UDC: 621.313:004.056 Info M str. 20-27

IDENTIFIKACIJA PROBLEMSKIH PITANJA IOT SISTEMA NA OSNOVU ISO/IEC REFERENTNE ARHITEKTURE
IDENTIFICATION OF IOT SYSTEM ISSUES BASED ON ISO / IEC REFERENCE ARCHITECTURE

Vanja Mišković, Željko Gavrić

REZIME: IoT je revolucionarna promjena u području interneta i informacionih tehnologija uopšte. Mnogobrojne su primjene IoT platformi i doprinos koji one imaju na život, rad i okruženje svakog čovjeka. U okviru visoko heterogenih IoT tehnologija standardizacija predstavlja osnovu za dalji razvoj. U ovom radu opisana je ISO/IEC referentna arhitektura i najznačajnije karakteristike IoT sistema. U zaključku rada identifikovani su i pojašnjeni problemi kao polazne tačke za nove istraživačke radove.

KLJUČNE REČI: IoT sistemi, ISO/IEC referentna arhitektura, IoT karakteristike i nedostaci.

ABSTRACT: IoT is a revolutionary change in the field of the Internet and information technology in general. There are numerous applications of IoT platforms and the contribution they make to each person's life, work and environment. Due highly heterogeneous IoT technologies, standardization is the basis for further development. This paper describes the ISO/IEC reference architecture and the most important features of an IoT system. In conclusion, problems were identified and clarified as the starting points for new research papers.

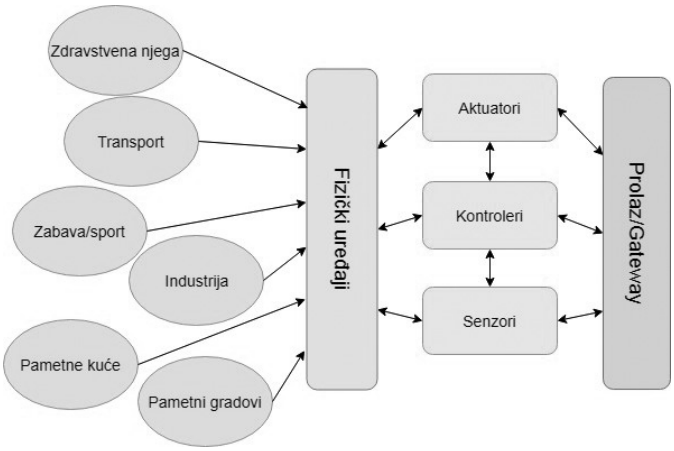
KEY WORDS: IoT systems, ISO/IEC reference architecture, IoT features and drawbacks.

1. UVOD

Mark Weiser je još davne 1988. kreirao kovanicu eng. *ubiquitous computing*, skraćeno *Ubicomp*, i objasnio je "*kao budućnost u kojoj će računari, ili periferni uređaji, biti ugrađeni u objekte koje svakodnevno koristimo tako da niko neće primjećivati njihovo prisustvo. Računari će biti fiksni, ali i prenosivi, povezani ožičenim ili bežičnim vezama. Omogućiće korisnicima da nesmetano razmjenjuju svoje podatke i programe, i biće ih koji su jako mali veličine bedža. Nove mreže će morati da podrže mnogo više ovakvih uređaja jer je ubiquitous era u kojoj svaki* čovjek *ima više računara*" [1,2]. Upravo smo na dobrom putu da ostvarimo Weiser-ovu viziju, ili smo ipak u fazi "prožimanja" (eng. *pervasive*) [3,4] našeg života sa različitim računarskim sklopovima, a u sljedećim generacijama će postati dio svakodnevnice i sveprisutni (eng. *Ubiquitous*). Internet inteligentnih uređaja (eng. Internet *of Things - IoT*) je realizacija sveprisutnog računarstva i nakon *www* usluge i *mobilnog* interneta, *IoT* je revolucionarna promjena u području interneta i informacionih tehnologija uopšte.

Jednu od aktuelnih definicija za IoT dao je ISO/IEC JTC 1 tehnički odbor za Informacione tehnologije: "*IoT je infrastruktura koja se sastoji od međusobno povezanih objekata, ljudi, sistema i izvora informacija i omogućuje im inteligentne usluge za procesiranje informacija iz fizičkog i virtuelnog svijeta i adekvatno reagovanje na osnovu dobijenih rezultata*" [5]. IoT omogućuje ne samo bilo kome već i bilo čemu da se poveže u internet prostor. Odnosi se na svijet u kom su fizički objekti i ljudska bića, kao i virtuelni podaci i sajber okruženje, u interakciji jedni sa drugima u isto vrijeme i u zajedničkom IoT prostoru [7].

Iako postoji više šablona/paterna IoT platformi koji su već u zreloj fazi, svima su zajedničke sljedeće komponente: koncept fizičkog **objekta** (eng. *thing*), **pristupna mreža** (eng. *edge*) i sama **platforma**. Fizički objekt može da ima različite procesorske/memorijske mogućnosti kao senzor, aktuator ili kontroler, te nije običan objekt već inteligentan objekt. Sa druge strane je povezan sa pristupnom mrežom, drugim objektom, **prolazom** ka jednom ili više IoT sistema [8], a što je prikazano na Slici 1.



Slika 1 – *IoT oblasti primjene*

Pristupna mreža (eng. *edge*) predstavlja operativni domen IoT sistema. Može biti tako mala da predstavlja jedan uređaj povezan direktno sa IoT platformom, ili velika kao proizvodni pogon. Pristupna mreža može sadržati u sebi i izvjestan nivo pretprocesiranja prikupljenih senzorskih podataka. Pretprocesiranjem se želi povećati pouzdanost, tačnost podataka i rasteretiti serverske komponente od nekorektnih podataka. U okviru pretprocesiranja obično se podaci procesiraju kroz nekoliko ili svih pet navedenih faza [9]: *validacija* (identifikacija izvora), *transformacija* (isti format zapisa za sve prikupljene podatke), *pročišćavanje* (eliminacija nemogućih stanja), *redukcija* (aregacija podataka prije skladištenja ukoliko se obradom ne dobija relevantna informacija) i *unakrsna provjera* (jednostavni algoritmi zaključivanja i upoređivanja senzorskih podataka). Mrežna topologija pristupne mreže može da bude „ad-hoc" mreža (najprostije rješenje) ili mreža povezana pre-

ko jednog ili više protokola (kompleksnija izvedba) sa nula ili više rutera koji je povezuju sa većom mrežom ili na oblak tehnologiji baziranoj IoT platformi.

