

## **UTICAJ INTERNET INTELIGENTNIH UREĐAJA NA MODERNE TRENDOVE U OSIGURANJU**

### **Sažetak**

*Internet inteligentnih uređaja (engl. Internet of Things, IoT), Blockchain tehnologija, softverski roboti i razni aspekti veštačke inteligencije, kao trendovi u okviru IV industrijske revolucije<sup>1</sup>, imaju veliki potencijal za primenu u oblasti osiguranja.*

*IoT uređaji senzorima mogu da registruju pokret, dim, temperaturu, zvuk, osvetljenje, vlažnost i slično, aktuatorima mogu da reaguju tako što nešto uključe, isključe, pomere, otvore, zatvore, itd, i mogu da pošalju podatke preko Interneta osiguravajućim kompanijama. Osiguravači na kraju obrađuju primljene podatke od inteligentnih uređaja i mogu da ih koriste za izradu kvalitetnijih tarifa, preciznije merenje rizika, adekvatnije određivanje premije pojedinačnog osiguranika, automatsko dobijanje podataka o štetama, precizniju procenu šteta, preventivu, ...*

*U svetu postoje veliki broj primera uspešno realizovanih projekata u osiguravajućim kompanijama u kojima se koristi Internet inteligentnih uređaja.*

**Ključne reči:** *Internet inteligentnih uređaja, Internet stvari, IoT, osiguranje*

### **Summary**

*Internet of Things (IoT), Blockchain technology, software robots and various aspects of artificial intelligence, as trends within the Fourth Industrial Revolution, have great potential for applications in insurance field.*

*IoT sensors can detect motion, smoke, temperature, sound, lighting, humidity and the like, they can respond by switching something on with actuators, switching off, moving, opening, closing, etc., and sending data via the Internet to insurance companies. Insurers process the data received from intelligent devices and can use it to create better tariffs, more accurate risk measurement, more adequate determination of the premium of an individual insured person, automatic receiving of claims data, more accurate claims assessment, prevention, etc.*

1 Pavlović, B. (2019). *Robot Usage in Insurance*, XVII međunarodni simpozijum „Osiguranje na pragu IV industrijske revolucije“, Zlatibor

*There are several examples of successful projects in the world in insurance companies that use the Internet of intelligent devices.*

**Keywords:** *Internet of Things, IoT, insurance*

## Uvod

Internet inteligentnih uređaja čini veliki broj uređaja sa sensorima, koji su priključeni na Internet i samostalno prikupljaju, dele i koriste podatke bez pomoći čoveka, izvršavajući softverske komande koje je postavio čovek.

IoT uređaji omogućavaju suštinsku digitalizaciju, odnosno obezbeđuju povezivanje digitalnog i fizičkog sveta, tako što sensorima očitani parametri stvarnog sveta ulaze digitalizovani u virtuelni svet Interneta. Po potrebi je moguća i inverzna transformacija, tako što obrađeni podaci zahtevaju intervenciju u stvarnom svetu koja se vrši preko aktuatora. Sa druge strane, potencijalna opasnost je činjenica da ova inovacija previše zadire u privatnost i može imati veliki uticaj na privatni život čoveka.

Na Internet mogu biti povezani televizori, frižideri, sijalice, termostati, radijatori, zvučnici, kontejneri za smeće, prekidači, itd. čiji senzori registruju pokret, dim, temperaturu, zvuk, osvetljenje i slično. Procena Gartnera<sup>2</sup> je da će tokom 2020. godine, broj inteligentnih uređaja povezanih na Internet premašiti 20 milijardi.

Predmet rada je analiza mogućnosti za unapređenje poslovanja delatnosti osiguranja korišćenjem tehnologije Interneta inteligentnih uređaja, kao i izazova koji se pri tom javljaju. Cilj rada je da ukaže na potencijalne koristi od uključivanja osiguravajućih kompanija iz regiona u jedan od trendova koji donosi IV industrijska revolucija.

Naziv Internet of Things<sup>3</sup> je uveo britanski naučnik koji se vodio istraživanje RFID senzora na Masačusetskom tehnološkom institutu (MIT) u Kembridžu, Kevin Ešton, 1999. godine s ciljem da opiše sistem koji povezuje Internet sa fizičkim svetom preko sveprisutnih senzora.

## Definicija

Internet inteligentnih uređaja definiše se<sup>4</sup> kao globalna mrežna infrastruktura koja omogućava povezivanje fizičkih i virtuelnih uređaja interoperabilnim komunikacionim protokolima i inteligentnim interfejsima.

2 Vega, M. (2019). *Connect All the Things – Internet of Things Statistics 2020*. <http://review42.com>

3 Eshton, K. (2009). *That 'Internet of Things' Thing*. <http://www.rfidjournal.com>

4 Radenković, B., Despotović-Zrakić, M. i dr. (2017). *Internet inteligentnih uređaja*. Fakultet organizacionih nauka, Beograd

Internet inteligentnih uređaja se zasniva na velikom broju različitih tehnologija, koje su neophodne za stvaranje okruženja za njegovo funkcionisanje. To su: poluprovodnici, čipovi, procesori, memorije, itd, od kojih je napravljen potreban hardver, softverski moduli za povezivanje uređaja, kao što su npr. API konektori, specijalizovani operativni sistemi i slično, tzv. IoT platforme i bežična ili kablovska mreža, u koju su uređaji povezani.

## Komponente IoT sistema

IoT sistem se sastoji iz tri osnovne komponente: inteligentni (engl. smart) uređaji, mrežna infrastruktura na koju su uređaji povezani i sistemi koji primaju, čuvaju i obrađuju podatke koje generišu i šalju pametni uređaji.

### *Pametni uređaj*

Inteligentni uređaj je jednostavan računar, koji ima napajanje, memoriju, procesor, ulazno/izlazni interfejs za senzore i komunikacioni interfejs, koji može da komunicira s drugim uređajima u okruženju i izvodi operacije koje su unapred programirane. Pametni uređaji se sastoje od nekoliko komponenti. Ključna komponenta svakog IoT pametnog uređaja su senzori za praćenje stanja u okruženju, koji prema vrsti fizičke pojave koju mere, mogu biti podeľjeni na: toplotne, mehaničke, hemijske, optičke, senzore zračenja, akustičke i ostale senzore. Tu spadaju i aktuatori ili upravljački motori koji na osnovu promena u okruženju koje detektuju senzori, izvršavaju aktivnosti u fizičkom svetu, kao i mikrokontroleri sa interfejsima za povezivanje na druge uređaje: senzore, aktuatore i komunikacione uređaje za bežični prenos podataka. Na kraju, upravljačka komponenta je mikroročunar koji ima mikroprocesor, memoriju i ulazno-izlazne uređaje.

Najčešće se koriste sledeći operativni sistemi otvorenog koda za pametne uređaje: Contiki, kao prvi operativni sistem koji je omogućio IP komunikaciju, implementiran u programskom jeziku C i FreeRTOS, operativni sistem koji omogućava pokretanje aplikacije u realnom vremenu, baš kada neki događaj u sistemu treba da se dogodi i mogućava TCP/IP komunikaciju.

IoT uređaji se povezuju, razmenjuju podatke i analiziraju ih bez učešća ljudi u tim procesima. Ljudska intervencija je potrebna samo pri instalaciji i programiranju uređaja.

Internet inteligentni uređaji mogu biti: kućni aparati, štampači, automobili, industrijske mašine, uređaji u energetske sistemima, uređaji u zdravstvenim sistemima i drugi. Iako su po svojstvima slični, računari, pametni telefoni i ruteri ne smatraju se IoT uređajima, nego delom tradicionalnog Interneta. OECD, s druge strane, smatra<sup>5</sup> da takva podela nije ispravna, jer su pomenuti uređaji mozak i srce svakog sistema u koji su uključeni pametni uređaji.

