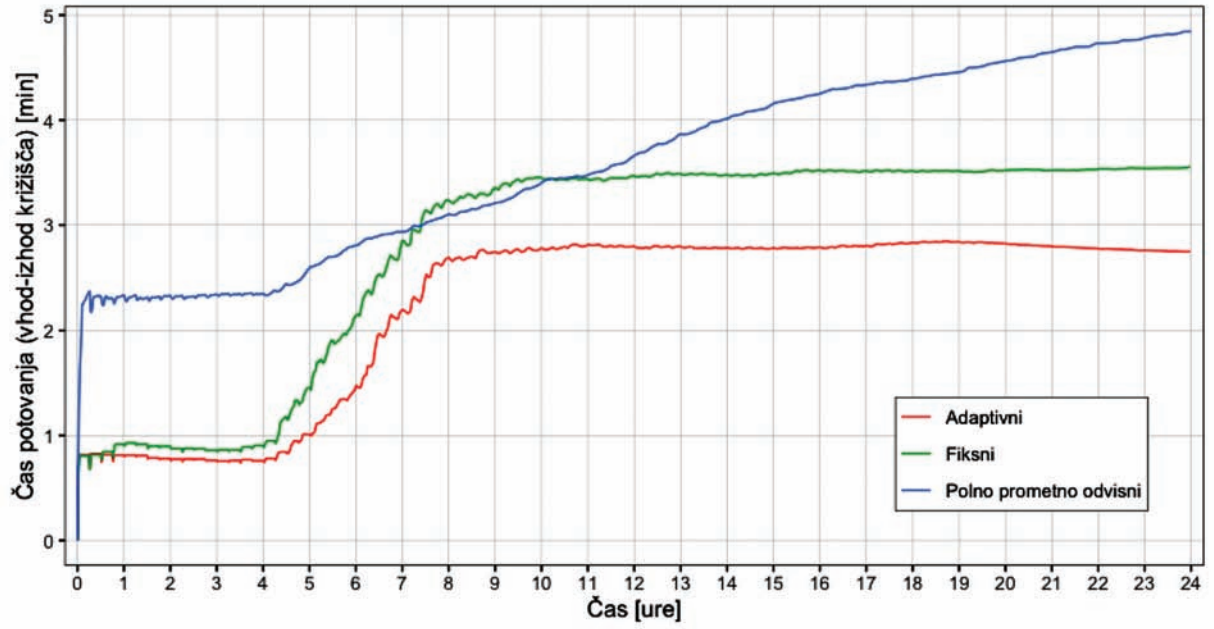
Prometno omrežje Podutik je sestavljeno iz štirih semaforiziranih križišč. Simulacije so bile izvedene z enakimi vhodnimi podatki dodajanja vozil, čez celotno simulacijo približno 140.000 vozil kumulativno. Osnovne metrike osredotočene na čas, so prikazane v Tabeli 2. Časi programov se glede na metriko razlikujejo, pri čemer se togi fiksni program ne izkaže najslabše v vseh primerih.

4.4.3 Primerjava rezultatov algoritmov

Iz rezultatov simulacij prometnega omrežja Podutik je s Slike 15 razvidno, da fiksni program s togim delovanjem deluje primerljivo s polno prometno odvisnim programom, kjer ima polno prometno odvisni program hitrejše čase potovanja pri manjših obremenitvah prometnega omrežja. Polno prometno odvisni program pri večjih prometnih obremenitvah s podaljševanjem zelenih faz zapira hiter prehod križišč iz drugih strani. Kot najbolj obetaven algoritem se je v tem primeru izkazal adaptivni program, ki v povprečju bolj optimalno upravlja cikle in vidno skrajša potovalne čase vozil. Smiselno je omeniti, da tudi v tem prometnem omrežju ni natančno definirano, kje natančno vozila vstopajo v simulacijo, zato bi bilo bolj objektivno simulacijo izvesti na prometnem omrežju z daljšimi cestnimi odseki. V vseh treh primerih je na podlagi podatkov orodja SUMO srednja vrednost relativne hitrosti prikazala anomalije v simulatorju pri uporabi različice 0.31.

Tabela 3: **Rezultati časov trajanja vozil glede na različne prometne algoritme na prometnem omrežju Podutik.**

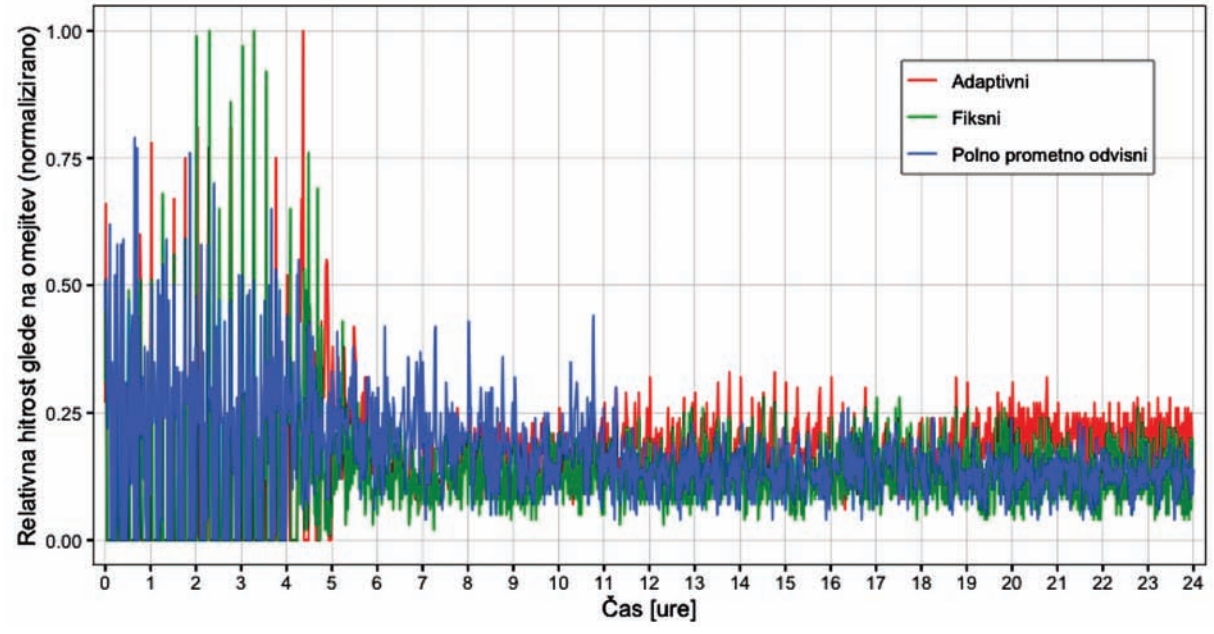
Metrike	Fiksni program	Polno prometno odvisni program	Adaptivni program
Povprečni čas čakanja vseh vozil [sekund]	3.511,92	1.513,51	3.477,96
Vsota vseh srednjih časov (mediana) v celotni simulaciji [sekund]	5.057.168,26	5.751.135,37	5.008.257,33
Povprečna relativna hitrost vseh vozil v razponu [0-1]	0,14	0,15	0,18
Mediana potovanja vozila [sekund]	169,20	159,52	135,19



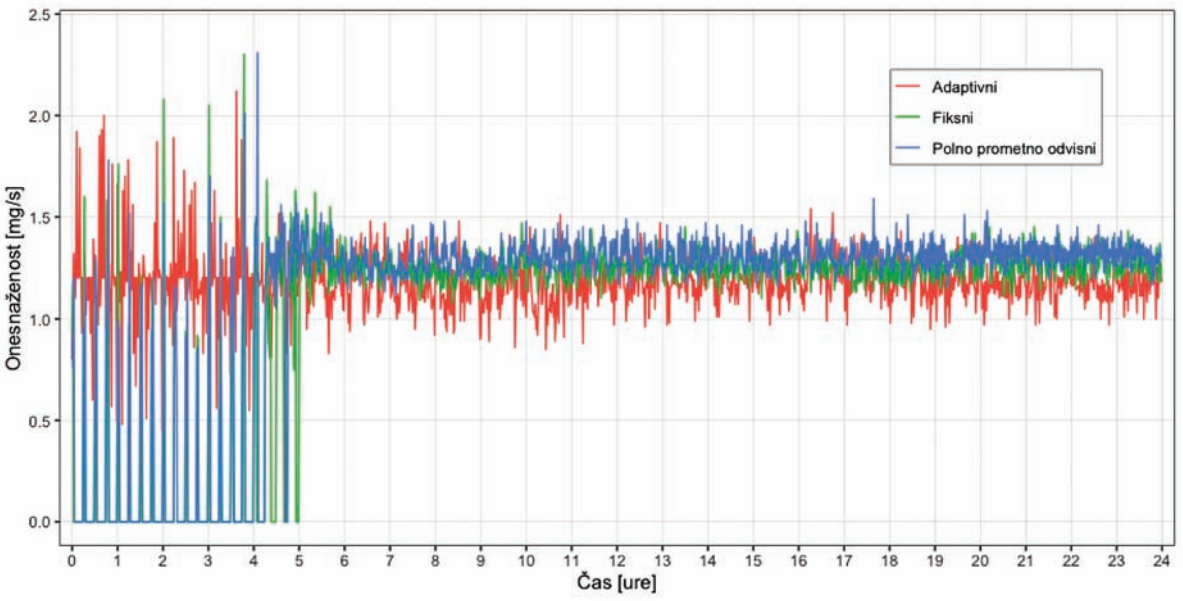
Slika 13: **Srednja vrednost časa potovanja vozil za simulacijo Podutik. Višja kot je vrednost na Y osi nižje so hitrosti in posledično višja so zasičenja v omrežju.**

Relativna hitrost se glede na čas simulacije razlikuje na posameznem programu v normirani obliki, ki je grafično povzet na Sliki 13. Polno prometno odvisni program se že na začetku zasiči in vrača najslabše rezultate. Adaptivni program ima podobna zasičenja kot fiksni program, pri čemer se pri adaptivnemu čas potovanja v povprečju skrajša za 30 sekund.

Relativna hitrost se glede na čas simulacije razlikuje na posameznem programu v normirani obliki, ki je grafično povzet na Sliki 14. Kot najslabši se izkaže polno prometno odvisni program, saj privzeti pragovi niso primerni za konkretno simulacijo na podlagi vozil, ki se konstantno linearno kopičijo v simulaciji. Fiksni program dosega relativno dobre



Slika 14: **Srednja vrednost relativne hitrosti vozil za simulacijo Podutik.**



Slika 15: **Povprečna onesnaženost vozil v prometnem omrežju Podutik za čas trajanja simulacije.**

rezultate kjer pride pri adaptivnem programu do dodatnega izboljšanja za povprečno 30 sekund pri potovanju vsakega vozila.

Na Sliki 15 je predstavljena emisijska onesnaženost z delci NOx pri vseh prometnih programih, pri predpostavki, da vozila vozijo z motorji standarda Euro5, ki je najpogosteje zastopan na slovenskih cestah. Stopnja onesnaženosti je pogojena s pospeševanjem in zaviranjem vozil, ki se v prometnem omrežju odražajo z višjo onesnaženostjo z začetkom jutranje prometne konice po 5:00 uri. Rezultati nakazujejo, da fiksni program povzroča največjo onesnaženost v primerjavi z ostalimi programi.

5 SKLEP

Na Svetu predstavlja preučevanje optimizacije prometnih omrežij še vedno velik izziv zaradi velike količine dejavnikov, ki na lahko simulacijo vplivajo v realnem okolju. Pri vnaprej znanih vhodnih podatkih lahko z orodjem SUMO preučujemo odzive različnih algoritmov ali pa druge dejavnike, kot so maksimalne prometne obremenitve posameznih cestnih odsekov ali semaforiziranih križišč, in s tem zmanjšamo čas potovanja vozil ter obenem znižamo onesnaženost okolja.

V delu je predstavljen celovit sistem za simulacijo optimizacijskih algoritmov na dveh različnih prometnih tokovih. V delu smo se najprej posvetili definiciji podatkov ter predstavitvi posebnosti prometnih omrežij, na katerih smo testirali optimizacijske algoritme. Na podlagi podatkov, razpoložljivih tehnologij in potencialnih možnostih za integracijo, smo predstavili arhitekturo rešitve in podporna orodja kot spletni grafični vmesnik za namene evalvacije. Implementirana rešitev podpira tri optimizacijske algoritme ter dve testni prometni omrežji z možnostjo nadaljnjih nadgradenj. Na podlagi razvitega spletnega orodja za analitiko smo povzeli osnovne značilnosti algoritmov ter njihove globalne lastnosti obnašanja algoritmov v obdobju trajanja posamezne simulacije 24-urnega cikla.

Pri pripravi sistema za simulacijo prometnih tokov smo naleteli na številne izzive s strani komunikacijskih protokolov med posameznimi komponentami sistema. Implementirali smo tudi globalno analitiko rezultatov za celotno obdobje trajanja simulacije, česar orodje SUMO v osnovi ne podpira. Pri integraciji algoritmov je bila priprava vhodnih podatkov semaforske logike otežena zaradi nestandardiziranega formata opisa semaforskih logik, ki je pripravljen na rastrski sliki v formatu PDF. Iz simuliranih prometnih omrežij smo ugotovili, da adaptiven algoritem v simulaciji Šoštanj ne deluje bolje od polno prometno odvisnega programa. Pri prometnem omrežju Podutik so rezultati pričakovani. V osnovi ugotovitve kažejo, da adaptivni algoritmi vračajo boljše rezultate od togega fiksnega deterministčnega algoritma. V prihodnjem delu se bomo osredotočili na izboljšavo obstoječih algoritmov ter razširili testne podatke z novimi prometnimi omrežji.

ZAHVALA

Raziskava je bila finančno podprta s sredstvi programa EkoSmart s strani Republike Slovenije in Evropske unije iz Evropskega sklada za regionalni razvoj. Raziskava je bila mogoča s prenosom znanja in domenskih izkušenj podjetja ISKRA d. o. o., Stegne 21, 1000 Ljubljana.

LITERATURA

[1] Akiyama, Takamasa & Okushima, Masashi. (2006). Implementation of cordon pricing on urban network with practical approach. Journal of Advanced Transportation. 40. 221 - 248. 10.1002/atr.5670400208.

[2] Cheng, Y. (2017).Increasing Robustness of Differential Evolution by Passive Opposition,volume 454, pages 85–94.

[3] Gartner, N. (1990). Opac: Strategy for demand-responsive decentralized traffic signal control. IFAC Proceedings Volumes, 23(2):241 – 244. IFAC/IFIP/IFORS Symposium on Control, Computers, Communications in Transportation, Paris, France, 19-21 September.

[4] Hong Wei, Wang Yong, Mu Xuanqin and Wu Yan, »A cooperative fuzzy control method for traffic lights,« ITSC 2001. 2001 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.01TH8585), 2001, pp. 185-188.

[5] Hu, Y., Thomas, P., & Stonier, R. (2007). Fuzzy control of traffic signals accompanying pedestrian crossings. In: Proceedings of the 2007 WSEAS international conference on computer engineering and applications, Gold Coast, Australia, January 17–19 (pp. 288–292).

[6] J. Favilla, A. Machion and F. Gomide, »Fuzzy traffic control: adaptive strategies,« Second IEEE International Conference on Fuzzy Systems, 1993, pp. 506-511 vol.1, doi: 10.1109/FUZZY.1993.327519.

[7] Kim, J., A fuzzy logic control simulator for adaptive traffic management, IEEE International Conference on Fuzzy Systems, vol. 3, 1997, pp. 1519- 1524.

[8] Kosonen, I. (2003). Multi-Agent Fuzzy Signal Control Based on Real-Time Simulation. Transportation Research Part C: Emerging Technologies, 11(5), 389-403.

[9] Mirchandani, P. and Fei-Yue Wang (2005). Rhodes to intelligent transportation systems. IEEE Intelligent Systems, 20(1):10–15.

[10] Pappis C. and Mamdani E. (1977). A Fuzzy Logic Controller for a Traffic Junction. IEEE Transactions on Systems, Man and Cybernetics. Vol. SMC-7, No. 10, pp. 707–717.

[11] Sayers, T., Anderson, J. and Bell, M. (1998), »Traffic Control System Optimisation: A Multiobjective Approach«, Griffiths, J.D. (Ed.) Mathematics in Transport Planning and Control, Emerald Group Publishing Limited, Bingley, pp. 37-46.

[12] Sen, S. and Head, K. (1997). Controlled optimization of phases at an intersection. Transportation Science, 31(1):5–17.

[13] Teodorovic, D., 1999. »Fuzzy logic systems for transportation engineering: the state of the art,« Transportation Research Part A: Policy and Practice, Elsevier, vol. 33(5), pages 337-364, June.

[14] Trabia, M., Kaseko, M. S., Ande, M. (1999). A Two-Stage Fuzzy Logic Controller for Traffic Signals. Transportation Research Part C: Emerging Technologies, 7(6), 353-367.

[15] Zhanbo Sun; Wan Li; Xuegang (Jeff) Ban; and Tianyu Huang: An Adaptive Traffic Signal Control System (ACS-Lite) in Heavily Congested Arterial Traffic: Experiences and Lessons Learned; CICTP 2018 : Intelligence, Connectivity, and Mobility. 2018.

[16] Zhang, Y. and Ye, Z. (2008). Short-term traffic flow forecasting using fuzzy logic system methods. Journal of Intelligent Transportation System 12 102–112.

Sandi Gec je zaposlen kot asistent na Fakutelti za računalništvo in informatiko Univerze v Ljubljani. V raziskovalno-razvojnih projektih se je ukvarjal z uporabo semantičnih tehnologij pri razvoju oblačnih sistemov, bazami znanja ter integracijo podpornih rešitev v oblaku. Svoje znanje je apliciral na Horizon 2020 projektih SWITCH, ENTICE in DECENTER. Trenutno se v okviru Horizon 2020 projekta ONTOCHAIN ukvarja z novimi pristopi tehnologije veriženja blokov, predvsem s pametnimi pogodbami ter komunikacijo med verigami in zunaj verige.

▪

Vlado Stankovski je redni profesor računalništva in informatike. Ima bogate izkušnje na področju programskega inženirstva, računalništva v oblaku, na robu in v megli, porazdeljenih sistemov, semantike ter tehnologij umetne inteligence (strojno, globoko učenje). Sodeloval je pri načrtovanju, razvoju in integraciji tehnologij vmesne programske opreme. Sodeloval je pri več nacionalnih in mednarodnih projektih, v konzorciju Superračunalniški center Slovenije, na projektu pametne specializacije IQ DOM ter v gruči za programsko inženirstvo projektov Obzorje 2020 kot predstavnik projektov ENTICE, SWITCH in DECENTER. Vlado Stankovski je znanstveno-tehnični koordinator projekta Naslednje generacije interneta ONTOCHAIN.

▪

Marko Bajec je redni profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Je vodja Laboratorija za podatkovne tehnologije in Iot Demo Centra. Raziskovalno in aplikativno se ukvarja s podatkovno intenzivnimi sistemi, njihovim razvojem in obvladovanjem. Sodeloval je pri razvoju različnih podatkovnih platform, vključno s platformo za mobilno in elektronko zdravstvo, platformo za analizo medijev, platformo za simulacijo in upravljanje prometa itd. V zadnjem času se poglobljeno ukvarja z govornimi tehnologijami. V svoji karieri je vodil ali koordiniral več kot 30 raziskovalnih in aplikativnih projektov ter prejel več priznanj in nagrad za prenos znanja v prakso.

▪

Slavko Žitnik je docent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer poučuje predmete s področja podatkovnih baz in obdelave podatkov. Raziskovalno se ukvarja z obdelavo naravnega jezika, predvsem na semantični ravni. Je član več strokovnih združenj, sodeluje pri organizaciji konferenc s področja informatike in pri projektih, povezanih z obdelavo podatkov na področju interneta stvari.

Primerjava varnosti in pomnjenja gesel: ugotavljanje uporabnosti tradicionalne metode in metode igrifikacije

Leon Bošnjak, Viktor Taneski
Fakulteta za elektrotehniko, računalništvo in informatiko, Univerza v Mariboru, Koroška cesta 46, 2000 Maribor
leon.bosnjak@um.si, viktor.taneski@um.si

Izvleček

Besedilna gesla so dandanes še vedno najbolj pogost mehanizem avtentikacije, predvsem zaradi enostavne uporabe in implementacije, ter lažje pomljivosti. Kljub številnim prednostim pa so s postopnim povečanjem procesorske moči računalnikov postala dovzetna za številne napade, zaradi česar se je pojavila potreba po daljših, bolj varnih, ter težje zapomljivih geslih. Posledično so bile raziskane številne alternativne sheme avtentikacije, med drugim tudi grafična gesla. Študija, ki so jo leta 2017 izvedli McLennan in sodelavci, je predstavila novo shemo grafične avtentikacije, imenovano Game Changer Password System (GCPS), v sklopu katere so znaki gesla predstavljeni s položaji igralnih figuric. Čeprav avtorji ocenjujejo uporabnost sheme kot obetavno, rezultati študije ne dosegajo zadostne stopnje veljavnosti, saj ne upoštevajo zahtevane varnosti gesel. Poleg tega so avtorji ugotovili, da je potrebno rezultate primerjati tudi s tradicionalnimi gesli. V tej raziskavi smo preučili pomljivost in čas vnosa besedilnih in GCPS gesel, ter rezultate med obema metodama statistično primerjali. Pokazali smo, da so besedilna gesla boljša tako glede pomljivosti, kot tudi hitrosti vnašanja, kar opravičuje njihovo uveljavljenost kot osnovni mehanizem avtentikacije.

Ključne besede: Gesla igrifikacije, besedilna gesla, pomljivost gesel, varnost gesel, statistična primerjava

Comparison of password security and memorability: assessing the usability of traditional and gamification methods

Abstract

Textual passwords are the most common authentication mechanism due to their ease of use and implementation, as well as high memorability. As the computer processing power continued to increase, textual passwords gradually became less secure, resulting in an increased demand for longer, more secure and harder-to-remember passwords. As a result, other authentication schemes such as graphical passwords have been explored. A study by McLennan *et al.* in 2017 introduced a new authentication scheme called Game Changer Password System (GCPS), which uses game figure positions as password characters. The usability of the scheme was evaluated as promising, however these conclusions suffered from validity threats as the passwords used in the study did not represent secure GCPS passwords. In addition, the proposed scheme was not compared to the traditional passwords. In this study, we examined password recall rates and reaction time (login time), and we compared the results between the textual and GCPS passwords. We conclude that textual passwords are still superior both in terms of memorability and input speed, which justifies their prominence as a primary authentication mechanism.

Keywords: Gamification method passwords, textual passwords, password memorization, password security, statistical comparison

1 UVOD

Besedilna gesla so prevladujoča metoda avtentikacije že od šestdesetih let prejšnjega stoletja, ko se je prvič pojavila potreba po zaščiti občutljivih digitalnih podatkov [8]. Takrat so se uveljavila, ker jih je bilo enostavno implementirati, si jih je bilo mogoče zlahka zapomniti, hkrati pa so zagotavljala tudi zadostno varnost. Ker pa se je moč računalniške obdelave z leti povečevala (v skladu z Moorovim zakonom [7]), je kratka in preprosta gesla postopoma postajalo vse lažje razbiti. Čeprav so strokovnjaki za varnost kot odgovor na vse pogostejše zlorabe podatkov zagovarjali uporabo daljših in bolj zapletenih gesel, je pomnjenje le-teh postala težavna, kar je uporabnike spodbudilo, da se zatečejo k slabim praksam upravljanja z gesli. Žal takšna rešitev ostaja zgolj začasna: ker naj bi se procesorska moč računalnikov še naprej povečala, si bodo uporabniki dolga in zapletena gesla za več storitev, do katerih dostopajo, vedno težje zapomnili.

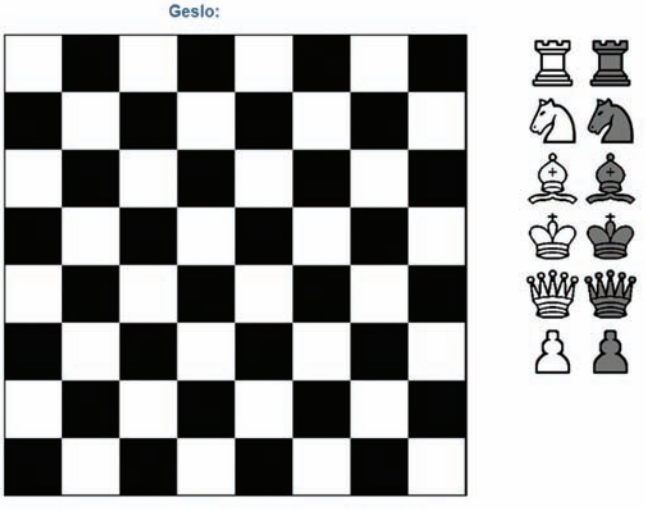
Posledično je bilo na področju informacijske varnosti v zadnjih nekaj desetletij izvedenih veliko raziskav na tematiko alternativnih shem avtentikacije. Čeprav obstoječe raziskave doslej še niso odkrile očitno boljše metode, obstaja nekaj obetavnih alternativ, ki bi lahko v prihodnosti dopolnile ali celo nadomestile besedilna gesla. Na primer, grafična gesla ohranjajo številne prednosti besedilnih gesel, kot sta enostavna uporaba in pomljivost, hkrati pa lahko zaradi svoje razširljivosti znatno povečajo stopnjo varnosti.

Tako kot besedilna gesla, so tudi grafična gesla avtentikacijski mehanizem, ki temelji na znanju. Glavni cilj grafičnih gesel je uporaba slik ali oblik za zamenjavo besedila, saj so številne kognitivne in psihološke študije pokazale, da si ljudje veliko bolje zapomnijo slike kot besede [20]. Najbolj splošno sprejeta teorija, ki pojasnjuje to razliko, je teorija dvojnega kodiranja [10], ki nakazuje, da se verbalni in neverbalni spomini v možganih obdelujejo in predstavljajo drugače. Slike, ki jim je pripisan zaznan pomen na podlagi neposrednega opazovanja, so predstavljene na način, ki ohranja opazovane zaznavne značilnosti. Besedilo je predstavljeno s simboli, ki izražajo asociativno spoznavni pomen. Posledično vsakršna dodatna obdelava, ki je potrebna za verbalni spomin, kognitivno nalogo oteži. Tako si lahko človek zlahka zapomni obraze ljudi, kraje, ki so jih obiskali, ter stvari, ki so jih opazovali dlje časa. Grafična gesla so se skozi čas razvila iz preprostega prepoznavanja obrazov, risb in kognitivnih shem do grafičnih metod igrifikacije [21, 13].

V študiji iz leta 2017 so McLennan in sodelavci [16] predstavili novo shemo grafične avtentikacije, imenovano Game Changer Password System (v nadaljevanju GCPS). Metoda predpostavlja standardno igralno ploščo poljubne namizne igre, na katero mora uporabnik v določenem zaporedju postaviti igralne figurice, pri čemer vsaka pozicija igralne figure na plošči predstavlja znak gesla. Primer metode GCPS je prikazan na sliki 1, kjer je prikazana grafična metoda na osnovi šahovnice.

Rezultati eksperimenta so pokazali, da so si uporabniki v več starostnih skupinah razmeroma enostavno zapomnili GCPS gesla (77 % povprečna natančnost v treh poskusih), čeprav je posamezen vnos trajal razmeroma dolgo (povprečni čas 28 sekund). V sklopu drugega eksperimenta, ki je trajal 10 tednov, so avtorji ugotovili, da se je sposobnost udeležencev, da si zapomnijo svoja gesla, sčasoma povečala (82 % povprečna natančnost), medtem ko so se njihovi reakcijski časi zmanjšali (povprečni čas 11 sekund).

Čeprav so ti rezultati sicer obetavni, na njihovi osnovi ne moremo sklepati o uporabnosti metode GCPS zaradi metodoloških pomanjkljivosti omenjene študije. Varnostna analiza metode GCPS je pokazala, da bi bilo za skladnost s trenutnimi varnostnimi zahtevami potrebno geslo z najmanj 7 znaki [6]. Prav tako v času pisanja tega članka NIST specifikacije določajo minimalno dolžino besedilnega gesla 8 znakov [1]. Ker so bili poskusi izvedeni na dvo- in štirimestnem geslu, so dobljene natančnosti vnosov in



Slika 1: **Grafični prikaz šahovnice pri metodi GCPS.**

reakcijski časi najverjetneje preveč optimistični. Prav tako so avtorji izpostavili, da bi bilo potrebno rezultate primerjati z že uveljavljenimi avtentikacijskimi metodami, kot so na primer tradicionalna gesla.

Namen obstoječe raziskave je razširiti delo [16] ter preučiti, ali so pri avtentikaciji grafična gesla GCPS bolj zapomljiva v primerjavi z besedilnimi gesli. V sklopu izvedenega eksperimenta smo določili varnostne politike, s katerimi smo zagotovili zadostno varnost izbranih gesel.

Raziskovalni vprašanji, na kateri smo odgovarjali, sta:

- Ali so izbrana grafična gesla bolj zapomljiva kot klasična besedilna gesla?
- Ali je čas, potreben za uspešno prijavo, nižji pri grafičnih kot pri besedilnih geslih?

Da bi odgovorili na zadana raziskovalna vprašanja, smo nad vzorcem študentov izvedli pilotno študijo. Eksperiment je potekal v dveh fazah. V prvi fazi so si študenti ustvarili uporabniške račune, ki so bili zaščiteni z obema metodama, torej s klasičnimi besedilnimi gesli, ter grafičnimi gesli GCPS. Po natanko dveh tednih je sledila druga faza raziskave, v kateri so se isti študentje poskusili ponovno prijaviti v uporabniške račune, ki so si jih ustvarili v prvi fazi. Pri tem smo merili število napačnih vnosov gesel, ter hitrost vnosa posameznih gesel.

1.1 Motivacija

Zaradi svoje zasnove grafična gesla (kot je GCPS) ohranjajo številne prednosti klasičnih, besedilnih shem avtentikacije: so relativno enostavna za implementacijo in intuitivna za uporabo, od uporabnika ne zahtevajo, da ima fizične žetone, poleg tega pa njihova izrazito vizualna podoba omogoča, da si je takšna gesla lažje zapomniti in pozneje priklicati na podlagi asociacij. Ker je takšne sheme možno enostavno razširiti, prav tako omogočajo drastično povečanje varnosti, zaradi česar bi takšne sheme lahko v prihodnosti potencialno dopolnile ali celo nadomestile besedilna gesla.

V tej raziskavi nameravamo preučiti predvsem dva ključna vidika uporabnosti: pomljivost in čas vnosa gesel. Izvorna študija je v sklopu izvedenih eksperimentov že preučevala oba vidika [16], vendar avtorji pri tem niso upoštevali takratnih varnostnih zahtev, niti niso svojih rezultatov primerjali z drugimi avtentikacijskimi metodami, kot so predlagali avtorji v [6]. Naša motivacija je razširiti obstoječe študije metode GCPS in rezultate primerjati primerjati s klasičnimi besedilnimi gesli, z namenom, da bi ugotovili, kakšna je izvedljivost in uporabnost metod grafične avtentikacije GCPS v praksi.

1.2 Organizacija članka

V nadaljevanju članka bo sledila predstavitev sorodnih del in izbranih tipov grafičnih gesel. Tretje poglavje povzema glavne metode raziskovanja. Podrobneje bomo predstavili obe raziskovalni vprašanji, postopek raziskovanja in način izvedbe meritev. Četrto poglavje bo predstavilo glavne rezultate, ki jih bomo v petem poglavju podrobneje analizirali. V zadnjem poglavju bomo na kratko povzeli bistvo in rezultate članka, ter predlagali nekaj možnih smernic za nadaljnje delo.

2 SORODNA DELA

Čeprav so gesla še vedno najbolj pogosta metoda avtentikacije [8], so bile njihove številne pomanjkljivosti [22] prvič zaznane že pred več kot štiridesetimi leti, ko sta avtorja Morris in Thompson besedilna gesla označila kot šibko točko varnosti informacijskega sistema [17]. Izvedla sta eksperiment, v katerem sta preučevala tipične navade uporabnikov pri izbiri lastnih gesel. Poročala sta, da so številni uporabniki sistema UNIX izbrali gesla, ki so bila zelo šibka: kratka, vsebovala so samo male črke ali številke, ali pa so se pojavljala v različnih slovarjih. Konec devetdesetih let prejšnjega stoletja sta avtorja Zviran in Haga prišla do podobne ugotovitve [26]. Dvajset let kasneje pa smo s pomočjo sistematičnega pregleda literature s tega področja ugotovili, da se stanje ni bistveno spremenilo, in sicer so uporabniki ter njihova gesla še vedno »Ahilova peta« varnosti informacijskih sistemov [22]. Med identificiranimi težavami so: ponovna uporaba gesel, več različnih gesel, ki si jih je treba zapomniti, šibka gesla, človeške omejitve pri pomljivosti gesel, zapisovanje gesel, ter deljenje osebnih gesel z ostalimi uporabniki sistema. Večina teh težav je tesno povezana s spominskimi omejitvami uporabnikov, ki jim onemogočajo, da bi si zapomnili več kompleksnih gesel za različne uporabniške račune [2]. Posledično so identificirane težave povzročile val raziskav na tematiko alternativnih metod avtentikacije, med katerimi so tudi grafična gesla.

Študija iz leta 2000 [5] uporablja standardno izvedbo predstavitvenega kompleta orodij *Passfaces*, ki od

udeležencev zahteva, da si zapomnijo 4 obraze in pravilno izberejo vse 4: enega v vsaki od 4 mrež z devetimi obrazi. Mreže so na zaslonu prikazane ena za drugo, vrstni red predstavitve ter obrazov v vsaki mreži pa ostaja nespremenjen. Kljub temu je vrstni red obrazov znotraj vsake mreže naključno izbran, prav tako pa nobena mreža ne vsebuje obrazov, ki se pojavijo v drugih mrežah. Avtorji so pri metodi *Passface* poročali o procentualno manj napačnih prijavah kot pri navadnih geslih. Naprednejša študija grafičnih gesel, ki temelji na prepoznavanju obrazov, je bila narejena leta 2004 [9]. Avtorji so raziskovali kako uporabniki izbirajo grafična gesla, ter ali so le-ta dovolj varna. Ugotovili so, da če uporabnike prisilimo, da si izberejo varnejša grafična gesla, s tem negativno vplivamo na njihovo pomljivost, kar nas pripelje nazaj do besedilnih gesel.

Čeprav se prav pomljivost grafičnih gesel pogosto izpostavlja kot njihova glavna prednost pred besedilnimi gesli, so obstoječe študije na to tematiko omejene in ne podajajo prepričljivih dokazov, ki bi podpirali to trditev [21]. V času nastavna prvih grafičnih gesel je bilo le-ta z uporabo tradicionalnih metod napadov (napad z grobo silo ali napad s slovarjem) težje zlomiti, so pa bila dovzetna za druge vrste napadov, kot so napadi z opazovanjem (*angl.* shoulder surfing), analiza vročih točk (*angl.* hotspot analysis), in drugi načini socialnega inženiringa (*angl.* social engineering) [21, 15]. Napad z opazovanjem je ključna pomanjkljivost grafičnih gesel, saj lahko napadalci (zlonamerni ali ne) lažje opazujejo in si zapomnijo grafične konstrukcije kot besedilne [4]. Avtorji v [24] so predlagali določene obrambne tehnike za zaščito pred takšnimi napadi, ki so se v splošnem izkazale kot delujoče, čeprav lahko njihova implementacija zmanjša uporabnost metode. Hkrati so določene grafične sheme gesel občutljive tudi na pomnilniške motnje (*angl.* memory interference), ki nastanejo, ko si morajo uporabniki zapomniti več različnih gesel za številne sisteme (kar je sicer pogost izziv tudi pri besedilnih geslih) [14].

