SorS

30.susret
osiguravača i
reosiguravača
Sarajevo

DAVOR ŠKOBIĆ, Croatia osiguranje d.d. Mostar
dr. sc. KREŠIMIR FERTALJ, red. prof.,
Fakultet elektrotehnike i računarstva Zagreb

INTEGRACIJA PODATAKA OSIGURAVAJUĆIH DRUŠTAVA

Insurance companies' data integration

Sažetak

Razvojem ekonomije i poslovnih aktivnosti, potrebe za osiguranjem rastu. U želji da kvalitetno i efikasno odgovori traženim parametrima, osiguranja imaju zadatak usvajati nova tehnološka dostignuća kako bi pružili kvalitetnu uslugu, ali i zaštitili svoje interese. Prikupljanje velikog broja relevantnih podataka je potrebno za što bolju procjenu rizika. Integracijom podataka između osiguravajućih društava stvara se jasnija slika stanja na tržištu. Zajednički interes svih osiguranja je suzbiti prevare u osiguranju, te su u tom području najveće mogućnosti za napredak u razmjeni podataka. Razmijenjeni podaci se mogu koristiti u razne svrhe, najprije u svrhu rudarenja podataka, stvaranja modela za prepoznavanje nepoželjnih aktivnosti u segmentu obrade i isplate šteta. Tehnologije razmjene su različite, od primitivnih (komunikacija elektronskom poštom, razmjena tabličnih datoteka), do razvoja aplikativnih rješenja baziranih na razmjeni podataka u standardnim formatima kao XML i JSON. Uz mnoge prepreke koje razmjena podataka postavlja osiguravajućim društvima, kao što su povjerljivost i kontrola, tehnologija lanca blokova sa svojim osnovnim konceptima postavlja nove standarde razmjene i komunikacije. U tom polju se vidi dalja mogućnost integracije podataka, za koju je potrebno napraviti inicijalne slučajeve korištenja, sa testom u stvarnom okruženju. U radu se razmatra trenutno stanje integracije podataka između osiguranja u Bosni i Hercegovini, te iznose novi i postojeći teorijski koncepti integracije, te se navode različiti slučajevi korištenja i teorijski principi novih rješenja u poboljšanju poslovanja osiguravajućih kuća.

Ključne riječi: *osiguranje, integracija podataka, analiza podataka, blockchain, prevencija prevare*

1. Uvod – Što je osiguranje?

Osiguranje možemo definirati kao djelatnost u kojoj za određenu premiju osiguravajuća kuća pokriva dogovorene rizike sa osiguranikom u slučaju ostvarenja neželjenog događaja. U slučaju realizacije nepovoljnih događaja iz ugovorene police, osiguranik prijavljuje događaj osiguravajućem društvu, te se kreće

u proces obrade štete. Osiguranje prilikom zaključenja police, a kasnije i tokom eventualne obrade štete, prikuplja velike količine podataka u strukturiranom i nestrukturiranom obliku, koje čuva u svojim arhivama (računalne ili fizičke arhive). To su osobni podaci osiguranika i ugovaratelja, podaci o predmetima osiguranja u raznim oblicima, te podaci o štetnim događajima. Količina tih podataka je velika, te je potrebno iste obraditi i iskoristiti u različite svrhe.

2. Upotreba i analiza podataka u osiguranju

Prikupljeni podaci u fazama prodaje i obrade osiguranje, kao i eventualnih obrada šteta se koriste za kompletiranje poslovnog procesa. Osim dijela završetka poslovnog procesa, prikupljene podatke je uputno analizirati. Rudarenje podataka ili *data mining*, možemo definirati kao otkrivanje zanimljivog znanja u velikim količinama podataka [1]. Rudarenje podataka prema [2] dijelimo u četiri kategorije, a to su:

- Analiza predviđanja (eng. Prediction analysis),
- Analiza asocijacije (eng. Association analysis),
- Analiza grupiranja (eng. Clustering analysis),
- Analiza anomalija i relativnosti slijeda (eng. Anomaly and sequence relativity analysis).

Područja primjene rudarenja podataka u osiguranju su velika, te ih dijelimo u nekoliko kategorija.

1. Upravljanje odnosom s korisnicima (eng. customer relationship managment) [2]
   Upravljanje odnosom s korisnicima je važno područje unutar rudarenja podataka [3], jer daje mogućnosti za shvaćanje prave vrijednosti određenog klijenta za osiguravajuću kuću, u smislu određivanja njegove profitabilnosti [4]. U radu [4] prikazana je metoda rudarenja podataka stablo odlučivanja (eng. decision tree) gdje je izvršena klasifikacija korisnika usluge obaveznog osiguranja od autoodgovornosti u preferencijske grupe na osnovu uspostavljenog modela. Također, moguće je izvršiti procjenu karaktera klijenta, te ih klasificirati i grupirati na osnovu različitih parametara [5]. Praćenjem podataka o klijentu i građenjem odnosa prema istome sprečava se odlazak klijenta u konkurentska poduzeća [2]. Poprečna prodaja (eng. cross-sell) i rastuća prodaja (eng. up-sell) su također pojmovi koji se vežu za klijenta, gdje se na osnovu rudarenja podataka o navikama potrošača nude proizvodi koji bi mogli zainteresirati klijenta, te tako povećati njegovo zadovoljstvo uslugom, uz poboljšanje prodajnog rezultata [2].
2. Upravljanje rizikom (eng. risk managment) [2]
   Kao što je i slučaj kineskog tržišta [2], upravljanje rizikom na domaćem tržištu se provodi po metodi disperzije rizika, gdje se rizik umanjuje na

način da se osigura što veći broj osoba, te da se zarađenom premijom pokriju eventualne štete. Mogućnosti daljeg razvoja ovog segmenta se vide korištenjem algoritama strojnog učenja, kao u primjeru korištenja neuronskih mreža gdje je izvršeno grupiranje (eng. clustering) osiguranika na osnovu njihove rizičnosti, te osiguranje može na osnovu svoje politike izvršiti potrebne korake kod primanja u osiguranje [6]. Također, izvršavanje rudarenja podataka nad velikim podacima (eng. big data) daje velike mogućnosti u ovom području [7]. Veliki podaci su pojam za nestrukturirane podatke koji se prikupljaju u raznim oblicima, kao što su podaci sa društvenih mreža i ostalih mrežnih lokacija, arhivska građa u obliku skeniranih PDF dokumenata, podaci nastali raznim aktivnostima (eng. log podaci), koji se mogu analizirati metodama rudarenja tekstom (eng. text mining), izvlačenja znanja iz statičkih dokumenata [8].

