https://doi.org/10.37528/FTTE/9788673954165/POSTEL.2022.034

UPRAVLJANJE PODACIMA U PAMETNIM GRADOVIMA

Vesna Radonjić Đogatović[1], Marta Ivanović[2]
[1]Univerzitet u Beogradu - Saobraćajni fakultet, v.radonjic@sf.bg.ac.rs
[2]Roaming Networks, marta.ivanovic@roamingnetworks.rs

Rezime: *Upravljanje podacima predstavlja skup procesa i veština koji su neophodni za organizaciju, čuvanje i deljenje podataka dobijenih tokom istraživačkog procesa. Upravljanje velikom količinom podataka od fundamentalnog je značaja za realizaciju pametnih gradova. Jedinstveni okvir za upravljanje podacima je kritičan za pametan grad i sve njegove aplikacije. U ovom radu razmatrani su ključni zahtevi za procese prikupljanja, obrade i distribucije podataka u pametnim gradovima, a posebna pažnja je posvećena zahtevima vezanim za privatnost i unapređenje bezbednog upravljanja podacima.*

Ključne reči: *Bezbednost, Internet stvari, Pametan grad, Privatnost, Upravljanje podacima*

1. Uvod

Od pametnog grada se očekuje korišćenje računarskih i komunikacionih resursa, integracija, kao i upravljanje i analiza ogromnih količina podataka da bi se omogućilo poboljšanje bezbednosti, efikasnosti i produktivnosti svih segmenata pametnog grada, a time i kvaliteta života građana [1].

Jedna od karakteristika savremenog, tzv. digitalnog doba je velika količina podataka u elektronskom obliku koja iz godine u godinu postaje sve veća, pogotovo u kompleksnim mega-korporacijama i visoko rizičnim radnim okruženjima. Pretraživanje, korišćenje i pravilno upravljanje podacima u svakom privrednom okruženju danas predstavlja izazov, kao i bezbednost i adekvatno skladištenje podataka [2]. Zbog toga, upravljanju podacima treba posvetiti posebnu pažnju.

Pametni gradovi predstavljaju urbana područja u kojima se podaci prikupljaju korišćenjem različitih metoda i uređaja. Integracija različitih ugrađenih uređaja i sistema u okviru pametnog grada omogućava funkcionisanje Interneta stvari (IoT, *Internet of things*) u pametnim gradovima. IoT generiše ogromnu količinu podataka koji se mogu iskoristiti za poboljšanje bezbednosti i efikasnosti, kao i omogućavanje novih servisa za stanovnike grada [3].

Proces upravljanja podacima sastoji se od tri faze:

- prikupljanja,
- obrade i
- deljenja, tj. distribucije podataka.

Prikupljanje podataka podrazumeva primenu standarda koji obezbeđuju doslednost kada se koriste različite tehnike prikupljanja podataka. Na primer, podaci dobijeni sa senzora u bežičnim senzorskim mrežama (WSN, *Wireless Sensor Network*) i mobilnim *ad hoc* mrežama (MANET, *Mobile Ad hoc Network*) moraju biti istog tipa i formata da bi se omogućila integracija podataka zajedno sa efikasnom obradom [1].

Obrada podataka može uključivati različite operacije kao što su brisanje, klasifikacija, pretraživanje, itd. Obim baza podataka, kao i potreba za obradom i procenom ogromnih količina podataka u poslovne svrhe u stalnom je porastu [3].

Osim prikupljanja i obrade podataka, neophodni su različiti obrasci pristupa podacima i alati za analizu podataka kako bi se nadgledale i poboljšale performanse aplikacija i servisa za efikasnu distribuciju podataka u okviru pametnog grada. Mere kvaliteta podataka će uspostaviti ravnotežu između efikasnosti i troškova na osnovu ciljeva pametnih gradova. Korišćenje podataka obezbeđuje ponovnu upotrebu prikupljenih podataka identifikacijom aplikacija i servisa koji zahtevaju isti skup podataka. Ovi aspekti su usko povezani i zahtevaju kritičku analizu tačnosti i efikasnosti u odnosu na troškove.