Na splošno je uporabnost grafičnih avtentikacijskih shem vprašljiva. Raziskave kažejo na dejstvo, da sta varnost in uporabnost avtentikacijskih metod pogosto obratno sorazmerni [3]: povečanje varnosti pomeni zmanjšanje uporabnosti in obratno. To velja tudi za grafična gesla [13]. Pri doseganju želenega ravnovesja varnosti in uporabnosti nam lahko v prihodnosti pomaga umetna inteligenca, ter kombinacija različnih avtentikacijskih shem [25].

Osrednji del naše raziskave je študija, ki so jo opravili avtorji v [16]. Študija predstavlja novo avtentikacijsko metodo GCPS, v sklopu katere so znaki gesla grafično predstavljeni s premiki figuric na igralno ploščo. Čeprav to ni prva študija, ki raziskuje uporabnost grafičnih gesel, je prva, ki se osredotoča na GCPS avtentikacijske metode: igro šaha ter igro monopolija. Omenjena študija predstavlja obetavne rezultate, kljub določenim pomanjkljivostim. Nekatere so že identificirali avtorji sami (na primer, predlagani metodi nista bili primerjani z že obstoječimi besedilnimi gesli), nekatere pa so kasneje izpostavili avtorji v [6].

3 METODE RAZISKOVANJA

Ta študija, ki je raziskava v teku, raziskuje predlagano avtentikacijsko metodo GCPS iz [16] in jo primerja s klasičnimi besedilnimi gesli v sklopu klasičnega eksperimenta. Pilotno študijo smo izvedli na vzorcu študentov Fakultete za elektrotehniko, računalništvo in informatiko ter študentov Filozofske fakultete Univerze v Mariboru. Dobljeni rezultati so bili statistično obdelani ter interpretirani v diskusiji na koncu članka.

3.1 Eksperiment

Podatke za analizo smo zbrali s pomočjo eksperimentalne metode, pri čemer smo se zgledovali na eksperi- ment, ki so ga izpeljali avtorji v okviru [16]. Avtorji so izvedli dva eksperimenta. Tekom prvega eksperimenta so si udeleženci ustvarili gesla za dostop do fiktivnega uporabniškega računa. Po preteku 15 - 20 min so se ponovno prijavili v svoj račun z namenom testiranja dolgoročnega spomina. Omenjen eksperiment so avtorji nadgradili v longitudinalni študiji, v sklopu katere so v časovnem obdobju 10 tednov opazovali pomljivost in hitrost vnosa GCPS gesel. Ker nam čas in organizacija študentov nista dopuščala, da bi oba eksperimenta izvedli v polnem obsegu, smo se odločili, da se bomo osredotočili na prvi eksperiment, drugega pa smo izvedli v okrnjenem obsegu. Da bi bili rezultati našega eksperimenta primerljivi s tistimi, ki so jih producirali avtorji v [16], smo eksperiment načrtovali na podoben način. Eksperiment smo nadgradili z dodatno avtentikacijsko metodo, in sicer s klasičnimi besedilnimi gesli, kar nam je omogočilo, da smo lahko obe metodi statistično primerjali in odgovorili na zadana raziskovalna vprašanja.

Glavna cilja eksperimenta sta: ugotoviti, ali so izbrana grafična gesla na podlagi šahovnice bolj zapomljiva kot klasična besedilna gesla, ter ali je čas, potreben za prijavo pri besedilnih geslih krajši kot pri grafičnih.

3.2 Udeleženci

Prve faze eksperimenta se je skupaj udeležilo 110 študentov Univerze v Mariboru. Od tega jih je bilo 75 vpisanih na smer Informatika in tehnologija komuniciranja na Fakulteti za elektrotehniko, računalništvo in informatiko, in 35 na smer Psihologija na Filozofski fakulteti. Od skupno 110 udeležencev je bilo 68 moških in 42 žensk, pri čemer jih je bilo 90 vpisanih v prvi letnik, ter 20 v drugi letnik dodiplomskega študija. Povprečna starost udeležencev je 20,27 let (SD = 1,23). Obe fazi eksperimenta je končalo skupaj 83 udeležencev, ki smo jih upoštevali v končni analizi.

3.3 Izvedba eksperimenta

Udeleženci so dobili dostop do spletne aplikacije, kjer so bili pozvani k ustvarjanju novega uporabniškega računa. Za zaščito računa so morali ustvariti najprej navadno, besedilno geslo in nato še GCPS grafično geslo s premiki šahovskih figuric na šahovnico.

V prvi fazi je bila naloga udeležencev ustvariti besedilno geslo, za katerega so menili, da je dovolj varno, da bi ga sami uporabili kot dejansko geslo. Enako je veljalo tudi za grafična gesla. Takoj po registraciji uporabniških računov so se morali udeleženci dvakrat prijaviti v sistem: z novo ustvarjenim besedilnim in grafičnim geslom (v nadaljevanju bo ta del eksperimenta naslovljen kot »Prijava 1«). Sledil je 15 – 20 minutni odmor (kognitivni psihologi trdijo, da se informacije po največ 20 sekundah shranijo v dolgoročnem spominu), med katerim so udeleženci morali izpolniti demografski vprašalnik, ter vprašalnik o namiznih igrah in geslih. S tem smo zmanjšali verjetnost, da bi med odmorom udeleženci vadili na novo ustvarjena gesla. Po odmoru smo udeležence pozvali, da ponovno vnesejo svoje besedilno ter grafično geslo (v nadaljevanju bo ta del eksperimenta naslovljen kot »Prijava 2«). Pri tem je potrebno poudariti, da udeleženci niso bili vnaprej obveščeni o tem, da se bodo morali v sistem prijaviti večkrat. Udeležencem smo omogočili tri poskuse, da pravilno vnesejo svoje geslo, pri čemer smo za vsakega udeleženca merili reakcijski čas in število potrebnih poskusov do uspešne prijave. Reakcijski časi so bili izmerjeni v sekundah (s), in sicer od začetka tipkanja besedilnega gesla oziroma premikanja igralnih figuric, do pritiska na gumb »Prijava«.

Druga faza eksperimenta je potekala natanko dva tedna po prvi fazi. Udeleženci, ki so sodelovali v prvi fazi, so se morali ponovno prijaviti v sistem, pri čemer so morali vnesti besedilna in grafična gesla, ki so si jih ustvarili v prvi fazi eksperimenta (v nadaljevanju bo ta del eksperimenta naslovljen kot »Prijava 3«). Ponovno smo jim omogočili največ tri poskuse prijave, prav tako smo ponovno merili reakcijski čas ter število potrebnih poskusov do uspešne prijave.

3.4 Pravila pri ustvarjanju gesel

Dosedanje raziskave iz obstoječe literature kažejo, da uporabniki predvidoma izbirajo šibka gesla, ki jih je enostavno ugotoviti ali zlomiti, razen v primerih, ko je določena politika izbiranja gesel [22]. Za ta namen smo določili ustrezno politiko izbiranja gesel tako pri besedilnih kot tudi pri geslih GCPS. Pri določanju le-te smo izhajali iz politike besedilnih gesel, ki je najbolj pogosta v literaturi [11]. Za to politiko smo izračunali ustrezno teoretično entropijo oz. entropijo, kot bi jo imeli, če bi bila izbira znakov v geslu enakomerna. Ustrezno politiko gesel smo za (približno) enako entropijo sestavili tudi pri grafični metodi. Na ta način smo želeli obe metodi primerjati z vidika realnega primera, kjer je izbor gesla prepuščen uporabnikom. S tem jim olajšamo izbiro gesel in skušamo zagotoviti, da je izbrano geslo bolj podobno realnemu geslu, ki bi ga lahko uporabniki uporabili pri ustvarjanju računa na določeni spletni strani ali spletni storitvi.

3.4.1 Besedilna gesla

Ker včasih tudi določena varnostna politika ni zagotovilo, da bodo uporabniki izbrali močno geslo, smo se odločili, da zastavimo varnostno politiko izbiranja besedilnih gesel, ki ne bo prezahtevna za uporabnike. Namreč, če je politika zastavljena prestrogo, lahko deluje tudi kontraproduktivno, saj se uporabniki prej nagibajo k zamenjavi varnosti z lažjo pomljivostjo (»password« lahko postane »Password1!« kar je v osnovi enako (ne)varno). V končni fazi smo se odločili za varnostno politiko, ki vsebuje naslednja pravila:

- Geslo mora imeti vsaj 8 znakov
- Geslo mora vsebovati vsaj eno veliko črko
- Geslo mora vsebovati vsaj eno malo črko

- Geslo mora vsebovati vsaj eno številko
- Geslo mora vsebovati vsaj en poseben znak
- Geslo ne sme biti beseda iz slovarja

3.4.2 Gesla GCPS

Da bi bila izbrana grafična gesla primerljiva z besedilnimi smo morali tudi pri grafičnem načinu avtentikacije določiti politiko izbiranja gesel, ki bo primerljiva tisti iz besedilnih gesel glede na težavnost ter varnost izbranega gesla. Avtorji originalnega članka [16] so v osnovi že določili neko politiko gesel, in sicer: udeležencem je bilo dovoljeno uporabiti le dve ali štiri figurice za izdelavo gesla, posamezna lokacija na šahovnici pa je lahko bila uporabljena le enkrat. Prav tako pravilni vrstni red postavljanja figuric na šahovnici ni bil zahtevan. Te omejitve so se izkazale za premalo striktne, da bi bila ustvarjena gesla dovolj varna pred napadom z grobo silo [6]. V našem eksperimentu smo omenjena pravila nadgradili po predlogih [6]. Ustvarjena gesla GCPS morajo vsebovati:

- Vsaj 5 figuric
- Največ eno belo trdnjavo
- Največ enega belega kralja
- Največ dva bela konja
- Največ dva bela kmeta
- Največ eno vročo pozicijo
- Največ dve manj vroči poziciji

Vroče pozicije smo pridobili iz originalnega članka [16], v katerem je bila izvedena frekvenčna analiza uporabljenih figuric in pozicij na šahovnici. Vrstni red postavljanja figuric na šahovnici lahko pripomore k izbiri močnejšega in bolj varnega gesla [6], zato je bilo uporabnikom naročeno, da naj le to upoštevajo. Prav tako ni bilo nobenih omejitev glede lokacij na šahovnici, kar pomeni, da lahko uporabniki na eno lokacijo postavijo tudi več figuric.

4 REZULTATI

Preverili smo pravilnost vnesenih besedilnih in grafičnih gesel ob prvi prijavi (takoj po prvi registraciji) ter ob drugi in tretji prijavi. V tej sekciji bomo povzeli rezultate naše študije tako, da bomo statistično primerjali rezultate iz obeh faz eksperimenta. V nadaljevanju bomo predstavili še reakcijske čase, oziroma potrebne čase za prijavo v sistem. Kot je bilo že omenjeno, je obe fazi eksperimenta končalo le 83 študentov, kar smo pri obdelavi rezultatov tudi upoštevali.

4.1 Pravilnost vnesenih gesel

Tabela 1 prikazuje število potrebnih poskusov do uspešne prijave za izbrano avtentikacijsko metodo v posamezni fazi eksperimenta. Če spomnimo: »Prijava 1« predstavlja število potrebnih poskusov za prijavo v sistem takoj po ustvarjanju gesel, »Prijava 2« predstavlja število potrebnih poskusov za prijavo v sistem po 10-20 minutnem odmoru in »Prijava 3« predstavlja število potrebnih poskusov za prijavo po dveh tednih, ko je potekala druga faza eksperimenta.

Iz sekcije »Prijava 1« v Tabeli 1 je razvidno, da so se z besedilnim geslom v treh poskusih uspešno prijavili vsi razen enega udeleženca (98,8 %). 74 od 82 (90,2 %) udeležencev je pravilno geslo vneslo že pri prvem poskusu, šest (7,3 %) jih je vneslo pravilno geslo pri drugem poskusu, dva udeleženca (2,4 %) pa sta pravilno geslo uspela vnesti v tretjem poskusu.

Iz iste tabele je razvidno, da je za uspešno prijavo z geslom GCPS v povprečju potrebnih več poskusov. Le 53 od vseh 83 (63,7 %) udeležencev je uspelo vtipkati pravilno geslo v treh poskusih. Od teh 53 se je 45 (84,9 %) uspelo prijaviti v prvem poskusu, le dva udeleženca (3,8 %) sta se uspela prijaviti v dveh poskusih, šest (11,3 %) se je uspelo prijaviti v treh poskusih.

Da smo rezultate lahko primerjali z rezultati iz članka [16] smo analizirali tudi rezultate iz sekcije »Prijava 2«, v sklopu katere so se udeleženci posku-

Tabela 1: **Število prijav v posamezni fazi eksperimenta**

	Prijava 1		**Prijava 2**		**Prijava 3**	
Št. prijav	Besedilna gesla	GCPS	Besedilna gesla	GCPS	Besedilna gesla	GCPS
1	74	45	71	53	43	32
2	6	2	8	3	14	4
3	2	6	2	3	7	4
Neuspešno	1	30	2	24	19	43

šali prijaviti v svoje uporabniške račune po 10-20 minutnem odmoru, podobno kot v [16]. Opazimo lahko, da je v primerjavi s »Prijavo 1« število udeležencev, ki se jim je uspelo prijaviti v treh poskusih ali manj pri besedilnih geslih skoraj enako (81/83 oz. 97,6 %) in celo višje pri GCPS (59/83 oz. 71,1 %). Drugače povedano, 71,1 % udeležencev se je s pomočjo šahovnice uspelo uspešno prijaviti v treh poskusih ali manj, pri čemer se je kar 53 od teh 59 (89,9 %) udeležencev uspešno prijavilo že v prvem poskusu.

Za podrobnejšo analizo smo uporabili neparametrični Wilcoxonov statistični test, saj je Shapiro-Wilk test normalnosti pokazal, da vse razlike med pari naborov podatkov niso v skladu z normalno porazdelitvijo ($p < 0,05$ v vseh primerih).

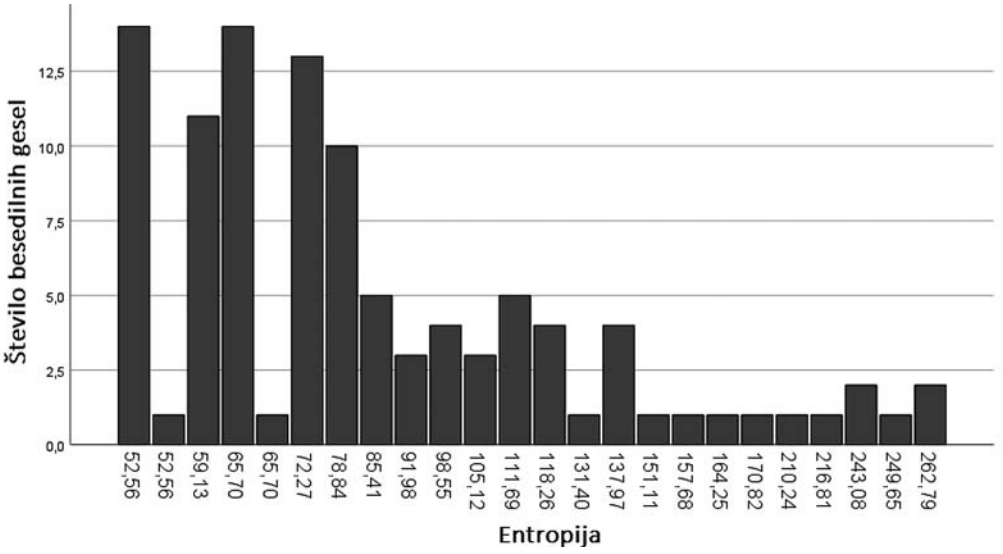
Pri besedilnih geslih Wilcoxonov neparametrični test ni pokazal statistično značilne razlike v številu potrebnih prijav med »Prijavo 1« in »Prijavo 2« ($T = 66$ pri $p = 0,38$). Pri GCPS pa je bila ta razlika signifikantna ($T = 57,5$ pri $p < 0,05$) saj se je več udeležencev uspelo prijaviti že v prvem poskusu.

Po dveh tednih pa se je število potrebnih poskusov za uspešno prijavo pri obeh avtentikacijskih metodah pričakovano povečalo, kot je razvidno iz stolpca »Prijava 3«. Iz zadnjega stolpca v Tabeli 1 je razvidno, da je 64 od vseh 83 (77,1 %) udeležencev uporabilo pravilno besedilno geslo v treh poskusih ali manj, od tega le 43 (67,2 %) v prvem, 14 (21,9 %) v drugem, ter 7 (10,9 %) v tretjem poskusu. Preostalim 19 izmed vseh 83 (22,9 %) udeležencev se ni uspelo prijaviti. Rezultati so bistveno slabši pri metodi GCPS. Le 40 izmed vseh 83 (48,2 %) udeležencev se je uspešno prijavilo v treh poskusih ali manj, od tega 32 (80 %) v prvem, 4 (10 %) v drugem, in 4 (10 %) v zadnjem poskusu. Kar 43 oziroma 51,8 % udeležencev pri prijavi v sistem z grafičnim geslom ni bilo uspešnih. Primerjava med »Prijava 2« in »Prijava 3« pa je tokrat pokazala statistično signifikantno razliko za obe metodi, tako besedilna ($T = 807,5$ pri $p < 0,05$) kot gesla GCPS ($T = 385,5$ pri $p < 0,05$).

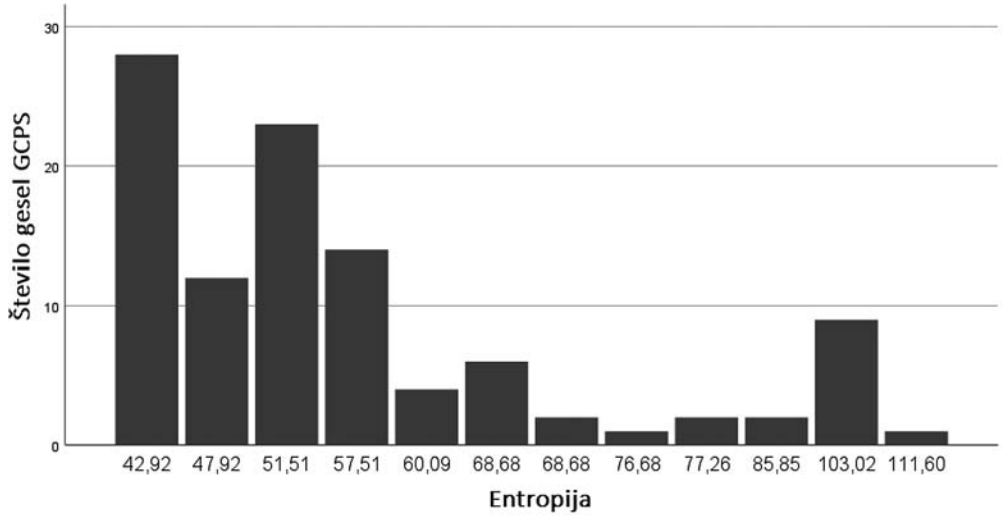
Nadaljnje primerjave obeh metod v različnih fazah so razkrile statistično signifikantne razlike med besedilnimi gesli ter gesli GCPS v vseh treh fazah eksperimenta: $T1 = 841$, $T2 = 676,5$ in $T3 = 905,5$ (pri teh statističnih testih je $p < 0,05$).

Podrobnejša analiza uspešnih prijav nam je pomagala boljše razumeti uporabnost posameznih metod. Pogledali smo, ali obstaja korelacija med številom potrebnih prijav za obe metodi v posameznih fazah eksperimenta. Uporabili smo neparametrični Spearmanov korelacijskih statistični test, saj je Shapiro-Wilk test normalnosti pokazal, da vse razlike med pari naborov podatkov niso v skladu z normalno porazdelitvijo ($p < 0,05$ v vseh primerih). Rezultati so pokazali, da korelacije med številom potrebnih prijav pri obeh metodah v fazah »Prijava 1« ($r = 0,162$, $p = 0,085$) in »Prijava 2« ($r = 0,08$, $p = 0,930$) ni. V zadnji fazi »Prijava 3« pa statistična korelacija ($r = 0,207$, $p < 0,05$) med številom potrebnih prijav pri obeh metodah obstaja.

Da bi dobili boljši vpogled v ustvarjena gesla, smo poleg števila uspešnih prijav in reakcijski čas za do-



Slika 2: **Graf entropije za ustrezno število besedilnih gesel.**



Slika 3: **Graf entropije za ustrezno število gesel GCPS.**

ločeno metodo izračunali tudi entropijo ustvarjenih gesel pri registraciji. Entropija je pomembna, saj nam pove kako nepredvidljivo in neuganljivo je geslo. Dejansko predstavlja verjetnost naključja (kako verjetno je, da bo napadalec izbral prav to geslo) [18]. Čeprav obstajajo boljši načini izračuna moči oz. verjetnosti določenega gesla [23], smo se za potrebe tega eksperimenta odločili za entropijo, saj cilj tega eksperimenta ni analiza moči gesel. Slika 2 in slika 3 prikazujeta grafa entropije za posamezne metode v času registracije (ustvarjanja gesel).

Wilcoxonov neparametrični test je pokazal, da so udeleženci ustvarjali besedilna gesla s signifikantno višjo entropijo (Mdn = 72,3) kot pa gesla GCPS (Mdn = 51,5), T=415, p<0,05.

4.2 Reakcijski čas

Tabela 2 prikazuje potrebne čase za uspešno prijavo za posamezno avtentikacijsko metodo v posamezni fazi eksperimenta. Podobno kot pri Tabeli 1 »Prijava 1« predstavlja čas, potreben za uspešno prijavo v sistem takoj po ustvarjanju gesel, »Prijava 2« predstavlja čas, potreben za uspešno prijavo v sistem po 10-20 minutnem odmoru in »Prijava 3« predstavlja čas, potreben za uspešno prijavo po dveh tednih, ko je potekala druga faza eksperimenta.

Iz zgornje tabele je razvidno, da je povprečni reakcijski čas za besedilna gesla malo daljši v fazi »Prijava 1« (M = 12,98, SD = 19,61) kot pa v fazi »Prijava 2« (M = 11,25, SD = 9,35). Ponovno smo uporabili neparametrični Wilcoxonov statistični test (Shapiro-Wilk test normalnosti je pokazal, da vse razlike med pari naborov podatkov niso v skladu z normalno porazdelitvijo, $p < 0,05$ v vseh primerih), ki ni pokazal statističnih razlik ($T = 1720$ in $p = 0,917$). Pri GCPS smo opazili signifikantno daljši čas v fazi »Prijava 1« (M = 28,49, SD = 16,52) kot pa v fazi »Prijava 2« (M = 20,09, SD = 10,24) ($T = 667$ in $p < 0,05$). Podobno kot pri pravilnosti vnesenih gesel sklepamo, da so udeleženci na začetku potrebovali malo več časa, da se navadijo na svoje geslo.

Tabela 2: **Reakcijski časi (v sekundah) po posameznih fazah**

		Minimum	Maksimum	Povprečje	Std. odklon
Prijava 1	Besedilna gesla	3,70	178,23	12,98	19,61
	GCPS gesla	7,94	86,19	28,49	16,52
Prijava 2	Besedilna gesla	3,83	65,69	11,25	9,35
	GCPS gesla	4,31	58,66	20,09	10,24
Prijava 3	Besedilna gesla	3,79	47,37	13,33	8,72
	GCPS gesla	3,60	77,02	23,1	11,89

V fazi »Prijava 3« se je reakcijski čas povečal tako pri besedilnih (M = 13,33, SD = 8,72) kot tudi pri geslih GCPS (M = 23,1, SD = 11,89). Pri obeh metodah je bila razlika reakcijskega časa med fazami »Prijava 2« in »Prijava 3« signifikantna ($p < 0,05$), in sicer za besedilna gesla je bil T = 2463, za GCPS gesla pa T = 2247.

Očitna razlika med povprečnima časoma, potrebnima za prijavo z geslom GCPS in besedilnim geslom v vseh fazah eksperimenta je bila tudi statistično utemeljena. Rezultati Wilcoxonovih neparametričnih testov so: T1 = 3251, T2 = 3181 in T3 = 3179 za posamezno fazo (pri vseh statističnih testih je $p < 0,05$).

5 RAZPRAVA

Avtorji v [16] poročajo o 77 % skupnem povprečju uspešnih vnosov gesel v treh poskusih. Čeprav bi avtentikacijski sistem v realnem okolju moral zagotavljati višjo pomljivost, so nižje vrednosti pričakovane, saj gre za popolnoma nov sistem, prav tako pa so udeleženci ustvarjali nova gesla ter pred tem niso bili opozorjeni, da si je potrebno novo-ustvarjena gesla zapomniti. V našem eksperimentu je bilo skupno povprečje že tekom registracije še nižje, in sicer 63,7 %, kar pomeni, da so udeleženci potrebovali razmeroma še več poskusov za vnos pravilnega gesla. Pri tem moramo izpostaviti, da je takšno povprečje še vedno obetavno, če upoštevamo dejstvo, da smo v našem eksperimentu implementirali dodatne omejitve. Varnostne politike, ki smo jih določili v sklopu ustvarjanja novih GCPS gesel so ustrezale priporočenim politikam, namenjenim besedilnim geslom. Takšne zahteve v realnosti prinašajo dodatno breme pri ustvarjanju (in kasnejšem pomnjenju) gesla. Namreč, če varnostne politike niso dovolj stroge, si uporabniki lahko ustvarijo tekstovna in grafična gesla, ki ne dosegajo zahtevanega nivoja varnosti.

Za primerjavo, tekstovna gesla so v sklopu prve prijave dosegla kar 98,8 % skupno povprečje uspešnih vnosov. Čeprav se je ta odstotek tekom kasnejših prijav po pričakovanjih zmanjševal, so udeleženci po dveh tednih še vedno dosegali višje skupno povprečje uspešnih vnosov (77,1 %), kot z metodo GCPS takoj po registraciji (63,7 %). Statistična primerjava med obema metodama je pokazala, da je bila razlika v pravilnosti vnosa signifikantna tekom vseh treh prijav.

Analiza reakcijskih časov je razkrila podobne rezultate. Tekom registracije so udeleženci za uspešno prijavo z besedilnim geslom potrebovali v povprečju 15 sekund manj kot z geslom GCPS. Čeprav se je ta razlika v drugi in tretji prijavi zmanjšala za okoli 5 sekund, razlike v reakcijskem času med metodama ostajajo signifikantne. Rezultati nakazujejo, da je potreben kompromis med varnostjo in uporabnostjo večji pri geslih GCPS kot pri besedilnih geslih.

Kot zanimivost lahko izpostavimo še, da je število uspešnih prijav z metodo GCPS v fazi »Prijava 2« manjše kot pa pri »Prijava 1«. Najverjetnejša razlaga predvideva, da so rezultati takšni, ker gre za novo avtentikacijsko metodo, ki ima še dodatne omejitve in bolj strogo varnostno politiko, kot je bila zahtevana v [16]. To lahko dodatno obremeni kognitivni spomin, kar lahko vpliva na čas, ki ga udeleženci potrebujejo, da se navadijo na novo avtentikacijsko metodo, ter novo-ustvarjena gesla. Na večje število napak v »Prijavi 1« je tako najvernetneje vplivalo prav nepoznavanje nove metode.

5.1 Pomljivost izbranih gesel

Odgovor na prvo raziskovalno vprašanje: »Ali so izbrana grafična gesla bolj zapomljiva kot klasična besedilna gesla?« lahko najdemo v podpoglavju 4.1, kjer so statistični testi v vseh fazah eksperimenta pokazali statistične razlike med besedilnimi gesli ter gesli GCPS. V fazi »Prijava 3« je število udeležencev, ki so se v treh poskusih uspešno prijavili z besedilnimi gesli 77,1 %, z gesli GCPS pa le 48,2 %. V splošnem so takšni rezultati podobni rezultatom nekaterih predhodnih študij [13]: grafična gesla so v osnovi manj uporabna kot besedilna, če pa povečamo zahteve po varnih grafičnih geslih, postanejo še manj uporabna. Kako težko je sestaviti geslo GCPS prikazuje tudi izračunana entropija za gesla, ki so si jih udeleženci izbrali ob prvi registraciji v sistem. Rezultati kažejo na to, da so izbrana gesla GCPS manj varna kot pa navadna besedilna gesla, kar je glede na zgoraj povedano tudi pričakovano.

Korelacijska analiza pa je pokazala, da zmožnost pomnjenja besedilnih gesel ne vpliva na zmožnost pomnjenja grafičnih gesel, in obratno. Drugače povedano, če si uporabniki lažje (oz. težje) zapomnijo besedilna gesla, to ne pomeni, da si bodo lažje (oz. težje) zapomnili tudi gesla GCPS. Čeprav lahko iz tabele 1 razberemo, da si uporabniki besedilna gesla v splošnem zapomnijo lažje kot grafična, rezultati korelacijske analize nakazujejo na dejstvo, da je zmožnost pomnenja besedilnih konstruktov neodvisna od zmožnosti pomnjenja grafičnih konstruktov. Pozitivna korelacija, ki smo jo opazili v fazi »Prijava 3«,

je nastala zaradi dvo-tedenskega premora pri obeh metodah; tabela 1 prikazuje, da je v zadnji fazi pomljivost obeh tipov gesel znižana zaradi postopnega propada spomina (t.j. pozabljanje).

Zavedamo se, da je ekološka veljavnost rezultatov omejena, saj študija ne predstavlja realnega primera, v sklopu katerega bi uporabniki vsakodnevno uporabljali svoja gesla. Pričakovano je, da pomljivost postopoma upada s časom, na kar lahko negativno vpliva tudi pogostost vnašanja gesel. Zato so avtorji v [16] izvedli še dodaten eksperiment, v katerem so preučevali pomljivost gesel GCPS v daljšem časovnem obdobju (10 tednov). Izveden eksperiment v tem članku predstavlja osnovo za nadaljnje raziskave na tem področju.

5.2 Reakcijski čas

Odgovor na drugo raziskovalno vprašanje: »Ali je čas, potreben za uspešno prijavo, nižji pri grafičnih kot pri besedilnih geslih?« lahko najdemo v podpoglavju 4.2, kjer so statistični testi pokazali statistično signifikantne razlike med povprečnimi časi, potrebnimi za vnašanje izbranega gesla v vseh fazah. Tudi na tem področju so bila besedilna gesla boljša s povprečnim časom 11,25 sekund v fazi »Prijava 2« v primerjavi s povprečnim časom 20,09 sekund za gesla GCPS.

Rezultati presenetljivo kažejo na dejstvo, da je povprečni čas vnosa GCPS gesla v fazah »Prijava 2« in »Prijava 3« hitrejši kot pa v originalnem članku [16], kar bi lahko nakazovalo na to, da se udeleženci relativno hitro navadijo na tovrstna gesla, ter postopek njihovega vnašanja. S to trditvijo se skladajo tudi rezultati drugega eksperimenta v sklopu študije [16], ki so pokazali, da je bil povprečni reakcijski čas za gesla GCPS približno 11 sekund.

5.3 Omejitve

5.3.1 Vzorec

Vzorec, ki smo ga imeli možnost izbrati za to raziskavo, ter podatki, ki smo jih pridobili in so navedeni v tem članku, morda niso popolnoma reprezentativni, ter ne predstavljajo splošne populacije. Nadalje, primerjavo med dvema metodama avtentikacije (besedilna gesla in GCPS) je potrebno izvesti na bistveno večjem in bolj raznolikem vzorcu (npr. primerjave je možno izvajati med različnimi starostnimi skupinami, študijskimi smermi, študenti z različnimi nivoji informacijske pismenosti, itn.).

5.3.2 Ekološka veljavnost eksperimenta

Gesla, ki so si jih uporabniki izbirali tekom eksperimenta, ne predstavljajo dejanskih gesel, ki bi ščitila realne uporabniške račune, temveč so bila ustvarjena izključno za namen te raziskave. To je sicer pogosta omejitev pri eksperimentih, ki se ukvarjajo z avtentikacijskimi metodami.

V sklopu tovrstnih študij gesel so pomembna vprašanja vezana tudi na ekološko veljavnost. Pri tem nas posebej zanima, ali je izsledke raziskovalne študije mogoče posplošiti iz opazovanega vedenja v laboratoriju na okolja v resničnem življenju [19], oziroma, ali se udeleženci študije obnašajo tako, kot bi se sicer obnašali uporabniki v resničnem življenju. Ekološka veljavnost je v študijah uporabnikov zelo pomembna, saj lahko že same informacije, ki jih uporabnikom podamo v začetni fazi eksperimenta, vplivajo na njihovo vedenje tekom študije. Avtorji v [12] so raziskali vpliv, ki ga zasnove uporabniških študij dejansko imajo na ekološko veljavnost izvedenih eksperimentov. Prišli so do zaključka, da so udeleženci pristranski in da se njihovo vedenje lahko spremeni že samo zaradi seznanjenosti z dejstvom, da sodelujejo v študiji gesel.

Izrazi »eksperiment«, »realistična zasnova« in »resnični podatki« so tesno povezani s kontekstom ekološke veljavnosti. V našem primeru lahko izraz »eksperiment« opredelimo kot laboratorijsko študijo, kjer uporabniki niso v njihovem naravnem okolju, izraz »realistična zasnova« lahko definiramo kot okolje, v katerem se uporabniki ne zavedajo, da jih preučujemo (npr. doma, v službi itd.), izraz »resnični podatki« pa bi lahko predstavljal gesla iz resničnega sveta, ki jih uporabniki uporabljajo v vsakdanjem življenju.

5.3.3 Implementacija grafičnega vmesnika

Pri implementaciji grafične metode avtentikacije, ki temelji na igrifikaciji, smo uporabili enak grafični vmesnik, kot je opisan v izvirnem članku [16], v katerem je bila ta metoda predstavljena. Moramo se zavedati, da kakršnekoli spremembe v implementaciji lahko vplivajo na končne rezultate primerjave, saj uvajanje drastičnih sprememb spreminja dejansko zasnovo grafične metode. Upoštevali smo nekaj nasvetov, ki so jih podali avtorji v [6], saj le-ti predstavljajo zgolj varnostno izboljšavo metode in omogočajo ustvarjanje močnejšega gesla, ne spreminjajo pa izgleda in delovanja same metode. En primer takšne

izboljšave je vrstni red postavljanja figuric na šahovnici, kar avtorji originalne metode niso upoštevali, čeprav vemo, da je vrstni red znakov v besedilnem geslu zelo pomemben, saj je od tega odvisno kako močno bo končno geslo [23]. Zavedamo se, da bi ob drugačnem načinu implementacije grafičnega vmesnika lahko dobili drugačne rezultate, kar je tematika naših nadaljnjih raziskav.