3. Otkrivanje prevare (eng. fraud detection)
   U osiguranju, kao i u ostalim društvima koja se bave financijskom djelatnošću moguće su prevare, koje svake godine uzimaju određeni dio zarade društvima, gdje se smatra da od 20% do 25% zahtjeva sadrži određenu prevaru, što rezultira 10% povećanjem isplata šteta [9]. Prevara je prilagodljiv zločin, te traži uporabu inteligentne analize podataka u poljima otkrivanja znanja u bazama podataka (eng. knowledge discovery in databases KDD), rudarenja podataka, strojnog učenja (eng. machine learning) i statistike [10][11].
   Sve ove primjene rudarenja podataka su u uporabi dulji period, te se i dalje razvijaju. Svrha svih spomenutih primjena ide u jednom od dva smjera, povećanje premije i smanjenje isplaćenih šteta.
   Po pitanju primjene novih tehnologija u osiguranju, kao i prisutnih izazova potrebno je istaknuti sljedeće tri stavke: rudarenje osjećaja (eng. sentiments mining), osiguranje temeljeno na upotrebi (eng. usage based insurance), i rudarenje podataka sa očuvanjem privatnosti (eng. privacy-preserving data mining).
4. Rudarenje osjećaja (eng. sentiments mining)
   Rudarenje osjećaja definira se kao prepoznavanje osjećaja određenog pojedinca ili populacije na osnovu njihovih tekstualnih zapisa, prvenstveno na društvenim mrežama. U radu [12] prezentirana je metoda integracije heterogenih podataka u svrhu određivanja i vizualizacije osjećaja povezanih sa događajima velikih razmjera u geografski ograničenim prostorima. Analiza se vrši na osnovu komentara društvenih mreža, te se vrši vizualizacija na geografskoj karti kako bi jasno mogli uočiti osjećaje povodom određenih događaja (prirodne i ljudske katastrofe). Poznajući osjećaje određenog područja na određene događaje, moguće je prilagoditi ponudu i proizvode za to područje, u svrhu većeg zadovoljstva klijenata i zadovoljenja njihovih potreba [8].

5. Osiguranje temeljeno na upotrebi (eng. usage based insurance)
   Vrsta osiguranja koja se temelji na automatskom prikupljanju i obradi podataka, te se temelji na naplati u odnosu na korištenje usluge. Za detekciju korištenja koriste se IoT uređaji kojima se, npr. prati način i količina vožnje automobila kako bi se ista naplatila, kretanje ljudi kako bi se izvršila naplata i obračun putnog osiguranja. Realizacija istog se predlaže u kombinaciji s tehnologijom lanca blokova (eng. Blockchain) [13]. Prisutnošću novih odredbi koje određuju pravila i načine postupanja, kao što je *GDPR* [14] na razini Europske unije, potrebno je dati veliku važnost na privatnost korisnika. Stoga se kao pojam nameće rudarenje podataka sa očuvanjem privatnosti (eng. privacy-preserving data mining).

Skupljanje i analiza podataka su u stalnom porastu, te se isti koriste u različite poslovne svrhe kako bi se izvršila korist od znanja stečenog metodama rudarenja podataka. Uza sve prednosti ovog načina prikupljanja i obrade podataka, javlja se bojazan od narušavanja privatnosti zbog toka i spremanja podataka potencijalno osjetljivih podataka. Metode koje omogućavaju ubiranje znanja iz podataka, uz očuvanje privatnosti, nazivaju se rudarenje podataka s očuvanjem privatnosti (eng. Privacy-Preserving Data Mining, skraćeno PPDM) [15]. Za razliku od klasičnih metoda rudarenja podataka [15] (rudarenje pravilima udruženja (eng. association rule mining), klasifikacija (eng. Classification), stvaranje klastera (eng. clustering), PPDM metode se razlikuju po tome što uklanjaju određene segmente podataka [16], kako bi očuvale privatnost, a opet u konačnici dale kvalitetne rezultate. Privatnost unutar PPDM može se ostvariti na više razina [15], a to su:

- Očuvanje privatnosti prilikom prikupljanja podataka (eng. Data Collection Privacy) na način da prihvatni uređaj (senzor) prikupljene podatke šalje u obliku slučajno formiranog niza (eng. random). Također, originalne vrijednosti se nikada ne čuvaju već se koriste samo u procesu generiranja novog slučajnog niza podataka,
- Privatnost podataka prilikom objave (eng. Data Publishing Privacy), kod situacija kada se podaci izlažu javno ili trećim stranama, a sve u svrhu daljnje analize, poželjno je izvršiti anonimizaciju zapisa. PPDM u situacijama objave podataka se naziva očuvanje privatnosti podataka prilikom objavljivanja (eng. Privacy Preserving Data Publishing, skraćeno PPDP). Anonimizicija zapisa se vrši primjenom nekog od modela privatnosti [15], koji se temelje na kombinaciji operacija: generalizacija (eng. generalisation), potiskivanje (eng. suppression), anatomizacija (eng. anatomization), premetanje (eng. pertubation),
- Rudarenje s privatnosti izlaznih podataka (eng. Data Mining Output Privacy) – rezultati operacije rudarenja podataka sami po sebi otkrivaju mnogo podataka, te su mogući napadi na rezultate operacija kako

bi se otkrili podaci iz kojih su proizašli ovi rezultati, te su definirane višestruke metode zaštite podataka na ovoj razini [15],
- Distribuirana privatnost (eng. Distributed Privacy) – U situacijama gdje više entiteta želi rudariti globalno stanje u obliku agregatnih statistika na bazi spojenih podataka sa više izvora, sve bez otkrivanja svojih podataka ostalim entitetima, predlaže se korištenje predloženih rješenja iz područja kriptografije, sigurno računanje s više strana (eng. secure multiparty computation, skraćeno SMC).