ISO/IEC je u standardu 30141:2016 definisao referentnu arhitekturu IoT sistema. IoT referentna arhitektura (IoT RA) opisana u ovom dokumentu [6] daje konceptualni model-KM (eng. *conceptual model - CM*), referentni model (eng. *Reference Model - RM*) i referentnu arhitekturu (eng. *Reference Architectures - RA*) koja se sastoji iz različitih arhitektonskih pogleda. IoT RA ne samo da opisuje „šta je sve potrebno" za izgradnju IoT sistema, već takođe ukazuje i „kako" će domeni i entiteti IoT sistema komunicirati u IoT integralnom sistemu. Opisane su: karakteristike IoT sistema; domeni IoT sistema; KM i RM, te pogledi RA; i interoperabilnost IoT entiteta [6]. IoT RA je takođe pogodna za identifikaciju značajnih problema razvoja i primjene IoT sistema.

U nastavku rada je pregledno analizirana priroda IoT platformi i dat je uvid u sve značajne karakteristike. Objašnjena je i jedna od najzačajnijih standardizovanih arhitektura IoT sistema prema standardu 30141:2016. Na osnovu prethodnih poglavlja identifikovani su nedostaci današnjih IoT platformi i dat zaključak rada.

2. KARAKTERISTIKE IOT SISTEMA

Značajne karakteristike IoT sistema se grupišu u: sistemske karakteristike, servisne karakteristike, karakteristike komponenti i dodatne opšte karakteristike [6].

2.1. *Sistemske karakteristike*

Auto-konfiguracija - Podrazumjeva samostalno umrežavanje uređaja, samostalno nuđenje/ odgovaranje na tražene usluge i uopšte rad uređaja po principu „plug & play". Ovdje je bitno napomenuti da ovakav način rada podrazumjeva implementaciju odgovarajućih sigurnosnih i mehanizama autentifikacije. Primjeri protokola koji su već implementiranti za potrebe autokonfiguracije su: DHCP (eng. *Dynamic Host Configuration Protocol* ili protokol za dinamičko konfigurisanje računara), Zero Configuration Networking (ZeroConf), Bonjour, UPnP.

Jasno razdvajanje funkcija uređaja i upravljanja istim - Obično su za neki uređaj funkcije njegovog rada i funkcije upravljanja njim na različitim pristupnim tačkama, tj. obrađuju se u različitim softverskim komponentama. Značaj ovakvog pristupa je u tome što administrator sistema može da pristupi uređaju i njegovim podacima, a privatni podaci krajnjeg korisnika ovog uređaja nisu mu dostupni.

Veoma distribuiran sistem - IoT podrazumjeva sistem čije su komponente rasprostranjene širom zgrade, grada, ili šire države, svijeta. Podaci su takođe distribuirani, a različiti entiteti IoT sistema procesiraju podatke.

Mrežna komunikacija - IoT sistem podrazumjeva najrazličitije tipove mreža. Često su mreže ograničenog dometa i male snage (*eng. proximity networks*) mreže koje formiraju lokalne veze za IoT uređaje. Širokopojasne mreže koje povezuju lokalne mreže sa internetom, i koje mogu biti žičane i bežične, posebno namjenjene IoT sistemu ili zajedničke mreže opšte namjene. Lokalne mreže koriste obično specifične protokole koji odgovaraju posebnoj namjeni te mreže. Širokopojasne mreže koriste obično IP protokol, odnosno HTTP protokol ili neki drugi protokol za prosljeđivanje poruka na višem nivou protokol steka. Neke mreže imaju takvu prirodu slanja podataka da im nije potrebna stalna veza, već se u određenim vremenskim intervalima vrši slanje podataka. Mrežna struktura mora biti dinamična i treba uzeti u obzir svojstva kao što su *QoS*, otpornost na greške, sigurnost i upravljačke mogućnosti. Primjeri korištenih protokola: lokalne IoT mreže koriste obično IEEE 802.15.4(ZigBee)/IEEE 802.15.1(Bluetooth) i IEEE 802.11(WiFi) komunikacione protokole na fizičkom i sloju veze podataka. Podaci mogu biti preneseni pomoću *6LowPAN* protokola koji je zamjena za IoT IP / UDP protokol.

Upravljanje radom mreže - IoT sistemi zahtijevaju da mreže budu upravljive, a na koji način zavisi od tipa mreže. Sistemi upravljanja su neophodni pri početnom umrežavanju i uključuju identifikovanje i adresiranje uređaja, uloge uređaja u mreži i mogućnost dinamične promjene stanja mreže. Dodavanjem / uklanjanjem postojećih uređaja u toku rada mreže mijenja se njena opšta topologija.

Rad u *realnom vremenu* - U vrijeme dok se neki spoljašnji proces odvija sistem na osnovu njegovih prikupljenih podataka daje rezultat obrade i omogućuje različite vrste odgovora, informacija i aktivnosti baziranih na dobijenim rezultatima obrade. Pri čemu je bitno da se rezultati dobiju sa postavljenom učestalošću i nekada su to čak mili sekunde.

*Sposobnost predstavljanja sistemu (*eng. *Self-description*) - Ova karakteristika podrazumijeva da sve komponente IoT sistema mogu da pošalju informacije o svojoj ulozi u sistemu, svojim mogućnostima, uslugama koje nude na određenim interfejsima i stanju u kom se trenutno nalaze. Ova osobina je od značaja za IoT sistem kada se više IoT sistema treba udružiti, ili jedan IoT sistem treba proširiti sa novim uređajima. Primjer samostalnog predstavljanja uređaja: Bluetooth uređaji svoje ime i listu usluga prosljeđuju jedni drugima kada se povezuju.

Prijavljivanje na IoT uslugu - IoT sistem može da funkcioniše na bazi plaćanja njegovih usluga od strane krajnjih korisnika. U tom slučaju moraju postojati mehanizmi kojim se korisnici prijavljuju za korištenje usluge, sistem koji upravlja prijavama i naplatom usluge.

2.2. *Servisne karakteristike*

Svjesnost sadržaja (eng. Content-Awareness) - Uređaji i servisi svjesni sadržaja podataka koje prenose ili obrađuju mogu da adaptiraju svoje interfejse prema njima, apstrahuju aplikacione podatke, povećaju preciznost prosljeđivanja podataka, otkriju određene usluge i omoguće korisniku prigodnu interakciju. Svjesnost sadržaja može da se koristi za podešavanje rutiranja, brzine isporuke, kao i sigurnosnih mehanizama u skladu sa lokacijom, kvalitetom usluge i osjetljivošću podataka.

