

Regulacija tržišta usluga Interneta stvari u pametnim gradovima

Weber, Mario

Doctoral thesis / Disertacija

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:168:554495>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-07-27**



Repository / Repozitorij:

[FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repository](#)





Sveučilište u Zagrebu
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Mario Weber

REGULACIJA TRŽIŠTA USLUGA INTERNETA STVARI U PAMETNIM GRADOVIMA

DOKTORSKI RAD

Zagreb, 2019.



Sveučilište u Zagrebu
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Mario Weber

REGULACIJA TRŽIŠTA USLUGA INTERNETA STVARI U PAMETNIM GRADOVIMA

DOKTORSKI RAD

Mentor:
prof. dr. sc. Ivana Podnar Žarko

Zagreb, 2019.



University of Zagreb
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Mario Weber

MARKET REGULATION OF INTERNET OF THINGS SERVICES IN SMART CITIES

DOCTORAL THESIS

Supervisor:
Professor Ivana Podnar Žarko, PhD

Zagreb, 2019

Doktorski rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva, na Zavodu za telekomunikacije.

Mentor: prof. dr. sc. Ivana Podnar Žarko

Doktorski rad ima: 122 stranica

Doktorski rad br.: _____

O mentoru:

Ivana Podnar Žarko je redoviti profesor na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva gdje predaje kolegije u području raspodijeljenih informacijskih sustava. Diplomirala je, magistrirala i doktorirala u polju elektrotehnike na FER-u, 1996., 1999. odnosno 2004. godine.

Zaposlena je na Zavodu za telekomunikacije FER-a od 1997. godine. Usavršavala se na Tehničkom sveučilištu u Beču, Austrija i Ecole Polytechnique Fédérale de Lausanne (EPFL), Švicarska. U prosincu 2017. godine izabrana je u zvanje redovitog profesora. Sudjelovala je u nizu istraživačkih projekata financiranih iz domaćih izvora i fondova EU, a trenutno je voditelj FER-ovog Laboratorija za Internet stvari i tehnički koordinator H2020 projekta symbIoTe: Symbiosis of smart objects across IoT environments. Sudjeluje kao istraživač u radu Znanstvenog centra izvrsnosti za znanost o podacima i kooperativne sustave koji je prvi je nacionalni centar izvrsnosti u području tehničkih znanosti u Hrvatskoj. Objavila je preko 60 znanstvenih radova u časopisima i zbornicima radova u području raspodijeljenih sustava, Interneta stvari i obrade velike količine podataka te je bila član programskog odbora većeg broja međunarodnih znanstvenih skupova.

Prof. dr. sc. Podnar Žarko je član svjetske stručne udruge IEEE, a od 2011. do 2014. godine je bila predsjednica Odjela za komunikacije Hrvatske sekcije IEEE. Primila je nagradu Hrvatske sekcije IEEE za izniman inženjerski doprinos u 2013. godini.

About the Supervisor:

Ivana Podnar Žarko is Full Professor at the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia (UNIZG-FER) where she teaches distributed information systems. She received her B.Sc., M.Sc. and Ph.D. degrees in electrical engineering from UNIZG-FER, in 1996, 1999 and 2004, respectively.

She is affiliated with the Department of Telecommunications at UNIZG-FER from 1997. She was a guest researcher and research associate at the Technical University of Vienna, Austria, and a postdoctoral researcher at the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland. She was promoted to Full Professor in December 2017. She has participated in a number of research projects funded by national sources and EU funds, and is currently leading the UNIZG-FER Internet of Things Laboratory. Ivana Podnar Žarko is the Technical Manager of the H2020 project symbIoTe: Symbiosis of smart objects across IoT environments, and is currently participating in the Centre of Research Excellence for Data Science and Advanced Cooperative Systems, which is the first national center of excellence in the field of technical sciences in Croatia. She has co-authored more than 60 scientific journal and conference papers in the area of large-scale distributed systems, IoT, and Big data processing, and has and has served as a program committee member for a number of international conferences and workshops.

Prof. Ivana Podnar Žarko is a member of IEEE and was the Chapter Chair of IEEE Communications Society, Croatia Chapter (2011-2014). She has received the award for engineering excellence from the IEEE Croatia Section in 2013.

SAŽETAK

Uspjeh usluga Interneta stvari (IoT-usluga) uvelike ovisi o standardima, ali i o regulatornim pravilima koja trebaju biti postavljena od strane donositelja politika (vlada, regulatora). Bez definiranih standarda, sučelja i protokola, pravo širenje IoT-a teško će biti moguće. Osim toga, pravodobna uspostava ravnoteže između standarda i pravila s jedne strane, te slobodnog razvoja IoT usluga i samoregulacije s druge strane, predstavlja veliki izazov. Ukoliko donositelji politika u početku razvoja postave previše restriktivne regulatorne mjere, mogu ugušiti razvoj IoT-a. Istovremeno izostanak regulatornih mjera ne daje nikakvu pravnu sigurnost poduzećima što može dovesti do smanjenja ulaganja u IoT-bazirana rješenja.

Sadržaj doktorske disertacije obuhvaća istraživanje u području Interneta stvari koje su svojstvena pametnim gradovima, s naglaskom na pitanja regulacije tržišta elektroničkih komunikacija. Disertacija analizira moguću regulaciju tržišta Interneta stvari (IoT) i definira taksonomiju IoT-usluga za primjenu u gradovima. Cilj je predložiti metodu za definiranje regulatornih zahtjeva i analizu njihovog utjecaja na usluge Interneta stvari u području pametnih gradova koji bi s jedne strane bili prihvatljivi industriji i poticali daljnji razvoj IoT-usluga, a s druge strane definirali jasna pravila koja bi ujedno predstavljala pravnu sigurnost za investitore u ovo područje. Za izradu predloženog modela potrebno je postojeće znanstvene/industrijske modele prilagoditi regulatornim pravilima koja su jasno postavljena za različita područja elektroničkih komunikacija, a opet daju dovoljno slobode da se stvori poticajno investicijsko okruženje. U radu je predložena taksonomija usluga Interneta stvari za različita područja primjene povezivanjem tehničkih obilježja pojedinih IoT usluga s regulatornim obilježjima. Presjekom obilježja za svaku pojedinu ulogu u lancu vrijednosti dana je preporuka za lakšu implementaciju IoT usluge. Na kraju je predložen poslovni model koji je pogodan za manje države, veličine Republike Hrvatske, u kojima gradovi samostalno nemaju dovoljno resursa za implementaciju projekata pametnog grada.

Ključne riječi: pametni gradovi, Internet stvari, regulatorna obilježja, poslovni model

MARKET REGULATION OF INTERNET OF THINGS SERVICES IN SMART CITIES

The introduction of new technologies is never easy and requires significant persuasion of people in the reliability and security of new technologies, but also the recognition of potential of new technologies. A good example of this is from the last millennium, exactly March 1875. Today Western Union is known as a world-wide company for long distance money transfer. However, very few people know that Western Union was at that time the largest and most advanced telecommunications company in the United States. They were significant market power telecom operator. At that time, an unnamed innovator, Alexandra Graham Bell, offered his \$ 100,000.00 (\$ 2 million worth today) worth patent, today known as Bell's telephone, to the president of the Western Union Administration, William Orton. William Orton refused his offer. In the next few years, new small companies started using Bell's phone to take a portion of the market that was previously reserved for Western Union. When they saw that they are losing market, they tried to develop their own phone but, unfortunately, it was too late. They have never returned to the place they have occupied with their very successful telegraphic business model. Often, Western unit story is used in a business context as an anecdote that leaders with no visibility can adversely affect the future of a successful business. This is a good example of how sociological, political and technical aspects can affect development and business decisions.

From the example above, it is evident that new technology affects a complete life cycle, from sociological aspects, through policy to business decisions itself, which can affect the development of new technologies. One of these new technologies that can surely change the services we are familiar with today is the Internet of Things (IoT).

IoT is a network that connects objects from different environments to a large-scale IP-based network and forms the basis for the development of so-called smart environments, such as smart homes, factories or even cities. Unlike the current vertical development of particular areas and technologies (from motion sensor technology, wireless sensor networks, processing of large amounts of data), adding a new programming interface allows the concept of the IoT to be realized.

One of the areas in which IoT is most frequently used is the area of smart cities where ICT enables significant savings for the city budget and improves quality of life for citizens through different on-line city services.

The use of ICT is needed due to the rapid increase in urban environments. According to the United Nations' latest report, 55% of the world's population lives today in urban environments. According to the same report in the 1950s, 30% of the population lived in urban environments, and according to projections by 2050, 68% of the world's population would live in urban environments. Already today North America has 82% urban environment, Latin America 81%, and Europe 74%. This can be seen in the number of cities with more than 10 million inhabitants, of which there were only 3 in 1970, and it is expected that in 2030 there will be 43 cities with over 10 million inhabitants.

The Republic of Croatia follows European urbanization trends and is currently at 56.9% of urban population, and according to forecasts by 2050, it will have 71.3% of urban population.

Such a sudden rise in population in cities demands and usually triggers economic activities. Cities become in the centre of numerous activities, economic, social, cultural, and sociological and others. Rapid urban development creates strong pressure on existing infrastructure that was originally not intended for such a population growth, and expansion of the existing infrastructure may be very restrictive. That is where ICT can help to improve the existing processes, thus increasing the efficiency of the outdated infrastructure. In addition, the synergy of all stakeholders in the city (through cooperation between all city services and companies) achieves savings and greater efficiency in providing city services and at the same time can achieve additional earnings, thereby reducing budget dependence. With digital transformation from classic to smart cities, cities have to change the way of thinking and focus on innovation and use of technology to gain added value.

In the simplest way saying the smart city, represent an innovative city that uses the potential of ICT to increase the quality of life of people in cities and increase the efficiency of city services.

There are a number of obstacles that cities need to solve. One of them is certainly legal regulation that does not follow the rapid development of technology. Unlike the electronic communications that are over-regulated in some segments, the smart city

services market is not regulated at all. Legal regulation is not clear and there are fears of all stakeholders that by implementing their own solutions, they will get into the costs and in few years, law may be put out of force or become deficient. At the same time, the European Commission has published several framework regulations that govern certain segments of smart cities, such as energy, road safety, and user privacy.

Different stakeholders of smart city service each for himself must implement certain requirements arising from the above-mentioned directives.

In order to define and implement intelligent cities more easily, the ecosystem of intelligent cities needs to be described. The ecosystem of smart city services does not only apply to the city itself but also includes everything the city and its surroundings make, such as citizens with their social activities, infrastructure and technology. This is a broad term that goes beyond the city's boundaries and expands with every new service, new set of connected devices, new infrastructure, or even old infrastructure that use ICT technology to improve its usage. By introducing new IoT-based technology solutions, cities are increasingly becoming a living organism that can respond to the needs of citizens. They could also repair themselves as needed, learning from the environment how to react and behave in specific situations based on experience.

In order to achieve such transformation, challenges need to be addressed such as: structuring organization (city services) from vertical to horizontal structure; creation of algorithms and schematics that describe information generated by sensors; creating algorithms for analysis and processing of data obtained from sensors and creating additional value them; adoption of mechanisms for easy and massive installation and ensure reliable readings from the sensors to be calibrated.

The realization of IoT-based smart city services requires from all stakeholders to take specific roles within each layer of IoT stack. This is the reason that usually more than one service provider in a partnership relationship is involved in providing a single service. The most common roles within the IoT chain are: Infrastructure Provider, IoT Platform Provider, IoT Service Integrator, IoT User, End User. In addition, you can fine-tune the granulation of roles and get Device providers, IoT connectivity providers, and Developers of IoT services and applications.

The ecosystem of smart city services, as an emerging complex system that has the potential to present set of innovations, can potentially introduce new rules of conduct

among the stakeholders within value chain. Currently, scientists, politicians, CEOs of large companies in Europe and the United States are leading debate over possible behavioural rules. When introducing new regulation, the complexity of the IoT system should be taken into consideration. Therefore, the problem should be considered from several levels with a view to the future. Special attention should be taken to what market regulation brings, that is, how it can affect innovation and massive deployment of IoT solutions in society and the business environment. The US and European regulations regarding IoT in general (including the segment of smart cities) go in the same direction. Most of the discussions focus on the impact of technology on segments that are of interest to particular countries. In that way, US conducts discussions in area of privacy and security with special focus on IoT in the military industry while on the other hand, Europe focuses on the areas of consumer protection in different areas. Due to its directives, the EC puts a great pressure on the development of new technologies and services, ie, creating additional value from existing capacities. The European regulatory framework that should take into consideration when developing smart city services is the e-call directive, energy efficiency directive, roaming regulation, General data protection regulation and the e-privacy that can significantly affect service development.

Today great number of IoT services one could find on the market in different sectors, however, most of currently available solutions are vertically oriented standalone solutions. These solutions are usually bound to an ecosystem that can develop around one IoT platform. Vertically oriented solutions, among other things, do not share infrastructures and generated data between themselves (e.g., temperature and concentration of CO₂ are important for air quality monitoring system but at the same time can be used for calculation of green routes for bicycles and irrigation systems). Due to that, it is necessary to classify services according to their characteristics to better understand technical and regulatory requirements of these services. This paper identifies the technical and regulatory characteristics of smart city services that need to be well-positioned to develop successful IoT services in the context of smart cities, but also to meet legal and technical requirements that are currently in place or could be set up as regulatory requirements in the near future. Based on the detailed analysis of the smart city services, we distinguish and classify their technical and regulatory characteristics.

The technical characteristics of smart cities are mainly related to quality of service (QoS) and other technical parameters that are strictly related to the network or design of smart city services.

They may be related to the device, network, platform or service itself. Some of the technical characteristics are common, that is, they are used in almost all services. The technical characteristics used in smart city services, regardless of whether we are talking about a device, network, platform, or service, are:

- Number of end users – the real number of users who will use the service
- Number of IoT devices – the number of devices that will generate sensor data
- Data volume – complete volume of generated data per service
- Time sensitivity – Sensitivity to Data Delay (e.g. Health Care)
- Location-based services – Service dependency of location
- Billing – whether or not billing is made
- Scalability – the ability to expand the capacity of a service for a larger number of users or devices
- Platform openness and interoperability – existing market solutions are closed, proprietary solutions that are not compatible with other vendor systems. Interoperability solves the problem of locking services to one supplier.

In addition to the common technical characteristics, there are also technical features that are specific to devices:

- Communication mode – service may use wired or wireless communications network
- Computing capability – Should the device have computing capability for logical operations and simpler algorithms.
- Bandwidth – data transfer rate between devices and IoT platforms
- Delay – is the service sensitive to delays when receiving information
- Jitter – might not influence most services; however, for some specific services its influence may become significant
- Loss of data – some services may be highly sensitive to data loss and thus special mechanisms should be in place

Regulatory characteristics are related to legal acts and bylaws relevant to Smart City services. They are predefined by the national or EU directives and applicable to all EU member states. The most critical characteristics of services are:

- Lawfull interception – most states have a law that allows interception of data traffic, voice calls, messages and more recently OTT services such as Viber, Whatsapp, Telegrams, Signals, and similar.
- Service dependability - ability to avoid service failures that are more frequent and more severe than acceptable
- Personal data protection - one of the fundamental human rights, which stipulates that citizens have the right to protect their personal data. The new Regulation on Personal Data Protection and the ePrivacy Regulation further protects the rights of EU citizens.
- Security: concepts and solutions preventing cyber-attacks at the device and service level
- Operator switch – ability to change an IoT operator, i.e., any stakeholder from the IoT value chain
- Roaming - the ability to use the service after leaving the national network
- Interoperability and open access to data and services - as regulatory characteristic primarily refers to publicly funded smart city services and is closely related to the change of service provider

Based on previously identified characteristics, the taxonomy of smart city services is proposed. The proposed taxonomy provides a classification of major characteristics, both technical and regulatory, which are vital to be determined for any Smart City service during an initial phase of service requirements specification. Thus, it can guide Smart City stakeholders through the process of identifying key characteristics of their future services in accordance with service technical and regulatory requirements. However, this classification does not give an answer whether the individual service comply with the regulatory and technical requirements in order to be sucessfully implemented and used in practice. The proposed taxonomy is used to identify the key requirements for several selected examples of smart cities, namely smart (electricity) meters, smart parking, intelligent traffic systems, smart street lighting, and mobile crowd sensing.

All four services that are used as an example are the most commonly used smart city services. All of them have different characteristics and helps in significantly improving quality of life or increasing speed of services, which ultimately leads to greater citizen satisfaction.

All regulatory and technical characteristics are identified through the research, and a comparison of the characteristics of smart city services is given. Based on that, regulatory recommendations for each role in the value chain for all four smart city services are set and general regulatory recommendations for each role in the value chain are identified as follows:

- Device provider – interoperability and security
- Infrastructure provider – Roaming, Lawfull interception
- IoT platform provider – Interoperability (service and platform), Dependability, Platform provider switch, Privacy, Security and Open access
- IoT service integrator – Service provider switch, Security and Privacy
- IoT user – Privacy
- End user – Trust (if user generates data)

To conclude, the most important regulatory characteristics for a device provider are interoperability at the level of device protocol stack and security issues, also at the device level, where data integrity and authorized access to device is of primary importance. An IoT connectivity provider is responsible to ensure device roaming (relevant only to MCS with wearable devices since devices used in other use cases are stationary) and lawful interception. The main concerns of an IoT platform provider refer to platform dependability and security. With respect of dependability, availability and reliability of services offered by the platform are the most important requirement of the analyzed services, while data integrity, accuracy and completeness as well as authorized access to services and corresponding data are the most important security-related requirements. Moreover, an IoT platform provider should have obligation to offer an interoperable solution with well-defined service interfaces so that provider switch is possible. It also needs to enable open data access in case of Smart Parking and MCS, and define adequate policies to protect personal data ensuring user privacy. Similarly, to the IoT platform provider, the main concerns of an IoT service integrator relate to service

security and user privacy. We expect that IoT service integrator can be changed in all use cases except in Smart Street Lighting. Application developer needs to guarantee data integrity within a developed application and ensure that only authenticated users have access to certain data and services. In case the application stores some personal data, appropriate policies need to be defined. Note that in case of Smart Street Lighting, we do not expect that a mobile application will be developed for end users. For an IoT user, privacy concerns are the most important, while an end user has no specific regulatory obligations except to rightfully report readings in case of MCS, and requires trust in the entire ecosystem when its personal data is collected, stored and processed.

Since examples and best practices presented in Western Europe and their business models do not correspond to economic conditions in the Republic of Croatia and in the countries with similar GDP, a business model has been developed for each role in the value chain and presented through the business canvas model, which includes all regulatory characteristics. The Business Canvas Model provide tools that guide one to business thinking while at the same time keeping key points on view for both the one that define model and the entire team and all other stakeholders. Simply put, the business canvas model provides the framework for getting the most value out of new ideas while at the same time looking at all the potential risks and assumptions that they bring. Such a business model is presented through a smart parking service.

SADRŽAJ

Uvod	1
1. Pametni gradovi u kontekstu Interneta stvari	11
1.1. Arhitektura Interneta stvari	12
1.1.1. IoT-A Referentni model	14
1.1.2. ITU-T Y.2060	17
1.2. Protokoli Interneta stvari	20
1.3. Koncept i arhitektura pametnih gradova	23
1.4. Ekonomski potencijal pametnih gradova	28
1.5. Ekosustav usluga pametnih gradova	32
2. Regulatorni okvir za pametne gradove	40
2.1. Povijesni pregled regulacije u svijetu	40
2.1.1. Europa	40
2.1.2. Sjedinjene Američke Države	42
2.2. Europski regulatorni okvir za pametne gradove	43
2.2.1. E-call	43
2.2.2. Energy Efficiency directive	45
2.2.3. Roaming regulation directive	46
2.2.4. Uredba (EU 2016/679) o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (GDPR)	48
2.2.5. Uredba o E-privatnost (e-PR)	51
2.3. Mogući smjerovi regulacije	52
2.4. Preporučeni smjer	53
2.5. Praćenje i implementacija	54
3. Pregled tehničkih i regulatornih obilježja usluga pametnih gradova	56
3.1. Tehnička obilježja usluga pametnih gradova	57
3.2. Regulatorna obilježja usluga pametnih gradova	62
4. Taksonomija usluga pametnih gradova	72
4.1. Primjeri usluga	73

4.1.1. Pametna brojila električne energije.....	73
4.1.2. Pametno parkiranje	74
4.1.3. Suradno opažanje okoline u pokretu.....	75
4.1.4. Pametna (inteligentna) ulična rasvjeta	77
4.2. Rezultati istraživanja	78
4.3. Poslovni odnosi u lancu vrijednosti.....	84
5. Poslovni model usluga pametnih gradova	92
5.1. Poslovni model usluge pametnog parkiranja.....	95
5.2. Metoda za definiranje regulatornih zahtjeva i analiza njihovog utjecaja na usluge Interneta stvari u području pametnih gradova.....	102
5.3. Prijedlog poslovnog modela za države male i srednje veličine poput RH	104
6. Zaključak	108
Literatura	111
Popis slika.....	116
Životopis	118
Biographical Note	121

UVOD

Uvođenje novih tehnologija nikada nije jednostavno i zahtijeva znatno uvjeravanje ljudi u pouzdanost i sigurnost nove tehnologije, ali isto tako i u prepoznavanje potencijala nove tehnologije. Dobar primjer toga seže u period iz prošlog tisućljeća, točnije iz ožujka 1875. godine. Naime, poduzeće Western Union danas svi u svijetu poznaju kao poduzeće koje se bavi razmjenom novca na velikim udaljenostima, međutim vrlo mali broj ljudi zna da je poduzeće Western Union u to doba bilo najveće i najdominantnije telekomunikacijsko poduzeće u SAD-u. U to vrijeme, nepoznati inovator Alexandar Graham Bell je predsjedniku uprave Western Union-a Williamu Ortonu ponudio svoj patent za (Bellov) telefon za iznos od 100.000,00\$ što predstavlja današnju vrijednost od 2 milijuna dolara. William Orton je ponudu odbio. U sljedećih nekoliko godina manje kompanije počele su koristiti Bellov telefon kako bi ugrabile dio tržišta koje je do tada bilo rezervirano za Western Union. Kad su u Western Unionu vidjeli da gube tržište, pokušali su razviti vlastiti telefon, ali na njihovu žalost bilo je prekasno. Nikad se više nisu vratili na mjesto koje su zauzeli svojim vrlo uspješnim poslovnim modelom temeljenim na telegrafu. Često se ova priča zna koristiti u poslovnom kontekstu kao anegdota kako lideri bez vizije mogu negativno utjecati na budućnost poslovanja uspješnog poduzeća. Upravo je ovo dobar primjer koliko sociološki, politički i tehnički aspekti mogu utjecati na razvoj i poslovne odluke. Naime, predsjednik Western Uniona je bio vizionar i dobro je znao što akustični telegraf (kako su ga zvali u to vrijeme) može značiti za područje telekomunikacija. U vrijeme kada je Bell dao ponudu, Western Union je bio pod strahovitim pritiskom konkurencije, ali i zakonodavstva. Mnoge su manje tvrtke gradile svoje telegrafске mreže i preuzimale klijente nižim cijenama, međutim problem je bila i politika jer su politički lideri bili zabrinuti zbog monopola koji Western Union ima. Kako bi se povećala konkurentnost, neki su političari čak zagovarali direktnu podršku novostvorenim poduzećima koja bi se borila s Western Unionom. Političari su išli toliko daleko da su ih smatrali prijetnjom za nacionalnu sigurnost s obzirom da je 90% telegrafskog prometa išlo preko njih. Vlada se bojala hipotetske mogućnosti promjene informacija u tekstu od strane Western Uniona, a vezano uz politiku ili gospodarstvo. Zbog tolikog pritiska Western Union se grčevito borio da zadrži poziciju u području telegrafa što je otvorilo tržište za druge igrače u području telefona koji su vidjeli

priliku za uzimanje dijela tržišta. William Orton je bio vizionar i znao je što to znači, te je u vrijeme kad je Bell došao sa svojom idejom već dao svojim ljudima razviti sličan takav sustav. Međutim, tadašnji Bellov sustav je imao problem pouzdane transmisije govora na velike udaljenosti što je bio glavni fokus poduzeća. S druge strane Orton se bojava da bi takav sustav preopteretio postojeću mrežu Western Uniona te bi izgubili na kvaliteti.

Iz gore navedenog primjera vidljivo je da nova tehnologija utječe na kompletan životni ciklus, od socioloških aspekata, preko politike do samih poslovnih odluka koje mogu utjecati na razvoj nekih tehnologija. Jedna od takvih novih tehnologija koje zasigurno mogu promijeniti usluge s kojima smo danas upoznati je Internet stvari.

Mreža svih mreža, kako volimo nazivati Internet, odavno nije samo mreža računala, već također povezuje različite uređaje koji imaju sposobnost slanja i primanja informacija o stanju uređaja na mreži. Internet stvari (engl. Internet of Things, IoT) je koncept koji omogućuje umrežavanje različitih stvari i objekata iz svakodnevnog života te njihovu međusobnu komunikaciju putem Interneta, bez ljudske interakcije, a sve, naravno, s ciljem poboljšanja uvjeta i načina na koji živimo. Pojam „Internet of Things“ je prvi upotrijebio Kevin Ashton, direktor MIT Auto-ID centra, 1999. godine u prezentaciji za Procter & Gamble, ali je do učestalije upotrebe tog pojma prošlo još nekoliko godina. Formalno uvođenje pojma IoT je zabilježeno 2005. godine u izvješčaju ITU Internet report od strane organizacije International Telecommunication Union (ITU) [1]. U kolovozu 2013. je fraza „Internet of Things“ prihvaćena kao nova riječ u Oxfordskom engleskom rječniku gdje je definirana kao „predloženi razvoj Interneta gdje svakodnevni objekti imaju mogućnost povezivanja, te slanja i primanja podataka“. Razvojem IoT tehnologije, svaki uređaj oko nas će komunicirati s drugim uređajem i slati mu podatke ili ga kontrolirati, ovisno o prikupljenim podacima.

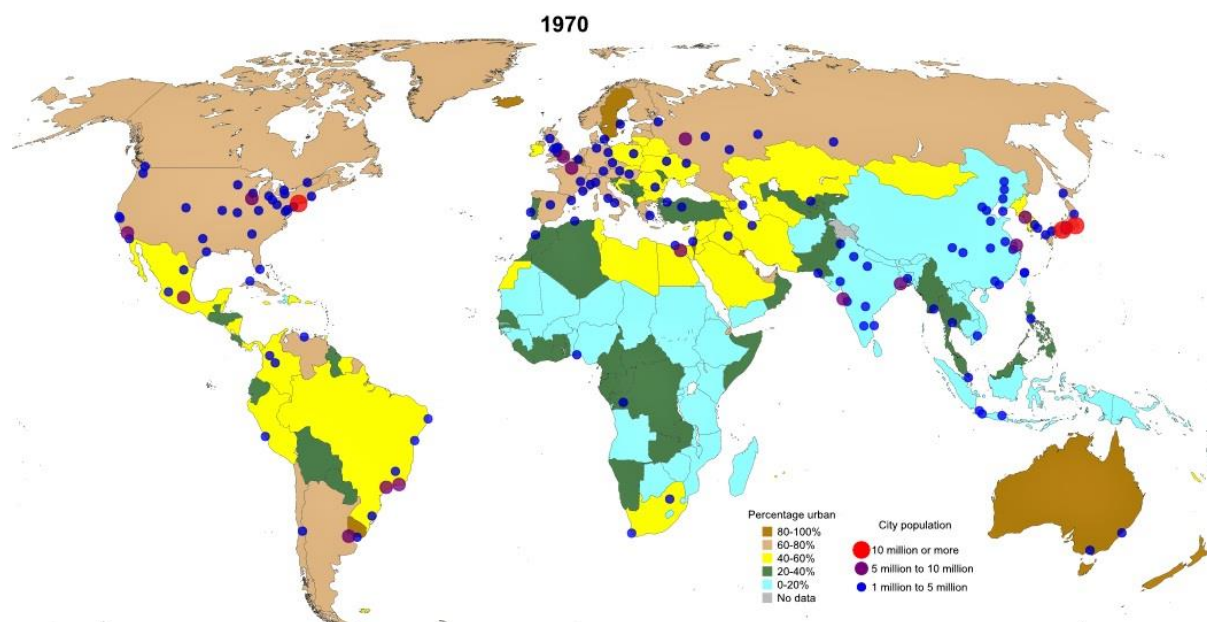
Internet stvari je mreža koja povezuje objekte iz različitih okolina u jedinstvenu mrežu velikih razmjera temeljenu na protokolu IP, a čini osnovu za razvoj tzv. pametnih okolina, npr. pametnih kuća, tvornica ili čak gradova. Za razliku od dosadašnjeg vertikalnog razvoja pojedinih područja i tehnologija (od tehnologija povezivanja uređaja u pokretu, bežičnih senzorskih mreža, obrade velikih količina podataka), dodavanjem novog programskog međusloja moguće je ostvariti koncept Interneta stvari. Programski međusloj omogućuje povezivanje različitih tehnologija i platformi, a čini podlogu za razvoj naprednih usluga bez posjedovanja do sada potrebnih znanja o svakoj tehnologiji zasebno, a u svrhu razvoja novih usluga [2]. Umrežavanje sve većeg broja objekata koji nas okružuju rezultirat će velikom količinom generiranih podataka koji moraju biti pohranjeni, obrađeni i prezentirani u

prihvatljivom obliku. Primjene usluga u području IoT-a su raznolike, od korisničkih aplikacija koje će pružati dodanu vrijednost samo korisniku koji ih je definirao do cjelokupnih grana znanosti kojima je omogućeno pojednostavljeno dijeljenje resursa, prikupljanje podataka iz velikog broja senzora, statistička analiza tih podataka ili čak zaključivanje nad podacima u stvarnom vremenu [3].

Jedno od područja u kojima se Internet stvari najčešće primjenjuje je upravo područje pametnih gradova gdje su upotrebom informacijske i komunikacijske tehnologije (IKT) omogućene značajne uštede za gradove, a stanovnicima gradova se podiže kvaliteta života omogućavanjem različitih gradskih usluga on-line putem.

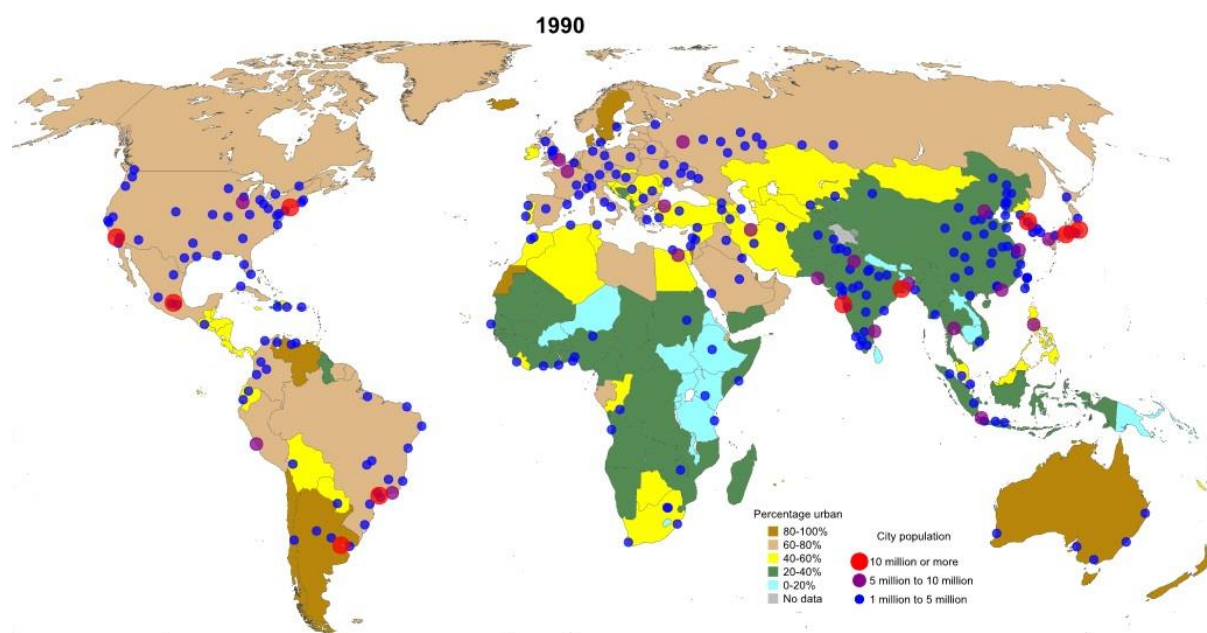
Upotreba IKT-a potrebna je upravo zbog naglog povećanja urbanih sredina. Prema zadnjem izvještaju Ujedinjenih naroda (UN DESA – UN Department of Economic and Social Affairs), „The 2018 Revision of World Urbanization Prospects“ [4], više od polovice stanovništva zemlje živi u gradovima. Točnije, 55% stanovništva živi u urbanim sredinama u 2018. godini. Usporedbe radi, 50-ih godina prošlog stoljeća 30% svjetske populacije je živjelo u urbanim sredinama, a procjenjuje se da bi do 2050 godine 68% svjetske populacije moglo živjeti u urbanim sredinama. Danas su najurbaniziranije regije svijeta Sjeverna Amerika gdje 82% populacije živi u urbanim sredinama, a slijede Latinska Amerika i Karibi s 81% i Europa sa 74%.