5 OECD (2015). *OECD Digital Economy Outlook 2015*. OECD Publishing

### **Mrežna infrastruktura**

Mrežnu infrastrukturu čine ruteri, svičevi, kablovi, i sl. Uobičajeno su IoT uređaji povezani na Internet bežičnim putem. Bežične senzorske mreže koriste male višenamenske platforme koje se samostalno bežično povezuju i prikupljene podatke iz senzora dostavljaju udaljenim sistemima koji obrađuju podatke.

Međusobna komunikacija inteligentnih uređaja omogućava očitavanje merenja raznih fizičkih parametara, daljinsko upravljanje različitim uređajima, praćenje zdravstvenog stanja pacijenata, sigurnosni nadzor na daljinu, automatizaciju raznih industrijskih procesa itd.

Najčešće se koriste sledeći protokoli za komunikaciju IoT uređaja:

- Ethernet (IEEE 802.3 standard) je najšire korišćena žična tehnologija za LAN i WAN mreže, karakterističan po tome što svaki uređaj u Ethernet mreži ima karticu za interfejs s 48-bitnom MAC adresom, koja je jedinstven identifikator uređaja;
- Wi-Fi (IEEE 802.11 standard) je tehnologija za lokalne bežične mreže;
- WiMAX (IEEE 802.16 standard) je dobio ime od engl. Worldwide Interoperability for Microwave Access, to je širokopolasna bežična tehnologija koja se može koristiti na većim udaljenostima, s većom brzinom protoka i za više korisnika od Wi-Fi tehnologije.
- Bluetooth (IEEE 802.15.1 standard) predstavlja primer ad hoc bežičnog umrežavanja velikog broja uređaja putem radio-talasa;
- ZigBee (IEEE 802.15.4 standard) omogućava pristup LR-WPAN (engl. Low Rate Wireless Personal Area Networks) bežičnoj mreži kratkog dometa i malih brzina prenosa podataka.

### **Sistemi za obradu i čuvanje podataka**

Optimalno rešenje za razvoj i korišćenje aplikacija koje koriste IoT podatke je računarstvo u oblaku.

Računarstvo u oblaku (eng. Cloud Computing) omogućava korisnicima, na zahtev, putem Interneta, pristup svim potrebnim računarskim resursima: serverima, skladištima podataka, aplikacijama, servisima itd. Zasniva se na tehnologiji virtuelizacije, koja podrazumeva smeštanje servisa i podataka korisnika na deljenim resursima i infrastrukturi provajdera.

Povećanjem korišćenja interneta inteligentnih uređaja značajno se povećava količina podataka koji se prenose preko Interneta i čuvaju u skladištima podataka širom sveta. Takve podatke nije moguće obrađivati primenom tradicionalnih alata za upravljanje bazama podataka. Zato su razvijeni novi načini skladištenja i analize velikih količina podataka u realnom vremenu, zasnovani na Big Data tehnologijama.

Pojam Big Data podrazumeva informacioni resurs velike količine, velike brzine i velike raznovrsnosti podataka, koji zahteva nove i inovativne metode obrade i optimizacije informacija i poboljšanje uvida u sadržaj podataka i donošenje odluka.

## Komercijalni proizvodi za IoT

Velike svetske tehnološke kompanije su prepoznale potencijal Internet inteligentnih uređaja i ulažu velika sredstva u razvoj njegovih pojedinih komponenti<sup>6</sup>. Najpoznatiji komercijalni proizvodi su Amazonov pametni virtuelni asistent Alexa, Appleov asistent Siri na mobilnim uređajima, Samsungov pametni televizori i slični uređaji za domaćinstvo koji su povezani na Internet. Čipove za IoT hardver proizvode Texas Instruments, Intel, Silicon Labs, itd. Koristi se mrežna oprema kompanija Cisco, Huawei i Ericsson. Usluge računarstva u oblaku obezbeđuju Google Cloud Platform, Amazon Web Services, Microsoft Azure, IBM Watson i drugi provajderi. Povezivanje omogućavaju najveći mobilni operateri, operateri koji obezbeđuju satelitske veze i specijalizovani operateri za IoT mreže kao što je SigFox i LoRa Alliance. Razvijena su i specifična softverska razvojna okruženja za IoT, kao što su Eclipse i Arduino IDE i operativni sistemi prilagođeni za IoT, kao npr. Raspbian.

## Istorijski razvoj i pregled literature

Veliki broj autora u svetu se bavio Internetom inteligentnih uređaja u poslednjih četrdesetak godina, dok se su primenom ove tehnologije u delatnosti osiguranja autori počeli intenzivnije baviti relativno skoro, pre desetak godina. Autori u Srbiji su takođe pokazali interesovanje za ovu temu.

Osnovni koncept povezanih pametnih uređaja je razrađen na Univerzitetu Carnegie Mellon na modifikovanom uređaju Coca-Cole za prodaju pića 1982. godine, koji je mogao da obavesti centralu koliko još limenki ima za prodaju i da li su limenke kojima je dopunjen uređaj dovoljno rashlađene.

Mark Weiser<sup>7</sup> je 1991. godine u svom radu „Kompjuter XXI veka“ opisao viziju savremenog Interneta inteligentnih uređaja, dok je Reza Raji<sup>8</sup> 1994. godine objavio u IEEE časopisu koncept IoT.

Prvi pokušaji realizacije Interneta inteligentnih uređaja bili su Microsoft at Work (MaW)<sup>9</sup> i Novell Embedded System Technology (NEST).<sup>10</sup> MaW je obezbeđivao protokole za povezivanje aparata za fotokopiranje i fax mašine sa kompjuterom i Lexmark je isporučio prvi takav uređaj, WinWriter 600, 1994. godine. Zbog malo uređaja koji su podržavali takav protokol, od projekta se odustalo već 1995. godine. Novell je želeo da poveže na mrežu uređaje kao što su TV set top box, uređaje za prodaju slatkiša i slično. Lexmark i još nekoliko proizvođača štampača su se uključili u projekat 1994. godine. Iz istih razloga kao i Microsoft, Novell je odustao od projekta NEST 1997. godine.

6 OECD (2018). IoT Measurement and Application. *OECD Digital Economy Papers No. 271*. OECD Publishing.

7 Weiser, M. (1991). The Computer for the 21<sup>st</sup> Century. *Scientific American* 265 (3), p. 94-104.

8 Raji, R. (1994). Smart Networks for Control. *IEEE Spectrum* 31 (6), p. 49-55.

9 Baran, N. (1995). Whatever Happened To... Microsoft At Work? *Byte Magazine Vol 20* (7) p. 30.

10 Salamone, S. (1995). Novell Builds a NEST. *Byte Magazine Vol 20* (8) p. 151-152.

Naziv Internet of Things<sup>11</sup> je uveo britanski naučnik na Masačusetskom tehnološkom institutu (MIT) u Kembridžu, Kevin Ešton, 1999. godine, kao naslov prezentacije za Procter & Gamble o unapređenju njihovog lanca snabdevanja.

Cisco je uveo zanimljivu definiciju Interneta inteligentnih uređaja, kao trenutak kada će više uređaja nego ljudi biti povezano na Internet, što se dogodilo 2008 godine. Iste godine grupa kompanija među kojima su bili Cisco i Sun, promovisala je IPSO (engl. IP for Smart Objects) Alliance s ciljem promovisanja korišćenja IP protokola za umrežavanje pametnih uređaja.

Sektor za standardizaciju telekomunikacija Agencije Ujedinjenih nacija ITU (engl. International Telecommunication Union) formirao je radnu grupu Global Standards Initiative on Internet of Things (IoT-GSI), koja je 2012. godine definisala IoT<sup>12</sup> kao globalnu infrastrukturu informatičkog društva koja omogućava napredne usluge (fizičkim i virtualnim) umrežavanjem stvari, pritom se zasnivajući na postojećim i interoperabilnim informacionim i komunikacionim tehnologijama u razvoju.

Domaći autori su u poslednjih nekoliko godina objavili radove o primeni IoT u infrastrukturi obrazovnih institucija,<sup>13</sup> edukativnim igrama,<sup>14</sup> nadgledanju kulturne baštine,<sup>15</sup> unapređenju maloprodaje,<sup>16</sup> merenju zdravstvenih parametara u uređajima u odeći,<sup>17</sup> železničkom saobraćaju,<sup>18</sup> itd.