6 ZAKLJUČEK

V tem članku so predstavljeni rezultati raziskave, v kateri smo primerjali navadna besedilna gesla z grafičnimi gesli GCPS, ki so bila predstavljena v [16]. Glavna cilja raziskave sta bila ugotoviti ali so gesla GCPS bolj zapomljiva kot klasična besedilna gesla, ter ali je čas, potreben za prijavo v sistem krajši pri besedilnih geslih, kot pri geslih GCPS.

Pokazali smo, da so besedilna gesla boljša od grafičnih tako glede pomljivosti kot tudi hitrosti vnašanja. Takšni rezultati upravičujejo tudi njihovo razširjenost in vseprisotnost kot najbolj pogosto uporabljen način avtentikacije. GCPS je v obeh eksperimentih konsistentno dosegal slabše rezultate. Kljub temu, da je GCPS bolj kompleksen kot besedilna gesla, pa rezultati kažejo, da se uporabniki hitro naučijo kako sistem uporabljati. Ob tem je povprečni reakcijski čas še vedno hitrejši kot pa pri nekaterih grafičnih metodah avtentikacije [25]. K temu zaključku se nagibajo tudi avtorji v [16] saj je bil povprečni reakcijski čas v drugem eksperimentu celo 11 sekund, kar je skoraj dvakrat hitreje kot pri GCPS shemi, ki smo jo testirali v našem eksperimentu.

V tej raziskavi smo uporabili nadgrajeno GCPS shemo, ki je uvedla varnostne politike za doseganje ustre- znega nivoja varnosti glede na obstoječa priporočila [6]. S tem smo se želeli približati povprečni varnosti politiki, ki je implementirana v okviru besedilnih gesel. Posledično so bili rezultati nekoliko slabši kot pri [16], saj se je število udeležencev, ki so se uspešno prijavili v treh poskusih zmanjšalo. Določanje uravnoteženih varnostnih politik pri GCPS načinu avtentikacije (ter tudi na splošno pri grafičnih geslih) je zahtevno. Z dodatnimi raziskavami bi za gesla, ki temeljijo na namiznih igrah, lahko določili dobro ravnovesje med pomljivostjo in njihovo odpornostjo na surovo silo in napade s slovarjem. Nekateri predlogi so bili podani v [16] in [6], ki so predlagali, da bi od uporabnikov zahtevali, da naj uporablja več kombinacij, več figuric, lokacij, barv in potez. Vpliv tovrstnih varnostnih politik na pomljivost in uporabnost grafičnih gesel ostaja predmet nadaljnjih empiričnih raziskav.

Predstavljeni rezultati v tej raziskavi so preliminarni. V nadaljnjih raziskavah se bomo osredotočili predvsem na vpliv različnih eksperimentalnih skupin na pomljivost in čase vnosov izbranih gesel GCPS, ter na njihovo pomljivost v daljšem časovnem obdobju.

LITERATURA

[1] NIST special publication 800-63B. https://pages.nist.gov/800-63-3/sp800-63b.html. Accessed: 2022-7-10.

[2] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[3] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567, 2012.

[4] Leon Bosnjak and Bostjan Brumen. Shoulder surfing: From an experimental study to a comparative framework. *CoRR,* abs/1902.02501, 2019.

[5] Sacha Brostoff and M Angela Sasse. Are passfaces more usable than passwords? a field trial investigation. *People and Computers*, pages 1–20, 2000.

[6] Boštjan Brumen. Security analysis of game changer password system. *Int. J. Hum. Comput. Stud.*, 126:44–52, 2019.

[7] Boštjan Brumen and Viktor Taneski. Moore's curse on textual passwords. In *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1360–1365, 2015.

[8] Sadie Creese, Duncan Hodges, Sue Jamison-Powell, and Monica Whitty. Relationships between password choices, perceptions of risk and security expertise. In Louis Marinos and Ioannis Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, volume 8030 of *Lecture Notes in Computer Science*, pages 80–89. Springer Berlin Heidelberg, 2013.

[9] Darren Davis, Fabian Monrose, and Michael K Reiter. On user choice in graphical password schemes. *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13, page 11, 2004.*

[10] Dennis J Delprato. Mind and its evolution: A dual coding theoretical approach. *The Psychological Record*, 59:295–300, 2009.

[11] Roberto Dillon, Shailey Chawla, Dayana Hristova, Barbara Göbl, and Suzana Jovicic. Password policies vs. usability: When do users go »bananas«? In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 148–153, 2020.

[12] Sascha Fahl, Marian Harbach, Yasemin Acar, and Matthew Smith. On the ecological validity of a password study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 13:1–13:13. ACM, 2013.

[13] Haichang Gao, Wei Jia, Fei Ye, and Licheng Ma. A survey on the use of graphical passwords in security. *Journal of Software, 8(7), 2013.*

[14] Haichang Gao, Licheng Ma, Wei Jia, and Fei Ye. Multiple password interference in graphical passwords. *International Journal of Information and Computer Security, 5(1):11–27, 2012.*

[15] Wei Hu, Xiaoping Wu, and Guoheng Wei. The security analysis of graphical passwords. In *2010 International Conference on Communications and Intelligence Information Security*, pages 200–203, 2010.
[16] Conor Mclennan, Philip Manning, and Samantha E. Tuft. An evaluation of the game changer password system: A new approach to password security. *Int. J. Hum. Comput. Stud.*, 100:1–17, 2017.
[17] Robert Morris and Ken Thompson. Password security: A case history. *Commun. ACM*, 22(11):594–597, nov 1979.
[18] Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM Conference on Computer and Communications Security*, CCS '05, pages 364–372. ACM, 2005.
[19] Mark A. Schmuckler. What is ecological validity? a dimensional analysis. *Infancy*, 2(4):419–436, 2001.
[20] Roger N Shepard. Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning and Verbal Behavior*, 6:156–163, 1967.
[21] Xiaoyuan Suo, Ying Zhu, and G.S. Owen. Graphical passwords: a survey. In *21st Annual Computer Security Applications Conference (ACSAC'05)*, pages 10 pp.–472, 2005.
[22] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. Systematic overview of password security problems. *Acta Polytechnica Hungarica*, 16(3):143–165, 2019.
[23] Viktor Taneski, Marko Kompara, Marjan Heričko, and Boštjan Brumen. Strength analysis of real-life passwords using markov models. *Applied Sciences*, 11(20), 2021.
[24] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. Shoulder surfing defence for recall- based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, New York, NY, USA, 2011. Association for Computing Machinery.
[25] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as graphical passwords—a new security primitive based on hard ai problems. *IEEE Transactions on Information Forensics and Security*, 9(6):891–904, 2014.
[26] Moshe Zviran and William J. Haga. Password security: An empirical study. *J. Manage. Inf. Syst.*, 15(4):161–185, mar 1999.

▪

Leon Bošnjak je zaposlen kot asistent za področje informatike na Fakulteti za eletrotehniko, računalništvo in informatiko na Univerzi v Mariboru. Leta 2014 je magistriral iz informatike in tehnologij komuniciranja. Leta 2022 pa je uspešno končal doktorski program Računalništvo in informatika. V okviru raziskav se ukvarja z informacijsko varnostjo, bolj specifično z tekstovnimi in grafičnimi gesli, ter drugimi metodami overjanja.

▪

Viktor Taneski je asistent na Fakulteti za elektrotehniko, računalništvo in informatiko na Univerzi v Mariboru. Doktoriral je leta 2019 iz tematike Markovih modelov ter vpliv podatkovnih zbirk za usposabljanje Markovih modelov na dokončno ocenjevanje moči gesel. Njegovo raziskovalno delo je povezano z varnostjo informacijskih sistemov, varnostjo gesel ter s človeškimi vidiki in navadami, povezanimi z ustvarjanjem in uporabo gesel.

Nadaljevalno učenje s superpozicijo v transformerjih

Marko Zeman, Jana Faganeli Pucer, Igor Kononenko, Zoran Bosnić
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, Ljubljana, Slovenija
{marko.zeman, jana.faganeli, igor.kononenko, zoran.bosnic}@fri.uni-lj.si

Izvleček

V mnogih aplikacijah strojnega učenja se novi podatki nenehno zbirajo, npr. v zdravstvenem varstvu, za vremenske napovedi itd. Raziskovalci si pogosto želijo sistem, ki bi omogočal nadaljevalno učenje novih informacij. To je izjemnega pomeni tudi v primeru, ko vseh podatkov ni mogoče shranjevati v nedogled. Največji izziv pri nadaljevalnem strojnem učenju je težnja nevronskih modelov, da po določenem času pozabijo prej naučene informacije. Da bi zmanjšali pozabljanje modela, naša metoda nadaljevalnega učenja uporablja superpozicijo z binarnimi konteksti, ki zavzemajo zanemarljiv dodaten pomnilnik. Osredotočamo se na nevronske mreže v obliki transformerjev, pri čemer smo naš pristop primerjali z več vidnimi metodami nadaljevalnega učenja na nizu klasifikacijskih nalog obdelave naravnega jezika. V povprečju smo dosegli najboljše rezultate: 4,6% izboljšavo pri ploščini pod krivuljo ROC (angl. AUROC - area under the receiver operating characteristic) in 3,0% izboljšavo pri ploščini pod krivuljo PRC (angl. AUPRC - area under the precision-recall curve).

Ključne besede: globoko učenje, nadaljevalno učenje, strojno učenje, superpozicija, transformer, klasifikacija besedil

Continual learning with superposition in transformers

Abstract

In many machine learning applications, new data is continuously collected, e.g., in healthcare, for weather forecasting etc. Researchers often want a system that allows for continuous learning of new information. This is extremely important even in the case when not all data can be stored indefinitely. The biggest challenge in continual machine learning is the tendency of neural models to forget previously learned information after a certain time. To reduce model forgetting, our continual learning method uses superposition with binary contexts, which require negligible additional memory. We focus on transformer-based neural networks, comparing our approach with several prominent continual learning methods on a set of natural language processing classification tasks. On average, we achieved the best results: 4.6% and 3.0% boost in AUROC (area under the receiver operating characteristic) and AUPRC (area under the precision-recall curve), respectively.

Keywords: deep learning, continual learning, machine learning, superposition, transformer, text classification

1 UVOD

Ljudje imamo naravno sposobnost nenehnega pridobivanja in razvijanja znanja ter veščin. Ta sposobnost, imenovana nadaljevalno ali vseživljenjsko učenje, je mogoča zaradi našega dolgoročnega spomina in enostavnega prenosa znanja med podobnimi nalogami. Vendar pa nadaljevalno učenje še vedno predstavlja velik izziv pri strojnem učenju. Trenutno najbolj priljubljeni modeli strojnega učenja so globoke nevronske mreže, ki pogosto trpijo zaradi obsežnega pozabljanja modela [1, 7]. To pomeni, da modeli ponavadi pozabljajo predhodno naučene informacije in si zapomnijo le nedavno opazovane vzorce [10]. V naši problemski domeni novi podatki postanejo na voljo v obliki novih nalog, in sicer na zaporedni način.

Da bi se soočili z omenjenimi izzivi, raziskovalci poskušajo najti načine za ublažitev pozabljanja modelov in prilagoditev modela za novo nalogo tako pomnilniško kot hitrostno učinkovito.

Najenostavnejša rešitev je naučiti različne naloge v ločenih globokih nevronskih mrežah [8]. Vendar pa je v tem primeru glavna težava velika poraba

pomnilnika, saj se število globokih nevronskih mrež povečuje linearno s številom nalog.

Številni obstoječi pristopi zahtevajo veliko pomnilnika ali arhitekturne spremembe, ki jih je pogosto težko izvesti. Eden najpreprostejših in najbolj pomnilniško učinkovitih pristopov uporablja superpozicijo, ki omogoči učenje več nalog v eni nevronski mreži z omejenim pozabljanjem in majhno porabo pomnilnika na nalogo [2]. Superpozicija se je že izkazala za koristen pristop v polno povezanih in konvolucijskih nevronskih mrežah v domeni računalniškega vida [2, 12].

Predlagamo novo rešitev, kjer uporabljamo superpozicijo v transformerjih [11], ki dosegajo najboljše rezultate na področju obdelave naravnega jezika (ONJ). V strojnem učenju transformer predstavlja specifično obliko nevronske mreže, ki poskuša razumeti povezave med zaporednimi entitetami, npr. besedami v stavkih. Transformerji s pomočjo mehanizmov pozornosti odkrivajo, kako oddaljeni elementi v nekem zaporedju vplivajo drug na drugega [11]. Pri transformerjih pridobimo na zmogljivosti ob ohranjanju pozitivnih učinkov superpozicije v polno povezanih mrežah.

2 SORODNA DELA

Ponavljalne metode temeljijo na shranjevanju dela učnih primerov iz prejšnjih nalog, ki se nato med učenjem modela ponovno uporabijo. Lopez-Paz in Ranzato [4] sta razvila pristop *Gradient Episodic Memory* (GEM). Ta zmanjša pozabljanje, saj omogoča koristen prenos znanja iz prejšnje naloge z malo dodatnega pomnilnika in preprečuje, da bi vrednost funkcije izgube iz preteklih nalog naraščala. Ker se učni primeri hranijo za vsako nalogo in se občasno ponavljajo, se računske in pomnilniške zahteve povečujejo sorazmerno s številom naučenih nalog.

Arhitekturne metode zmanjšujejo pozabljanje z uporabo sprememb v arhitekturi mreže in uvedbo parametrov, specifičnih za nalogo. Običajno večji del mreže ostane fiksiran, manjši del pa se prilagodi na novo nalogo [6, 14].

Regularizacijske metode se zanašajo na en sam model in manjšajo pozabo z uvedbo omejitev za posodobitev uteži nevronske mreže. Kirkpatrick in sod. [3] so predlagali metodo EWC (*angl.* Elastic Weight Consolidation), ki kaznuje razliko med starimi in novimi parametri naloge. Natančneje, EWC zmanjša pozabljanje z uravnavanjem funkcije izgube, kar upočasni spreminjanje parametrov, pomembnih za predhodne naloge. Poleg tega so Schwarz in sod. [9] predlagali spremembo, imenovano sprotni EWC (*angl.* Online EWC), ki ne presega linearne rasti računskih zahtev. Poleg tega so Zenke in sod. [13] predlagali ublažitev pozabljanja tako, da posameznim sinapsam (tj. parametrom) omogočijo, da ocenijo svojo pomembnost. Podobno kot [3], ta pristop kaznuje spremembe najpomembnejših sinaps, tako da se lahko nove naloge naučijo z minimalnim pozabljanjem starih.

Superpozicija [2] je drugačna oblika metod za nadaljevalno učenje, ki jo podrobneje predstavljamo v razdelku 3.

3 SUPERPOZICIJA

Pri globokem učenju superpozicijski pristop omogoča učenje več nalog v eni sami nevronski mreži z minimalnim prepletanjem med nalogami. Glavni navdih prihaja iz dela Cheunga in sod. (PSP, [2]), kjer avtorji predstavljajo način za izkoriščanje odvečnih parametrov, da se naučijo več nalog v eni mreži, hkrati pa zmanjšajo pozabljanje modela.

Splošna ideja metode superpozicije je, da se N različnih nalog uči zaporedoma z uporabo algoritma vzratnega razširjenja napake v eni sami mreži z L nivoji. Matrike uteži (parametrov, ki jih je mogoče naučiti) so označene z W_1, W_2, . . . , W_{L-1} in se spreminjajo skozi učenje vseh nalog. Za omogočanje uporabe superpozicijie uporabljamo strukturo, imenovano *kontekst*, ki je predstavljena z množico binarnih vektorjev. Kontekst se najprej uporabi med učenjem nalog in se kasneje uporabi za obnovitev ustreznih uteži mreže za specifično nalogo.

Konteksti: V polno povezanih nevronskih mrežah so konteksti predstavljeni v obliki kontekstnih matrik, ki so kvadratne in diagonalne. Omenjene kontekstne matrike služijo za prehod med nalogami, in sicer se množijo z matrikami uteži. Matrike uteži se nenehno spreminjajo glede na fiksne kontekstne matrike. Konteksti delujejo le kot ključ za odklepanje predhodno naučenih nalog in se med učenjem ne spreminjajo. Vse kontekstne matrike vključujejo na diagonali samo elemente, ki so naključno izbrani med {−1, 1} (kot je predlagano v [2]), ostali elementi pa so enaki 0.

Učenje: Posamezno nalogo učimo, dokler ni dosežena želena točnost na validacijski množici po-

datkov. Nato se matrike uteži posodobijo z uporabo kontekstov. Preko vseh nivojev mreže izvedemo množenje matrik uteži s kontekstnimi matrikami. Ta postopek posodobitve uteži se ponovi za vsako novo nalogo z ustreznim naborom kontekstnih matrik.

Testiranje: Ko model naučimo vseh N nalog, lahko pridobimo ustrezne uteži modela za določeno nalogo z rahlo izgubo predhodnega znanja. Tudi tokrat je posodobitev uteži potrebno izvesti nad vsemi matrikami uteži. Na primer, če želimo ekstrahirati primerne uteži za tretjo nalogo, moramo trenutne uteži pomnožiti z inverznimi kontekstnimi matrikami od predzadnje naloge (po zadnji nalogi ne množimo s konteksti) do tretje naloge. Konteksti za prvo in drugo nalogo v tem primeru niso pomembni. Uporaba takega načina množenja zagotavlja pridobitev mrežnih uteži, ki so primerne za določeno nalogo, ob tem pa rahlo izgubimo na zmogljivosti modela.

3.1 Superpozicija v transformerjih

V transformerjih je naš kontekst v obliki kontekstnih vektorjev, ki so označeni s $C_1, C_2, \ldots, C_{L-1}$. Število kontekstnih vektorjev je enako številu matrik uteži za posamezno nalogo. Vendar ima vsaka naloga, razen zadnje, svoj nabor $L - 1$ kontekstov, kar pomeni, da imamo skupaj $(N - 1)$ $(L - 1)$ kontekstnih vektorjev. Konteksti se uporabljajo za transformacijo matrik uteži W_i. Pred uporabo med nalogami se kontekstni vektor predhodno pretvori v kontekstno matriko, kjer se vrednosti iz vektorja kopirajo v kontekstne matrike.

Razlikujemo dve vrsti matrik: (1) *polne* kontekstne matrike in (2) *redke* kontekstne matrike. Polne matrike vsebujejo le elemente iz množice {−1, 1} in so enake velikosti kot pripadajoče matrike uteži. V primeru polnih matrik izvajamo množenje po elementih. Redke matrike pa so predstavljene le z diagonalnimi binarnimi elementi iz {−1, 1}, medtem ko so ostali elementi 0. V tem primeru je pogoj, da so matrike kvadratne in diagonalne, z matrikami uteži pa jih matrično množimo. Ko se kontekstne matrike pomnožijo z matrikami uteži, se dimenzije slednjih v nobenem primeru ne spremenijo. Zaradi želje po pomnilniško učinkoviti metodi uporabljamo polne kontekstne matrike le v primeru majhnih pripadajočih matrik uteži, redke kontekstne matrike pa uporabimo za večje pripadajoče matrike uteži.

V polno povezanih mrežah kontekstne matrike uporabljamo tudi v prvem nivoju mreže, kar povzroči, da indirektno vplivajo tudi na vhodne podatke. Nasprotno pa v transformerjih apliciramo kontekste šele v mehanizmu pozornosti, kjer ne vplivamo na vhodne podatke.

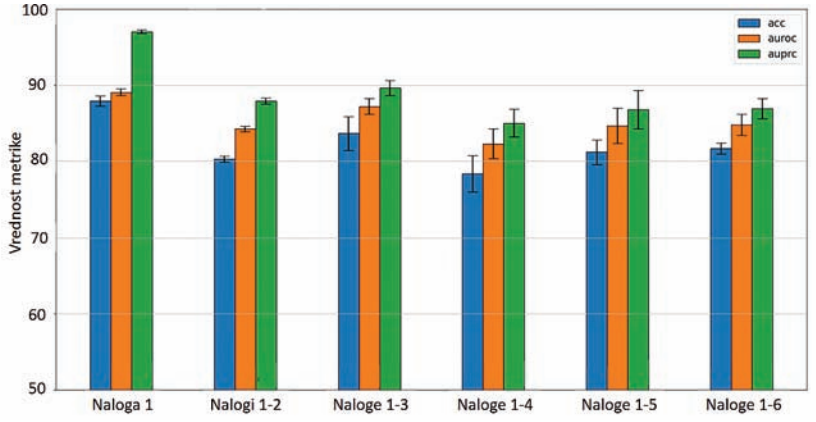
4 REZULTATI

4.1 Način vrednotenja

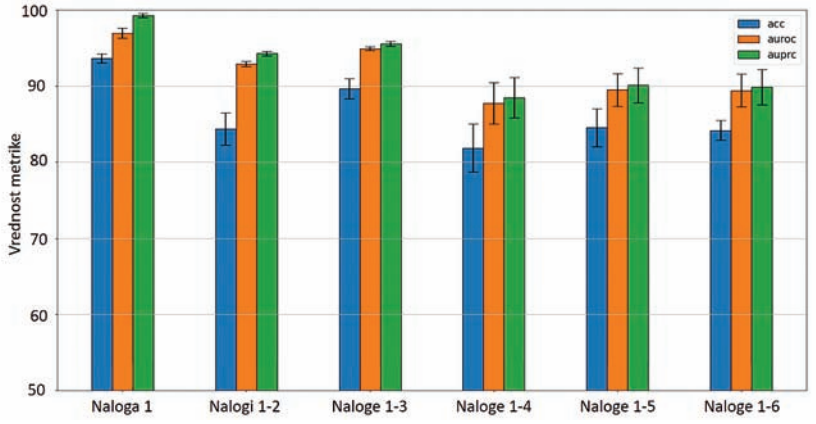
Naš pristop ocenjujemo z učenjem šestih nalog s področja obdelave naravnega jezika. Pri vseh nalogah gre za binarno klasifikacijo, in sicer zaznavanje sovražnega govora, analiza razpoloženja pri IMDb (angl. Internet Movie Database) komentarjih, zaznavanje neželenih sporočil, analiza komentarjev na platformah Amazon in Yelp, zaznavanje vab za klike in zaznavanje humorja. Vseh šest nalog ima podatke v obliki tekstovnih primerov, kjer ima posamezen primer na vhodu zaporedje besed ali stavkov, na izhodu pa binarno labelo (v primeru sovražnega govora labela pove, ali gre za sovražni govor ali ne). Tekstovni primeri so predprocesirani z algoritmom *Word2Vec* [5], ki posamezne besede spremeni v številske vektorje velikosti 32. Uspešnost merimo pri vseh naučenih nalogah. Vrstni red nalog je izbran naključno in je enak pri vseh metodah. Pri eksperimentih merimo točnost, AUROC (ploščino pod krivuljo ROC - angl. receiver operating characteristic) in AUPRC (ploščino pod krivuljo PRC - angl. precision-recall curve). Učenje trenutne naloge prenehamo, ko se AUROC na validacijski množici te naloge preneha izboljševati. Naš model sledi arhitekturi, ki je bila predlagana v [11] in vsebuje en nivo transformerskega kodirnika, ki mu sledita dva polno povezana nivoja (s 64 in 2 nevroni).

4.2 Primerjalne metode

Najprej predstavljamo primerjavo uporabe superpozicije v polno povezanih mrežah (PPM) v primerjavi z transformerskimi mrežami glede na vse tri metrike (tj. točnost, AUROC, AUPRC). Na sliki 1 prikazujemo, kako se vrednosti naših ocenjenih meritev spreminjajo med učenjem šestih nalog. Ko je učenje vsake zaporedne naloge končano, izračunamo povprečno vrednost metrike za vse do sedaj naučene naloge. Navpični stolpci pri nalogi i predstavljajo povprečne vrednosti nalog 1, ..., i. Ker se naše naloge razlikujejo po težavnosti, lahko opazimo, da povprečne vrednosti med učenjem nihajo. Iz grafov je razvidno, da je uporaba superpozicije v transformerju boljša od prve do zadnje naloge glede na vsa tri merila.



(a) Polno povezana mreža



(b) Transformer (naš pristop)

Slika 1: **Primerjava povprečnih vrednosti evalvacijskih metrik do i-te naloge z uporabo superpozicije v (a) polno povezani mreži in (b) transformerju.**

Za strnjeno predstavitev rezultatov iz vseh drugih primerjalnih metod v nadaljevanju prikažemo le vrednosti ocenjevalnih metrik po tem, ko so vse naloge naučene. To je enako zadnjim trem stolpcem (z desne strani) s slike 1. Ker so nekatere naše naloge neuravnotežene pri distribuciji ciljnih razredov, poročamo o AUROC in AUPRC metrikah. V tabeli 1 primerjamo našo metodo s tremi priljubljenimi pristopi nadaljevalnega učenja: *EWC* (angl. Elastic Weight Consolidation) [3], *Online EWC* (angl. Online Elastic Weight Consolidation) [9] in superpozicijo v polno povezanih mrežah [2]. Poleg tega primerjamo naš pristop z metodo, kjer vsako nalogo učimo v ločeni mreži, tako da ne more priti do pozabljanja modela (s tem torej dobimo zgornjo mejo uspešnosti). Ta pristop pričakovano dosega najboljše rezultate, vendar je izjemno pomnilniško neučinkovit. Kot je prikazano v tabeli 1, je naša metoda s superpozicijo v transformerjih boljša od drugih metod nadaljevalnega učenja glede na AUROC in AUPRC. Od druge najuspešnejše metode je naš pristop v povprečju šestih nalog boljši za 4,6 % pri AUROC in 3,0 % pri AUPRC.

Tabela 1: **Primerjalna analiza metod po naučenih šestih klasifikacijskih nalogah. Rezultati predstavljajo povprečje vseh šestih nalog. Najboljša rezultata (z neupoštevanjem ločenih mrež) sta krepko označena.**

Metode	AUROC	AUPRC
Ločene mreže (transformer)	94.0 ± 0.1	94.5 ± 0.1
Ločene mreže (PPM)	90.3 ± 0.1	91.3 ± 0.1
EWC [3]	74.4 ± 1.4	74.2 ± 4.1
Online EWC [9]	70.7 ± 2.0	73.1 ± 0.5
Superpozicija v PPM	84.8 ± 2.3	86.9 ± 2.0
Superpozicija v transformerjih	**89.4 ± 2.4**	**89.9 ± 2.7**

5 ZAKLJUČEK

Predstavili smo novo metodo nadaljevalnega učenja, kjer uporabljamo superpozicijski pristop znotraj transformerske arhitekture nevronskih mrež. Naša rešitev zmanjša pozabljanje modela med učenjem več nalog in doseže najboljšo zmogljivost med primerjanimi metodami. Glavna omejitev našega dela je ta, da so vse naloge vezane na isto globoko nevronsko mrežo in zato naš pristop služi le nalogam, ki jih je mogoče naučiti s podobno mrežno arhitekturo. Naše delo bi lahko dodatno izboljšali z možnostjo učenja nalog z različnimi velikostmi vhoda ali izhoda. V prihodnosti želimo razširiti našo metodo, da bo primerna za različne velikosti podatkov, pa tudi za različne mrežne arhitekture z združevanjem metode z drugimi pristopi regularizacije. Naše delo širi uporabnost superpozicijskega principa in ker smo prvi, ki smo omogočili uporabo superpozicije v transformerjih, verjamemo, da lahko naše delo ustvari novo vejo raziskav na področju nadaljevalnega učenja.

LITERATURA

[1] Magdalena Marta Biesialska, Katarzyna Biesialska, and Marta Ruiz Costa-jussà. Continual lifelong learning in natural language processing: a survey. In *COLING 2020, The 28th International Conference on Computational Linguistics: December 8-13, 2020, Barcelona, Spain (online): proceedings of the conference*, pages 6523–6541. Association for Computational Linguistics, 2020.

[2] Brian Cheung, Alexander Terekhov, Yubei Chen, Pulkit Agrawal, and Bruno Olshausen. Superposition of many models into one. *Advances in neural information processing systems*, 32, 2019.

[3] James Kirkpatrick, Razvan Pascanu, Neil Rabinowitz, Joel Veness, Guillaume Desjardins, Andrei A. Rusu, Kieran Milan, John Quan, Tiago Ramalho, Agnieszka Grabska-Barwinska, Demis Hassabis, Claudia Clopath, Dharshan Kumaran, and Raia Hadsell. Overcoming catastrophic forgetting in ne- ural networks. *Proceedings of the National Academy of Sciences of the United States of America*, 114(13):3521–3526, 2017.

[4] David Lopez-Paz and Marc'Aurelio Ranzato. Gradient episodic memory for continual learning. In *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pages 6470–6479, 2017.

[5] Tomás Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. Efficient estimation of word representations in vector space. In Yoshua Bengio and Yann LeCun, editors, *1st International Conference on Learning Representations, ICLR 2013, Scottsdale, Arizona, USA, May 2-4, 2013, Workshop Track Proceedings*, 2013.

[6] Behnam Neyshabur, Hanie Sedghi, and Chiyuan Zhang. What is being transferred in transfer learning? *Advances in neural information processing systems, 33:512–523, 2020.*

[7] German I. Parisi, Ronald Kemker, Jose L. Part, Christopher Kanan, and Stefan Wermter. Continual lifelong learning with neural networks: A review. *Neural Networks*, 113:54–71, 2019.

[8] Sebastian Ruder. An overview of multi-task learning in deep neural networks. *CoRR*, abs/1706.05098, 2017.

[9] Jonathan Schwarz, Wojciech Czarnecki, Jelena Luketina, Agnieszka Grabska-Barwinska, Yee Whye Teh, Razvan Pascanu, and Raia Hadsell. Progress & compress: A scalable framework for continual learning. In *International Conference on Machine Learning*, pages 4528–4537. PMLR, 2018.

[10] Mariya Toneva, Alessandro Sordoni, Remi Tachet des Combes, Adam Trischler, Yoshua Bengio, and Geoffrey J. Gordon. An empirical study of example forgetting during deep neural network learning. In *International Conference on Learning Representations*, 2019.

[11] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pages 6000–6010, 2017.

[12] Mitchell Wortsman, Vivek Ramanujan, Rosanne Liu, Aniruddha Kembhavi, Mohammad Rastegari, Jason Yosinski, and Ali Farhadi. Supermasks in Superposition. *NIPS*, (NeurIPS), 2020.

[13] Friedemann Zenke, Ben Poole, and Surya Ganguli. Continual learning through synaptic intelligence. *34th International Conference on Machine Learning, ICML 2017, 8:6072–6082, 2017.*

[14] Fuzhen Zhuang, Zhiyuan Qi, Keyu Duan, Dongbo Xi, Yongchun Zhu, Hengshu Zhu, Hui Xiong, and Qing He. A Comprehensive Survey on Transfer Learning. *Proceedings of the IEEE,* 109(1):43–76, 2021.

▪

Marko Zeman je magistriral iz računalništva in informatike na Univerzi v Ljubljani, Fakulteti za računalništvo in informatiko leta 2020. Trenutno je raziskovalec in doktorski študent na Fakulteti za računalništvo in informatiko v Laboratoriju za kognitivno modeliranje. Njegova raziskovalna zanimanja so predvsem globoko učenje, nevronske mreže in metode nadaljevalnega učenja.

▪

Jana Faganeli Pucer je docentka na Fakulteti za računalništvo in informatiko. Njeno raziskovalno delo je osredotočeno na strojno učenje, predvsem na aplikacijo metod strojnega učenje v okoljskih znanostih. Več let sodeluje z Agencijo Republike Slovenije za okolje na področju kakovosti zraka.

▪

Igor Kononenko je doktor računalniških znanosti in redni profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani ter predstojnik Laboratorija za kognitivno modeliranje. Njegova raziskovalna področja so umetna inteligenca, strojno učenje, nevronske mreže in kognitivno modeliranje. Je (so)avtor 225 člankov na teh področjih ter 13 učbenikov (dve knjigi izšli v Angliji).

▪

Zoran Bosnić je profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Raziskovalno se ukvarja z umetno inteligenco, zlasti s strojnim učenjem. Osredotoča se pretežno na učenje iz podatkovnih tokov in na interdisciplinarne aplikacije strojnega učenja. Na tem področju je tudi (so)avtor okoli 70 znanstvenih člankov.

Uporaba informacijskih tehnologij pri svetovalnem in psihoterapevtskem delu s skupinami v času epidemije covid-19

Tadeja Batagelj
Svetovalni center za otroke, mladostnike in starše Maribor, Lavričeva 5, 2000 Maribor
tadeja.batagelj@guest.arnes.si

Izvleček

Izbruh epidemije covid-19 je v svetovalni in terapevtski prostor prinesel številne nenadne spremembe. Izvajalci storitev so morali v kratkem času spremeniti način delovanja in iz svetovanja v živo preiti na delo na daljavo, večinoma preko na splet. Zaradi razmer so se pojavile povečane stiske pri uporabnikih storitev, kar je vodilo v povečane potrebe po tovrstnih obravnavah. Pri tem pa je analiza stanja pokazala, da so se izvajalci tovrstne pomoči s spremembami soočali brez jasnih smernic in dokazov o učinkovitosti novih oblik dela. Namen prispevka je osvetliti teoretične ugotovitve raziskav glede skupinskih oblik svetovalnega in terapevtskega dela na daljavo, osvetliti uporabnosti in pomanjkljivosti informacijskih tehnologij, ki tovrstno delo omogočajo ter predstaviti praktične izkušnje in mnenja uporabnikov tovrstnih oblik dela na Svetovalnem centru za otroke, mladostnike in starše Maribor. Vsi predstavljeni rezultati vodijo do ugotovite, da je skupinsko svetovalno in terapevtsko delo preko videokonferenc kljub nekaterim omejitvam in ob pomanjkanju teoretičnih dokazov o učinkovitosti, v praksi učinkovit in pri uporabnikih dobro sprejet način dela, za katerega bi bilo smiselno, da se v prihodnosti v večji meri uvaja v svetovalno in terapevtsko delo.

Ključne besede: epidemija covid-19, skupinska terapija, skupinsko svetovanje, svetovanje na daljavo, vzgoja in izobraževanje

Use of information technologies in counselling and psychotherapeutic work with groups during the COVID-19 epidemic

Abstract

The outbreak of the Covid-19 epidemic brought many sudden changes in the counselling and therapeutic space. The counselling and therapy service providers had to change the way they work in a short period of time and move from in-person counselling to online counselling. The resulting situation has increased distress among the service users, which has consequently increased the need for professional treatment. However, the analysis of the situation has shown that the counsellors and therapists have had to adapt to changes without unambiguous guidelines and instructions as well as evidence of the effectiveness of new forms of work. The purpose of this paper is to highlight the theoretical findings of research into forms of group counselling and therapeutic work of teleworking, to highlight the pros and cons of using such information technology and to present the practical experiences and opinions of users of such forms of work in The Counselling Centre for Children, Adolescents and Parents Maribor. All the presented results lead to the conclusion that group counselling and therapeutic work via videoconferencing, despite certain limitations and lack of theoretical evidence of effectiveness, are effective in practice and well accepted among users and thus should also be used in the future.