Najbolji prikaz naglog porasta urbanih sredina može se vidjeti iz vremenske karte (Slika 1-4) UN-a za urbane sredine i urbane aglomeracije iz 1970. godine, 1990. godine, 2018. godine i projekcije za 2030. godinu.

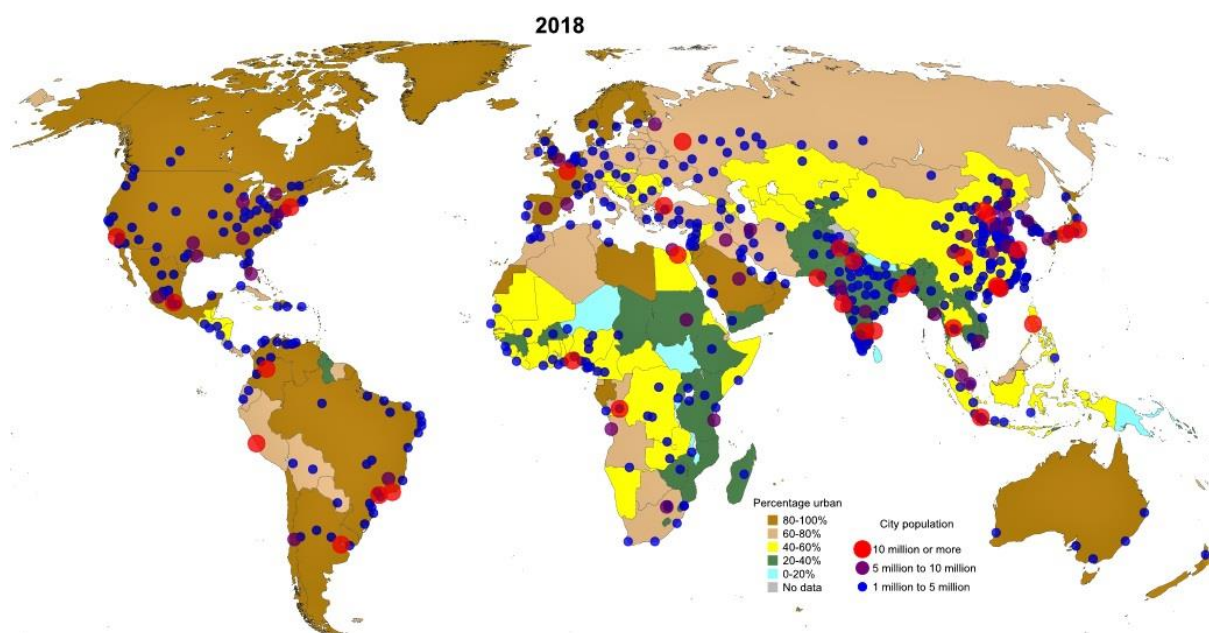


Slika 1: Postotak urbanizacije 1970. godine [4]

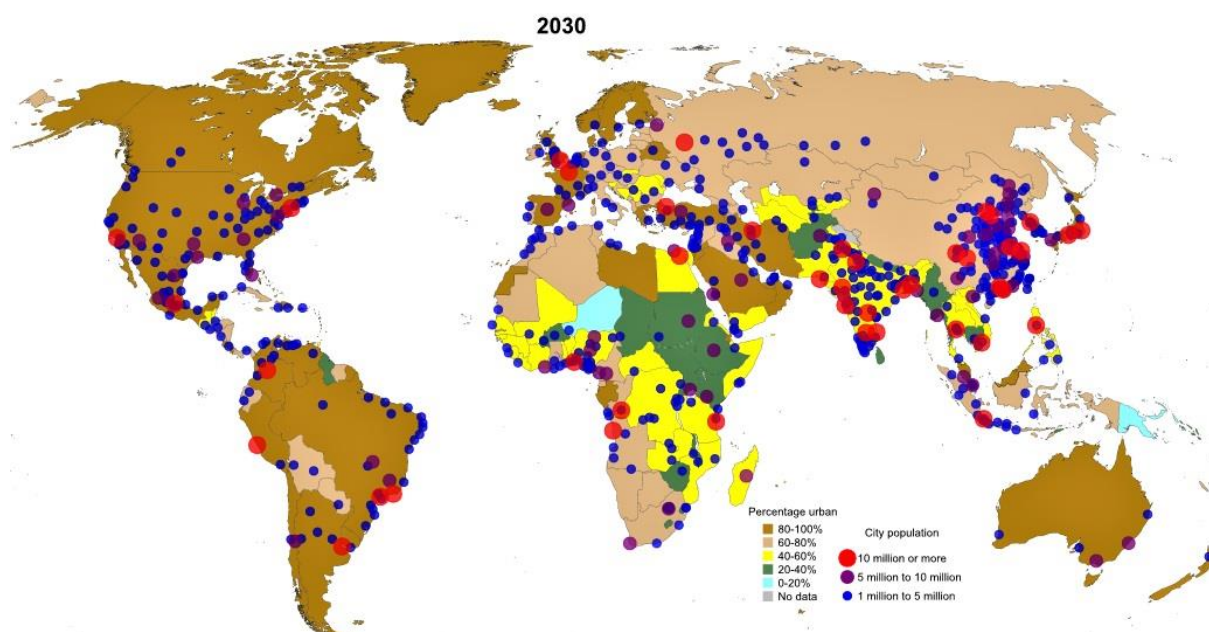
Iz slika 1-4 je vidljivo kako se predviđa da će broj gradova s više od 10 milijuna stanovnika narasti s 3 u 1970. godini na predviđenih 43 u 2030. godini, od kojih će većina biti na području Azije i Afrike.



Slika 2: Postotak urbanizacije 1990. godine [4]



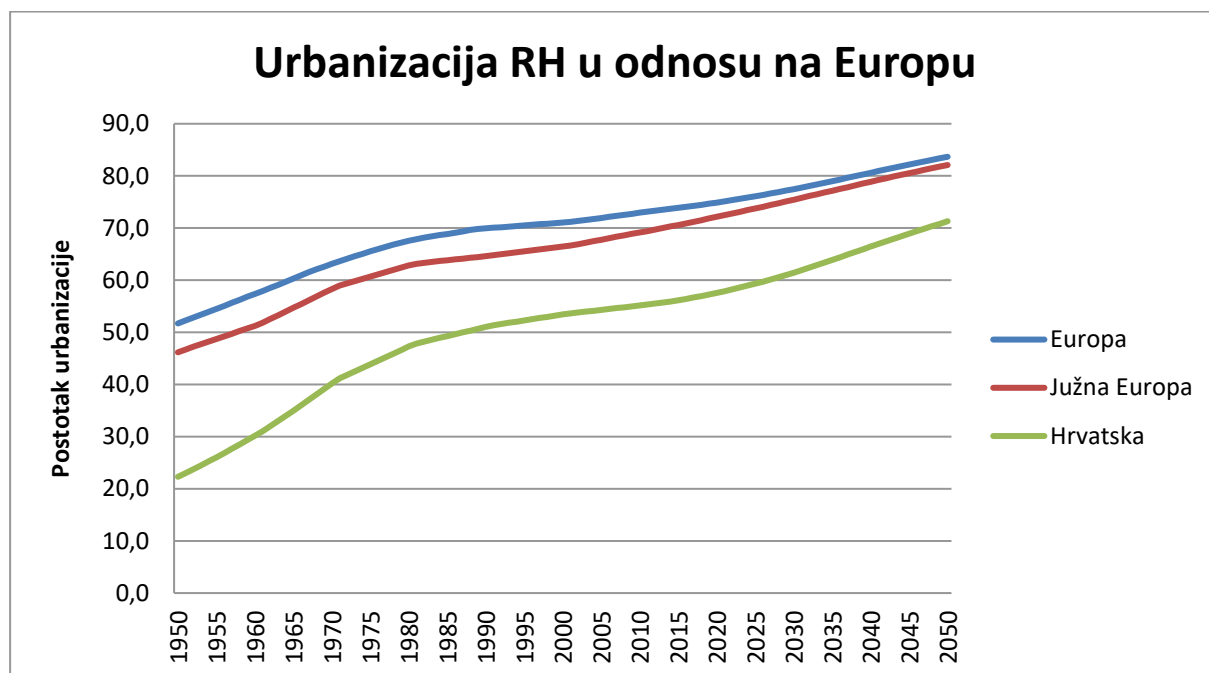
Slika 3: postotak urbanizacije 2018. godine [4]



Slika 4: Postotak urbanizacije 2030. godine [4]

U kontekstu ovog doktorskog rada zanimljivo je pogledati i podatke za Republiku Hrvatsku što je vidljivo na slici 5. Od 1950. godine, kada je u RH bilo svega 22,3% urbanog stanovništva koje je, kao i u ostatku Europe, lagano, ali gotovo linearno raslo do danas kada

RH ima 56,9% urbanog stanovništva, s predikcijom rasta do 71,3% urbanog stanovništva u 2050. godini.



Slika 5: Urbanizacija RH u odnosu na Europu

Zbog takvog naglog porasta urbanizacije, u zadnjih nekoliko godina, gradovi su postali pokretači gospodarskih aktivnosti u većini zemlja Europske unije i svijeta, a ujedno su postali i središte gospodarskih, društvenih, kulturnih, socioloških i brojnih drugih aktivnosti. Takav istaknuti i brzi napredak gradova prati i pritisak na nužni razvoj ključnog segmenta, a to je infrastruktura. Sinergijom svih dionika u gradu (međusobnom suradnjom svih gradskih službi i tvrtki) postižu se uštede i veća učinkovitost kod pružanja gradskih usluga, ali ujedno se ostvaruje i mogućnost dodatne zarade, čime se umanjuje ovisnost o proračunu. Primjer velikih gradova koji su krenuli u transformaciju iz klasičnih gradova u pametne gradove pokazuje da je promjena u upravljanju gradskim infrastrukturama i uslugama nužna. Takvom transformacijom gradovi moraju promijeniti i dosadašnji način razmišljanja te fokus staviti na inovativnost i korištenje tehnologije s ciljem ostvarivanja dodatne vrijednosti.

Pametani grad najjednostavnije rečeno predstavlja inovativan grad koji koristi potencijal IKT-a kako bi povećao kvalitetu života ljudi u gradovima, te povećao učinkovitost gradskih službi i usluga.

Pametani grad započinje svoj razvoj kvalitetnom izradom dugoročne strategije održivog razvoja i na temelju takve strategije priprema modele upravljanja i razvoja strateških inicijativa.

Dobro planirani i razrađeni gradovi predstavljaju zaokruženi i integrirani koncept, a ne niz parcijalno implementiranih tehnoloških rješenja. Na temelju toga koncept pametan grad uključuje: interoperabilnost svih gradskih sustava koji su međusobno povezani i nesmetano komuniciraju i izmjenjuju informacije koje koriste za različite potrebe, analizu i djelovanje gradskih službi na temelju podataka prikupljenih od građana i sustava na terenu, analizu potreba grada i građana radi podizanja kvalitete života građana, te suradnju svih dionika na tržištu pametnog grada, od javnih službi i privatnog sektora do akademske zajednice i ostalih dionika.

Na putu razvoja pametnih gradova postoji mnoštvo prepreka koje (putem) treba prebroditi. Jedna od njih je zasigurno i nedostatak regulative, odnosno zakonskog okvira koji uređuje pitanje pametnih gradova. Naime, u većini segmenata tržišta elektroničkih komunikacija postoje jasno uređeni zakonski okviri koji postavljaju određena pravila ponašanja i oni kao takvi daju s jedne strane svojevrsnu sigurnost proizvođačima opreme, proizvođačima usluga i operatorima da rade ispravno i da su njihove investicije zaštićene od zakonskih promjena, a s druge strane štite korisnike njihovih usluga i same države od štetnih posljedica. Upravo taj segment nedostaje na tržištu pametnih gradova. Zakonska regulativa nije jasna i postoji bojazan svih dionika da će implementacijom vlastitih rješenja ući u troškove koje će zakon kroz koju godinu možda staviti izvan snage ili će postati manjkavi.

S druge strane imamo dosta okvirnih regulativa, pogotovo u Europi koje uređuju pojedina područja, npr. energetiku, cestovnu sigurnost, zaštitu privatnosti korisnika, što direktno utječe na implementaciju usluga u pametnim gradovima. Svi uključeni dionici na tržištu ne trebaju implementirati sve funkcionalnosti usluga pametnih gradova. Različite uloge u razvoju i pružanju usluga pametnih gradova daju različite obveze dionicima. Pregled takvih uloga s regulatornim obvezama je ključan za masovniju i bržu implementaciju rješenja pametnih gradova. Upravo jedan takav pregled je dan i u ovom radu. Na temelju takve podjele dan je i prijedlog poslovnog modela na razini države Hrvatske koji odgovara svim državama veličine i ekonomskog statusa poput Republike Hrvatske.

Za vrijeme provođenja analize relevantne literature i postojećih projekata pametnih gradova moglo se zaključiti da i dalje postoje praznine i prostori vezani uz analizu regulatornih aspekata usluga pametnih gradova, njihove interoperabilnosti i relevantnih primjera najbolje prakse. U ovoj disertaciji predstavljena je taksonomija obilježja usluga pametnih gradova, kao i četiri karakteristična primjera usluga pametnih gradova kroz koje su identificirana njihova regulatorna i tehnička obilježja sukladno predloženoj taksonomiji. Na temelju napravljene analize, identificirani su glavni tehnički i regulatorni zahtjevi za najčešće klase usluga pametnih

gradova. Ova obilježja, gradski planeri i ostali dionici uključeni u razvoj takvih usluga mogu koristiti za jednostavnu identifikaciju ključnih tehničkih i regulatornih aspekata na koje se trebaju fokusirati za vrijeme planiranja, dizajniranja, implementacije i razmještanja usluga pametnih gradova.

Nakon definiranja regulatornih i tehničkih obilježja usluga pametnih gradova definirane su i uloge u ekosustavu pametnih gradova, ili bolje rečeno, definirano je tko je uključen u dizajn, implementaciju i pružanje usluge pametnog grada i kako su dionici međusobno povezani. Od proizvođača uređaja pa do krajnjeg korisnika dosta je uloga koje daju svoj specifični doprinos pružanju pojedine usluge pametnog grada. Potrebne su njihove međusobne veze, podjela odgovornosti i jasno definirana pravila kako bi se postiglo jednostavno i nesmetano razmještanje i funkcioniranje neke usluge.

Mnogi gradovi u svijetu su već započeli svoju digitalnu transformaciju. U Europskoj Uniji, niz istraživačkih projekata financiranih iz fondova EU je dalo snažan poticaj ovom procesu s mnoštvom inovacija i primjerima dobre prakse koji se sada šire diljem Europe. Jedan od prvih i dobro poznatih primjera je SmartSantander¹ projekt koji je poslužio kao početni primjer za ostale projekte koji su slijedili poput projekata Organcity² i Open & Agile Smart Cities³. Synchronicity⁴ je primjer projekta velikih razmjera koji integrira puno različitih izvora podataka širom gradova korištenjem softverskih komponenti FIWARE. Međutim, gore navedeni projekti su uglavnom usmjereni na tehničke aspekte i skaliranje pilot projekata pametnih gradova, dok su regulatorni aspekti većim dijelom ostali nepokriveni. U Sjedinjenim Američkim Državama, Bijela kuća je prepoznala da „novoosnovane zajednice civilnih lidera, znanstvenika, tehnologa i kompanija udružuju snage kako bi izgradile pametne gradove – zajednice koje grade infrastrukturu kako bi kontinuirano unaprjeđivale prikupljanje, agregiranje i korištenje podataka u svrhu povećanja kvalitete života njenih građana“ [5], a u 2016. godini Vijeće savjetnika predsjednika za znanost i tehnologiju je predložilo razvoj platforme za pametne gradove i predstavilo to kao „Gradski Web“ gdje svi ključni dionici dijele svoja iskustva, rezultate i najbolju praksu [6]. Iako gore spomenuti projekti i inicijative predstavljaju značajan primjer uspješnih projekata pametnih gradova, potrebna je dodatna analiza i klasifikacija osnovnih regulatornih aspekata usluge pametnih gradova koja će potaknuti širenje ovakvih usluga u drugim gradovima.

¹ <http://www.smartsantander.eu/>

² <https://organcity.eu/>

³ <https://oascities.org/>

⁴ <https://synchronicity-iot.eu/>

Iako se može pronaći velik broj članaka o uslugama pametnih gradova i njihovoj tehničkoj realizaciji, prema vlastitoj procjeni postoji svega mali broj članaka koji se bave regulatornim pitanjima i zakonskim obvezama sudionika uključenih u ekosustav pametnih gradova. U [7] autori se bave regulatornim okvirom vezanim uz zaštitu podataka sukladno novoj uredbi Europske komisije, a to je Uredba o zaštiti osobnih podataka (GDPR) te pokušavaju dati odgovor na pitanje hoće li nova zakonska regulacija usporiti razvoj pametnih gradova ili neće. GDPR se obično veže uz zaštitu privatnost podataka, a to je fokus u [8] kao putu za „sistematizaciju područja aplikacija, tehnologija, tipova privatnosti, napadača i izvora podataka za napadače, dajući strukturu pojmu „pametna grad“ kako bi se identificirale prijetnje na privatnost i moguće odgovore na te prijetnje“. Autori su istražili nove standarde pametnih gradova u [9], međutim, zakonska regulativa nije pokrivena ovim člankom.

Prvi članak koji je spomenuo pojam i uveo taksonomiju usluga pametnih gradova pripremljen je od strane Benjelloun et al. [10] s fokusom na projekte vezane uz logistiku bez upliva u druga područja usluga pametnih gradova. U članku o novim taksonomijama projekata pametnih gradova [11], autori predlažu klasifikaciju uzimajući u obzir različite aspekte projekata pametnih gradova. Ujedno su identificirali ograničenu taksonomiju za ciljeve, alate i sudionike, ali ona nije prikladna za regulatorne aspekte koji su detaljno opisani u ovoj disertaciji. Rad koji je po temi najbliži istraživanju provednom u pripremi ove disertacije je pripremljen od strane EU inicijative Smart Cities Information System (SCIS)[12]. U dokumentu su opisani pojedinačni slučajevi scenarija „najlošije prakse“ koji su nastali zbog ograničenih lokalnih, regionalnih ili nacionalnih zakonskih regulativa koji mogu omesti uspješne projekte. Zbog toga je navedeni rad komplementaran sa zaključcima iz ove disertacije gdje se identificiraju općenita regulatorna pravila koja treba uzeti u obzir u ranim fazama projekata pametnih gradova.

Glavni doprinos ove disertacije je predložena taksonomija pametnih gradova koja identificira ključna tehnička i regulatorna obilježja usluga pametnih gradova. Na temelju predložene taksonomije napravljena je analiza reprezentativnih primjera stvarnih usluga pametnih gradova koji su odabrani zbog svoje dobre prihvaćenosti u stvarnom životu pametnih gradova i/ili zbog svojih zanimljivih tehničkih aspekata. Jedan od glavnih doprinosa je skup pravila regulatornih preporuka za svaku ulogu u lancu vrijednosti Interneta stvari. Preporuke se mogu koristiti kao pomoć dionicima tijekom procesa planiranja i dizajniranja rješenja pametnih gradova. Korištenjem ovih preporuka, dionici mogu jednostavno identificirati svoje

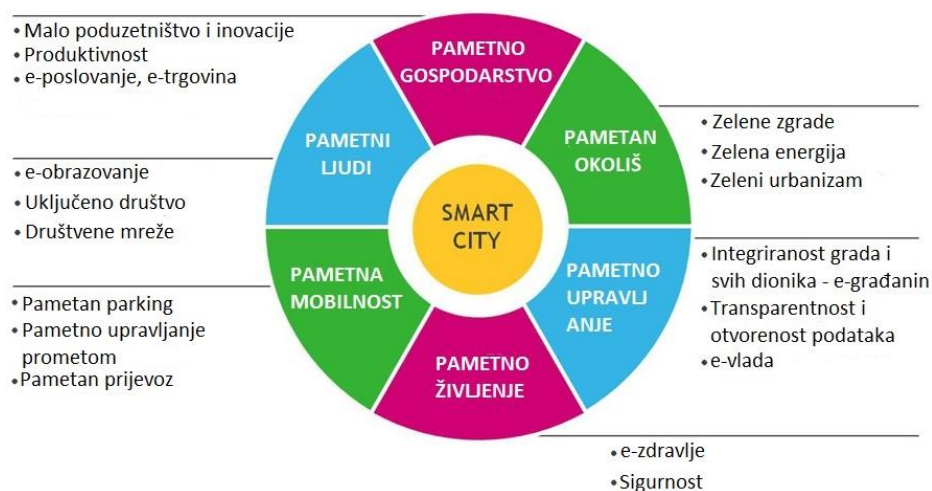
odgovornosti i fokusirati se samo na ključne aspekte i na taj način skratiti razvojni proces usluge.

Jedan od doprinosa su poslovni odnosi u lancu vrijednosti iz kojih je lako vidljivo tko ima ugovorne odnose s kim u lancu i tko je odgovoran za koji dio posla. Također, na temelju toga, može se vidjeti i u slučajevima kvarova, ispada ili povreda podataka (na primjer gubitka osobnih podataka), tko treba preuzeti odgovornost te tko je odgovoran kod mogućih tužbi. Za svaku ulogu u lancu vrijednosti dan je primjer poslovnog modela kroz tzv. „model platna poslovnog modela“. Pomoću ovoga dionici jednostavnije mogu odrediti s kime žele i trebaju imati međusobne odnose i ne moraju trošiti vrijeme na istraživanje. Uz to, dan je i konkretan prijedlog poslovnog modela za države male i srednje veličine koji na nacionalnoj razini predlaže platformu za usluge koje obuhvaćaju više sektora i više segmenata, poput usluga u cestovnom prometu, a koju gradovi mogu iskoristiti i za svoje potrebe i postavljenje svojih usluga. Tako bi gradovi mogli replicirati postojeće tehničko rješenje iz jednog grada na druge gradove i tako smanjiti troškove.

1. PAMETNI GRADOVI U KONTEKSTU INTERNETA STVARI

Gradovi diljem svijeta u zadnjih 10 godina ulažu značajne napore kako bi napravili potpunu transformaciju iz klasičnih gradova kakve poznajemo do takozvanih pametnih ili inteligentnih gradova, tj. gradova koji su samoodrživi i koji razumiju važnost infrastrukture. Takvi gradovi ulažu u infrastrukturu i tehnologiju kako bi poboljšali performance grada [13] jer je još od rimskog doba poznato da ulaganje u infrastrukturu (a u rimsko doba to su bile ceste) rezultira porastom globalnog bruto domaćeg proizvoda (BDP).

Uvođenjem novih infrastrukture i korištenjem IKT-a ovakvi gradovi postaju efikasniji, održivi i bliži svojim građanima jer poboljšavaju kvalitetu života u svim segmentima, odnosno gradovi uvođenjem IoT-a sve više postaju živi organizam koji može odgovoriti na potrebe svojih građana, ali može i sam sebe korigirati prema potrebi. Ovo se pogotovo može vidjeti kroz 6 kategorija na koje se gradske usluge mogu podijeliti, a to su područja interesa: gospodarstvo, ljudi, upravljanje, pokretljivost (mobilnost), okoliš i življenje [14].



Slika 6: Prikaz podjele pametnih gradova u 6 područja interesa

Na slici 6 prikazana je podjela pametnih gradova na 6 interesnih područja s različitim uslugama koje ta područja pokrivaju. Svako od interesnih područja pridonosi razvoju gradova,

bilo u infrastrukturnom, socijalnom, gospodarskom ili nekom drugom aspektu. Usluge pametnih gradova bit će objašnjenje i opisane u poglavlju 4.

1.1. Arhitektura Interneta stvari

Trenutačno ne postoji opće prihvaćena definicija Interneta stvari. Sama definicija još uvijek nije jasna te je najčešće predmet filozofskih rasprava. Naime, većina autora koji se bave ovim područjem imaju svoju definiciju koja se manje ili više razlikuje od drugih definicija. Sve navedeno dovelo je do situacije u kojoj umjesto jedne definicije postoje mnoge definicije. Neke od definicija koje se najčešće pojavljuju u stručnoj literaturi dane su u nastavku.

U osnovi, IoT se može definirati kao mreža objekata koji su u mogućnosti detektirati i izmjenjivati informacije između sebe, ali se navedena mreža razlikuje od Interneta u nekoliko drugih aspekata [1].

Šire prihvaćena je definicija ITU-a iz 2005., međutim ona je dosta općenita te glasi: IoT je globalna infrastruktura informacijskog društva, koja međupovezivanjem stvari (fizičkih i virtualnih) omogućava napredne usluge, a bazira se na postojećim i naprednim interoperabilnim uslugama IKT-a [1].

RFID grupa definira IoT kao svjetsku mrežu međusobno povezanih objekata, od kojih svaki posjeduje jedinstvenu adresu i komunicira putem standardnih komunikacijskih protokola [15].

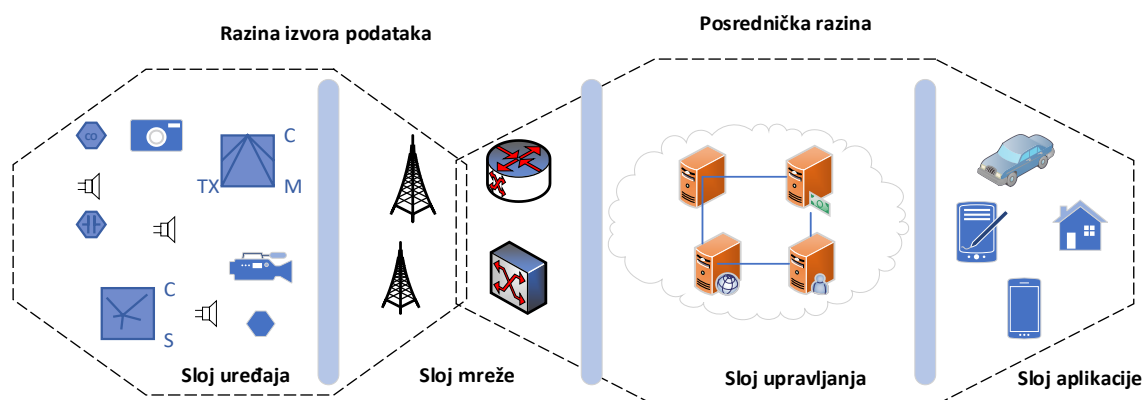
Svoje poimanje pametne okoline dao je i Forrester te ono glasi: Upotreba IKT-a kako bi se postigla veća svijest, interakcija i efikasnost komponenata kritične infrastrukture, usluga gradske administracije, obrazovanja, zdravstva, javne sigurnosti, transporta i uslužnih programa [16].

Europski klaster istraživačkih projekata vezanih uz IoT, IoT European Research Cluster (IERC), navodi kako je IoT integralni dio budućeg Interneta, a definira ga kao dinamičku globalnu mrežnu infrastrukturu s mogućnošću samo-konfiguracije, tj. mrežu koja se bazira na standardnim i interoperabilnim komunikacijskim protokolima, te mrežu u kojoj fizičke i virtualne „stvari“ imaju identitet, fizička obilježja i virtualne osobnosti, a također koriste inteligentna sučelja dok su istovremeno neprimjetno integrirane u informacijskoj mreži [17].

IERC daje i svoje viđenje pojma „stvari“ (Things) te ih definira kao aktivne dionike u poslovnim, informacijskim i društvenim procesima, pri čemu između „stvari“ te između „stvari“ i okoline postoji međudjelovanje i komunikacija. Navedeno međudjelovanje i

komunikacija se ogleda kroz izmjenu podataka i informacija koje su prikupljene iz okoline. Odgovarajući autonomno na stvarne/fizičke događaje iz okoline i njihov utjecaj na pokrenute procese, „stvari“ pokreću akcije i kreiraju usluge bez ili uz direktnu ljudsku intervenciju [17].

„Stvari“ se dodatno mogu definirati i kao stvarni/fizički ili digitalni/virtualni subjekti koji postoje i kreću se u vremenu i prostoru te se mogu identificirati. Stvari se obično identificiraju prema dodijeljenom identifikacijskom broju, imenu i/ili lokacijskoj adresi.



Slika 7: Pojednostavljeni prikaz arhitekture IoT-a

Slika 7. pokazuje pojednostavljenu arhitekturu Interneta stvari koja se sastoji od 4 sloja: uređaja, mreže, upravljanja i aplikacije.

Sloj uređaja sačinjavaju mreža postavljenih senzora i aktuatora, te njihova povezivost s mrežnim slojem. Ovo je ključan dio sustava Interneta stvari budući da se na ovoj razini generiraju podaci na kojima se IoT temelji. Glavna svrha senzora je prikupljanje podataka iz okoline, odnosno stvarnog svijeta. Postoje različite vrste senzora koji se koriste i upravo više-senzorski pristup je odlika IoT-a. Sensori su direktno ili indirektno povezani na IoT mrežu, a sam transportni mehanizam (I2C ili SPI) koji će se koristiti ovisi o aplikaciji. Navedeni transportni mehanizmi tvore komunikacijski kanal između senzora i aplikacije za prikupljanje podataka. Sami senzori se prema [18] mogu kategorizirati u 3 skupine: senzori pokreta, senzori okoline i lokacijski senzori.

Senzori pokreta bilježe promjene u pokretima i smjeru pokreta, senzori okoline bilježe svaku promjenu u parametrima okoline. To su senzori poput senzora svjetla, tlaka i koriste se za pomoć pri odlučivanju IoT sustava. Npr, kod automatizacije kuće paljenje i gašenje grijanja ovisi o temperaturi u kući. Lokacijski senzori se koriste za određivanje fizičke lokacije samog objekta i (koriste se) kod lokacijskih usluga, poput pametnog parkiranja ili zelenih ruta.

Mrežni sloj se koristi za povezivanje sloja uređaja i sloja upravljanja ili kao poveznica između dva uređaja. Način povezivanja ovisi o vrsti usluge i uređaja koji se koristi. Može biti žičano ili bežično, korištenjem WiFi-a, mobilnog prometa, Bluetootha, fizičkom žicom ili nekom drugom tehnologijom. Ova razina se brine o općenitim zahtjevima od uspostavljanja komunikacijskih veza do protokola. Budući da postoji veliki broj protokola ovaj sloj ih treba što više implementirati kako bi uređaji mogli komunicirati između sebe.

Sloj upravljanja se može gledati kao najbitniji sloj u IoT arhitekturi gdje se većina procesiranja i upravljanja događa. Svi podaci koje senzori šalju kad se stave u kontekst i značaj stvarnog svijeta nam daju sliku onog što se događa. Međutim, kada se ti podaci upare s naprednom analitikom može se vrlo točno predvidjeti budućnost. Upravo se to događa u ovom sloju: prikupljanje podataka, pročišćavanje, analiza i priprema za razumljivi prikaz. Ovi podaci su naposljetku dostupni na Internetu. Dakle, jednostavno rečeno ova razina je zadužena za odlučivanje i povezivost s kraja na kraj. Primjer pametne usluge u budućnosti može biti sljedeći. Vaš avion kojim se vraćate kući kasni i večera koju ste pripremili u pećnici bi trebala duže ostati ugrijana. Podaci o kašnjenju automatski alarmiraju vašu pećnicu koja produljuje vrijeme grijanja.

Na vrhu se nalazi sloj aplikacije ili prezentacije koji rezultate analize napravljene na sloju upravljanja prikazuje korisniku. Ovaj sloj je korisnički orijentiran i obavlja različite zadatke za korisnika. Korisnika ne zanima što se događa u pozadini već ga zanima završna informacija. Na prethodnom primjeru možemo vidjeti da korisnika ne bi zanimalo kako je pećnica došla do informacije o kašnjenju već ga samo zanima informacija da će pećnica duže ostati ugrijana. Danas već postoje brojne IoT aplikacije koje uključuju pametno parkiranje, pametnu kuću, pametan prijevoz, zdravlje i slično.

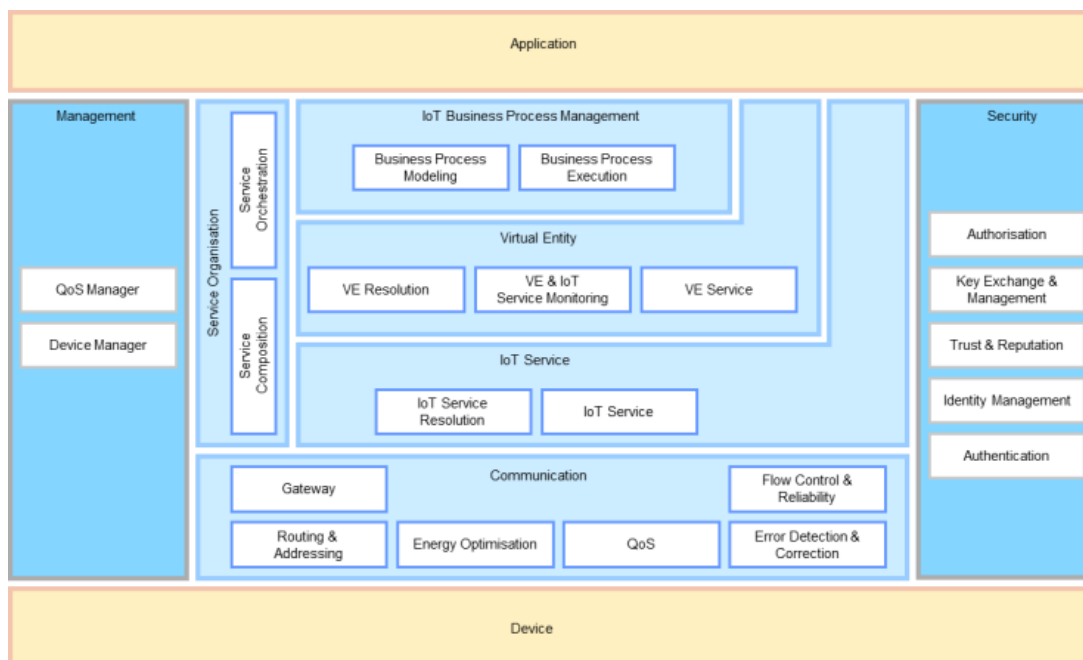
Unazad nekoliko godina razvijeni su referentni modeli i arhitekture koje predstavljaju generičke arhitekture IoT-a koje se mogu, ovisno o specifičnim potrebama projekata, prilagoditi. Dva takva modela su: IoT-A koji će se kasnije koristiti kao referentni model, te model predložen od svjetske telekomunikacijske zajednice (ITU) Y.2060.