## Koncept IoT

Osnovni koncept Interneta inteligentnih uređaja je objašnjen na Slici 1. Ključna osobina IoT uređaja je dodavanje vrednosti klasičnim proizvodima njihovim povezivanjem na Internet, odnosno dodavanje digitalne usluge fizičkom proizvodu koja unapređuje njegovu osnovnu funkciju. Na taj način se dobija novi proizvod, kroz sinergiju fizičkog proizvoda i digitalne usluge, koji zajedno imaju veću vrednost, nego što je zbir njihovih pojedinačnih vrednosti.

11 Eshton, K. (2009). *That 'Internet of Things' Thing*. <http://www.rfidjournal.com>

12 Global Standards Initiative on Internet of Things (2012). *Recommendation ITU-T Y.2060*

13 Simić, K., Despotović-Zrakić, M. i dr. (2015). *Model infrastrukture obrazovne institucije zasnovan na Internetu inteligentnih uređaja*. Infoteh Jahorina Vol 14. str. 681-685.

14 Petrović, L., Jezdović, I. i dr. (2017). *Razvoj edukativne igre zasnovane na Internetu inteligentnih uređaja*. Infoteh Jahorina Vol. 16, str. 506-509.

15 Matejić, T., Marković, N. i dr. (2017). *Monitoring dobara materijalne kulturne baštine primenom interneta inteligentnih uređaja*. Časopis Info M 64, str. 11-17.

16 Tomanović, I. (2017). *Primena internet inteligentnih uređaja u unapređenju maloprodaje*. Časopis Info M 64, str. 18-25.

17 Rodić Trmčić, B., Labus, A. & Bodanović Z. (2016). *Model mobilnog zdravstva zasnovan na tehnologijama wearable computinga*. Časopis Info M 57, str. 48-54.

18 Mladenović, S., Uzelac, A. i dr. *IoT u železničkom saobraćaju – realnost i izazovi*. In: Zbornik radova sa XXXIV Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju, PosTel 2016.

Slika 1. Logika proizvoda i usluga u Internetu inteligentnih usluga

Predmet	+	hardver i softver	=	Funkcija predmeta	+	Dodatna digitalna usluga
	+		=	Merenje vremena	+	Telefoniranje
	+		=	Čuvanje stvari u kutiji	+	Dopuna
	+		=	Vožnja	+	Iznajmljivanje bicikla i upravljanje flotom
	+		=	Rashlađivanje	+	Uspostavljanje energetske efikasnosti, daljinsko upravljanje i smanjenje troškova
	+		=	Vožnja	+	Osiguranje, naplata korišćenja, sprečavanje krađa, prepoznavanje stila vožnje
	+		=	Osvetljavanje	+	Bezbednosni nadzor, kontrola temperature i daljinska kontrola
	+		=	Bilo šta	+	Uputstva za instalaciju i održavanje, raspored i istorija održavanja, naplata korišćenja, usluga dopune, provera garancije, osiguranje, itd.

Izvor: Fleisch, E., Weinberger, M. & Wortmann, F. (2014). *Business Models and the Internet of Things*. Bosch IoT Lab White Paper, p. 8.

Appleov sat, iWatch, je i dalje sat, ali ima i mikrofon, zvučnik, GSM karticu ili bluetooth vezu sa mobilnim telefonom, tako da može da posluži i za telefoniranje i za pristup sadržajima mobilnog telefona iPhone. Pomenuti sat ima i dodatnu funkciju modnog detalja. Kutija kompanije Intellion pored osnovne funkcije čuvanja predmeta, ima senzore koji detektuju njenu popunjenost i kada se isprazni do određenog nivoa, kutija kontaktira prodavca da pošalje dopunu proizvoda. Bicikl sa elektronikom za upravljanje otključavanjem bicikla i GPS uređajem za omogućavanje praćenja njegove trenutne lokacije, od običnog prevoznog sredstva postaje sofisticirani uređaj. IoT bicikl se može iznajmiti bez kontakta sa prodavcem, preuzimanjem sa određenih lokacija u gradu uz pomoć mobilne aplikacije i umesto vraćanja na istu lokaciju može se ostaviti bilo gde u gradu. Klima uređaj sa sensorima, koji je povezan na Internet, omogućava daljinsko upravljanje preko mobilne aplikacije ili web sajta i uspostavljanje energetske efikasnošću prostora u kome se nalazi. Na kraju, bilo koji uređaj IoT transformacijom može biti značajno unapređen. U najvećem broju slučajeva može se pratiti njegovo održavanje, realnije naplaćivati njegovo korišćenje, poboljšati osiguranje uređaja, omogućiti pristup uputstvima za instalaciju i korišćenje, itd.

## Karakteristike IoT

Glavne karakteristike IoT uređaja su:

- dinamički se prilagođavaju okruženju i samostalno reaguju na promene iz okruženja,
- konfigurišu se uz minimalno učešće korisnika,
- međusobno komuniciraju standardizovanim interoperabilnim komunikacionim protokolima,
- imaju jedinstven identifikator, na primer IP adresu ili jedinstveni identifikator resursa (eng. Uniform Resource Identifier, URI), pomoću koga korisnici mogu da pristupaju uređaju preko Interneta, daljinski upravljaju uređajem, konfigurišu ga i prate njegov status,
- povezani su u računarsku mrežu koja omogućuje da međusobno komuniciraju i da budu vidljivi ostalim uređajima i aplikacijama.

## Biznis modeli i Internet inteligentnih uređaja

Razvoj Interneta je doveo do radikalne transformacije standardnih biznis modela u raznim oblastima. U prvoj fazi komercijalnog razvoja Interneta od 1995. do 2005. godine, biznis modeli su koristili Internet samo kao infrastrukturu za npr. e-trgovinu. Od 2005. godine, u drugoj fazi, biznis modeli su počeli da koriste Internet na način društvenih mreža, tako da korisnici mogu da doprinose sadržaju. Pojavili su se novi biznis modeli kao što su Open Source zajednice, prikupljanje sredstava Crowdfunding i slični. U trećoj fazi razvoja



Interneta, od 2015. godine, kod Interneta inteligentnih uređaja, senzori doprinose stvaranju dodatne vrednosti kroz dva modela: digitalno opremljeni proizvodi i senzor kao servis.

### **Digitalno opremljeni proizvodi**

Ovaj biznis model podrazumeva da su fizički proizvodi opremljeni velikim brojem novih digitalnih mogućnosti, koje se obično baziraju na upotrebi senzora i na taj način obezbeđuju dodatnu vrednost. Sastoji se od 6 komponenti<sup>19</sup>:

1. Physical Freemium – fizički proizvod se prodaje zajedno sa besplatnom (engl. Free) digitalnom uslugom, kao što je npr. instalacija i uputstvo za održavanje. Tokom korišćenja proizvoda, korisnici mogu da odluče da plaćaju naprednu digitalnu uslugu (engl. Premium) kao što je npr. daljinski nadzor nad ispravnosću proizvoda.
2. Digitalni dodatak – primenjuje se na fizičke proizvode, čija osnovna verzija se prodaje jeftino, praktično po fabričkoj ceni i kod kojih je moguće posle kupovine aktivirati dodatne funkcionalnosti ili poboljšati postojeće performanse. Primer može biti automobil sa relativno malom snagom motora, kod koga se može dokupiti po želji dodatna količina konjskih snaga i to poboljšanje daljinski aktivirati od strane proizvođača.
3. Digitalno zaključavanje – kod fizičkih proizvoda, senzori onemogućavaju korišćenje rezervnih delova ili potrošnog materijala koji nije od originalnog proizvođača, kao što je npr. laserski štampač koji ne dozvoljava korišćenje dopunjenih ili repariranih tonera.
4. Proizvod kao mesto prodaje – fizički proizvod postaje digitalna prodavnica ili mesto na kome se vrši digitalno oglašavanje. Npr. mobilni telefon može da očita bar ili QR kod sa proizvoda i otvori web prodavnicu koja za konkretan proizvod nudi dodatke ili rezervne delove sa popustom.
5. Samoopslužujući objekat – fizički proizvod koji može samostalno da naruči preko Interneta nešto što mu je potrebno za nesmetani rad, kao npr. pametni motor koji samostalno naručuje motorno ulje, kada mu količina ulja padne ispod definisanog nivoa.
6. Daljinsko korišćenje i nadgledanje uslova za rad – fizički proizvod koji može da pošalje podatke o sopstvenom statusu i uslovima iz okruženja u kome radi, zahvaljujući čemu može da se preventivno deluje i spreče kvarovi, kao i naplaćuje usluga koju proizvod pruža umesto da se prodaje proizvod. Primer su pametni štampači, čiji rad vlasnici nadgledaju preko Interneta i koje korisnici dobijaju besplatno, a zatim plaćaju mesečno korišćenje po broju odštampanih stranica.