Keywords: Covid-19 epidemic, education and training, group counselling, group therapy, online counselling

1 UVOD

Epidemija covid-19 je v svetovalni in terapevtski prostor prinesla veliko negotovosti in sprememb. Na spremembe se ni bilo mogoče pripraviti vnaprej, zaradi česar je bilo prilagajanje še zahtevnejše. Pouk na daljavo, okrnjenost in spremenjenost vzgojno-izobraževalnega procesa so zahtevali hitre prilagoditve tako učiteljev, kot učencev in staršev. Hitre spremembe in naraščajoča negotovost pa so vodili v vedno nove in večje stiske, zaradi katerih so se po

prvotnem zatišju otroci, mladostniki in starši vedno pogosteje obračali tudi na Svetovalni center Maribor. V teh okoliščinah je bil pomemben hiter odziv strokovnih služb in zagotavljanje kratkih čakalnih dob je bilo oteženo.

Svetovalni center Maribor z namenom celostne in strokovne podpore uporabnikom intenzivno sodeluje tudi s svetovalnimi službami na šolah. Na Svetovalnem centru smo v času epidemije covid-19 zaznali povečane potrebe po psihološki, specialno-pedagoški in podobni podpori vsem udeležencem vzgojno-izobraževalnega procesa. Z namenom nudenja podpore čim večjemu številu uporabnikov, smo želeli v kar največji meri ohraniti skupinske oblike dela. Zaradi ukrepov za omejevanje gibanja in združevanja pa smo morali tako v svetovalnih službah kot v Svetovalnih centrih začeti iskati nove in izvirne pristope pri svojem delu in se seznanjati z različnimi možnostmi, ki jih nudijo sodobne informacijske tehnologije.

2 IZZIVI IN MOŽNOSTI ZA SKUPINSKE OBLIKE DELA V ČASU EPIDEMIJE COVID-19

Skupinsko svetovanje preko spleta je relativno nova modaliteta za vodenje skupin. Raziskave, ki bi evalvirale učinkovitost skupinskih oblik dela preko spleta (kot so svetovanje, terapija, vodenje in podobno) ali postavljale jasne smernice za izvajanje tovrstnih oblik pomoči, so redke. Med številnimi strokovnjaki [11, 13] je v preteklosti veljalo prepričanje, da je zaradi vseh omejitev, ki jih tovrstna oblika dela prinaša, učinkovitost skupinskih oblik dela na daljavo okrnjena do te mere, da je pod vprašanjem upravičenost izvajanja tovrstnih oblik svetovanja in terapije. Med posameznimi avtorji je veljalo celo prepričanje, da »Online terapija« ni zares terapija [6]. Weinberg [19] povzema nekatere omejitve dela na daljavo in ugotavlja, da medtem, ko je dve komponenti terapevtske aliance, to sta dogovora glede ciljev in nalog, možno brez večjih ovir doseči tudi pri skupinah na daljavo, pa ostaja predvsem vprašljiva tretja komponenta, to je kvaliteta odnosov znotraj skupine. Glavna ovira pri prehodu od interakcije v živo k interakciji preko zaslona je odsotnost očesnega stika, ki je velikega pomena ne samo za oblikovanje skupinske dinamike in zaupnosti, temveč je tudi povratna informacija terapevtu glede odzivanja posameznih udeležencev skupinskega svetovanja ali terapije. Pri srečevanjih na daljavo je prav tako težko poskrbeti za usmerjanje pozornosti udeležencev. Vzdrževanje pozornosti pri delu preko videokonference je oteženo zaradi številnih distraktorjev v okolju, pomanjkanja osebnega stika in težjega odzivanja na neverbalno komunikacijo udeležencev. Pri tem je lahko v pomoč več samorazkrivanja terapevta in spodbujanje udeležencev k uporabi domišljije. Prehod na delo na daljavo z uporabo sodobnih tehnologij, kot so videokonferenčni sistemi, od terapevta zahteva dodatna znanja in treninge tako na področju skupinskega svetovanja in terapije kot na področju same tehnologije.

Z izbruhom epidemije covid-19 je delo na daljavo kljub strokovno utemeljenim pomislekom postalo nuja in številne skupine so bile primorane svoja srečanja nadaljevati na način videokonferenc, hkrati pa so se povečale potrebe po strokovni pomoči [9], zaradi česar so se oblikovale številne nove skupine. Tako je postalo nujno, da se strokovnjakom, strokovnim delavcem v šoli in v zunanjih strokovnih institucijah čim prej ponudi pregled raziskav in jasne smernice za delo skupin preko spleta. Randomiziranih raziskav na tem področju je sicer še vedno malo, dostopne ugotovitve pa so sledeče [19]:

- Udeleženci, ki so bili del spletnih skupin za samopomoč, so poročali o večji opolnomočenosti.
- Video-konferenčne skupine so izvedljive, učinki pa so primerljivi kot v skupinah, ki se srečujejo v živo.
- Skupine, ki temeljijo na vedenjsko – kognitivnih principih dosegajo podobne učinke, kot intervencije, ki potekajo v živo, a je doseganje primerljivih rezultatov običajno dolgotrajnejše.
- Učinkovitost spletnih skupin se poveča z uvedbo gradiva za samopomoč.
- Tako videokonferenčne skupine kot skupine, ki temeljijo na izmenjavi pisnih mnenj (ang. *chat group*) kažejo pomembna izboljšanja v primerjavi s kontrolno skupino, vendar kažejo videokonferenčne skupine primerjalno pomembnejše izboljšanje mentalnega zdravja.
- Učinkovitost spletnih oblik skupinskega dela se razlikuje glede na modaliteto vodenja, vključene posameznike in glede na naravo težav in teme, ki se na skupini odpirajo. Pri mlajših, bolj izobraženih, je možnost uporabe IKT v svetovalni dejavnosti večja, hkrati so večji tudi učinki tovrstnega svetovanja. Večje učinke kažejo skupine, ki delajo po vedenjsko-kognitivnih principih, a upoštevati je potrebno, da je tudi raziskav na teh skupinah več (verjetno zaradi lažjega merjenja učinkov).

- Omejitve dela na daljavo se najbolj intenzivno kažejo na področju oblikovanja skupinske klime in zaupnosti.

Tudi nekatere slovenske raziskave potrjujejo ugotovitve, da kakovost komunikacije in dela na daljavo ni enaka kot v tradicionalnih oblikah, saj manjka predvsem osebni stik s sogovorniki, ta stik pa lahko interakcija ob pomoči sodobnih tehnologij samo delno nadomesti [6], kar velja tako za individualne kot za skupinske oblike dela.

Békés in Aafjes-van Doorn [1], ki sta izvedli pregled podatkov, pridobljenih s strani 145 psihoterapevtov iz Severne Amerike in Evrope, ugotavljata, da je kljub stresnim okoliščinam v času epidemije Covid-19, odnos strokovnjakov praktikov do psihoterapije na daljavo, relativno pozitiven. Ugotavljata, da na sam odnos do tovrstnih oblik dela sicer vplivajo pretekle izkušnje z delom na daljavo, priprava terapevta in klienta in subjektivni občutki tekom samih srečanj, ki so pogosto občutek večje utrujenosti, manjšega samozaupanja in kompetentnosti, manjše povezanosti in avtentičnosti. Te vsebine bi bilo smiselno in koristno naslavljati na treningih, izobraževanjih, supervizijah in intervizijah.

Raziskave na področju spletnih skupin so maloštevilne in potrebnih je več raziskav, da bi se raziskalo učinkovitost tovrstnega načina dela za različne posameznike in vsebine. Odprta ostajajo številna, predvsem etična vprašanja, vprašanja zaupnosti informacij in s tem povezanih nevarnosti spleta, možnosti za izgradnjo dobrega odnosa, vpliv odsotnosti očesnega stika in fizične bližine in podobno. Vse to so vprašanja, ki doprinašajo k učinkovitosti skupinskih oblik dela in jih je potrebno ob delu na daljavo še posebej nasloviti.

3 DELO SVETOVALNIH SLUŽB IN ZUNANJIH STROKOVNIH INSTITUCIJ V ČASU EPIDEMIJE COVID-19

Mrvar, Jeznik, Šarić in Šteh [7] navajajo: »Ob izbruhu epidemije covida-19 se je življenje in delo v vzgojno-izobraževalnih ustanovah v trenutku izjemno spremenilo. Skupnost otrok, učencev oz. dijakov in strokovnih delavcev se je preselila v virtualni prostor.« Z namenom podpore so bila izdana priporočila za delo z uporabniki, izvedene pa so bile tudi raziskave o tem, kako se je način dela v času epidemije spremenil.

3.1 Predlogi in priporočila za delo šolske svetovalne službe v času izolacije zaradi epidemije

Kmalu po izbruhu epidemije covid-19 in selitvi vzgojno izobraževalnega, svetovalnega in terapevtskega dela na daljavo, sta se Zavod RS za šolstvo in Oddelek za pedagogiko in andragogiko Filozofske fakultete UL odzvala na novo nastale razmere in podala nekaj predlogov za delo šolske svetovalne službe v času izolacije zaradi epidemije [17]. Predlogi so se nanašali na:

- ohranjanje stika z udeleženci vzgojno-izobraževalnega procesa,
- dejavnosti v oddelčni skupnosti,
- pripravo napotkov za samostojno učenje doma,
- vprašanja motivacije učencev za šolsko delo,
- seznanjenost o bolezni covid-19 in ukrepih v zvezi z epidemijo in
- na skrb zase.

Posebej so bili izpostavljeni predlogi za individualni pogovor z učenci/dijaki na daljavo. Predlogov in navodil za skupinsko izvajanje podpore in pomoči je bilo manj. Svetovalke ZRSŠ [14] so svetovale, da se svetovalna služba vključi v izvajanje videokonferenčnih razrednih ur, kamor se lahko vključi delavnice iz socialnega in čustvenega učenja. Omenile so tudi možnost organiziranja posebne skupine učencev ali dijakov, ki potrebujejo še dodatno spremljanje, razbremenilne pogovore, konkretnejšo spodbudo in pomoč.

V aprilu 2020 je bila na Oddelku za pedagogiko in andragogiko Filozofske fakultete Univerze v Ljubljani izvedena raziskava, namen katere je bil proučiti, kako se je svetovalna služba soočala z vprašanji, izzivi in težavami, ki so se pojavili med izvajanjem izobraževalnega in svetovalnega dela na daljavo [7]. Dve vprašanji v raziskavi sta se nanašali na sodelovanje svetovalnih delavcev v času dela od doma z drugimi udeleženci, to je s sodelavci, učenci oziroma dijaki, kolegi svetovalnimi delavci in na oceno tega sodelovanja. Iz rezultatov je razvidno, da so bili v stalnem stiku z učitelji oz. vzgojitelji, da so si nudili medsebojno podporo, se posvetovali in reševali aktualne težave. Glede sodelovanja z učenci oz. dijaki raziskava ugotavlja precejšnje razlike glede odzivnosti in sodelovanja, globalna ugotovitev pa je, da »tisti učenci in dijaki, ki že v času rednega pouka niso dobro sodelovali, se tudi sedaj slabo ali pa sploh ne odzivajo«. Tudi glede sodelovanja s starši so rezultati

raziskave podobni – pomemben delež staršev ostaja neodziven. Tudi tisti svetovalni delavci, ki so sodelovanje ocenili kot dobro, pa opozarjajo, da manjka osebni stik.

Hkrati so navajali, da je (bilo) v času izobraževanja na daljavo več dela, da je to bolj naporno (za vse udeležene), mnogim se je delavnik raztegnil čez ves dan. Večina dela je potekala individualno, z učenci in dijaki ter učitelji preko e-pošte in videokonferenc, s starši pa je prevladovala komunikacija po spletni pošti. Ugotovitev o prevladujočih načinih komunikacije in o povečanem obsegu dela na področju svetovalne službe, mora nujno voditi v razmišljanje o možnih rešitvah za nastalo situacijo. Ena od možnih rešitev je lahko v skupinskih oblikah dela.

3.2 Primernost skupinskih oblik dela za delo z udeleženci VIZ

Skupinske oblike dela, kot so svetovanje in terapija, so v vzgojno-izobraževalnem prostoru (ob ustrezni usposobljenosti strokovnega delavca) primerne za vse skupine uporabnikov – tako učence, kot starše in učitelje [16]. V skladu s standardi ameriške psihološke agencije APA [16] skupinsko svetovanje praviloma poteka v skupini od 5 do 15 udeležencev z dvema voditeljema, ki sta za tovrstno delo ustrezno usposobljena. Običajno se skupine srečujejo enkrat tedensko in posamezno srečanje traja eno ali dve uri. Številne skupine so oblikovane z namenom psihoterapevtske podpore na točno določenem področju (na primer depresija, anksioznost, motnje hranjenja in podobno), druge pa se usmerjajo na bolj splošna vprašanja izboljšanja socialnih spretnosti, pomoč pri spoprijemanju z jezo, izgubo, sramežljivostjo, osamljenostjo ali nizko samopodobo ali na aktualne izzive vsakdanjika. V šolskem okolju so skupinske oblike dela učinkovite tudi pri spodbujanju izvršilnih funkcij, pridobivanju učnih in organizacijskih veščin, obravnavi tem s področja poklicne orientacije, izgradnji rezilientnosti, podpori staršem pri vprašanjih glede šolanja njihovega otroka ali kot oblika intervizije učiteljev ali drugih strokovnih delavcev in podobno.

Čeprav je vključitev v skupino tujcev lahko sprva zastrašujoča misel, ima skupinsko delo številne prednosti, ki jih individualno svetovanje in pomoč ne moreta nuditi. Prednost skupinskega svetovanja in drugih oblik skupinskega dela z uporabniki je, da omogoča deljenje izkušenj, takojšnje povratne informacije s strani udeležencev skupine in medsebojno učenje. Pomembna prednost skupine je tudi podpora, ki jo skupina nudi posamezniku in normalizacija težav, ki jo lahko posameznik doživi v skupini. Pogosto je namreč prepričanje, da je posameznik v stiski sam, da določeno težavo doživljamo le on, v skupini pa lahko člani spoznajo, da gredo tudi drugi člani skupine skozi podobne težave in da niso sami. Hkrati pridobijo dobrodošle ideje, kako se lahko z neko težavo in stisko soočijo.

Medsebojna podpora je pomembna prednost skupinskega svetovanja, vendar to ni edina prednost skupine. Vsako skupino vodita en ali dva usposobljena voditelja, ki člane skupine učita z dokazi podprtih strategij za reševanje problemov. Zanemariti ne gre niti časovne in finančne ekonomičnosti takih oblik dela, saj lahko en ali dva strokovna delavca v določenem časovnem terminu nudita podporo večjemu številu uporabnikov, kar je še posebej dobrodošlo v časih povečanih stisk in negotovosti, kot je tudi obdobje epidemije covid-19. Zaradi vsega navedenega je lahko intenzivnejše uvajanje skupinskih oblik dela v času dela v živo ali na daljavo, pomembna dopolnitev za svetovalne delavce, s katero lahko delujejo na vseh osnovnih vrstah dejavnosti, predvsem pa na področju razvojnih in preventivnih dejavnosti [12].

4 UPORABNOST INFORMACIJSKIH TEHNOLOGIJ, KI OMOGOČAJO DELO S SKUPINAMI NA DALJAVO

Izbruh epidemije je pred izvajalce strokovne pomoči na področju duševnega zdravja postavil številne nove izzive. Poleg tega, da so se pojavile povečane potrebe po psihološki podpori in pomoči, so razmere onemogočale neposreden stik uporabnika s strokovnjakom. Hiter razvoj spleta je že v času pred izbruhom epidemije omogočal tudi razvoj psihološke dejavnosti na spletu, posledično je to pomenilo pojav več razprav o učinkovitosti in etičnosti tovrstnega dela. Izvajanje psihološke dejavnosti na daljavo ni omejeno samo na splet, temveč storitve na daljavo omogočajo tudi telefoni, televizija, radio in različne oblike dopisovanja. Najbolj uporabljene aplikacije za tovrstno dejavnost so Zoom, MS Teams, Google Meet, Skype, Viber. Raziskave nam zaenkrat nudijo le omejena spoznanja o ustreznosti in učinkovitosti posameznega komunikacijskega sredstva za izvajanje psihološke dejavnosti, tako z vidika medsebojnih primerjav posameznih oblik psihološke prakse na daljavo, kot tudi z vidika primerljivosti teh metod

s tradicionalnimi oblikami psiholoških postopkov v živo. Še posebej je izrazito pomanjkanje raziskav o učinkovitosti skupinskih oblik svetovanja in terapije na daljavo.

Društvo psihologov Slovenije [10] ugotavlja, da je trenutno na razpolago več različnih komunikacijskih sredstev za izvajanje psihološke dejavnosti na daljavo. Raziskave nam za enkrat nudijo le omejena spoznanja o ustreznosti in učinkovitosti posameznega komunikacijskega sredstva za izvajanje psihološke dejavnosti, tako z vidika medsebojnih primerjav posameznih oblik psihološke prakse na daljavo, kot tudi z vidika primerljivosti teh metod s tradicionalnimi oblikami psiholoških postopkov »v živo«. Drugo odprto vprašanje glede uporabe telekomunikacijskih tehnologij ostaja vprašanje varnosti in zaupnosti podatkov. V Sloveniji pri tem izhajamo iz zakona o varovanju osebnih podatkov in kodeksa poklicne etike psihologov. Oba dokumenta se aplicirata tudi pri delu na daljavo. Informacijski pooblaščenec v zvezi s tem pojasnjuje [8] da »se glede posamezne programske opreme ne more vnaprej soditi, ai je njena uporaba skladna z zakonodajo o varstvu osebnih podatkov, oziroma dovoljevati njene uporabe, saj je nenazadnje poleg samih tehnoloških vidikov skladnosti odvisna tudi od samega načina uporabe, informiranja ose in drugih zahtev«.

Informacijski pooblaščenec [8] ugotavlja tudi, da »zakonodaja o varstvu osebnih podatkov prav gotovo ne prepoveduje uporabe spletnih orodij in načinov komuniciranja, je pa pri njihovi uporabi potrebno zagotoviti varnost in zaupnost podatkov, saj gre za obdelavo posebnih varstvo osebnih podatkov, katerih prenos po javnih telekomunikacijskih omrežjih mora potekati na šifriran način. Na strani upravljavca podatkov je tako treba preveriti, ali posamezno orodje omogoča varovanje zaupnosti, predvsem z omogočanjem šifrirane komunikacije, ki nepooblaščenim osebam preprečuje seznanitev z vsebino komunikacije, na strani posameznika pa je odgovornost za varno namestitev in uporabo posameznega tovrstnega orodja.«

Zaradi vsega navedenega, smo se na Svetovalnem centru za otroke, mladostnike in starše odločili, da za uporabo v svetovalne in terapevtske namene izberemo zoom, ki je eden od najzmogljivejših videokonferenčnih sistemov trenutno, saj omogoča, da več uporabnikov hkrati z vklopljenim zvokom in sliko sodeluje v videokonferenčni sobi. Na Arnesu so z nakupom licenc omogočili vsem učiteljem na slovenskih osnovnih in srednjih šolah, uporabnikom iz vrtcev, dijaških domov, glasbenih šol in svetovalnih centrov, brezplačno uporabo sistema z vsemi funkcionalnostmi in varnostnimi mehanizmi.

5 PRAKTIČNE IZKUŠNJE PRI IZVAJANJU SKUPINSKIH OBLIK DELA NA DALJAVO V SVETOVALNEM CENTRU MARIBOR

Ob intenzivnem sodelovanju s svetovalnimi službami smo v Svetovalnem centru Maribor zaznali povečane potrebe po strokovni pomoči tako staršem, otrokom in mladostnikom, kot strokovnim delavcem šol. Kljub zavedanju omejitev spletnega skupinskega dela smo se zaradi možnosti podpore večjemu številu uporabnikov in ob prednostih, ki jih skupinske oblike dela prinašajo, odločili za izvedbo več skupinskih programov. Pri izbiri videokonferenčnega sistema smo izhajali predvsem iz enostavnosti sistema in poznavanja sistema pri naših uporabnikih. Ker je Arnes šolam omogočil brezplačno uporabo sistema Zoom, smo sklepali, da je sistem pri starših ter otrocih in mladostnikih dovolj poznan, da bo omogočal enostavno uporabo. Hkrati je bil pomemben kriterij za izbiro tega sistema tudi brezplačna uporaba in podpora, ki so jo v primeru težav in vprašanj nudili na Arnesu. Poleg tega smo želeli za čim večjo učinkovitost najti orodje za delo na daljavo, ki bi uporabnikom omogočal uporabniško izkušnjo, ki je čim bolj podobna izkušnji skupinskega srečevanja v živo [5] – pri tem so se kot uporabne izkazale predvsem naslednje možnosti, ki jih je omogočal Zoom:

- Bela tabla (ang. *whiteboard*)
- Klepet (ang. *chat*)
- Razdelitev v manjše skupine za lažjo delitev mnenj (ang. *breakout rooms*)
- Krajše ankete za hitro odločanje ali iskanje skupnih mnenj (ang. *polls*)

Programi, so potekali preko videokonference Zoom ali po hibridnem modelu (kombinacija srečanj v živo in preko videokonference) so bili:

- Neverjetna leta – trening starševstva, namenjen staršem vzgojno zahtevnejših predšolskih otrok.
- Učimo se učiti – delavnice namenjene učencem druge in tretje triade z namenom spoznavanja sebe kot učenca, učenje organiziranja časa, preizkušanje različnih strategij učenja in razvijanje veselja do učenja.

- HOPS – delavnice namenjene učencem tretje triade za spodbujanje izvršilnih funkcij, kot so organizacija, pozornost, spomin, začenjanje z aktivnostjo in podobno.
- Trening branja – za učence 4. in 5. razredov, ki se spopadajo s šibkostmi na področju branja ali jim za branje primanjkuje motivacije.
- Pogumen kot tiger – delavnice namenjene staršem predšolskih otrok s povečano anksioznostjo
- Cool Kids in Chilled – delavnice za spoprijemanje z anksioznostjo za otroke in mladostnike ter njihove starše
- Supervizija za učitelje – namenjena učiteljem in svetovalnim delavcem kot strokovna in medsebojna podpora v času sprememb, povečanega obsega dela in negotovosti.

Po zaključku posameznih skupinskih programov, je bila izvedena tudi evalvacija s strani udeležencev in izvajalcev. Evalvacija je praviloma potekala v obliki nestrukturiranega intervjuja ali krajše ankete. Povzamemo lahko, da so bile vse oblike skupinskega dela na daljavo kljub določenim omejitvam izvedbe dobro sprejete. Iz odgovorov udeležencev in izvajalcev lahko povzamemo nekatere prednosti in ovire ter izpeljemo priporočila za nadaljnje izvajanje skupinskih oblik dela na daljavo.

Med prednostmi takega načina dela so udeleženci navajali:

- možnost delitve mnenj, izkušenj,
- pridobivanje praktičnih napotkov za reševanje težav,
- učinkovitost naučenih strategij,
- časovna ekonomičnost,
- večja sproščenost, kot pri srečanjih v živo in
- zmanjšanje občutka osamljenosti.

Omejitve skupinskega dela na daljavo, ki so jih udeleženci zaznavali, so bile podobne tistim, o katerih beremo v raziskavah. Poleg pomislekov glede zasebnosti in pasti, ki jih prinaša deljenje zasebnosti preko spleta, so čutili manjšo povezanost skupine zaradi pomanjkanja osebnega stika in neverbalne komunikacije. Nekateri učenci so izrazili pomisleke zaradi manjše zasebnosti – v kolikor do spleta dostopajo iz skupnega prostora v stanovanju, kamor imajo kadarkoli dostop tudi drugi družinski člani. Pomembna ovira so lahko tudi tehnične težave, vendar udeleženci na Svetovalnem centru tega niso posebej izpostavljali.

Skupinsko delo je glede na izkušnje uporabnikov Svetovalnega centra Maribor dobrodošla dopolnitev k podpori, pomoči in svetovanju v času izrednih razmer zaradi epidemije [2, 3, 4]. Vsekakor je pri načrtovanju tovrstnih aktivnosti potrebno upoštevati omejitve in posebnosti, ki jih prinaša videokonferenčni način srečevanja. Med možnimi rešitvami in prilagoditvami so delo v manjših skupinah, ki omogoča bolj poglobljeno diskusijo, dodatne spodbude voditeljev, dodatna gradiva za samopomoč, digitalne oblike nagrajevanja in spodbujanja, spodbujanje k prosti diskusiji med odmori z namenom večjega povezovanja članov skupine in podobno [2, 3, 4, 9 in 18].

6 SKLEP

Spremenjene okoliščine prinašajo potrebo po spremenjenih oblikah svetovanja in terapije. Na področju skupinskega dela na daljavo so potrebne dodatne raziskave. Posebej ostajajo odprta vprašanja vzpostavljanja skupinske povezanosti in dinamike, vpliv pomanjkanja neposredne interakcije, predvsem očesnega stika in vprašljiva kvaliteta vzpostavljenih odnosov. Prehod na spletne oblike skupinskega svetovanja zahteva znanje in trening. Kljub odprtim vprašanjem, pomanjkanju teoretičnih izhodišč in smernic, pa so se skupinske oblike svetovanja v času epidemije izkazale kot učinkovita in dobrodošla oblika dela za vse vključene skupine uporabnikov. Uporabniki so kot posebej dobrodošlo izpostavljali možnost deljenja izkušenj, medsebojnega učenja in medsebojno podporo. Ob strogem omejevanju gibanja in združevanja, so jim tedenska srečanja omogočala stik z drugimi ljudmi in lajšala občutek osamljenosti.

Skupinsko svetovanje in terapija tako ostajata pomembni obliki dela z uporabniki tudi v času omejitev in sprememb in sta lahko dobrodošlo strokovno in ekonomično dopolnilo k delu, predvsem pa omogočata kontinuirano nudenje pomoči uporabnikov ne glede na zdravstvene ali druge razmere, ki bi onemogočale srečevanje v živo.

LITERATURA

[1] Békés, V., in Aafjes-van Doorn, K. (2020). Psychotherapists' attitudes toward online therapy during the COVID-19 pandemic. Journal of Psychotherapy Integration, 30(2), 238-247. http://dx.doi.org/10.1037/int0000214

[2] Batagelj, T. (2020). Podpora učencem s šibkimi izvršilnimi funkcijami v času šolanja od doma. V Cigur, A. in Vuk, N. (ur.), VIII. Mednarodna strokovno-znanstvena konferenca Izzivi in težave sodobne družbe (str. 57-65). RIS Dvorec. https://www.ris-dr.si/data/attachment/a5d907c1122676441ed98f3c

6b33c94e6fb0bb97/1611840977Bilten_Izzivi_in_te_ave_sodobne_dru_be_2020.pdf
[3] Batagelj, T. (2021). Trening starševstva »Neverjetna leta« v času epidemije COVID-19. V Dajčar, M. in Novak, M. (ur.), IX. mednarodna konferenca Izzivi in težave sodobne družbe (str. 11-19). RIS Dvorec. https://www.ris-dr.si/data/attachment/1337657643fd0d52ac5e7876743a129134fb40a7/1629126744BILTEN_IZZIVI_IN_TE_AVE_SODOBNE_DRU_BE_2021.pdf
[4] Batagelj, T. in Mičić, S. (2021). Pomoč in podpora učencem s primanjkljaji na področju izvršilnih funkcij v času šolanja na daljavo. Sodobna pedagogika, 72(138), 218-233.
[5] Djurdjič, V. (2022). Videokonference za novo dobo. Monitor, 32 (1), 82-87.
[6] Essig, T. (2010). Be warned: »Online therapy« is not therapy, not really (blog post). https://www.psychologytoday.com/us/blog/over-simulated/201003/be-warned-online-therapy-is-not-therapy-not-really
[7] Gregorčič Mrvar, P., Jeznik, K., Šarić, M in Šteh, B. (2021). Soočanje svetovalnih delavk in delavcev v vzgojno-izobraževalnih ustanovah z epidemijo covida-19. Sodobna pedagogika, 72(138), 150-167.
[8] Informacijski pooblaščenec (b. d.). Mnenje glede on-line psihoterapevtske terapije. https://www.ip-rs.si/mnenja-gdpr/6048a487a0043
[9] Kastelic, N., Kmetič, E., Lazić, T., Okretič, L. (2021). Kako motivirati učence pri poučevanju na daljavo. Priročnik za učitelje. Univerza v Ljubljani, Filozofska fakulteta: Oddelek za psihologijo.
[10] Kovač, B., Seršen, S., Samojlenko, L., Gosar, D. (b. d.). Zagotavljanje psiholoških storitev na daljavo s pomočjo spleta in drugih komunikacijskih sredstev. http://www.dps.si/wp-content/uploads/2020/05/1_Zagotavljanje-psiholo%C5%A1kih-storitev-na-daljavo-slovenski-prevod-EFPA-smernic.pdf
[11] Markowitz, J. C., Milrod, B., Heckman, T. G., Bergman, M., Amsalem, D., Zalman, H. Ballas, T., Neria, Y. (25. 9. 2020). Psychotherapy at a Distance. ajp.psychiatryonline.org. https://ajp.psychiatryonline.org/doi/10.1176/appi.ajp.2020.20050557
[12] Mikuž, A., Kodrič, J., Musil, B., Svetina, M., Juriševič, M. (30. 10. 2020). Psihosocialne posledice epidemije covid-19 in spremljajočih ukrepov za otroke, mladostnike in družine. Klinična-psihologija.si. http://klinicna-psihologija.si/wp-content/uploads/2020/11/psihosocialne-posledice-epidemije-covid19-psiholo%C5%A1ka-stroka.pdf
[13] Parks, C. D. (2020). Group dynamics when battling a pandemic. Group Dynamics: Theory, Research, and Practice, 24(3), 115-121.
[14] Priporočila za delo svetovalnih delavcev z učenci na daljavo. (27. 10. 2020). skupnost.sio.si. https://skupnost.sio.si/mod/folder/view.php?id=337341
[15] Programske smernice svetovalne službe v osnovni šoli. (13. 5. 1999). Kurikularna komisija za svetovalno delo in oddelčno skupnost.
[16] Psychotherapy: Understanding group therapy. (31. 10. 2019). apa.org. https://www.apa.org/topics/psychotherapy/group-therapy
[17] Šarić, M. in Gregorič Mrvar, P. (20. 4. 2020). Nekaj predlogov za delo šolske svetovalne službe v času izolacije zaradi epidemije. Zdpds.si. https://zdpds.si/obvestila/nekaj-predlogov-za-delo-solske-svetovalne-sluzbe-v-casu-izolacije-zaradi-epidemije/
[18] Webster-Sratton, C. (2020). Hot Tips for IQ Group Leaders Delivering the Incredible Years Video Parent Programs via On-Line Tele-Sessions. incredibleyears.com. https://incredibleyearsblog.wordpress.com/2020/08/12/hot-tips-for-iy-group-leaders-delivering-parent-programs-online/
[19] Weinberg, H. (2020). Online Group Psychotherapy: Challenges and Possibilities During COVID-19 – A Practice Review. Group Dynamics: Theory, Research, and Practice, 24(3), 201-211.

▪

Tadeja Batagelj je psihologinja in direktorica Svetovalnega centra za otroke, mladostnike in starše Maribor. Diplomirala in magistrirala je na Oddelku za psihologije Univerze v Ljubljani. Je vedenjsko kognitivna terapevtka pod supervizijo, akreditirana izvajalka programov Neverjetna leta in Cool kids. Svetovalno in terapevtsko dela predvsem z otroki in mladostniki ter njihovimi starši, predava staršem in strokovnim delavcem šol in vrtcev, s strokovnimi prispevki se redno pojavlja na strokovnih konferencah. Pri delu v praksi izbira individualne in skupinske oblike svetovanja in terapije, pri čemer se po potrebi pogosto poslužuje tudi informacijskih tehnologij.

Možnosti vpeljave tehnologije veriženja blokov v prehranske oskrbovalne verige

Mitja Gradišnik, Martin Domajnko, Muhamed Turkanović
Fakulteta za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, Koroška cesta 46, 2000 Maribor
mitja.gradisnik@um.si, martin.domajnko@student.um.si, muhamed.turkanovic@um.si

Izvleček

Številni škandali povezani s kakovostjo, poreklom ali oporečnostjo prehranskih izdelkov, ki smo jim bili priča v zadnjih letih, so omajali zaupanje potrošnikov v prehranske izdelke na naših policah. Potrošniki v odgovor na škandale pričakujejo večjo transparentnost porekla in načina proizvodnje prehranskih produktov. Slednje toliko bolj velja za prehranske produkte z višjo dodano vrednostjo, kot so pridelki iz lokalne ali ekološke pridelave ter izdelki z geografsko zaščitenim poreklom.

Vpeljava tehnologij veriženja blokov vpeljuje v oskrbovalne prehranske verige nove možnosti, s pomočjo katerih je mogoče doseči višjo stopnjo sledljivosti in transparentnosti pridelave prehrambnih izdelkov. Dosledno vodenje zapisov o izdelku omogoča sledenje prehrambnim izdelkom v oskrbovalni verigi. Pri tem so zapisi v verigah blokov decentralizirani, javno preverljivi in nespremenljivi ter kot taki odporni na kasnejše manipulacije. V nadaljevanju predstavimo zasnovo prototipne programske rešitve za sledenje lokalno pridelanim izdelkom, ki je podprta s tehnologijami veriženja blokov.

Ključne besede: oskrbovalne prehranske verige, tehnologije veriženja blokov, transparentnost prehranskih izdelkov

Possibilities of introducing blockchain technology in food supply chains

Abstract

In recent years, numerous scandals related to the quality, origin or objectionability of food products have severely shaken consumer confidence in food products on our shelves. Accordingly, consumers expect clear transparency about the origin and method of food production. The latter is even more relevant for food products with higher added value, such as products from local or organic production and products with a geographically protected origin.

The introduction of blockchain technologies introduces new possibilities into food supply chains, with the help of which a high degree of traceability and transparency of food production can be achieved. Consistent record keeping makes it possible to keep track of food products in the supply chain. Such records in the blockchains are decentralized, publicly verifiable and unchangeable, and as such resistant to subsequent manipulation. In the following paper, we present a prototype implementation of a solution for tracking locally-grown products supported by blockchain technologies.

Keywords: Blockchain, food supply chain, food traceability

1 UVOD

Globalizacija prehranskih trgov je močno pospešila pretok živilskih produktov preko mej nacionalnih držav [1], [2]. Na naših policah se tako znajdejo prehranski izdelki, ki izvirajo iz različnih predelov sveta ter so, preden so dosegli naše prodajne police, prepotovali na tisoče kilometrov [3]. Posledica slednjega je širok nabor prehranskih izdelkov, med katerimi lahko potrošniki izbiramo. Tako je povsem običajno, da so sezonski produkti na naših trgovskih policah čez celo leto. Številne dobavne verige posledično težko natančno določijo, od kod določen produkt izhaja in pod kakšnimi pogoji je bil pridelan [4]. Proizvajalci hrane ponudijo izjemno malo ali celo nič informacij o dobaviteljih na drugem ali tretjem nivoju dobave [5].