1.1.1. IoT-A Referentni model

Slika 8 predstavlja Europski referentni model arhitekture Interneta stvari (IoT-A) [19][20] razvijen od strane više partnera unutar europskog istraživačkog projekta FP7. Referentni model IoT-A ima za cilj omogućiti korisnicima interoperabilnost različitih rješenja na komunikacijskom i uslužnom sloju.

Referentni model IoT-A omogućuje tvrtkama izradu svojih specifičnih arhitektura i rješenja, budući da referentni model opisuje glavne građevne blokove, te omogućuje izbor dizajna koji se može nositi s različitim specifičnim zahtjevima vezanim uz funkcionalnost, performanse, sigurnost i razvoj pojedinih aplikacija. Referentna arhitektura se može gledati kao matrica iz koje je moguće izvesti različite arhitekture ovisno o pojedinačnim zahtjevima. Kako bi to bilo moguće, treba postojati veliki skup svih mogućih funkcionalnosti, mehanizama i protokola koji će se koristiti za izradu pojedinačne arhitekture.

Referentna arhitektura IoT-A sastoji se od više slojeva, počevši od sloja uređaja, komunikacijskog sloja, preko upravljačkog sloja do aplikacijskog sloja. Po vertikalnoj osi proteže se upravljanje kvalitetom usluge te sigurnost.



Slika 8: Referentni model arhitekture Interneta stvari IoT-A

Sloj uređaja: služi za integraciju različitih uređaja, bez obzira na dobavljača i funkcionalnosti. Uređaji se tretiraju kao virtualni senzori povezani na platformu.

Komunikacijski sloj: daje skup metoda za povezivanje i komunikaciju uređaja koji koriste različite protokole. Osim toga komunikacijski sloj sadrži metode za usmjeravanje temeljene na sadržaju. Glavni zadatak je interoperabilnost različitih uređaja i premošćivanje razlika u protokolima.

Sloj usluge (engl. *IoT service*): sadrži podatke o svim uslugama. Ovaj sloj vraća opis usluge te daje poveznicu na sve resurse koje ta usluga koristi. Dodatna funkcionalnost ovog sloja je i obrada informacija te slanje obavijesti aplikacijama i uslugama vezanim uz resurse i fizičke objekte koje koriste.

Sloj virtualnog entiteta (engl. *virtual entity*): ova sloj održava i organizira informacije vezane uz fizičke objekte što omogućuje pretraživanje usluga prema resursima i njihovim povezanim fizičkim objektima. Također omogućuje pretragu usluga na temelju fizičkih objekata s kojima su povezane. Na upit o fizičkom objektu vraća adrese svih usluga koji su povezani s njime.

Sloj organizacije usluge (engl. *service organization*): je centralni sloj koji djeluje kao komunikacijski poveznik nekoliko slojeva. Koristi se za sastavljanje i orkestraciju usluga različitih razina apstrakcije. Ovaj sloj učinkovito povezuje upite s višeg sloja ili iz vanjskih aplikacija s jednostavnim uslugama koje IoT resursi omogućuju. Sloj organizacije usluge sastoji se od dvije funkcijske komponente. Jedna služi za sastavljanje, a druga za orkestraciju usluga. Usluga sastavljanja je centralni koncept arhitekture budući da IoT usluge često imaju ograničene funkcionalnosti zbog slabije računalne snage i životnog vijeka baterije IoT objekata. Komponenta sastavljanja usluge u takvim situacijama pomaže slaganju više različitih jednostavnih usluga kako bi odgovorila na pitanje dobiveno od višeg sloja apstrakcije, npr. povezivanjem usluge detekcije vlage s uslugom temperature može se dobiti usluga detekcije požara.

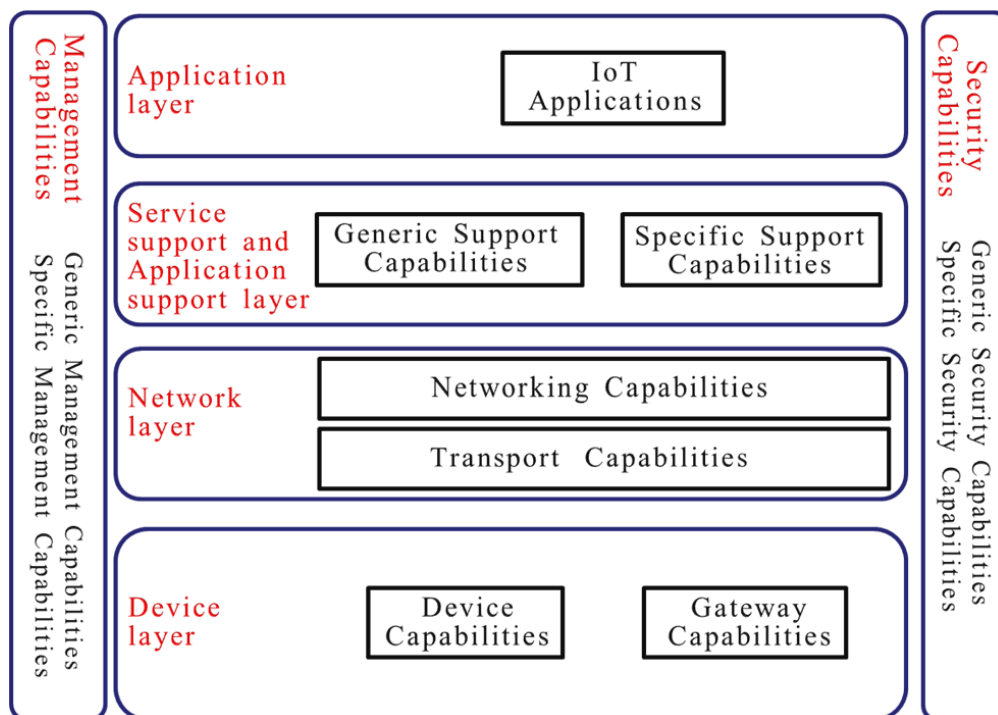
Sloj upravljanja IoT poslovnim procesima (engl. *IoT Business Process Management*): omogućuje integraciju tradicionalnih sustava, uobičajenih u poslovnom svijetu, za upravljanje poslovnim procesima s referentnim modelom IoT-A. Svrha ovog sloja je omogućiti funkcionalne koncepte i sučelja za povezivanje i proširivanje (obogaćivanje) tradicionalnih poslovnih procesa s posebnostima IoT svijeta. Na taj način kompanije mogu učinkovito iskoristiti IoT sustav, držeći se uobičajenih standarda i primjenjujući najbolju praksu, čime se izbjegavaju dodatna opterećenja i troškovi zbog korištenja izoliranih i vlasničkih rješenja u području Interneta stvari.

Sloj upravljanja (engl. *management layer*): je odgovoran za slaganje i praćenje svih akcija koje uključuju jedan ili više ostalih slojeva arhitekture. Primjer takve akcije je stavljanje IoT sustava u stanje spavanja radi uštede energije. Drugi primjer je interakcija između aplikacije i uređaja koja zahtjeva praćenje od strane barem dvije grupe.

Sigurnosni sloj (engl. *security layer*): odgovoran je za sigurnost i privatnost IoT sustava. Odrađuje inicijalnu registraciju klijenta prema mreži na siguran način, čime se osigurava da samo provjereni klijenti imaju pristup uslugama na IoT infrastrukturi. Osim toga ovaj sloj osigurava zaštitu privatnih korisničkih podataka putem funkcije anonimnosti (prilikom pristupa resursima i uslugama korisnički identitet ostaje anonim) i sposobnosti prekidanja veza (osigurava da korisnik može više puta koristiti resurse bez da napadač uspije uspostaviti vezu između tih korištenja). Sigurnosni sloj također osigurava komunikaciju između krajeva koji su statički autorizirani za međusobnu komunikaciju ili si međusobno vjeruju.

1.1.2. ITU-T Y.2060

IoT arhitektura ITU-a se temelji na slojevitom modelu (prikazano na slici 9.), pri čemu niži slojevi služe kao gradivni blokovi usluga višeg sloja te je stoga usporediva s prethodno prikazanom arhitekturom IoT-A. Četiri osnovna sloja u arhitekturi ITU-a obuhvaćaju: sloj uređaja koji se sastoji od sloja senzora i poveznica, mrežni sloj, upravljački sloj i aplikacijski sloj [21].



Slika 9: IoT referentni model Y.2060

Referentni model ITU-T Y.2060 [21] na slici 9 sastoji se od 4 sloja, te razina upravljačkih i sigurnosnih mogućnosti. Četiri razine od kojih se sastoji su:

- Aplikacijski sloj
- Sloj za podršku uslugama i aplikacijama
- Mrežni sloj
- Sloj uređaja

Aplikacijski sloj

Sadrži IoT aplikacije. Sve IoT aplikacije su smještene i rade na ovoj razini.

Sloj za podršku uslugama i aplikacijama

Ovaj sloj sastoji se od dvije grupe mogućnosti i olakšava rad aplikacijama dajući mi zajedničke resurse koje mogu koristiti sve IoT aplikacije:

- Opće mogućnosti podrške
Opće mogućnosti podrške su zajedničke mogućnosti koje se mogu koristiti od strane različitih IoT aplikacija, kao što je na primjer obrada podataka ili pohrana podataka. Ove mogućnosti mogu biti pozvane i korištene i od strane posebnih mogućnosti podrške, na primjer, za izradu drugih posebnih mogućnosti podrške.
- Posebne mogućnosti podrške
Posebne mogućnosti podrške su određene mogućnosti koje zadovoljavaju zahtjeve raznolikih aplikacija. Mogu se sastojati od različitih grupa s detaljnim mogućnostima kako bi omogućile različite funkcijske podrške različitim aplikacijama za Internet stvari.

Mrežni sloj

Mrežni sloj odgovoran je za funkcije povezivosti, a sastoji se od dva dijela: mrežnih i transportnih sposobnosti koje su svojevrsna spona između aplikacija i usluga, te se koristi za prijenos podataka i identificiranje uređaja i korisnika.

Mrežne sposobnosti pružaju odgovarajuće kontrolne funkcije mrežnog povezivanja, kao što su funkcijske kontrole pristupnih i transportnih resursa, upravljanje mobilnošću ili provjera autentičnosti, autorizacija i provjera korisnika (AAA).

Transportne sposobnosti usredotočene su na pružanje usluge povezivosti za prijenos specifičnih podataka IoT usluga i aplikacija, kao i za prijenos informacija vezanih za kontrolu i upravljanje internetom.

Sloj Uređaja

Sloj uređaja se logički može podijeliti u dvije skupine: sposobnosti uređaja i sposobnosti prilaznog uređaja.

Sposobnosti uređaja uključuju direktnu interakciju s komunikacijskom mrežom. To znači da su uređaji u mogućnosti prikupljati i dostavljati informacije direktno (bez potrebe prilaznog uređaja) komunikacijskoj mreži. Također, od nje mogu direktno i primati informacije (na primjer, naredbe). Isto tako, uređaji indirektnom komunikacijom, korištenjem prilaznog uređaja, mogu prikupljati i dostavljati te primati informacije od komunikacijske mreže.

Uređaji imaju i sposobnost izrade ad-hoc mreža u scenarijima gdje je potrebna veća skalabilnost i brzo uvođenje usluge.

Uređaji zbog uštede električne energije imaju i mogućnost „spavanja i buđenja“ što znači da mogu podržati mehanizme za uštedu energije na način da se uređaj u trenucima kada nije aktivan pošalje na „spavanje“ te se sve periferne jedinice u tom trenutku isključuju, a takt se smanjuje čime se dovodi do uštede energije.

Prilazni uređaj ima mogućnost podrške višestrukog sučelja što znači da dopušta povezivanje uređaja preko više različitih žičanih ili bežičnih tehnologija, kao što su CAN sabirnica, WiFi, ZigBee ili Bluetooth. Na mrežnom sloju prilazni uređaj može komunicirati s različitim tehnologijama kao što su javna telefonska govorna mreža (PSTN), pokretna mreža treće ili četvrte generacije, LTE, Ethernet i DSL.

Osim toga prilazni uređaj ima sposobnosti konverzije protokola koje su potrebne u dvije situacije. Jedna je kada uređaji koriste različite komunikacijske protokole, na primjer jedan koristi ZigBee, a drugi Bluetooth, a druga je za kod komunikacije između sloja uređaja i mrežnog sloja koji koriste različite protokole. Na primjer, uređaj koristi protokol ZigBee, a na mrežnom sloju se koriste protokole 3G tehnologije.

Sposobnosti upravljanja

Na sličan način kao što se to radi u tradicionalnim komunikacijskim mrežama tako i kod IoT-a sposobnost upravljanja pokriva tradicionalne pogreške, konfiguracije, performanse i sigurnosne klase.

Sposobnost upravljanja kod IoT-a može se kategorizirati u općenite i specifične sposobnosti upravljanja od kojih općenite sposobnosti upravljanja pokrivaju upravljanje uređajima poput udaljene aktivacije ili deaktivacije, dijagnostike, statusnih informacija ili osvježavanja softvera. Osim toga nudi i upravljanje topologijom lokalne mreže, te upravljanje prometom i zagušenjima.

Specifične sposobnosti su više vezane uz specifične zahtjeve pojedinih aplikacija. Na primjer, zahtjev za nadgledanjem visokonaponskih vodova kod Smart Grid usluge.

Sposobnosti sigurnosti

Kao i kod sposobnosti upravljanja i ove su podijeljene u dvije kategorije općih i specifičnih sigurnosnih sposobnosti i protežu se kroz sva četiri sloja. Opći su neovisni od aplikacija i uključuju:

- Na aplikacijskom sloju: autorizaciju, autentikaciju, zaštitu povjerljivosti i cjelovitosti podataka aplikacije, zaštitu privatnosti i anti-virus.
- Na mrežnom sloju: autorizaciju, autentikaciju, povjerljivost signalizacijskih i korištenih podataka i zaštitu cjelovitosti signalizacije.
- Na sloju uređaja: autorizaciju, autentikaciju, provjeru cjelovitosti uređaja, kontrolu pristupa, zaštitu povjerljivosti i cjelovitosti podataka.

Specifične sposobnosti sigurnosti su vezane uz zahtjeve pojedinih aplikacija, na primjer sigurnosni zahtjevi za mobilno plaćanje.

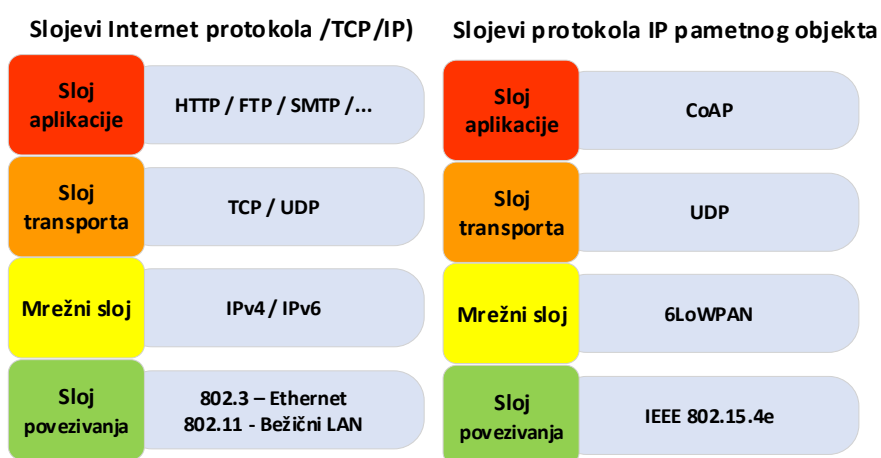
1.2. Protokoli Interneta stvari

Protokoli spadaju u jednu od ključnih komponenata IoT sustava. Upravo jedan od razloga zašto je razvoj IoT-a i M2M-a otežan je velik broj raznolikih komunikacijskih protokola koji se koriste u današnjoj industriji kao što su industrijski protokol za dobivanje podataka sa senzora, komunikacijski protokol za slanje tih podataka na poslužitelj u oblaku te protokol za

udaljeno upravljanje uređajima koji omogućuju udaljenu promjenu softvera. Osim toga, vlastiti IoT protokoli su često vezani uz poslovne modele. Ponekad zbog toga nisu cjeloviti jer podržavaju samo postojeće poslovne modele i rješenja. S druge strane neka rješenja su preglomazna zbog čega traže velike zahtjeve koje mali senzori ne mogu ispuniti.

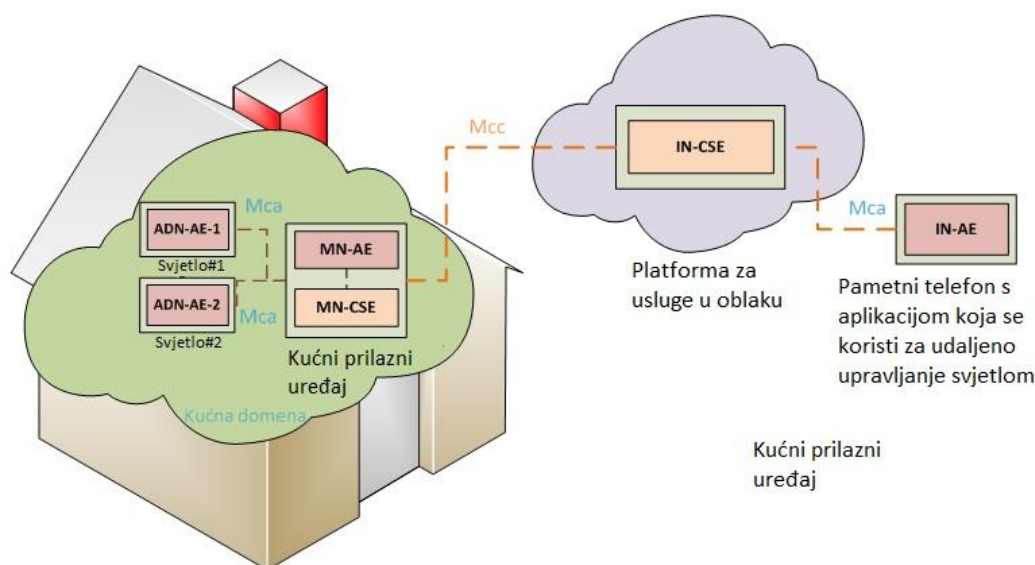
S aspekta regulacije tržišta potrebni su otvoreni, standardizirani protokoli koji će omogućiti povezivanje svih dijelova sustava u jednu cjelinu uz davanje najboljih mogućih funkcionalnosti i performansi sustavu.

Slika 10 prikazuje usporedni protokolni složaj za običan Internet promet i kod IoT objekata.



Slika 10: Usporedni prikaz tradicionalnih i IoT protokola [22]

Protokoli koji su se najviše izdvojili po broju implementacija i otvorenosti su MQTT i COAP. OneM2M je pokrenut 2012. godine kao globalna inicijativa koja bi trebala osigurati najefikasnije uvođenje M2M komunikacijskih sustava i Interneta stvari. Cilj oneM2M-a je priprema tehničkih specifikacija za općeniti sloj M2M usluga koji se može ugraditi u različite hardvere i softvere kako bi povezali širok spektar uređaja diljem svijeta s M2M aplikacijskim poslužiteljima.

Slika 11: Funkcijska arhitektura oneM2M-a⁵

Kod funkcijske arhitekture oneM2M-a definirana su dva osnovna tipa entiteta. Jedan je AE (engl. Application entity, hrv. Aplikacijski entitet), a drugi je CSE (engl. Common Service Entity, hrv. Entitet opće usluge). U primjeru iz slike 11 svjetla i pametni telefon predstavljaju AE entitet. U oblaku je smješten IN-CSE (engl. Infrastructure node CSE, hrv. Infrastrukturni čvor CSE) kod oneM2M2 pružatelja usluge, dok je MN-CSE (engl. Middle Node CSE, hrv. Središnji čvor CSE-a) smješten u kućnom preklopniku. OneM2M je definirao dvije referentne točke Mca i Mcc. Prva služi kao sučelje između AE i CSE, dok je druga sučelje između CSE čvorova. U primjeru sa slike 11, pametni telefon kontrolira svjetla 1 i 2 na način da IN-AE (aplikacijski čvor u pametnom telefonu) komunicira direktno s platformom u oblaku gdje je smješten IN-CSE preko sučelja Mca, te kroz sučelje Mcc upravlja sa svjetlima kroz MN-CSE koji je povezan sučeljem Mca sa svjetlom.

Uz MQTT i COAP značajniji IoT protokoli su XMPP, RESTfull HTTP i AMQP.

MQTT (*Message Queuing Telemetry Transport*) [23] je dizajniran za povezivanje fizičkih objekata i mreža s aplikacijama. Cilj mu je prikupiti podatke s različitih fizičkih uređaja i prenijeti ih do IT infrastrukture. Ciljana skupina su velike mreže malih uređaja koje treba nadgledati i kontrolirati iz oblaka. Predstavlja jednostavan protokol koji se temelji na modelu interakcije objavi-pretplati. Zbog svojih obilježja poput male veličine, malen procesorske

⁵ <http://www.onem2m.org/application-developer-guide/architecture>

snage, minimalnih podatkovnih paketa, te učinkovitog usmjeravanja informacija (paketa) prema jednom ili više prijemnika idealan je za IoT usluge.

COAP (*Constrained Application Protocol*) [24] je protokol predviđen za rad s čvorovima i mrežama s ograničenim resursima, a po funkcionalnosti je usporediv s protokolom HTTP. COAP paketi su puno manji od HTTP paketa, te su jednostavni za pripremu dok njihovo raščlanjivanje ne zahtjeva previše radne memorije kod uređaja s malom procesnom snagom i memorijom. Koristi transportni protokol UDP, a ponavljanje i preslagivanje datagrama je implementirano na aplikacijskom sloju.

XMPP (*Extensible Messaging and Presence Protocol*) [25] je protokol definiran još u doba kada IoT nije postojao, a koristio se primarno za izmjenjivanje poruka i informacija o prisutnosti. Proširen je na signalizaciju za VoIP, objavljivanje sadržaja i usmjeravanje XML podataka. Jedan je od kandidata za upravljanje potrošačkom bijelom tehnikom poput perilica, sušilica i hladnjaka. Nije praktičan za mreže lošije kvalitete budući da zahtjeva stalnu TCP vezu i ne sadrži efikasno binarno kodiranje.

RESTful HTTP [24] koristi TCP i posebno je zanimljiv za povezivanje potrošačkih kućnih uređaja, poput pametnih telefona i tableta, budući da omogućava gotovo potpunu implementaciju HTTP stoga dostupnu na različitim platformama koje se mogu povezati na Internet i otvarati web-stranicu. Uspješno se koristi kod manjih mreža lošije kvalitete i manje snage gdje se zahtijevaju poruke s kašnjenjem od nekoliko sekundi (npr. upravljanje potrošnjom energije u pametnim kućama).

AMQP (*Advanced Message Queuing Protocol*) [26] je otvoreni standard za izmjenjivanje poslovnih poruka između aplikacija ili organizacija. Kod AMQP protokola sve je vezano uz rep poruka. AMQP šalje transakcijske poruke između poslužitelja. Budući da je potekao iz bankarske industrije, može pouzdano obraditi na tisuće transakcija u repu. Za komunikaciju koristi TCP što mu omogućava pouzdanu vezu od točke do točke. Kao osiguranje, svaka primljena poruka mora se potvrditi. AMQP je fokusiran na praćenje svih poruka i osiguranje njihove isporuke bez obzira na greške. Za primjenu u području Interneta stvari AMQP je najprikladniji za razinu upravljanja, odnosno, IoT platforme.

1.3. Koncept i arhitektura pametnih gradova

Ubrzani porast broja stanovništva u gradovima zahtjeva prilagodbu gradova u svakom pogledu, od infrastrukturnih promjena do načina upravljanja gradovima. Takve potrebe

potaknule su razvoj novih tehnoloških rješenja koja su primjenu pronašla u širem urbanom ekosustavu gdje se kroz digitalnu povezivost različitih segmenata i usluga u gradu omogućuje lakše i učinkovitije upravljanje tim istim uslugama. Razvojem naprednih usluga i sam život u gradu postaje lakši. Samo neka od područja koje donose značajne uštede i podižu kvalitetu života su:

- **Energija:** postavljanjem senzora i izgradnjom naprednih ICT mreža, te korištenjem napredne analitike grade se pametne energetske mreže koje pomažu energetskim distributerima da efikasnije upravljaju potražnjom i ponudom, te omoguće efikasnije korištenje energije korištenjem inteligentnih distribucijskih sustava.
- **Voda:** pametno upravljanje vodom daje holistički pogled na sustave voda i otpadnih voda, te zahvaljujući nizu senzora postavljenih kroz sustave cijevi vizualizira podatke o potrošnji, kvaliteti, protoku, tlaku i drugim naprednim parametrima. Senzori daju podatke u stvarnom vremenu, a napredna analitika podataka prati i daje izvještaje o stanju sustava i omogućuje učinkovito upravljanje sustavom voda.
- **Promet:** za većinu gradova vrlo je teško ili gotovo nemoguće graditi nove ceste, željeznice ili luke te stoga mnogi gradovi povećavaju prometne kapacitete upotrebom senzora i lokacijskih tehnologija u prometnoj infrastrukturi. Dobivenim podacima i upotrebom napredne analitike u stvarnom vremenu smanjuju se gužve i vrijeme prijevoza, a konačan cilj je izrada inteligentnog transportnog sustava kroz sve segmente prometa.
- **Ljudi i socijalni programi:** različita rješenja u ovom području omogućuju ljudima ostvarenje kvalitetnijih životnih ciljeva, kao izradu usluga koje će ostvarivati bolje rezultate, a gdje će građanin biti u središtu. To su usluge poput socijalne pomoći, obiteljskih usluga, usluge zapošljavanja ili usluge pomoći ljudima s invaliditetom.
- **Zdravstvo:** prema IBM-u [27] u 2010. godini 30% svih računalnih podataka predstavljale su medicinske slike koje nisu bile povezane s pametnim sustavima. Upravo tu je vidljivo da zdravstveni sustavi trebaju biti povezani i inteligentni, a cilj je da se korištenjem tehnologije doprinese naprednijem sustavu zdravstvene zaštite i omoguće bolje i točnije dijagnoze, olakša liječnicima

tretiranje bolesti, olakša pronalazak novih načina liječenja različitih bolesti, a ljudima olakša donošenje mudrijih odluka vezanih uz njihovo zdravlje.

- **Obrazovanje:** aplikacije napredne analitike obrazovanja omogućavaju različita rješenja koja pomažu pri učenju i predavanjima izvan učionice. Izazov ovakvog sustava je kako nadgledati rezultate učenika i osmisliti nove inovativne metode učenja kako bi se povećali sami rezultati učenja.

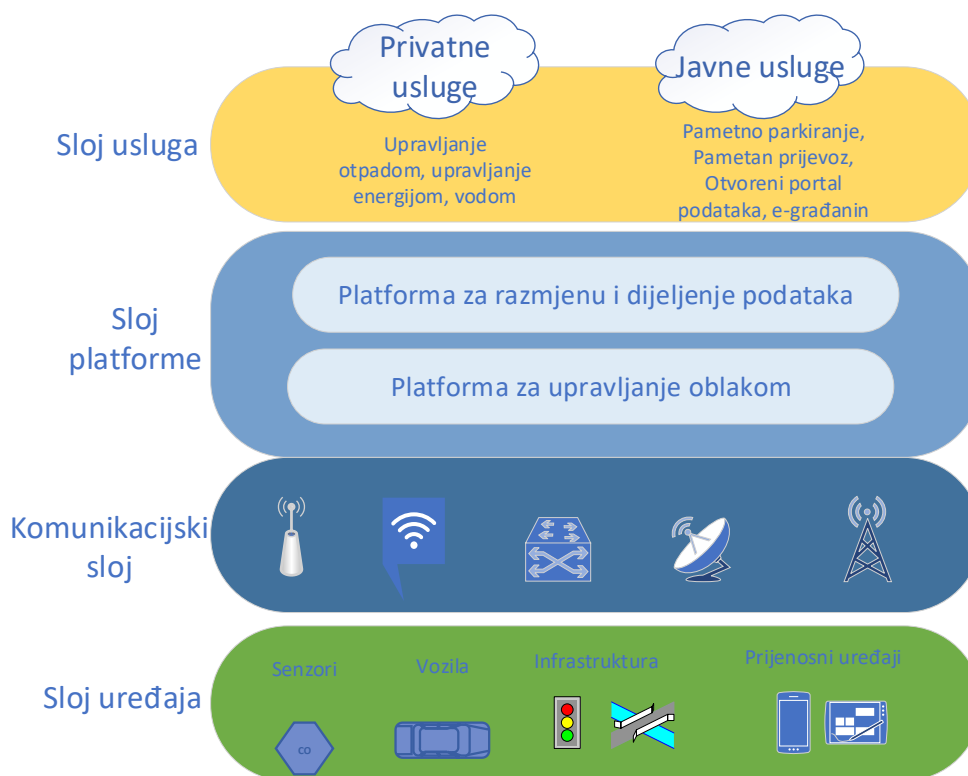
Definicija pametnog grada mora pokriti navedena područja korištenjem naprednih IKT tehnologija. Pretraživanjem na internetu moguće je pronaći različite definicije pametnog grada, međutim, definicije standardizacijskih tijela mogu se prepoznati kao najpreciznije pa je tako posebna radna skupina ITU-T-a koja se bavi pametnim gradovima napravila analizu preko 100 definicija pametnih gradova kako bi predložila sljedeću definiciju:

“Pametan samoodrživ grad je inovativan grad koji koristi IKT i druga sredstva kako bi unaprijedio kvalitetu života ljudi, efikasnost gradskih službi i usluga te konkurentnost, istodobno osiguravajući gospodarske, socijalne i aspekte okoliša za potrebe sadašnjih i budućih naraštaja.“ [28]

Od brojnih drugih definicija koje se mogu pronaći, treba još istaknuti dvije definicije. Jednu je definirao Američki ured za promet, a drugu standardizacijsko tijelo ISO. Te dvije definicije uz ITU-ovu se mogu smatrati kao najcjelovitije, odnosno, najbolje opisuju pametan grad. Definicija Ureda za promet Sjedinjenih Američkih Država povezuje pametan i povezan grad u definiciji i kaže da je „pametan grad onaj gdje gradska uprava i građani koriste najbolja moguća sredstva, uključujući i IKT, kako bi postigli svoje zajedničke ciljeve. To najčešće uključuje gospodarski razvoj, održivost okoliša i unaprjeđenje kvalitete života za građane. Povezani grad je onaj u kojem su svi važni gradski sustavi, poput prometa, komunalnih sustava, zapošljavanja, zdravstva, sigurnosti i obrazovanja sposobni međusobno komunicirati kako bi se koordinirali i smanjili otpad.“ [29]

S druge strane standardizacijsko tijelo ISO pametan grad prepoznaje kao „onaj koji dramatično povećava tempo kojim poboljšava svoje socijalno ekonomske ishode i ishode održivosti okoliša, odgovarajući na izazove poput promjene klime, povećanje populacije i političke i gospodarske nestabilnosti..., temeljito poboljšavajući angažman društva, primjenu metoda suradničkog vodstva, funkcioniranje gradskih sustava te upotrebu podataka i moderne tehnologije..., a sve s ciljem pružanja bolje usluge i kvalitete života onih koji žive ili su

uključeni u funkcioniranje grada (stanovnici, poduzeća, posjetitelji) sada i u predvidivoj budućnosti bez nepravdnog ugrožavanja drugih i degradacije prirodnog okoliša.“ [30]



Slika 12: Pojednostavljena arhitektura pametnih gradova

Na slici 12 prikazana je pojednostavljena arhitekturu pametnih gradova koja se sastoji od 4 sloja, sloja uređaja, komunikacijskog sloja, sloj platforme i sloja usluga. Sloj uređaja je najniži sloj i predstavlja uređaje iz fizičkog svijeta. Komunikacijski sloj služi za povezivanje, odnosno, prijenos podataka očitanih sa senzora prema poslužiteljima (obično u oblaku) gdje se radi analitika. Sloj platforme predstavlja pamet usluga pametnih gradova. Podijeljena je u dva dijela jedan dio koji je zadužen za razmjenu podataka i drugi dio koji služi za upravljanje uređajima i infrastrukturom, odnosno, raspolaže i upravlja resursima potrebnim za pojedine aplikacije. Na vrhu se nalazi sloj usluge koji vrši prezentaciju same usluge krajnjim korisnicima. Kao što se može vidjeti na slici kod pametnih gradova IKT je isprepletena s tradicionalnom infrastrukturom. IKT ima ključnu ulogu kod pametnih gradova jer između ostalog djeluje i kao platforma za prikupljanje informacija i podataka koji omogućuju bolje razumijevanje načina na koji grad troši resurse i usluge za svoje poslovanje. Na slici 12 mogu se vidjeti dva skupa usluga, jedan su privatne usluge, a drugi su javne. Privatne usluge predstavljaju usluge koje su financirane privatnim sredstvima i ne moraju u potpunosti biti

dostupne javnosti. S druge strane javne usluge su potpuno otvorene i financirane su javnim novcem. Transformacija postojećih gradskih usluga upotrebom IKT-a omogućuje: kvalitetniju energetska učinkovitost, učinkovitiji i transparentniji rad gradske infrastrukture, kvalitetnije cestovne mreže, efikasniji sustav distribucije vode, kvalitetnije upravljanje otpadnim vodama, povećanu sigurnost i brojne druge usluge.