Pametni grad se sastoji od različitih kategorija krajnjih korisnika, kao što su građani, državne agencije, industrijski partneri, itd. Svaki krajnji korisnik ima svoj skup zahteva za aplikacije i servise pametnog grada, kao i za kvalitet servisa [2]. Na primer, građanima u pametnoj kući je prvenstveno potrebna dobra povezanost sa društvenim mrežama i video striming visoke rezolucije, dok javne zdravstvene ustanove mogu zahtevati bezbedne veze sa serverima na *cloud*-u za čuvanje i preuzimanje osetljivih informacija o zdravstvenoj zaštiti pacijenata. Stoga je upravljanje podacima značajno za diferenciranu distribuciju podataka i dodeljivanje prioriteta na osnovu različitih kategorija krajnjih korisnika, servisa i aplikacija u pametnom gradu.

Ovaj rad je organizovan na sledeći način. Nakon uvodnog dela, u drugom poglavlju razmatrani su najznačajniji koncepti za upravljanje podacima, pristup i arhitektura održivog sistema upravljanja podacima u pametnim gradovima. Aspekti bezbednosti i privatnosti podataka razmatrani su u trećem poglavlju, sa posebnim osvrtom na upravljanje energijom i saobraćajem i transportom u pametnim gradovima. U četvrtom poglavlju data su zaključna razmatranja.

2. Značaj upravljanja podacima u pametnim gradovima

Odgovarajuće upravljanje podacima je osnova za pametne gradove. Suštinski, pametan grad povezuje informacione i komunikacione tehnologije radi distribucije podataka. Podaci iz IoT aplikacija, senzora i postojećih gradskih partnerskih sistema koriste se za analitiku kako bi podstakli ispunjavanje novih ciljeva razvoja grada. Ovo uključuje *open-source* podatke, *crowd-source* podatke, kao i podatke sa drugih povezanih uređaja ili izvora [4].

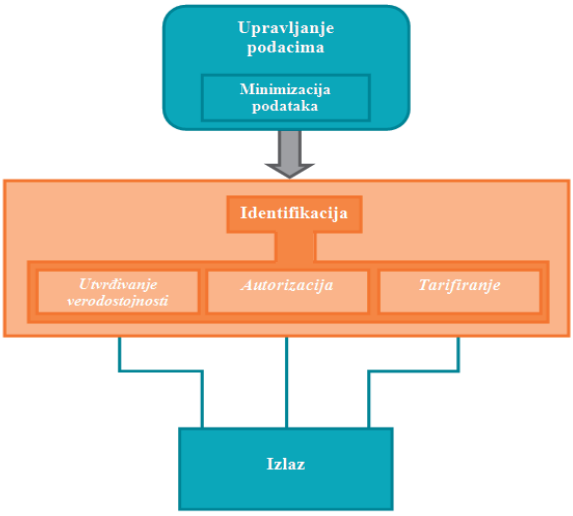
Za upravljanje podacima od velikog značaja su sledeći koncepti:

1. *Big data* predstavlja koncept koji definiše podatke pomoću karakteristika:
   - veliki obim podataka,
   - podaci se ne mogu prethodno rasporediti u tabele baze podataka i
   - podaci se kreiraju velikom brzinom i moraju se brzo prikupiti i obraditi.
2. Minimizacija podataka predstavlja značajan problem zbog prikupljanja i obrade velike količine ličnih podataka u bazama podataka različitih

institucija [3]. Cilj je da se ograniči prikupljanje i skladištenje privatnih podataka od strane velikih organizacija koje mogu zloupotrebiti ove podatke. Minimiziranje skupa podataka i vremena skladištenja može pomoći u zaštiti privatnosti pojedinca, koja može biti narušena od strane države ili drugih velikih organizacija.

3. *Data mining* može pomoći u donošenju odluka u mnogim oblastima kao što su maloprodaja, razvoj, telekomunikacije, zdravstvo, osiguranje i poštanske usluge. Koristi se za određivanje novih trendova kupovine, identifikaciju nezakonitih radnji i prevara korišćenjem kreditnih kartica, itd.
4. AAA (*Authentication*, *Authorization*, *and Accounting*) arhitektura obuhvata utvrđivanje verodostojnosti, autorizaciju i tarifiranje i ima značajnu ulogu u današnjim mrežnim tehnologijama. Bežičnim pristupnim tačkama je potreban AAA za zaštitu, takođe se AAA može koristiti za pristup mreži udaljenih korisnika [3]. AAA obuhvata sledeće elemente:
   - Klijent: Klijent je korisnik koji treba da pristupi mreži.
   - *Inline Security Getaway* (Autentifikator): Odgovoran je za utvrđivanje uslova pristupa korisnika.
   - Server baze podataka: Služi za skladištenje podataka koji će pomoći da se donese odluka o pristupu i potvrđuje kredencijale korisnika za pristup mreži.
   - AAA server: Preuzima zahtev klijenta od autentifikatora. Donosi konačnu odluku o finaliziranju pristupa mreži za klijenta.
   - Obračunski sistem: Prati proces korisnikovog pristupa mreži. Ovaj sistem je kontrolisan i u stanju je da prikupi informacije o korisnikovom pristupu mreži u određenom vremenskom periodu [3].