19 Fleisch, E., Weinberger, M. & Wortmann, F. (2014). *Business Models and the Internet of Things*. Bosch IoT Lab White Paper

### **Senzor kao servis**

Model podrazumeva skupljanje, obradu i prodaju podataka koji se dobijaju od senzora. Omogućava da očitavanje podataka koje vrši senzor i obrada podataka nisu više integrisani u jednu aplikaciju, nego podatke iz jednog senzora može koristiti ceo ekosistem različitih aplikacija. Fokus ovog biznis modela nije na usluzi, nego na obezbeđenju podataka za razne digitalne usluge. Primer je američka kompanija Streetline koja je instalirala senzore na parking mesta u nekoliko manjih američkih gradova (St. Petersburg na Floridi, San Mateo i Oakland u Kaliforniji, itd.) i prodaje informaciju o slobodnim parking mestima zainteresovanim vozačima, ali i gradskim vlastima koje ih obrađuju na nivou celog grada u cilju poboljšanja usluge i praćenja naplate parkiranja.

### **Primena IoT**

Implementacija inteligentnih uređaja se može sresti u velikom broju različitih oblasti, uključujući osiguranje, o čemu će biti kasnije više reči u ovom radu. To su monitoring vitalnih parametara pacijenata i sportista korišćenjem odevnih IoT uređaja, pomoć pacijentima u svakodnevnom životu i medicinski servisi, bezbednosni nadzor, praćenje vremenskih prilika, zagađenosti vazduha, buke, požara i poplava, automatizacija sistema navodnjavanja i kontrola staklenih bašti u poljoprivredi, plaćanje preko Point of Sale terminala, vojna primena u naprednim oružjima i sistemima i slično.

Automatizacija stanova, kancelarija, odnosno kuća i poslovnih zgrada je moguća pomoću pametnih uređaja za kontrolu struje, svetala i grejanja, daljinskog upravljanja medijima, praćenja energetske efikasnost, automatizacije održavanja, daljinskog očitavanja i merenja različitih parametara, senzora za hemijsko, biološko, radiološko i nuklearno narušavanje bezbednost prostora, itd.

Gradovi postaju pametni zahvaljujući telemetriji koja uključuje pametne parkinge, daljinska merenja, upravljanje odnošenjem komunalnog otpada i postavljanje raznih automata po gradu, zatim inteligentnim transportnim sistemima, pametnom upravljanju gradskim saobraćajem, povezivanju građana sa javnom infrastrukturom, upravljanju gradskom distributivnom električnom mrežom, itd.

Industrijska postrojenja i fabrike su značajno unapredili svoj svakodnevni rad implementacijom kontrole lanca snabdevanja u kome se prati tok pojedinačnih proizvoda, dok se popunjenošću magacina i uslovima čuvanja u njima upravlja pametnim uređajima. Upravljanje određenim proizvodnim procesima je omogućeno zahvaljujući pametnim IoT uređajima. Jedan od primera je održavanje optimalnog nivoa kiseonika tokom sušenja mesa. Takođe, primer je i zalivanje njiva optimalnom količinom vode u zavisnosti od izmerne vlažnosti zemljišta.

Upravljanje voznim parkom podrazumeva da IoT uređaji omogućavaju uvođenje autonomnih vozila i unapređenje sledećih usluga: bezbednosti vozača

i putnika, servisa za hitne slučajeve, upravljanja i nadzora iznajmljenih vozila, integracije servisa za zabavu i informacije za putnike, GPS servisa, kao i udaljeno dijagnostikovanje kvarova, odnosno ispravnosti vozila.

Logistika i transport su takođe plodno tle za primenu pametnih uređaja koji mogu da mere vibracija, proveravaju da li su kontejneri zatvoreni, pronalaze pojedinačni artikal u velikim lučkim magacinima, prate gustinu javnog saobraćaja u cilju pronalaženja optimalnih puteva snabdevanja, uočavaju oštećenja kolovoza, prate isporuku robe, itd.

Razni uređaji su u današnje vreme dobili Internet konekciju i određeni nivo inteligentnog ponašanja. Prema istraživanju Gartnera<sup>20</sup> više od polovine svih inteligentnih uređaja su kućni potrošački proizvodi, ali su najprodavaniji IoT uređaji u svetu sigurnosne kamere i pametna električna brojila.

## Izazovi u primeni IoT

Mnoge kompanije se uzdržavaju od primene novih tehnologija, jer nisu sigurne da su očekivane koristi od implementacije dovoljno velike da se isplati borba sa svim izazovima. Implementacija Interneta inteligentnih uređaja donosi određene nedoumice u vezi bezbednosti rada na Internetu. Sa povezivanjem uređaja na Internet, javlja se ozbiljna pretnja od napada hakera i zloupotrebe podataka iz senzora. U slučaju uspešne kompromitacije podataka sa senzora, dodatni rizik je u automatskom odgovoru sistema na pogrešne ulazne podatke, koji sigurno ne može biti adekvatan. Zbog toga se od početka implementacije IoT tehnologije, posebna pažnja obraća na cyber bezbednost. S obzirom da je cela IoT platforma povezana na Internet i otvorena za napade, ne može se nikad potpuno sigurno tvrditi da hakeri neće uspeti u svojim namerama. Ipak primenom sledećih mera, može se rizik od hakerskih napada svesti na razumnu meru: uvođenje demilitarizovane zone u sistem, sistematsko upravljanje identitetima na lokalnoj mreži, VPN konekcije sa IoT uređajima, nadgledanje upada u sistem, adekvatno upravljanje mrežnom opremom, ažuriranje verzija operativnog sistema i softvera, primena svih raspoloživih zakrpa, redovna procena cyber rizika uz pomoć IT revizora, izvođenje penetration testova, detekcija ranjivosti sistema i priprema plana mera za slučaj otkrivanja napada hakera.

Skladištenje i obrada velike količine podataka koja dolazi od IoT uređaja može predstavljati izazov za standardnu serversku opremu koja inače zadovoljava potrebe prosečne kompanije. Takođe, transport velike količine podataka od IoT uređaja do mesta u kompaniji gde se podaci obrađuju, zahteva izuzetnu mrežnu infrastrukturu.

Povraćaj investicije u IoT nije potpuno izvestan, što dodatno otežava odluku rukovodstva kompanije o implementaciji. Pored bezbednosnih rizika,

20 Antić, D. (2019). Šta je Internet of Things (Internet inteligentnih uređaja)? <http://samoobrazovanje.rs>

upravljanje organizacionim promenama koje zahtevaju rušenje „silosa“ u organizacijama, povećava neizvesnost uspeha implementacije. Uvođenje IoT integriše i menja sve procese i sektore u kompaniji, na šta pojedini sektori često nisu spremni. Takođe, zahteva nova znanja i tehnološke veštine, usvajanje novih modela poslovanja, kao i promenu načina rada i razmišljanja zaposlenih, čemu se određeni broja radnika ne može prilagoditi.