Senzori postavljeni u gradovima omogućavaju gradskim čelnicima pristup prostornim, ekonomskim i informacijama o okolišu u njihovom gradu u stvarnom vremenu. Na taj način, IKT nije zadužena samo za uspostavu definiranih funkcija nego i za bolju povezivost i komunikaciju između građana, uprave, privatnih dionika i ostalih zainteresiranih strana u izradi i planiranju gradskih procesa. Kako bi definirali pametan grad na njega moramo gledati s aspekta cjeline koja stavlja naglasak na međupovezanost i razvoj sljedećih 6 elemenata sukladno slici 6:

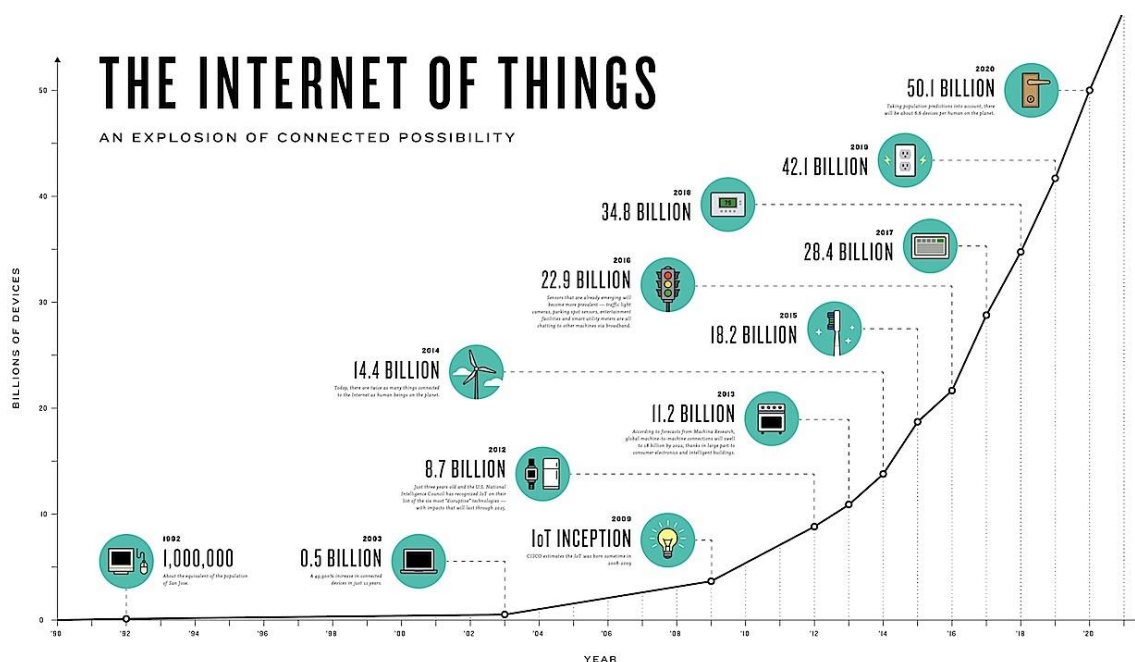
- Pametno gospodarstvo: naglasak pametnih gradova je na e-poslovanju i e-trgovini, povećanoj produktivnosti i inovativnosti kroz korištenje IKT-a;
- Pametni ljudi: naglasak je na građanima koji žive i rade u gradu. Građani žele jednostavnost pristupa usluzi, žele biti informirani o funkcioniranju grada, trošenju sredstava te sudjelovati u donošenju odluka;
- Pametno upravljanje: odnosi se na prakse koje vode učinkovitijem upravljanju gradovima, poput optimizacije procesa, poslovne inteligencije, optimizacije ljudskih potencijala i slično. Za to je potrebno osigurati integriranost grada sa svim ključnim dionicima;
- Pametna mobilnost: neizostavan dio svakog grada je i mobilnost u različitim oblicima. Ona se može optimizirati upotrebom IKT-a kroz usluge pametnog parkiranja, identifikacije problema u prometu u stvarnom vremenu, itd. Najznačajnije usluge se odnose na transportne i logističke usluge koje koriste IKT.
- Pametan okoliš: zaštita okoliša korištenjem IKT-a jedan je od ključnih segmenata gradova za dugoročnu održivost grada. To su usluge poput praćenja i smanjenja razine raznih vrsta onečišćenja u gradu, primjerice kvalitete zraka. Tu se ubrajaju i obnovljivi izvori energije, energetske mreže temeljene na IKT-u, pametno mjerenje, zelene zgrade, planiranje zelenih površina. Dobar primjer su i usluge poput pametne ulične rasvjete, upravljanja otpadom, odvodnih sustava i sustava vode.

- Pametno življenje: odnosi se na održivi način života vezan uz usluge koje omogućava IKT. Također se odnosi i na zdravo i sigurno življenje u ubrzanom gradu s različitim kulturološkim sadržajima.

1.4. Ekonomski potencijal pametnih gradova

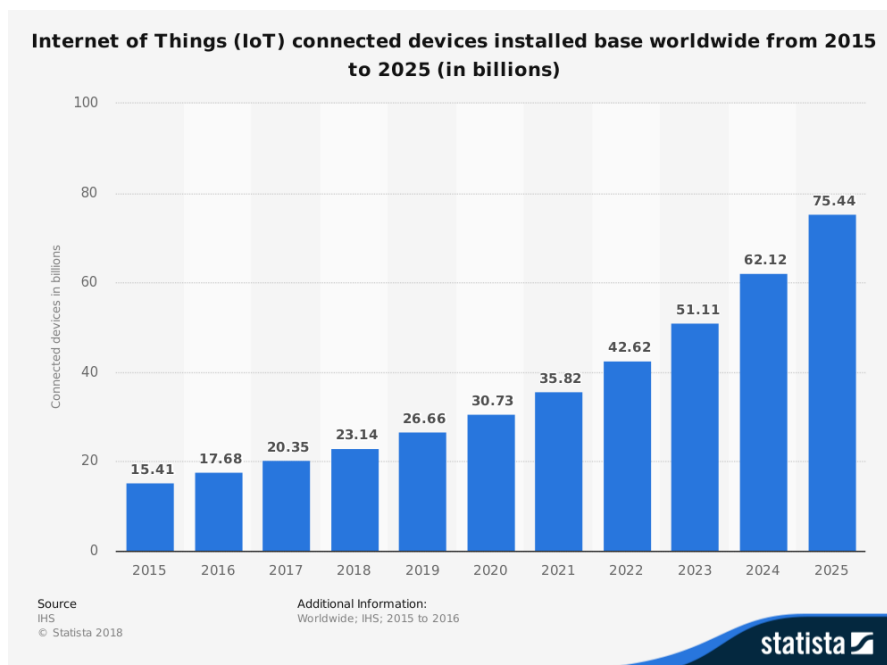
Potencijal ekonomskog iskorištavanja i primjene IoT-a uočio je časopis „The Economist“ na temelju istraživanja iz lipnja 2013. godine kada je ispitano mišljenje 779 poslovnih stručnjaka kako bi se definirao poslovni indeks IoT-a. Rezultat je pokazao da tri četvrtine kompanija ili aktivno istražuje ili koristi IoT, a 96% njih je navelo da će u sljedeće 3 godine koristiti IoT u nekom obliku. Procjena potencijalnog rasta IoT tržišta u sljedećih nekoliko godina varira i po broju povezanih uređaja i po ekonomskom rastu tržišta. Tako je, na primjer, Gartner procijenio da će do 2020. biti 30 milijardi uređaja povezanih na Internet s jednoznačnom IP adresom, što bi predstavljalo dodatnih 1,9 bilijuna (10^{12}) US dolara za svjetsko gospodarstvo [31]. Cisco i Ericsson su u isto vrijeme predvidjeli da će do 2020. ta brojka dosegnuti iznos od 50 milijardi [32][33] povezanih objekata na Internet, što će donijeti 14 milijardi US dolara svjetskom gospodarstvu. Slika 13 prikazuje broj povezanih uređaja na Internet do 2020. godine prema Ciscovom predviđanju, a slika 14 prema istraživanju Statista iz 2018. godine. Kasnija predviđanja ipak pokazuju konzervativnije brojke, odnosno smanjuju broj povezanih uređaja. Za usporedbu značaja vrijednosti taj iznos je veći od ukupnog BDP-a 17 zemalja članica EU 2011. godine [34]. Također, IDC je u listopadu 2013. godine predvidio da će do 2020. biti 212 milijardi „objekata“ što bi predstavljalo 8,9 bilijuna dolara godišnje s godišnjim rastom od 7,9% [35].

Jedan od značajnih segmenata IoT-a svakako otpada na tržište pametnih gradova koje kontinuirano raste i svaki daljnji razvoj gradova je teško zamisliv bez uporabe Interneta stvari. Tržište pametnih gradova raste velikom brzinom i iako su procjene različite svi se slažu da će vrijednost tržišta prijeći 1 bilijun US dolara 2020. godine.



Slika 13: Broj povezanih uređaja na Internet do 2020. godine⁶

Tako prema Grand View Research-u svjetsko tržište pametnih gradova bi do 2025. godine trebalo doseći vrijednost od 2.57 bilijuna US dolara s godišnjom stopom rasta od 18.4% u predviđenom periodu [36].

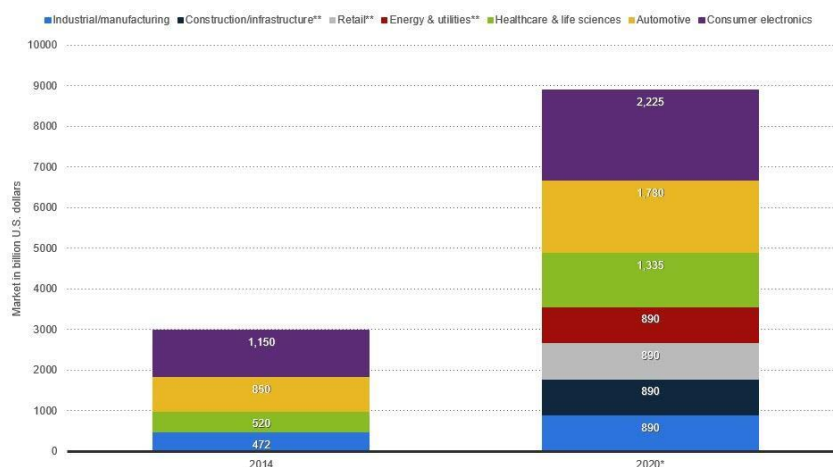


Slika 14: Broj instaliranih povezanih uređaja

⁶ Cisco Internet of Things Infographic (2016)

Najčešći razlog porasta broja rješenja za pametne gradove je vođen povećanjem broja stanovnika, potrebom za boljim upravljanjem limitiranim nacionalnim resursima, te stavljanjem fokusa na održivi okoliš. Brojni su zahtjevi postavljeni na tržištu poput unaprjeđenja pokretljivosti, pametne zgrade i kuće, optimalno iskorištavanje električne energije, ali i kvalitetnije i efikasnije administrativne usluge. Tržište će također profitirati od inicijativa pokrenutih od strane lokalnih i regionalnih vlada, stanovnika i lokalnih poduzeća koja će implementirati rješenja za probleme njihovih sredina. Prema sličnome istraživanju Forbesa, kombinirano tržište pametnih gradova je procijenjeno na 1,5 trilijuna US dolara što pokriva segmente energije, transporta, zdravlja, zgrada, infrastrukture i uprave (slika 15). Kada se to usporedi s BDP-om država u 2014. godini ovaj iznos se nalazi iznad BDP-a Španjolske što bi ga činilo 12. BDP u svijetu [37]. Prema istome istraživanju u 2025. godini se očekuje 25 pametnih gradova koji su ispunili više od 5 uvjeta da budu pametni gradovi od kojih će 50% biti iz Europe i sjeverne Amerike. Od gradova Amsterdam slovi kao najperspektivniji pametan grad u budućnosti. Međutim, bez obzira na potencijal, izazovi u pronalaženju izvora financiranja i pravog poslovnog modela za razvoj gradova su veliki, budući da većina gradova nema mogućnost za projekte velikih razmjera što rješenja pametnih gradova zasigurno jesu.

Size of the Internet of Things market worldwide in 2014 and 2020, by industry (in billion U.S. dollars)

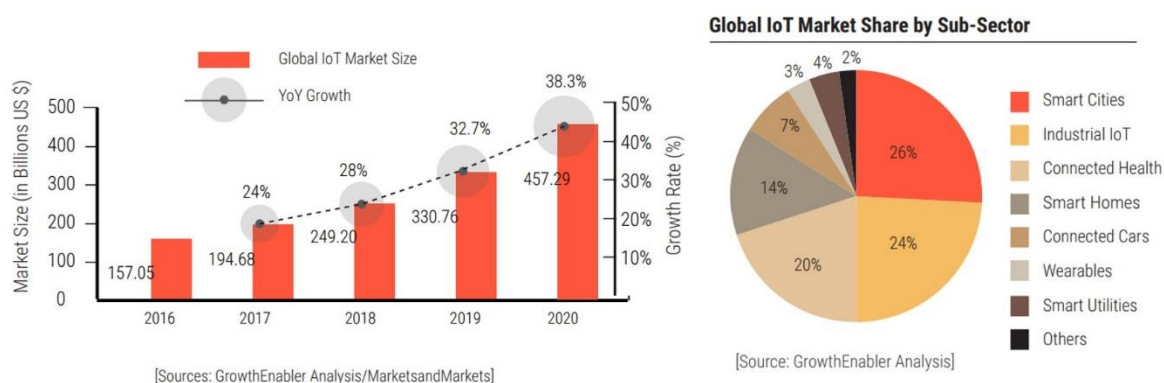


Slika 15: Tržišni potencijal prema Statistici⁷

⁷ Louis Columbus, 2017 Roundup Of Internet Of Things Forecasts, Forbes

Svakako treba istaknuti podatak od Frost & Sullivana kao jedne od najutjecajnijih konzultantskih kuća i njihovu procjenu da će tržište pametnih gradova 2025. godine biti vrijedno 1,56 bilijuna US dolara od čega će na pametan transport otpadati 423 milijuna US dolara. Najveći godišnji porast imati će sektor energije sa stopom od 28.7%, a najviše će ulagati područja Europe i Sjeverne Amerike.

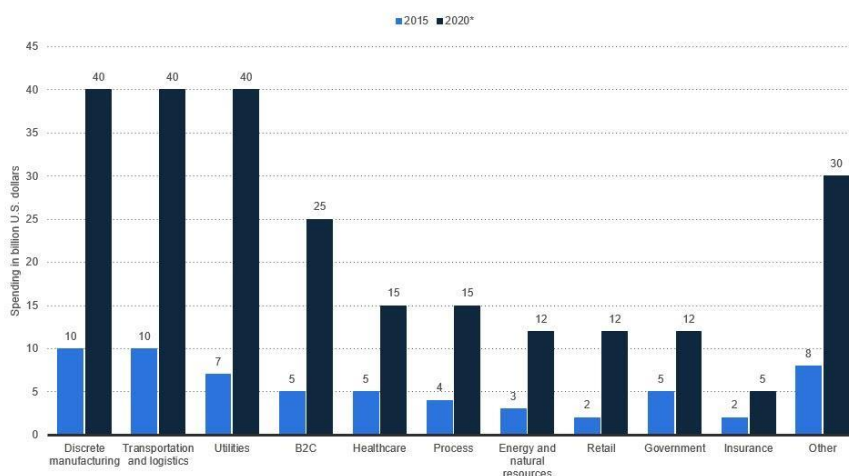
Zanimljivi su i podaci Europske komisije prema kojima do 2020. godine svjetsko tržište pametnih gradova će vrijediti 1.3 bilijuna US dolara što predstavlja veliki potencijal za europske tvrtke [38]. Vezano uz Europsku komisiju važno je istaknuti da će se prema njima, a prema regulaciji ERDF-a, svake godine uložiti oko 16 milijuna US dolara u razvoj pametnih gradova u periodu od 2014. do 2020. godine.



Slika 16: Udjel pojedinih segmenata IoT-a na tržištu

Internet of Things spending worldwide by vertical 2015 and 2020

Spending on Internet of Things worldwide by vertical in 2015 and 2020 (in billion U.S. dollars)



Slika 17: Potencijal tržišta prema područjima²

Slika 16 prikazuje još jedno istraživanje potencijala pametnih gradova gdje je prikazan postotni udjel pojedinih segmenata IoT-a na tržištu, dok se na slici 17 prikazuje potencijal tržišta prema područjima prema istraživanju Statiste.

1.5. Ekosustav usluga pametnih gradova

Pametni gradovi, kao potpuno novi koncept, predstavljaju mnogo više od samog korištenja tehnologije u svrhu olakšavanja uvođenja novih gradskih usluga. Oni više predstavljaju cjelokupnu strategiju specifičnu za svaki grad koja jasno definira gradske strateške ciljeve i definira praktičan vodič kako postići te ciljeve. Pametni gradovi zahtijevaju potpuno novi pristup upravljanju infrastrukturom i uslugama, kao i nove komunikacijske mehanizme prema svojim građanima. Treba postaviti kontinuirani i iterativni proces kako bi se identificirale, razmjestile i ponudile nove usluge koje su korisnički orijentirane, gdje su korisnici postavljeni u središte čime utječu na budućnost postojećih i novih usluga. U tako dinamičnoj okolini, najčešće se koriste pilot projekti koji nam na praktičnim primjerima služe kao testovi za pokazivanje prednosti digitalne transformacije.

Tipičan pionirski primjer usluge pametnih gradova je usluga Smart Metering koja koristi pametna brojala za udaljeno mjerenje potrošnje električne energije u kućanstvima. Tim

mjerenjima distributer električne energije i potrošač mogu pristupiti udaljeno te dobiti uvid o potrošnji električne energije kućanstva u stvarnom vremenu. Druga vrlo popularna usluga je Smart Parking koja je obično jedna od prvih usluga pametnih gradova budući da se uvođenjem ove usluge dramatično mogu smanjiti prometne gužve u gradovima zbog vozača koji traže parkirna mjesta. Postoje i brojni drugi primjeri usluga pametnih gradova, na primjer, detekcija curenja vode, pametna distribucija električne energije, pametna ulična rasvjeta ili detekcija zagađenosti zraka. Velik broj takvih usluga danas je dostupno i postavljeno u mnogim gradovima diljem svijeta. Dodatno, nastaju i inovativne usluge „životnog stila“ koje ne zahtijevaju neki specifični IoT uređaj, senzor ili neku drugu gradsku povezanu infrastrukturu, već ciljaju na građane i njihove životne navike. Naravno, takva vrsta usluga zahtjeva korištenje pametnih telefona i mobilnih aplikacija. Na primjer, Bologna je nedavno predstavila novu inovativnu uslugu koja pokušava pridobiti građane da koriste javni prijevoz, bicikle ili jednostavno hodaju. Aplikacija prati aktivnosti građana kako bi stvorila osobne bodove koji se onda mogu mijenjati za vaučere, na primjer, robu i usluge u lokalnim trgovinama. Ovakva vrsta usluge također ulazi u segment usluga pametnih gradova budući da koristi IKT kako bi se postigli strateški ciljevi grada Bologne⁸ za smanjenje broja automobila u gradskom središtu.

Ekosustav usluga pametnih gradova ne odnosi se samo na sam grad, već uključuje i sve što grad i njegova okolina čine, poput građana sa svojim društvenim aktivnostima, infrastrukture i tehnologije. To je širok pojam koji prelazi okvire samog grada i širi se svakom novom uslugom, novim skupom povezanih uređaja, novom infrastrukturom ili čak i starom infrastrukturom koja se koristi na novi način budući je povezana IKT tehnologijom.

Uvođenjem novih tehnoloških rješenja temeljenih na Internetu stvari gradovi sve više postaju živi organizam koji može odgovoriti na potrebe građana, ali također i popraviti sam sebe prema potrebi učeći iz okoline kako reagirati i ponašati se u pojedinim situacijama na temelju iskustva. Važno je napomenuti da gradovi već posjeduju i koriste veliku količinu infrastrukture koja može biti povezana korištenjem IKT-a, konkretno korištenjem Interneta stvari.

Prema [39] najveći izazovi usluga pametnih gradova su sljedeći:

- Tradicionalan način organizacije gradskih službi stvara problem budući da je svaka služba odgovorna za svoju infrastrukturu. Ovo predstavlja jedan od glavnih izazova i bez obzira što ovaj problem nije direktno vezan uz tehnologiju,

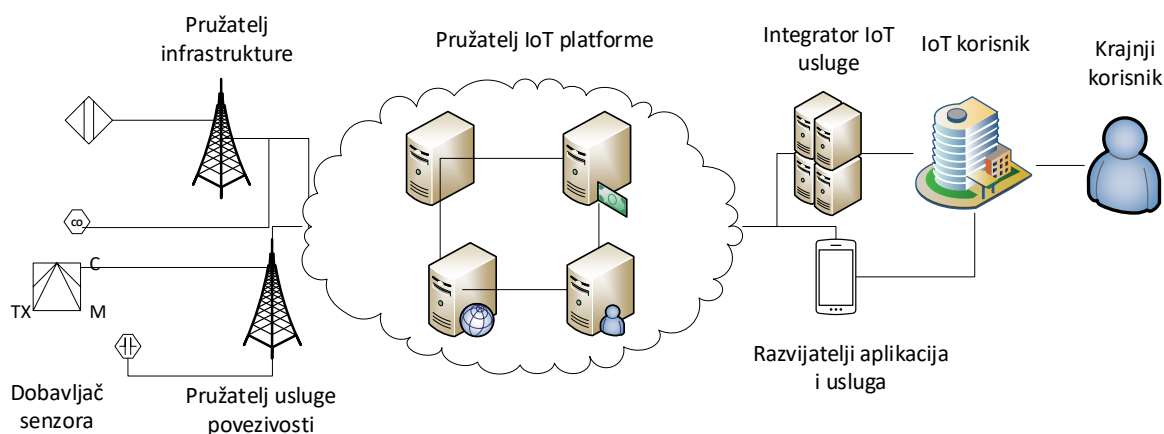
⁸ Bella Mossa and the Better Points applicaion, više informacija dostupno na <https://www.bellamossa.it/>

već administrativnu organizaciju posla u gradu, rješavanje ove prepreke će zahtijevati značajnu promjenu u načinu razmišljanja zaposlenika u gradskim službama.

- Izrada algoritama i shema koji opisuju informacije generirane od strane senzora u različitim aplikacijama, a što omogućuje razmjenu tih istih informacija između različitih gradskih usluga.
- Izrada algoritama za analizu i obradu podataka dobivenih od senzora razasutih po gradu i stvaranje dodatne vrijednosti od njih.
- Mehanizmi za povoljniju masovnu instalaciju i što je važnije za održavanje takvih instalacija, što uključuje čistu energiju.
- Osiguranje pouzdanih očitavanja sa senzora i efikasna kalibracija velike količine senzora postavljenih po cijelom gradu, od uličnih rasvjetnih tijela do kanti za otpad.

Ekosustav usluga pametnih gradova sastoji se od usluga izrađenih korištenjem IoT stoga. Tipičan IoT stog visoke razine je uvijek slojevit i obično počinje od sloja „stvari“ na dnu stoga gdje su različiti uređaji, senzori, aktuatori i mrežni pristupnici postavljeni u lokalni prostor. Povrh sloja stvari nalazi se mrežni sloj koji uređajima u sloju „stvari“ pruža povezivost prema IoT platformi. IoT platforma je obično implementirana unutar infrastrukture oblaka i predstavlja virtualnu reprezentaciju stvarne fizičke „stvari“, na primjer, IoT platforma može pružati uslugu dohvaćanja sirovih podataka očitanih od strane umreženih senzora ili može implementirati specifične metode za pokretanje aktuatorskih funkcija na određenim umreženim uređajima. Osim toga, IoT platforme su također odgovorne za upravljanje ugrađenim „stvarima“ i služe kao izvor sirovih podataka za analitiku i pružanje usluga više razine koje su ponuđene krajnjim korisnicima.

Slijedeći referentne arhitekture IoT-a koje zahtijevaju različite vještine za implementaciju, postavljanje i operativno održavanje, sama realizacija usluge pametnih gradova temeljena na IoT tehnologiji zahtjeva od svih dionika (nositelja) da preuzmu specifične uloge unutar svakog od prethodno nabrojanih slojeva IoT složaja. Upravo je iz tog razloga obično više pružatelja usluga u partnerskom odnosu uključeno u pružanje jedne usluge. Slika 18 prikazuje identificirane dionike i lanac vrijednosti za IoT-bazirane usluge pametnih gradova koji proširuje inicijalni lanac vrijednosti prvotno predstavljen u [40].



Slika 18: lanac vrijednosti IoT modela

Unutar IoT lanca vrijednosti mogu se identificirati u četiri glavne uloge:

- **Pružatelj infrastrukture:** ovo su pružatelji IoT uređaja i pružatelji usluge povezivosti na Internet. U slučaju kada je mreža operatora elektroničkih komunikacija korištena za pružanje povezivosti, infrastrukturni operator je ujedno i pružatelj elektroničke komunikacijske usluge u skladu sa Zakonom o elektroničkim komunikacijama. Infrastrukturni operator pruža mrežnu povezivost (bilo žičanu ili bežičnu) koja se koristi za povezivanje instaliranih uređaja na Internet. Ovakva mreža treba se izgraditi, postaviti i održavati kako bi se osigurala kontinuirana dostupnost i povezivost uređaja. To je usluga koja se obično pruža za određenu mjesečnu naknadu i djelomično se ili u potpunosti sastoji od prijenosa signala putem mreže elektroničkih komunikacija.
- **Pružatelj IoT-platforme:** je dionik koji pruža uslugu IoT platforme i funkcije sustava koji omogućuje jednostavan i brz pristup do senzorskih podataka te funkcije upravljanja uređaja, ali također nudi i agregiranje podataka radi razvoja novih usluga. Pružatelj IoT-platforme odgovoran je za nadzor heterogenih uređaja i prikupljanje podataka s različitih senzora. Za uspješan razvoj njegovog poslovnog modela ključno je korištenje standardnih protokola.
- **Integrator IoT usluga:** je pružatelj usluga pametnih gradova vezanih uz IoT rješenja koja su omogućena korištenjem jedne ili više IoT platformi i dodaju nove vrijednosti platformama na kojima su temeljeni.
- **IoT-korisnik:** je kupac usluga pametnih gradova koji koristi nove, inovativne mrežne komponente u svojim proizvodima (na primjer, pametno brojilo električne energije) i/ili

pruža inovativne usluge, poput usluge udaljenog mjerenja električne energije krajnjem korisniku. Na primjer, poduzeće koje je distributer električke energije koristi pametna brojila kako bi unaprijedilo svoju trenutačnu ponudu proizvoda i usluga. Postojeća, klasična brojila mijenja novim pametnim uređajima koji mogu ponuditi potpuno novu uslugu građanima kao što je informacija o potrošnji električne energije u stvarnom vremenu ili dinamička promjena tarifnog plana na temelju njihove potrošnje. IoT korisnici obično imaju kontakt ili direktno s pružateljem usluge infrastrukture od kojih koriste pružene usluge niže razine unutar njihove infrastrukture ili s integratorom IoT usluga koji nudi pakete usluga visoke razine rađene na nekoj IoT platformi.

- Krajnji korisnik: je korisnik na kraju IoT lanca vrijednosti koji kupuje i/ili koristi usluge pametnih gradova. Krajnji korisnik može biti privatna osoba ili može biti poduzeće.

Detaljnijom analizom uloga u IoT lancu vrijednosti može se uočiti mogućnost daljnje granulacije IoT uloga koje bi potencijalno povećale tržišno natjecanje, a zasigurno bi otvorile i prostor za razvoj novih poduzeća i novih poslovnih modela:

- Pružatelj uređaja (opreme): je proizvođač i/ili preprodavač senzorskih uređaja (ili IoT uređaja). Ovaj pružatelj se bavi razvojem, implementacijom i održavanjem pametne, umrežene, fizičke infrastrukture postavljene u gradskoj okolini. Pružatelj uređaja nudi senzore, aktuatora, mrežne pristupnike i ostale umrežene uređaje koji mogu biti ili direktno povezani na Internet ili mogu činiti bežičnu mrežu senzora koji imaju mogućnost agregiranja podataka kao i s lokalnim pametnim prostorima.
- Pružatelj IoT povezivosti: nudi povezivost uređaja prema Internetu korištenjem različitih tehnologija, ali najčešće upotrebom tehnologija male snage, koje pokrivaju široko područje (engl. Low-power wide area, LPWA). Povezivost kod bežičnih tehnologija se može ostvariti korištenjem nelicenciranog spektra (poput Zigbee, LoRa ili Sigfox) ili licenciranog spektra (poput NB-IoT, 5G, LTE, LTE-A). Dizajner usluge pametnih gradova mora dobro razmisliti o zahtjevima nad uslugama i na temelju toga odlučiti koju tehnologiju će koristiti budući da nelicencirani spektar nije štićen, ali je zato slobodan za korištenje. To znači da ukoliko postoje smetnje na tom frekvencijskom pojasu jer netko drugi također koristi istu tehnologiju ne postoji zakonski mehanizam kojim bi se usluga ili korisnici usluge zaštitili. S druge strane, licencirani spektar košta, ali je zato štićen od strane države i ukoliko netko u tom pojasu radi smetnje, država je

dužna poduzeti mjere kako bi se te smetnje otklonile. Nadalje, ukoliko je korišten nelicencirani spektar za povezivanje svih uređaja koji čine određenu uslugu (ili više njih) pametnih gradova, tada takva usluga ulazi u kategoriju usluga internetskog društva i nije regulirana od strane nacionalnog regulatornog tijela. Međutim, ukoliko je korišten licencirani spektar za povezivanje uređaja, sve pružene usluge moraju slijediti stroga pravila regulatornog okvira elektroničkih komunikacija i nacionalnih i EU zakona. U ovoj doktorskoj disertaciji navedene usluge ćemo nazivati nereguliranim, odnosno reguliranim uslugama. Očito je da je takvu podjelu između usluga teško uspostaviti u kompleksnim okolinama s mnogo heterogenih uređaja i više različitih IoT platforma koje tvore ekosustav usluga pametnih gradova.

- Razvijatelj IoT-aplikacija i usluga: nudi razvoj IoT usluga i aplikacija (obično mobilne i web-aplikacije) temeljene na dostupnim uređajima i platformama. Razvijatelj IoT-aplikacija i usluga razvija aplikacije za IoT-korisnike i krajnje korisnike, na primjer građane.

U razmatranje ćemo uzeti jedan konkretan primjer usluge pametnog grada na kojem ćemo objasniti predloženi IoT lanac vrijednosti i specifične uloge u navedenom lancu vrijednosti. Za primjer ćemo uzeti uslugu pametnog parkiranja koja je stvarno implementirana u Splitu.