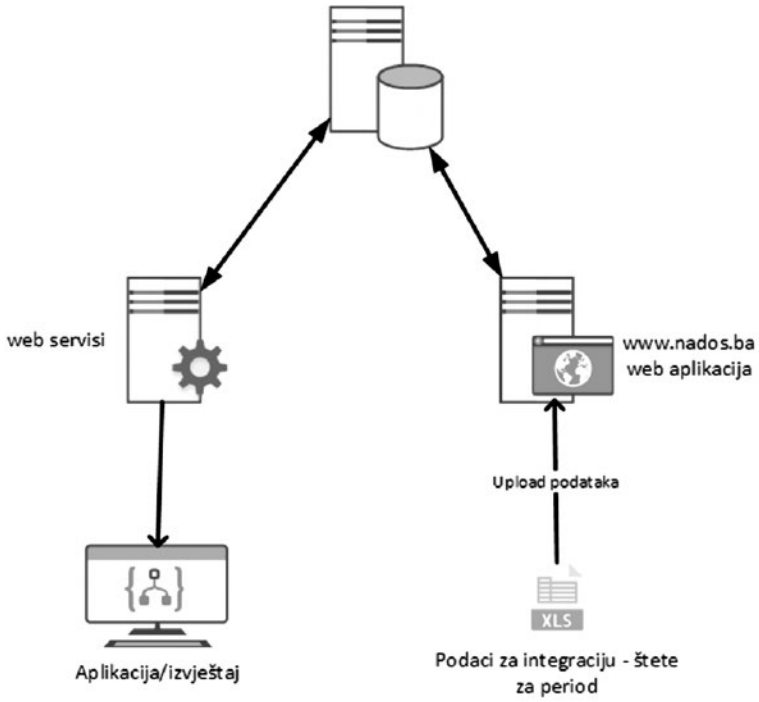
Sve metode koje se koriste u PPDM je potrebno izmjeriti kako bi se odredila njihova kvaliteta, te su predložene sljedeće metrike [15]:
- metrika razine privatnosti (eng. privacy level metrics) – mjere koliko su podaci sigurni sa točke gledišta mogućnosti otkrivanja podataka,
- metrika kvalitete podataka (eng. data quality metrics) – mjere količinu gubitka informacija,
- metrika kompleksnosti (eng. complexity metrics) – mjere efikasnost i skalabilnost različitih tehnika.

Najvažnije od svega, primjena ovog rješenja ogleda se u mnogim sustavima kao što su [15]: PPDM računarstvo u oblaku (eng. cloud computing PPDM), PPDM e-zdravlje (eng. E-health PPDM), PPDM usluge temeljene na lokaciji (eng. Location-Based Services PPDM), PPDM senzor bežične mreže (eng. Wireless Sensor Networks PPDM). Kako je industrija osiguranja široko rasprostranjena, njen doticaj sa problematikom privatnosti kod rudarenja podataka je vidljiv u prve tri navedene sfere kroz već implementirana prikupljanja podataka koja se nalaze u oblaku, sustave zdravstvenog osiguranja, te i u sustavima naplate osiguranja po upotrebi (eng. usage based insurance) gdje se posebno ističe problem narušavanja privatnosti korisnika, u kojem se prate podaci kretanja i ponašanja korisnika za upravljačem vozila kao mjerilo za određivanje konačne cijene osiguranja.

3. Integracija podataka u osiguranju

Zbog želje za kvalitetnom analizom podataka i smanjenja rizika, osiguravajuće kuće imaju potrebu prikupiti što više podataka o strankama o osiguranju ili predmetima osiguranja. Cilj je prikupiti podatke iz što više vjerodostojnih izvora. Razmjena podataka između osiguranja se može smatrati jednim od takvih izvora. Trenutno u Bosni i Hercegovini integracija podataka osiguravajućih društava se radi na razini razmjene podataka o štetama iz obaveznog osiguranja autoodgovornosti. Pravila razmjene se određuju na razini nadležne agencije na razini entiteta, Agencija za nadzor osiguranja FBiH (*www.nados.ba*) i Agencija za osiguranje RS (*www.azors.rs.ba*).

Slika 1. Shema razmjene podataka NADOS FBiH



Kao što je vidljivo na slici 1, na razini Federacije BiH se razmjena vrši na način da se podaci za prijenos prema agenciji pripreme u odgovarajućoj datoteci, te preko web aplikacije unesu u bazu podataka. Korištenje podataka je moguće putem web servisa ili putem aplikacije (pregled izvještaja).

Na razini entiteta Republika Srpska, koji je pod nadzorom AZORS, razmjena podataka se radi na način da se podaci pripreme u .xls datoteci koja se šalje na AZORS putem email sustava. AZORS radi spajanje datoteka svih osiguranja u jednu, te istim putem vraća svim osiguranjima na korištenje.

Na ovaj način se riješila potreba pravilnog obračuna bonusa i malusa za korisnike osiguranja, gdje se na osnovu podataka o štetama u prethodne 3 godine osiguraniku određuje razina popusta koju ostvaruje. Ako ne postoji razmjena podataka između osiguranja, ne bi bilo jednostavno pratiti štete osiguranika koji mijenjaju osiguranje, te bi se otvorio prostor za krive obračune i prevare u osiguranju.