Svjesnost konteksta (eng. Context-Awareness) - Svjesnost konteksta je osobina IoT uređaja, servisa ili sistema koji može da nadgleda svoje operativno okruženje i događaje u okviru tog okruženja radi određivanja informacija kao što je *Kada?*, *Gdje?*, ili u *Kom redoslijedu?* se jedan ili više značajnih događaja dogodio u fizičkom svijetu [6]. Anind Dey definiše aplikaciju svjesnu konteksta na sljedeći način [10]: "Kontekst je svaka informacija koja može da se koristi za karakterizaciju situacije entiteta. Entitet je osoba, mjesto ili objekat koji se smatra relevantnim za interakciju između korisnika i aplikacije, uključujući korisnika i samu aplikaciju." Kada je u pitanju kontekst korisnika Abowd i Mynatt [11] su identifikovali 5W (Who, What, Where, When, Why) kao minimum informacija koje treba prikupiti da bi se razumio kontekst korisnika. Prije IoT ere sistemi svjesni konteksta prikupljali su podatke iz ograničenog broja hardverskih i softverskih senzora. U ovim situacijama, prikupljanje i analiza podataka senzora je lako izvodljiva zbog ograničenog broja izvora. IoT predviđa eru u kojoj su milijarde senzora povezane sa internetom, što znači da nije izvodljivo obraditi sve podatke prikupljene od tih senzora. Stoga će svjesnost konteksta odigrati ključnu ulogu u odlučivanju koje od podataka treba obraditi [12].

Pravovremenost (*eng. Timeliness*) - IoT sistem mora u tačno određenim vremenskim trenucima ili periodičnim intervalima da izvrši određene aktivnosti, funkcije ili servise. U ovom smislu, bitni su podaci kao što je latencija, frekvencija uzorkovanja, džiter sistema, fazni šum signala itd. Navedene karakteristike se kontrolišu da bi se garantovala potrebna preciznost rada sistema. Primjer kontrolnih petlji u industriji na proizvodnim linijama je najbolji primjer da bi se izrazila kritičnost pravovremenosti sistema.

2.3. *Karakteristike komponenti*

Kombinovanje/prekombinovanje IoT komponenti (eng. Composability) - Mogućnost diskretnih entiteta IoT sistema da se povezuju u integralni IoT sistem radi postizanja zajedničkih ciljeva i radnih zadataka. Pri zamjeni komponente drugom sistemske funkcije treba da ostanu nepromijenjene. Primjer bi mogao biti u senzorskoj opremi jednog proizvođača koja je u potpunosti zamjenjiva sa senzorima drugog proizvođača.

Vidljivost/otkrivanje (eng. Discoverability) – Osobina vidljivosti omogućava korisnicima, uslugama i uređajima da pronađu ne samo uređaje na mreži već i usluge koje ti uređaji nude. Ova usluga je jako bitna kada je potrebno dodati nove uređaje u sistem, a koji treba da zadovolje kriterijume kao što je određena geografska lokacija, određeni sigurnosni mehanizmi i sama konfiguracija uređaja.

Modularnost je osobina komponenti da se mogu kobinovati u različite konfiguracije prema potrebama IoT sistema. Dok god se na osnovu interfejsa i istih upita dobijaju isti standardizovani rezultati sama interna realizacija nekog uređaja nije važna za IoT sistem i taj uređaj se smatra modularnim.

Umreženost - Dva uređaja u IoT sistemu preko odgovarajuće mrežne tehnologije moraju moći izvršiti potrebnu razmjenu informacija, a za potrebe funkcionisanja sistema.

Djeljivost resursa - Određene komponente bi se mnogo racionalnije koristile ukoliko bi njihove mogućnosti moglo da koristi više IoT aplikacija.

Jedinstveno identifikovanje - Svi entiteti IoT sistema trebaju biti jedinstveno identifikovani i na osnovu identifikacije sledljivi. IPv4, IPv6, URI, i Fully Qualified Domain Names (FQDNs) se koriste za jedinstveno i nedvosmisleno identifikovanje mrežnih krajnjih tačaka u internet aplikacijama. Hardverski uređaji pa i softver može da ima jedinstven identifikator proizvođača, na primjer: UUID (*eng. Universal Unique Identifier*), OID (*eng. Object IDentifier*). Za fizičke uređaje se koriste RFID tagovi, barkodovi. Za ljude se mogu koristiti biometrijske tehnike.

2.4. *Druge značajne karakteristike*

Kompatibilnost – IoT sistem mora da nudi podršku zastarjeloj tehnologiji i plan prelaska na nove tehnologije radi finansijske isplativosti novih ulaganja u sistem sa jedne strane, a sa druge strane treba voditi računa da starija oprema ne učini sistem „ranjivom" na napade ili otkaze pri radu. Komponente trebaju biti dobro definisane, a što podrazumjeva ne samo njihovu konfiguraciju, već i sigurnost, pouzdanost, komunikativnost itd. Bez ovako definisanih komponenti ne bi bilo moguće procijeniti da li čitav IoT sistem zadovoljava ciljeve za koje je projektovan.

Iskorišćenost resursa (eng. Usability) - Fleksibilnost uređaja se u realnosti usklađuje sa ekonomičnošću istog i obično je to zlatna sredina između uređaja posvećenih samo jednoj namjeni i bez mogućnosti drugačije hardverske konfiguracije ili programskog podešavanja i sa druge strane uređaja „opšte namjene" sa mogućnošću različitih hardverskih konfiguracija i visokim stepenom programibilnosti [6].

Robusnost sistema – Pouzdanost rada sistema je jako bitna, pogotovo pouzdanost podataka koji se u svim IoT sistemima koriste za donošenje odluka. Ukoliko su podaci korumpirani ili ih nema ovakve odluke će izostati. Potrebna je takođe i pouzdanost mrežne konekcije za prenos podataka i komandi, kao i bilo kog drugog IoT entiteta. Otpornost na greške IoT sistema se postiže tako što se greška u radu jednog uređaja ne smije širiti na cijeli sistem, već se na vrijeme detektuje i uređaj zamijeni rezervnim. Kada su u pitanju mreže koristi se tip isprepletene (eng. *mesh*) topologije.

Sigurnosni aspekti IoT sistema - *Dostupnost* je garancija svim ljudima korisnicima i servisima da će ukoliko su autorizovani moći da pristupe i koriste usluge IoT sistema. *Povjerljivost* podataka je garant IoT sistema da podaci korisnika neće biti otkriveni trećem licu. Mnoge podatke koji prolaze kroz IoT sistem treba tretirati kao povjerljive. Na primjer: IoT senzori za otkrivanje pokreta mogu otkriti da li je neko prisutan u prostorijama ili ne, a što bi lopovi mogli da iskoriste za ciljanje imanja. Slična zabrinutost odnosi se na pametna brojila - gdje čak i frekvencija poslatih poruka treba da ne zavisi od stope potrošnje električne energije [6]. *Integritet* podataka je značajan aspekt sigurnosti IoT sistema. Zaštita integriteta podataka znači zaštitu protiv promjene ili uništenja podataka. *Bezbjednost* (eng. Safety) po-

drazumjeva primjenu odgovarajućih sigurnosnih mehanizama da bi se zaštitili korisnici od povreda, gubitka imovine, spriječilo oštećivanje opreme, garantovala odgovornost.