Grad Split je drugi najveći grad u Republici Hrvatskoj i najveći grad na jadranskoj obali s gotovo 200000 stanovnika, a ujedno je i glavna trajektna luka na Jadranu. Split je i jedan od najstarijih gradova u Hrvatskoj i njegovo središte je prožeto uskim uličicama koje nisu oblikovane i predviđene za velik broj vozila. Točnije, središte grada je rađeno u rimsko doba kada nije uopće bilo vozila osim kočija. Broj vozila se za vrijeme ljetne sezone utrostručuje, što uzrokuje vrlo velike probleme s parkingom kojega je gotovo pa nemoguće pronaći i s neizostavnim prometnim gužvama. Parkirališta u gradu su upravljana od strane gradskog poduzeća Split Parking d.o.o. koje je odgovorno za upravljanje, održavanje i naplatu parkirnih mjesta. Prema našem modelu lanca vrijednosti Split Parking predstavlja IoT-korisnika koji obogaćuje svoja postojeća parkirna mjesta s dodatnim uređajima koji pružaju informaciju o zauzetosti parkirnog mjesta, a tradicionalna usluga parkiranja je proširena s aplikacijom za mobilne uređaje koja navodi vozača do slobodnog parkirnog mjesta. Kako bi osigurao ovu uslugu, Split Parkingu je potreban pružatelj usluge infrastrukture koji će postaviti senzorske uređaje na njihova parkirna mjesta kako bi mogli nadgledati njihovu zauzetost. Pružatelj

uređaja (senzora) je proizvođač parkirnih senzora čija je odgovornost osigurati nesmetanu i jednostavnu integraciju različitih tipova odgovarajućih senzora s IoT-plattformom. Kako bi se to ostvarilo, uređaji bi trebali podržati otvorene protokole dok pružatelj uređaja treba osigurati cjelovitost i sigurnost prijenosa podataka za vrijeme komunikacije između uređaja i platforme. Pružatelj infrastrukture ima dvojaku ulogu u ovom primjeru. Prva uloga je ustvari uloga pružatelja usluge mreže uređaja koji povezuje uređaje s Internetom i IoT platformom direktno bez korištenja tuđe infrastukture i ugovora s drugim operatorima, dok je druga uloga vezana uz pružanje povezivosti koja se može postići kroz ugovor s operatorom elektroničkih komunikacija. Zbog svoje dvojake uloge, pružatelj infrastrukture mora osigurati *roaming* ukoliko je to potrebno i zakonsko presretanje poziva ukoliko je to traženo od tijela zaduženih za provođenje mjera tajnog nadzora, te u tom slučaju treba otvoriti sučelja prema tijelima odgovornim za provođenje mjera tajnog nadzora. Pružatelj usluge IoT platforme osigurava softversku platformu za upravljanje uređajima i prikuplja podatkovne tokove sa svih uređaja kako bi integrator IoT usluga uvijek imao pristup ažuriranim podacima koji se koriste za pružanje naprednih IoT-usluga Split Parkingu. Split Parking bi vjerojatno najradije surađivao samo s integratorom IoT-usluge koji nudi odgovarajuću uslugu parkiranja integriranu s mobilnom aplikacijom koja je korisnički orijentirana. Međutim, budući da je Split Parking pružatelj usluge krajnjim korisnicima, njegova glavna odgovornost je čuvanje privatnosti korisničkih podataka i dodatno, kao vlasnik parkirnih mjesta, odgovoran je i za ostale tehničke i regulatorne zahtjeve pružene usluge pametnog parkiranja. Stoga Split Parking treba ući u partnerstvo s pružateljem usluge infrastrukture, pružateljem platforme i pružateljem usluge integracije IoT-usluge kako bi svojim građanima i turistima mogao ponuditi novu aplikaciju i uslugu pametnog parkiranja.

Uvedene usluge pametnih gradova najčešće koriste vlastita rješenja koja nisu međusobno kompatibilna i kao takva mogu biti implementirana i kao zatvorena rješenja. Ovo predstavlja veliku fragmentaciju koja je detektirana u [41], kao jedna od najvećih zapreka rasta ekosustava pametnih gradova. Kako bi se zaobišla postojeća gradska organizacija, gdje je svaki ured odgovoran za svoj segment i funkcionalnosti, potrebno je interoperabilno rješenje i bez obzira što nije direktno vezano uz tehnologiju, rješavanje ove prepreke predstavlja promjene u načinu razmišljanja gradskih djelatnika ili promjenu same organizacijske strukture. Interoperabilnost, kako je definirano prema ETSI-jevoj tehničkoj komisiji TISPAN [42], predstavlja sposobnost komuniciranja uređaja različitih proizvođača opreme između sebe unutar iste mreže (istog sustava). Prethodno spomenuti dokument TISPAN-a identificira

različite aspekte interoperabilnosti (tehničke, sintaktičke, semantičke i organizacijske). U kontekstu pametnih gradova, sintaktički i semantički aspekti spadaju u najistaknutije aspekte interoperabilnosti. Sintaktički aspekti se odnose na korištenje otvorenih i standardiziranih protokola, dok se semantički odnose na rješenja i sheme koji opisuju informacije dobivene od senzora u različitim aplikacijama kako bi se omogućila korisna razmjena informacija između različitih gradskih usluga. Postojeća rješenja najčešće su temeljena na vlastitim podatkovnim modelima koje druge aplikacije ili usluge ne mogu razumjeti i prepoznati te stoga proces integracije uređaja i podataka kroz više domena i IoT rješenja postaje zapreka.

Ključni element za postizanje interoperabilnosti u takvoj okolini s više postojećih sustava i heterogenih uređaja i informacijskih modela je korištenje horizontalne platforme za labavo povezanu integraciju vertikalnih rješenja. Ovakav pristup je predložen u [43] kako bi se omogućila interoperabilnost vertikalna pametnih gradova. Autori su predstavili novi pristup koji se „sastoji u definiranju skupa modularnih, općenitih specifikacija (engl. *the Smart City Platform Specification*) za implementaciju horizontalnih ICT platformi, kako bi se omogućila interoperabilnost između vertikalnih silosa“. Usporediv pristup je predložen i u H2020 projektu symbIoTe [44] koji je implementirao jedinstvenu međuslojnu platformu za interoperabilnost Interneta stvari koja je objavljena kao javno dostupan softver. SymbIoTe proširuje postojeće IoT platforme i uređaje sa specifičnim adapterima koji implementiraju funkcionalnost vezanu uz semantičku interoperabilnost i kontrolu pristupa temeljenu na atributima kako bi se povrhu platforme i uređaja ponudilo ujednačeno sučelje temeljeno na protokolu REST. Dodatne informacije o projektu symbIoTe su dostupne u [45].

2. REGULATORNI OKVIR ZA PAMETNE GRADOVE

Ekosustav usluga pametnih gradova, kao nadolazeći kompleksan sustav koji ima potencijala predstaviti mnoštvo inovacija, potencijalno može uvesti i nova pravila ponašanja među dionike lanca vrijednosti. Trenutačno znanstvenici, političari, voditelji velikih poduzeća u Europi i SAD-u vode debate oko mogućih pravila ponašanja. Kod uvođenja regulacije treba uzeti u obzir kompleksnost IoT sustava, stoga se problem treba razmatrati s više razina s pogledom na budućnost. Svakako treba paziti što regulacija tržišta donosi, odnosno kako može utjecati na inovacije te prilagodbu i brzinu širenja IoT-rješenja u društvu i poslovnom okruženju. U nastavku je dan pregled rasprava privatnog sektora i javnosti oko ključnih problema IoT-a koji uključuju privatnost, sigurnost, etiku, povjerljivost podataka, konkurentnost, ekonomski razvoj i slobodu inovativnosti.

2.1. Povijesni pregled regulacije u svijetu

2.1.1. Europa

Europa je zbog definiranja svojih visokih ciljeva najdalje došla u segmentu IoT-a i trenutačno je regulativa na području nekoliko sektora ta koja potiče IoT-razvoj u Europi. Sljedeći dokumenti definiraju smjernice relevantne za područje IoT-a:

1. „*The Energy Services Directive*“: direktiva o smanjenju potrošnje energije različitih vrsta uređaja i energetske usluga 2006/32/EC. Sukladno ovoj direktivi očekuje se kako će 80% kućanstva do 2020. imati instalirane pametne mjerače energije.
2. „*e-Call Directive*“: prema prvim najavama direktiva je trebala stupiti na snagu do sredine 2015. godine, međutim zbog uvođenja tehnologije u automobile i testiranja, obveza je nastupila tek od 2018. godine. Sukladno ovoj direktivi sva nova vozila moraju imati ugrađene uređaje koji će u slučaju nesreće automatski zvati broj 112 te na taj način hitnim službama osigurati ključne informacije poput GPS koordinata, podataka o vozaču i slično.

3. „*The EU 531/2012 Roaming Regulation*“: direktiva za Roaming uvodi važne promjene koji mogu pomoći EU tržištu, poput uvođenja agregatora kao veleprodajnog pružatelja usluge.

Debata o važnosti IoT-a u Europi se započela voditi u 2006., a nastavila u ožujku 2007. godine kada je i službeno prihvaćen koncept IoT-a u Commission Communication on RFID [46].

U studenome 2008. godine je u izvješću „Future Networks and Internet“ prepoznato da IoT ima veliki potencijal za razvoj novih usluga, ali istovremeno predstavlja rizik u smislu zaštite privatnosti pojedinca [47]. Prepoznata je potreba za raspravom o arhitekturi i upravljanju IoT-a, te su sve zemlje članice pozvane da promiču decentralizirano upravljanje koje bi osiguralo povjerljivost, sigurnost, privatnost i etičko upravljanje podacima koji se izmjenjuju kod IoT-a [47].

Europska komisija (EK) je 2009. godine prihvatila strateški akcijski plan IoT-a u 14 točaka [48] koji je predstavljao skup principa upravljanja IoT-om, procjenu mogućih rizika, financiranje zajedničkog istraživanja, sudjelovanje u internacionalnom dijalogu, te integraciju IoT-a u 4 istraživačko razvojna projekta javno-privatnog partnerstva. U lipnju 2010. godine EK je osnovala stručnu radnu skupinu koju sačinjavaju stručnjaci različitih profila, uključujući znanstvenike, tehničare, predstavnike industrije, pravnih i društvenih znanosti, a koji su savjetodavno tijelo EK vezano uz glavne probleme koji uključuju upravljačke mehanizme, vlasništvo podataka, privatnost, sigurnost, standarde i svjetsku suradnju.

EK je 2012. godine provela javnu raspravu o upravljanju IoT-om, kojoj je prethodio online upitnik s uključenih 600 ispitanika. U upitniku su prikupljali viđenje prikladnog pristupa upravljanju kako bi se potaknuo brži razvoj IoT-a, a istovremeno osigurala odgovarajuća zaštita građana EU. Odazvali su se različiti profili tvrtki i građana, od čega je 50% bilo zainteresiranih građana, 27% akademskih i udruga civilnog društva, 11% predstavnika industrije i njihovih udruga i 12% ostalih. Rezultati su pokazali zajednički stav da će IoT donijeti značajan ekonomski i sociološki napredak, a pogotovo će pridonijeti u području zdravlja, samostalnog življenja, te podrške za osobe s invaliditetom. U svemu ostalom vidjela se velika razlika u razmišljanju građana i građanskih udruga koji žele strožu regulaciju u odnosu na industriju. Prema rezultatima 77% ispitanika je podržalo izradu pokazatelja procjene utjecaja na zaštitu podataka, što uključuje zahtjeve za pristankom korisnika na prikupljanje podataka, anonimnost podataka, ograničeno korištenje i zadržavanje podataka, te privatnost. Zanimljivo da je većina

odgovora pokazala da će IoT imati mnogo etičkih pitanja vezanih uz prikupljene podatke, ali ujedno su pokazali da razvoj IoT-a ne bi trebao dovesti do sociološke nepravde. 92% ispitanika se složilo s potrebom standarda i smjernica IoT-a koji bi osigurali povjerljivost, integritet i dostupnost, ali je velik broj ispitanika napomenuo da bi se smjernice i standardi trebali definirati u okviru više dionika tržišta uz sudjelovanje korisničkih udruga, civilnog društava i regulatora u odnosu na javna tijela i privatne dionike.

Zaključak stručne IoT grupe Europske unije iz prosinca 2012. bio je da postoji znatno neslaganje između poslovne zajednice (prvenstveno industrije) i javnog mijenja oko većine problema, ali posebno se može izdvojiti privatnost, sigurnost, te potreba za bržim razvojem konkurentnosti u IoT okruženju [49]. Na temelju takvog zaključka EK je europskom RAND institutu dodijelila izradu smjernica upravljanja IoT-om. Njihovo izvješće objavljeno u kolovozu 2013. godine navodi da se IoT razvija ubrzano i da predstavlja izazov za tradicionalne poslovne, tržišne, upravljačke i socijalne modele. Posebice ekonomsko, sociološko-političko, pravno i tehnološko upravljanje Internetom je temeljeno na pretpostavci o racionalnom izboru, tržišnoj snazi i efikasnoj samoorganizaciji koja je najviše prilagođena sustavima pod ljudskom kontrolom. S obzirom da interaktivni autonomni sustavi IoT-a dosta odskakuju od ove paradigme [50], preporuka RAND-a je korištenje pristupa „blagog zakonodavstva“ koji će objединiti standarde, nadgledanje i etički karakter, ali će ujedno dati slobodu industriji da se na najjednostavniji način prilagode zahtjevima regulative. To bi trebalo dati prostora razvoju IoT-a u EU.

2.1.2. Sjedinjene Američke Države

Za razliku od Europe koja svojim regulatornim djelovanjem potiče razvoj IoT-a, u SAD-u je i debata o IoT-u sporadična i rastrkana. Većina debata je vođena od strane pojedinih Federalnih agencija koje imaju interesa samo za pojedine segmente IoT-a. Tako je na primjer, u 2012. godini Nacionalni institut za standardizaciju i tehnologiju objavio Okvir i plan za izradu standarda za interoperabilnost Smart Grid-a (Framework and Roadmap for Smart Grid Interoperability Standards) [51], čime su zahvatili samo jedan segment IoT-a. Državni ured je u 2013. godine istraživao mogućnost korištenja IoT-a za praćenje oružja za masovno uništavanje, a Ministarstvo domovinske sigurnosti kontinuirano postavlja i senzorske sustave za detekciju kemijskih i bioloških prijetnji [52]. Obavještajna zajednica je također pokazala interes za IoT područje te je još 1999. godine CIA investirala u brojna IoT startup poduzeća,

između ostalog i u poduzeća Tendril Networks i Ember Corporation koja se bave proizvodnjom bežičnih senzora [53].

Prvu ozbiljniju raspravu pokrenula je u travnju 2013. godine Trgovačka komisija (FTC) zatraživši komentare o utjecaju IoT-a na privatnost i sigurnost [54]. Pristiglo je samo 27 odgovora od čega je preko 60% bilo od industrije ili njihovih udruga. Slijedom navedenog, komentari su bili protiv regulacije. Većina komentara je išla u smjeru samoregulacije te odmicanju od utjecaja vlade u izradi standarda privatnosti i sigurnosti koji bi, po njihovom, mogli ugroziti razvoj i inovacije IoT-a. Industrija vjeruje da bi izrada certifikata za sigurnost i privatnost s njihove strane mogla polučiti dovoljnu zaštitu korisnika.

U studenome 2013. godine FTC je održao javnu radionicu o IoT-u kako bi istražili probleme sigurnosti i privatnosti zbog povećeg broja povezanih uređaja [55] s ciljem informiranja komisije o razvoju IoT-a. Na toj radionici predsjednica FTC-a je istaknula ključne izazove od kojih je glavni bio gubitak osobnih podataka koji su prikupljeni i pohranjeni. Kao tri glavna načela izdvojila je podatkovnu transparentnost, jednostavan izbor kontrole osobnih podataka i model privatnosti [55]. Okrugli stol je kasnije otvorio raspravu o dodatnim problemima upravljanja poput korištenja IoT-a u svrhu nadzora građana od strane vlade. Predloženo je nekoliko opcija zaštite privatnosti i sigurnosti korisnika kao što su samoregulacija, izrada ovjerenih certifikata odobrenja, implementacija kodeksa ponašanja, početak korištenja postojećeg zakona o korisnicima te razvoj nove regulacije IoT-a. Stav FTC-a je da se trebaju iskoristiti postojeći zakoni i postojeća regulativa prije razmišljanja o uvođenju nove regulacije. Zaključak panela je da će regulacija ovisiti o tome dolazi li prihod poduzećima isključivo od IoT proizvoda i usluga ili planiraju unovčiti korisničke podatke kroz prodaju usluga za analizu podataka.

Prema dosadašnjim aktivnostima, rasprava u SAD-u je tek započela. Također, za razliku od EU koja je ranije započela s raspravama na ovu temu, identificirani su slični problemi upravljanja. Slijedom svega navedenog, budućnost upravljanja i regulacije IoT-a u EU i SAD-u za sada je dosta nedefinirana.

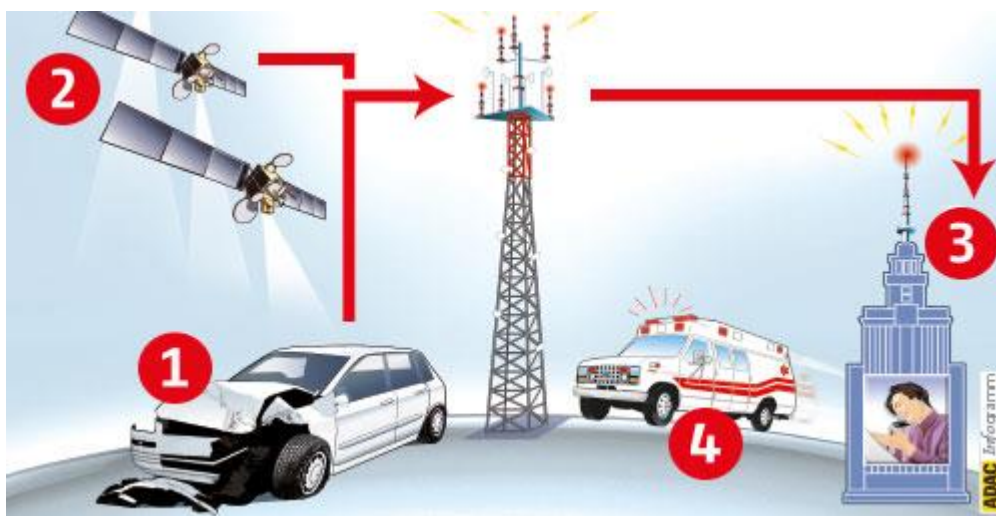
2.2. Europski regulatorni okvir za pametne gradove

2.2.1. E-call

E-call predstavlja direktivu Europske unije kojom se pokušava stati na kraj ljudskim gubicima tijekom prometnih nesreća. Prema direktivi, u trenutku teške prometne nesreće,

sustav u vozilu automatski vrši poziv prema jedinstvenom europskom broju za hitne službe 112 uz automatski prijenos lokacije vozila. Tijekom 2012. godine oko 28000 ljudi je poginulo, a više od 1,5 milijun ljudi je ozlijeđeno u preko 1,1 milijun prometnih nesreća na EU cestama. Osim same tragedije gubitka života i ozljeda procijenjeno je da nesreće uzrokuju i direktan trošak za društvo u iznosu od 130 milijardi € svake godine.

Procjena je da bi se uvođenjem ovog sustava reakcija hitnih službi mogla ubrzati i do 40% u urbanim područjima, odnosno, 50% u ruralnim područjima te bi moglo biti spašeno najmanje 2500 ljudi godišnje [56].



Slika 19: Aktivacija eCall sustava prilikom nesreće [57]

eCall se aktivira automatski čim senzori unutar vozila i/ili procesor (na primjer zračni jastuk) detektiraju tešku nesreću (broj 1 na slici 19). Nakon što je aktiviran, sustav zove jedinstveni broj za hitne službe 112, uspostavlja poziv s odgovarajućim centrom i šalje detaljne informacije o nesreći (npr, minimalan skup podataka) hitnoj službi. Minimalan skup podataka uključuje vrijeme nesreće, točnu poziciju (koordinatu) unesrećenog vozila i smjer kretanja vozila. Također, može sadržavati i podatke o vozaču, poput krvne grupe, različitih alergija i slično (broj 2 i 3 na slici 19). Po primitku poziva hitne službe na temelju dobivenih podataka kreću na teren (broj 4 na slici 19).

eCall se može aktivirati i ručno pritiskom na dugme u vozilu u slučaju kada je vozač svjedok nesreće.

Sukladno donesenoj direktivi svako vozilo proizvedeno u EU mora imati ugrađen sustav za pozivanje broja 112 u slučaju nesreće od 1. svibnja 2018. godine.

Osim ovakvog sustava neki proizvođači vozila su počeli ugrađivati i druge detekcije unesrećenog vozača, na primjer, ukoliko vozač ne drži upravljač vozila nekoliko trenutaka auto

ga upozorava zvučno te stavljanjem obavijesti na info ekran. Ukoliko i nakon takvog upozorenja vozač nastavi voziti vozilo bez držanja upravljača, vozilo preuzima kontrolu nad upravljanjem i zaustavlja vozilo pored ceste te automatski zove hitnu službu budući je pretpostavka da je vozaču potrebna pomoć.

2.2.2. Energy Efficiency directive

Prva direktiva za energetske učinkovitost (2006/32/EC)[58] stupila je na snagu u travnju 2006. godine. Ona predstavlja okvir za povećanje energetske učinkovitosti kod krajnjih korisnika i energetskih usluga. Ona je uključivala i indikativne ciljeve uštede energije po državama članicama. Želja EK je bila da se smanji udio stakleničkih plinova te ovisnost o energetskim izvorima izvan EU. Prema tadašnjim procjenama, ukoliko se ništa ne bi poduzelo, utjecaj vanjskih izvora bi narastao s 50% na 70% do 2030. godine.

Sama svrha direktive je da se korištenje energije učini ekonomičnije i efikasnije:

- Uspostavljanjem indikativnih ciljeva, inicijativa i institucionalnih, financijskih i zakonodavnih okvira potrebnih za uklanjanje prepreka na tržištu i nedostataka koji utječu na efikasno korištenje energije.
- Stvaranjem uvjeta za razvoj i promociju tržišta energetskih usluga, te programa za uštedu energije kao i ostalih mjera koje imaju za cilj povećanje učinkovitosti.

Glavni cilj ove direktive postavljen je na način da svaka država članica mora prihvatiti i postići indikativnu uštedu energije od 9% do 2016. godine.

Ova direktiva je u međuvremenu zamijenjena novom direktivom 2012/27/EU [59] koja postavlja skup obvezujućih mjera kojima bi EU trebala dostići svoje postavljene ciljeve od 20% energetske učinkovitosti do 2020. godine. Direktiva zahtjeva od svih zemalja članica da energiju koriste efikasnije u cijelom potrošačkom lancu, od proizvođača do krajnjeg potrošača. 2016. godine EK je predložila nadogradnju ove direktive postavljanjem novog cilja, a to je dostizanje 30% energetske učinkovitosti do 2030. godine.

Nova direktiva uključila je i niz dodatnih mjera poput:

- Distributeri ili preprodavači energije moraju godišnje ostvariti 1,5% energetske uštede kroz implementaciju mjera energetske učinkovitosti;
- Zemlje EU mogu se odlučiti za postizanje energetske učinkovitosti i drugim sredstvima, poput povećanja učinkovitosti sustava grijanja, postavljanjem dvostrukih izo stakla na prozore ili izolacijom krovova;

- U zemljama EU javni sektor treba kupovati energetske učinkovite zgrade, proizvode i usluge;
- Svake godine vlade u zemljama EU moraju renovirati minimalno 3% zgrada koje posjeduju ili imaju kako bi bile energetske učinkovite;
- Krajnji korisnici trebaju imati mogućnost boljeg upravljanja potrošnjom. Ovo predstavlja jednostavan i besplatan pristup podacima o potrošnji kroz pojedinačna mjerenja;
- Davanje nacionalnih poticaja za mala i srednja poduzeća da prođu energetske preglede;
- Velike poduzeća će raditi preglede vlastite potrošnje energije kako bi se identificirali načini za njihovo smanjenje;

Kako bi se dostigli ciljevi iz navedenih direktiva te ispunile sve mjere navedene u energetskej direktivi, postavljene su i prateće direktive koje će to olakšati poput Direktive o unutarnjem tržištu električne energije i plina iz 2009. godine (2009/72/EC i 2009/73/EC) koja je uključena u treći energetskej paket, a koja od svih država članica zahtjeva da osiguraju implementaciju inteligentnog sustava mjerenja koji će pomoći aktivnom uključivanju potrošača na tržište električnom energijom i plinom.

Ovom direktivom EU ima namjeru do 2020. godine zamijeniti najmanje 80% električnih brojila pametnim brojlama gdje god je to isplativo. Uvođenje pametnih brojila i pametnih mreža može smanjiti emisije stakleničkih plinova do 9% godišnje te u sličnom postotku godišnje smanjiti potrošnju električne energije u kućanstvima. Kako bi se izmjerila ekonomičnost svaka zemlja EU provela je analizu troškova i koristi na temelju smjernica EK. Slična procjena napravljena je i na pametnim brojlama za plin [60].

Uvođenjem pametnih brojila potrošači će dobiti i mogućnost dinamičkih ugovora gdje se cijena može mijenjati dinamički ovisno o potrošnji.

2.2.3. Roaming regulation directive

Uredba o Roamingu pozivima u EU zemljama direktno je povezana s uvođenjem digitalne preobrazbe Europske unije u digitalno društvo. Prva uredba [61] postavljena je 2007. godine kada se EK nakon dvije godine rasprave i pokušaja spuštanja Roaming cijena odlučila umiješati i zakonski regulirati maksimalan iznos cijena Roaming. Tijekom 2008. i 2009. godine predviđeno je daljnje spuštanje cijena s trajanjem do 2012. godine do kada se očekivalo da će tržište samo postaviti određene mjere vezane uz Roaming. Budući da se to nije dogodilo, 2012.

godine donesena je nova uredba[62] kojom se produljuje period smanjenih Roaming cijena do 2017. godine.

U prijedlogu Strategije jedinstvenog digitalnog tržišta za Europu[63] i inicijative Digitalna agenda[64] za Europu jedna od mjera je bila i potpuno ukidanje Roaming naknada. Uredba o Roamingu u javnim pokretnim komunikacijskim mrežama u Uniji [65] iz 2015. godine konačno je donijela prijedlog postepenog smanjivanja i na kraju konačnog ukidanja Roaming naknada za krajnje korisnike u EU. S danom 15. srpnjem 2017. godine Roaming između EU članica je u potpunosti uklonjen.

EK je shvatila da ovakva uredba može snažno utjecati ne samo na korištenje pokretnih mreža, nego i na razvoj dodatnih usluga što je za razvoj digitalnog društva bilo neophodno. Usluge temeljene na IoT tehnologijama, a vezane uz promet bile su vrlo ograničene isključivo na pojedine zemlje zbog visokih Roaming naknada. Ukidanjem naknada tržište dobiva inicijativu za razvoj, pogotovo u sektoru logistike i transporta.

Pravila unutar uredbe, znana i pod nazivom „Roam Like at Home“, predviđaju da korisnik za korištenje usluga pokretnih komunikacija ne mora plaćati dodatne troškove. Korisnici imaju koristi od ove uredbe za slanje tekstualnih poruka, glasovnih poziva ili podatkovnog prometa dok su izvan matične zemlja, ali na području EU. Pravilo nalaže da korisnik plaća identičnu cijenu poziva unutar EU, bez obzira gdje se nalazi, koliko bi plaćao da zove iz svoje države. U stvarnosti to znači da operator korisniku pozive odbija od postojećih tarifnih planova koje ima ugovorene. Ova uredba je prvenstveno namijenjena za ljude koji povremeno putuju izvan svoje domovine, bilo radi godišnjeg odmora ili posla. Nije namijenjena da se koristi kao trajni Roaming. Ovakva odredba imala je negativan utjecaj na proizvođače pružatelje IoT usluga koji su mislili zaobići visoke Roaming naknade te koristiti jedan broj u svim državama, ali ovakva odredba je to onemogućila. Postoji mogućnost korištenja specijalnih IoT/M2M brojeva koje dodjeljuje ITU i koje se mogu koristiti na razini cijelog svijeta međutim njihovo korištenje je financijski zahtjevnije. Ovakvo pravilo koje zahtjeva da u svakom kvartalu korisnik provede više vremena kod kuće nego vani smatra se ispravnim korištenjem Roaming usluge. Uredba ne postavlja direktne limite korištenja ovakvog Roaming, već je usluga ograničena paketom koji korisnik ima ugovoren sa svojim pružateljem usluge.

Bojazan koja se javljala kod operatora vezano uz trošak koji će imati zbog gubitka Roaminga pokazala se neopravdanom budući da je već prva godina korištenja pokazala da su korisnici zbog ukinutih Roaming naknada počeli značajnije koristiti pokretnu mrežu u

inozemstvu, čime se broj minuta korištenja mreže povećao, a što je u konačnosti smanjilo ili neutraliziralo gubitke koje su operatori imali ukidanjem Roaming naknada.

Pozitivan efekt koji je Roaming regulacija donijela vidljiv je posebice kod usluga transporta i logistike koje su postale jeftinije za krajnje korisnike, a čime su i same IoT usluge postale pristupačnije.

2.2.4. Uredba (EU 2016/679) o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (GDPR)

Još od početka prvih naselja u davnim vremenima one grupe ili pojedinci koji su imali informacije imali su i prevlast. Informacija daje ljudima moć kojom mogu upravljati drugim ljudima, mogu dobivati poslove, mogu dobivati ratove. Danas ljudi sve više postaju svjesni koliko su informacije, pogotovo, osobne informacije bitne i kako ih treba štiti.

Slikovito se to može objasniti ovako. Vozač u osiguravajućoj kući ugovara kasko osiguranje za vozilo, a na kraju mu prodavač u vozilo stavi kutiju veličine kutije šibica što vozač uskoro zaboravlja. Nakon 6 mjeseci vozač dobiva pismo kojim ga osiguravajuća kuća obavještava da je oprezan i siguran vozač te mu stoga vraća određeni iznos premije. Vozač je sretan zbog toga no ne zna odkud osiguravajućoj kući takvi podaci. Nakon novih 6 mjeseci vozač ponovno dobiva pismo osiguravajuće kuće. Obavještavaju ga da je premija osiguranja povećana jer je na temelju podataka iz područja u kojem živi uočeno da je naselje nesigurno. Ovo pokazuje kako je osiguravajuća kuća na temelju osobnih podataka donijela dvije poslovne odluke, a da sam vozač nije bio svjestan korištenja svojih osobnih podataka.

Na sličnom principu rade i mnoge popularne aplikacije, poput aplikacije Waze, koje prikupljaju informacije iz prometa te na temelju toga određuju ponašanje ili aplikacije za traženje parkirnih mjesta koje na temelju lokacije unutar koje ćelije se nalazite i GPS koordinate traže najbliže parkirno mjesto.

Ovakve usluge će sve više biti dostupne u svijetu zahvaljujući IoT tehnologiji, međutim postavlja se pitanje što je granica do koje se smije ići? Još jedan primjer govori o sličnoj situaciji. Vozač vozi auto i senzor u vozilu detektira da je prekoračio brzinu. O tome obavještava vozača, ali istovremeno šalje podatak policiji. Čiji je podatak o prekoračenju brzine? Je li taj podatak vlasništvo vozača ili proizvođača automobila koji ugrađuje takve module u vozilo ili je taj podatak vlasništvo policije?

Ovo su samo neka od brojnih pitanja koja se zadnjih godina postavljaju dolaskom novih tehnologija.

Opća uredba o zaštiti osobnih podataka pokušava odgovoriti upravo na ta pitanja. Iako je zakon o zaštiti osobnih podataka postojao i prije, do sada nije bio primjenjivan, a zakonodavna tijela, odnosno, agencije koje provode taj zakon nisu imali ovlaštenja i zakonskih mogućnosti kažnjavanja.

Još 1995. godine EU je donijela prvu Uredbu o zaštiti osobnih podataka koja je postavila minimalan skup standarda za obradu podataka u EU. Međutim, kako je tehnologija napredovala, uvidjelo se da i uredbu treba unaprijediti. Početkom 2012. godine EK je donijela plan za reformu zaštite podataka na razini EU kako bi Europa bila spremna za digitalno doba. Reforma je prihvaćena u prosincu 2015. godine i tada je potpredsjednik za jedinstveno digitalno tržište, Andrus Ansip, rekao: „Digitalna budućnost Europe se jedino može temeljiti na povjerenju. S čvrstim zajedničkim standardima za zaštitu podataka građani mogu biti sigurni da imaju kontrolu nad svojim osobnim podacima“.

27. travnja 2016. Europski parlament i Vijeće donijeli su Uredbu (EU 2016/679)[66][67] o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (dalje: GDPR) koja je u svim državama članicama stupila na snagu danom 25. svibnja 2018. godine.

Opća Uredba prije svega donosi:

- harmonizirani zakon o zaštiti privatnosti u svim EU članicama,
- štiti i osnažuje privatnost svih građana EU i
- preoblikuje način na koji organizacije pristupaju osobnim podacima.

GDPR predstavlja novi skup pravila pripremljenih kako bi građani EU dobili veću kontrolu nad svojim osobnim podacima. Cilj je pojednostaviti regulatorno okruženje za poslovanje kako bi građani i poduzeća u Europskoj uniji mogla u potpunosti iskoristiti digitalno gospodarstvo. Cijela reforma se zasniva na tome da se današnji zakoni (pogotovo vezani uz osobne podatke, privatnost i suglasnost) prilagode vremenu interneta u kojem živimo. Većina stvari u životima ljudi vezana je uz podatke. Primjerice, financijski sektor (banke, osiguranja, itd.), telekomi, društvene mreže, pa čak i trgovci mješovitom robom, prikupljaju i obrađuju osobne podatke svojih korisnika. Po GDPR-u, poduzeća moraju osigurati da su podaci prikupljeni legalno pod vrlo strogim uvjetima, ali posebno moraju voditi računa u koju svrhu se podaci prikupljaju, kako se obrađuju i čuvaju. Također, moraju štiti podatke od nelegalnog korištenja i krađe.

Novost koju GDPR uvodi je i „pravo na zaborav“. Mnoga velika poduzeća poput Google, Facebooka i Microsofta čuvaju korisničke podatke te ih koriste u različite svrhe i nakon što korisnik napusti uslugu koju je koristio. Zahvaljujući GDPR-u, građani imaju mogućnost zatražiti brisanje svih podataka o korisniku nakon što to pojedinac zatraži. Dakle, GDPR je primjenjiv na sva poduzeća uključujući i ona koja se nalaze izvan EU, ali posluju na području EU ili uslugu pružaju građanima EU.