Po drugi strani so prehranski trg v zadnjih letih pretresli številni škandali, ki so močno omajali zaupanje potrošnikov v kakovost in varnost prehranskih izdelkov na naših policah in zmožnost regulatorjev, da obstoječi trg ustrezno nadzirajo [6]. V medijih so tako odmevali številni incidenti povezani s ponarejanjem in napačnim označevanjem živil, zamenjavo in redčenjem surovin ter ponarejanjem ali napačnim navajanjem porekla surovin [1]. Posebej na udaru so predvsem kakovostnejši prehranski izdelki višjega cenovnega razreda, kot je na primer italijansko ekstra deviško olivno olje [7]. Skupni trg Evropske unije je na primer v letu 2013 močno pretresla afera s primešanim konjskim mesom številnim izdelkom iz govejega mesa [8]. Nadaljnjo, kanadska raziskava opravljena v letu 2018 je razkrila, da kar 44% od skupno pregledanih 382 izdelkov, ki vsebujejo morske sadeže, ni bilo ustrezno označenih. V našem medijskem prostoru so v zadnjih letih predvsem odmevala ugibanja povezana z nejasnim izvorom briških češenj [9] ter goljufije povezane s prodajo sadja in zelenjave iz integrirane pridelave iz tujine na lokalnih tržnicah pod oznako lokalno pridelane hrane [10]. Pridobivanje zaupanja potrošnikov v ponujene prehranske izdelke prestavlja eden izmed ključnih ciljev pridelovalcev in trgovcev prehranskih izdelkov [2], [11].

V odgovor na omajano zaupanje v prehranske verige, potrošniki čedalje bolj prepoznavajo pomembno vrednost lokalno pridelane prehrane v kratkih oskrbovalnih verigah. Za potrošnike je ključna tudi transparentnost samega procesa pridelave. Potrošnikom prikimava tudi Evropska komisija v Skupni kmetijski politiki [12], v kateri ob splošni trajnostni naravnanosti pridelave hrane poudarja tudi pomembnost krepljenja sistemov lokalne pridelave hrane in izboljšanje položaja pridelovalcev v vrednostnih verigah. Potrošniki posledično od predelovalcev pričakujejo jasen vpogled v podatke o varnosti izdelkov, njihovi kakovosti in trajnostni naravnanosti njihove pridelave [1]. Raziskava navad potrošnikov opravljena v letu 2016 razkriva, da je za 94 % potrošnikov pomembna transparentnost pridelovalcev pri procesu pridelave živil, ki jih ti kupujejo [8]. Še več, za hrano, katere poreklo in način pridelava sta jasni in transparentni, so pripravljeni plačati več.

Učinkovitost informiranja potrošnikov o posameznih prehranskih izdelkih predstavlja ključni vzvod, ki je tesno povezan s pridobivanjem njihovega zaupanja. Slednje predstavlja odločilni dejavnik tudi za dosego višje stopnje uspešnosti v verigi pridelave hrane v splošnem [13]. Izkaže se, da utečeni sistemi sledljivosti živil ne zagotavljajo konsistentnega in zadostnega pretoka informacij vzdolž prehrambnih verig [14]. V odgovor na kompleksnost sodobnih dobavnih verig se pojavlja potreba po razvoju naprednejših in učinkovitejših rešitev za sledenje prehranskim produktom, ki nadgrajujejo obstoječe sheme evidentiranja in označevanja prehranskih produktov izvedenih z oznakami odtisnjenih na embalaži izdelka. Napredek v informacijskih in komunikacijskih tehnologijah odpira vrata novih načinom sledenja produktom v prehranski verigi, ki so zmožni potrošnikom ponuditi hitri in transparentni način vpogleda v poreklo in procese pridelave hrane. Predvsem v zadnjih letih je bila kot ena izmed pomembnih prebojnih tehnologij na omenjenem področju prepoznana tehnologija veriženja blokov [1]. Za razliko od centraliziranih informacijskih rešitev, katerim primanjkuje učinkovitosti pri zagotavljanju transparentnosti informacij ter podpore sodelovanju in zaupanju med akterji [15], [16], ponujajo informacijske rešitve temelječe na tehnologijah veriženja blokov učinkoviti pristop k reševanju navedenih aktualnih izzivov v prehranski industriji. V nadaljevanju prestavimo zasnovo prototipa tovrstne programske rešitve, namenjene sledenju lokalno pridelanih prehranskih produktov.

2 VPELJAVA TEHNOLOGIJ VERIŽENJA BLOKOV

Za dosego večje transparentnosti glede izvora prehranskih izdelkov, morajo akterji v prehranski verigi učinkovito izmenjati relevantne podatke, ki utemeljujejo deklarirano kakovost in poreklo produktov [1]. V odziv na aktualne potrebe in želje potrošnikov, so podjetja začela prostovoljno investirati v napredne rešitve sledenja izdelkom v prehrambnih verigah, ki ponujajo natančen vpogled v podatke o sledljivosti. Takšna izmenjava podatkov sicer močno presegajo obseg, ki ga predpisujejo zakonodajalci [17]. Tehnologije veriženja blokov skupaj z nekaterimi drugimi sodobnimi tehnologijami in pristopi, kot so pametne pogodbe in decentralizirana zasnova aplikacij, ponujajo številne možnosti za izgradnjo programskih rešitev, ki so odporne na manipuliranje zapisov o lastnostih produktov ali njihovo cenzuro izvedeno s strani katerega izmed akterjev vključenega v oskrbovalno prehransko verigo.

2.1 Tehnologije veriženja blokov

Čeprav sloves tehnologij veriženja blokov primarno izhaja iz finančnega sektorja, je bila v zadnjih letih njena uporabnost uspešno demonstrirana na številnih domenah, vključno s sektorjem oskrbe s hrano. Pomembnejše domene, na katerih je bila demonstrirana uporabnost tehnologij veriženja blokov, so bančništvo, zavarovalništvo, delitvena ekonomija in medicina [18]. V domeni bančništva je kot primer uporabe tehnologij veriženja blokov zagotovo potrebno omeniti digitalno valuto Bitcoin in vrsto sorodnih platform digitalnih kovancev, ki se po njem zgledujejo. V zavarovalništvu so priložnosti tehnologij veriženja blokov kažejo predvsem v novih rešitvah pri zaznavanju in preprečevanju goljufij. Slednje omogoča odprtost, trajnost zapisov in enostavnost njihovega deljenja med zavarovalnicami. Tehnologije veriženja blokov so uporabljene tudi v programskih rešitvah iz domene medicine in zdravstvene nege, na primer pri zagotavljanju transparentnosti dobavne verige ali preverjanju ustrezne kvalificiranosti zdravstvenega osebja.

Uspeh tehnologij veriženja blokov primarno izhaja iz njihove podpore realizaciji programskih rešitev, ki jih odlikuje zanesljivost, transparentnost in nespremenljivost zapisanih podatkov [19]. Jedro tehnologij veriženja blokov predstavlja digitalna, decentralizirana in porazdeljena hramba podatkov, v katero je mogoče zapisovati transakcije s ciljem ustvariti trajen in pred kasnejšimi manipulacijami varen zapis [20]. To se doseže s kriptografskim podpisovanjem vsakršne posamezne transakcije. Ob podpori tovrstnih tehnologij lahko dogodke, ki se zgodijo tekom potovanja prehranskih izdelkov po prehrambni verigi, v obliki transakcij dodajamo v časovno urejene zapise verige blokov [16]. Hramba podatkov izvedenih transakcij je organizirana v med seboj povezane podatkovne bloke, preko katerih je omogočen njihov prenos, obdelava, hranjenje in predstavitev v ljudem berljivi obliki. Ker gre pri tehnologiji veriženja blokov za t. i. način shranjevanja »samo-za-dodajanje« (ang. append-only), se le ta naslavlja tudi kot tehnologija glavne knjige (ang. ledger), katere terminologija se črpa iz ekonomskih okvirjev, kjer se zapisi transakcij nikoli ne brišejo ali posodabljajo, temveč se za namene vodenja celovite sledljivosti sprememb zgolj dodajajo informacije o spremembah.

Zaradi porazdeljenega načina shranjevanja transakcij je nujno potrebno omrežje vozlišč, ki hrambo transakcij v celoti podvoji med slehernim vozliščem omrežja. Ker so si vozlišča v omrežju enakovredna in avtonomna, imenujemo omrežje decentralizirano, kar posledično pomeni, da se omrežje ne zanaša na zaupanja vredno tretjo/centralno stran [21]. Vsakemu ustvarjenemu bloku je glede na vsebino, ki jo nosi, izračunana zgoščevalna vrednost (angl. hash), na katero se blok sklicuje. Slednje daje konceptu osnovo za zagotavljanje integritete zapisanih podatkov. Vsaka kasnejša manipulacija vsebine podatkovnih blokov tako ne bi mogla ostati neopažena, saj manipulacijo razkrije neskladje izračunane zgoščevalne vrednosti bloka z njegovo zgoščevalno vrednostjo zapisano v sledeči blok [21].

Zapisi o kakovostnih atributih in poreklu prehranskih izdelkov, zapisani v verige blokov, so posledično odporni proti kasnejšim manipulacijam katerega koli akterja v oskrbovalni verigi, kar omogoča izgradnjo zaupanja v deklarirane podatke o izdelkih. S takšnim pristopom k varnosti in transparentnosti deljenih informacij je mogoče doseči bolj varno, transparentno in natančno izmenjavo podatkov.

Decentraliziranost in porazdeljenost, ki jih vpeljejo tovrstne programske rešitve, v praksi omogočita, da nobenemu izmed akterjev v prehranski oskrbovalni verigi ni potrebo prevzemati pobude za zbiranje in hrambo podatkov, saj se odgovornost enakomerno porazdeli med vse akterje. Posledično se tudi vzdržuje transparentnost in zaupanje, saj si nobeden izmed akterjev ne more prisvojiti prevlade nad omrežjem in zaradi tega kakorkoli spreminjati podatkov omrežja. Pomembno je poudariti, da vpeljava sledenja preko zapisov v verige blokov v nobenem pogledu ne nadomešča notranjih informacijskih sistemov posameznih akterjev v prehranski verigi, temveč jih zgolj dopolnjuje.

Pomembno komponento v naboru tehnologij veriženja blokov prestavljajo pametne pogodbe (ang. smart contracts). Te predstavljajo ključno razširitev tehnologij veriženja blokov [16], ki močno pripomore k uporabnosti tovrstnih tehnologij. Navedeno razširitev predstavlja doprinos platforme Ethereum tehnologijam veriženja blokov, zaradi katere se tovrstne tehnologije veriženja blokov v angleškem jeziku poimenujejo kar Blockchain 2.0. V grobem opišemo pametne pogodbe kot računalniški protokol, ki zagotavlja avtomatizirano elektronsko izvrševanje zapisanih določb v pogodbah, ki so definirane v programski logiki. Iz tehničnega vidika lahko pametne pogodbe

opišemo kot programsko kodo ali aplikacije, ki jih je mogoče namestiti v verigo blokov [22]. Ko so pametne pogodbe shranjene v verige blokov, pridobijo javno dostopni in znani unikatni naslov, ki omogoča, da se nanjo sklicujemo in jo prožimo. Sama izvedba pogodbe oz. programske logike se izvaja znotraj t. i. navideznih strojev vsakega posameznega vozlišča omrežja verig blokov, pri čemer se morebitne spremembe v stanju prav tako zabeležijo v verigo blokov. S tem se doseže, da so pametne pogodbe poštene, nespremenljive, avtomatizirane, varne in trajne [23].

2.2 Vpetost v ostale tehnologije

Tehnologije veriženja blokov predstavljajo osrednjo komponento naprednih programskih rešitev za sledenje izdelkom v prehranskih verigah, saj omogočijo decentralizirano in transparentno izmenjavo ključnih informacij preko javnodostopnega omrežja. Vendar tehnologije veriženja blokov same po sebi pri implementaciji učinkovitih programskih rešitev za sledenje izdelkom v prehranskih verigah niso dovolj. Dopolnjujemo jih s številnimi drugimi sodobnimi tehnologijami, zaradi katerih tovrstne rešitve dosežejo višjo stopnjo uporabnosti in boljšo sprejetost med uporabniki.

Za doseganje sledljivosti izdelkov v prehranskih verigah je ključno, da so ti ustrezno označeni čez celotno pot po prehranski verigi, torej od pridelave ali proizvodnje do končnega potrošnika. Za povečanje učinkovitosti sledenja izdelkov se običajno uporabi označevanje s QR kodami ali v zadnjih letih zaradi svoje zanesljivosti in učinkovitosti čedalje pogosteje uporabljenimi NFC in RFID značkami [14]. Prednost vpeljave RFID značk v primerjavi s tiskanimi črtnimi kodami ali QR kodami se kaže v hitrosti odčitavanja, možnostih njene avtomatizacije in doseganje višje produktivnosti [21], [24].

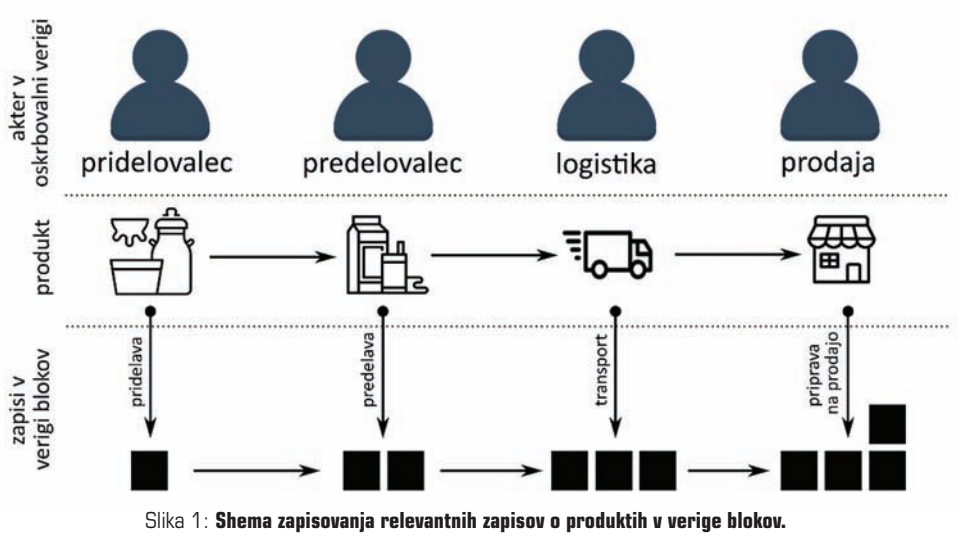
Pomemben prispevek k avtomatizaciji zajema relevantnih podatkov, preko katerih je zagotovljena transparentnost, predstavljajo tehnologije in rešitve povezave z internetom stvari (angl. Internet of Things). Slednje zajemajo širok spekter senzorjev in naprav za avtomatizirano zbiranje in prenos okoljskih podatkov. Primer uporabe tehnologij interneta stvari bi bilo zbiranje podatkov o temperaturi za vzdrževanje hladne verige pri prenosu temperaturno občutljivih izdelkov. Pretrganje hladne verige pri transportu tovrstnih izdelkov bi lahko imelo negative posledice na njihovo končno kakovost.

Ker verige blokov niso primerne za zapise večjih količin podatkov, kot smo to vajeni pri uporabi podatkovnih baz, so pri realizaciji rešitev ključne tehnologije, ki to omejitev verig blokov odpravljajo. Obseg zmožnosti količine zapisanih podatkov se glede na sorodne rešitve običajno razširi z vpeljavo datotečnega sistema, kot je npr. IPFS (angl. Interplanetary File System), ki vpeljuje protokol in omrežje P2P namenjeno porazdeljenemu hranjenju in deljenju datotek. Zapisi o prehranskih produktih so tako lahko porazdeljeni med verigami blokov in zapisi v datotečnih sistemih, pri čemer se poskrbi, da se s pomočjo kriptografskih pristopov ohrani varnost in integriteta zapisanih podatkov.

2.4 Vpliv tehnologij veriženja blokov na oskrbovalne verige

Pričakovanja glede pozitivnega vpliva vpeljave tehnologij veriženja blokov v prehranske verige so relativno visoka in zajemajo tako tehnološki, družbeni in ekonomski vidik napredka navedenega področja [1]. Od programskih rešitev namenjenih podpori sledenju in transparentnosti podatkov o produktih v prehranskih verigah se pričakuje množica lastnosti, ki bi jih naj tovrstne sodobne rešitve posedovale. Ključne lastnosti odličnosti rešitev v podpro sledljivosti prehranskih izdelkov so tako zagotavljanje sledljivosti izdelkov po celotni prehranski verigi, odprava centralizacije, podpora zaupanju med akterji, koordinacija in nadzor, skladnost z veljavnimi predpisi in čim nižja cena takšnega sledenja [25].

Kot enega izmed ključnih faktorjev kakovosti je prav gotovo potrebno izpostaviti sledljivost prehranskih produktov v verigi. Slednje se doseže z doslednim beleženjem stanja produktov, ki potujejo po verigi s strani vseh akterjev iz prehranske verige, ki so s produktom prišli v stik. Kakovost prehrambnega produkta določata dva ključna parametra, njegovo poreklo in kakovost pridelave ter ustreznost kasnejšega rokovanja z njim, ko ta potuje po prehranski verigi do potrošnikov. Na primer, za kakovost samega izdelka ob samem poreklu je ključnega pomena tudi zagotavljanje ustrezne obravnave med transportom. Neustrezni transport lahko tako hitro izniči vrednost visoke kakovosti pridelave ali porekla izdelka. Slika 1 prikazuje shemo zapisovanja relevantnih informacij o produktih v oskrbovalni verigi v verige blokov. Za zapisovanje podatkov so glede na fazo, v kateri se nahaja produkt odgovorni posamezni akterji oskrbovalne verige.



Slika 1: **Shema zapisovanja relevantnih zapisov o produktih v verige blokov.**

Dosledno zbrani in natančno zapisani podatki v prehranskih verigah imajo za končne potrošnike nizko vrednost, če ti podatkom ne zaupajo. Uporaba tehnologij veriženja blokov podpre zaupanje v zapisane podatke preko njihove nespremenljivosti, ki jo vpeljemo preko transakcij v decentralizirali in porazdeljeni arhitekturi [25]. Zapisi v verigi blokov so odporni proti kasnejšim manipulacijam, saj ne omogočajo naknadnega popravljanja ali njihovega izbrisa. Takšno zaupanje v zapise je doseženo s kriptografskimi pristopi in metodami vgrajenimi v protokol, s pomočjo katerih je napad na integriteto zapisov mogoče uspešno razkriti.

Pri zagotavljanju navedenih atributov kakovosti je seveda ključno, da so rešitve izvedene v skladu z vsemi veljavnimi standardi in predpisi, pri čemer se daje v zadnjih letih veliki poudarek na varstvu osebnih podatkov in zasebnosti akterjev.

2.5 Sorodne rešitve

Programske rešitve, ki vpeljujejo tehnologije veriženja blokov v domeno prehranskih verig, so zelo vezana na okolje, v katerem delujejo, in kontekst namena uporabe [1], [26]. V praksi to pomeni, da splošne programske rešitve, ki bi zadovoljile širok spekter uporabe trenutno ne obstajajo. Pogosto je potrebno izdelati prilagojene in specializirane rešitve, ki so prilagojene specifičnim potrebam poslovanja in uporabnikov. Ker je vpeljave tehnologij veriženja blokov v prehranske verige relativno nov pristop, se velika večina tovrstnih projektov, trenutno nahaja v fazah konceptualne zasnove, implementacije rešitve ali manjših pilotnih študij namenjenih dokazovanju ustreznosti zasnove koncepta. Nekaterim izmed zasnov se je sicer že uspelo prebiti v fazo delovanja v realnem okolju.

Eno izmed večjih podjetji, ki je v svoje delovne procese vpeljalo tehnologije veriženja blokov, je ameriška trgovska verige Walmart, ki je tehnologijo vpeljalo v oskrbovalne verige uvožene kitajske svinjine in mehiških mangov [27]. Izkušnje podjetja razkrijejo, da se je po vpeljavi tehnologij veriženja bloka dostopnost do podatkov o poreklu posameznih produktov bistveno izboljša, in sicer od prejšnjih nekaj dni s tradicionalnim pristopom poizvedovanj do vsega skupaj nekaj sekund z novim sistemom. Za podjetje je primarni cilj vpeljave tehnologij veriženja blokov izboljšati varnost hrane, saj je sedaj mogoče z natančnim beleženjem podatkov v vseh fazah oskrbovalne verige pripomoči k zagotavljanju zahtevanih higienskih standardov, tveganj, prevar in nenazadnje hitri identifikaciji oporečnih izdelkov. Vpeljava tehnologij veriženja blokov je v primeru podjetja Walmart vpeljana primarno za interne potrebe podjetja pri upravljanju odnosov s svojimi dobavitelji.

Francoski trgovec z živili Carrefour je vpeljal tehnologije veriženja blokov v svoje oskrbovalne verige z namenom izboljšanja integritete izdelkov, ki jih prodajajo na svojih policah [28]. Popolna sledljivost in transparentnost glede izvora živil in upoštevanja zahtevanja standardov je bila v oskrbovalne verige vpeljana z namenom ponuditi potrošnikom vpogled v izvor in poreklo izdelkov s ciljem dviga stopnje zaupanja potrošnikov v njihove izdelke. Potrošnikom je bila transparentnost oskrbovalnih verig omogočena za več vrst izdelkov, in sicer za meso, ribe, sadje,

zelenjavo in mlečne izdelke. Za podoben pristop k zagotavljanju integritete ponujenih izdelkov se je odločila pivovarna Down Stream [29], ki velja za prvo pivovarno, ki je svoji kupcem transparentno razkrila vse podatke o proizvedenem pivu. Konkretno so potrošnikom na voljo informacije o uporabljenih sestavinah in uporabljene metode varjenja piva.

Tehnologije veriženja blokov predstavljajo hrbtenico zagotavljanja integritete oskrbovalnih verig fundacije FairChain [30]. Temeljni cilj fundacije je vzpostavljanje oskrbovalnih verig, v katerih je zagotovljena transparentnost in enakopravnost vseh akterjev, pri čemer je močan poudarek na zagotavljanju pravične porazdelitve zaslužka med vsemi akterji v oskrbovalni verigi. Fundacija trenutno vzpostavlja pravične oskrbovalne verige za oskrbo s kavo in čokolado. Končnim kupcem navedenih izdelkov je tako omogočen vpogled v celotno pravično oskrbovalno verigo, s čimer se krepi njihovo zaupanje v prizadevanja in poslanstvo fundacije FairChain.

3 REŠITEV ZA SLEDENJE POREKLA IZDELKOV

3.1 Cilji in namen rešitve

Prototip rešitve ja nastal kot plod sodelovanja različnih partnerjev iz področja maloprodaje prehranskih produktov, razvoja inovativnih programskih rešitev in akademske sfere, pri čemer je naloga posameznega partnerja prispevati domensko znanje iz svojega področja, kar je bilo za implementacijo tovrstne rešitve nujno. Implementirana rešitev je v prvi fazi projekta namenjena podpori lokalne prodajalne svežega sezonskega sadja, zelenjave in drugih lokalnih pridelkov, pri čemer je namen razvite programske rešitve preko transparentnosti oskrbovalnih verig okrepiti zaupanje potrošnikov v integriteto ponujenih izdelkov. Poslovni cilj prodajalne je namreč potrošnikom ponuditi čim večjo izbiro lokalnih produktov slovenskih pridelovalcev, pri čemer ponujeni pridelki prepotujejo čim krajšo transportno pot med njivo in krožnikom ter tako ohranijo svežino, okus in visoko hranilno vrednost. Kupci ponujenih pridelkov in izdelkov so tako gospodinjstva kot večji odjemalci, ki skrbijo za preskrbo gostinskih lokalov in javnih zavodov. Lokalni slovenski izdelki so sicer del ponudbe, ne predstavljajo pa celotne ponudbe prodajalne. Posledično uporablja prodajno mesto jasne označevanje pridelkov in izdelkov z oznakami njihovega porekla.

Oznake porekla veljajo sicer za uveljavljeni in med potrošniki dobro sprejeti pristop označevanja izvora in kakovostnih značilnosti izdelkov. Glede na značilnost izdelka, ki ga označujejo, je v uporabi širok spekter oznak, med katerimi so nekatere v uporabi v ožjem geografskem področju, druge so prepoznane širše, na primer na področju Evropske unije. Med bolj prepoznavnimi in široko sprejetimi je zagotovo t. i. »evropski list«, ki označuje organsko pridelane izdelke. Izdelke lokalne pridelave naročnik označuje z oznako »lokalno.je«. Med pogosteje videnimi so še »zaščitena geografska označba« in označbe »evropske posebnosti«.

Osrednji cilj rešitve sledenja prehranskim izdelkom v kratki oskrbovalni verigi s pomočjo tehnologij veriženja blokov je razširiti uveljavljen pristop označevanja kakovosti in porekla izdelkov z oznakami oz. nalepkami, običajno odtisnjenih ali prilepljenih na embalažo izdelkov. S pomočjo vpeljave tehnologij veriženja blokov ob podpori drugih sodobnih informacijsko komunikacijskih tehnologij je mogoče potrošniku preko uporabe njegovega mobilnega telefona ponuditi natančen in povsem transparenten vpogled v poreklo izdelka ali uporabljene surovine in pristope, ki so bili uporabljeni za njegovo pridelavo oz. proizvodnjo. Zapisi v verigah blokov jasno pričajo tudi o dolžini prepotovane poti kot o porabljenemu času, ki ga je izdelek potreboval, da je dosegel košarico potrošnika. Glavni motiv je utrditi zaupanje potrošnikov v dejansko kakovost izdelkov s sicer v osnovi višjo dodano vrednostjo. Ob podpori sodobnih informacijsko telekomunikacijskih rešitev je mogoče osnovno sosledje dogodkov v oskrbovalni verigi izdelka zapisano v tekstovni obliki obogatiti z dodatnim multimedijskimi vsebinami, kot so slike in video posnetki, in tako ponuditi poglobljeno predstavo o uporabljenih procesih pridelave.

3.2 Podprte faze prehranskih oskrbovalnih verig

Implementacija prototipa programske rešitve za sledenje poreklu prehranskih izdelkov se upira na generični proces oskrbovalne verige, kot ga v svoji raziskavi predstavijo Caro et al. [31]. Glede na uporabljen procesni model oskrbovalne verige smo v prototipu programske rešitve podprli pet temeljnih akterjev, in sicer:

1. pridelovalca,
2. predelovalca,
3. distributerja,

4. prodajalca,
5. potrošnika.

Naloga pridelovalca v oskrbovalni verigi je poskrbeti za pridelavo primarnih pridelkov. Ti lahko potujejo po verigi navzdol neposredno ali jih predelovalci vmes predelajo v sekundarne prehranske produkte. Naloga distributerjev je poskrbeti za prenos prehranskih produktov med pridelovalci, predelovalci in trgovci in pri tem poskrbeti, da se kakovost izdelkov med transportom (čim bolj) ohrani. Naloga trgovec v oskrbovalni verigi je ponuditi produkte potrošnikom in jih omogočiti transparenten vpogled v zapise o izbranem izdelku iz oskrbovalne verige in ga podpreti pri odločanju o nakupu skladnem z njegovimi načeli.

Uporabljen model procesa oskrbovalne verige predstavlja posplošeno različico modela, v katerega so vključeni ključni akterji in faze, ki jih običajno srečamo v običajnih oskrbovalnih verigah. V literaturi je sicer mogoče zaslediti razširjene modele z dodatnim naborom akterjev, kot so regulatorji in avtoritete za certificiranje prehranskih proizvodov in proizvodnih procesov. Glede na uporabljen model predlagana implementacija rešitve prav tako ne vključuje ponudnika, naloga katerega je zagotoviti vstopne surovine uporabljene v delovnih procesih pridelave na kmetijah. Sicer pa zasnova prototipa omogoča možnost kasnejši dopolnitev implementacije modela.

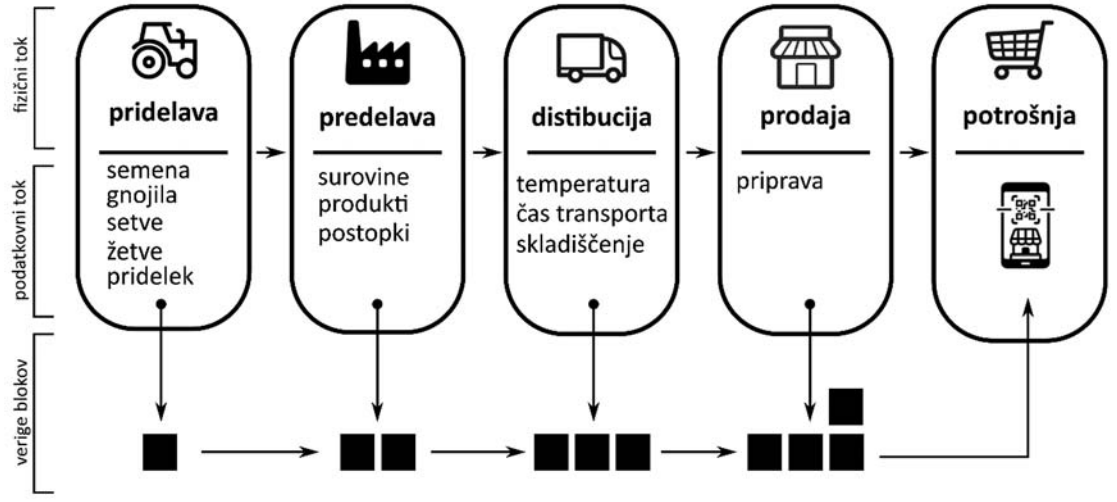
Posamezne vloge v modelu oskrbovalne verige je mogoče preslikati v faze prehranske oskrbovalne verige, znotraj katerih posamezni akterji aktivno delujejo. Model oskrbovalne verige z implementiranim procesnim in podatkovnim tokom in pripadajočimi zapisi v verige blokov prikazuje slika 2. Na podlagi izbranega modela smo v prototipu rešitve podprli sledeče faze:

1. **pridelava** – faza zajema vse kmetijske aktivnosti izvedene na kmetijah ali farmah. Za potrebe zagotavljanja transparentnosti pridelave je potrebno v začetni fazi natančno definirati način pridelave in morebitne surovine, ki so bile pri tem uporabljene. Ključni podatki, ki definirajo pridelavo, so lokacija pridelave, uporabljena škropiva in gnojila, poreklo in vrsta semen, način krmljenja živine. Slednje daje končnem potrošniku jasen vpogled v način pridelave, predvsem ko govorimo o ekološki pridelavi.
2. **predelava** – faza zajema vse delovne procese, v katerih iz primarnih pridelkov pridelanih v predhodni fazi, nastanejo novi sekundarni izdelki. Na primer, ekološka kmetija lahko iz ekološko pridelanega sadja pripravi marmelado. V tem primeru predstavljajo surovine za pripravo marmelade primarne sestavine, nastala marmelada pa sekundarni prehranski produkt. Vrednost dosežene kakovosti daje tem izdelkom uporaba kakovostnih primarnih sestavin in ustreznih tehnoloških procesov predelave. Oba vidika je potrebno upoštevati pri modeliranju zapisov v verige blokov.
3. **distribucija** – faza distribucije ne ustvarja ali spreminja produktov, temveč je njena ključna naloga, da poskrbi za izmenjavo produktov med ostalimi akterji v oskrbovalni verigi. Kljub temu ima izvedba distribucije pomembni vpliv na kakovost produktov. Neustrezno izvedena distribucija, pri kateri pogoji transport niso optimalni, zmanjša vrednost na začetku verige še tako kakovostnemu prehranskemu produktu.
4. **prodaja** - v fazi prodaje se izvede prevzem produktov in njihova priprava na prodajo. Pri tem je ključno, da se posamezne izdelke ustrezno opremi z oznakami, ki omogočajo potrošnikom vpogled v celotno pot produkta po prehranski oskrbovalni verigi.
5. **potrošnja** – v zadnji fazi oskrbovalne verige osredno vlogo prevzame potrošnik, ki izbira med razpoložljivimi produkti na podlagi osebnih preferenc in načel izbire živila na podlagi transparentno zapisanih sledi iz oskrbovalne verige izdelka.

3.3 Podatkovni model rešitve

Pomembna značilnost na tehnologijah veriženja blokov temelječih aplikacij, ki jo je potrebno vzeti v obzir pri načrtovanju podatkovnega modela, je javnost objavljenih zapisov. Vsi zapisi zapisani v verige blokov so namenjeni podpori transparentnosti, kar pomeni, da so javno dostopni in preverljivi. Pri načrtovanju podatkovnega modela je tako potrebno paziti, da podatkovni modeli na vsebujejo podatkov, objava katerih bi bila za posameznega akterja škodljiva. Iskanje ravnovesja med čim večjo stopnjo transparentnosti oskrbovalne verige in poslovnimi interesi sodelujočih akterjev ostaja ena izmed ključnih aktivnosti načrtovanja podatkovnega modela.

Namen in cilji uporabe prototipne rešitve skupaj z uporabljenim procesnim modelom oskrbovalnih verig dejejo jasen okvir podatkovnega modela, na podlagi katerega se za posamezni produkt v oskr-



Slika 2: **Shema faz in toka zbranih podatkov prehranskih oskrbovalnih verig.**

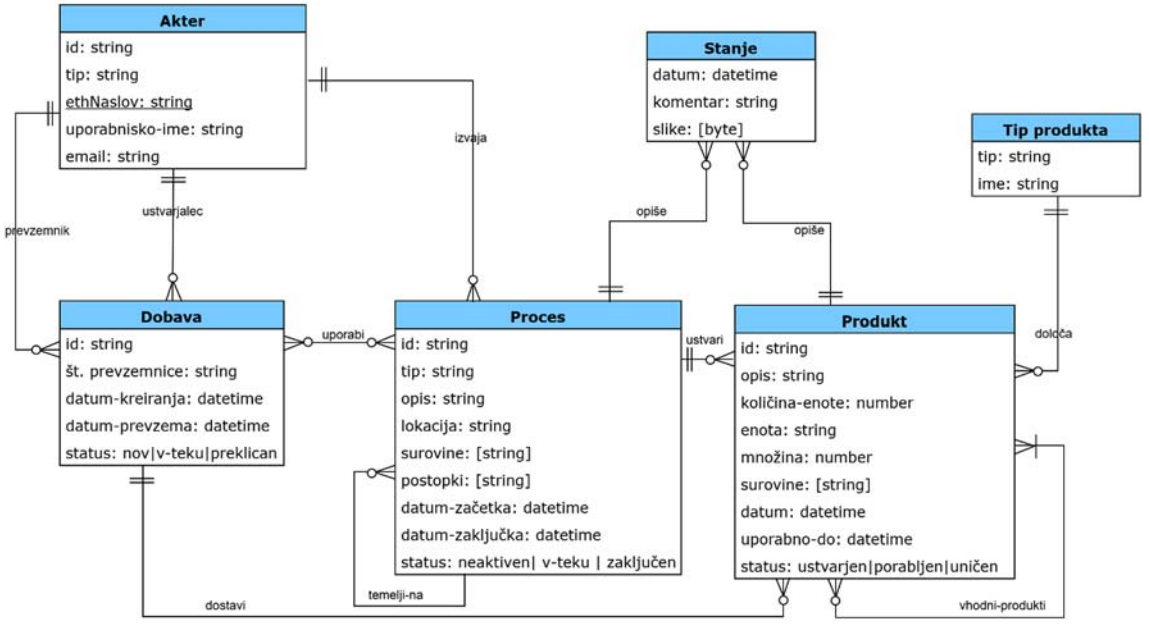
bovalni verigi zbirajo, obdelujejo in hranijo podatki. Podatkovni model uporabljen v prototipni rešitvi temelji na treh ključnih entitetah, s katerimi je mogoče opisati izvor, kakovost in obdelavo prehranskih izdelkov v prehranski oskrbovalni verigi, in sicer med pridelovalcev in potrošnikom. Ključne entitete, na katerih sloni podatkovni model rešitve, so naslednje:

1. **produkt** – definira količino prehranskega produkta izbranega tipa, ki tvori zaključeno enoto in ji je mogoče slediti po prehranski verigi. Ključni namen entitete je opisati osnovne atribute kakovosti produkta. Za sledljivost je nujno zagotoviti poenoteno označevanje produktov, saj produktov z različnimi kakovostnimi atributi ali poreklom ni dovoljeno mešati.
2. **proces** – opisuje lastnosti in načine obdelav, uporabljenih v oskrbovalni verigi za pridelavo, predelavo ali transport prehranskih produktov. Ključni procesi, ki se pojavijo v prehranski verigi, so setve, žetve, trgatve ter množica drugih obdelav, pri katerih se primarni pridelki predelajo v sekundarne živilske produkte. Ključne lastnosti procesov opisujejo način obdelave surovin in pri tem uporabljene temeljne surovine, kot so semena, gnojila ali krma, z vplivom na končno kakovosti prehranskih produktov. Procesi obdelave predstavljajo pomemben vidik kakovosti prehranskega produkta, saj opišejo način njihove pridelave.
3. **dobava** – opisuje in sledi predajam sledljivih prehranskih produktov med različnimi akterji v prehranski verigi in lastnosti okolja, ki zagotavljajo ohranitev kakovosti produktov. Sledenje predajam med akterji v prehranski verigi ustvarja sled, preko katere je mogoče potrditi poreklo prehranskega produkta.