Zaštita privatnosti (eng. Protection of personally identifiable information - PII) - Kada su u pitanju osnovna načela privatnosti, različita shvatanja postoje u različitim zemljama, ali sljedeća četiri načela se smatraju prihvaćenim širom svijeta [13]: *Načelo o postojanju privatnosti*: Nosilac podataka (osoba) ima identitet i ostale relevantne i promjennjive podatke za koje osoba smatra da pripadaju njegovom/njenom domenu privatnosti. *Načelo o uskraćivanju prava pristupa*: Nosilac podataka ima pravo i mora mu biti omogućeno da uskrati neke ili sve svoje lične podatke drugim osobama i organizacijama. *Načelo pouzdanog korišćenja*: Osoba ili organizacija koja prima lične podatke i pohranjuje ih, naziva se kontrolor ili kolekcionar. Ovaj kolekcionar informacija ima obavezu da kontroliše dijeljenje i obradu ličnih podataka prema navodima u zakonskoj deklaraciji o privatnosti elektronskih podataka. *Načelo o kontroli dijeljenja podataka*: Nosilac podataka ima pravo da ograniči mogućnost da kolekcionar dijeli podatke sa drugim organizacijama ili osobama radi daljeg procesiranja.

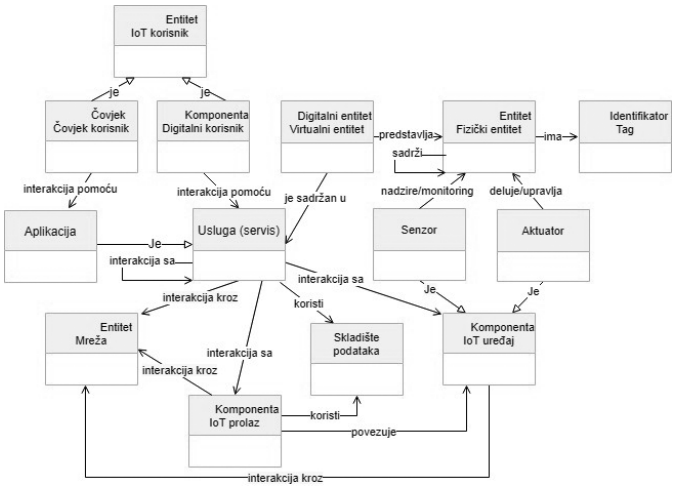
U okviru sveprisutnih sistema nameću se sljedeća načela sveprisutnog sistema svjesnog privatnosti svojih korisnika [14]: *Načelo otvorenosti i transparentnosti*: Ovo načelo podrazumijeva da se u samoj suštini sistema svjesnih konteksta podrazumijeva prikupljanje ličnih podataka. *Načelo o izboru i pristanku*: je već opisano načelo o kontroli dijeljenja podataka. *Načelo anonimnosti i pseudo – anonimnosti*: Ukoliko bi korisnik mogao ostati anoniman za sistem, većina korisnika bi dozvolila neograničeno prikupljanje i dijeljenje podataka. Takođe postoji mogućnost da se omogući korisniku pseudo – anonimnost. Ovo bi podrazumijevalo promjenu identifikatora korisnika za pristup sistemu za svaku sljedeću prijavu na sistem, ili za određeni period vremena. Upravo je slična ideja prihvaćena u Bluetooth standardu – uređaj je prije za identifikaciju koristio fizičku adresu, a sada standard propisuje mogućnost promjene adrese između glavne i prateće stanice za vrijeme uspostavljene sesije [15]. *Načelo blizine i lokacije* (*eng. proximity and locality*): Podaci bi se smjeli prikupljati samo u slučaju kada je korisnik u blizini senzorskog uređaja i kada pomoću definisane procedure za autentifikaciju odobri prikupljanje podataka. Novi standardi propisuju mogućnost korišćenja i mnogo boljih vidova sigurnosne zaštite od PIN koda, ali to zavisi od same implementacije senzorskog uređaja [16]. Načelo o lokaciji podrazumijeva da se podaci ne mogu dijeliti neograničeno, već da podrazumijevaju lokalni pristup na nivou jedne sobe, zgrade ili šireg prostora. *Načelo adekvatnih sigurnosnih mehanizama*: Svaka od komponenti IoT sistema ima svoje specifične sigurnosne mehanizme. *Načelo o pristupu i resursima*: Sistem mora imati mogućnost razlikovanja prihvatljivog u odnosu na neprihvatljivo ponašanje.

Karakteristike podataka – 5V (eng. Data– Volume, Velocity, Veracity, Variability and Variety) IoT sistema su: količina, brzina, istinitost, promjenljivost i raznolikost. *Heterogenost IoT sistema je uvijek prisutna* - od heterogenosti domena, sistema i proizvoda. Ovo je jedan od najvećih izazova IoT sistema, jer svi ti različiti dijelovi moraju biti interoperabilni. *Pravne regulative* koje se primjenjuju u okviru IoT sistema mogu biti podjeljene u sljedeće kategorije: bezbjednost, RF regulative, zaštita prava potrošača (krajnjih korisnika sistema).

Skalabilnost podrazumijeva da se sistem u različitim aspektima može jednostavno proširivati, jer radom će se povećavati broj korisnika, broj senzorskih uređaja, količina skladištenih podataka, itd. *Pouzdanost* je stepen do koga korisnik ili drugi zainteresovani učesnici imaju poverenja da će se proizvod ili čitav IoT sistem ponašati onako kako je predviđeno.

3. KONCEPTUALNI MODEL, REFERENTNI MODEL I ARHITEKTONSKI POGLEDI

Apstrakcijom i generalizacijom karakteristika IoT sistema definisan je **konceptualni model**. Konceptualni model daje strukturu i definiciju koncepâta, kao i veza između IoT entiteta.

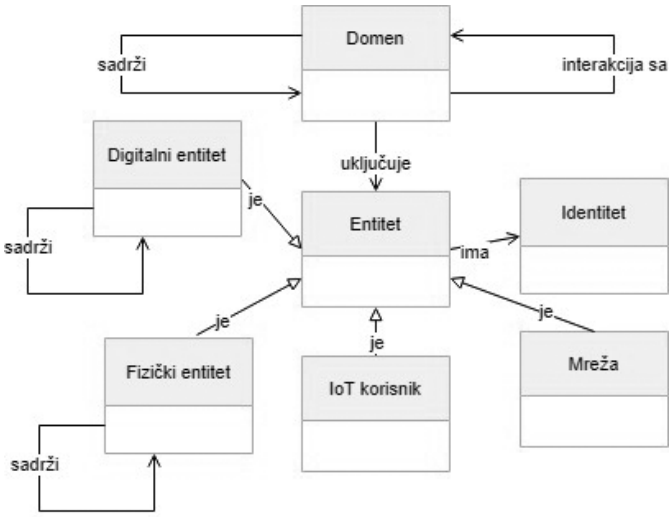


Slika 2 – *UML opšti model IoT koncepata*

Pomoću UML jezika je prikazan opšti model IoT koncepâta, a ilustrovan je na Slici 2. Korisnik IoT sistema može da bude čovjek ili digitalni korisnik, tj. automatizovana usluga. Čovjek ima interakciju sa sistemom pomoću aplikacije koja je specijalna vrsta usluge i pri tome naravno koristi mrežu. Digitalni korisnik ima interakciju sa sistemom preko usluge takođe kroz mrežnu infrastrukturu. Jedna usluga može da bude u interakciji sa drugim uslugama sistema. Fizički entitet je objekt iz realnog svijeta, a njim ili upravlja aktuator ili ga nadgleda senzor. Fizički entitet može da ima pridružen tag koji nagdleda senzor. Virtuelni entitet je reprezentacija fizičkog entiteta u IT svijetu. Senzori i aktuatori su vrste IoT uređaja. Mogu direktno preko mreže biti u interakciji sa sistemom ili preko prolaznih uređaja. Skladište podataka čuva podatke IoT uređaja i one koji su rezultat rada IoT usluga.