Na primjeru rada osiguranju u Ujedinjenom kraljevstvu možemo naći dodatne primjere integracije podataka između osiguranja [17]:

- *Claims Underwriting Exchange (CUE)* – Sprema sve podatke nastale iz prijavljenih šteta koja uključuju vozila, kućanstva i osobne ozljede neovisno hoće li šteta biti isplaćena ili neće. Svrha sustava je spremiti sve štete u jednu centralnu bazu podataka i spustiti razinu premije koju plaćaju poštenih korisnici polica osiguranja, a sprečavajući slučajeva višestruke prijave iste štete i krivog tumačenja povijesti šteta.
- *Insurance Fraud Register (IFR)* – lista svih osoba koji su osuđivani za prevare u osiguranju. Cilj je smanjiti iznose premija poštenim korisnicima.
- *Motor Insurance Anti-Fraud and Theft Register (MIAFTR)* – Popis svih vozila koji su upisani kao otpisana (totalna šteta) zbog nesreće ili su ukradena i nepronađena, koristi se za sprečavanje prevara u osiguranju.
- *My Licencse Database* – baza podataka sa statusom svake vozačke dozvole, sa ciljem provjere podataka koja osiguranja primaju od korisnika.
- *Motor Insurance Database (MID)* – Nacionalna baza podataka koja pokazuje status osiguranja svakog osiguranog vozila u Ujedinjenom kraljevstvu. Pokazuje je li vozilo osigurano i u kojem osiguravajućem društvu.

Format podataka koji se dostavljaju u Bosni i Hercegovini propisuju agencije za nadzor. U tom smjeru imamo i svjetski postavljene standarde koje propisuje ACORD [19]. ACORD je neprofitna organizacija u vlasništvu kompanija u osigurateljnoj branši čija je uloga da stvara standarde definiranja pojmova u osiguranju kao stavki informacijskog sustava, te definira standarde komuniciranja između aktera osigurateljne branše, vertikalne, ali i horizontalne. Cilj je na jednom mjestu imati definirane standardne definicije pojmova u osiguranju kako bi mogli razviti informacijski sustav koji će sadržavati sve potrebne podatke.

Slika 2. Opća shema industrije osiguranja

Industriju osiguranja vertikalno možemo podijeliti na 3 sloja, a to su reosiguranja, osiguranja i brokeri/posrednici. Osiguranja definiraju pakete osiguranja, te ih prodaju izravno klijentima ili preko posrednika/brokera. Reosiguranja su društva koja preuzimaju rizik (djelomično ili cjelokupno) od osiguranja uz zamjenu za odgovarajući dio prihodovane premije po polici. Kako bi ova struktura funkcionirala, potrebno je definirati standarde komunikacije između ovih slojeva, gdje nastupaju organizacije kao što je ACORD. Također, horizontalnu komunikaciju možemo definirati kao komunikaciju organizacija koje pripadaju istom sloju u cilju razmjene podataka.

Svi navedeni načini komunikacije definirani su trenutno prihvaćenim i provjerenim tehnologijama kao što su tablični dokumenti (.xls, .csv), polustruktuirani dokumenti (xml), koje se šalju putem web aplikacija, web servisa ili FTP razmjenom. U novije vrijeme postoji ideja uporabe blockchain tehnologije za razmjenu podataka u osiguranju, ali i za ostale uporabe, zbog njezinih svojstava vjerodostojnosti podataka, te visokoj razini povjerenja sudionika u osiguranju.

4. Blockchain

Još jedna tehnologija koja je u skorije vrijeme zaživjela kroz digitalnu valutu Bitcoin, te platformu Etherum, zove se lanac blokova (eng. Blockchain). Definirana je kao javna glavna knjiga distribuirana preko mreže, koja sprema transakcije (poruke poslane iz jednog čvorišta mreže u drugo) izvršene među sudionicima mreže. Prije unosa zapisa u lanac blokova (zapis blokova, niz blokova), svaka transakcija se potvrđuje od čvorova u mreži u suglasju sa mehanizmom konsenzusa većine. Upisane informacije ne mogu biti promijenjene ili izbrisane i u bilo koje vrijeme svaka transakcija može biti rekreirana [20]. Također, u [20] se nalazi detaljno objašnjenje rada tehnologije lanca blokova, gdje se ista opisuje kao dugi lanac koji se periodično povećava kada se informacije o novim transakcijama dodaju na njegov kraj. Transakcije se grupiraju u blokove, gdje se blokovi vežu lančano za onaj prethodni. Održava se mrežom čvorova, koji provjeravaju validnost transakcija, te dodaju ih u nove blokove u procesu zvanom rudarenje. Na primjeru transfera novca između Alice i John možemo shvatiti način rada. Alice odlučuje prebaciti novac iz svog digitalnog novčanika u novčanik korisnika John, a koji se identificira adresom. Alice određuje količinu novca koji želi prebaciti, te šalje tu informaciju svim čvorovima u mreži. Transakcija je digitalno potpisana od strane njenog novčanika, što potvrđuje da informacija dolazi od njenog novčanika i da ne može biti izmijenjena od nekog drugog. Čvorovi u mreži provjeravaju ispravnost digitalnog potpisa kojim je potpisana transakcija. Također, provjeravaju dostupnost sredstava pošiljatelja na osnovu sume prethodnih transakcija. Ako je transakcija moguća, ista se dodaje u novi blok. Novi blok sadrži listu