Na slici 1 prikazana je arhitektura održivog sistema upravljanja podacima.



Slika 1. Arhitektura održivog sistema upravljanja podacima

Pametni gradovi moraju integrisati podatke iz svih dostupnih izvora. Ovo prevazilazi uobičajeni problem nemogućnosti deljenja podataka zbog njihove

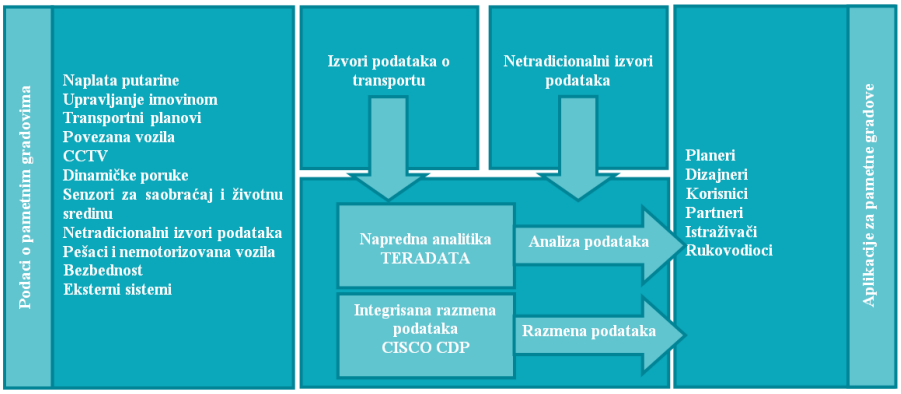
raspoređenosti u različite klase. Da bi se objedinili svi podaci i omogućila analiza koja prevazilazi pojedinačne klase ili organizacije, predlaže se pristup koji podrazumeva ukidanje klasa podataka [4]. Ovo rešenje za upravljanje pametnim gradom, u kombinaciji sa analizom, pruža različite mogućnosti za pametne gradove. Sa porastom potrebe za pametnim upravljanjem podacima, dolazi i do povraćaja investicija ili smanjenja troškova u gradu. Tim sredstvima se zatim mogu finansirati drugi projekti pametnih gradova.

Jedan primer prednosti unapređenja raspoloživosti podataka je mogućnost da se podaci iz povezanih i autonomnih vozila, zajedno sa analitikom kretanja građana dobijenih sa pametnih telefona, koriste za formiranje realne slike o ponudi i tražnji za gradskim prevozom. Na taj način, koriste se podaci o transportu, koji beleže gde ljudi žive i rade, kako bi urbanisti poboljšali prelazna rešenja i primenili inovativna transportna rešenja. Ovo su vitalne komponente analitičkog ekosistema sposobne da se integrišu, analiziraju i dele ogromne količine podataka u realnom vremenu. Ekosistem uključuje skladište podataka i analitičku platformu. To omogućava pametnom gradu da optimizuje resurse, poboljša infrastrukturu, kvalitet života stanovnika i omogući održivi ekonomski razvoj.

Pristup pametnom upravljanju podacima podrazumeva uspostavljanje, razvoj i povezivanje mogućnosti upravljanja podacima širom pametnog grada. Dakle, pametno upravljanje podacima omogućava:

- integraciju podataka sa senzora, drugih automatizovanih izvora i dodatnih podataka o gradu u jedinstvenu platformu kao koherentan tok podataka,
- automatsko korišćenje više izvora podataka u centralizovanom skladištu koje omogućava deljenje i analizu podataka i
- deljenje podataka, pri čemu način upravljanja kontroliše pristup podacima za svakog korisnika [4].