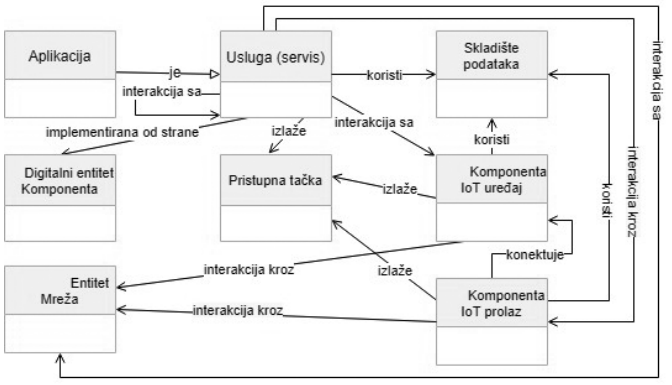
Pojednostavljen model IoT sistema sa 4 fundamentalna entiteta je definisan na Slici 3. Čine ga: objekt (Fizički entitet), Korisnik IoT-a, IT sistemi (Digitalni entitet) i komunikaciona mreža. Digitalni entitet može biti: aplikacija, usluga, virtuelni entitet, skladište podataka, IoT uređaji i IoT prolazi. Korisnik može biti čovjek ili neka usluga. Fizički entitet je objekt koji je

jedinstveno identifikovan, diskretan i može biti upravljan/posmatran. Svi entiteti imaju pridružene identifikatore koji mogu biti različiti u zavisnosti od vrste entiteta. Svi entiteti komuniciraju preko mreže. Kod nekih IoT sistema postoji potreba da se izvrši dekompozicija sistema u više domena – Domen.



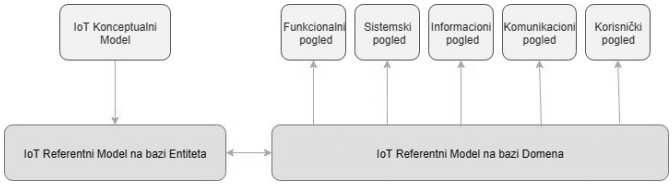
Slika 3 – *UML model 4 fundamentalna entiteta*

Servis/usluga je apstraktan koncept. Servis implementira jedna ili više komponenti. Takođe može biti i više alternativnih implementacija istog servisa. Entiteti koji komuniciraju preko mreže postavljaju svoje pristupne tačke dostupne na mreži. Podaci vezani za servise, IoT uređaje i IoT prolazne uređaje nalaze se u skladištu podataka. Servis nudi takođe pristupnu tačku na mreži.

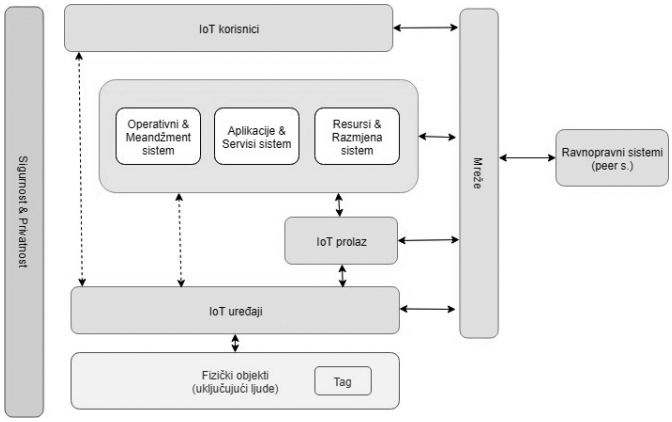


Slika 4 – *UML model IoT entiteti i koncept pristupne tačke*

RM – referentni model je apstraktno radno okruženje za razumjevanje značajnih veza između entiteta određenog okruženja i za razvoj konzistentnih standarda i specifikacija koje će podržati to okruženje [17]. RM nije vezan ni za jednu konkretnu tehnologiju ili standard. RM je definisan na osnovu OASIS SOA Reference Model (SOA-RM) TC [17]. RM služi za: kreiranje standarda za objekte u okviru modela i za njihove veze, edukaciju stejkholdera, poboljšanje komunikacije između ljudi; određivanje jasnih uloga i odgovornosti i dozvoljava komparaciju različitih entiteta. Iz KM-a se definiše IoT RM baziran na entitetima, zatim IoT RM baziran na domenu, a i iz njega pogledi: funkcionalni, sistemski, informacioni, komunikacioni i korisnički pogled kao što je prikazano na Slici 5.



Slika 5 – *Veza između KM, RM i referentne arhitekture zasnovane na pogledima*



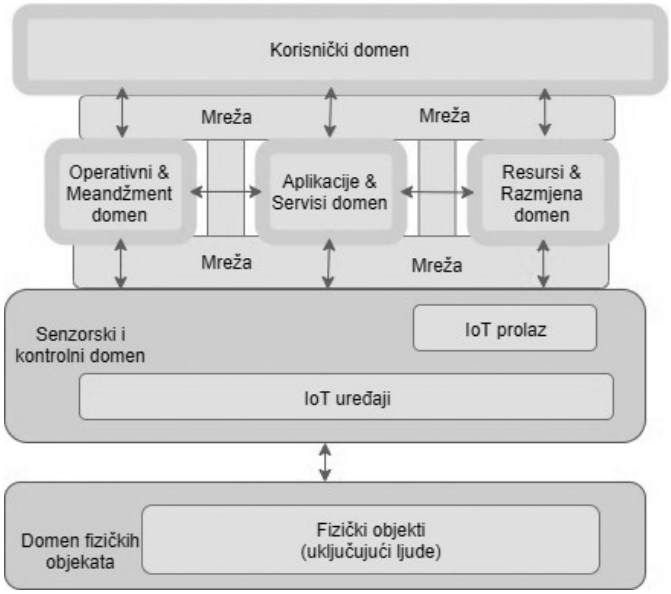
Slika 6 –*RM baziran na entitetima*

RM baziran na entitetima je ilustrovan na Slici 6. Na dnu sistema su fizički objekti iz realnog svijeta i mogu biti u pitanju i ljudi. Imaju tagove koji ih jedinstveno identifikuju. O načinu identifikacije je već prethodno pisano u ovom radu. IoT uređaji povezuju fizičke objekte u IoT platforme. IoT uređaji mogu biti senzori ili aktuatori. Preko mreže su povezani u sistem, a neki mogu imati mogućnost i diretnog povezivanja sa internetim. IoT prolazi su uređaji koji mogu imati mnoge funkcije, kao što je skladištenje podataka, analitika nad podacima IOT uređaja, oblici procesiranja podataka i sama aplikacija za potrebe korisnika. Na osnovu prikupljenih podataka iz IoT uređaja moguće je da se procesiranjem u realnom vremenu donese odluka o aktivnostima aktuatora. IoT prolazni uređaji su danas često mobilni uređaji [18]. Ovi uređaji mogu da implemetiraju i algoritme iz domena vještačke inteligencije za potrebe donošenja odluka [19].