transakcija koje je potrebno potvrditi, te u zaglavlju bloka se sprema sažetak (eng. *hash*) bloka, kao i sažetak prethodnog bloka kako bi novonastali blok upisali u lanac blokova, čvorovi počinju proces rudarenja, gdje je u radu naveden primjer sa korištenjem *proof-of-work* načina potvrde transakcije. Ovaj način se bazira da 51% čvorova u mreži mora potvrditi transakciju kako bi se ista upisala u lanac. Razvoj tehnologije lanca blokova može se promatrati kroz iteracije u verzijama 1.0, 2.0 i 3.0 [21]. Verzija 1.0 strogo se veže za kriptovalute i bitcoin [22]. Lanac blokova se koristi kao decentralizirana glavna knjiga za spremanje transakcija kriptovaluta. Korisnici spremaju svoje vjerodajnice u digitalne novčanike, i koriste ih za transfer novca. Verzija 2.0 je dobila još jednu mogućnost, a to je spremanje, potvrda i prijenos ugovora/svojstava. Polja primjene kreću od korištenja tehnologije lanca blokova kao decentralizirane kopije lokalnih baza, a i za ostale sofisticiranije potrebe. Najveće svojstvo koje je donio lanac blokova 2.0 (eng. Blockchain 2.0) je integracija sa pametnim ugovorima (eng. smart contracts). Pametni ugovori su dijelovi koda, spremljeni na lanac blokova, programirani tako da imaju određeno ponašanje kada se ispune određeni uvjeti, te se izvršavaju automatski bez kontrole treće strane. Kako bi se mogli pratiti događaji koji bi pokretali pametne ugovore, koriste se elementi zvani oracles koji prate podatke iz stvarnog svijeta, te ih šalju u lance blokova. Lanac blokova 3.0 (eng. Blockchain 3.0) se više ne tiče samo financijske primjene, već se primjena za tehnologiju nalazi i u sustavima vlada, zdravstva, znanosti, učenja itd.

U [20] su navedene i prednosti i nedostatci tehnologije lanca blokova.

Prednosti:

- Implementira dijeljeni repozitorij, koji se održava od čvorova: svi imaju pristup podacima. Također, spremajući podatke na čvorove, sprečava se gubitak podataka u slučaju neočekivanih događaja.
- Pruža povjerenje između stranaka, digitalni potpisi i validacija omogućavaju korektno ponašanje svakog od čvorova, bez potrebe za posrednikom.
- Svi imaju mogućnost pisanja i čitanja, postoji mogućnost korištenja u svrhu svjetskog repozitorija kojem pristupaju različite uloge.
- Svi imaju mogućnost ne samo vidjeti konačno stanje transakcija, već i povijest prošlih stanja, zagarantirana transparentnost.
- Nepromjenjiv je, podaci se ne mogu mijenjati ili uklanjati.
- Ne može biti upravljan od središnjeg autoriteta i ne može biti kontroliran/cenzuriran/ugašen.
- Sa pametnim ugovorima, aktivnosti mogu biti automatizirane.

Mane:

- Karakterizira ga visoka potrošnja energije.
- Rudarenje (eng. mining), čin dodavanja novih transakcija u lanac blokova, traži skup hardver, a većina računalne snage iskorištene u rudarenje

propada, jer je rudarenje organizirano na principu natjecanja između čvorova. Predlaže se promjena koncepta organizacije rudarenja iz dokaza rada (eng. proof-of-work) u dokaz uloga (eng. proof-of-stake).
- Replikacija podataka traži memorijski prostor: lokalne kopije lanca blokova se spremaju na svaki čvor, te se performanse ne mogu još usporediti sa bazama podataka (npr. Veličina lanca blokova za Bitcoin je 105 Gb, a Etherum 70 Gb, u trenutku pisanja [20])
- Dodavanje informacija je sporo, Bitcoin od 10 do 60 minuta, Etherum 15 sekundi.
- Nepromjenjivost i transparentnost mogu ugroziti korisničku privatnost i ugled, svaki čvor ima kopiju podataka i mogućnost pristupa.
- Pametni ugovori se ne mogu osloniti na vanjske API pristupne sustave, već podaci moraju biti dio nekog lanca blokova, kako bi se osigurala nepromjenjivost podataka izvora kojem se pristupa. Oracles tehnologija se može iskoristiti za pripremu podataka, te prijenos u lanac blokova, ali se mora osigurati robusnost takvog rješenja kako ne bi postao najslabija karika [20].
- Pametni ugovori mogu sadržavati pogreške nastale u programiranju. Zbog svog svojstva nepromjenjivosti, isti se ne mogu popraviti, te je potrebno iste reprogramirati, te prebaciti na novi lanac blokova, također prilikom toga prebaciti sve podatke i pokazivače.

Postoji veći broj prijedloga za primjenu ove tehnologije u industriji osiguranja [20]:
- Primjena pametnih ugovora za poboljšanje korisničkog iskustva i smanjenje operativnih troškova – svojstvo samostalnog izvršavanja može ubrzati procese obrade šteta i smanjenja ljudskog napora (automatska naplata kod oštećenja vozila popravkom na određenim mjestima, automatska naplata oštećenja u poljoprivredi na osnovu meteoroloških podataka, automatska naplata osiguranja nakon postavljenih očitanja IoT uređaja).
- Prevencija prevare – dijeljeni lanac blokova sa podacima polica udružen sa podacima drugih izvora (medicinski i policijski izvještaji), u svrhu sprečavanja prevara tijekom odštetnih zahtjeva. Također, u [23] se predlaže sustav razmjene podataka za borbu protiv prevare.
- Verifikacija unosa podataka/potvrda identiteta – u slučaju postojanja posebnog niza lanca blokova sa identifikacijskim podacima, isti se mogu povezati na sustave osiguranja za potrebu bržeg i vjerodostojnijeg unosa podataka.
- Plaćanje po korištenju (eng. Pay-per-use) – pametni ugovori bi mogli omogućiti korištenje polica zasnovanih na količini korištenja osiguranog objekta, sa podrškom IoT uređaja, na osnovu čijih podataka bi

se izvršila naplata osiguranja (ukoliko korisnik napusti inozemstvo, ukoliko se vozi automobil)
- Mreža za raspodjelu rizika (eng. Peer-to-peer insurance) – koncept zasnovan na DAO (decentralizirane autonomne organizacije) i pametnim ugovorima, kojim bi se omogućilo samoupravljanje organizacije.