Na slici 2 prikazan je prethodno opisani pristup pametnom upravljanju podacima.

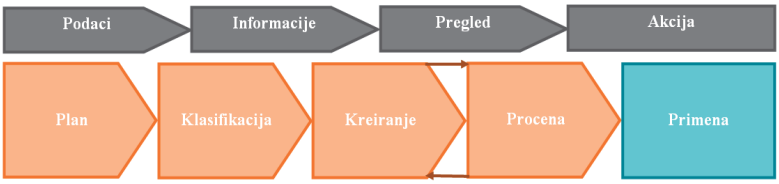


Slika 2. Pristup pametnom upravljanju podacima [4]

Pristup prikazan na slici 2 definiše dva kriterijuma:

- podaci su odmah dostupni i spremni za upotrebu i
- pravilna upotreba podataka donosi značajne koristi za grad.

Na slici 3 prikazana je jedna mogućnost sprovođenja pametnog upravljanja podacima u pametnim gradovima.

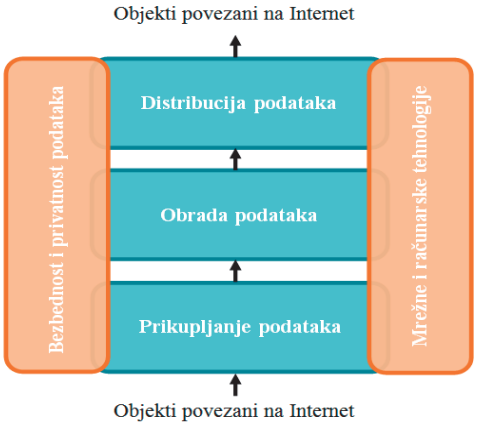


Slika 3. Faze implementacije pametnog upravljanja podacima

Pametno upravljanje podacima treba da podrži sve elemente pametnog grada. Ovaj pristup pomaže gradovima da evoluiraju od samostalnih ili usko fokusiranih projekata pametnih gradova do visoko integrisanih, poslovnih okruženja. Fokusirajući se na pametno upravljanje podacima, projektima pametnih gradova je zagarantovan uspeh kroz prikupljanje podataka, njihovu obradu i distribuciju do krajnjih korisnika.

3. Bezbednost i privatnost podataka

Realizacija pametnih gradova zavisi od interoperabilnog integrisanog pristupa. Značajan izazov u realizaciji pametnih gradova je upravljanje bezbednošću i privatnošću podataka, što je važno ne samo zbog sprečavanja potencijalnih nefunkcionalnosti aplikacija i servisa, već i da bi se sprečila paralizacija celog grada [5]. Da bi se omogućilo efikasno upravljanje podacima i eliminisale pretnje po bezbednost i privatnost koriste se mrežne i računarske tehnologije (Slika 4).



Slika 4. Pregled životnog ciklusa podataka

Kao što je ilustrovano na slici 4, posmatra se tok podataka kroz pametni grad počevši od različitih tehnologija za prikupljanje podataka, obradu i distribuciju. Ovo uključuje izazove u pogledu bezbednosti i privatnosti podataka, kao i softverske i tehnike virtuelizacije koje omogućavaju različite mrežne i računarske tehnologije za jednostavnije funkcionisanje pametnih gradova.

Analiziranje izazova bezbednosti i privatnosti u pametnim gradovima nije jednostavno zbog složenosti sistema i uključenosti brojnih učesnika. Osim tehnoloških i socio-ekonomskih faktora, odluke gradskih vlasti takođe utiču na bezbednost i privatnost.

Pametni gradovi predstavljaju novu eru Interneta i komunikacije, a sa njom dolazi i novi skup pretnji sajber bezbednosti. U pametnim gradovima, milijarde uređaja prikupljaju, čuvaju i obrađuju podatke koristeći hardver ugrađen u okruženje. Zahvaljujući heterogenosti tehnologija u pametnim gradovima, bezbednost i privatnost predstavljaju višedimenzionalni problem, za koji tradicionalna rešenja možda neće biti dovoljna.