Podatkovni model, ki ga prikazuje slika 3, vsebuje še nekatere pomožne entitete. Entiteta »Stanje« opisuje stanje produkta ali procesa v izbrani časovni točki. V podporo večji transparentnosti je preko stanja mogoče prehranskem produktu ali uporabljenem procesu pripeti tudi slikovno gradivo, ki služi kot dokaz odličnosti.

Entiteta »Produkt« je realizirana kot deljiva količina blaga, ki jo je mogoče, če je to seveda smiselno, s transformacijo razbiti na več manjših enot. Te so v podatkovnem zapisu zapisani kot novi produkti, ki temeljijo na izhodiščnem starševskem produktu zapisanem v atributu »vhodni-produkti«. Starševskem produktu, ki je bil razbiti na eno ali več manjših enot, se spremeni status v »porabljen«. Slednje nakazuje, da v obliki, kot je bil izvorno definiran, produkt zaradi transformacije več ne obstaja in ga v nadaljevanju več ni mogoče uporabljati. Transformacijo po istem mehanizmu je prav tako mogoče uporabiti v primeru, ko je produkt tekom nekega procesa transformiran v drugi produkt. Količinska pravilnost in smiselnost deljenja produktov pri transformacijah je sicer prepuščena uporabnikom sistema, ki za zapisane podatke tudi jamčijo.

Ključna lastnost zastavljene zasnove podatkovnega modela je njegova splošnost. Zastavljen podatkovni model je dovolj splošen, da ga bo mogoče kasneje enostavno vzdrževati in prilagajati konkret-



Slika 3: **Logični entiteto-relacijski model oskrbovalne verige.**

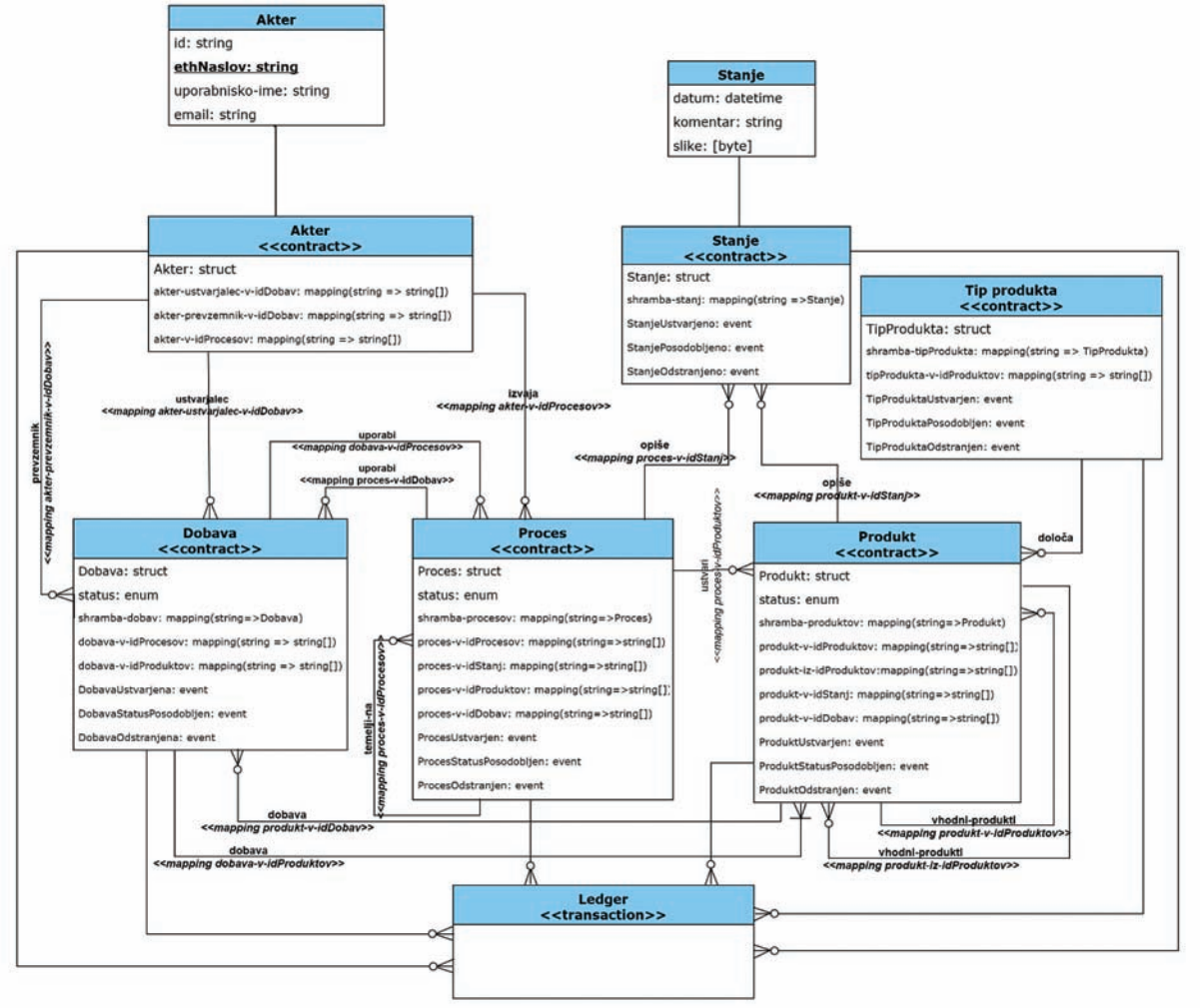
nemu namenu uporabe. Slednje omogoča visoka stopnja abstrakcije entitet podatkovnega modela in dinamičnost atributov, ki jih posamezne entitete podatkovnega modela hranijo. Osnovni nabor atributov uporabljenih entitet je zastavljen minimalistično. Zapisi v verigah blokov so namenjeni vsem akterjem v prehranski verigi, pri čemer sta osnovna cilja, ki ju zasledujemo, sledljivost in transparentnost. Izbira nabora zapisanih podatkov mora torej zasledovati zgolj navedena cilja. Nabori podatkov, ki ne podpirajo navedenih ciljev, se obdelujejo centralizirano v okviru domen posameznih akterjev.

3.4 Pretvorba v logični podatkovni model

Predhodno definiran visokonivojski konceptualni model rešitve je potrebno v nadaljevanju pretvoriti v logični podatkovni model, ki konceptualnemu modelu rešitve doda dodatne tehnične informacije. ER model kot tak je primeren za uporabo nad relacijskimi podatkovnimi bazami, ni pa primeren za uporabo v verigah blokov. Upoštevati je potrebno, da bo hramba podatkov, ki jih uporablja predstavljen prototip programske rešitve, razdeljena med lokalno podatkovno bazo in verigo blokov in s tem povezanimi pametnimi pogodbami. Pri metodi pretvorbe ER modela v logični model, primeren za uporabo v verigah blokov, smo se oprli na predhodno delo avtorjev Rek in Turkanović [23], ki vpeljeta zaključen nabor razširitev tako za konceptualni kot logični podatkovni model. Končni logični model predlagane rešitve, ki je prilagojen uporabi v porazdeljenih okoljih verig blokov, prikazuje slika 4.

Pomembna razširitev ER modela, ki je posledica prilagajanja posebnostim verig blokov, predstavljajo entitete, na podlagi katerih so ustvarjene pametne pogodbe. Od lokalno hranjenih entitet se v modelu ločijo po dodatni anotaciji <<contract>>. Posebnost podatkovnih modelov aplikacij, ki temeljijo na verigah blokov, predstavljajo zabeležke transakcij glavne knjige, ki jih zberemo v dodani entiteti »Ledger« označeno z anotacijo <<transaction>>. V tej neodvisni entiteti so hranjene vse transakcije v verigi blokov. Naslovi v verigah blokov so na podatkovnem modelu označeni z odebeljeno in podčrtano pisavo in ima svoj lasten podatkovni tip, tj. »address«.

Pomembna razširitev logičnega podatkovnega modela predstavljajo razširitve entitet, ki izhajajo iz konceptov tehnologij veriženja blokov in uporabljenih programskih jezikov in jih sicer pri običajnih relacijskih podatkovnih bazah ne srečamo. Prvo takšno razširitev predstavljajo preslikave podatkovnih tipov (angl. mapping), ki omogočajo gradnjo seznama preslikav poljubnih podatkovnih tipov v druge poljubne podatkovne tipe. Naslovi v verigah blokov (angl. address) predstavljajo pomemben koncept, ki v določenih situacijah odigra vlogo zunanjih ključev.



Slika 4: **Predlagani logični model rešitve.**

Drugo pomembno razširitev predstavljajo dogodki (angl. event), ki definirajo dogodke, ki jih lahko odda proženje funkcij pametnih pogodb in se trajno zabeležijo v verigo blokov. Oba navedena dodatna koncepta podatkovnih modelov sta posledica posebnosti uporabe programskega jezika Solidity, in jih kot take drugje ne srečamo. Atributi entitet ER modela se sicer preslikajo v atribute strukture struct pametne pogodbe.

3.5 Implementacija pametnih pogodb

Na podlagi definicij entitet zastavljenega logičnega modela so bile izpeljane pametne pogodbe. Iz vsake izmed entitet logičnega modela, označeno z anotacijo <<contract>>, izpeljemo samostojno pametno pogodbo, ki definira strukturo in obdelavo definiranih podatkov v verigah blokov. Na podlagi logičnega modela rešitve predstavljenega v predhodnem poglavju izpeljemo šest pametnih pogodb.

Slika 5 prikazuje programsko kodo izseka implementacije pametne pogodbe izpeljano iz entitete »Proces«, kot jo določa njena zasnova definirana v logičnemu modelu programske rešitve. Izsek programske kode prikazuje osnovno strukturo pametnih pogodb implementirano v programskem jeziku Solidity. Element »contract« predstavlja ovojni element prikazane pametne pogodbe in najavi njeno definicijo. Vsebina elementa nadrobneje definira strukturo in obnašanje pametne pogodbe preko definicij naštevalnih tipov, struktur, dogodkov in funkcij. Strukture v pametni pogodbi definirajo nabor atributov in uporabljenih naštevalnih tipov, kot jih definira entiteta, iz katere pametna pogodba izhaja. Namen funkcij je definirati obnašanje obdelave podatkov

```
contract ProcessStorage {
    bytes32 public constant PROCESS_STORAGE_POSITION =
        keccak256("diamond.standard.process.storage");

    enum ProcessStatus {
        UNDEFINED,
        ACTIVE,
        COMPLETED
    }

    struct Process {
        uint256 processId;
        string processType;
        string description;
        string location;
        string[] rawMaterials;
        string[] procedures;
        uint256 startDate;
        uint256 endDate;
        ProcessStatus status;
        // References
        address user;
    }

    struct Processes {
        uint256[] processIds;
        mapping(uint256 => Process) processStore;
        mapping(uint256 => uint256[]) processToProductIds;
        mapping(uint256 => uint256[]) processToInfoIds;
        mapping(uint256 => uint256[]) processToDeliveryIds;
        mapping(uint256 => uint256[]) processToProcessIds;
    }

    function processStorage() internal pure returns (Processes storage prs) {
        bytes32 pos = PROCESS_STORAGE_POSITION;
        assembly {
            prs.slot := pos
        }
    }
}
```

Slika 5: **Izsek implementacije pametne pogodbe »ProcesStorage« skladno z definicijo enitete »Proces« iz logičnega modela**

hranjenih v atributih pametne pogodbe. Pomembno vlogo v pametnih pogodbah nosijo tudi dogodki, na katerih sloni obveščanje o dogajanju v verigi blokov. Programsko kodo z definicijo dogodkov vezanih na pametno pogodbo, ki izhaja iz entitete »Proces«, prikazuje slika 6.

3.6 Tehnološki sklad rešitve

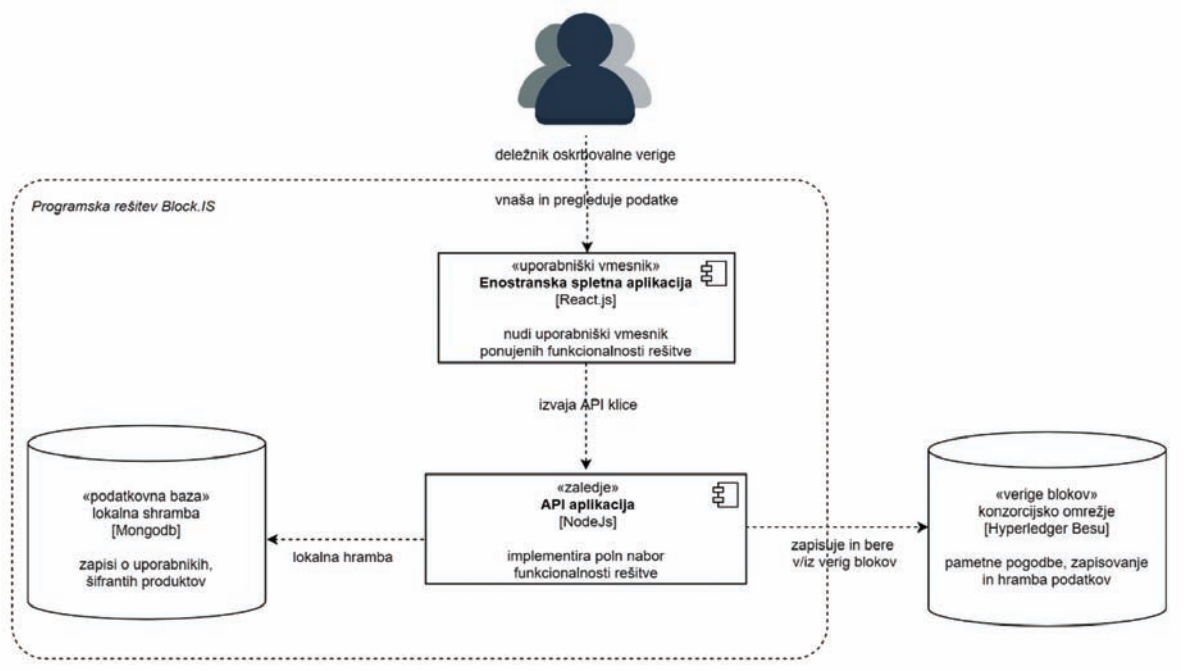
Da bi dosegli čim širši krog uporabnikov in enostavnost njegove uporabe je prototip implementiran kot hibridna mobilna aplikacija prilagojena uporabi tako na mobilnih napravah kot v brskalniku namiznih računalnikov. Za doseg končnih potrošnikov je ključnega pomena predvsem podpora mobilnim napravam. Kamera mobilne naprave uporabnikom omogoča skeniranje QR kod izdelkov, preko katerih enostavno dostopajo do sosledja dogodkov izdelka v prehranski oskrbovalni verigi.

```
pragma solidity 0.8.9;

import "./ProcessStorage.sol";

library ProcessLib {
    event ProcessCreated(
        uint256 processId,
        string processType,
        string description,
        string location,
        string[] rawMaterials,
        string[] procedures,
        ProcessStorage.ProcessStatus status
    );

    event ProcessStatusUpdated(
        uint256 processId,
        ProcessStorage.ProcessStatus status
    );

    event ProcessRemoved(uint256 processId);
}
```

Slika 6: **Programska koda dogodkov pametne pogodbe, ki izhajajo iz entitete »Proces«**

Pri zasnovi prototipa programske rešitve smo sledili trinivojski arhitekturi rešitve, pri katerem jasno razmejimo odgovornosti posameznega nivoja. Prototipna rešitev je implementirana po vzorcu odjemalce-strežnik, kar pomeni, da se obdelava uporabnikovih zahtev izvaja na zalednem strežniku. Najvišji nivo arhitekturne zasnove aplikacije predstavlja implementacija uporabniškega vmesnika. Ta je v osnovi implementiran s pomočjo knjižnice React.js [32] v programskem jeziku JavaScript. Funkcionalnosti rešitve, ki tečejo na strežniškem delu, so izpostavljene preko programskega vmesnika, zasnovanega po načelih arhitekture REST.

Prototipno aplikacijo od ostalih arhitekturno podobnih rešitev razlikuje predvsem implementacija podatkovnega nivoja. Za hranjenje podatkov se ne uporablja zgolj lokalna podatkovna baza, temveč se za delovanje aplikacije potrebni podatki berejo in zapisujejo v verige blokov preko pametnih pogodb. Podatkovni nivo predstavlja osrednjo komponento rešitve, ki nosi ključno poslovno logiko implementirano v okviru pametnih pogodb zapisanih v jeziku Solidity in omogoča navezavo na omrežje verig blokov. Zaradi optimizacije stroškov transakcij zapisov je namesto povsem javnega omrežja verig blokov bilo izbrano privatno konzorcijsko omrežje, ki temelji na programskem produktu Hyperledger Besu [33]. Za razliko od javnega omrežja Ethereum, v katerem se za izvrševanje transakcij zaračunava pristojbine, privatna konzorcijska omrežja omogočajo izvrševanje transakcij brez stroškov za končne uporabnike. Prav



Slika 7: **Shematski prikaz arhitekture programske rešitve.**

tako se z uporabo privatnih konzorcijskih omrežij izognemo stroškov s t. i. rudarjenjem, saj se v nasprotju z javnimi omrežji verig blokov, kjer se uporablja porazdeljen dogovor dokaz-o-delu (angl. proof of work), uporablja dokaz-o-avtoriteti (angl. proof of authority). Izbira tipa in načina delovanja omrežja verige blokov, ima torej pomemben vpliv na stroškovno upravičenost tovrstnega projekta.

Dosledno in transparentno sledenje dogodkom produktov v oskrbovalni verigi terja po obsegu veliko podatkov. Za razliko od klasičnih podatkovnih baz verige blokov same po sebi niso primerne hranjenju velikih količin podatkov, saj bi bilo takšno zapisovanje drago in časovno požrešno. Razkorak med za delovanje aplikacije potrebnim obsegom podatkov in omejitvami tehnologij veriženja blokov razrešimo s vpeljavo datotečnega sistema IPFS v arhitekturo rešitve. Podrobne podatke o kakovostnih atributih produktih v oskrbovalnih verigi, vključno s podatki o obdelavah, kot so sejanje, obiranje in predelave, hranimo v s strani za obdelavo pristojnega akterja digitalno podpisane JSON dokumente na javno dostopnem IPFS omrežju. V verige blokov tako zapišemo samo reference na podpisane JSON dokumente, kar ohrani tako transparentnost kot nespremenljivost zapisanih podatkov. Shematski prikaz arhitekture predstavljene programske rešitve povzema slika 7.

4 IZZIVI IMPLEMENTACIJE PROTOTIPA

Kljub številnim priložnostim, ki jih prinaša vpeljava tehnologij veriženja blokov v oskrbovalne verige, bo potrebno do njihove vpeljave v realna okolja rešiti še številne izzive. Do zdaj opravljene raziskave in preizkusi konceptov, ki jih je mogoče zaslediti v akademski in strokovni literaturi, so se osredotočali predvsem na demonstracijo tehnološke izvedljivosti zastavljenega koncepta. In vendar bo v prihodnje ob tehnoloških izzivih potrebno nasloviti tudi preostale zorne kote izvedljivosti zastavljenega koncepta.

Oskrbovalne prehranske verige predstavljajo okolja, v katerih sodeluje izjemno število različnih akterjev, ki vsak zase doprinesejo svoj delež k uspešnem delovanju oskrbovalnih verig. Da je zagotovljena natančna in nepretrgana sledljivost izdelkov, ki potujejo po oskrbovalni verigi, morajo pri soustvarjanju zapisov dosledno sodelovati vsi vključeni akterji. Ti morajo tudi prepoznati pomen tovrstnega početja, ki terja pri pridobivanju zaupanja končnih kupcev ponujenih prehranskih produktov vložek dodanega dela in truda.

Pri vpeljavi tovrstnih programskih rešitev je potrebno upoštevati tudi potrebo po pridobivanju dodatnih digitalnih veščin vključenih akterjev, ki jih pri svojem delu do sedaj niso potrebovali. Uporaba

programskih rešitev, ki temeljijo na tehnologijah veriženja blokov, med drugim od uporabnikov terja ustvarjanje in kasnejše rokovanje z uporabniku lastnimi pari zasebnih in javnih ključev. S pomočjo para javnega in zasebnega ključa je uporabnikom omogočeno zapisovanje podatkov v verige blokov in izkazovanje svoje istovetnosti nasploh. V strahu pred izgubo ključev se v mnogih primerih njihovo upravljanje prenaša na druge akterje ali sisteme, kar močno zmanjša varnost rešitev in smisel vpeljave tehnologij veriženja blokov nasploh.

Pogost je tudi strah pred javnim razkrivanje podatkov, ki jih zakonodajalec od akterjev v oskrbovalni verigi sicer ne zahteva. Vzpostavitev transparentih oskrbovalnih verig terja zaradi svoje kompleksnosti, vključenostih novih in še nepoznanih informacijskih tehnologij in vključenosti širokega nabora akterjev določen čas. Ugodni vplivi na zaupanje potrošnikov so zagotovo motivacija, da se bodo poiskali ustrezni odgovori tudi na netehnološke izzive, ki jih tovrstno sledenje prehranskim izdelkom prinaša.

5 SKLEP

Predstavljena zasnova prototipa programske rešitve v podporo sledenju lokalno pridelanim pridelkom in izdelkom v prehranski oskrbovalni verigi predstavlja potrditev koncepta uspešne vpeljave tehnologij veriženja blokov v oskrbovalne verige. Prototip pokaže tehnološko izvedljivost zasnove aplikacije, ki preko visoke stopnje transparentnosti dogajanja v prehranskih oskrbovalnih verigah pripomore k višji stopnji zaupanja potrošnikov v ponujene lokalne pridelke preko dokazovanja njihove integritete. Slednje se izkaže za ključno predvsem pri prehranskih izdelkih z višjo dodano vrednostjo, na primer lokalno ali ekološko pridelanimi živili ali prehranskimi izdelki z geografsko zaščitenim poreklom.

Tehnologije veriženja blokov ponujajo učinkovito platformo, s katero je mogoče doseči transparentnost in verodostojnost zapisanih podatkov. Ustvarjenih zapisov v verigah blokov kasneje več ni mogoče spreminjati, verodostojnost navedb o prehranskem izdelku pa je mogoče zaradi javne dostopnosti vedno preveriti. Decentralizirana zasnova obenem omogoča izgradnjo skupnosti med seboj enakovrednih in neodvisnih akterjev v oskrbovalni verigi, ki si skupaj prizadevajo pridobiti zaupanje potrošnikov. Tehnologije veriženja blokov sicer same po sebi ni bila dovolj za implementacijo tovrstnih programskih rešitev. Slednje je bilo skoraj nujno dopolniti s sodobnimi mobilnimi tehnologijami in tehnologijami v podporo označevanju izdelkov, s čimer se je dosegla prijetnejša uporabniška izkušnja uporabnikov rešitve.

Prikazan primer uporabe tovrstnih programskih produktov pri oskrbi z lokalno pridelanim sadjem in zelenjavo demonstrira temeljne zmožnosti tehnologij veriženja blokov v prehranskih verigah. Prestavljena zasnova programske rešitve je seveda mogoče uporabiti na mnogo kompleksnejših primerih izven okolja lokalne skupnosti. Produktom v verigah blokov se na primer lahko pripne digitalne certifikate, ki dokazujejo njihovo geografsko poreklo ali uporabo standardiziranih postopkov pridelave pridelkov oz. njihove kasnejše predelave.

ZAHVALA

Raziskovalni program št. P2-0057 je sofinancirala Javna agencija za raziskovalno dejavnost Republike Slovenije iz državnega proračuna. Za domensko znanje in ekosistem za razvoj omenjenih rešitev gre zahvala Zeleni točki, kakor tudi ITC Murska Sobota ter DIH AGRIFOOD.

LITERATURA

[1] K. Behnke in M. F. W. H. A. Janssen, »Boundary conditions for traceability in food supply chains using blockchain technology», *Int. J. Inf. Manage*., let. 52, str. 101969, jun. 2020.

[2] M. Garaus in H. Treiblmaier, »The influence of blockchain-based food traceability on retailer choice: The mediating role of trust», *Food Control*, let. 129, str. 108082, nov. 2021.

[3] U. Lehtinen, »Sustainable Supply Chain Management in Agri-food Chains», *Sustain. Challenges Agrofood Sect*., str. 150–174, feb. 2017.

[4] S. Köhler in M. Pizzol, »Technology assessment of blockchain-based technologies in the food supply chain», *J. Clean. Prod.*, let. 269, okt. 2020.

[5] S. A. Abeyratne in R. P. Monfared, »Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger«, *Int. J. Res. Eng. Technol.*, let. 05, št. 09, str. 1–10, sep. 2016.

[6] S. Stranieri, F. Riccardi, M. P. M. Meuwissen, in C. Soregaroli, »Exploring the impact of blockchain on the performance of agri-food supply chains«, *Food Control*, let. 119, str. 107495, jan. 2021.

[7] J. Yan, S. W. Erasmus, M. Aguilera Toro, H. Huang, in S. M. van Ruth, »Food fraud: Assessing fraud vulnerability in the extra virgin olive oil supply chain«, *Food Control*, let. 111, maj 2020.

[8] J. Astill idr., »Transparency in food supply chains: A review of enabling technology solutions«, *Trends Food Sci. Technol*., let. 91, str. 240–247, sep. 2019.

[9] »'Briške češnje' so še znamka, vredna ponarejanja«. [Na spletu]. Dostopno: https://www.rtvslo.si/radio-koper/prispevki/novice/briske-cesnje-so-se-znamka-vredna-ponarejanja/456296.

[10] E. Carl, »Tržaška veletržnica: najplodnejša njiva slovenskih kmetov«, 2013. [Na spletu]. Dostopno: https://www.rtvslo.

si/okolje/trzaska-veletrznica-najplodnejsa-njiva-slovenskih--kmetov/312530.
[11] E. Garbarino in M. S. Johnson, »The different roles of satisfaction, trust, and commitment in customer relationships«, *J. Mark.*, let. 63, št. 2, str. 70–87, 1999.
[12] »Skupna kmetijska politika 2023-2027«. [Na spletu]. Dostopno: https://www.gov.si/zbirke/projekti-in-programi/skupna--kmetijska-politika-po-letu-2020/. [Dostopano: 17-mar-2022].
[13] »With natural capital and trust, Canada can become an agrifood powerhouse«. [Na spletu]. Dostopno: https://www.theglobeandmail.com/report-on-business/rob-commentary/with-capital-and-trust-canada-can-become-an-agrifood--powerhouse/article30989002/. [Dostopano: 17-mar-2022].
[14] R. Badia-Melis, P. Mishra, in L. Ruiz-García, »Food traceability: New trends and recent advances. A review«, *Food Control*, let. 57, str. 393–401, nov. 2015.
[15] M. el Maouchi, O. Ersoy, in Z. Erkin, »TRADE : A Transparent, Decentralized Traceability System for the Supply Chain«, *Proc. 1st ERCIM Blockchain Work. 2018. Eur. Soc. Soc. Embed. Technol*. (EUSSET), št. 10, str. 1–8, 2018.
[16] J. Sunny, N. Undralla, in V. Madhusudanan Pillai, »Supply chain transparency through blockchain-based traceability: An overview with demonstration«, *Comput. Ind. Eng.*, let. 150, str. 106895, dec. 2020.
[17] A. Banterle in S. Stranieri, »The consequences of voluntary traceability system for supply chain relationships. An application of transaction cost economics«, *Food Policy*, let. 33, št. 6, str. 560–569, dec. 2008.
[18] A. Pazaitis, P. De Filippi, in V. Kostakis, »Blockchain and value systems in the sharing economy: The illustrative case of Backfeed«, *Technol. Forecast. Soc. Change*, let. 125, str. 105–115, dec. 2017.
[19] G. Mirabelli in V. Solina, »Blockchain and agricultural supply chains traceability: research trends and future challenges«, *Procedia Manuf.*, let. 42, str. 414–421, jan. 2020.
[20] H. Treiblmaier, »The impact of the blockchain on the supply chain: a theory-based research framework and a call for action«, *Supply Chain Manag.*, let. 23, št. 6, str. 545–559, nov. 2018.
[21] A. Kamilaris, A. Fonts, in F. X. Prenafeta-Boldú, »The rise of blockchain technology in agriculture and food supply chains«, *Trends in Food Science and Technology*, let. 91. Elsevier, str. 640–652, 01-sep-2019.
[22] »Ethereum«. [Na spletu]. Dostopno: https://ethereum.org/en/. [Dostopano: 19-apr-2022].
[23] P. Rek in M. Turkanovi, »Data modelling for Blockchain Oriented Software Engineering«, *Cent. Eur. Conf. Inf. Intell. Syst.*, str. 377–384, 2021.
[24] C. Costa, F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, in P. Menesatti, »A Review on Agri-food Supply Chain Traceability by Means of RFID Technology«, *Food Bioprocess Technol.*, let. 6, št. 2, str. 353–366, feb. 2013.
[25] S. Saurabh in K. Dey, »Blockchain technology adoption, architecture, and sustainable agri-food supply chains«, *J. Clean. Prod.*, let. 284, str. 124731, feb. 2021.
[26] M. M. Queiroz, R. Telles, in S. H. Bonilla, »Blockchain and supply chain management integration: a systematic review of the literature«, *Supply Chain Manag.*, let. 25, št. 2, str. 241–254, feb. 2020.
[27] A. Kamilaris, A. Kartakoullis, in F. X. Prenafeta-Boldú, »A review on the practice of big data analysis in agriculture«, *Comput. Electron. Agric.*, let. 143, str. 23–37, dec. 2017.
[28] »Food blockchain | Carrefour Group«. [Na spletu]. Dostopno: https://www.carrefour.com/en/group/food-transition/food--blockchain. [Dostopano: 22-mar-2022].
[29] »DOWNSTREAM | The World's 1st Blockchain Beer«. [Na spletu]. Dostopno: https://www.down-stream.io/. [Dostopano: 22-mar-2022].
[30] »FairChain Foundation – Returning production and profit to the countries of origin«. [Na spletu]. Dostopno: https://fairchain.org/. [Dostopano: 22-mar-2022].
[31] M. P. Caro, M. S. Ali, M. Vecchio, in R. Giaffreda, »Blockchain-based traceability in Agri-Food supply chain management: A practical implementation«, *2018 IoT Vert. Top. Summit Agric. - Tuscany, IOT Tuscany 2018*, str. 1–4, jun. 2018.
[32] »React – A JavaScript library for building user interfaces«. [Na spletu]. Dostopno: https://reactjs.org/. [Dostopano: 31-mar-2022].
[33] »Hyperledger Besu – Hyperledger Foundation«. [Na spletu]. Dostopno: https://www.hyperledger.org/use/besu. [Dostopano: 31-mar-2022].

▪

Mitja Gradišnik je raziskovalec na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Raziskovalno se ukvarja s sodobnimi pristopi pri razvoju programskih rešitev, kakovostjo in obvladovanjem staranja programskih produktov ter praktično uporabo metod podatkovnega rudarjenja v programskem inženirstvu. Raziskovalne in aplikativno sodeluje na več projektih, ki se odvijajo v okviru Inštituta za informatiko.

▪

Martin Domajnko je magistrski študent na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Ukvarja se z razvojem in raziskovanjem decentraliziranih aplikacij, tehnologije veriženja blokov in decentraliziranih digitalnih identitet ter je del raziskovalne skupine Blockchain Lab:UM Inštituta za informatiko.

▪

Muhamed Turkanović je visokošolski učitelj, izredni profesor, na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Je vodja raziskovalne skupine Blockchain Lab:UM Inštituta za informatiko, namestnik predstojnika Inštituta za informatiko, vodja slovenskega EDIH-a DIGI-SI, vodja Digitalnega inovacijskega stičišča Univerze v Mariboru, vodja projektov H2020, Horizont Evropa, Interreg Alpine Space ter ARRS CRP. Njegovi trenutni raziskovalni interesi vključujejo področja tehnologij veriženja blokov, podatkovnih tehnologij ter digitalnih identitet.

Priložnosti zlivanja tehnologij SIEM, SOAR in strojnega učenja v procesih inteligence tveganj in samodejnega odzivanja na kibernetske incidente

Andrej Bregar[1], Sašo Gjergjek[1], Miran Novak[2], Damir Orlić[1]
[1]Informatika d.o.o., Vetrinjska ulica 2, 2000 Maribor
[2]Melamin d.d., Tomšičeva cesta 9, 1330 Kočevje
andrej.bregar@informatika.si, saso.gjergjek@informatika.si, miran.novak@melamin.si, damir.orlic@informatika.si

Izvleček

V sodobnih informacijskih okoljih in sistemih, ki se selijo v oblak, temeljijo na konceptih interneta stvari in podpirajo avtomatizacijo poslovanja v kontekstu industrije 4.0, imamo opravka z masovnimi podatki in obsežnim omrežnim prometom med povezanimi napravami. V takšni količini podatkov si je nemogoče zamisliti zaznavanje anomalij, varnostnih tveganj in potencialnih kibernetskih incidentov brez avtomatiziranih pristopov, ki uporabljajo tehnike strojnega učenja in umetne inteligence. Ključne so zlasti tehnologije za upravljanje varnostnih informacij in dogodkov (SIEM) ter za avtomatizacijo, orkestriranje in odzivanje na kibernetska tveganja (SOAR). V članku pojasnimo, kaj pridobimo z vpeljavo postopkov in tehnologij za avtomatizacijo odzivov na kibernetske incidente. Umestimo jih v širši proces obravnave in reševanja incidentov ter v kontekst življenjskega cikla in primerov uporabe na področju inteligence varnostnih groženj in tveganj. Analiziramo možnosti uvajanja in neposredne integracije gradnikov tehnologij SIEM in SOAR kakor tudi vključevanja pristopov umetne inteligence za namen avtomatiziranega zaznavanja in orkestriranja kibernetskih incidentov. Preučimo učinke zlivanja in sinergije tehnologij SIEM, SOAR in strojnega učenja, hkrati pa se dotaknemo tistih organizacijskih in tehnoloških vidikov, ki odpirajo izzive, težave ter priložnosti. Izpostavimo tudi dobre prakse in pristope, ki jih vpeljujemo v sklopu kompetenčnega centra za kibernetsko varnost.