Različite vrste aplikacija i/ili usluga postoje u okviru IoT sistema. Sve one imaju pridružena skladišta podataka. Analitika tj. analitičke usluge su prisutne u sistemu vezano za IoT uređaje ali i same komponente i rad sistema. Konačno tu su i poslovne aplikacije vezane za komercijalnu upotrebu sistema. Aplikacije i usluge komuniciraju sa IoT uređajima preko pristupne mreže dok međusobno koriste servisnu mrežu. Operativni i manadžment sistem omogućuje nadgledanje i kontrolu svih uređaja. Sistem za pristup resursima na osnovu autorizacije korisnika dozvoljava pristup samoj IoT usluzi, administraciji IoT sistema ili pristup na poslovnom nivou vezan za sisteme obračuna i naplate usluga. IoT korisnici ukoliko su ljudi koriste odgovarajući uređaj u vidu mobilnog uređaja, tableta ili

nekog posebnog uređaja za IoT platformu. Korisnički uređaj u nekim slučajevima je u direktnoj vezi sa IoT uređajima ili IoT prolazima. Primjer su pametni telefoni i prenosivi senzorski uređaji, gdje je mobilni uređaj ujedno i prolaz i direktno povezan sa senzorima na tijelu [18,19]. Peer –sistemi mogu biti drugi IoT sistemi ili druga vrsta sistema.

RM na bazi entiteta (Slika 6.) i **RM na bazi domena** (Slika 7.) su potpuno konzistentni što se može vidjeti i prema samim nazivima domena: Korisnički domen, Operativni i manadžment domen, Aplikacioni domen, Senzorski i kontrolni domen, Pristupni i domen razmjene resursa, te na dnu Domen fizičkih objekata.



Slika 7 *–RM baziran na domenima*

Iz domenskog RM-a proizlaze **pogledi IoT referentne arhitekture**: funkcionalni, sistemski, informacioni, komunikacioni i korisnički pogled.

Funkcionalni pogled razlikuje dvije vrste funkcija: u okviru domena i međudomenske funkcije. U okviru senzorskog/kontrolnog domena - SKD prisutne su funkcije: očitavanje podataka, slanje komadni aktuatorima, identifikacija, pristup mreži, izvršenje logike za određivanje stanja i ponašanja uređaja, interpretacija podataka dobijenih senzora a ponekad i korelacija. Upravljanje resursima je pod kontrolom viših funkcija operativnog i manadžment domena i omogućuje ažuriranje softvera, podešavanje konfiguracije. Kada su u pitanju izvori podataka bitno je naglasiti da pored fizičkih senzorskih uređaja izvori se mogu naći i u softverskom/virtuelnom okruženju. Pa se obično navodi sljedeća podjela senzora [20,21]: fizički, virtuelni i logički senzori. Fizički senzori podrazumjevaju hardversku multifunkcionalnu platformu. Virtuelni senzori predstavljaju softverske izvore podataka. Logički senzor predstavlja kombinaciju više fizičkih ili virtuelnih senzora.

Aplikaciono servisni domen (eng. *Application Service Domain*) ASD domen predstavlja skup funkcija koje implementiraju logiku za realizaciju specifičnih poslovnih funkcionalnosti za pružaoce usluga/servisa u AS domenu. Operativni i menadžment domen (eng. *Operation & management domain - OMD*) OMD obuhvata sljedeće funkcije: održavanje sistema, zatim praćenje i detektovanje nastalih problema u radu, proaktivna predikcija mogućih problema, takođe poseban sistem optimizacije rada uređaja. Domen kontrole resursa (eng. *Resource & interchange domain - RID*) DKR ima kao osnovne funkcije kontrolu pristupa resursima i mogućnost dijeljenja resursa između više IoT sistema. Korisnički domen (eng. *User domain - UD*) KD obuhvata različite vrste korisničkih interfejsa za interakciju sa IT sistemom. Međudomenske funkcije su sljedeće: sigurnost, bezbjednost, pouzdanost, povjerenje i privatnost, umreživost, interoperabilnost, itd.

Dok funkcionalni pogled daje pregled sistema preko njegovih funkcionalnih komponenti, sistemski pogled daje pregled sistema preko fizičkih komponenti. **Sistemski pogled** daje sljedeće aspekte: ključne fizičke komponente, generalizovanu arhitekturu, strukturu sistema sa distribucijom i topologijom komponenti, tehnički opis komponenti.

Komunikacioni pogled opisuje komunikacione mreže IoT sistema i entitete koje one povezuju. Četiri su mreže obično dio IoT sistema: mreže malog dometa; pristupne mreže; servisne mreže koje povezuju elemente u okviru i između DKR, ASD i OMD domena; i korisnička mreža povezuje korisnički domen sa IoT sistemom tj. ASD i OMD domenima, a IoT i druge ne-/IoT sisteme sa DKR domenom.

Informacioni pogled je jako složen i prestavlja sve informacije sistema koje kreiraju komponente koje ga koriste, nadgledaju i kontrolišu. Takođe informacija je relevantna za sistem i odgovara na pitanja 5w – who, where, what, when, why. Odnosno objašnjava podatke sistema kontekstualno. Strang i Linnhoff-Popien su dali sažeti pregled različitih pristupa modeliranja kontekstnih podataka [22]: model ključ-vrijednost, modeli sa hijerarhijom tagova za označavanje, grafički modeli, objektno-orjentisani modeli, logički modeli, modeli bazirani na ontologiji. Danas razvojem semantičkog veba [23] modeli bazirani na ontologijama su prihvaćeni kao najpogodniji za modelovanje kontekstnih informacija i dalju manipulaciju njima posredstvom inteligentnih algoritama mašinskog učenja.

Korisnički pogled sa korisničke perspektive pojašnjava način razvoja, testiranja, rada i korišćenja IoT sistema. Definiše uloge i poduloge korisnika, te njihove aktivnosti.