Pojava GDPR-a najviše je utjecala na poduzeća u IKT sektoru jer industrija „velikih podataka“ u pravilu koristi pseudonimizirane podatke koji joj omogućavaju spajanje podataka iz više izvora. Ti podaci odnose se na isti pseudonim i detektiranje obrazaca ponašanja vezanih uz taj pseudonim, a poslije se mogu komercijalizirati, bilo u reklamne ili neke druge svrhe, poput utvrđivanja razloga i rješenja problema prometne zagušenosti na određenoj lokaciji, slanja obavijesti i upozorenja, predviđanja širenja epidemija, predviđanje potrošnje energije.

Pseudonimizirani podaci su oni gdje se podaci iz više izvora, koji se odnose na jednu osobu, povezuju putem pseudonima. Pomoću ključa za usporedbu pseudonima može se otkriti stvarni identitet fizičke osobe. S druge strane, anonimizirani podaci su oni iz kojih se ni na koji način ne može saznati na koju se osobu odnose.

Korištenjem anonimiziranih podataka ne mogu se spajati podaci iz više izvora koji se odnose na jednu osobu pa se time ne mogu niti detektirati obrasci ponašanja te osobe.

Prema članku 6. GDPR-a, obrada osobnih podataka je zakonita ako se provodi na temelju barem jedne od dopuštenih osnova. Jedna od dopuštenih pravnih osnova je i legitimni interes voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika.

Prema stavovima industrije, GDPR osigurava dovoljna jamstva po pitanju primjene pravne osnove legitimnog interesa, budući da legitiman interes voditelja obrade nije dovoljan da bi obrada podataka bila zakonita. Naime, on iziskuje odgovarajući test proporcionalnosti, odnosno balansa između interesa voditelja obrade s jedne strane i ispitanika s druge strane, koji se procjenjuje od slučaja do slučaja, te ispunjavanje paralelno i svih ostalih načela zaštite osobnih podataka.

Kada je riječ o industriji „velikih podataka“, tvrtke smatraju da primjena pseudonimizacije ili enkripcije jamči dovoljnu zaštitu privatnosti koja istovremeno omogućava inovacije zasnovane velikim podacima.

GDPR uredba već sama po sebi donosi ograničenja koja bi mogla usporiti razvoj usluga Internet stvari (RFID tagovi su postavljeni u kategoriji online identifikatora) ili poskupiti

njihovu implementaciju, ali najveći problem mogao bi nastupiti u kombinaciji s direktivnom o e-privatnosti koja direktno zadire u pitanje povjerljivosti kod komunikacije stroja sa strojem, odnosno kod Interneta stvari.

2.2.5. Uredba o E-privatnost (e-PR)

Direktiva o zaštiti privatnosti (Directive 2002/58/EC)[68] je donesena još 2002. godine i naslanjala se na direktivu o zaštiti osobnih podataka. Kasnije su rađene dorade unutar direktive vezane uz kolačiće na web-preglednicima gdje su korisnici morali davati privole za prikupljanje podataka, a zbog čega je direktiva prozvana „cookie law“.

Nova pravila su trenutačno u izradi i prva verzija je dana na čitanje u Parlament te je izazvala veliku nelagodu među industrijom. Za razliku od dosadašnjih verzija koje su bile direktive, nova će biti Uredba (kao i GDPR) što znači da odmah stupa na snagu, dok se direktiva mora ugraditi u lokalne zakone.

Sama uredba je prvenstveno namijenjena zaštiti osobnih podataka u elektroničkim komunikacijama što obuhvaća širok spektar usluga, od glasovnih poziva, weba, interneta (mail, apps, ...), instant poruka, OTT usluga, i slično. To također uključuje i spam, direktni marketing, telekom operatore, razvijatelje mobilnih aplikacija, online oglašavanje, ali između ostalog i Internet stvari.

U trenutačnom prijedlogu i dalje se govori o kolačićima koji bi trebali biti više korisnički orijentirani što znači da će svaki korisnik u svom pregledniku moći postaviti što želi dopustiti, a što ne i više svaka stranica neće trebati pitati navedena pitanja već će se automatski povlačiti dozvole iz postavki preglednika.

Vezano uz Internet stvari dio koji može usporiti razvoj je vezan uz članak 6 prijedloga Uredbe o e-privatnosti (dalje e-PR) koji propisuje uvjete dopuštenosti obrade elektroničkih komunikacijskih podataka, ne predviđa legitimni interes voditelja obrade kao jednu od dopuštenih osnova te upućuje da se obrada, čak i uz pristanak korisnika, treba, u pravilu, obavljati putem anonimizirane obrade informacija.

Zbog nemogućnosti za personalizirane usluge predloženi članak 6 e-PR može predstavljati ograničenje razvoja inovativnih usluga temeljenih na analizi velikih podataka.

U recitalu 12 e-PR pojašnjava se da se njezine odredbe odnose i na komunikaciju između strojeva: „Povezani uređaji i strojevi sve više međusobno komuniciraju služeći se elektroničkim komunikacijskim mrežama (internet stvari). Prijenos komunikacija između strojeva uključuje prijenos signala mrežom i stoga uobičajeno predstavlja elektroničku komunikacijsku uslugu“.

Kako bi se osigurala potpuna zaštita prava na privatnost i povjerljivost komunikacija te promicao pouzdan i siguran Internet stvari na jedinstvenom digitalnom tržištu, potrebno je pojasniti da bi se ova Uredba trebala primjenjivati na prijenos komunikacija među strojevima. Stoga bi se načelo povjerljivosti sadržano u ovoj Uredbi trebalo primjenjivati i na prijenos komunikacija između strojeva

Operatori elektroničkih komunikacija smatraju kako sam prijenos komunikacija ne ulazi u pitanje zaštite osobnih podataka pojedinaca sukladno GDPR-u, čime se sektor elektroničkih komunikacija prekomjerno regulira.

Iako industrija ima više primjedbi na e-PR i njegovu primjenu zajedno s GDPR-om, može se zaključiti kako se osnovna prepreka razvoju tržišta vidi u precizno postavljenom konceptu legitimne osnove za obradu elektroničkih komunikacijskih podataka koji ne uključuje pravo na obradu zasnovano na legitimnom interesu voditelja obrade.

Uz to, industrija problematičnim smatra i širenje odredbi e-PR i na komunikaciju između strojeva što je vidljivo na vrlo jednostavnom primjeru Fitbit narukvice za praćenje fitness treninga. Regulativa eksplicitno uključuje komunikaciju između strojeva, ali definira komunikacijski podatak kao tekst, glas, video, slike, zvuk ili metapodatke o navedenim sadržajima. Fitbit šalje čiste (sirove) podatke. To nije niti tekst, niti glas, niti video, niti zvuk, a sigurno nije niti metapodatak, ali se svejedno može i ne mora tretirati kao podatak.

Prema stavu industrije, već sam GDPR predstavlja značajno ograničenje. Stoga još strože odredbe iz e-PR nemaju opravdanje i mogu značajno usporiti razvoj Interneta stvari.

2.3. Mogući smjerovi regulacije

Definiranje konkretnih i specifičnih smjerova tehničkog i regulatornog razvoja je u ovom trenutku preuranjeno, pa se stoga mogućnosti i mjere za operacionalizaciju zakonodavstva mogu sagledati s visokog nivoa kako je prikazano u tablici 1[50].

Svaki od mogućih smjerova ima svoje rizike i prednosti. Isto se može primijeniti i na tehnologiju pristupa mreži, prijenosu podataka i sigurnosti.

Smjer „bez regulacije“: najveću prednost daje malim poslovnim subjektima na tržištu gdje bi do punog izražaja mogla doći inovativnost. Problem je što se na ovaj način postavlja pitanje smjera razvoja IoT-a jer ne postoji garancija da će razvoj IoT-a biti u skladu s ciljevima EU. Sa zakonske strane predstavlja najjednostavnije rješenje i za regulatore jer se postojeće zakonodavstvo ne mijenja.

Smjer „blaga regulacija/zakonodavstvo“: ovaj smjer tržištu još uvijek dopušta dovoljno slobode u odlučivanju o najefikasnijem smjeru ispunjavanja zahtjeva. Na taj način bi se inovativnost trebala zadržati na visokoj razini. Također, u slučaju dostatnog poticaja i razumijevanja politike, moguća je visoka uspješnost razvoja uz usklađenost smjera razvoja s ciljevima EU. Regulatori bi u tom slučaju imali dodatnog posla oko nadgledanja, te donosioci strategije razvoja oko inovacijske politike te industrijske politike.

Tablica 1 – sažetak politika razvoja

Opcije	Aktivnost EK	Uspješnost	Korisnost
Bez akcije	Postojeće aktivnosti se ne mijenjaju	Nema garancije da će razvoj IoT biti u skladu s EU ciljevima	Tržišni igrači zadržavaju slobodu na tržištu
"Blago" zakonodavstvo	Nadgledanje, inovacijska politika, industrijska politika	U slučaju dostatnog poticaja i razumijevanja, moguća je visoka uspješnost uz poticanje usklađenosti s ciljevima politike EU-a.	Tržišni igrači zadržavaju određenu slobodu u odlučivanju o najefektnijem načinu ispunjavanja zahtjeva
"Čvrsto" zakonodavstvo	Harmonizacija i regulacija područja vezanih uz IoT (e-commerce, zaštita podataka, itd.)	U ovisnosti o opsegu regulacije, obavezna usklađenost može biti vrlo efikasna	Obzirom na ranu fazu razvoja tehnologije teško je predvijeti negativne utjecaje te će ih se teško izbjeći kod definiranja legislative

Smjer „Čvrsta regulacija/zakonodavstvo“: budući da je IoT još u početnoj fazi razvoja, teško se mogu predvidjeti svi mogući negativni utjecaji, pogotovo kod inovacija, stoga će iste biti teško izbjeći kod postavljanja zakonodavstva. Usmjeravanje politike prema EU ciljevima na ovakav način je vrlo efikasan, ali ovaj smjer izaziva i velike promjene u zakonodavstvu, pogotovo kod harmonizacije i regulacije područja vezanih uz IoT (e-commerce, zaštita podataka i slično).

2.4. Preporučeni smjer

Usporedbom učinkovitosti, djelotvornosti i usklađenosti predloženih regulatornih politika, pristup „blagog zakonodavstva“ je barem u bližoj budućnosti najbolji način da se stvori prostor za razvoj IoT-a, ubrza i unaprijedi tržište IoT-a te odgovori na nadolazeće izazove.

U tom bi slučaju Europska komisija trebala imati središnju ulogu u koordiniranju dijaloga vezanih uz IoT politiku kako bi se osiguralo sljedeće[50]: 1) zajedničko razumijevanje te potaknule koherentne i učinkovite mjere po sektorima, regijama i područjima politike; 2) podrška za smislene programe digitalne pismenosti i podizanje svijesti o IoT-u čime će se osnažiti samoregulacija i poboljšati individualna interakcija s IoT-om; 3) podrška i promicanje razmjene znanja, istraživanja i vrednovanja projekata zajedno s financiranjem te kontinuirana rasprava i objašnjavanje razvojne politike pogotovo vezane za identifikaciju, privatnost i etiku u IoT okruženju.

Iako etička povelja[50] može biti korisna komponenta samoregulacije, podrška općem pristupu nije izgledna u ovom trenutku. Cilj etičke povelje je zaštita vitalnih interesa potrošača u IoT okolini te vodič za razvijatelje IoT okolina i usluga. Kao privremena mjera, predlaže se stvaranje europskog etičkog tehnološkog brenda ('Ethical Tech' brand)[50] koji bi mogao potaknuti inovatore i pružatelje usluga da razviju etičku tehnologiju u skladu s potrebama tržišta i krajnjih korisnika. Na taj način krajnji korisnici bi mogli vidjeti koji brendovi se drže visokih etičkih standarda i na temelju toga odlučivati čije proizvode žele kupovati.

2.5. Praćenje i implementacija

Podaci potrebni za praćenje razvoja IoT-a i usluga za pametne gradove su fragmentirani i teško iskoristivi, stoga problem previše, premalo i nepouzdana informacije mogu usporiti daljnji razvoj. Očekuju se daljnje promjene u procesu praćenja razvoja IoT-a i usluga za pametne gradove kao i veliko povećanje količine podataka za praćenje o tome što se s IoT uslugama događa.

Kako bi se mogla razvijati i provoditi odgovarajuća fleksibilna i održiva politika IoT-a, problem previše podataka mora biti prevladan. U tom smislu, pozitivna je okolnost da različite upravljačke domene koje utječu i na koje utječe IoT pojedinačno prikupljaju i analiziraju prikupljene podatke. To stvara osnovu za koordinirani pristup izradi politike s jasno organiziranom informacijskom strukturom. Takav pristup bi omogućio praćenje utjecaja IoT-a u područjima koja ne mogu biti direktno mjerena, poput etike, privatnosti i sigurnosti te bi trebala dovesti do zajedničkog stvaranja politike kao i boljeg razumijevanja problematike. Informacije bi se trebale koristiti za stvaranje kvalitetnih scenarija za zajedničko istraživanje

nastajanja IoT-rješenja usmjerenih građanima. Kao i uvijek, važno je uspostaviti specifične i mjerljive indikatore koji podupiru predmetno praćenje.

3. PREGLED TEHNIČKIH I REGULATORNIH OBILJEŽJA USLUGA PAMETNIH GRADOVA

Veliki broj različitih IoT usluga se koristi u različitim područjima primjene, od ekologije i nadgledanja okoliša do sektora vlade te od usluga orijentiranih građanima do usluga orijentiranih tehnologiji. Samo neke od najčešće korištenih usluga navedene su u tablici 2.

Tablica 2: Popis usluga prema područjima primjene

Pametna kuća	Pametn grad	Okolina	Maloprodaja	Logistika	Industrija	Poljoprivreda
Upravljanje energijom	Pametno parkiranje	Meteorološka mjerenja	Upravljanje inventarom	Praćenje flote	Dijagnostika strojeva	Pametno navodnjavanje
Pametni uređaji	Upravljanje otpadom	Nadgledanje buke	Pametno plaćanje	Praćenje paketa	Praćenje objekata i automatizacija procesa	Praćenje usjeva
Otkrivanje provala	Hitni odgovori	Detekcija šumskih požara	Pametni automati za prodaju	Udaljena dijagnostika vozila		
Detekcija plinova ili dima	Pametna rasvjeta	Nadgledanje zagađenost i zraka		Generiranje i raspored ruta		

Trenutačno na tržištu prevladavaju vertikalno orijentirana samostalna rješenja. Takva rješenja su obično ograničena na ekosustav koji se može graditi isključivo oko jedne IoT-platforme [69]. Vertikalna rješenja, između ostalog, ne dijele infrastrukturu i generirane podatke između sebe, iako bi se navedena infrastruktura i podaci mogli koristiti i od strane nekih drugih usluga (na primjer, temperatura i koncentracija CO₂ su vrlo bitni u sustavima nadzora kvalitete zraka, ali također se mogu koristiti za izračun zelenih ruta za bicikliste ili sustave navodnjavanja parkova). Upravo iz tog razloga potrebna je klasifikacija usluga prema njihovim obilježjima kako bi se bolje razumjeli tehnički, ali i regulatorni zahtjevi tih usluga. U

ovom poglavlju su identificirana tehnička i regulatorna obilježja usluga pametnih gradova koja trebaju biti dobro postavljena kako bi se razvile uspješne IoT usluge u kontekstu pametnih gradova, ali i kako bi se ispunili zakonski i tehnički zahtjevi koji su trenutačno na snazi ili bi mogli biti postavljeni kao regulatorni zahtjevi u bliskoj budućnosti. Na temelju detaljno provedene analize usluga pametnih gradova razlikujemo i klasificiramo njihova tehnička i regulatorna obilježja.

3.1. Tehnička obilježja usluga pametnih gradova

Tehnička obilježja usluga pametnih gradova su uglavnom vezana uz kvalitetu usluge (engl. *Quality of Service*, QoS) i druge tehničke parametre koji su strogo vezani uz mrežu ili dizajn usluga pametnih gradova.

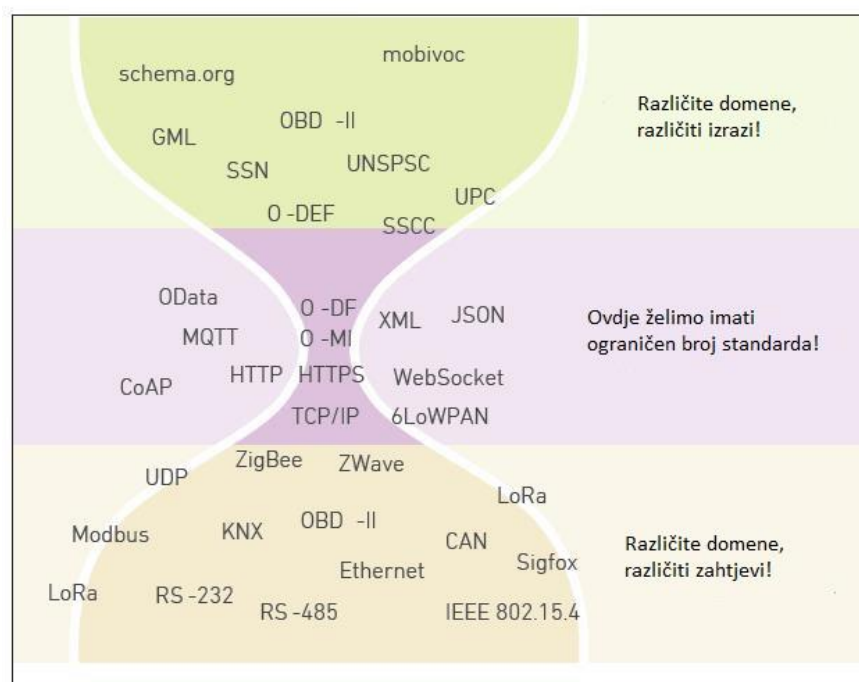
Sama tehnička obilježja mogu biti vezana uz uređaj, mrežu, platformu ili samu uslugu. Neka od tehničkih obilježja su zajednička, odnosno, koriste se u gotovo svim uslugama. U ovom poglavlju objasniti ćemo ključna tehnička obilježja, a kasnije ćemo razjasniti kako se ona uklapaju u pojedine dijelove usluga.

Tehnička obilježja koja se koriste u uslugama pametnih gradova, bez obzira govorimo li o uređaju, mreži, platformi ili usluzi su:

- Broj krajnjih korisnika: stvaran broj krajnjih korisnika (na primjer građana) koji će koristiti uslugu. Obilježja usluge značajno ovise o broju korisnika usluga. Neke usluge se temelje na velikom broju korisnika koji generiraju podatke i informacije (na primjer usluga waze koja sugerira prometne gužve u gradu), dok kod drugih usluga koje nisu predviđene za velik broj korisnika svako povećanje predstavlja problem izuzev usluga gdje su korisnici samo konzumenti podataka i informacija te stoga ne generiraju podatke i informacije nego ih samo koriste.
- Broj IoT uređaja: broj IoT uređaja koji će generirati podatke sa senzora ili će biti korišteni kao aktuator (na primjer ekran za prikaz broja slobodnih parkirnih mjesta u ulici ili garaži). Broj IoT-uređaja značajno utječe na dizajn i arhitekturu same usluge. Naime, što je veći broj uređaja generirati će se veći promet što predstavlja veće zahtjeve na mrežu, ali ujedno predstavlja i veliku količinu podataka za analitiku. Povećanjem uređaja treba povećati i propusnost usluge, diskovni prostor, ali i procesorsku snagu koja se koristi za njihovu obradu.

- Količina podataka: predstavlja kompletan volumen generiranih podataka po pojedinačnoj usluzi koja generira promet prema poslužiteljima gdje je smještena IoT platforma. Većina usluga pametnog grada generira vrlo malu količinu prometa (svega nekoliko kb), međutim postoje i specifične usluge koje zahtijevaju veće kapacitete propusnosti poput video nadzora kada nastaju velike količine podataka budući da se prema udaljenim lokacijama šalju video zapisi.
- Vremenska osjetljivost: neke usluge su osjetljive na kašnjenje u prijenosu podataka, poput usluga vezanih uz zdravstvo (e-zdravlje) ili autonomna vozila. Kod takvih usluga vrlo je važno reagirati promptno i trenutačno na određeni događaj i zbog toga je nužan uvjet za ovakvu uslugu imati uslugu dostupnu u stvarnom vremenu uz vrlo učinkovitu obradu podataka. Na primjer, medicinsko osoblje mora reagirati na vrijeme u slučaju detekcije kritičnog stanja pacijenta.
- Lokacijske usluge: ukoliko usluga ovisi o lokaciji, onda je vrlo bitno i predvidjeti takvu mogućnost te definirati je li potrebno pozicioniranje unutarnje ili vanjske lokacije. Dodatno, potrebno je identificirati odgovarajuće metode pozicioniranja za pojedinu uslugu. Na primjer, u slučaju usluge pametnog parkiranja precizna lokacija vozila je potrebna kako bi usluga mogla ponuditi odgovarajuće parkirno mjesto. Još jedna usluga koja zahtjeva vrlo precizno lociranje korisnika je pan-europska usluga eCall koja u slučaju nesreće javlja lokaciju korisnika. Ovo je posebno bitno jer u slučaju nesreće na autocestama potrebno je znati i smjer kretanja, a svaka minuta može puno značiti u spašavanju života.
- Naplata: usluge pametnih gradova mogu biti besplatne za krajnje korisnike ili se u nekim scenarijima mogu naplaćivati. Na primjer, moguća je mjesečna pretplata, naplata po korištenju i sl...). Gradovi usluge vezane uz gradske službe u pravilu ne naplaćuju, ali postoje i usluge koje se naplaćuju. Na primjer, parking i prijevoz se naplaćuje, ali je mobilna aplikacija za navigaciju ili vozni red u stvarnom vremenu besplatna.
- Skalabilnost: predstavlja mogućnost širenja kapaciteta usluga za povećani broj korisnika i umreženih uređaja. Naime, većina gradova počinje uvođenje novih usluga pilot projektima na manjim gradskim područjima te se postepeno usluga širi na ostatak grada. Iz tog razloga potrebno je prilikom dizajna softverske arhitekture predvidjeti mogućnost budućeg širenja usluge u pogledu povećanog broja i uređaja i krajnjih korisnika.

- Otvorenost platforme i interoperabilnost: najveći broj usluga pametnih gradova koje su danas implementirane u gradovima i dostupne za građane su rješenja temeljena na zatvorenim, vlasničkim rješenjima koja nisu međusobno kompatibilna te su implementirana isključivo kao samostalna rješenja. Takva rješenja najčešće koriste vlastite podatkovne modele koje druge usluge ne mogu razumjeti niti prepoznati te zbog toga proces integracije uređaja i podataka duž cijele domene, ali i IoT usluga postaje zapreka. Interoperabilnost usluga i uređaja jedan je od ključnih zahtjeva koje je potrebno implementirati kako bi se problem „zaključavanja“ na jednog dobavljača riješio. Danas postoje različiti standardi i standardizacijska tijela za pojedine segmente IoT-rješenja, ali to je potrebno suziti kako bi se u budućnosti usluge i uređaji na svim razinama jednostavno razumjeli. Na slici 20 vidi se prikaz brojnih standarada koji se danas koriste u IoT-rješenjima na različitim nivoima IoT složaja. Također, dok je interoperabilnost na tehničkoj razini širokom primjenom standardnih komunikacijskih protokola (npr. MQTT i CoAP) dobro riješena, interoperabilnost na semantičkoj i organizacijskoj razini i dalje predstavlja izazov. Kako bi postigli masovnije postavljanje i prihvaćanje usluga pametnih gradova, gradovi trebaju zahtijevati otvorene i interoperabilne infrastrukture i softverska rješenja koja se lako mogu integrirati s drugim rješenjima te na taj način stvoriti usluge koje koriste više platformi i pokrivaju više domena (npr. promet i nadgledanje okoliša). IoT platforme bi trebale otvoriti jednostavna i jednoznačna sučelja kako bi različite inovativne usluge i aplikacije mogle jednostavno koristiti i integrirati IoT uređaje i pripadajuće podatke upravljane od strane različitih IoT platformi. Ovo će uistinu stvoriti ekosustav usluga pametnih gradova, a programski okvir koji nudi funkcionalnost interoperabilnosti implementiran je u sklopu projekta symbIoTe financirano iz programa Obzor 2020 [70].



Slika 20: Različiti standardi na svim razinama [71]

Osim nabrojanih tehničkih karakteristika koje su zajedničke gotovo svim uslugama i uređajima, postoje i tehničke karakteristike koje su specifične za uređaje:

- **Komunikacijski model:** prilikom oblikovanja šireg gradskog rješenja, gradski planeri trebaju uzeti u obzir potrebnu komunikacijsku infrastrukturu kako bi osigurali da IoT uređaji imaju pristup Internetu, ali istovremeno trebaju uzeti u obzir i geografska obilježja gradskog područja. U ovisnosti o tim obilježjima trebaju odlučiti hoće li koristiti bežičnu ili žičanu komunikacijsku mrežu. Ukoliko se rade rekonstrukcije gradskog središta zbog npr. mijenjanja cijevi ili kanalizacije, onda je logično predvidjeti i postavljanje kableske kanalizacije kroz koju se mogu upuhati svjetlovodne niti za žičanu komunikaciju, a koja zasigurno predstavlja dugoročno rješenje. Međutim, ukoliko takve rekonstrukcije nisu planirane u bližoj budućnosti, onda je bežična mreža logičan slijed. Danas je na tržištu dostupan velik broj konkurentskih protokola i komunikacijskih tehnologija na sloju podatkovne poveznice i stoga bi za buduću uporabu barem dio standardiziranih opcija trebao biti podržan.
- **Računalne sposobnosti:** u ovisnosti o ovoj sposobnosti logika i operacije usluge mogu se dramatično mijenjati. U slučajevima kada uređaj ima dovoljno računalne (procesorske) snage neke logičke operacije i jednostavniji algoritmi

moгу se odrađivati na samom uređaju te na taj način smanjiti potrebu za komunikacijom prema poslužiteljima na kojima se nalazi platforma. S druge strane, osim što će to vjerojatno uzrokovati povećanje cijene uređaja, oni će trošiti i više električne energije. Iz tog razloga vrlo je bitno dobro i pažljivo procijeniti (odnosno izračunati) je li za pojedinačnu uslugu bolje da se računalna obrada izvodi na samom uređaju uz veću potrošnju energije ili će se analize i algoritmi raditi u oblaku ili na krajevima mreže.

- Potrošnja električne energije: predstavlja jednu od ključnih karakteristika svakog uređaja, pa tako i IoT uređaja. Danas su uređaji većinom napajani preko baterija te zahvaljujući sve boljoj efikasnosti uređaja i njihovim mogućnostima operacijskog moda slabog napajanja, kao i unaprijeđenih kapaciteta baterija, trajanje „života“ uređaja je znatno poboljšano. Međutim, neki uređaji zbog svojih karakteristika potrošnje i dalje trebaju biti napajani preko glavnog izvora napajanja, odnosno trebaju biti priključeni na stalan izvor električne energije. U zadnje vrijeme može se vidjeti i pojava tehnologije prikupljanja energije u kombinaciji s uređajima male snage, što daje vrlo dobre rezultate i osigurava dugi životni radni vijek uređaja [72].
- Izvor napajanja: izvor napajanja uređaja može biti baterijski ili stalan priključak na električnu mrežu ili može koristiti tehnologiju prikupljanja električne energije.
- Lokacija: ukoliko je neka od usluga lokacijski orijentirana, u tom slučaju je potrebno znati lokaciju uređaja, za što je potrebno koristiti npr. dodatan GPS čipset koji će se nalaziti na uređaju ili će se prilikom postavljanja svakog uređaja koji je statičan ručno zapisivati njegova lokacija. Primjerice, lokacija je ključna za uslugu pametnog parkiranja gdje usluga mora znati lokacije svakog senzora koji prati zauzeće parkirnog mjesta, a kako bi korisnika (čiju lokaciju također mora znati) mogla navoditi na odgovarajuće parkirno mjesto.

Postoje i tehnička obilježja koja su vezana uz povezivost svakog IoT uređaja koja uključuju:

- Jednosmjerna / dvosmjerna komunikacija: prilikom dizajna usluge bitno je razjasniti je li potrebna dvosmjerna komunikacija između IoT uređaja i poslužitelja što može značiti dodatni promet, ali i funkcionalnosti.

- Propusnost: vrlo je važno na temelju zahtjeva usluge dobro procijeniti brzinu prijenosa podataka između uređaja i IoT platforme (na primjer, video nadzor zahtjeva veću propusnost).
- Kašnjenje: neke usluge su vrlo osjetljive na kašnjenje kod zaprimanja informacija. Na primjer, usluge koje se temelje na podacima u stvarnom vremenu mogu drugačije reagirati zbog kašnjenja u mreži. Uzmimo za primjer uslugu navođenja do parkirnog mjesta. Ukoliko dođe do kašnjenja prijenosa podataka, može se korisnika navoditi do mjesta koje je već popunjeno.
- Jitter: ova karakteristika nema utjecaja na većinu usluga pametnih gradova, međutim, za neke specifične usluge može imati značajan utjecaj. Primjer usluga koje su osjetljive na jitter su video usluge ili online igre.
- Gubitak podataka: neke usluge vrlo su osjetljive na gubitak podataka i zbog toga je potrebno predvidjeti posebne mehanizme koji će osigurati da ne dođe do gubitaka (na primjer re-transmisija) podataka. Međutim, čak i bez takvih mehanizama neke usluge mogu funkcionirati ispravno i mogu biti dizajnirane da budu otporne na gubitak podataka.

Za poduzeća ili osobe koje se bave razvojem ili dizajnom usluga pametnih gradova važno je identificirati sva tehnička obilježja IoT uređaja, mreže i IoT platforme koja će se koristiti kako bi ih mogli mapirati na samu uslugu.

3.2. Regulatorna obilježja usluga pametnih gradova

Regulatorna obilježja su većinom vezana uz zakonske i podzakonske propise koji se odnose na specifične usluge pametnih gradova. Ona su najčešće unaprijed propisana od strane vlade, EU direktiva ili uredbi koje su primjenjive na sve zemlje članice. Najkritičnija obilježja usluga vezana su uz sljedećih sedam (7) obilježja:

- Zakonsko presretanje poziva: većina zemalja ima zakon koji propisuje mogućnost presretanja podatkovnog prometa, glasovnih poziva, SMS/MMS poruka ili u novije vrijeme i poruka preko OTT kao što su Viber, Whatsapp, Telegram, Signal i slični.

- Pouzdanost usluge: mogućnost izbjegavanja grešaka kod usluga koje se često ponavljaju i težeg su oblika nego je to dopustivo.
- Zaštita osobnih podataka: jedno od temeljnih prava EU nalaže da građani Europske Unije imaju pravo zaštite svojih osobnih podataka.
- Sigurnost: odnosi se na zaštitu IoT uređaja i usluga od kibernetičkih napada. IoT uređaji su povezani na mrežu i vrlo često su nezaštićeni te se preko njih mogu izvršiti napadi i upadi u druge, veće mreže.
- Promjena operatora (pružatelja usluge): mogućnost krajnjeg korisnika i/ili IoT korisnika da izvrši prebacivanje kompletne usluge i/ili platforme i/ili povezivosti na drugog pružatelja.
- Roaming: mogućnost korištenja usluge nakon što se napusti nacionalna mreža, odnosno kada je IoT uređaj registriran u gostujućoj mreži. Ova karakteristika je većinom vezana uz usluge transporta i logistike.
- Interoperabilnost i otvorenost prema podacima i uslugama: kao i kod tehničkih obilježja ova značajka važna je i za regulatornu domenu te se odnosi na međusobnu komunikaciju više različitih uređaja, platformi ili usluga. Interoperabilnost u regulatornom smislu se prvenstveno odnosi na javno financirane usluge pametnih gradova i blisko je povezano s promjenom pružatelja usluge.