Integracija sa sistemima sa zastarelom tehnologijom može biti izazov za implementaciju IoT u pojedinim kompanijama. Da li ima smisla zameniti mašinu staru 25 godina u fabrici, koja i dalje savršeno radi svoj posao, samo da bi nova mašina bila kompatibilna sa IoT tehnologijom? Da li će korist od uvođenja IoT biti dovoljno velika da isplati novu mašinu? Ako se ignorišu nove tehnologije, koliko će dugo kompanija opstati na tržištu?

Ne sme se zaboraviti ni uticaj IoT tehnologije na čovekovu okolinu. Senzori mogu da detektuju zagađenje, ali su i sami zbog svoje masovnosti značajna komponenta elektronskog otpada. Pošto se u današnje vreme manji elektronski uređaji ni ne pokušavaju popraviti nego se u slučaju bilo kakvog kvara odmah bacaju, nije neočekivan podatak da ljudi godišnje odbace<sup>21</sup> oko 50 miliona tona elektronskog otpada. Na žalost, samo oko 12% ovog otpada se reciklira, iako bi milioni kilovata električne energije mogli biti uštedeni, kada bi se recikliralo više. Velike količine IoT uređaja se izbacuju iz upotrebe godišnje i pošto se samo mali deo reciklira, to nepovoljno utiče na globalne klimatske promene.

Na kraju pravni rizik uvođenja IoT platformi ne može biti zanemaren. Pitanje vlasništva nad podacima je i dalje otvoreno, dok se privatnost podataka relativno lako može ugroziti.

Pri donošenju odluke o implementaciji IoT tehnologije, važno je dobro proučiti sve pomenute izazove. Ako se donese odluka, preduslov za uspešnu implementaciju je pripremanje strategije za izbegavanje svih potencijalnih problema.

## Dalji razvoj IoT

Internet inteligentnih uređaja će nastaviti svoj izuzetno brz razvoj zahvaljujući sledećim najnovijim tehnologijama koje već počinju da se implementiraju u praksi: računarstvo u magli (engl. Fog Computinga), 5G mobilne mreže i Blockchain.

### *Računarstvo u magli*

Kada bi svaki senzor, na svakom IoT uređaju na svetu, slao podatke u oblak, saobraćaj ka oblaku bi bio preopterećen. Pošto se na osnovu prikupljenih podataka u oblaku kreira akcija na određenom IoT uređaju pojavilo bi se

21 Suresh, P., Vijau, D. et. al. (2014). A state of the art review on the Internet of Things (IoT) - History, Technology and fields of deployment. In: *International Conference on Science, Engineering and Management Research (ICSEMR 2014)*. Chennai: Institute of Electrical and Electronics Engineers (IEEE).

nezanemarljivo kašnjenje akcije, zbog preopterećene mreže. Cena slanja svih podataka u oblak na obradu bi bila prevelika, a čekanje na povratnu informaciju neprihvatljivo dugo. Zato je realizovan decentralizovan mrežni dizajn za Internet inteligentnih uređaja, pa se od centralizovanog oblaka, prelazi se na fog i edge computing.

S obzirom na postojeću količinu podataka koju generišu IoT uređaji, brzinu mreže i brzinu reakcije, logično je da se obrada podataka izvršava dalje od oblaka, u edgeu, odnosno mestu koje je najbliže uređaju koji se prikuplja podatke ili u magli. IoT senzor je osnovni nivo edge computinga, dok se računarstvo u magli nalazi se u okolini mesta gde se prikupljaju podaci i ima za cilj da rastereti oblak od potreba edge computinga. Definicija američkog Nacionalnog instituta za standarde i tehnologiju fog computinga<sup>22</sup> kaže da je to horizontalna paradigma fizičkog ili virtuelnog resursa koji leži između pametnih uređaja i tradicionalnog data centra ili oblaka.

IoT uređaji i senzori koriste fog i edge za brzu razmenu i analizu podataka, dok se u oblaku smeštaju podaci za napredniju analizu radi stvaranja baze mašinskog učenja. Sve što mašine nauče u svom radnom veku biće smešteno u oblaku<sup>23</sup>, odakle će nove mašine i uređaji preuzimati uputstva i smernice za rad bez potrebe da ponovo prolaze fazu mašinskog učenja.

### **5G mreža mobilne telefonije**

Peta generacija mobilne telefonije naziva se 5G. Njen inicijalni standard je definisan krajem 2017. godine. Omogućuje deset do sto puta brži prenos podataka nego 4G. Brzina prenosa podataka je do deset gigabita u sekundi. Kašnjenje u prenosu je manje od milisekunde, što je jedna od ključnih prednosti. Ima sposobnost da međusobno poveže mnogo više uređaja kao što su senzori i IoT oprema nego 4G. Milimetarski kratki talasi koje 5G koristi mogu da prenose veliku količinu informacija, ali ne mogu da dođe daleko i ne prolaze dobro kroz prepreke poput zidova, tako da je za komforno korišćenje ove mreže neophodno mnogo više baznih stanica nego u slučaju ranijih generacija. Najveći svetski mobilni operateri su počeli s testiranjem, pojavili su se prvi 5G telefoni, ruteri, i ostala oprema. Finska je prva na svetu<sup>24</sup> pustila komercijalni 5G signal u junu 2018. godine, u Helsinkiju i još 3 grada.

### **Blockchain tehnologija**

Blockchain može da posluži kao medijum kroz koji pametni uređaji razmenjuju podatke, obezbeđujući njihovu pouzdanost i transparentnost. Pošto Blockchain tehnologija obezbeđuje bezbednu razmenu vrednosti između

22 Iorga, M., Feldman, L. et al. (2018). *Fog Computing Conceptual Model*. National Institute of Standards and Technology Special Publication 500-325

23 Kovanović, M. (2017). *Posle oblaka dolazi magla*. Beograd: PC Press 241.

24 Bujanja, B. (2019). *Sve o 5G tehnologiji: U petoj brzini!* Beograd: PC Press 267.

entiteta u distribuiranoj mreži, pojavila se nova klasa IoT aplikacija. Npr. proizvođači automobila mogu da koriste Blockchain za autentifikaciju interakcija između povezanog pametnog vozila koje se može smatrati IoT uređajem i putne infrastrukture.

### ***Integracija IoT sa najnovijim tehnologijama***

Integracija IoT sa veštačkom inteligencijom, Blockchain tehnologijom i računarstvom u magli donosi velike mogućnosti. Npr.<sup>25</sup> moguće je realizovati autonomno vozilo. Distribuirana i troškovno efikasna veštačka inteligencija, povezana preko brze mreže sa unutrašnjošću vozila, ali i spoljašnjim centrima upravljanja, može da donosi pravovremene odluke, na osnovu velikog broja integrisanih podataka koji se procesiraju pomoću računarstva u magli i u koje nema sumnje zahvaljujući Blockchain tehnologiji. Zahvaljujući tome, vozilo može da se kreće brzo, dinamično i bezbedno po javnim putevima, praktično bez intervencije čoveka.

Ethereum Blockchain je specijalizovan za pametne ugovore. Npr. podaci iz IoT uređaja mogu da izazovu određene akcije na osnovu ugovora o kasko osiguranju vozila. Ako senzori na vozilu detektuju oštećenje, veštačka inteligencija će odrediti veličinu oštećenja i cenu popravke i automatski će se prebaciti novac sa računa osiguravajuće kompanije na račun osiguranika.

Mašinsko učenje, kao deo veštačke inteligencije, ima veliku primenu u sprečavanju prevara u osiguranju. Zahvaljujući tome, moguće je prepoznati vrlo brzo i efikasno, sa velikom verovatnoćom, čak u portfelju najvećih osiguravača, veoma sofisticirane pokušaje prevara u osiguranju. Uključivanje IoT uređaja dodatno može da poboljša borbu protiv prevara. Npr. podaci iz senzora vozila mogu da pomognu da se otkrije kako je došlo do oštećenja vozila.

### **Primena IoT u osiguranju**

Postoji veliki potencijal u osiguravajućim kompanijama za primenu IoT za izradu kvalitetnijih tarifa, preciznije merenje rizika, adekvatnije određivanje premije za osiguranike, automatsko dobijanje podataka o štetama, precizniju procenu šteta, preventivu, itd.