Još jedan aspekt ranjivosti je fizički distribuirana priroda pametnih gradskih mreža, koje bi mogle da sadrže ogroman broj malih uređaja i senzora, a predstavljaju izazov u pogledu bezbednosti i privatnosti. Fizički distribuirane mreže otežavaju pružanje fizičke bezbednosti i povećavaju površinu napada. Isto tako, upotreba jeftinih uređaja i senzora najavljuje nove pretnje za bezbednost i privatnost. Na primer, provalnici mogu da koriste snimke kamere, podatke sa senzora pokreta, mikrofone ugrađene u pametne televizore i slično, da otkriju kada u kući nema nikoga [5]. Takve pretnje bezbednosti i privatnosti dodatno se povećavaju upotrebom malih i jeftinih IoT uređaja koji možda nemaju mogućnosti da podrže kriptografska rešenja neophodna za protivmere uobičajenih pretnji bezbednosti i privatnosti.

Pametne kuće su još jedna komponenta pametnih gradova koja će predstavljati ogromne pretnje za bezbednost i privatnost. Kućni aparati postaju pametniji svakim danom i građani bi uskoro mogli da kontrolišu sve aspekte svojih domova, kako lokalno, tako i daljinski putem sistema pametnih kuća. *Google Home* i *Amazon Echo* su dva najnovija uređaja koji omogućavaju svojim vlasnicima da kontrolišu delove svojih domova. Pametni televizori opremljeni mikrofonom i kamerama, sigurnosne kamere sa senzorima pokreta, pametni termostati, pametna svetla, pametni frižideri, pametne brave na vratima, pametna brojila i pametne roletne već su prisutni u mnogim domovima. Iako su takvi sistemi značajni i mogu pomoći da ljudi bolje upravljaju svojim domovima, problemi upravljanja njihovom bezbednošću i privatnošću i dalje nisu dobro proučeni.

Na primer, zlonamerni korisnici mogu zloupotrebiti prikupljene podatake sa ličnih uređaja koji se koriste u domovima. Prikupljeni podaci se mogu koristiti za profilisanje i praćenje korisnika ili za pokretanje drugih vrsta napada [5]. Najupečatljivija razlika između tradicionalne računarske bezbednosti, napada na privatnost i napada na pametne kuće je broj različitih načina na koje zlonamerni korisnici mogu da dobiju pristup. Provalnici mogu da odrede gde i kada da opljačkaju ciljanu kuću na osnovu signala sigurnosnih kamera, senzora pokreta, obrazaca korišćenja energije i mogu da dobiju pristup ciljnim domovima korišćenjem slabosti pametne brave. Takvi napadi ne mogu samo da prouzrokuju finansijsku štetu, već predstavljaju i ozbiljnu pretnju privatnosti.

3.1. Pretnje po bezbednost i privatnost

Platforma koja nadgleda i kontroliše gradsku infrastrukturu u pametnom gradu uvodi nekoliko novih pretnji po bezbednost i privatnost građana. Osnovni principi bezbednosti informacija su poverljivost, integritet i raspoloživost. Ovi principi važe i za druge aspekte pametnog grada. Poverljivost je potrebna da bi se zaštitila privatnost građana i važne informacije ostalih učesnika u upravljanju gradom. Integritet štiti podatke od modifikacija koje mogu dovesti do odluka štetnih po grad i njegove građane. U zahtevima za aktiviranje se potvrđuje autentičnost zahteva za izbegavanje neovlašćenih promena u fizičkoj infrastrukturi grada. Raspoloživost podataka je od suštinskog značaja

za upravljanje gradom. To je posebno potrebno u teškim situacijama i napadima, kada je potrebno koordinirati, na primer, spasilačke operacije za javnu bezbednost [6].

Kritična gradska infrastruktura mora biti zaštićena od zlonamernih napada bezbednosnim mehanizmima na platformi zasnovanoj na IoT. Štaviše, platforma mora da kontroliše pristup privatnim informacijama korisnika i podsistema. Generalno, napadi mogu ciljati IoT infrastrukturu u bilo kom trenutku, od uređaja na terenu, do komunikacionih kanala ili servera. Napad može pokušati da sabotira ili kompromituje podsisteme, preuzimajući kontrolu nad određenim aspektima grada. Drugi cilj su informativni podaci na IoT platformi, što ugrožava privatnost građana.

Osnovna klasifikacija pretnji obuhvata eksterne i interne pretnje.