Svakako da ovi koncepti imaju svoje mane, te je na istima potrebno dodatno raditi kako bi se prepoznala njihova primjena. U [20] dana je detaljna analiza slučajeva za navedene primjene u odnosu na elemente same tehnologije. Potrebno je napraviti analizu potrebe implementacije određenog rješenja tehnologijom lanca blokova. Analiza se sastoji od odgovora na sljedeća pitanja:
- Postoji li potreba za dijeljenom bazom podataka?
- Postoji li potreba da više stranaka upisuje podatke?
- Jesi li potencijalne stranke koje vrše upis nepovjerljive (tj. postoji li potreba zabrane izmjene prethodnih zapisa drugih autora)?
- Je li potrebno izbaciti posrednike (postoji li potreba izbaciti posrednike s povjerenjem iz potvrde/autentifikacije transakcija)?
- Postoji li potreba uvida povezanosti transakcija (tj. upis transakcija za istog korisnika neovisno od više autora)?

U tablici se nalaze rezultati analize iz [20]:

Tablica 1. Ocjena predloženih primjena tehnologije u odnosu na pitanja („+" pozitivna ocjena, „-„ negativna ocjena, „+/-„ primjenjive obje ocjene zavisno od konteksta)

	Dijeljena baza podataka	Više osoba za upis	Nepovjerljive osobe za upis	Izbacivanje posrednika	Povezane transakcije
Poboljšanje korisničkog iskustva i smanjenje operativnih troškova	+/-	+/-	+/-	+/-	+/-
Prevencija prevare	+	+	+	+	+
Unos podataka/ potvrda identiteta	+	+	+	+	+
Plaćanje po korištenju	+/-	+/-	+/-	-	-
Mreža za raspodjelu rizika	+	+	+	+	+

5. Sustav razmjene podataka za prevenciju prevare baziran na blockchain tehnologiji

Prevencija prevare je bitan faktor u poslovanju osiguravajućih društava jer je jedna od prepreka kvalitetnom financijskom rezultatu. Osobe koje žele zaraditi na prevari primjećuju praznine u načinima rada osiguravajućih društava, a to su [23]:

- Osiguranje istog predmeta osiguranja na više polica,
- Ista osoba uključena u višestrukim nevjerodostojnim prijavama šteta, ali u različitim ulogama (ugovaratelj, štetnik, oštećeni, svjedok)
- Isti obrasci korišteni u većem broju štetovnih zahtjeva u više osiguranja od istih ili različitih osoba (fraze u tekstu, ponavljajući uzroci).

Prema [23] osiguranja ulažu u sustave dostave podataka od javnih ustanova ili pribavljača podataka, kako bi imali što veće ulazne parametre za procjenu vjerodostojnosti štete. Na teritoriji Federacije BiH, razmjena podataka o štetama se najčešće odvija na pismenoj komunikaciji između osiguranja elektronskom poštom, osim u slučaju pregleda šteta iz područja osiguranja autoodgovornosti, za koje postoji aplikativno rješenje. Izazovi razmjene podataka između osiguranja su [23]:

- Dijeljenje povjerljivih podataka,
- Dijeljenje podataka preko državnih granica,
- Nepostojanje volje za podjelom podataka sa trećom stranom ili konkurencijom,
- Tko upravlja podacima koji se dijele
- Velika osiguranja više doprinose nego manja osiguranja, a dobivaju manje.

Tehnologija lanca blokova (eng. Blockchain) svoje prednosti ima u tome što osigurava nepromjenjivost, odgovornost i transparentnu usklađenost [23]. Samu tehnologiju smo već objasnili, ali njena implementacija mora biti zasnovana na tehnologijama otvorenog koda [23]. Isto je potrebno kako bi se oko tehnologije skupila kritična masa organizacija i iskoristila pune potencijale. [24] Zbog tehnologije otvorenog koda organizacije koje sudjeluju mogu imati povjerenje prema tehnologiji i odgovarati standardima industrije. Dijeleći temeljni dio, osiguranja se mogu fokusirati na rješavanje primijenjenih problema u industriji. Lanci blokova (eng. blockchain) rješavaju specifične probleme koje baze podataka nisu u mogućnosti riješiti, a to su:

- Potpuna distribucija,
- Visoka otpornost na prestanke u radu,
- Ne postoji potreba centralnog autoriteta.[23]

Prema [23] sustavi bazirani na tehnologiji lanca blokova mogu pomoći u radikalnoj promjeni industrije osiguranja. Na primjeru obrade štetovnih

zahtjeva mogu se vidjeti prednosti implementacije ove tehnologije. Kada sklapamo policu dobijemo uvjete na osnovu kojih se određuje možebitna isplata šteta. Zavisno od vrste štete i svih okolnosti pod kojima se ona dogodila, potrebno je imati i adekvatnu osobu za obradu štete. Obrada štete tako može biti i procesna (slijedi određene korake) ili da je bazirana na glasovanju (isplata i iznos odštete se određuje komisijski). Također, na osnovu dostavljenih podataka koji mogu biti u digitalnom ili fizičkom formatu, osoba zadužena za štetu donosi odluku o isplati štete, te iznosu za isplatu. U svemu tome, postoji i mogućnost prevare koju je potrebno istražiti, te postoji i praksa angažmana vanjskih suradnika za ove poslovne procese. Ukoliko implementiramo tehnologiju lanca blokova u ovakav sustav sa velikim brojem dokumenata, kao i suradnjom sa vanjskim suradnicima u procesu procjene i provjere valjanosti štetovnog zahtjeva, povećati će se povjerenje, te smanjiti mogućnosti nedozvoljenih izmjena. Svi podaci će biti transparentni, te će se moći izvršiti rekonstrukcija. Također, tehnologijom pametnih ugovora moći će se izvršavati automatski procesi obrade šteta. Mogućnost uspostavljanja konsenzusa tehnologijom lanca blokova će smanjiti potrebu postojanja centralnog autoriteta.