#### ***Tarife***

Obilje podataka od IoT uređaja može poslužiti osiguravajućim kompanijama da preciznije izmere rizike, uvedu veći broj parametara u tarife i tako adekvatnije naplate rizik osiguranicima, pa čak da u budućnosti uvedu i individualnu tarifu za svakog osiguranika. Trenutno se u osiguravajućim kompanijama najviše

---

<sup>25</sup> Rabah, K. (2018). Convergence of AI, IoT, Big Data and Blockchain: A Review. The Lake Institute Journal Vol. 1 (1), p. 1.18.

radi na upotrebljavanju podataka sa telematskih uređaja za osiguranje vozila za određivanje konkretnog rizika svakog vozača.

### **Preventiva**

Kada se identifikuje neodgovarajuće ponašanje ugovarača, osiguravač će biti u prilici da reaguje na vreme i predloži, a čak u određenim slučajevima i sprovede korektivne akcije. Takođe, unapred programirane korektivne akcije za pojedine vrste osiguranja, kao što su osiguranje imovine i odgovornosti, moći će automatski da isprave ljudske greške i tako značajno smanje frekvenciju šteta.

### **Rešavanje šteta**

Kada se dogodi osigurani slučaj, senzori će poslati dovoljno podataka za brzu procenu štete. Biće olakšano odlučivanje o opravdanosti odštetnog zahteva, jer će se za svakog osiguranika i osiguranu stvar znati da li se ponašaju u skladu sa ugovorenim uslovima, npr. da li je osigurani brod plovio odobrenom putanjom, da li su osigurane zalihe bile čuvane na odgovarajućoj temperaturi, i slično.

### **Ostalo**

Pored standardnih procesa iz delatnosti osiguranja, IoT se može primeniti i za poboljšanje korisničkog iskustva sa osiguravajućim kompanijama, odnosno za povećanje lojalnosti osiguranika. IoT može pomoći da se kreira dodatna vrednost i za osiguranika i za osiguravača i na taj način ojača njihova veza. Osiguravajuće kompanije mogu dobiti veliku količinu ličnih podataka osiguranika, koji mogu biti upotrebljeni za bolje razumevanje osiguranikovog zdravlja, uslova života, životne sredine u kojoj živi, kretanja, itd. s ciljem da mu se ponudi bolja i prilagođenija usluga.

Implementacija savremenih tehnologija u osiguranje, kao sporedni efekat, koji nije nevažan, menja utisak milenijalaca da je delatnost osiguranja dosadna, a proizvodi nerazumljivi. Naprotiv, budi im želju da rade u osiguravajućim kompanijama i da se interesuju za proizvode osiguranja, koji im omogućavaju dodatnu korist, kao npr. savete o stilu vožnje ili zdravlju.

## **Izazovi upotrebe IoT u osiguraju**

Kao i svaka druga tehnologija i IoT nosi sa sobom specifične izazove<sup>26</sup>.

### **1. Drastična promena postojećeg biznis modela**

Očigledne koristi od primene IoT za osiguravače su bolje upravljanje rizicima i smanjenje šteta. Te koristi dovode do znatnog smanjenja premije osiguranja, što može biti veliki problem za tradicionalni biznis

<sup>26</sup> Black, N. (preuzeto 2020.) *5 Challenges for IoT in the insurance industry*. [www.sas.com](http://www.sas.com)

model osiguranja. Kako štete postaju manje i ređe, prirodno se smanjuje i strah od rizika, odnosno smanjuje se potražnja za osiguranjem.

Tradicionalne osiguravajuće kompanije se suočavaju sa dodatnim problemom, jer se na polju IoT osiguranja takmiče sa novim kompanijama koje su fokusirane samo na taj segment, zbog čega mogu da posluju jeftinije i efikasnije. Takođe u IoT osiguranje planiraju uključene i proizvođači automobila i velike IT kompanije kao Google i Amazon, koje imaju inicijalnu prednost, jer su već razvile određenu IoT tehnologiju za vozila.

Na kraju, osiguranje koje se oslanja na Internet inteligentnih uređaja donosi velike popuste osiguranicima koji imaju manji rizik, i veliki minus onim drugim. Zato se može desiti da većina dobrih klijenata pređe kod novih tehnoloških kompanija koje koriste IoT u merenju rizika, dok loši ostaju kod tradicionalnih osiguravača, čime postojeća cena osiguranja kod njih postaje neodrživa.

Na kraju, kako IoT uređaji u autonomnim vozilima budu preuzimali brigu o sigurnosti u vožnji, tako će obavezno osiguranje od autoodgovornosti vozača i vlasnika postati manje bitno, a fokus će se premestiti na osiguranje od odgovornosti proizvođača vozila i upravljača puteva.

## **2. Upravljanje podacima**

Delatnost osiguranja se zasniva na korišćenju podataka iz prošlosti, naročito u aktuarstvu i donošenju poslovnih odluka. Pametni uređaji generišu ogromnu količinu podataka, koji se ne mogu obrađivati na tradicionalni način, što predstavlja poseban izazov za osiguravače koji nisu uspevali da obrade ni postojeće podatke na odgovarajući način.

## **3. Vlasništvo nad podacima**

Otvoreno pitanje, kome pripadaju podaci o osiguranicima ili njihovoj imovini koje prikupljaju IoT uređaji koje su osiguravači dali klijentima i koje osiguravači obrađuju, u zavisnosti od stava koji zauzmu regulatori, može dovesti do određenih problema u budućnosti.

## **4. Bezbednost podataka**

Internet inteligentnih uređaja je po svojoj prirodi interesantan i dostupan hakerima. Pored relativno velike ranjivosti uređaja kojima se prikupljaju podaci (kamere, senzori, itd.), transport velike količine podataka kroz Internet pruža dodatnu priliku hakerima da presretnu, iskoriste ili izmene podatke koje IoT uređaji šalju osiguravačima.

## **5. IoT tehnologija može postati konkurencija osiguranju**

Pojedini eksperti prognoziraju da će dalji razvoj primene IoT tehnologije u osiguranju ugroziti opstanak delatnosti osiguranja. Ako je npr. kuća stalno nadgledana raznim senzorima i video nadzorom, mogućnost da dođe do štete usled požara, izliva vode, provalne krađe i slično, svodi se na minimum, zbog čega će potencijalni osiguranici u velikoj meri izgubiti motivaciju da plaćaju premiju osiguranja.



## Primeri implementacije postojećih IoT uređaja u osiguranje

Često se informacije od postojećih senzora IoT uređaja, koji nisu namenjeni osiguranju, mogu iskoristiti tako da osiguranicima smanje izloženost rizicima, a osiguravačima da izbegnu štete, što će biti objašnjeno u nekoliko primera<sup>27</sup>.

Ugrađeni senzori u komercijalnu infrastrukturu mogu poslužiti za detekciju pojave dima, vode ili zagađenog vazduha, čime se smanjuje rizik od realizacije potencijalnih osiguranih opasnosti.

Senzori koji se nose u odeći ili obući da nadgledaju zdravstvene parametre, mogu da posluže i za upozorenje osiguraniku da se kreće u opasnoj zoni, kao i da daju informacije osiguravajućoj kompaniji koje onemogućavaju prevare u osiguranju.

Senzori u domaćinstvu ili poslovnom prostoru mogu da detektuju pojavu vlage u zidu, koja prethodi pucanju vodovodne cevi, i na vreme upozore osiguranika da popravi cev i spreči događanje velike štete usled izliva vode iz instalacije.

Čarape za dijabetičare sa senzorima koji upozoravaju na lošu cirkulaciju krvi u stopalima, visok pritisak i sl. mogu biti iskorišćene preventivno i za ostale osiguranike za upozorenje na eventualne predstojeće kardio-vaskularne probleme, što omogućava izbegavanje većih troškova zdravstvenog osiguranja.