Pošto platforma za pametne gradove omogućava pristup kritičnoj infrastrukturi i poverljivim podacima, može predstavljati metu eksternih napada. Informaciona platforma pametnog grada moraće da bude otporna na eksterne napadače. Eksterni napadači mogu napasti uređaje ili komunikacione kanale. Posebno treba uzeti u obzir sledeća pitanja:

- Neovlašćeni pristup podacima: Napadači mogu pokušati da pristupe privatnim podacima korisnika, komponentama ili podsistemu IoT okruženja. Na primer, potrošnja energije u gradskim područjima ili čak kućama je potencijalno interesantna za slučajeve neželjene komercijalne upotrebe. Platforma čuva informacije koje šalju senzori, tako da postoji rizik da napadač pokuša da pristupi ili izmeni privatne podatke.
- Neovlašćena kontrola uređaja: Odnosi se na uređaje integrisane u okruženje pametnog grada koji se kontrolišu automatski ili putem daljinskog upravljanja. To mogu biti displeji, semafori, sistemi grejanja ili čak protivpožarni izlaz. Platforma pod svim okolnostima mora sprečiti pogrešnu primenu ovih uređaja od strane eksternih napadača.
- Hakovanje i sabotaža: Postoji nekoliko mogućih scenarija gde eksterni napadači sabotiraju funkcionisanje gradske infrastrukture. Platforma mora da ponudi odgovarajuće mehanizme za sprečavanje upada i šifrovanje podataka kako bi se sprečio otkaz podsistema izazvanog neovlašćenim upadima. Kada napadač kompromituje delove sistema, on može da koristi ovaj kompromitovani podsistem da napadne kompletnu infrastrukturu pametnog grada, i tada bi delovao kao interni napadač.

Usled složenosti komponenti unutar pametnog grada, postoji nekoliko internih pretnji po bezbednost koje se moraju razmotriti. Interni napadači su posebno opasni. Oni dobro poznaju infrastrukturu, mogu direktno pristupiti ili kontrolisati sistem, pomoću gradske infrastrukture ili IoT platforme. Interni napadači mogu biti: korisnici ili administratori podsistema i hakeri koji su već kompromitovali delove sistema [6].

Jednom kada je deo sistema kompromitovan, hakeri mogu delovati kao interni napadači na ostatak infrastrukture. Mora se poštovati princip odbrane kako bi se izbeglo da kompromitovanje podsistema izazove napad na celokupnu infrastrukturu. Princip odbrane nalaže da se u sistem postavi više slojeva bezbednosne kontrole, tako da prevazilaženje jednog sloja bezbednosne kontrole i dalje ne kompromituje ceo sistem. U tom smislu se razmatra:

- Neovlašćeni interni pristup podacima: Interni napadači mogu imati mogućnost da zaobiđu određene mehanizme kontrole pristupa i tako pristupe podacima. Ako su podaci zaštićeni kriptografskim sredstvima, pristup važnim dokumentima je i dalje težak zadatak za interne napadače.

- Narušavanje integriteta podataka i uređaja: Integracija nekoliko podsistema u jednu platformu ugrožava integritet podataka komponenti sa neočekivanim sporednim efektima od drugih komponenti. Greške u softveru ili hardverski otkazi ne bi trebalo da utiču na podatke ili komunikaciju drugih komponenti.

3.2. Bezbedno upravljanje podacima u pametnim gradovima

Podaci prikupljeni u okviru pametnog grada moraju biti zaštićeni kako bi se smanjio rizik od krađe podataka koja može dovesti do krađe identiteta i finansijskih gubitaka. Neophodan je distribuirani okvir za IoT aplikacije koje prikupljaju, obrađuju i dele velike količine heterogenih podataka da bi se ostvarila bezbednost s kraja na kraj (E2E, *End-to-End*) i tačne informacije za potrebe donošenja odluka u skladu sa zahtevima privatnosti vlasnika podataka [6].

Zbog sve veće količine podataka u pametnim gradovima, koji su dostupni zahvaljujući ICT-u, predviđa se da će rizik i uticaj pretnji po bezbednost i privatnost biti sve veći i da može imati ozbiljne posledice po zajednicu. Stoga su istraživanja o rešenjima koja pružaju bezbedne operacije i omogućavaju zaštitu podataka i informacija od suštinskog značaja. Potrebno je realizovati bezbednu platformu za zaštitu senzora i uređaja, koja omogućava kontrolu pristupa resursima i bezbedno skladištenje i obradu podataka.