Nacionalno zakonodavstvo u mnogim zemljama svijeta nameće potrebu za omogućavanje zakonskog presretanja podatkovnog prometa, glasovnih poziva, SMS/MMS poruka, a u novije vrijeme i poruka preko OTT kao što su Viber, Whatsapp, Telegram, Signal, Messenger i slični. Opravdanje za takvo zakonodavstvo pronalazi se u pitanjima nacionalne sigurnosti. Ovo pitanje nije novo i u davna vremena s početka razvoja elektroničkih komunikacijskih usluga pozivi, odnosno, telegrafi su se nadgledali za potrebe zakona. To je vidljivo i iz uvodne priče o Western Unionu kojeg je politički vrh SAD-a želio oslabiti jer su se bojali njegove mogućnosti i kontrole presretanja i izmjena poruka. Međutim, dio vezan uz presretanje prije svega podataka je dodatno zakompliciran u slučaju Interneta stvari budući da arhitektura Interneta stvari dopušta i omogućava povezivanje stvari diljem svijeta u jednu uslugu ili jednu platformu. Stoga se postavlja otvoreno pitanje tko ima pravo i kome je dopušteno presretati podatke Interneta stvari? Zakonski gledano, usluga može biti smještena u jednoj državi i to obično tamo gdje se nalazi i poslužitelj, međutim, uređaji mogu biti

razmješteni duž više zemalja ili se uređaji mogu nalaziti u vozilima ili paketima koji prolaze kroz više različitih država. Dodatno, ukoliko se usluga nalazi u jednoj zemlji, a pružatelj usluge je multinacionalna kompanija koja zbog smanjenja troškova proizvodnje uređaja koristi SIM kartice jedne države bez obzira u kojoj od država će usluga biti pružana (odnosno cijela grupacija u tom slučaju koristi isti brojevni raspon). Na primjer, ukoliko usluga koja se pruža u Republici Hrvatskoj koristi strani broj, nacionalno tijelo zaduženo za provođenje funkcije tajnog nadzora gdje se, između ostalog, nalazi i zakonsko presretanje neće biti u mogućnosti dohvatiti IP adresu korisnika budući da uređaj dobiva IP adresu od GGSN entiteta u domaćoj mreži, a to je u ovom slučaju strana mreža (npr., Austrija, Njemačka ili Švedska) gdje hrvatske službe nemaju nikakvih zakonskih mogućnosti. Zbog navedenog ovo predstavlja ozbiljan problem i pitanje nacionalne sigurnosti može biti ugroženo. Koliki problem ovo predstavlja za nacionalnu sigurnost vidljivo je zadnjih godina kod migrantskih kriza i terorističkih napada koji su se događali diljem Europe. Naime, većina izbjeglica služi se pametnim telefonima, a za komunikaciju koristi OTT aplikacije koje su kriptirane s kraja na kraj. Jednom kada unutar EU kupe karticu mogu se kretati po cijeloj Europskoj uniji i koristiti OTT aplikacije bez da ih više mijenjaju. Na taj način njihova komunikacija ostaje zaštićena, a njihovo praćenje onemogućeno jer tijelo npr. iz Hrvatske ne može nadzirati osobu u Austriji i obratno.

Korištenje broja izvan zemlje u kojoj se nalazi pružatelj usluge, odnosno, izvan zemlje gdje je usluga kupljena, naziva se Roaming usluga. Usluga Roaming je stvorila veliki izazov za pružatelje usluga u Europi, međutim, Europska komisija je odlučila da za dobrobit EU i svih njenih građana sve države Europske Unije moraju djelovati kao jedno tržište (poznatije kao jedinstveno Europsko tržište) i stoga su donijeli Strategiju jedinstvenog digitalnog tržišta za Europu [63]. Kroz ovu strategiju Europska komisija je uvela pravilo „*Roam like at home*“. Tim pravilom kada korisnik koristi svoj mobilni uređaj za vrijeme puta izvan svoje domaće mreže, a unutar bilo koje druge države EU, ne mora platiti dodatne troškove za Roaming. Od ovog pravila koristi imaju svi građani EU kada pozivaju, šalju tekstualne poruke ili koriste podatkovni promet dok su u inozemstvu. Ovo Roaming pravilo [62] je dovelo i do razvoja IoT usluga budući da više nema Roaming troškova. Međutim, iako nema dodatnih troškova uvedena su pravila poštenog korištenja usluga koja su propisana Uredbom (EU)2016/2286 [73] poput toga da se mora više vremena kvartalno provesti u domaćoj mreži nego u inozemstvu. Za usluge Interneta stvari na fiksnim lokacijama ovo znači da multinacionalne kompanije koje smo spomenuli u dijelu zakonskog presretanja ne mogu koristiti jedan brojevni raspon (od jedne države) za sve IoT uređaje koji su postavljeni u različitim državama, odnosno po ovome će u

svakoj zemlji morati koristiti brojevni raspon te države ili će morati koristiti posebne IoT/M2M SIM kartice dodjeljene od strane ITU organizacije koje su skuplje, ali vrijede na području cijelog svijeta. U tom kontekstu, pružatelji usluga će morati prilikom dizajna same usluge obratiti pažnju na prirodu usluge kako bi se odabrao odgovarajući komunikacijski kanal, a da im pravila Roaming regulacije ne ograniče korištenje usluge.

Pouzdanost usluge je vrlo blisko povezana sa sigurnošću i predstavlja mogućnost isporuke usluge kojoj se može vjerovati, odnosno, na drugi način se može reći da je pouzdanost sustava sposobnost izbjegavanja kvarova usluge koji se ponavljaju i nisu prihvatljivi. Budući da pouzdanost vrlo često dolazi ruku pod ruku sa sigurnošću, imaju i zajedničke atribute.

Slika 21 prikazuje od kojih atributa se sastoji oslonjivost, koje su prijetnje na oslonjivost, sredstva kojima se brani i povezanost oslonjivosti sa sigurnošću.



Slika 21: Prikaz atributa pouzdanosti i poveznica sa sigurnošću

Kao što se može vidjeti i na slici 21, oslonjivost obuhvaća attribute raspoloživosti (engl. *Availability*), pouzdanosti (engl. *Reliability*), zaštite (engl. *Safety*), povjerljivosti (engl. *Confidentiality*), cjelovitosti (engl. *Integrity*) i održivosti (engl. *Maintainability*).

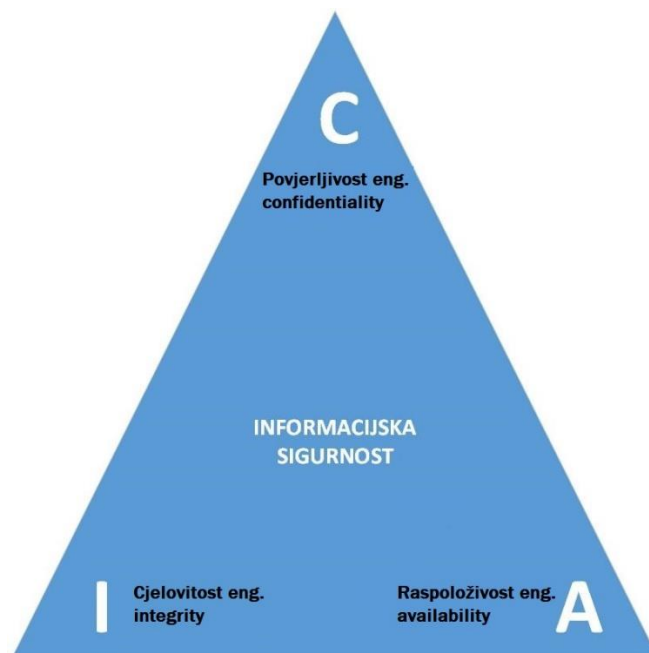
U ovom kontekstu pouzdanost sustava odnosi se na kontinuiranost usluge koja radi bez kvarova, odnosno, možemo reći da je pouzdanost usluge sposobnost sustava da isporuči uslugu

kako je i specificirano npr. 99,99% vremena. Zaštita (engl. *safety*) upućuje na izostanak ozbiljnih, odnosno katastrofalnih posljedica za korisnika i okolinu. Može se definirati i kao sposobnost sustava da djeluje bez katastrofalnih kvarova. Održivost (engl. *maintainability*) je sposobnost sustava ili usluge da nastavi normalno raditi bez kvarova i nakon modifikacija i popravaka.

Tri atributa su posebno izdvojena i o njima se vodi posebno računa budući oni direktno utječu na sigurnost usluge, odnosno sustava. Sigurnost sama po sebi predstavlja sposobnost sustava da se obrani od slučajnih ili namjernih upada.

Sigurnost je posebna grana IKT-a i kada govorimo o sigurnosti u svijetu Internet stvari, u stvari govorimo o Informacijskoj sigurnosti. Ona predstavlja skup procesa koje organizacija provodi radi zaštite informacijskih sustava i podataka od neovlaštene promjene, pristupa ili otkrivanja te osigurava kontinuitet poslovanja i obuhvaća ljude, procese, organizaciju i tehnologiju.

Tri osnovna načela na kojima počiva informacijska sigurnost su povjerljivost, cjelovitost i raspoloživost, koji se prema akronimu engleskih riječi još nazivaju i trijada CIA [74]. Slika 22 prikazuje osnovna načela informacijske sigurnosti.



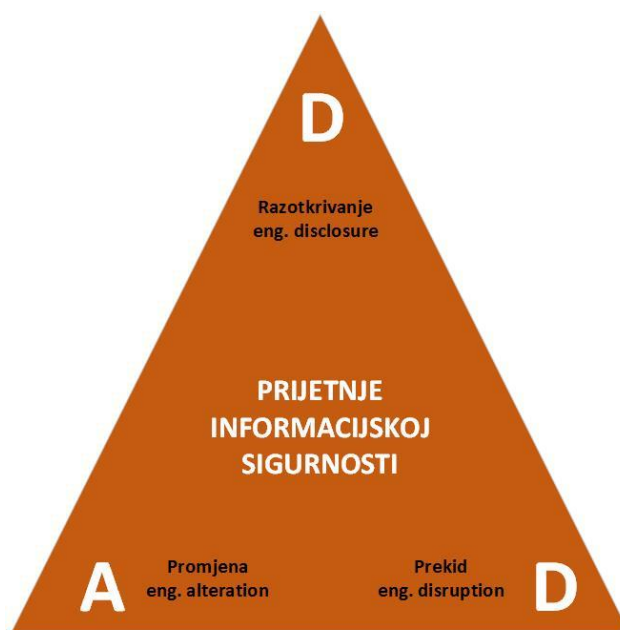
Slika 22: Osnovna načela informacijske sigurnosti

Načelo povjerljivosti (engl. *confidentiality*) označava osiguravanje tajnosti informacija tj. da se određena informacija može pročitati samo ako sve strane koje joj pokušavaju pristupiti imaju potrebne vjerodajnice. Povjerljivost se osigurava kroz kontrolu fizičkog i logičkog pristupa te upotrebom enkripcijskih algoritama. Kontrola fizičkog i logičkog pristupa počiva na ograničenju pristupa štićenim informacijama dok se upotrebom enkripcijskih algoritama informacija čini nečitljivom ukoliko se pri pristupanju ne upotrijebe odgovarajuće vjerodajnice. U praksi se često istovremeno provode sve tri vrste kontrole.

Načelo cjelovitosti (engl. *integrity*) označava zaštitu informacija od neovlaštene promjene u mirovanju ili prilikom transporta, bilo od osoba ili od strane malicioznog koda. Cjelovitost garantira da je primljena informacija u istom obliku i s istim sadržajem kakva je bila i u trenutku slanja.

Načelo raspoloživosti (engl. *availability*) označava osiguravanje dostupnosti informacija tj. da će pristup informacijama biti moguć u trenutku kada je on potreban osobi ili sustavu. Osiguravanje raspoloživosti informacija podrazumijeva i osiguranje raspoloživosti informacijskih sustava i servisa.

Uz načela informacijske sigurnosti potrebno je spomenuti i prijetnje osnovnim načelima informacijske sigurnosti koje su predstavljene kroz tzv. trijadu DAD. Načela informacijske sigurnosti se brinu da DAD trijada ne uspije zaustaviti rad usluge. Na slici 23 prikazane su prijetnje osnovnim načelima informacijske sigurnosti.



Slika 23: Prijetnje načelima informacijske sigurnosti

Prijetnja otkrivanja (engl. *disclosure*) je prijetnja povjerljivosti. Napadi na povjerljivost su mnogobrojni i mogu se definirati kao otkrivanje zaštićene informacije zaobilaženjem fizičkih i logičkih kontrola pristupa, otkrivanjem ključa enkripcije ili pobjeđivanjem enkripcijskog algoritma.

Prijetnja promjene (engl. *alteration*) je prijetnja cjelovitosti i predstavlja mijenjanje informacije u jednom dijelu ili cijelosti ili njeno brisanje.

Prijetnja prekida (engl. *disruption*) je prijetnja raspoloživosti informacije ili cijelog sustava. Raspoloživost može biti narušena na više načina: virusom, kvarom, napadom uskraćivanja usluge (DOS ili DDOS napadi) i slično.

Pitanje sigurnosti vrlo je važno ozbiljno shvatiti jer već prilikom prve pojave povezivanja uređaja na internetu, počeli su se javljati i sami napadi. Stuxnet se smatra prvim kibernetičkim oružjem koje su zajedno razvile američke i izraelske vojne snage. Stuxnetov maliciozni kod je ušao u Iransku nuklearnu elektranu tijekom 2010. godine te je namijenjen sabotazi PLC sklopova koji su prouzrokovali samouništenje dijelova postrojenja (centrifuge za odvajanje urana) neophodnih za obogaćivanje urana. Stuxnet se inicijalno širio preko MS Windows OS-a te je bio namijenjen za napad na PLC sklopovlje proizvođača Siemens. Iako ga klasificiraju kao crva, sam kôd se sastoji od više modula, jedan za širenje koda, drugi dio koda sadrži maliciozan sadržaj za PLC te treći modul koji je namijenjen za prikrivanje Stuxnet-a. Napad je prvi uočio Symantec (proizvođač sigurnosne opreme) koji je prijavio da je 60% računala u Iranu zaraženo određenom vrstom malicioznog koda no to nije ugrozilo operacije niti jednog računala. U to vrijeme jedino je nuklearna elektrana u Iranu prijavila oštećenja, iako se nije znao razlog. Drugi primjer takvih napada dogodio se u Ukrajini. Napad na elektranu u Ukrajini (23.12.2015.) prouzročio je nestanak struje za skoro pola regija u Ukrajini (oko 1.4 mil stanovnika) u razdoblju od nekoliko sati. Činjenica da se radi o ciljanom napadu i činu kibernetičkog napada kritične infrastrukture, govori da se nije radilo o izoliranom napadu već o napadu koji je bio kampanjski ciljan na sve distributere el. energije. Napad je nazvan trojanskim konjem BlackEnergy koji je bio pušten preko malicioznog makroa u office dokumentu. Ovaj trojanski konj omogućio je puštanje malicioznog koda Win32/KillDisk i nevidljiv pristup sustavima koji upravljaju kritičnom infrastrukturom koji su dalje s udaljene lokacije srušili operacije elektrane. Međutim jedan od najkritičnijih napada dogodio se u 2018. godini kada je skupina hakera upala u sustav Londonskog vodovoda i nekoliko dana

kontrolirala razinu tlaka u cijevima čime je dostup vode za građane bi značajno smanjen. Napadači su otkriveni tek nakon nekoliko dana, a u međuvremenu nitko nije uspio otkriti uzrok kvara ventila.

Uspjeh ovakvih napada sam po sebi govori koliko je važno shvatiti sigurnosna pitanja prilikom dizajna arhitekture usluga pametnih gradova.

Jedno od regulatornih obilježja koje kroz vrijeme može značajno utjecati na razvoj usluga pametnih gradova je promjena operatora, što se ne odnosi samo na pružatelje usluge mreže elektroničkih komunikacija, nego i na pružatelje usluge IoT platforme pa čak i integratora. Naime, ukoliko pružatelj usluge koristi vlastita i zatvorena rješenja, to predstavlja prepreku za promjenu pružatelja usluge kao i negativne posljedice koje ona donosi. Ovo je u svijetu poznato kao „lock-in“ problem budući da je tehnički vrlo zahtjevno zamijeniti takva rješenja bez dodatnih ulaganja. Međutim, promjena pružatelja usluge treba biti omogućena, a kod reguliranih usluga elektroničkih komunikacija je čak i obveza i kao takva do sada nije bila analizirana u praksi. Ovaj zahtjev je još jedan snažan argument u korist standardiziranih, otvorenih i interoperabilnih rješenja koja trebaju biti razmještena na svim slojevima IoT stoga za usluge pametnih gradova. Otvorenost podataka i usluga vrlo je blisko povezana s interoperabilnošću. Kako bi se ubrzalo razmještanje usluga pametnih gradova, one trebaju biti interoperabilne, pogotovo u gradovima koji su već započeli svoju digitalnu transformaciju. Kod takvih gradova vrlo je teško započeti integraciju usluga budući da je promjene potrebno napraviti u svim segmentima, što iziskuje značajna financijska sredstva. Ponekad zna biti povoljnije nabaviti novu uslugu koja će u startu ispunjavati potrebe Interneta stvari (otvorenost i interoperabilnost), nego vršiti konstantne nadogradnje nad postojećim sustavima. S druge strane otvaranje podataka i usluga prema drugim zainteresiranim stranama može rezultirati s brojnim zanimljivim inicijativama i idejama za nove usluge pametnih gradova. Možemo vidjeti vrlo uspješne primjere Europskih gradova, poput Barcelone, Santandera i Amsterdama, koji su stvorili vitalan ekosustav inovativnih aplikacija za građane.

Slijedeći Uredbu o zaštiti osobnih podataka koja je stupila na snagu 25. svibnja 2018. godine, kao i Uredbu o e-privatnosti koja bi prema navodima Europske komisije uskoro trebala biti dostupna i stupiti na snagu, veliki trud će biti ulož u zaštitu osobnih podataka. Obje zakonske regulative su temeljene na sigurnosnim obilježjima vezanim uz informacije, odnosno na informacijskoj sigurnosti. Uredbe postavljaju zahtjeve da postojeća infrastruktura u

gradovima bude dostupna i da se podaci otvore građanima. Budući da je u stvarnosti većinom infrastruktura u gradovima razmještena i u vlasništvu gradova, problem se odnosi na podatke koje je pružatelj IoT usluge prikupio i koji tvrdi da je vlasnik navedenih podataka. Dodatno, i sami građani mogu generirati značajnu količinu podataka vezanu uz njihovu okolinu korištenjem usluga koje opažaju okolinu u pokretu (engl. *Mobile Crowd Sensing*, MCS). Dakle, postavlja se pitanje tko je u stvari vlasnik tih IoT podataka? Tko ima pravo na njihovo korištenje i tko ima pravo pristupa infrastrukturi prema ulogama u lancu vrijednosti? Na primjer, kod gradskog masovnog prikupljanja podataka za nadzor kvalitete zraka gdje pojedinci koji posjeduju uređaje sa senzorima i pametne telefone dijele podatke vezane uz kvalitetu zraka na specifičnoj mikro-lokaciji, pitanje je tko je vlasnik tih podataka? Građani? Gradske službe? Pružatelj usluge IoT platforme? Ili netko drugi? Uzmimo u razmatranje još jedan primjer gdje je vozač prekoračio brzinu kretanja koja je dozvoljena u tom dijelu grada i to je detektirano od strane senzora ugrađenih u vozilo. Što bi u ovom slučaju računalo u vozilu trebalo napraviti? Poslati podatke policiji jer je prekoračena brzina ili ti podaci pripadaju vlasniku vozila i on bi trebao odlučiti što napraviti s njima ili podaci pripadaju proizvođaču automobila? Sukladno Uredbi o zaštiti osobnih podataka ovo su privatne informacije jer se mogu iskoristiti za jednoznačnu identifikaciju pojedinca i stoga ova informacija bi trebala pripadati vlasniku automobila. S druge strane, može se izraditi nova zakonska regulativa koja će zahtijevati da vlasnici automobila dijele informacije sa senzora u vozilima s državnim tijelima, poput policije u ovom slučaju. Na primjer, na tehničkom pregledu vozila, može se uvjetovati prolaz i dobivanje potvrde o ispravnosti vozila uvjetom da se da suglasnost za dijeljenje informacija iz vozila s državnim tijelima. U ovom konkretnom slučaju osobni podaci bi se morali dijeliti s trećom stranom.

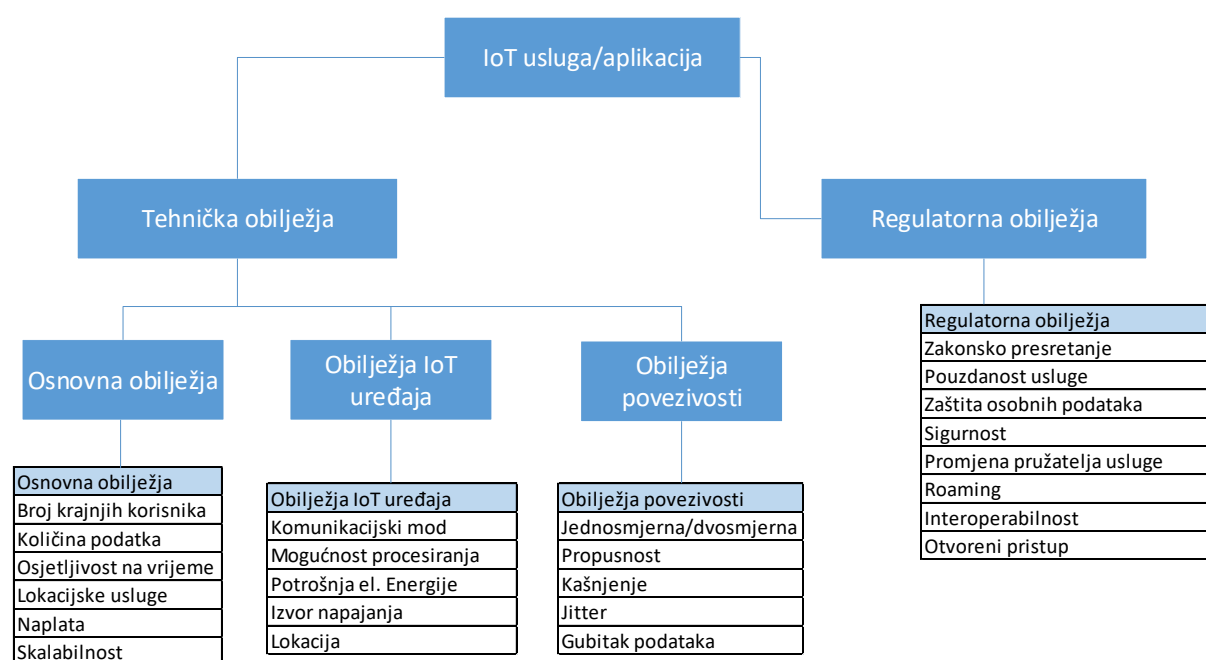
Prethodno opisana regulatorna obilježja opisuju samo dio regulatornih problema i potencijalnih pitanja koja se mogu javiti u budućnosti. Stoga je bitno da su sva pobrojena regulatorna obilježja dobro analizirana od strane svih dionika u lancu vrijednosti Interneta stvari za vrijeme inicijalnog planiranja usluge pametnog grada. Dodatno, lokalni zakonski i podzakonski propisi mogu predstavljati još jedno opterećenje za masovno razmještanje usluga pametnih gradova i stvoriti prepreke za replikaciju usluga, kako je to i identificirano u izvješću EU SCIS-a [75] gdje su prikazani brojni stvarni primjeri. Dane su preporuke nacionalnim vladama i lokalnim samoupravama što treba biti poboljšano kako bi se uklonile zakonske prepreke za repliciranje projekata u velikom broju gradova. U ovoj disertaciji je predložena lagana regulacija s nadgledanjem razvoja situacije, pogotovo u ranoj fazi razvoja pametnih

gradova i Interneta stvari kako bi se ostvarila bolja replikacija IoT projekata i u konačnosti masovno razmještanje usluga Internet stvari. Za specifične usluge za koje se detektira da trebaju regulaciju, jer inače neće imati uspjeha, potrebna je regulacija u većim razmjerima, na primjer na EU ili svjetskoj razini. Dobar primjer toga je pan-europska usluga eCall koju su osim zemalja EU koje su imale zakonsku obvezu, implementirale i druge zemlje koje nisu članice EU.

4. TAKSONOMIJA USLUGA PAMETNIH GRADOVA

U prethodnom poglavlju pobrojana su i opisana tehnička i regulatorna obilježja usluga pametnih gradova te je predstavljen model lanca vrijednosti s ulogama u njemu. Iz navedenih obilježja, pogotovo tehničkih obilježja, uočljivo je da se dio obilježja može odnositi i na usluge i na uređaje i takva obilježja su grupirana u jednu zajedničku skupinu pod nazivom osnovna obilježja. Osim toga postoje i posebna tehnička obilježja koja se odnose na same IoT uređaje te su nazvana obilježjima IoT uređaja. Komunikacija je posebna stavka i za uređaje i uslugu i zbog toga je ta grupa tehničkih obilježja izdvojena kao samostalna.

Na temelju prethodno identificiranih obilježja predložena je taksonomija usluga pametnih gradova koja je prikazana na slici 24.



Slika 24: Predložena taksonomija IoT usluga

Predložena taksonomija daje klasifikaciju najvažnijih i tehničkih i regulatornih obilježja koje se neizostavno moraju odrediti za svaku uslugu pametnog grada. Na ovaj način daje se vodič dionicima lanca vrijednosti pametnih gradova kroz proces identifikacije ključnih obilježja njihove buduće usluge koje utječu na tehničke zahtjeve tih usluga. Međutim, ova klasifikacija

ne daje odgovor je li pojedina usluga u skladu s regulatornim i tehničkim zahtjevima kako bi u praksi bila uspješno uvedena i korištena. U sljedećem poglavlju predložena taksonomija je korištena kako bi se identificirali ključni zahtjevi za nekoliko odabranih primjera usluga pametnih gradova, točnije za pametna brojila električne energije, pametno parkiranje, inteligentni prometni sustavi, pametna ulična rasvjeta i masovna mjerenja za nadzor kvalitete zraka u gradovima.

4.1. Primjeri usluga

Usluge na kojima će se pokazati predloženi model taksonomije usluga pametnih gradova izabrane su na temelju njihove brojnosti i zbog toga što one same koriste većinu ili sva obilježja predloženog modela.

4.1.1. Pametna brojila električne energije

Jedan od glavnih ciljeva Europske komisije bio je izmjena direktive o energetske učinkovitosti prema kojoj se očekuje da najmanje 80% kućanstava EU ima instalirana pametna brojila do 2020 [59]. Usluga pametnih brojila električne energije se koristi za mjerenje potrošnje električne energije u stvarnom vremenu. Krajnji korisnik potrošnju može nadgledati kroz zasebnu aplikaciju na mobilnom uređaju ili preko web-preglednika. Informacija o potrošnji električne energije se kasnije koristi od strane distributera električne energije kako bi se izvršila naplata prema stvarnoj potrošnji. Ovu informaciju distributer električne energije može koristiti i za stvaranje novog poslovnog modela, odnosno nove ponude u kojoj će krajnji korisnik imati mogućnost dinamičke promjene tarife u ovisnosti o svojoj potrošnji. Očito je da će distributer električne energije u ovom slučaju morati obrađivati osobne podatke krajnjeg korisnika kako bi mogao ponuditi takvu uslugu. Sukladno novoj Uredbi i okviru o zaštiti osobnih podataka distributer električne energije će morati dobiti suglasnost od krajnjeg korisnika za korištenje njegovih osobnih podataka u svrhu pružanja navedene usluge. Osim toga, distributer će morati i objasniti na koji način će koristiti osobne podatke.

Očekuje se da će broj krajnjih korisnika značajno narasti budući da sama direktiva predviđa kako će velika većina kućanstava EU imati ugrađena pametna brojila električne energije, ali i plina. Ova usluga je vremenski osjetljiva i stoga se očekuju stvarni ili gotovo stvarni podaci s vrlo malim odstupanjima. Usluga se nudi na poznatoj, fiksnoj, lokaciji, a

generirani podaci od jednog pametnog brojila su većinom mali. Naplata usluge se obično vrši na vremenskom intervalu od jednog mjeseca, a dodatne usluge se mogu naplaćivati prema zahtjevu. S regulatorne strane privatnost predstavlja najveći izazov. Naime, na temelju potrošnje korisnika, informacije o ponašanju korisnika, mogu identificirati korisnika, ali se one mogu iskoristiti i u ilegalne svrhe. Stoga politika privatnosti mora biti implementirana u skladu s uredbom GDPR [66,67]. Glavni zahtjev nad atributima oslonjivosti kod ove usluge je visoka pouzdanost (engl. *reliability*) jer se zahtjevaju odlične i kontinuirane operacijske performanse tijekom cijelog vremena trajanja usluge. U prethodnom poglavlju dan je opis konkretnog napada na distributere električne energije u Ukrajini stoga se posebna pažnja treba posvetiti sigurnosti, a glavni sigurnosni atribut bi trebao biti cjelovitost.

4.1.2. Pametno parkiranje

Prema članku [76] između 1927. i 2001. godine veći broj studija je napisano vezano uz krstarenje (spora vožnja kod traženja parkirnog mjesta) vozilima kroz uži centar gradova. Prema navedenim istraživanjima vozači u prosjeku troše između tri i pol (3,5) i četrnaest (14) minuta kako bi pronašli parkirno mjesto. Također, isto istraživanje je pokazalo da između osam (8) i sedamdesetičetiri (74) posto prometa u gradu je generirano zbog traženja parkirnog mjesta. Kako bi se promet učinio prohodnijim, gradovi uvode novu uslugu postavljajući senzore na parkirna mjesta u svrhu detekcije slobodnih mjesta. Tradicionalno se informacija sa senzora prikupljala na središnjem poslužitelju te se obično prikazivala na LCD ekranu na ulici. Korištenjem IKT-a informacija o stvarnom stanju slobodnih mjesta dostupna je putem mobilne aplikacija na pametnom telefonu. Dodatno, aplikacija na mobilnom uređaju može ponuditi i ugrađeni sustav navođenja do slobodnog parkirnog mjesta. Jedan od izazova za takvu aplikaciju je detekcija kada netko drugi zauzme mjesto koje je aplikacija namijenila za vas. Ukoliko ne postoje stupići kojima bi se vršila rezervacija parkirnih mjesta, a što bi se i dodatno naplatilo, takva aplikacija mora imati stvarnu informaciju o slobodnom mjestu te u slučaju zauzeća automatski vozača navoditi na sljedeće slobodno mjesto.

Zbog svoje prirode i velikog broja vozila u gradovima, usluga pametnog parkiranja ima veliki broj krajnjih korisnika, kako građana tako i posjetitelja grada. Usluga mora pružati informacije o slobodnim parkirnim mjestima na pojedinim lokacijama u stvarnom vremenu. Aplikacija za pametne telefone je obično besplatna za krajnje korisnike (građane i posjetitelje), međutim, troškovi razmještanja i održavanja (senzora i platforme) postavljene usluge može se

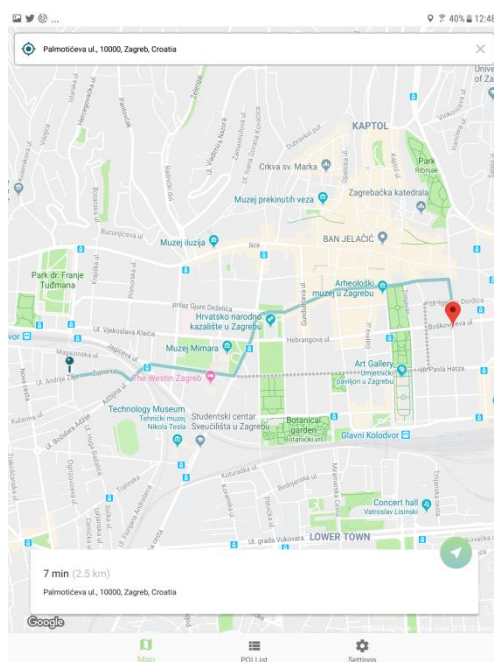
nadoknaditi od naplate parkirnog mjesta. Također, dodatne usluge, na primjer, rezervacija parkirnog mjesta može se dodatno naplatiti. Mobilna usluga treba odrediti i poslati GPS lokaciju korisnika zbog čega se može tretirati kao lokacijska usluga. Politika privatnosti mora biti implementirana i formulirana u skladu s Uredbom o zaštiti osobnih podataka (EU)2016/680 [66,67]. Sigurnosni atributi u kontekstu usluge pametnog parkiranja vezani su uz integritet definirajući ju kroz autentikaciju korisnika, preciznost (točnost) i potpunost podataka i informacija vezanih za pruženu uslugu. Jedan od glavnih zahtjeva koji predstavlja izazov za uslugu je visoka razina raspoloživosti koja zahtjeva odlične operacijske performanse i održavanje kako bi se osiguralo dugo vrijeme rada između kvarova i vrlo kratko vrijeme popravka kvarova. Drugi izazov predstavlja potreba za pružanjem integrirane usluge parkiranja za sva parkirna mjesta u gradu koja mogu biti na otvorenom prostoru i u garažama, a istovremeno mogu biti pružane od strane različitih pružatelja usluge parkiranja. U takvom okruženju jedino interoperabilna pojedinačna rješenja parkirne usluge mogu ponuditi aplikaciju za krajnje korisnike koja je dovoljno fleksibilna i prilagodljiva dinamičkim uvjetima okoline prometa šireg gradskog središta kako je i traženo. Otvoren pristup informacijama o parkirnom mjestu (na primjer, je li parkirno mjesto slobodno i lokacija parkirnog mjesta) je također presudno za tako integriranu uslugu pametnog parkiranja. Na temelju navedenog možemo zaključiti da je usluga pametnog parkiranja vrlo izazovna usluga i sa strane regulatornih i sa strane tehničkih zahtjeva.

4.1.3. Suradno opažanje okoline u pokretu

Suradna opažanja okoline u pokretu u gradovima danas sve više postaju brzorastuće usluge koje zahtijevaju aktivno uključivanje i angažman građana. Pojam „suradno opažanje“ opisuje usluge i aplikacije gdje pojedinci koji posjeduju nosivi uređaj s ugrađenim senzorima i/ili pametni telefon kolektivno dijele generirane podatke i izvlače informacije kako bi se izradila mjerenja i karta od zajedničkog interesa [77]. Na primjer, ovakva se usluga može koristiti za nadzor kvalitete zraka ili buke na gradskim ulicama zbog velikog broja mjerenja koja pokrivaju široko gradsko područje uključujući i mikrolokacije koje su teško dostupne službenim stanicama za mjerenje kvalitete zraka ili buke.