4. ZAKLJUČAK

Današnje IoT platforme su eklektična kombinacija komponenti preuređenih iz postojećih platformi, a koje pokušavaju da se pozabave trenutno identifikovanim problemima u vezi sa razvojem i primjenom IoT sajber-fizičkih sistema uključujući krajnje tačke: potrošače i industriju.

Svi sistemi se bave pitanjima registracije, uključivanjem velikog broja inteligentnih objekata i ogromnom količinom potecijalnih podataka [8]. Identitet objekata i drugih komponenti IoT sistema je bitan upravo za autorizaciju u procesu registracije i za davanje pristupa resursima autorizovanim korisnicima. Svi entiteti u konceptualnom modelu IoT sistema (Slika 3.) imaju posebno naglašen identitet. Identitet je takođe osnovni podatak za predstavljanje uređaja sistemu (eng *Se-*

lf-description sistemska karakteristika opisana u 2.1). Dosadašnji sistemi za upravljanje identitetima nisu prilagođeni IoT aplikacijama, velikom broju različitih objekata sa različitim ulogama i načinima identifikacije, takođe nisu se bavili M2M komunikacijama.

Za IoT sisteme problem su i sigurnosni aspekti i zaštita privatnosti, obrađeni u okviru poglavlja 2.4. Periferni uređaji, uglavnom senzori, zbog ograničenih hardverskih mogućnosti, nemaju mogućnost implementacije ozbiljnijih sigurnosnih mehanizama [24]. Ovdje leži i najveći problem po sigurnost IoT sistema. Daljinsko rekonfigurisanje, ažuriranje uređaja kao i nadzor su ranjive tačke budućih IoT tehnologija. IoT podrazumjeva umrežavanje do sada neumreženih sistema kod kojih nikakve sigurnosne mjere do sad nisu preduzimane. Kategorizacija problema privatnosti data je u [25]:

1) neovlaštena identifikacija;
2) neovlaštena lokalizacija i praćenje;
3) profilisanje ličnosti (na osnovu podataka o njegovim aktivnostima vrši se definisanje njegovih preferencija i profila ličnosti);
4) prezentacija ili interakcija sa privatnim podacima iz neznanja da su oni osjetljivi;
5) problem eliminacije privatnih podataka sa starih uređaja;
6) napadi na senzorsku opremu kojoj se mogu slati upiti preko internet konekcije;
7) problem povezivanja različitih sistema u IoT platforme – povezivanjem različitih centara podataka podaci gube kontekst u kom su se prethodno nalazili te imali različite dozvole od strane korisnika kom pripadaju.

Raznovrsnost IoT komponenti nameće pitanje integralnosti, interoperabilnosti i kompozitnosti [8]. Integralnost sistema podrazumjeva da svaka komponenta sistema nesmetano komunicira sa drugim komponentama sistema pomoću definisnih protokola i signlizacije. U IoT sistemima se povećava opterećenje mreže sa novim krajnjim uređajima i količinama podataka koje šalju, a sa druge strane su zahtjevi da se reakcije na događaje od strane sistema realizuju u što kraćem vremenskom roku. Pri čemu treba pravilno izbalansirati sigurnosne mehanizme. Da bi se istinski omogućila interoperabilnost između komponenti sistema IoT treba da riješi 4 nivoa problema [26]: mehanizmi za sintaksičke transformacije podataka u jedinstvenu strukturu, transformacija podataka iz različitih domena, semantičke transformacije podataka između komponenti koje ne podrazumjevaju samo istu strukturu podataka već isto značenje istih, i kontekstualne transformacije – svjesnost konteksta je potrebna karakteristika aplikacija i servisa IoT sistema. Sintksička i domenska transformacija su riješene, ali semantička i kontekstualna transformacija još čekaju svoje standardizacije u oblasti ontologija. Kompozitnost podrazumjeva mogućnost zamjene jedne komponente drugom istog ponašanja i karakteristika rada (opisana u 2.3.)

Skalabilnost IoT platformi u centrima/skladištima podataka kod većine implementiranih riješenja je nedovoljna za buduće potrebe i dizajnirana na osnovu tradicionalnih arhitektura. Gartner [27] definiše „web – scale IT“ kao sistemski orjentisan arhitektonski šablon koji omogućava brz i skalabilan razvoj i isporuku veb usluga zasnovanih na korištenju agilnih, jasnih i trajnih načela. Takođe navodi da je „web – scale IT“ arhitektura neophodna IoT platformama kako bi riješile problem skalabilnosti. „Web – scale IT“ je bolji pristup dizajniranju, izgradnji i upravljanju infrastrukturom cenatara podataka koji su pokrenule veb kompanije i provajderi oblaka kao što su Google, Amazon i Facebook [28]. Ključne karakteristike „Web – scale IT“ su: *hiperkonvergencija na x86 serverima*, *inteligencija u softveru*, *sve je distribuirano*, *Sistem samooporavka*; *API bazirana automatizacija i bogata analitika*.

Pošto se očekuje uključivanje velikog broja inteligentnih objekata koji kreiraju ogromnu količinu podataka nameće se sljedeće pitanje: koliko i kakve podatake prikupljati i skladištiti? Jedno od riješenja jeste da se dio sirovih podataka, a koji nisu od značaja za platformu, skladišti na korisničkim uređajima. Pošto bi tolika količina podataka bila vremenom prevelika za korisničke uređaje onda bi ih trebalo agregirati i takve slati prema platformi. Još jedan način da se smanji količina podataka i rastereti platforma od pogrešnih podataka jeste pročišćavanje [9] kojim se uklanjaju iz vremenskih nizova podaci koji predstavljaju nemoguća stanja senzora i nemoguće vrijednosti. Trenutno IoT platformama nedostaju tehnologije koje će koordinirati analitiku pristupne mreže i analitiku platforme.

Kada je u pitanju vlasništvo nad podacima današnjim sistemima nedostaje robusna kontrola koja će odgovarati na pitanja: gdje, kako, od strane koga i za šta se smiju koristiti podaci, te ko je njihov vlasnik: ponuđač IoT usluge, vlasnik aplikacije, vlasnik senzora, krajnji korisnik mobilnog telefona/ prolaza i slično. Takođe nedostaju pravne regulative koje će izbalansirati korisne inovacije IoT aplikacija i zaštitu prava potrošača.

U okviru visoko heterogenih IoT tehnologija standardizacija predstavlja osnovu za dalji razvoj IoT platformi, pa je i opisana referentna arhitektura značajan pomak naprijed ka budućnosti u kojoj će biti riješena sva problemska pitanja a navedene karakteristike IoT-a zadovoljene. Identifikovani problemi su polazne tačke za nove istraživačke radove. Nove inovacije će svakako stvoriti i nove aplikacije IoT sistema i pomjeriti nas u budućnost za kakvu sigurno ne možemo ni pretpostaviti koliko će promijeniti život, rad, okruženje i sve ono na što smo već naviknuti.