Podaci na platformu za podatke stižu sa različitih senzora, a aktuatori primaju komande za aktiviranje sa ove platforme. Platforma treba da nudi interfejse za različite vrste servisa, kao što su merenje i kontrola potrošnje energije ili saobraćajnih tokova. U nastavku su prikazane moguće upotrebe platforme za podatke u pametnom gradu.

3.2.1 Upravljanje energijom

Očekuje se da će do 2050. godine preko šest milijardi ljudi živeti u gradovima i okolnim regionima [6]. Shodno tome, autonomno i pametno funkcionisanje gradova biće kritičan zahtev u bliskoj budućnosti. Izazovi koji se odnose na sposobnost gradske infrastrukture da zadovolji potrebe svakog građanina u pogledu vodosnabdevanja, transporta, zdravstvene zaštite, obrazovanja, bezbednosti i korišćenja energije, moraju se rešiti kako bi se očuvali i unapredili ekonomski, društveni i ekološki uslovi za blagostanje građana. U tom smislu je potrebno obezbediti referentni sistem sposoban da inteligentno upravlja korišćenjem energije u okviru pametnog grada, koji će istovremeno omogućiti potpunu kontrolu nad pristupom podacima.

Postizanje energetske efikasnosti u zgradama zahteva interakciju između brojnih subjekata koji obezbeđuju praćenje potrošnje energije i povratne informacije o potrošnji, koristeći sisteme automatizacije i senzore, i sprovode ekonomske strategije za uštedu energije. Da bi se ispunili takvi zahtevi na nivou grada, neophodno je obezbediti zajedničku platformu koja informiše korisnike o potrošnji energije, kao i da korisniku daje mogućnost interakcije sa sistemom kako bi definisao specifične strategije za uštedu energije ili kontrolisao sopstvene uređaje integrisane u platformu. Platforma koja uključuje uređaje i podatke zahteva da budu ispunjeni bezbednosni zahtevi da bi se obezbedila privatnost korisnika, pouzdani izvori podataka, poverljivost i bezbedna komunikacija [6].

3.2.2 Pametan saobraćaj i transport

Jedan od glavnih budućih izazova u pametnim gradovima biće upravljanje stalno rastućom količinom gradskog saobraćaja, što je posebno izraženo u svetskim metropolama. U skoro svakom većem gradu na svetu, saobraćajne gužve koje pogađaju velike delove užeg gradskog jezgra predstavljaju svakodnevnu pojavu. Ovo nije problematično samo zbog veće količine buke i zagađenja uzrokovanih saobraćajem, već takođe uzrokuje veće troškove transporta i značajno smanjuje bezbednost građana u saobraćaju.

Postojeća saobraćajno-transportna infrastruktura u gradu mora biti kombinovana sa platformom koja nudi rešenja za poboljšanje načina funkcionisanja, nivoa informisanosti učesnika i njihove bezbednosti u saobraćaju i transportu. Ovo će omogućiti integraciju različitih izvora podataka o saobraćaju i transportu. Primena odgovarajuće platforme za podatke imaće veliki značaj u upravljanju gradskim saobraćajem i transportom, posebno kada su u pitanju vanredne situacije. Najvažniji cilj platforme u ovom kontekstu primene predstavlja povezivanje različitih nezavisnih sistema, kako bi se izbegle vanredne situacije ili njihovo brzo rešavanje u slučaju da se dogode.

Da bi se efikasno implementirali Inteligentni transportni sistemi (ITS, *Intelligent Transportation Systems*), potrebno je obezbediti bežični pristup sa malim kašnjenjem i visoko pouzdanim prenosom u realnom vremenu, što omogućava arhitektura 5G bežične komunikacione mreže. Neophodno je da se podaci prikupljaju sa različitih senzora koji se nalaze na vozilima i putevima i da se automatski prikupljeni podaci analiziraju u realnom vremenu [7].

Očekuje se da vozila imaju percepciju o sopstvenom okruženju. Kao rezultat toga, savremeno vozilo je postalo senzorska platforma koja prenosi i prima podatke iz svog okruženja. Takvi podaci se mogu koristiti za podršku naprednim bezbednosnim aplikacijama koje se koriste sa ciljem redukcije broja saobraćajnih nezgoda, povećanja efikasnosti saobraćaja i poboljšanja pristupa vozilima hitnih službi. Međutim, ove aplikacije zahtevaju koordinisan okvir, sa funkcijama koje podržavaju veoma nisko kašnjenje za signale upozorenja, veće brzine prenosa senzorskih podataka između vozila i infrastrukture, visoku mobilnost, pouzdanost i skalabilnost.