## Primeri implementacije IoT u osiguranju

Određena IoT rešenja su već implementirana u praksi i koriste ih osiguravači širom sveta, a postoji i jedan primer na tržištu osiguranja u Srbiji. U daljem tekstu biće više reči o nekoliko konkretnih primera primene ove tehnologije u delatnosti osiguranja.

### *Telematika u osiguranju vozila*

Jedna od prvih primena IoT u osiguranju je telematika. Pre više od deset godina, počelo je korišćenje senzora u vozilima, koji su osiguravačima slali podatke o stilu vožnje osiguranika s ciljem određivanja pojedinačnog profila rizika. Na početku su senzore osiguravači instalirali u vozila, dok u današnje vreme, senzore ugrađuju proizvođači vozila, a vozači i osiguravajuće kompanije koriste njihove podatke preko mobilnih aplikacija. U određivanju rizičnosti stila vožnje pojedinačnog vozača telematski IoT uređaji prikupljaju sledeće podatke<sup>28</sup>: pređena kilometraža, frekvencija vožnje, trajanje vožnje, doba dana vožnje (u špicu, noću, i sl.) učestalost naglog kočenja, brzina, način ubrzavanja, korišćenje uređaja u vožnji (radio, telefon, itd.), podaci o korišćenim putevima

27 Cannan, M., Lucker, J. & Spector, B. (2016). *Opting in: Using IoT connectivity to drive differentiation – the Internet of things in Insurance*. Westlake: Deloitte University Press.

28 Cannan, M., Lucker, J. & Spector, B. (2016). *Opting in: Using IoT connectivity to drive differentiation – the Internet of things in Insurance*. Westlake: Deloitte University Press.

(auto-put, seoski put, i sl.), ponašanje vozača u opasnim zonama i raspoloženja vozača tokom vožnje (bes, smirenost, itd.)

Skup parametara na osnovu kojih je ranije određivana cena polise (tip vozila, snaga motora vozila, starost i pol vozača, prethodne štete, i sl.), sada je proširen velikim brojem nabrojanih podataka. Osiguravači analiziraju korelacije prikupljenih podatke sa štetama i koriste ih da stimulišu poboljšanje stila vožnje osiguranika nižom cenom polise.

Mnoge svetske osiguravajuće kompanije su implementirale telematiku, dok je u Srbiji Triglav osiguranje prvo počelo da daje popuste na kasko osiguranje osiguranicima koji pristanu da koriste aplikaciju na mobilnom telefonu za praćenje stila vožnje, Drajev.

### ***IoT platforma za preventivno delovanje***

Danska osiguravajuća kompanija Topdanmark, razvila je IoT platformu za obradu podataka koji dolaze sa senzora koji su instalirani kod osiguranika. Na osnovu obrađenih podataka, platforma generiše izveštaje i upozorenja i tako preventivno deluje u sprečavanju nastanka osiguranih slučajeva. Robusna IoT platforma je zaštićena od cyber napada i ispunjava zahteve koje je nametnuo GDPR. Bazira se na tehnologijama edge computing, Amazon Kinesis analitika i Amazon S3 za računarstvo u oblaku, koje su razvijene u okviru Amazon Web Services. Integriše različite senzore, koji mogu da mere temperature, vlažnost i slično. IoT platforma je razvijena u programskim jezicima Java i Python.

Platformu za sada koriste u nekoliko slučajeva imovinskih osiguranja. Nadgleda se da li hladnjače osiguranika imaju optimalnu temperaturu u cilju sprečavanja nastanka štete na zalihama i ako temperatura poraste preko kritične vrednosti, šalje se SMS poruka osiguraniku da preduzme mere. Kod osiguranja imovine kuća i stanova izvršena je integracija sa LeakBot uređajima, u cilju detekcije izliva vode u domaćinstvima. Takođe, zahvaljujući integraciji sa landmark.dk portalom za merenje nivoa đubriva u cisternama sa đubrivom na farmama, osigurani farmeri se mogu preventivno upozoriti na eventualne anomalije.

### ***Digitalno zvono na ulaznim vratima***

Osiguravajuća kompanija iz SAD, American Family Insurance, zajedno sa partnerskom kompanijom za video nadzor Ring, ponudila je svojim osiguranicima popust 5% na premiju osiguranja kuća i stanova ako postave digitalno zvono na ulaznim vratima kompanije Ring. Kompanija Ring, takođe daje popust od 15% na svoj sistem video nadzora pod imenom Ring Video Doorbell. Ukoliko digitalno zvono detektuje pokrete u zoni koju pokriva, kao i u slučaju da posetilac pozvoni, pomoću povezanog video sistema iz zvona na Internet, prikazuje posetioca vlasniku domaćinstva kroz aplikaciju na mobilnom telefonu i omogućava komunikaciju vlasnika i posetioca. Noćni kvalitet snimka je isti kao i dnevni.

### **Google Nest vatrogasac u pametnim kućama**

Treća američka osiguravajuća kompanija po premiji, Liberty Mutual, u saradnji sa Googlovim sistemom za povezivanje uređaja u pametnim kućama, Nest, implementirala je požarni alarm u domaćinstvima svojih osiguranika. Liberty Mutual poklanja osiguranicima osiguranja imovine od požara Googleov IoT uređaj Nest, koji inače košta 99 USD, i daje im popust od 5% na premiju. U slučaju pojave dima ili ugljen monoksida, Nestov senzor ga detektuje i alarmira vlasnika putem mobilnog telefona.

### **Nosivi IoT uređaj u životnom osiguranju**

Američka kompanija za životno osiguranje, John Hancock, uključio je pametni sat u proizvod osiguranja života, Vitality. Proizvod je kreiran tako da nagrađuje osiguranike koji imaju zdrav život, što se utvrđuje na osnovu podataka iz pametnog sata. Posle testiranja proizvoda, zaključili su<sup>29</sup> da osiguranici koji kupe Vitality imaju 30% manje bolničke troškove od opšte populacije, hodaju skoro duplo više od prosečnog Amerikanca i imaju znatno više fizičkih aktivnosti kao što su plivanje i vožnja bicikla, žive duže i u proseku pristupaju aplikaciji 576 puta godišnje, odnosno imaju interakciju sa osiguravajućom kompanijom skoro 2 puta dnevno, za razliku od prosečnog osiguranika koji komunicira sa osiguravačem do 2 puta godišnje.

### **Pametna četkica za zube**

Kompanija Beam Digital iz američke države Teksas, proizvodi pametnu četkicu za zube, koja osim korišćenja za nadgledanje zdravlja zuba, ima ulogu i u smanjenju premije zdravstvenog osiguranja. Beam Digital zajedno sa osiguravajućim kompanijama National Guardian Life Insurance Company i Nationwide Life Insurance Company nudi proizvod zdravstvenog osiguranja zuba. Zahvaljujući povezanosti pametnih četkica za zube preko Interneta sa serverom koji se nalazi u kompaniji Beam Digital, kompanija je u mogućnosti da analizira oralnu higijenu i način i frekvenciju održavanja zuba svakog pojedinačnog osiguranika, kao i da mu pošalje preporuke za poboljšavanje održavanja zuba. U slučaju prihvatanja preporuka i promena navika u održavanju zuba, što dovodi do smanjenja kvarenja zuba, odnosno manjih šteta za osiguravača, premija zdravstvenog osiguranja se smanjuje.

### **Bodovanje ponašanja osiguranika**

Velika švajcarska IT kompanija sa godišnjim prihodom većim od 100 miliona evra, koja ima filijalu i u Srbiji, MSG Global Solution, razvila je softversko rešenje za analizu ponašanja osiguranika msg.IoTA od engl. Internet of Things Analyzer. Ranije su se modelirali rizici na osnovu istorijskih podataka, dok ovaj

29 Octo Group S.p.A. (2019). *The Power of Insurance IoT for Risk Management*. <http://www.octotelematics.com>

softverski alat, zahvaljujući obradi velike količine podataka dobijenih od raznih senzora, omogućava analiziranje rizika u realnom vremenu. Softver msg.IoTA omogućava osiguravajućim kompanijama da implementiraju sopstveni model bodovanja ponašanja osiguranika i bolje upoznaju osiguranikov način života. Tako su osiguravači u prilici da boje razumeju osiguranikove potrebe i ponude mu odgovarajući proizvod.