5. LITERATURA

[1] Weiser, M., Hot Topics: Ubiquitous Computing, IEEE Computer, 1993., str. 71-72.
[2] Weiser, M., The world is not a desktop, ACM Interactions, Vol. 1, broj 1., 1994., str. 7-8.
[3] Satyanarayanan, M.: Pervasive computing: vision and challenges, Personal Communications, IEEE , Vol. 8, broj 4., 2001., str. 10-17.
[4] Arnrich, B., Mayora, O., Bardram, J., Pervasive or Ubiquitous Healthcare, Methods Inf Med, Vol. 49, 2010., str. 65-66.
[5] ISO/IEC JTC 1, Internet of Things (IoT), Geneva, 2014. Dostupno: https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf [Pristupljeno: 4. Maj 2020.]
[6] ISO/IEC CD 30141:20160910(E): Information technology In-

ternet of Things Reference Architecture (IoT RA).Topic Maps. International Organization for Standardization, Geneva, Switzerland, 2016. Dostupno: https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf. [Pristupljeno: 4. Maj 2020.]
[7] CERP-IoT – Cluster of Europeasn Research Projects on the Internet of Things, Vision and Challenges for Realising the Internet of Things, Clusterbook, 1.1.The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects, 2010.
[8] ISO/IEC JTC 1, Internet of Things (IoT), White Paper: IoT 2020: Smart and secure IoT platform, IEC, Geneva, 2016. Dostupno: https://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf [Pristupljeno: 4. Maj 2020.]
[9] Ahmad, N.F., Hoang, D.B., Phung, M.H., Robust preprocessing for health care monitoring framework, 11th International Conference on e-Health Networking, Applications and Services (Healthcom), 16-18 Dec. 2009, Sydney, NSW, Australia, str. 169 – 174., PrintISBN: 978-1-4244-5013-8, DOI: 10.1109/HEALTH.2009.5406196.
[10] Dey, A.K., Understanding and Using Context, Journal:Personal and Ubiquitous Computing, Vol. 5, broj 1., 2001., str. 4-7.
[11] Abowd, G. D., Mynatt, E. D., Charting past, present, and future research in ubiquitous computing, ACM Trans. Comput.-Hum. Interact., 2000., str. 29-58., http://doi.acm.org/10.1145/344949.344988
[12] Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D., Context aware computing for the internet of things: A survey, Communications Surveys & Tutorials, IEEE, Vol.16, No 1,2014., str. 414-454.
[13] Wassernaar, J., Privacy rules, a steeple chase for systems architects, www.w3.org. 2006. , Dostupno: http://www.w3.org/2006/07/privacy-ws/papers/04-borking-rules/ [Pristupljeno: 4. Maj 2020.]
[14] Langheimreich M., Privacy by design: Principles of privacy-aware ubiquitous systems, Swiss Federal Institute of Technology Zurich, Zurich, Switzerland: Swiss Federal Institute of Technology (ETH), Dostupno: http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf [Pristupljeno: 4. Maj 2020.]
[15] Bluetooth SIG, BLUETOOTH SPECIFICATION Version 5.0 | Vol 1, Part A, 5.4.5 Privacy Feature, 06 December 2016 Dostupno: https://www.mouser.it/pdfdocs/bluetooth-Core-v50.pdf [Pristupljeno: 4. Maj 2020.]
[16] Bluetooth SIG, BLUETOOTH SPECIFICATION Version 5.0 | Vol 1, Part A, 5 SECURITY OVERVIEW, 06 December 2016 Dostupno: https://www.mouser.it/pdfdocs/bluetooth-Core-v50.pdf [Pristupljeno: 4. Maj 2020.]
[17] OASIS SOA Reference Model (SOA-RM) TC, Dostupno: https://www.oasis-open.org/committees/soa-rm/faq.php [Pristupljeno: 4. Maj 2020.]
[18] V. Mišković, Đ. Babić, PERVASIVE PERSONAL HEALTHCARE SERVICE DESIGNED AS MOBILE SOCIAL NETWORK, International Journal of Interactive Mobile Technologies - iJIM, Vol. 10, No. 4, Oct. 2016, ISSN: 1865-7923, DOI: https://doi.org/10.3991/ijim.v10i4.5913.
[19] V. Mišković, Đ. Babić, Implementation of the Flexible Bayesian Classifier for Assessment of Patient's Activities within the Real-time Personalized Mobile Application, Engineering, Technology & Applied Science Research – ETASR, Vol. 7, No. 1, pp. 1405-1412, Feb. 2017, ISSN(e-journal): 1792-8036, ISSN (print): 2241-4487.
[20] Baldauf, M., Dustdar, S., i Rosenberg, F., A survey on context-aware systems, Int. J. Ad Hoc and Ubiquitous Computing, Vol. 2, broj 4., 2007., str. 571-583.
[21] Indulska, J. i Sutton, P., Location management in pervasive systems, CRPITS'03: Proceedings of the Australasian Information Security Workshop, 2003., str.143–151.
[22] Strang, T. and Linnhoff-Popien, C., A Context Modeling Survey, First International Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp, 2004.
[23] Horrocks, I., Parsia, B., Patel-Schneider, P.F., Hendler, J., Semantic Web Architecture: Stack or Two Towers?, Principles and Practice of Semantic Web Reasoning 2005, str. 37-41.
[24] Marčeta, B., PROBLEMI AUTENTIFIKACIJE I AUTORIZACIJE U IOT OKRUŽENJU (ENG. PROBLEMS OF AUTHENTICATION AND AUTHORIZATION IN THE IOT ENVIRONMENT), Info M, str.4-10. , 2019., UDC: 004.42:004.72.057.4.
[25] Ziegeldorf1, J. H. , Morchon, O.C., and Wehrle1 K., Privacy in the Internet of Things: threats and challenges, Security Comm. Networks 2014; 7:2728–2742, Published online 10 June 2013 in Wiley Online Library (wileyonlinelibrary.com), DOI: 10.1002/sec.795.
[26] Industrial Internet Consortium, Industrial Internet Reference Architecture (Version 1.7), Object Management Group, Needham, MA, US, 2015.
[27] Gartner Inc., Infrastructure and Operations Leaders: Prepare for the IoT Rush, 2016.
[28] Nutanix, Overview of Web-Scale Infrastructure, 2014. Dostupno: http://releasd-images.s3.amazonaws.com/pdf/1403612302870.pdf [Pristupljeno: 4. Maj 2020.]

Dr Vanja Mišković, docent, Slobomir P Univerzitet, Doboj-Bijeljina, RS-BIH
E-mail: vanja.elcic@gmail.com
Oblasti interesovanja: Mobilno računarstvo, Senzorske mreže, Multimedije

Mr Željko Gavrić, istraživač saradnik, Fakultet organizacionih nauka, Univerzitet u Beogradu
E-mail: gavric.zeljko@yahoo.com
Oblasti interesovanja: Multimedije, HCI, Internet tehnologije