4. Zaključak

Iako mnogi gradovi već primenjuju neke funkcionalnosti pametnih gradova, većina se zadovoljava samo malim delom čitavog spektra mogućnosti koje pametan grad može da ponudi. Jedan od razloga je nedovoljan stepen integracije i analize dostupnih podataka. Najbolji rezultati od monetizacije podataka postižu se kada se primenjuje ceo proces od prikupljanja podataka do konverzije u informacije, sve do konačnog definisanja akcija i strategija delovanja. Prema tome, prikupljanje, skladištenje, korišćenje podataka, a zatim i delovanje na osnovu podataka je izuzetno dragoceno za pametne gradove, kako za njihov dalji razvoj, tako i za njihovu ekonomsku stabilnost.

Pametni gradovi zahtevaju pametno upravljanje podacima kako bi korisnici dobijali relevantne informacije, a programerima aplikacija omogućili da kreiraju nove usluge i koriste analitiku za kontinuirano poboljšanje sistema pametnog grada. Imperativ je postići konvergenciju različitih uređaja i sistema sa jedinstvenim okvirom za

upravljanje podacima kroz njihov životni ciklus. Krajnji cilj je poboljšanje kvaliteta života građana, smanjenje troškova života i postizanje održive životne sredine.

U ovom radu su identifikovana ograničenja i predstavljeni istraživački izazovi za upravljanje podacima, bezbednost i privatnost podataka. Istaknuto je da je neophodan razvoj platforme podataka koja omogućava obradu i distribuciju podataka uz zaštitu bezbednosti i privatnosti. Neophodno je usvojiti niz inovacija i poboljšanja kako bi se odgovorilo na izazove koje nameće sve brži razvoj pametnih gradova i zahteve za konstantnim poboljšanjima svih aspekata funkcionisanja pametnog grada.

Literatura

[1] A. Kirimtat, O. Krejcar, A. Kertesz, M. F. Tasgetiren, "Future Trends and Current State of Smart City Concepts: A Survey," *IEEE Access*, vol. 8, pp. 86448-86467, 2020, doi: 10.1109/ACCESS.2020.2992441.

[2] A. K. M. B. Haque, B. Bhushan, G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends", *Expert Systems*, Wiley, vol. 39, 2022, doi: 10.1111/exsy.12753

[3] W. Burange, H. D. Misalkar, "Review of Internet of Things in Development of Smart Cities with Data Management & Privacy", *International Conference on Advances in Computer Engineering and Application (ICACEA)*, IMS Engineering College, Gazijabad, Indija, 2015, str. 189-195.

[4] Teradata, "Smart Data Management is the Blueprint for Smart Cities", 2018, dostupno na: https://cutt.ly/xYctO2O

[5] A. Gharaibeh, S. J. Hussini, M. Guizani, "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies", *IEEE Communications Surveys & Tutorials*, 2017, vol. 19, br. 4, str. 2456-2501, doi: 10.1109/COMST.2017.2736886.

[6] J. M. Bohli, A. Skarmeta, M. V. Moreno, D. García, P. Langendörfer, "SMARTIE Project: Secure loT Data Management for Smart Cities", *International Conference on Recent Advances in Internet of Things (RIoT)*, str. 1-6, Singapur, 2015.

[7] L. Guevara, F. Auat Cheein, "The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems", *Sustainability*, 2020; vol. 12, br. 16: 6469, doi: 10.3390/su12166469

Abstract: *Data management is a set of processes and skills necessary to organize, store and share data obtained during the research process. Managing a large amount of data is of fundamental importance for the realization of smart cities. A unified data management framework is critical for a smart city and all its applications. This paper discusses the key requirements for the processes of data collection, processing and distribution in smart cities, and special attention is paid to the requirements related to privacy and the improvement of data management security.*

Keywords: *Security, Internet of Things, Smart City, Privacy, Data Management*

DATA MANAGEMENT IN SMART CITIES

Vesna Radonjić Đogatović, Marta Ivanović