Ključne besede: avtomatizacija odzivanja na kibernetske incidente, inteligenca kibernetskih groženj in tveganj, kibernetska varnost, SIEM, SOAR, strojno učenje

Consolidation of SIEM, SOAR and machine learning technologies to enhance the processes of threat intelligence and automated cyber incident response

Abstract

Because contemporary information systems are moving to the cloud, utilise IoT (Internet of Things) and aim to automate business processes in the context of Industry 4.0, we have to deal with big data and heavy network traffic among interconnected devices. Such amounts of data require an automated approach to the identification of anomalies, cybersecurity risks and potential cybersecurity incidents on the basis of artificial intelligence and machine learning. In this regard, especially SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) technologies play a key role. In the paper, we explain the benefits of procedures and technologies for the automation of responses to cybersecurity incidents. We place these processes and technologies into the broader incident response approach as well as into the context of the cyber threat intelligence life cycle and use cases. We analyse the possibilities to apply, integrate and consolidate SIEM and SOAR technologies, and discuss how to use artificial intelligence and machine learning for the purpose of automated identification and orchestration of cybersecurity incidents. We review synergistic effects resulting from the integration and consolidation of SIEM, SOAR and machine learning,

while we also address several organisational and technological issues, challenges and opportunities. Finally, we describe certain good practices and approaches which are being introduced within the scope of our security operations centre for the energy utilities domain.

Keywords: incident response automation, cyber threat intelligence, cybersecurity, SIEM, SOAR, machine learning

1 UVOD

Področje zagotavljanja kibernetske varnosti v informacijskih okoljih in sistemih postaja vse bolj kompleksno. Na to vpliva več skupin dejavnikov, ki zajemajo pogostost, resnost in vpliv kibernetskih napadov, raznolikost in naprednost napadalskih tehnik, sofisticiranost vektorjev in motivov vdorov, vpetost varnosti in informatizacije v družbo ter v poslovne in upravljalske sisteme kakor tudi mnoge druge vidike. Število zaznanih kibernetskih incidentov tako iz leta v leto konstantno narašča, hkrati pa se sorazmerno povečuje obseg njihovih posledic. Glede na statistike (Freedman, 2020; Morgan, 2020) je bilo zgolj v prvem četrtletju leta 2021 zaznanih okoli milijon kibernetskih napadov in blizu 20 milijonov primerov zlonamerne kode. Povprečen strošek okrevanja od kibernetskega napada znaša 5 milijonov EUR za večje organizacije oziroma 50.000 EUR za manjša podjetja. Globalna ocena stroškov posledic kibernetskega kriminala naj bi do konca leta 2025 tako na letnem nivoju narasla na kar 10,5 bilijonov EUR. Poleg tega se je v letu 2020 z ogroženimi podatki ali omrežji soočalo 54 % podjetij, z izsiljevalskim programjem pa naj bi bil vsakih 11 sekund napaden en poslovni informacijski sistem.

Napadalci svoje zlonamerne programe razvijajo, da so ti čedalje bolj škodljivi, številnejši in raznolikejši, zaradi česar jih je težko odkriti. Uporabljajo tudi najrazličnejše pristope, metode in tehnike, da pridejo v sistem, v katerem povzročijo škodo. Ti pristopi vključujejo napade DDoS (Distributed Denial of Service), zlorabo prijavnih podatkov, izsiljevalsko programje, socialni inženiring, napade »zero-day«, DNS (Domain Name System) tuneliranje, napade na naprave IoT (Internet of Things) in druge. V zadnjem času smo celo priča avtomatiziranim, inteligentnim in naprednim napadom, ki jih napadalci načrtujejo na podlagi strojnega učenja in umetne inteligence. Tako je poznanih nekaj sofisticiranih napadov DDoS, pri katerih je omrežje napadalskih računalnikov (botnet) usmerjala umetna inteligenca (Jefferson, 2022). Čeprav si razvijalci varnostnih rešitev prizadevajo razviti boljše in kakovostnejše programske rešitve za obrambo pred kibernetskimi napadi, je varnostnim strokovnjakom, ki se trudijo zaznati in preprečiti kibernetske incidente, to zaradi vseh opisanih dejavnikov in raznolikih napadalskih pristopov zelo težko doseči. Dodatno njihovo nalogo otežuje velik obseg naprav, omrežnega prometa in varnostnih dogodkov, s katerim se soočamo v sodobnih informacijskih okoljih in sistemih, ki podpirajo avtomatizacijo celotnega poslovanja, se selijo v oblak in temeljijo na konceptih interneta stvari, zaradi česar imamo pri zagotavljanju kibernetske varnosti opravka z masovnimi podatki in obsežnim omrežnim prometom med povezanimi napravami. Da je zaznavanje kibernetskih incidentov in pravočasno odzivanje nanje zahtevna naloga, potrjujejo statistike o povprečnem času, ki preteče od incidenta do trenutka, ko varnostna skupina zazna ta incident, ter do trenutka, ko se nanj odzove. V letu 2021 je povprečni skupni izmerjeni čas 287 dni, od tega 212 dni za zaznavo incidenta in 75 dni za ukrepanje (IBM, 2021). Poraja se torej ključno vprašanje, ali je količina varnostnih dogodkov in incidentov v računalniških sistemih in omrežjih obvladljiva za varnostne analitike, v kolikor nimajo le-ti na voljo ustrezne, delno ali popolno avtomatizirane tehnološke podpore.

Eden ključnih dejavnikov za obseg, posledice in zapletenost kibernetskih napadov v sodobnih informacijskih okoljih in sistemih je velika odvisnost ljudi, družbe, držav in poslovnih okolij od informacijske tehnologije. To odvisnost narekuje vpetost v koncepte in tehnologije, kot so svetovni splet, oblačne storitve in tehnologije, internet stvari, industrija 4.0, informatizacija in avtomatizacija poslovnih procesov, elektronsko poslovanje, neprekinjeno poslovanje, storitve 24/7, oddaljeno delo in delo od doma, socialna omrežja, vrednost in zaupnost elektronskih osebnih in poslovnih podatkov, kritična infrastruktura idr. To pomeni, da pridobivajo uspešno izvedeni kibernetski napadi za napadalce vse večjo (škodljivo) vrednost. Posledica je porast kibernetskega kriminala, ki prinaša številna kibernetska tveganja in ranljivosti, ki obsegajo finančne izgube, zmanjšano konkurenčnost, zmanjšan tržni delež, sistemske izpade, osebno škodo posameznikov ter v hujših primerih

celo širše negativne in neželene socialne, politične in ekonomske učinke. Iz teh razlogov je obravnava kibernetskih groženj, tveganj in vdorov še toliko bolj kompleksna, saj so potencialni napadi vpeti v vsa področja družbe. In sicer se je na različnih nivojih potrebno soočiti z:

- napadi na kritično infrastrukturo in geopolitično motiviranimi napadi, ki so strateškega in političnega pomena ter so bili v preteklosti izvedeni na elektroenergetska omrežja (Ukrajina, ZDA), jedrske elektrarne (Iran, Indija), plinovode, zdravstvene ustanove in drugo infrastrukturo;
- napadi na podjetja in poslovne sisteme, ki predstavljajo gospodarski kriminal in so bili v preteklosti ciljani na številna podjetja, na primer na nemškega proizvajalca koles Canyon, ki posluje na osnovi spletno naravnanega poslovnega modela, zaradi česar je vdor povzročil zamude pri proizvodnji in dobavi ter nedostopnost sistema (Bracely, 2020);
- napadi na posameznike.

Preostanek članka sestoji iz petih poglavij. V drugem poglavju analiziramo in predstavimo zmožnosti, koncepte, pomen in pridobitve avtomatizacije zaznavanja kibernetskih incidentov in odzivanja nanje. Izpostavimo tudi izzive, težave, omejitve in priložnosti avtomatizacije. V tretjem poglavju opišemo tehnologije SIEM, SOAR in strojnega učenja v povezavi s postopki avtomatizacije zaznavanja in obravnave kibernetskih incidentov. Nato preučimo možnosti zlivanja, integracije in medsebojnega dopolnjevanja teh tehnologij. Četrto poglavje umesti tehnologije in postopke avtomatizacije v kontekst dveh pomembnih samostojnih področij – odzivanja na incidente (incident response) ter inteligence kibernetskih groženj in tveganj (threat intelligence). Pokazano je, kako lahko avtomatizacija izboljša učinkovitost postopkov v okviru teh dveh področij. V petem poglavju povzamemo, kako se področja avtomatizacije zaznavanja kibernetskih incidentov lotevamo v kompetenčnem centru za kibernetsko varnost za domeno energetike. Članek zaključuje šesto, sklepno poglavje.

2 AVTOMATIZACIJA ODZIVANJA NA KIBERNETSKE INCIDENTE

Zaradi dejstev, omejitev, težav in izzivov, opredeljenih v uvodnem poglavju prispevka, si je nemogoče zamisliti zaznavanje anomalij, varnostnih tveganj in potencialnih kibernetskih incidentov brez pomoči avtomatiziranih pristopov. Ključno vlogo tako dobivajo koncepti in postopki samodejnega zaznavanja kibernetskih incidentov in odzivanja nanje. V zadnjih letih zato stremimo k temu, da bi se odzivanje na kibernetske incidente avtomatiziralo na osnovi algoritmov, strojnega učenja in umetne inteligence, saj tudi napadalci pogosto uporabljajo avtomatizirana orodja za napade, kakršni so na primer napadi DDoS in napadi socialnega inženiringa.

Avtomatizirano odzivanje na kibernetske incidente pomeni, da organizacija dvigne nivo varnosti na podlagi boljših, močnejših in hitrejših ukrepov – algoritmov, strojnega učenja in umetne inteligence – v primeru kibernetskega napada ali druge kršitve varnosti in tako omeji učinek na poslovanje organizacije. Storitve avtomatiziranega odzivanja na incidente postajajo primarne in so bistvene za delovanje organizacij. S pomočjo teh storitev in postopkov lahko razbremenimo varnostno skupino, saj omogočajo samodejno zaznavanje kibernetskih groženj in incidentov ter odziv nanje. Poudariti pa je potrebno, da se kljub avtomatiziranemu procesu kaže zavedati, da je interakcija varnostih strokovnjakov še vedno potrebna.

Glavni namen vpeljave postopkov in tehnologij avtomatiziranega odzivanja na kibernetske incidente je razbremenitev varnostne skupine v organizaciji, kajti praktično nemogoče je spremljati in obdelati tako veliko število podatkov ter sprožiti najustreznejši odziv na vsako grožnjo. S pomočjo umetne inteligence ter zapisanih pravil in procesov, ki se izvajajo v realnem času, sistem zazna incident in nanj nato ustrezno reagira, zaradi česar je interakcija varnostnih strokovnjakov nujna le deloma oziroma v omejenem obsegu. Na podlagi tega se polni baza znanja sistema za nadaljnje ukrepanje ter odpravljanje varnostnih lukenj, s čimer se dvigne nivo varnosti. Tako tudi zmanjšujemo število lažno pozitivnih in lažno negativnih primerov. Ustrezna vpeljava učinkovitih postopkov in tehnologij za samodejno odzivanje na kibernetske incidente lahko doprinese k znižanju stroškov organizacije, čeprav je začetna investicija za avtomatizacijo nekaj večja. Če postopki in tehnologije niso pravilno vpeljani, pa lahko to povzroči škodo organizaciji, bodisi z vidika financ ali varnosti.

Z avtomatizacijo odzivov na kibernetske incidente lahko ukrepamo proti številnim težavam, ki jih prinaša kibernetska varnost v sodobnih kompleksnih informacijskih okoljih in sistemih. Če povza-

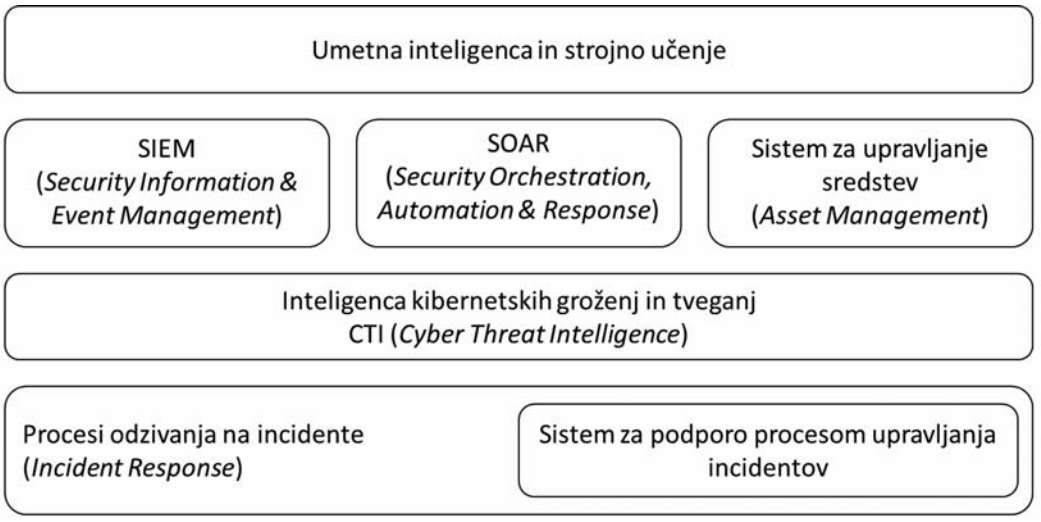
memo, lahko s temi ukrepi dosežemo mnoge prednosti. Mednje sodijo:

- razbremenitev varnostne skupine ter primarna osredotočenost analitikov na triažo in reševanje zahtevnejših forenzičnih primerov;
- avtomatizacija obravnave enostavnih in ponavljajočih se incidentov;
- povečanje učinkovitosti in uspešnosti procesov zaznavanja in obravnave kibernetskih groženj ter incidentov;
- standardizacija postopkov ukrepanja ob incidentih;
- zmanjšanje deleža lažno pozitivnih in lažno negativnih primerov;
- spremljanje in izboljševanje ključnih indikatorjev in kazalnikov učinkovitosti;
- gradnja in izboljševanje baze znanja o kibernetskih incidentih ter o novih vektorjih in oblikah napadov;
- zmožnost odkrivanja vzorcev v kibernetskih napadih in incidentih;
- poenotena in sistematična integracija informacijskih virov;
- obvladovanje velike množice naprav, virov in varnostnih dogodkov;
- optimizacija področja inteligence kibernetskih groženj in tveganj ter dvig udejanjanja tega področja na višji taktični nivo;
- zmožnost izkazovanja proaktivnosti, kar vključuje zavedanje širše varnostne slike v sistemu in izven njega, predvidevanje varnostnih tveganj in ranljivosti ter ukrepanje ob razpoznanih tveganjih, še preden ta preidejo v napade in incidente;
- boljša komunikacija in poročanje znotraj varnostne skupine.

Popolna avtomatizacija je v določenih primerih neizvedljiva ali neustrezna. Zato je smotrno analizirati in presoditi, kaj je smiselno avtomatizirati in na kateri stopnji. Pri tem je potrebno neodvisno obravnavati vsako fazo procesa zaznavanja kibernetskih incidentov in odzivanja nanje. Stopnjo avtomatizacije določimo za faze priprave, zaznavanja in obveščanja, triaže in analize, omejevanja in nevtralizacije ter aktivnosti po incidentu. Za določitev stopnje lahko uporabimo več metrik, kot so pričakovana korist avtomatizacije, tveganje, učinkovitost, cena ali zgodovina kazalnikov predhodnih avtomatizacij. Praviloma upoštevamo lestvico desetih stopenj avtomatizacije, ki je bila vpeljana že pred nekaj desetletji (Sheridan & Verplank, 1978) ter se razteza od prve stopnje popolnega človeškega nadzora do najvišje stopnje računalniškega odločanja. Stopnjo avtomatizacije lahko opišemo tudi po obsegu in po zrelosti. Po obsegu so na najvišjem nivoju avtomatizacije natančno specificirana in zapisana pravila avtomatizacije odziva, npr. v obliki postopka (playbook), ki pokrije tudi primere odhoda varnostnih analitikov iz podjetja. Po zrelosti pade pri omejeni avtomatizaciji večina bremena na uporabnika, zaradi česar težimo k pametni avtomatizaciji, ki pokriva triažo in zbiranje podatkov, ali zlasti k zreli avtomatizaciji, ki vključuje avtomatizacijo preiskave, proaktivni lov na grožnje ter napredne tehnike zbiranja in izkoriščanja podatkov.

Avtomatizacija odpira nekaj težav, pasti in izzivov. Prva potencialna težava je efekt »jo-jo«, katerega podlaga je, da je zaradi nerazumevanja razporeditve virov včasih lažje vzpostaviti model kot ga vzdrževati, saj viri niso potrebni le za načrtovanje, implementacijo in testiranje, temveč tudi za kasnejše vzdrževanje. Avtomatizacija se lahko zalomi tudi pri pooblastilih, organizaciji in modelu komuniciranja, zaradi česar je bistvenega pomena podpora vodstva. Ključne pasti in izzivi pa se skrivajo v pravnih in pogodbenih vidikih. To pomeni, da je potrebno nasloviti in pravno regulirati vprašanje krivde in odgovornosti za določene postopke. Kdo je namreč kriv, če zaradi samodejnega odziva sistema pride do izpada oziroma zastoja v produkciji (ker na primer požarni zid prekine vse komunikacije)? Dodatni vidik je dinamična stopnja avtomatizacije. V tem kontekstu lahko sistem zazna stanje in če je varnostna ekipa zasedena, je sam pooblaščen za določena avtomatizirana opravila. Če so analitiki na voljo, pa posreduje sistem le-tem potencialni incident v odločanje, s čimer se stopnja avtomatizacije dinamično zmanjša.

Za avtomatizacijo odzivanja na kibernetske incidente uporabimo sklad povezanih postopkov in tehnologij, ki jih prikazuje slika 1. Osnovni nivo so tehnike umetne inteligence in strojnega učenja, ki so integrirane v tehnologiji SIEM in SOAR. Za učinkovito upravljanje varnostnih dogodokov in omrežnega prometa na povezanih napravah neposredno integriramo tudi sistem za upravljanje sredstev. Te tehnologije nudijo podporo postopkom inteligence kibernetskih groženj in tveganj ter procesom odzivanja na incidente. Vsi gradniki so podrobneje opisani v nadaljevanju članka.



Slika 1: **Postopki in tehnologije za avtomatizacijo odzivanja na kibernetske incidente**

3 VPELJAVA TEHNOLOGIJ SIEM, SOAR IN STROJNEGA UČENJA

3.1 Umetna inteligenca in strojno učenje

Umetna inteligenca lahko olajša in pohitri delo s podatki ter pogosto najde vzorce v masovnih podatkih, ki jih sicer ne bi zasledili ali bi jih bilo možno opaziti le s težavo. Zato jo s pridom uporabljajo tako napadalci na eni strani (Jefferson, 2022) kot varnostni analitiki v varnostni skupini na drugi strani (Saini idr., 2020). Napadalcem omogoča načrtovanje naprednih in zapletenih vektorjev napadov ter samodejno proženje kibernetskih napadov, pri čemer je zmožna:

- identificirati potencialne programske ranljivosti sistemov s skeniranjem le-teh;
- analizirati vzorce obnašanja uporabnikov in delovanja informacijskih sistemov ter v skladu z ugotovljenimi vzorci predvideti uspešne vektorje napadov, npr. prepričljive izsiljevalske napade in socialni inženiring na podlagi značilnosti uporabnikov;
- usmerjati kibernetske napade s posnemanjem poznanih ljudi ali nadrejenega kadra na osnovi generiranja govora, teksta in/ali videa;
- analizirati učinkovitost pristopov in vektorjev napadov ter jih aktivno izboljševati;
- usmerjati omrežje napadalskih računalnikov (botnet) v sofisticiranih napadih DDoS.

Hkrati lahko tudi varnostna skupina uporabi metode umetne inteligence in strojnega učenja za razpoznavanje vzorcev običajnega in neobičajnega obnašanja uporabnikov ter delovanja IT sistemov. Ti vzorci opišejo značilnosti kibernetskih napadov, omogočajo zaznavanje anomalij in odstopanj ter pomenijo osnovo za predvidevanje kibernetskih napadov. S tem zagotovijo mehanizme za samodejno odzivanje in ukrepanje. Tako je tudi na strani varnostne ekipe eden osnovnih scenarijev uporabe algoritmov strojnega učenja zaznavanje napadov DDoS (Saini idr., 2020).

3.2 SIEM (Security Information and Event Management)

Sistem za upravljanje varnostnih informacij in dogodkov SIEM (Miller idr., 2010; Thomas, 2018) zagotavlja celovit prikaz omrežnega prometa varovanega okolja. Omogoča spremljanje varnostnih dogodkov v realnem času ter pregled in analiziranje za nazaj. Analizira dnevniške podatke (log) iz različnih sistemov, ki so povezani z njim, na primer aplikacijskih in spletnih strežnikov, strežnikov Linux in Windows, delovnih postaj, podatkovnih baz, aktivnih imenikov, požarnih pregrad, usmerjevalnikov, avtentikacijskih programov, programov za zaščito pred škodljivo in zlonamerno programsko opremo idr. Ko SIEM zazna potencialno grožnjo, proži opozorilo.

Sistem SIEM ima nekaj omejitev. Omejen je na razpoznavanje incidentov, ki so razvidni iz »logov«, kar pomeni, da ne zna prepoznati oziroma opisati incidentov iz drugih vrst virov (ki niso »logi«). Prav tako ni zmožen orkestrirati postopkov odziva na incidente. Predvsem pa ne povezuje, združuje in selek-

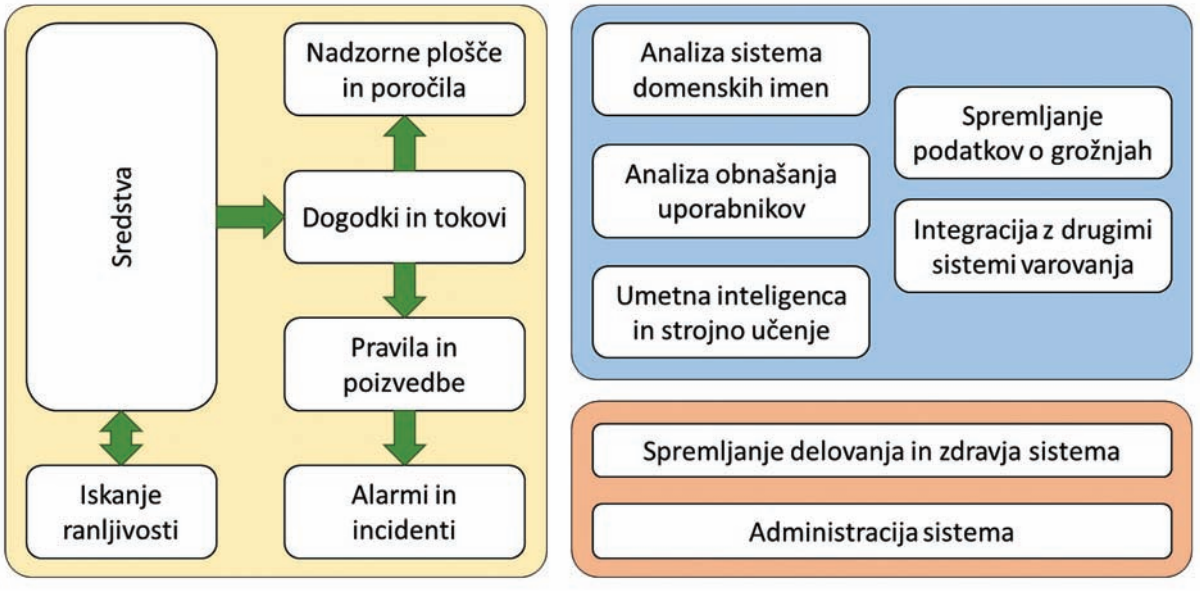
cionira sorodnih opozoril, zato lahko kot posledica (pre)velikega števila proženih opozoril pride do preobremenitve varnostne ekipe.

Sistem SIEM sestoji iz več gradnikov, ki so shematsko prikazani na sliki 2. Nekateri od njih (ne vsi!) v ozadju aplicirajo strojno logiko in umetno inteligenco ter jih lahko uporabimo za avtomatizirano odzivanje na kibernetske incidente. Eden relevantnejših gradnikov za namen avtomatiziranega odzivanja na kibernetske incidente je analiza vedenja uporabnikov (UBA – User Behaviour Analytics), ki razpoznava zlonamerne in tvegane uporabnike, nenavadne in neobičajne aktivnosti uporabnikov ter zlorabe uporabniških računov in pravic dostopa. Prav tako vključuje izračun ocen tveganosti uporabnikov na osnovi dnevniških zapisov njihovih aktivnosti. Naslednji pomembni gradniki so pravila, poizvedbe in referenčne množice, ki na podlagi evidentiranih varnostnih dogodkov in tokov izvedejo neko akcijo, denimo kreiranje opozorila ali incidenta. Dogodki in tokovi predstavljajo omrežni promet, ki ga sistem SIEM pridobiva iz različnih virov. Ker vseh dogodkov in tokov ni možno pregledati, je ključnega pomena avtomatizacija s pravili, ki omogoča samodejno zaznavanje sumljivih ali nevarnih kombinacij le-teh. Bolj ko zapolnimo bazo s pravili, poizvedbami in referenčnimi množicami, tem bolj izpopolnimo ozadje gradnikov, kar zagotavlja boljše in natančnejše delovanje. S tem zmanjšamo število lažno pozitivnih primerov. Pravilno konfigurirani gradniki sistema SIEM imajo velik vpliv na avtomatizirano odzivanje na kibernetske grožnje in incidente.

3.3 SOAR (Security Orchestration, Automation and Response)

Sistem za varnostno orkestracijo, avtomatizacijo in odzivanje SOAR (Bedell, 2019; Imam, 2019; Reichenberg, 2021) je enoten sistem oziroma platforma, ki združuje tri ključne funkcionalnosti, in sicer avtomatizacijo varnostnih operacij, odzivanje na varnostne incidente ter upravljanje groženj, tveganj in ranljivosti. Pri tem podpira štirifazni cikel zaznavanja incidentov, triaže, odzivanja in prioretizacije, v okviru katerega omogoča avtomatizacijo ponavljajočih se postopkov odzivanja na varnostne grožnje, standardizacijo odzivov na incidente ter prihranek časa varnostnega osebja za bolj pomembna in zahtevnejša opravila triaže.

Platforma SOAR je skupek varnostnih orodij in programov za zbiranje in obdelavo podatkov o grožnjah iz množice različnih virov, pri čemer uporabi človeško znanje, umetno inteligenco in strojno učenje z namenom analize podatkov ter prioretizacije aktivnosti v okviru postopkov odzivanja na incidente. Bistvena sta koreliranje in združevanje opozoril o zaznanih incidentih ter definicija odzivov v obliki natančno opisanih postopkov (playbook). Primer opisa takšnega postopka odziva v notaciji BPMN (Business Process Model and Notation) je razviden na sliki 3.



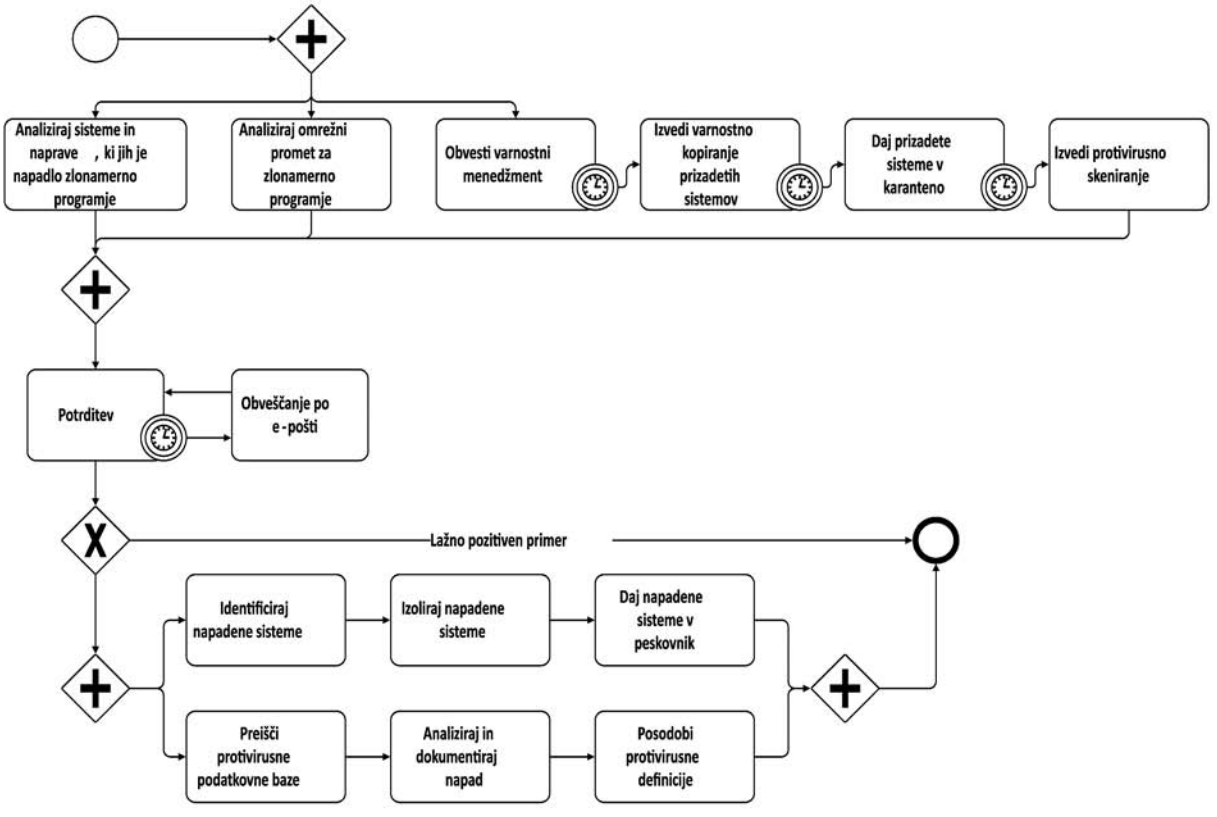
Slika 2: **Gradniki sistema SIEM**

Uporabo sistema SOAR lahko ponazorimo na primeru. Ko pride do poskusa vdora v sistem prek požarnega zidu iz nepooblaščenega IP (Internet Protocol) naslova s prijavo po metodi »brute force«, se najprej izvrši samodejna detekcija poskusa vdora, kateri sledijo operacije obveščanja varnostne ekipe, komunikacije s požarnim zidom in nazadnje samodejno blokiranje IP naslova. Podobnih scenarijev uporabe tehnologije SOAR je še nekaj. Med njimi so:

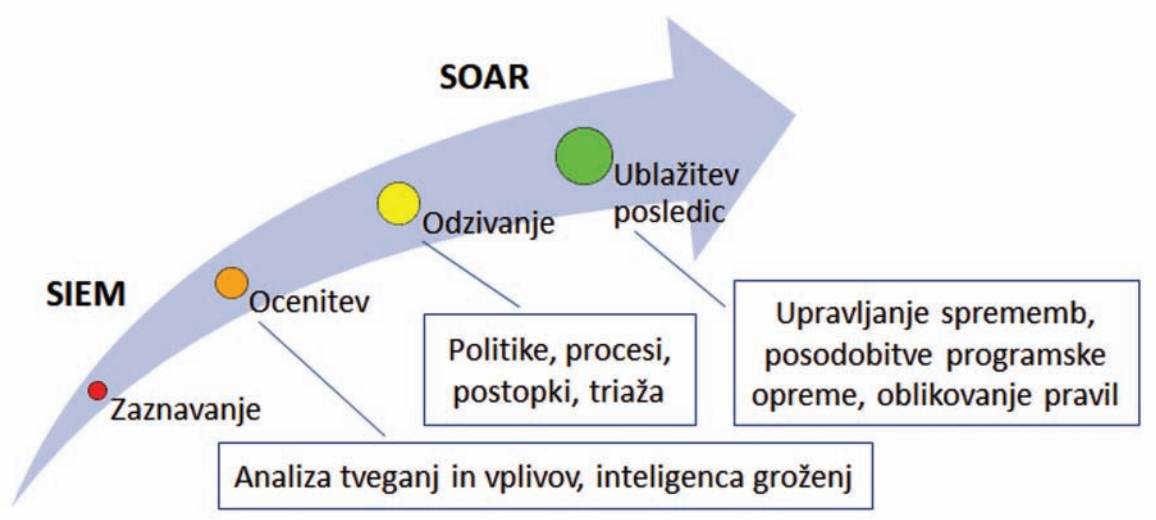
- »Ribarjenje«: Integracija tehnologije SOAR in inteligence groženj skrajša odzivni čas pri iskanju in obdelavi škodljivih informacij, prisotnih v zlonamerni e-pošti.
- Iskanje ranljivosti: Hekerji izkoriščajo ranljivosti za vdor, zato je iskanje ranljivosti ključno za obvladovanje tveganj. SOAR lahko izboljša iskanje in poročanje ranljivosti ter omogoči varnostni ekipi, da vpelje dodatne točke nadzora.
- Zlonamerni omrežni promet: SOAR lahko omogoči samodejno triažo zlonamernega omrežnega prometa na osnovi specifičnih vzorcev in indikatorjev.
- Ponudniki varnostnih storitev: SOAR je na podlagi analiz varnostnih podatkov, metrik in indikatorjev zmožen avtomatizirati ter orkestrirati akcije za zadostitev zahtevam SLA (Service Level Agreement).

Če povzamemo, so ključni koncepti tehnologije SOAR naslednji:

- orkestracija in avtomatizacija: jasno definirani postopki izvajanja varnostnih operacij na osnovi pridobljenih varnostnih podatkov;
- proučevanje groženj in upravljanje primerov: prioretizacija groženj z grupiranjem v skupne tipe/primere glede na sorodne značilnosti in medsebojne korelacije/povezave;
- okolje za varnostni operativni center: pregled opozoril, odzivanje, komunikacija in sodelovanje;
- poročanje in analiza: vpogled v varnostne trende.