Kako ova tehnologija može biti iskorištena u sprečavanju prevara u osiguranju? Prema [23] moguće je napraviti sustav koji osigurava smanjenje razine prevare u osiguranju. Potrebno je pratiti integritet police, štete i predmeta osiguranja. Samim time se smanjuju mogućnosti krivotvorenja, dvostrukog knjiženja, izmjena na dokumentima i ugovorima. Uza sve to, ova tehnologija ne sprečava rizik povezan sa određenim oblicima prevara, te se naznačava daljnja potreba za alatima detekcije prevare i sustava za istraživanje prevare. Potrebno je imati sustav koji će odgovarati pitanja "tko je tko" i "tko zna koga"[23]:

- Bihevioralna analiza: potrebno je pratiti ponašanje stranaka, polica i predmeta osiguranja kroz kanale i linije poslovanja,
- Deskriptivna i prediktivna analiza: Mora omogućavati identificiranje skupina, anomalija i treniranje modela,
- Analiza nestrukturiranih podataka,
- Analiza veza (eng. Link analysis),
- Upravljanje slučajevima i upozorenjima (eng. Alert and Casa Managment),
- Izvještavanje prema regulatoru,
- Izvještavanje o gubitcima (eng. Loss Reporting).

Korištenje ove tehnologije u razmjeni podataka između osiguranja, agenata, reosiguranja, brokera i svih ostalih koji su akteri u industriji osiguranja je prema [23] moguće. Najveći problem su različite arhitekture i nedostatak zajedničkih standarda. Tehnologija lanca blokova ima potencijale za rješavanje problema razmjene podataka. Ukoliko osiguranja uspiju spremiti u sustav lanca blokova svaku transakciju koja se odvija u poslovnim procesima vezanim za

određenu policu, životni ciklus police i vlasnika police se može rekonstruirati. To pojednostavljuje proces obrade šteta i smanjuje razinu prevare. Obrada šteta u osiguranju je distribuiran proces koji uključuje osiguranje, osiguranika i treću stranu, te je taj proces često označen sa određenom razinom nepovjerenja. Ukoliko u određenim točkama procesa obrade štete se vrše zapisi u lanac blokova, te daje uvid strankama u postupku, a i regulatoru, vrši se izbjegavanje nepovjerenja. Upisom podataka u sustav lanca blokova, stvara se distribuirana baza podataka koja je dostupna svim akterima industrije osiguranja, te se smanjuje kompleksnost poslovanja (podaci na jednom mjestu). Primjena ove tehnologije bi značila i standardizaciju poslovnih procesa unutar osiguranja, poslovnih termina, ugovorne dokumentacije i sl. Također, prema [23] zadržavanjem trenutno nestandardizacije u osiguranju, ali uvođenjem sustava za razmjenu podataka o prevarama bi se napravio napredak u trenutnom polju. U svemu tome trebalo bi paziti na kontrolu pristupa (tko što može vidjeti), te anonimnost podataka (zaštita privatnosti).

Uvođenje tehnologije lanca blokova će ići postepeno, te bi u tom pravcu trebalo djelovati u smjeru dokazivanja koncepta u sljedećim pravcima [23]:

- Lanac blokova za razmjenu podataka sudionika u borbi protiv prevara – sustav za verifikaciju identiteta korisnika, te zaštitu od pranja novca, korupcije, financiranja terorizma, kao i zaštita od krađe identiteta.
- Lanac blokova za spremanje i praćenje identiteta u svrhu prevencije prevare – tehnikama analize društvenih mreža (tko je tko i tko komunicira s kim) u svrhu sprečavanja prevare, pratiti ključne podatke o osobama kako bi se lakše vršila verifikacija osoba.
- Lanac blokova za spremanje podataka o razinama rizika u svrhu smanjenja prevare – vođenje evidencije o vrijednostima predmeta osiguranja i njihovih rizika.
- Lanac blokova za čuvanje povijesti lanca snabdijevanja – evidencija predmeta osiguranja, kako bi korisnici mogli pronaći informacije o ukradenim ili falsificiranim proizvodima, ili lažnim transakcijama.

6. Zaključak

Razvojem ekonomije i poslovnih aktivnosti, potrebe za osiguranjem rastu. U želji da kvalitetno i efikasno odgovori traženim parametrima, osiguranja imaju zadatak usvajati nova tehnološka dostignuća kako bi pružili kvalitetnu uslugu, ali i zaštitili svoje interese. Prikupljanje velikog broja relevantnih podataka je potrebno za što bolju procjenu rizika. Integracijom podataka između osiguravajućih društava stvara se jasnija slika stanja na tržištu. Zajednički interes svih osiguranja je suzbiti prevare u osiguranju, te su u tom području najveće mogućnosti za napredak u razmjeni podataka. Razmijenjeni podaci se mogu koristiti u razne svrhe, najprije u svrhu rudarenja podataka, stvaranja modela za prepoznavanje nepoželjnih aktivnosti u segmentu obrade i isplate šteta.