Švajcarsko osiguranje Die Mobiliar je prvo primenilo softversko rešenje msg.IoTA 2018. godine.

### ***Korišćenje dronova u proceni šteta***

Osiguravajuća kompanija Erie Insurance iz istoimenog grada američke države Pensilvanija, koja pripada grupi najvećih američkih kompanija sa liste U.S. Fortune 500, prva je osiguravajuća kompanija koja je počela da koristi dronove za procenu imovinskih šteta. Kamera sa drona je povezana na kompjutersku mrežu i direktno emituje sve što snimi na kompjuter procenitelja šteta. Korist od ovakvog načina procene je višestruka, izviđaj se obavlja brže, procenitelji se ne dovode u opasnost zbog pristupa oštećenim zgradama, snimanje sa visine, kombinovano sa zumiranjem detalja daje potpunu sliku oštećenja i otežava prevare u osiguranju.

### ***Osiguranje IoT investicija***

Na kraju, biće pomenut i jedan primer suprotne veze<sup>30</sup> Interneta inteligentnih uređaja i osiguranja. Osiguravajuća kompanija Hartford Steam Boiler (HSB), deo jedne od najvećih svetskih reosiguravajućih kompanija, Munich Re, zajedno sa američkom kompanijom specijalizovanom za IoT rešenja, Relayr, među prvima na svetu, 2016. godine, ponudila je mogućnost da tehnološke kompanije osiguraju svoje investicije u IoT.

## **Zaključak**

Delatnost osiguranja se zasniva na statistici, a bez podataka nema statistike. S druge strane IoT uređaji obezbeđuju ogromne količine podataka, tako da je njihova upotreba u osiguranju prirodna i neizbežna.

Analizom podataka dobijenih od IoT uređaja, osiguravači mogu mnogo bolje da upoznaju osiguranike, što im omogućava precizniju procenu rizika, poboljšanje kontrole rešavanja šteta, smanjenje troškova poslovanja, adekvatnije određivanje cene polise, unapređenje pojedinih aspekata poslovanja osiguravajuće kompanije, što sve na kraju vodi do ubrzanog rasta i sticanja

30 Bond, J. (2016). *IoT Infrastructure Investments to be Covered by First-of-a-Kind Industrial Insurance*. <http://www.munichre.com>

prednosti u odnosu na konkurenciju koja nastavlja da radi na tradicionalni način.

Uvođenje IoT tehnologije u osiguranje je dobro i za osiguranike, jer im osiguravajuća kompanija koja koristi Internet inteligentnih uređaja obezbeđuje ponudu skrojenu po ličnim potrebama, popuste na premiju, jednostavniji postupak zaključenja ugovora, bolje upravljanje rizikom tokom trajanja ugovora, određeni nivo sprečavanja nastanka pojedinih vrsta šteta, itd.

Ovaj rad je sistematično pokazao da je uvođenje Internet inteligentnih uređaja u osiguranje dobitna kombinacija za sve učesnike u procesu osiguranja. U svetu se već uveliko koristi, kao što je ovde opisano kroz primere. S obzirom da se sreću prve primene IoT tehnologije u oblasti osiguranja i u regionu, može se zaključiti da će u budućnosti Internet inteligentnih uređaja dobijati sve više na značaju na regionalnim tržištima osiguranja.

## Literatura

1. Antić, D. (2019). Šta je Internet of Things (Internet inteligentnih uređaja)? <http://samoobrazovanje.rs>
2. Baran, N. (1995). Whatever Happened To... Microsoft At Work? *Byte Magazine Vol 20 (7)* p. 30.
3. Big Data Task Force. (2018). *Big Data and the Role of Actuary*. American Academy of Actuaries.
4. Black, N. (preuzeto 2020.) *5 Challenges for IoT in the insurance industry*. [www.sas.com](http://www.sas.com)
5. Bujanja, B. (2019). *Sve o 5G tehnologiji: U petoj brzini!* Beograd: PC Press 267.
6. Cannan, M., Lucker, J. & Spector, B. (2016). *Opting in: Using IoT connectivity to drive differentiation – the Internet of things in Insurance*. Westlake: Deloitte University Press.
7. Eshton, K. (2009). *That 'Internet of Things' Thing*. <http://www.rfidjournal.com>
8. Fleisch, E., Weinberger, M. & Wortmann, F. (2014). *Business Models and the Internet of Things*. Bosch IoT Lab White Paper.
9. Global Standards Initiative on Internet of Things (2012). *Recommendation ITU-T Y.2060*.
10. Iorga, M., Feldman, L. et al. (2018). *Fog Computing Conceptual Model*. National Institute of Standards and Technology Special Publication 500-325
11. Kovanović, M. (2017). *Posle oblaka dolazi magla*. Beograd: PC Press 241.
12. Mango, D. (2015). The Internet-of-Things and Actuarial Engineering. *Actuarial Review Vol. 42(6)*.
13. Matejić, T., Marković, N. i dr. (2017). Monitoring dobara materijalne kulturne baštine primenom interneta inteligentnih uređaja. *Časopis Info M 64*, str. 11-17.
14. Maynard, T. (2019). 50 billion pairs of eyes. *The Actuary*, magazine of the Institute & Faculty of Actuaries. <http://www.theactuary.com>

15. Mladenović, S., Uzelac, A. i dr. IoT u železničkom saobraćaju – realnost i izazovi. In: Zbornik radova sa XXXIV Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju, PosTel 2016.
16. Octo Group S.p.A. (2019). *The Power of Insurance IoT for Risk Management*. <http://www.octotelematics.com>
17. OECD (2015). *OECD Digital Economy Outlook 2015*. OECD Publishing.
18. OECD (2018). IoT Measurement and Application. *OECD Digital Economy Papers No. 271*. OECD Publishing.
19. Pavlović B. (2019). *Robot Usage in Insurance*. XVII međunarodni simpozijum „Osiguranje na pragu IV industrijske revolucije“, Zlatibor.
20. Petrović, L., Jezdović, I. i dr. (2017). *Razvoj edukativne igre zasnovane na Internetu inteligentnih uređaja*. Infoteh Jahorina Vol. 16, str. 506-509.
21. Rabah, K. (2018). Convergence of AI, IoT, Big Data and Blockchain: A Review. *The Lake Institute Journal* Vol. 1 (1), p. 1.18.
22. Radenković, B., Despotović-Zrakić, M. i dr. (2017). *Internet inteligentnih uređaja*. Fakultet organizacionih nauka, Beograd.
23. Raji, R. (1994). Smart Networks for Control. *IEEE Spectrum* 31 (6), p. 49-55.
24. Rodić Trmčić, B., Labus, A. & Bodanović Z. (2016). Model mobilnog zdravstva zasnovan na tehnologijama wearable computinga. *Časopis Info M* 57, str. 48-54.
25. Salamone, S. (1995). Novell Builds a NEST. *Byte Magazine* Vol 20 (8) p. 151-152.
26. Simić, K., Despotović-Zrakić, M. i dr. (2015). *Model infrastrukture obrazovne institucije zasnovan na Internetu inteligentnih uređaja*. Infoteh Jahorina Vol 14. str. 681-685.
27. Suresh, P., Vijau, D. et. al. (2014). A state of the art review on the Internet of Things (IoT) - History, Technology and fields of deployment. In: *International Conference on Science, Engineering and Management Research (ICSEMR 2014)*. Chennai: Institute of Electrical and Electronics Engineers (IEEE).
28. Tomanović, I. (2017). Primena internet inteligentnih uređaja u unapređenju maloprodaje. *Časopis Info M* 64, str. 18-25.
29. Vega, M. (2019). *Connect All the Things – Internet of Things Statistics 2020*. <http://review42.com>
30. Weiser, M. (1991). The Computer for the 21<sup>st</sup> Century. *Scientific American* 265 (3), p. 94-104.