Slika 3: **Primer postopka odziva (playbook)**



Slika 4: **Nivoji uporabe tehnologij SIEM in SOAR**

3.4 Zlivanje tehnologij SIEM in SOAR

Sistem SIEM pomaga pri zaznavanju groženj in incidentov na podlagi podatkov, ki se zbirajo iz aplikacij, sistemov in infrastrukture. Lahko sproži opozorila, vendar mora varnostna ekipa sama poskrbeti za odziv. Tehnologija SOAR pomaga oceniti resnost in lastnosti opozoril na podlagi varnostnih podatkov, se je zmožna samodejno odzvati na grožnje ter sledi aktualnim varnostnim trendom na podlagi inteligentne analize masovnih podatkov. Tehnologija SOAR tako nadgrajuje tehnologijo SIEM, vendar so funkcionalnosti slednje – zbiranje, analiziranje in poročanje o varnostnih dogodkih – še vedno osnova dela varnostnih analitikov in vsakega varnostnega operativnega centra. SIEM in SOAR sta tako komplementarni tehnologiji. SIEM predstavlja osnovo, SOAR pa dvigne učinkovitost varovanja in izkoristek virov na višji nivo, in sicer na podlagi razbremenitve ljudi od varnostnih opozoril, sprostitve kadrov, neposredne integracije različnih orodij na skupni enotni točki ter dobro definiranih procesov odzivanja in ukrepanja. Slika 4 povzema dopolnjujoče se nivoje uporabe tehnologij SIEM in SOAR. V tabeli 1 pa je podana neposredna primerjava glede na osnovne dejavnike (Reichenberg, 2021).

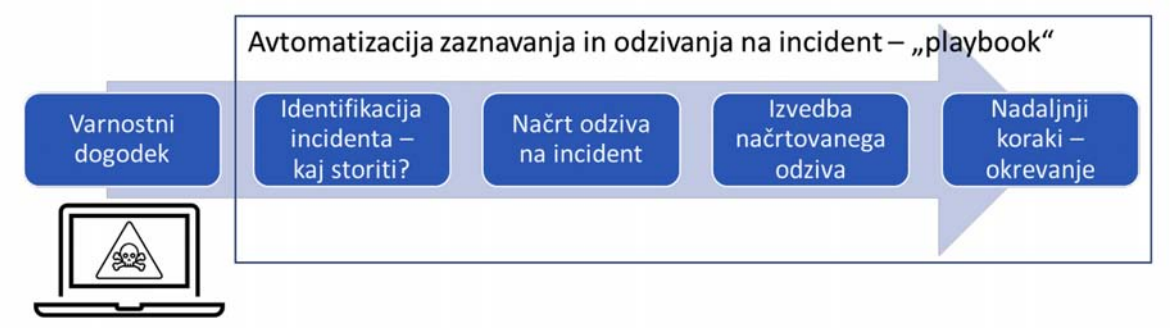
4 ODZIVANJE NA INCIDENTE IN INTELIGENCA GROŽENJ

4.1 Odzivanje na kibernetske incidente

Odzivanje na incidente (incident response) je eno temeljnih področij kibernetske varnosti, ki uvaja sistematične pristope k odpravljanju posledic napadov, incidentov in vdorov (Chai idr., 2022). Cilj je omejiti posledice kibernetskih napadov, skrajšati čas okrevanja in zmanjšati stroške. V praksi se velikokrat uporabljajo inteligentni pristopi k odzivanju na kibernetske incidente (Brown & Roberts, 2017). To pomeni, da proces odzivanja ni omejen zgolj na pripravo načrta odziva in izvedbo tega odziva na osnovi vzpostavljenega načrta, temveč je potrebno v okviru procesa analizirati in celostno razumeti informacije o napadu, identificirati napadalce ter spoznati njihove motive in vzorce delovanja. Za ta namen je ključna

Tabela 1: **Komplementarnost in primerjava tehnologij SIEM in SOAR**

	SIEM	**SOAR**
Namen	Informacije na osnovi varnostnih dogodkov in dnevniških zapisov	Analiza in inteligenca groženj z uporabo raznovrstnih orodij na enotni platformi (programi za zaščito pred zlonamerno kodo, upravljanje končnih točk, SIEM …)
Zmožnosti	Realnočasovna analiza varnostnih dogodkov	Definicija tokov in postopkov za odzivanje na incidente, standardizacija aktivnosti, izboljšanje sodelovanja
Podatkovni viri	Notranji viri, opozorila	Notranji in zunanji viri, avtomatizacija odzivov na opozorila



Slika 5: **Uporaba avtomatizacije in tehnologije SOAR v postopku odzivanja na incident**

avtomatizacija zaznavanja kibernetskih incidentov, zlasti v povezavi s tehnologijo SOAR. Kot kaže slika 5, sta lahko avtomatizacija in tehnologija SOAR tesno vpeti v splošni proces odzivanja na incidente, kakršnega opredeljujejo Chai idr. (2022). Ta proces znatno izboljšata in ga dvigneta na višji nivo. Zelo smotrno je tudi, da ju integriramo v vse tri stebre varnostnega operativnega centra, s čimer postaneta eni od bistvenih tehnologij, ključni sestavni del večine varnostnih postopkov in dejavnik podpore delu ljudi. Pri tem se morata vklopiti v življenjski cikel delovanja VOC (Kafol & Bregar, 2017).

4.2 Inteligenca kibernetskih groženj in tveganj

Inteligenca kibernetskih groženj in tveganj (threat intelligence) pomeni obdelavo informacij, ki jih organizacija uporabi, da bi razumela, kaj jo ogroža, jo je ali jo bo ogrožalo (Baker, 2022; Pace, 2018). Na podlagi teh informacij je organizacija zmožna identificirati tveganja, se pripraviti nanje in jih preprečiti. Pridobi namreč relevantno znanje o tveganjih, vzpostavi obrambne mehanizme in premosti tveganja, ki bi lahko ogrožala vire ter škodila njenemu poslovanju in ugledu.

Rešitve za inteligenco groženj in tveganj zbirajo, filtrirajo in analizirajo podatke o napadih in napadalcih, s katerimi pridemo v stik prek različnih virov in ki ogrožajo vire. Njihovi cilji so:

- biti »na tekočem« z množico groženj in tveganj, kar vključuje tudi metode in vektorje napadov, ranjivosti, cilje napadov in identifikacijo napadalcev;
- postati proaktiven v zvezi z grožnjami in tveganji na podlagi oblikovanja priporočil in postopkov za ukrepanje proti napadom;
- informirati o nedavnih in ponavljajočih se tveganjih ter posledicah za poslovanje.

SOAR in avtomatizacija zaznavanja kibernetskih incidentov predstavljata ključno tehnologijo za inteligenco kibernetskih groženj in tveganj, saj gradita bazo znanja ter avtomatizirata odzive, s tem pa izboljšata nivo, zmogljivost in učinkovitost inteligence in obveščanja. Na ta način je organizacija zmožna slediti cilju, da se dvigne na čim višjo raven inteligence, najbolj zaželeno na nivo strateške inteligence, ki privede do razumevanja visokonivojskih trendov in motivov napadalcev za namen vzpostavitve strateške kibernetske varnosti in odločanja. S tem se presežeta nivoja taktične inteligence, ki sloni na zajemanju atomarnih indikatorjev groženj ali kompromitiranja (IoC – Indicators of Compromise) v obrambnih sistemih, ter operacijska inteligenca, ki je sposobna izvajanja prednostnih in ciljnih varnostnih operacij na podlagi dobrega razumevanja infrastrukture, obrambnih zmožnosti in napadov. To lahko povezujemo z zmožnostjo in zahtevnostjo inteligence groženj, ki na najvišjem strateškem nivoju podpira aktivnosti zaznavanja in raziskovanja notranjih groženj, spremljanja napadalskih kampanij ter zavajanja napadalcev (Baker, 2022).

S pomočjo inteligence kibernetskih groženj okrepimo varnostno ekipo, pridobimo prednosti v zvezi z zaznavanjem groženj in incidentov, odločanjem na podlagi teh groženj in incidentov, odzivanjem ter krepitvijo politik obvladovanja tveganj. Primarno okolje uporabe tehnik in postopkov inteligence kibernetskih groženj je predvsem v varnostnem operativnem centru, kjer z integracijo v sisteme SIEM in SOAR dvignemo nivo varnosti. VOC mora spremljati in identificirati pokazatelje kompromitiranja, kakršni so IP (Internet Protocol) in URL (Uniform Resource Locator) naslovi, domenska imena, registri, definicije DLL (Dynamic Link Library) idr. Ti pokazatelji lahko razkrijejo nenavaden ali neobičajen omrežni promet,

lokacijske nepravilnosti, anomalije v privilegiranih uporabniških računih, povečanje obsega prenosa podatkov iz podatkovnih baz ali prek aplikacijskih programskih vmesnikov in druga varnostna tveganja.

Inteligenca groženj je udejanjena v obliki šestfaznega življenjskega cikla, ki sestoji iz faz specifikacije zahtev, zbiranja informacij, obdelave informacij, analize, razširjanja ugotovitev in povratnih informacij. S časom se učinkovitost procesa inteligence izboljšuje, kar pomeni, da več obdelanih podatkov izboljša celoten varnostni sistem.

5 AVTOMATIZACIJA ODZIVANJA V VOC ZA ENERGETIKO

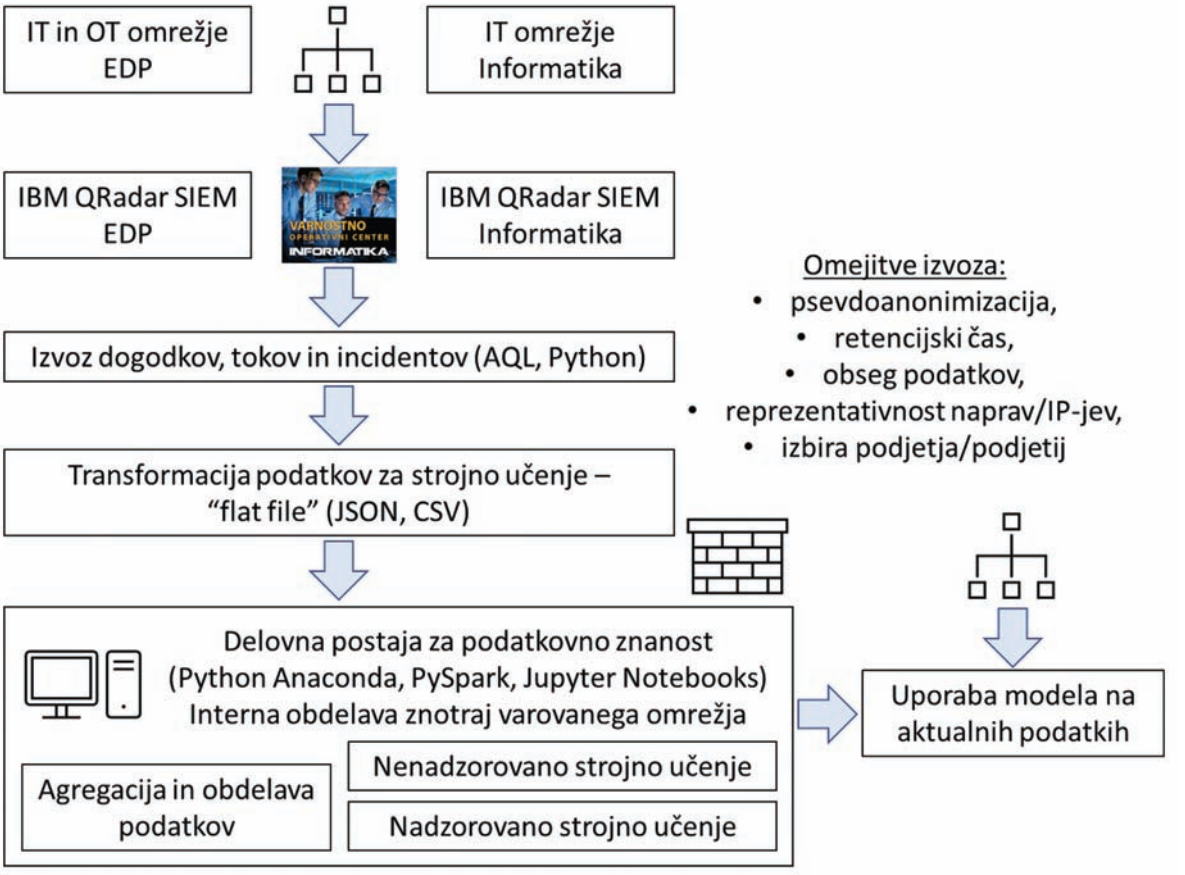
Kompleksni kibernetski sistemi, kakršni so sistemi deležnikov na slovenskem energetskem trgu, so podvrženi veliki množici komunikacijskih dogodkov med povezanimi napravami. Za te dogodke je na neavtomatiziran način ali z omejenim naborom pravil težko ali nemogoče ugotoviti, ali predstavljajo resne oziroma relevantne kibernetske grožnje, napade in incidente, katere je potrebno obravnavati z ustrezno pozornostjo. Za okolje slovenskega energetskega sektorja lahko zato prinese znatno korist izgradnja specifičnih lastnih modelov zaznavanja varnostnih anomalij na osnovi uporabe tehnik umetne inteligence in strojnega učenja. Eden ciljev vsakega modela strojnega učenja je namreč maksimizacija točnosti, kar v kontekstu kibernetske varnosti pomeni minimizacijo lažno pozitivnih in lažno negativnih zaznanih incidentov in napadov. Izkušnje kažejo, da je v ta namen potrebno vsak model pravilno prilagoditi oziroma učiti glede na dejanske podatke in problemsko domeno. Če je model pretreniran (preveč specifičen) ali podtreniran (preveč generičen), ne more zagotoviti popolne uporabnosti. Komercialni izdelki temeljijo na razmeroma splošnih tehnologijah in modelih umetne inteligence za kibernetsko varnost ter so učeni na podatkih iz drugih poslovnih domen in okolij. To pomeni, da so razmeroma generični in ne morejo enako učinkovito pokriti zaznavanja varnostnih incidentov v vseh sistemih. Ker ima slovenski elektroenergetski sektor, tako kot tudi ostali sektorji kritične infrastrukture, svoje specifike, lahko maksimalni učinek in uporabno vrednost dosežemo le z razvojem, raziskovanjem in verifikacijo specifičnih lastnih modelov umetne inteligence in strojnega učenja za kibernetsko varnost.

Podatke, ki se zbirajo v sistemu za upravljanje varnostnih informacij in dogodkov (SIEM) varnostnega operativnega centra za energetiko, uporabljamo kot učne vzorce v procesu strojnega učenja modela umetne inteligence za zaznavanje varnostnih incidentov. Podatki VOC povejo, kateri dogodki in katere kombinacije dogodkov v informacijskem omrežju so nevarne in neželene, so posledica vdorov in napadov ter predstavljajo vir kibernetskih groženj, incidentov in tveganj. Takšen model na osnovi učenja in razpoznavanja vzorcev v zgodovinskih izvoženih podatkih sistema SIEM, ki je vzpostavljen v okviru VOC, pridobi zmožnost posplošenega sklepanja, na podlagi katerega bo v prihodnosti kritične kombinacije dogodkov in tokov v omrežju samodejno in v realnem času napovedal (klasificiral, razvrstil) kot različne tipe incidentov. Postopek strojnega učenja in infrastruktura sta predstavljena na sliki 6. Podrobnejša razlaga je zaradi dolžine prispevka izpuščena. Poudariti pa je potrebno, da sta osnova za izvedbo aktivnosti izgradnje modela strojnega učenja za zaznavanje in odzivanje na kibernetske grožnje pridobljeno soglasje deležnikov na elektroenergetskem trgu za obdelavo podatkov, ki jih VOC zbira s sistemom SIEM, ter podpis ustreznega dogovora o nerazkrivanju informacij.

Modele gradimo na osnovi treh metod strojnega učenja. Te so:

- *časovna vrsta* (nenadzorovano učenje), na osnovi katere iščemo odstopanja (lokalne maksimume/minimume) v primerih incidentov;
- *segmentacija* (nenadzorovano učenje), ki sestoji iz dveh zaporednih korakov, in sicer (1.) iz segmentiranja naprav glede na značilnosti v zgodovinskih učnih podatkih ter (2.) iz segmentiranja naprav v realnem času in ugotavljanja odstopanj v segmentih glede na prvi korak, pri čemer pomeni sprememba potencialni incident;
- *klasifikacija* (nadzorovano učenje), kjer lahko dogodke in tokove klasificiramo v dva razreda (je/ni incident) ali v več razredov, ki določajo vrsto in/ali resnost incidenta.

Za uravnoteženo in učinkovito učenje potrebujemo raznolike IP-je glede na vzorce prometa, IP-je z veliko dogodki/tokovi, IP-je z visokim razmerjem med incidenti in dogodki/tokovi (če v učnih podatkih ni zadostnega deleža izstopajočih vzorcev incidentov, se model ni sposoben naučiti razpoznavanja odklonov, ki predstavljajo potencialne incidente) ter relevantne naprave oziroma IP-je glede na kontekst



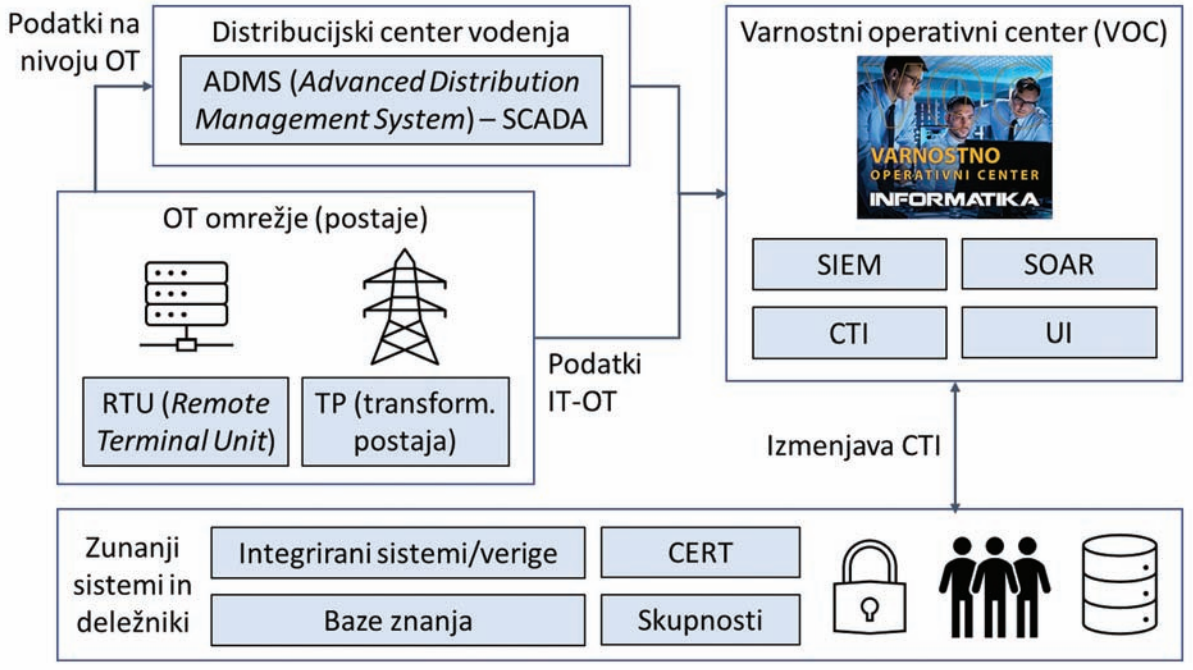
Slika 6: **Postopek strojnega učenja in infrastruktura**

(podatkovni strežniki, aplikacijski strežniki, delovne postaje, DNS itd.). Pri izvozu in obdelavi podatkov upoštevamo predpisani retencijski čas in ustrezen obseg izvoza glede na metodo strojnega učenja, prostorske omejitve in zahteve posameznih deležnikov v VOC. Obdobje in obseg izvoza se tako za nadzorovano in nenadzorovano učenje razlikujeta. Podatki za strojno učenje so zajeti v treh skupinah:

- *dogodki:* domena, izvorni IP naslov vira, vrata izvora, ciljni IP naslov vira, vrata cilja, uporabnik, visokonivojska kategorija, nižjenivojska kategorija, naziv dogodka, opis dogodka, število združenih dogodkov, čas dogodka;
- *tokovi:* domena, izvorni IP naslov vira, vrata izvora, ciljni IP naslov vira, vrata cilja, vrsta toka, čas prvega paketa, čas shranjevanja posameznega paketa, število zlogov na izvoru, število prejetih zlogov na cilju, skupno število zlogov, število posredovanih paketov na izvoru, število prejetih paketov na cilju, skupno število paketov, protokol, vrsta aplikacije;
- *incidenti:* ID, domena, izvorni IP naslovi virov, ciljni IP naslovi virov, opis incidenta, vrsta incidenta, vrsta vira incidenta, začetni čas prvega dogodka/toka v incidentu, čas zadnjega dogodka/toka v incidentu.

Osnovni, trenutno podprti nivo zaznavanja kibernetskih incidentov je nivo IT omrežja, kjer deluje VOC. Kasneje bo potrebno zaznavanje in odzivanje pokriti na vseh IT-OT integriranih nivojih kritične infrastrukture, to je od najnižjega nivoja OT omrežja, prek vmesnega nivoja distribucijskega centra vodenja, do najvišjega nivoja IT omrežja. Med temi nivoji potekajo vertikalne povezave, saj lahko pride do varnostnih incidentov na kateremkoli od njih. Koncept zaznavanja in odzivanja na varnostne incidente v IT-OT integrirani kritični infrastrukturi za področje elektroenergetike je ponazorjen na sliki 7.

Sektorski varnostni operativni center za področje energetike je zelo kompleksna entiteta, ki združuje tri temeljne elemente – ljudi, procese in tehnologijo



Slika 7: **Zaznavanje varnostnih incidentov v elektroenergetski kritični infrastrukturi**

– ter omogoča neprekinjeno in varno obratovanje kritične infrastrukture. Slediti mora zakonodaji in regulativi ter udejanjati ustrezne standarde, ki pomenijo osnovo za celovit program upravljanja kibernetske varnosti (Bregar, 2021). V tem kontekstu bi praktična ponazoritev v članku vpeljane rešitve presegala razpoložljivi obseg članka. Kljub temu je v nadaljevanju podan kratek vzorčni opis nekaterih standardnih odzivov na incidente, katerim je bil sistem izpostavljen v praksi in katerih zaznavo smo avtomatizirali.

S strojnim učenjem ter tehnologijama SIEM in SOAR smo avtomatizirali zaznavo različnih tipov incidentov. Med njimi so potencialno nevarne povezave IRC (Internet Relay Chat), izkoriščanje ranljivosti (exploit), neobičajno povečan tok omrežnega prometa in neobičajna sprememba aktivnosti uporabnikov. Ob poskusu vzpostavitve povezave IRC prek vrat 6667 na zunanji IP naslov je sistem to zaznal kot varnostni dogodek. Sprožil se je standardni postopek odziva, ki je vključeval pregled in analizo (povezanih) dogodkov, preverjanje IP naslova vira v varnostnih bazah (VirusTotal, X-Force idr.) ter pregled dnevniških zapisov. Naslov vira je bil v več bazah označen kot nevaren. Šlo je za zaporedje dogodkov poskusa vzpostavitve povezave in komunikacije po protokolu TCP (Transmission Control Protocol), katerim je po 30 sekundah sledil dogodek prekinitve povezave (Teardown TCP Connection). Zabeležba o prekoračitvi časa sinhronizacije v dnevniku je nakazala, da je bila nevarna povezava ustrezno prekinjena.

Na podoben način so bili zaznani in obravnavani tudi ostali tipi varnostnih dogodkov. V primerih incidenta povečanega izhodnega prometa (Large Outbound Transfer) in incidenta izkoriščanja ranljivosti ob uspešni prijavi uporabnika je postopek odziva zajemal analizo dogodkov med aktivnostmi varnostnega incidenta in po njih, preverjanje varnostnih baz ter pregled dnevniških zapisov. Povečanje izhodnega prometa je bilo zaznano na podlagi 1801 tokov, ki so nakazovali na večji obseg izmenjave podatkov. Ker pa so ciljna vrata 3481 običajno v uporabi v aplikaciji MS Teams, je bila ugotovljena komunikacija z zunanjim IP naslovom, ki je v večini baz označen kot nenevaren.

Ključno je, da v primerih varnostnih dogodkov in incidentov niso upoštevani le jasno definirani postopki, temveč tudi dogovorjeni odzivni časi. Pri enem kompleksnejših primerov s kratkim zahtevanim odzivnim časom je šlo za napad na aplikacijski strežnik s kombinirano uporabo več tehnik vdora v sklopu penetracijskega testiranja. Incident se je pričel 10:14 in je bil na prvem nivoju VOC zaznan že ob 10:15. Varnostni dogodek je bil nemudoma eskaliran na višji nivo, razrešen in poročan naročniku, v katerega infrastrukturo je posegal.

6 SKLEP

Kot posledico vpetosti informacijskih tehnologij v vsakodnevno življenje, poslovanje podjetij in celotno družbo, velikih količin omrežnega prometa in varnostnih podatkov, velikega števila medsebojno povezanih naprav ter obsega in resnosti kibernetskih incidentov si ne moremo zamisliti zaznavanja anomalij, varnostnih tveganj in potencialnih kibernetskih incidentov brez avtomatiziranih pristopov. Ključne so zlasti tehnologije SIEM in SOAR ter tehnike strojnega učenja in umetne inteligence. Z njimi lahko povečamo učinkovitost in uspešnost zaznavanja groženj in incidentov, zmanjšamo število lažno negativnih in lažno pozitivnih primerov, gradimo znanje o novih oblikah in vektorjih napadov ter razbremenimo varnostne analitike reševanja preprostih in ponavljajočih se problemov, na podlagi česar so se analitiki zmožni prednostno posvetiti zahtevnejšemu forenzičnemu delu in triaži. Avtomatizacija zaznavanja incidentov je tudi osnova za proces samodejnega odzivanja na incidente, ki poskrbi, da celovito odpravimo vzroke in posledice incidenta, blokiramo nadaljnje napade, zagotovimo neprekinjeno delovanje sistema, upravljamo infrastrukturne vire ter spremljamo in izboljšamo ključne indikatorje učinkovitosti. Takšen pristop dodatno optimizira proces inteligence tveganj, katerega dvigne na višji taktični nivo. To pomeni, da se zavedamo širše varnostne slike v našem sistemu, na spletu ter z vidika aktualnih motivov, taktik in vektorjev vdorov napadalcev. Postanemo lahko bolj proaktivni, s čimer smo zmožni o varnostnih problemih, tveganjih in ranljivostih razmišljati vnaprej ter nismo omejeni zgolj na tiste od njih, ki se dejansko zgodijo. Ob zaznanih tveganjih na ta način pravilno in pravočasno ukrepamo, še preden preidejo v napade in incidente.

Prispevek je povezal različne dejavnike avtomatizacije zaznavanja kibernetskih incidentov in odzivanja nanje. Pojasnil je sinergijo posameznih tehnologij in pristopov. Podal je smernice in dobre prakse njihove vpeljave ter uporabe v različnih okoljih, zlasti v varnostnih operativnih centrih. Predstavil je lasten pristop k avtomatizaciji, ki ga vpeljujemo na osnovi metod strojnega učenja.

LITERATURA

[1] Baker, K. (17. 3. 2022). *What is cyber threat intelligence? 2022 Threat Intelligence Report*. Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

[2] Bedell, C. (2019). *Definitive Guide to SOAR*. Annapolis: CyberEdge Press. https://gallery.logrhythm.com/white-papers-and-e-books/definitive-guide-to-soar.pdf

[3] Bracely, J. (6. 1. 2020). Canyon targeted by cyber attack: Massive criminal cyber attack targets Canyon's online business. *Cycling Weekley*. https://www.cyclingweekly.com/news/canyon-targeted-cyber-attack-445948

[4] Bregar, A. (2021). Program upravljanja kibernetske varnosti – celovit pristop k izboljšanju odpornosti organizacije. *Korporativna varnost*, 2021(27), 28–30.

[5] Brown, R. & Roberts, S. J. (2017). *Intelligence-driven incident response: Outwitting the adversary*. O'Reilly Media.

[6] Chai, W., Beaver, K. & Rosencrance, L. (2022). *Incident response*. TechTarget. https://www.techtarget.com/searchsecurity/definition/incident-response

[7] Freedman, L. F. (13. 2. 2020). Ransomware attacks predicted to occur every 11 seconds in 2021 with a cost of $20 billion. *National Law Review*, 10(44).

[8] IBM (28. 7. 2021). *IBM Report: Cost of a data breach hits record high during pandemic*. IBM Newsroom. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

[9] Imam, F. (12. 3. 2019). *Security Orchestration, Automation and Response (SOAR)*. Infosec Institute. https://resources.infosecinstitute.com/topic/security-orchestration-automation-and-response-soar/

[10] Jefferson, B. (8. 2. 2022). The 15 most common types of cyber attacks. *Lepide, Data Security & Compliance Blog.* https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

[11] Kafol, C. & Bregar, A. (2017). Cyber security – building a sustainable protection. V B. Katalinic (ur.), *DAAAM International Scientific Book 2017* (str. 81–90). Vienna: DAAAM International Vienna.

[12] Miller, D., Harris, S., Harper, A., VanDyke, S. & Blask, C. (2010). *Security Information and Event Management (SIEM) Implementation.* New York: McGraw-Hill Osborne Media.

[13] Morgan, S. (13. 11. 2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine.* https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[14] Pace, C. (2018). *The threat intelligence handbook*. CyberEdge Press.

[15] Reichenberg, N. (2021). *What is SOAR – Security Orchestration & Automation.* Siemplify. https://www.siemplify.co/resources/what-is-soar-security-orchestration-automation/

[16] Saini, P. S., Behal, S. & Bhatia, S. (2020). Detection of DDoS attacks using machine learning algorithms. V M. N. Hoda (ur.), *Proceedings of the 7th International Conference on Computing for Sustainable Global Development* (str. 16–21). New Delhi: IEEE. https://doi.org/10.23919/INDIACom49435.2020.9083716

[17] Sheridan, T. B. & Verplank, W. L. (1978). *Human and computer control of undersea teleoperators.* Massachusetts Institute of Technology.

[18] Thomas, A. E. (2018). *Security operations center – SIEM use cases and cyber threat intelligence*. CreateSpace Independent Publishing Platform.

▪

Andrej Bregar je doktoriral na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru. Področja njegovega strokovnega in raziskovalnega dela obsegajo operacijske raziskave, večkriterijske odločitvene metode, inteligentne in odločitvene sisteme, upravljanje s poslovnimi procesi, procesno in storitveno usmerjene arhitekture, razvoj informacijskih rešitev, podatkovne in programirne tehnologije, projektno vodenje, informatizacijo v energetiki ter kibernetsko varnost. Redno predava v domačem in mednarodnem okolju ter je avtor več znanstvenih in strokovnih člankov.

▪

Sašo Gjergjek je diplomiral na Fakulteti za varnostne vede s področja informacijske varnosti. Svojo študijsko pot je nadaljeval na isti fakulteti, kjer je magistriral s področja varstvoslovja. Trenutno se ukvarja s kibernetsko varnostjo v varnostno operativnem centru za področje energetike. Vpet je tudi v raziskovalno dejavnost s področja kibernetske varnosti.

▪

Miran Novak je s svojo več kot 30 letno vpetostjo v IKT stroko v slovenskih elektrodistribucijah izvrsten poznavalec razmer in organizacije informatike v energetiki. Univerzitetno diplomo in znanstveni magisterij je dosegel na Ljubljanski Univerzi, na Fakulteti za računalništvo in informatiko. Poleg organizacije informatike v energetiki so njegovo področje raziskovanja odnosi med procesi in pa informacijska varnost. Objavljal je članke na domačih in mednarodnih konferencah ter strokovnih revijah. Več kot desetletje je član organizacijskega odbora Posvetovanja informatikov v energetiki (PIES). Na področju standardizacije se ukvarja s sistemi vodenja, aktivno vzdržuje certifikat CIS – Information Security Manager. Vključen je v več formalnih in neformalnih organizacij za proučevanje kibernetske varnosti.

▪

Damir Orlić je raziskovalec na področju matematike in področju kibernetske varnosti. Zaposlen je v podjetju Informatika d.o.o., kjer se ukvarja s kibernetsko varnostjo.

Iz Islovarja

Islovar je spletni terminološki slovar informatike, ki ga že več kot 20 let ureja jezikovna sekcija Slovenskega društva INFORMATIKA. Slovar je javno dostopen za vpoglede in vnašanje novih izrazov. Slovar najdete na naslovu http://www.islovar.org.

celovítost -i ž *(angl. integrity)* lastnost, ki zagotavlja točnost in popolnost informacijskega sistema, storitve; sin. neokrnjenost, integriteta

CIA cíje krat. ž *(angl. confidentiality, integrity and availability, CIA)* osnovna načela informacijske varnosti: zaupnost, celovitost, razpoložljivost

korektívni ukrèp -ega -épa -a m *(angl. corrective action)* aktivnosti za odpravo neskladnost, nepravilnosti, pomanjkljivosti; sin. popravljalni ukrep

neskládnost -i ž *(angl. nonconformity)* neizpolnjevanje postavljenih zahtev

ranljívost -i ž *(angl. vulnerability)* lastnost sredstva, sistema, ki lahko omogoči uresničitev varnostne grožnje

skládnost -i ž *(angl. compliance)* izpolnjevanje postavljenih zahtev

várnostna grôžnja -e -e ž *(angl. security threat, threat)* možnost, da se zgodi varnostni incident, kar lahko povzroči škodo

várnostni dogódek -ega -dka m *(angl. security event)* dogodek, ki nakazuje na možnost kršenja informacijske varnostne politike ali odpovedi varnostnih kontrol; prim. varnostni incident

várnostni incidènt -ega -ênta m *(angl. security incident)* neželen in nepričakovan varnostni dogodek, ali zaporedje dogodkov, ki z veliko verjetnostjo ogrožajo informacijsko varnost; prim. incident, varnostni dogodek

zanesljívost -i ž *(angl. reliability)* lastnost sredstva, sistema, ki zagotavlja ustrezno izvajanje načrtovanih funkcij i

zaúpnost -i ž *(angl. confidentiality)* lastnost sredstva, sistema, ki zagotavlja, da informacije niso nepooblaščeno razkrite

Izpitni centri ECDL

ECDL (European Computer Driving License), ki ga v Sloveniji imenujemo evropsko računalniško spričevalo, je standardni program usposabljanja uporabnikov, ki da zaposlenim potrebno znanje za delo s standardnimi računalniškimi programi na informatiziranem delovnem mestu, delodajalcem pa pomeni dokazilo o usposobljenosti. V Evropi je za uvajanje, usposabljanje in nadzor izvajanja ECDL pooblaščena ustanova ECDL Fundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics) to pravico pridobilo Slovensko društvo INFORMATIKA. V državah Evropske unije so pri uvajanju ECDL močno angažirane srednje in visoke šole, aktivni pa so tudi različni vladni resorji. Posebno pomembno je, da velja spričevalo v 148 državah, ki so vključene v program ECDL. Doslej je bilo v svetu v program certificiranja ECDL vključenih že preko 16 milijonov oseb, ki so uspešno opravile preko 80 milijonov izpitov in pridobile ustrezne certificate. V Sloveniji je bilo doslej v program certificiranja ECDL vključenih več kot 18.000 oseb in opravljenih več kot 92.000 izpitov. V Sloveniji sta akreditirana dva izpitna centra ECDL, ki imata izpostave po vsej državi.

AGORA

Micro Team

Znanstveni prispevki

Kratki znanstveni prispevki

Strokovni prispevki

Prispevki iz konference Dnevi slovenske informatike

Informacije

ISSN 1318-1882
9 771318 188001