Tehnologije razmjene su različite, od primitivnih (komunikacija elektronskom poštom, razmjena tabličnih datoteka), do razvoja aplikativnih rješenja baziranih na razmjeni podataka u standardnim formatima kao XML i JSON. Uz mnoge prepreke koje razmjena podataka postavlja osiguravajućim društvima, kao što su povjerljivost i kontrola, tehnologija lanca blokova sa svojim osnovnim konceptima postavlja nove standarde razmjene i komunikacije. U tom polju se vidi dalja mogućnost integracije podataka, za koju je potrebno napraviti inicijalne slučajeve korištenja, sa testom u stvarnom okruženju.

Na teritoriji Bosne i Hercegovine nadležnost osiguranja je na razini entiteta, što nam postavlja dva različita autoritativna tijela za entitetske teritorijalne cjeline. Neusklađenost reformi i inovacija, što u zakonodavstvu, što u tehnološkim rješenjima osiguranjima stvara dvostruke napore zadovoljenja dva regulatorna tijela u sklopu jedne državne cjeline. Trenutna razmjena podataka u entitetu Federacija Bosne i Hercegovine je riješena već opisanom aplikativnom razmjenom podataka koja se sastoji od web aplikacije i web servisa za integraciju u aplikativna rješenja osiguranja. Tehnološko rješenje na području entiteta Republika Srpska trenutno nije na toj razini već se podaci razmjenuju u tabličnim datotekama, što traži od osiguranja samostalno rješavanje predmetnog problema ukoliko je potrebno postići veću razinu automatizacije. Sa tehnološke strane, rješenja bazirana na web aplikacija i web servisima mogu ponuditi dovoljno za brzu i jednostavnu provjeru baza podataka. Uz postojeću razmjenu podataka o štetama iz autoodgovornosti, osiguranja imaju priliku na isti način stvoriti i ostale zajedničke baze podataka koje bi im pomogle u svakodnevnom poslovanju.

Literatura

[1] Han Jiawei, Kamber M., Data Mining: concepts and techniques, San Francisco: Morgan Kaufman Publishers, 2001: 188-228

[2] Yu Yan, Haiying Xie, Research on the Application of Data Mining Technology in Insurance Informatization, Ninth International Conference on Hybrid Intelligent Systems, 2009: 202-205

[3] Ngai E.W.T., Xiu L., Chau D.C.K., "Application of data mining techniques in customer relationship management: A literature review and classification", Expert Systems with Applications, vol. 36, p. 2592-2602, 2009

[4] Xiahou J., Xu Y., Zhang S., Liao W., "Customer Profitability Analysis of Automobile Insurance Market Based on Data Mining", The 11th International Conference on Computer Science & Education (ICCSE), p. 603-609, 2016.

[5] Hui, S. C., Jha G., "Data mining for customer service support", Information&Managment, vol 38(1), p. 1-13, 2000.

[6] Jiang L., Model of the Insurance Risk Rating based on Neural Network, International Conference on Smart City and Smart Engineering, p. 375-377, 2016.

[7] Jiang L., Quantitative model of Insurance Risk Managment System based on Big Data, International Conference on Smart City and Smart Engineering, p. 590-593, 2016.

[8] Pathak G., Jha A. N., Critical Review of Data Mining Techniques for Insurance Service Operations, International Conference on Technology and Business Management, p. 7-11, 2017.

[9] Sheshasayee A., Thomas S.S., Implementation of Data Mining Techniques in Upcoding Fraud Detection in the Monetary Domains, International Conference on Innovative Mechanisms for Industry Applications, p. 730-734, 2017.

[10] Bolton R.J., Hand D.J., "Statistical fraud detection: "A review", Statistical science, vol. 17(3), p. 235-249, 2002.

[11] Yan C., Li Y., The Identification Algorithm and Model Construction of Automobile Insurance Fraud Based on Data Mining, Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2015.

[12] Pino C., Kavasidis I., Spampinato C., Assessment and Visualization of Geographically Distributed Event-related Sentiments by Mining Social Networks and News, 13th Annual Consumer Communications & Networking Conference, 2016.

[13] Gatteschi V., Lamberti F., Demartini C., Pranteda C., Santamaria V., "Blockchain or not blockchain, that is the question of the insurance and the other sectors", IT professional IEEE, in press, p. 1-12, 2017.

[14] Što je GDPR?, *https://gdpr2018.eu/sto-je-gdpr/, 25.5.2018.*

[15] Mendes R., Vilela J.P., "Privacy-Preserving Data Mining: Methods, Metrics and Applications", IEEE Access, Volume 5, 2017.

[16] Aggarwal C.C., Yu P.S., ąA General Survey of Privacy-Preserving Data Models And Algorithms", *Privacy Preserving Data Mining*, p. 11-52, 2008.

[17] Why Don't Insurance Companies Just Share Data With Each Other?, 18.8.2014., *https://www.bewiser.co.uk/knowledge-base/insurance-thoughts/why-dont-insurance-companies-just-share-data-each-other*, 25.5.2018.

[18] Wang Q., Guo Y.C., Li M., Zhao X.F., ACORD Standards based SOA Solution for Insurance Industry Combine ACORD eForms with Business Services through Xforms Standard, IEEE International Conference on e-Business Engineering, p. 247-254, 2008.

[19] About ACORD, *https://www.acord.org/ACORD-about/ACORD-About*, 25.5.2018.

[20] Gatteschi V., Lamberti F., Demartini C., Pranteda C., Santamaria V., "Blockchain or not blockchain, that is the question of the insurance and the other sectors", IT professional IEEE, in press, p. 1-12, 2017.

[21] Swan M., Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol, California US, p. 1-152, 2015.

[22] Tschorsch F., Scheurmann B., "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", IEEE Communications Survey Tutorials, vol. 18, no. 3, p. 2084-2123, 2016.

[23] Nath I., "Data Exchange Platform to fight Insurance Fraud on Blockchain, IEEE International Conference on Data Mining Workshops, 821-825, 2016.

[24] Disributed Ledger Technology: beyond Blockchain, a report by the UK Government Chief Scientific Advisor, 2016