Usluga zahtjeva senzore za detekciju kvalitete zraka koji se mogu lagano nositi i koji djeluju kao IoT uređaji. Takvi uređaji su povezani s pametnim telefonima korisnika na kojima se nalazi mobilna aplikacija koja prikuplja podatke s prijenosnog senzora i šalje ih u oblak

[78,79] dok građani prolaze gradom (na biciklu ili pješke). U slučaju nadgledanja kontrole buke koristi se mikrofoni na mobilnom uređaju preko kojeg se vrši snimanje buke. Ovdje je potrebno istaknuti da je i senzore ugrađene u prijenosne IoT uređaje i mikrofoni u pametnom telefonu potrebno redovito kalibrirati kako bi očitavanja bila vjerodostojna, dok istovremeno građani trebaju biti upoznati kako provesti mjerenja. Svako mjerenje kvalitete zraka ili buke ima lokacijsku oznaku generiranu od strane GPS modula u pametnom telefonu čime je usluga lokacijska. Interes građana za korištenje usluge je moguće potaknuti zbog dijeljenja podataka sa zajednicom i mogućnosti pristupa prikupljenim podacima koji gusto pokrivaju gradsku okolinu. U mobilnoj aplikaciji⁹ za suradno opažanje okoline u pokretu za praćenje kvalitete zraka iz primjera, pod imenom CUPUS, cilja se na zajednicu čiji su članovi zainteresirani za kvalitetu zraka, a to su biciklisti i njihove udruge jer su najviše pogođeni lošom kvalitetom zraka u gradovima. Na slici 25 vidi se primjer karte Zagreba s dobivenim mjerenjima nekih vozača bicikla.



Slika 25: primjer aplikacije na kojoj su prikazane rute dvije biciklističke rute, najkraća i alternativna „zelena“ ruta s boljom kvalitetom zraka

Uzevši u obzir da je priroda usluge temeljena na mjerenjima koje dobrovoljno provodi pojedinac, najzanimljivija obilježja ovakve usluge koja će biti komentirana su oslonjivost i sigurnost. Ključni atributi sigurnosti i oslonjivosti su raspoloživost, pouzdanost, zaštita,

⁹ CUPUS – Crowdsensing, dostupno na Google Play

održivost, cjelovitost i povjerljivost. U našem primjeru zaštita nije u opisu ove usluge, kao što nije niti pouzdanost i povjerljivost budući je cilj informacije dijeliti s drugima. Kada se bolje pogleda, cjelovitost se može definirati kroz točnost i dosljednost i zbog toga ona u našem primjeru treba biti sačuvana kako bi se postigla i zadržala vjerodostojnost usluge, a očitani podaci se konstantno moraju analizirati i nadgledati od strane stručnjaka kako bi se zadržalo povjerenje u uslugu. Održivost može predstavljati veliki izazov budući da se prijenosni senzori moraju periodički kalibrirati (zakonski je uređeno da se senzori za detekciju plinova moraju održavati, a što uključuje i kalibraciju, jedan puta godišnje). Priroda usluge je da mnogo ljudi generira informacije, stoga se i senzori nalaze kod ljudi koji dobrovoljno vrše mjerenja. Pitanje je koliko će ljudi biti voljni nositi senzore na kalibraciju, a u ovisnosti o odgovoru rezultati mjerenja mogu biti diskutabilni. Posljednji atribut koji je bitan je raspoloživost. Ona uvelike ovisi o dobrovoljcima koji nose senzore i njihovoj volji i želji da vrše mjerenja, stoga je ključni problem ove usluge svježina podataka, odnosno kada su podaci u bazi bili zadnji put osvježeni. Iz tog razloga atributi oslonjivosti mogu se vrlo teško odrediti.

4.1.4. Pametna (inteligentna) ulična rasvjeta

U današnjem svijetu smanjenje potrošnja električne energije je jedna od najvažnijih tema za razvoj održivih gradskih područja. Prema [80] urbana područja troše preko 70% električne energije svijeta i generiraju preko 50% stakleničkih plinova. Javna gradska rasvjeta troši velik postotak od ukupno potrošene električne energije u gradovima zbog svojeg stalnog operativnog rada tijekom noći. Prema izvještaju Europske komisije [80] koji je dio strategije Digitalne agende za Europu 2020 [64], na javnu rasvjetu se troši u pravilu oko 60% ukupnih troškova električne energije lokalne samouprave. Također, klasična javna rasvjeta je podložna kvarovima i vrlo je skupa za održavanje što dodatno podiže troškove rasvjete.

Pametna ili inteligentna ulična rasvjeta odnosi se na uslugu gdje se javna ulična rasvjeta prilagođava pokretima pješaka, biciklista, vozila. U ovom slučaju ukoliko nema pokreta na ulici rasvjeta se smanji čime se uvelike štedi na potrošnji električne energije. Po dolasku pješaka, biciklista ili vozila svjetlo se automatski pojačava. S ugrađenim sensorima prisutnosti i kamerama ovakva rješenja mogu prikupljati i slati dodatne informacije koje mogu pomoći gradskim službama kod nadgledanja grada i kod brzih reakcija u okolnostima kritičnima za sigurnost građana. Senzori i kamere se također mogu koristiti i za detekciju prometnih zagušenja ili za usluge pametnog parkiranja kako bi pratili slobodna mjesta.

Očekivani broj krajnjih korisnika ove usluge je velik s obzirom da su svi pješaci, biciklisti i vozila korisnici. Usluga se pruža u stvarnom vremenu na fiksnoj lokaciji i stoga se temelji na interakciji na lokalnoj razini što u konačnosti smanjuje kompleksnost usluge. Usluga javne ulične rasvjete kao dodatna vrijednost na postojeću uslugu pružatelje javne rasvjete se neće dodatno naplaćivati od korisnika, ali dodatne usluge koje ona omogućava se mogu naplaćivati. Ukoliko se detekcija korisnika vrši korištenjem kamera na temelju prepoznavanja lica, politika privatnosti za krajnje korisnike mora biti implementirana u skladu s Uredbom o zaštiti osobnih podataka i Uredbom o e-privatnosti [66,67]. Ukoliko se ne vrši detekcija korisnika kamerom, nema ni prikupljanja osobnih informacija stoga niti politika privatnosti nije potrebna. Ključni sigurnosni atribut je cjelovitost koji je definiran kroz točnost i dosljednost, dok se od atributa oslonjivosti ističe pouzdanost budući da sustavi rasvjete trebaju imati kontinuitet ispravnog rada svjetla tijekom cijelog vremena rada, a to ovisi o informacijama sa senzora. Promjena pružatelja usluge nije bitna za ovu uslugu budući je usluga namijenjena za javne tvrtke. Ključno obilježje koje nije toliko bitno za ovu uslugu, ali je bitno za ostale usluge koje koriste postavljenje senzore i kamere, odnosno, podatke dobivene od senzora na stupu javne rasvjete je otvoren pristup. Stupovi ulične rasvjete mogu imati dodatne resurse, poput senzora okoline (za mjerenje temperature, kvalitete zraka, buke i slično) ili kamera koje se mogu koristiti od strane drugih usluga. Kod takvih slučajeva stroga kontrola pristupa treba biti aktivirana kako bi pristup podacima bio ograničen isključivo na autorizirane korisnike koji imaju pravo pristupa podacima generiranim od strane tih uređaja. Važno je napomenuti da stupovi javne rasvjete mogu čak udomačiti i bazne postaje pokretnih mreža (na primjer 5G, LoraWan, WiFi, Sigfox, i slično).

4.2. Rezultati istraživanja

Rezultati istraživanja prikazani su na temelju prethodno opisana 4 scenarija. Sva regulatorna i tehnička obilježja identificirana u scenarijima koji su poslužili kao primjer su prikazana u tablici 3. U tablici se radi usporedba analiziranih usluga u skladu sa taksonomijom predloženom na početku ovog poglavlja.

Tablica 3: Usporedba tehničkih i regulatornih obilježja usluga pametnih gradova

Usluga pametnog grada	Pametna brojila	Pametno parkiranje	Suradno opažanje okoline u pokretu	Pametna ulična rasvjeta
Osnovna obilježja				
Broj krajnjih korisnika	Veliki	Veliki	Srednje/Veliki	Veliki
Količina podataka	Mala	Mala	Mala	Mala /Velika
Vremenska osjetljivost	Gotovo stvarno vrijeme	Stvarno vrijeme	Gotovo stvarno vrijeme, na zahtjev	Stvarno vrijeme
Lokacijske usluge	Ne	Da	Da	Da
Naplata	Da	Da	Ne	Ne
Skalabilnost	Da	Da	Da	Da
Regulatorna obilježja				
Zakonsko presretanje	Ne	Da	Da	Ne
Pouzdanost	Visoka dostupnost	Visoka dostupnost	-	Postojanost
Privatnost	Politika	Politika	Politika	Politika / nije bitno
Sigurnost	Cjelovitost	Cjelovitost	Cjelovitost	Cjelovitost
Promjena pružatelja usluge	Da	Da	Da	Nije bitno
Roaming	Nije bitno	Nije bitno	Da	Nije bitno
Interoperabilnost	Politika	Politika	Politika	Politika
Otvoren pristup	Da	Da	Da	Da
IoT uređaj				
Pristup	Žičano ili bežično	Žičano ili bežično	Bežično	Bežično
Procesorska mogućnost	Ne	Ne	Ne	Da
Izvor napajanja	Stalan izvor	Baterija ili stalan izvor	Punjiva baterija	Stalan izvor
Potoršnja električne energije	Mala	Mala	Mala	Mala
Lokacija	Fiskna	Fiskna	Mobilna	Fiskna
Povezivost				
Jednosmjerna / dvosmjerna	Jednosmjerna / dvosmjerna	Jednosmjerna	Dvosmjerna	Dvosmjerna
Propusnost	Mala	Mala	Mala	Mala/Srednja
Kašnjenje	Best effort	Malo (do 5 sec)	Best effort	Best effort

Jitter	Nije bitno	Nije bitno	Nije bitno	Nije bitno
Gubitak podataka	Vrlo mali	Vrlo mali	Mali	Vrlo mali

Na temelju usporedbe usluga pametnih gradova koje su koristile predloženu taksonomiju i uloge objašnjene u modelu lanca vrijednosti usluga pametnih gradova, identificirane su regulatorne preporuke i važni aspekti za svaku od uloga lanca vrijednosti.

Kod usluge pametnog parkiranja detektirane su sljedeće uloge s potencijalnim regulatornim obvezama:

- Pružatelj uređaja: je odgovoran za interoperabilnost između različitih uređaja, te uređaja i IoT platforme i sigurnosti uređaja;
- Pružatelj usluge infrastrukture: odgovoran je za Roaming, međutim budući da se ova usluga pruža na fiksnoj lokaciji aktivnosti Roaminga nikada neće biti. Budući da je ovdje uključena i usluga elektroničkih komunikacija, mora se otvoriti sučelje za zakonsko presretanje;
- Pružatelj usluge IoT platforme: mora osigurati interoperabilnost između platforme i usluga. Također, treba osigurati oslonjivost, omogućiti promjenu pružatelja platforme, brinuti se o privatnosti, sigurnosti i otvorenom pristupu.
- Pružatelj IoT usluge: mora se brinuti oko sigurnosti i privatnost
- IoT korisnik: je zadužen za brigu oko privatnosti
- Krajnji korisnik: nema regulatornih obveza iako kod mnogih društvenih usluga povjerenje o usluzi uvelike ovisi o krajnjem korisniku.

U prijašnjim poglavljima su već objašnjene uloge unutar modela IoT lanca vrijednosti za primjer usluge pametnih gradova. Komunikacija između različitih usluga u gradovima predstavlja jedan od ključnih izazova za interoperabilnost između platformi i usluga. Raspoloživost kao jedan od ključnih atributa oslonjivosti je presudna za uslugu pametnog parkiranja. Važna je i mogućnost promjene pružatelja usluge. Europska komisija često zna istaknuti promjenu pružatelja usluge kao jedan od temeljnih prava krajnjih korisnika. Privatnost i sigurnost osobnih podataka korisnika je definirana i EU direktivama, dok je otvorenost pristupa podacima senzora neophodna za mogući razvoj drugih inovativnih usluga. Kod scenarija usluge pametnog parkiranja, otvoreni podaci bi bili lokacija slobodnih parkirnih mjesta. U našem primjeru, pružatelj usluge IoT platforme je isto što i pružatelj same IoT usluge,

a to je privatno poduzeće koje je razvilo uslugu pametnog parkiranja. Sukladno regulatornim preporukama pružatelj IoT usluge trebao bi dopustiti promjenu pružatelja IoT usluge ukoliko to korisnik zatraži, ali isto tako bi se trebao pobrinuti za sigurnosti i privatnost podataka budući da usluga prikuplja podatka s različitih izvora. U scenarijima poput ovoga krajnji korisnici (vozači, vlasnici vozila za koje se plaća parkirno mjesto) obično nemaju nikakve odgovornosti i za njih nema preporuka. Međutim, kroz mobilnu aplikaciju korisnik može poslati informacije vezane uz nepropisno parkirana vozila slanjem slike navedenog vozila s geo-lokacijom vozila i komentarom. U tom slučaju, povjerenje sa strane korisnika je potrebno.

Tablica 4: Regulatorne preporuke za svaku ulogu u IoT lancu vrijednosti

		Analizirani primjeri			
Uloga u modelu IoT lanca vrijednosti	Regulatorna obilježja	Pametna brojila	Pametno parkiranje	Suradno opažanje okoline u pokretu	Pametna ulična rasvjeta
Pružatelj usluge uređaja	Ineroperabilnost (stoga protokola)	DA	DA	DA	DA
	Sigurnost (cjelovitost i autorizirani pristup uređaju)	DA	DA	DA	DA
Pružatelj usluge IoT povezivosti	Roaming	NE	NE	DA	NE
	Zakonsko presretanje	DA	DA	DA	DA
Pružatelj usluge IoT platforme	Interoperabilnost (platforme i usluge)	DA	DA	DA	DA
	Oslonjivost	Pouzdanost	Visoka raspoloživost	Raspoloživost	Pouzdanost
	Promjena pružatelja IoT platforme	DA	DA	DA	DA
	Sigurnost	Cjelovitost	Autentikacija korisnika, točnost i potpunost podataka	Cjelovitost	Cjelovitost
	Privatnost	Politika (Pravila)	Politika (Pravila)	Politika (Pravila)	Nije bitno
	Otvoren pristup	NE	DA	DA	NE
Integrator IoT usluge	Promjena pružatelja usluge	DA	DA	DA	NE
	Sigurnost	Cjelovitost	Autentikacija korisnika, točnost i	Cjelovitost	Cjelovitost

			potpunost podataka		
	Privatnost	Politika (Pravila)	Politika (Pravila)	Politika (Pravila)	Politika / nije bitno
Razvijatelj aplikacija	Sigurnost	Cjelovitost, autentikacija korisnika	Autentikacija korisnika, točnost i potpunost podataka	Cjelovitost	N/A
	Privatnost	Politika (Pravila)	Politika (Pravila)	Politika / nije bitno	N/A
IoT korisnik	Privatnost	DA	DA	DA	DA (ukoliko se koristi prepoznavanje lica)
Krajnji korisnik	Povjerenje (ukoliko korisnik stvara podatke)	DA	DA	DA	DA (ukoliko se koristi prepoznavanje lica)

Tablica 4 identificira najvažnija regulatorna obilježja za sve primjere koji su korišteni u ovom radu. Općenito kada se pogleda tablica 4 uočljivo je da se dio regulatornih obilježja ponavlja u svim scenarijima. Bez obzira je li riječ o usluzi Internet društva, usluzi u području logistike, energije ili nekom drugom području postoje zajednička obilježja koja se mogu izvući u jednu jedinstvenu tablicu koja bi bila primjenjiva na sve IoT usluge, a kroz koju bi se definirala općenita regulatorna obilježja za svaku ulogu u IoT lancu vrijednosti.

Tablica 5: Općenite regulatorne preporuke za svaku ulogu u IoT lancu vrijednosti

Uloga u modelu IoT lanca vrijednosti	Regulatorna obilježja
Pružatelj uređaja	Interoperabilnost i sigurnost
Pružatelj usluge infrastrukture	Roaming, Zakonsko presretanje
Pružatelj usluge IoT platforme	Interoperabilnost (platforme i usluge), Pouzdanost, Promjena pružatelja platforme, Privatnost, Sigurnost i Otvoren pristup
Pružatelj IoT usluge	Promjena pružatelja usluge, Sigurnost i Privatnost
IoT korisnik	Privatnost
Krajnji korisnik	Povjerenje (ukoliko korisnici generiraju podatke)

Regulatorna obilježja najčešće su vezana uz nacionalne i EU zakonske i podzakonske propise i kao takva su podložna promjeni. U tablici 5 je dan opseg regulatornih preporuka koje

se ne bi trebale mijenjati kroz vrijeme, odnosno koje predstavljaju osnovu za uspješan razvoj i implementaciju usluga pametnih gradova.

Može se zaključiti da su najvažnija regulatorna obilježja za proizvođača uređaja interoperabilnost na razini protokola na sloju podatkovne poveznice i problemi sigurnosti, kao i cjelovitost podataka i autorizacija pristupa prema uređajima. Pružatelj usluge povezivosti je odgovoran za osiguravanje funkcionalnosti Roaminga (koji su važni samo za uslugu suradnog opažanja okoline u pokretu iz našeg primjera, ali i općenito kod usluga gdje je važna pokretljivost jer je riječ o prijenosnim uređajima koji mogu prijeći granice domaće mreže) i funkcije tajnog nadzora (zakonsko presretanje). Glavna briga za pružatelja usluge platforme oslonjivost i sigurnost. Kada se gleda oslonjivost najvažnije zahtjeve usluga predstavlja raspoloživost i pouzdanost (engl. *reliability*), dok cjelovitost podataka, točnost i autorizirani pristup usluzi i pripadajućim podacima predstavljaju najvažnije zahtjeve vezane uz sigurnost. Osim toga, pružatelj usluge platforme ima obvezu pružanja interoperabilnog rješenja s jasno definiranim sučeljem usluge kako bi promjena pružatelja usluge bila moguća. On treba omogućiti i otvoreni pristup podacima (u primjeru kod usluge pametnog parkiranja i suradnog opažanja okoline u pokretu), kao i definirati odgovarajuću politiku za zaštitu osobnih podataka osiguravajući tako privatnost korisnika. Slično obvezama pružatelja usluge platforme, glavna briga integratora usluge pametnih gradova vezana je uz sigurnost usluge i privatnost korisnika. Očekivano je da se integrator IoT usluge može promijeniti (u našim primjerima u svim scenarijima, osim kod pametne javne ulične rasvjete). Razvijatelji aplikacija trebaju osigurati cjelovitost podataka unutar razvijene aplikacije i da samo autorizirani korisnici imaju pristup do određenih podataka i usluga. Odgovarajuća politika mora biti implementirana u slučaju da aplikacija čuva neke osobne podatke. Važno je napomenuti da se u primjeru pametne javne ulične rasvjete ne očekuje da će aplikacija biti razvijena za krajnje korisnike. Za krajnjeg korisnika, privatnost predstavlja najveći izazov, dok krajnji korisnik nema nekih specifičnih regulatornih obveza osim ispravnih mjerenja kod usluge suradnog opažanja okoline u pokretu za praćenje kvalitete zraka i zahtjeva povjerenje u cijeli ekosustav kada se prikupljaju, spremaju ili obrađuju njegovi osobni podaci.

Jedan od većih problema gradova koji žele krenuti u smjeru digitalne transformacije je pronalazak sredstava za realizaciju njihovih projekata pametnih gradova. Svjedoci smo prvog vala vrlo uspješnih istraživačkih projekata vođenih od strane projekata financiranih iz fondova EU u kojima su gradska uprava koja je imala viziju i mali poduzetnici provodili digitalizaciju korištenjem „bottom-up“ pristupa bez obzira na nacionalne vlade i nacionalne strategije.

Međutim, u okolinama koje zaostaju kada se gleda na postavljenu infrastrukturu, sam koncept razvoja pametnog grada mora pratiti logičan slijed događaja i mora biti u skladu s razvojem potrebne gradske infrastrukture, što uključuje i odgovarajuću komunikacijsku infrastrukturu. Upravo zbog tog razloga, ukoliko želimo ubrzati razvoj pametnih gradova jedan od preduvjeta je pripremljena i izrađena nacionalna strategija za razvoj pametnih lokalnih okolina ili gradova s akcijskim planom koji jasno i nedvosmisleno definira ciljeve i načine kako ih postići. Važno je napomenuti da takva strategija ne smije biti napravljena samo za gradove već treba uzeti u obzir i ostale lokalne samouprave gdje se većinom nalaze manja mjesta. Uz navedenu nacionalnu strategiju, svaka regija (županija ili grad) bi trebala pripremiti svoju vlastitu strategiju koja će pratiti upute iz nacionalne strategije, ali će istovremeno uzeti u obzir specifičnosti svoje regije. Nacionalne i regionalne ili lokalne strategije zahtijevaju strateško planiranje i implementaciju odgovarajućih inicijativa i projekata koji će omogućiti povećanje kvalitete života i stvoriti nova radna mjesta u svojoj regiji. Osim toga, takvi projekti bi trebali dovesti do povećanja gospodarskog i društvenog razvoja zbog većeg tržišnog natjecanja. Strategija razvoja pametnih gradova treba uključiti metodološki okvir i primjere najboljih praksi za razvoj rješenja pametnih gradova, a u isto vrijeme istražiti područja aplikacija i usluga koje mogu dati najbolje efekte te na koje strateške ciljeve se orijentirati. Sličan pristup strategiji je dan od strane EU gdje su odabrani gradovi pratili dobar primjer mentorskih gradova pritom prilagođavajući rješenja specifičnostima regionalne i nacionalne strategije.

4.3. Poslovni odnosi u lancu vrijednosti

Poslovni odnosi u lancu vrijednosti govore koje uloge u predloženom modelu lanca vrijednosti imaju ugovore ili mogu imati ugovore s drugim sudionicima u lancu vrijednosti. Odnosi koje ćemo objasniti u ovom poglavlju se temelje na predloženom modelu lanca vrijednosti definiranom u poglavlju 1.5. na slici 18.

Poslovni odnosi bit će objašnjeni kroz nekoliko sljedećih slika gdje se vidi tko s kim komunicira, a na kraju poglavlja će se dati pojašnjenje na jednom primjeru tko je odgovoran ukoliko dođe do propusta.

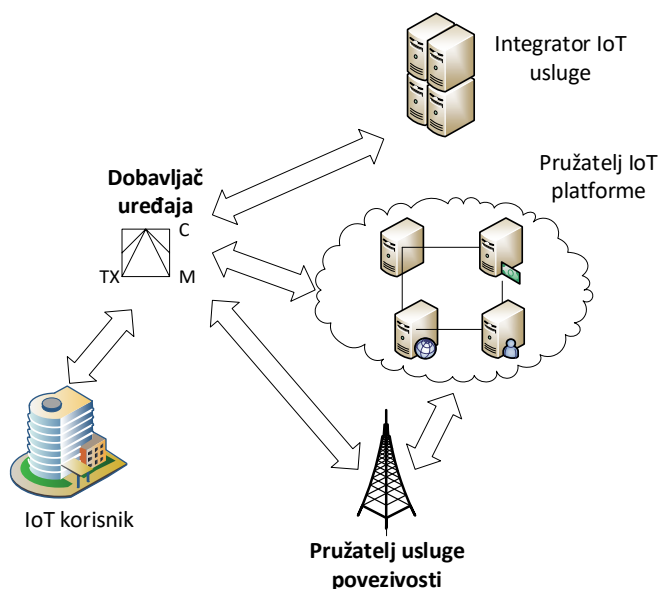
Slika 26a prikazuje odnose pružatelja IoT uređaja i pružatelja IoT povezivosti. Iz slike 26a je vidljivo da pružatelj IoT uređaja ima ili može imati ugovor s:

- Pružateljem IoT platforme radi povezivanja uređaja na platformu.
- Integratorom IoT usluge koji dohvaćati informacije s uređaja.

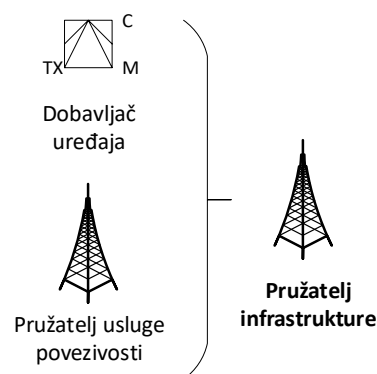
- IoT korisnikom koji može direktno nabavljati uređaje.
- Pružateljem usluge povezivosti radi povezivanje uređaja s uslugom.

Na istoj slici vidi se i pružatelj usluge povezivosti koji može imati ugovor s:

- Pružateljem IoT uređaja radi usluge povezivosti
- Pružateljem IoT platforme radi usluge povezivosti



Slika 26a: Odnosi pružatelja uređaja i povezivosti

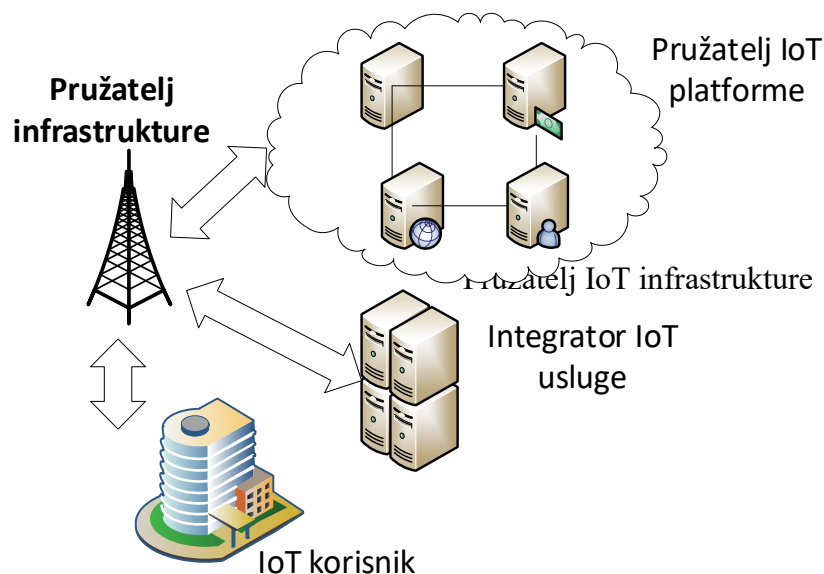


Slika 26b: Pružatelj infrastrukture

Slika 26b pokazuje međusobne odnose pružatelja infrastrukture i pružatelja IoT uređaja i pružatelja usluge povezivosti. Točnije, pružatelji IoT uređaja i usluge povezivosti zajedno čine pružatelja IoT infrastrukture.

Na slici 27 vidi se pružatelj infrastrukture koji može imati odnose s:

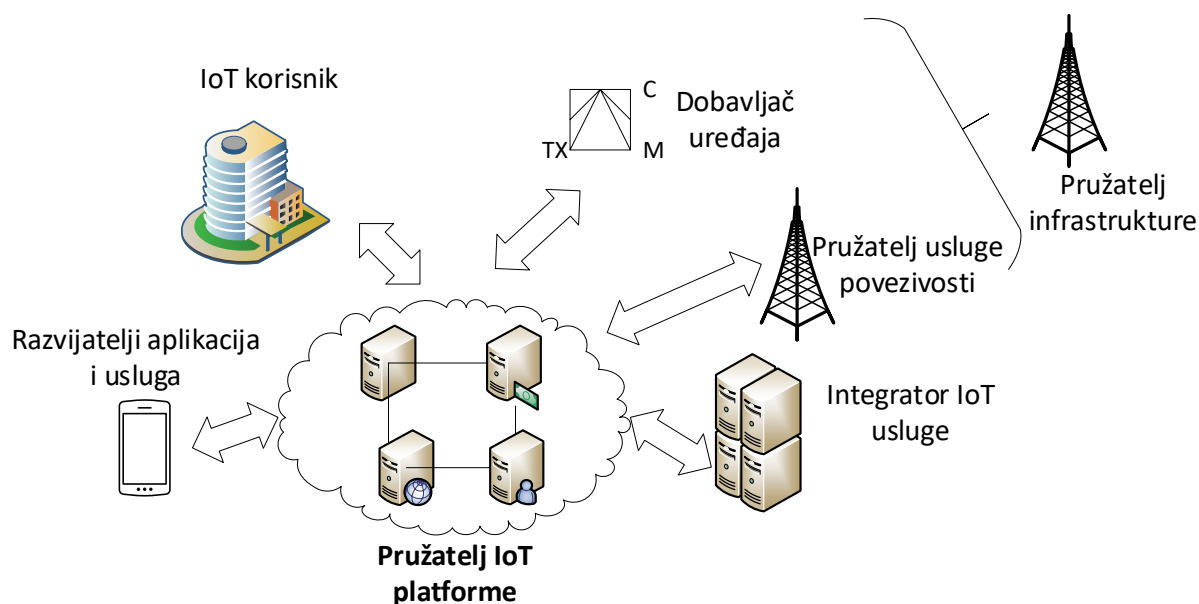
- Pružateljem IoT platforme radi povezivanja uređaja s platformom.
- Integratorom IoT usluge koji dohvaća informacije s uređaja.
- IoT korisnikom koji može direktno nabavljati uređaje



Slika 27: Mogući odnosi pružatelja infrastrukture

Središnju poziciju u identificiranom modelu lanca vrijednosti ima pružatelj IoT platforme (na slici 28) koji može imati odnose s:

- Pružateljem IoT uređaja
- Pružateljem usluge povezivosti
- Integratorom IoT usluge koji povezuje sve funkcionalnosti usluge korištenjem platforme.
- Razvijateljem aplikacija i usluga koji će koristiti platformu za dohvaćanje podataka koje koristi aplikacija i usluge.
- IoT korisnikom koji ujedno može biti pružatelj IoT platforme.



Slika 28: Mogući odnosi pružatelja IoT platforme

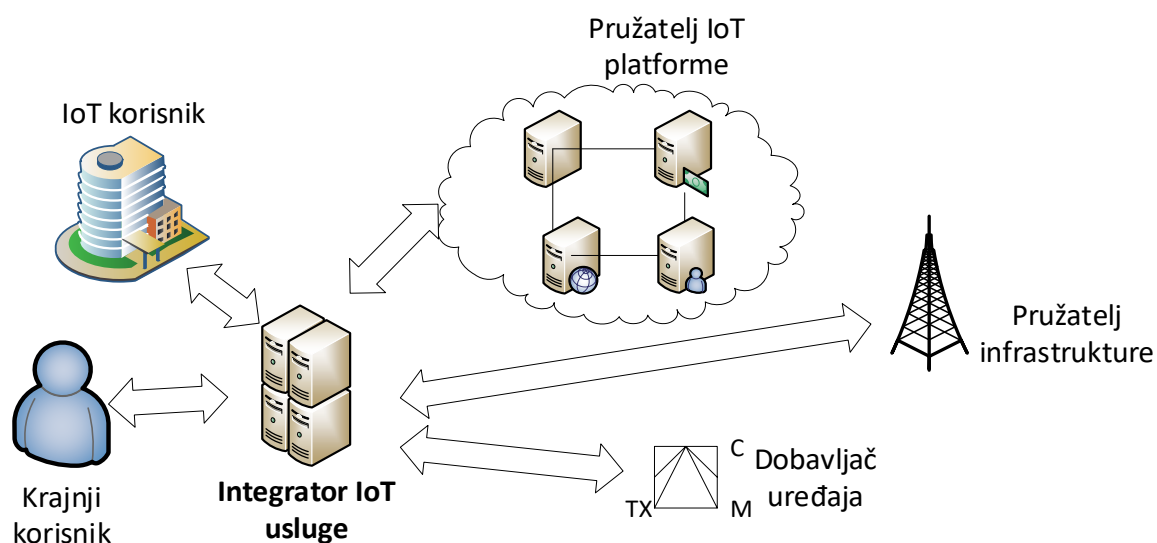
Posebna poveznica je između pružatelja IoT platforme i IoT integratora koji moraju blisko surađivati na razvoju IoT usluge. Konkretno, IoT integrator sam razvoj usluge temelji na IoT platformi.

Lanac vrijednosti IoT uloga nastavlja integrator IoT usluge čiji se mogući kontakti vide na slici 29. On u stvari prilagođava, odnosno integrira nove vrijednosti u postojeći poslovni model IoT korisnika i tako služi kao poveznica između pružatelja IoT platforme i IoT korisnika, a može imati ugovore s:

- Proizvođačem IoT uređaja radi povezivanja uređaja.
- Pružateljem infrastrukture radi usluge povezivosti i uređaja.
- Pružatelje IoT platforme za dohvaćanje informacija s uređaja.
- IoT korisnikom radi dogovoriranja funkcionalnosti usluge.
- Krajnjim korisnikom može davati i dohvaćati podatke s uređaja.

Na slici 29 uočava se kako integrator IoT usluga može imati odnose s proizvođačem IoT uređaja i pružateljem infrastrukture, a koji sačinjavaju proizvođač uređaja i pružatelj povezivosti. Naime, kod definiranja ugovora i međusobnih odnosa integratora ne zanima na

koji način će doći do podataka. To je dio oko kojeg se moraju pobrinuti pružatelj uređaja ili infrastrukture i zbog toga pružatelja povezivosti nema u mogućim međusobnim odnosima.

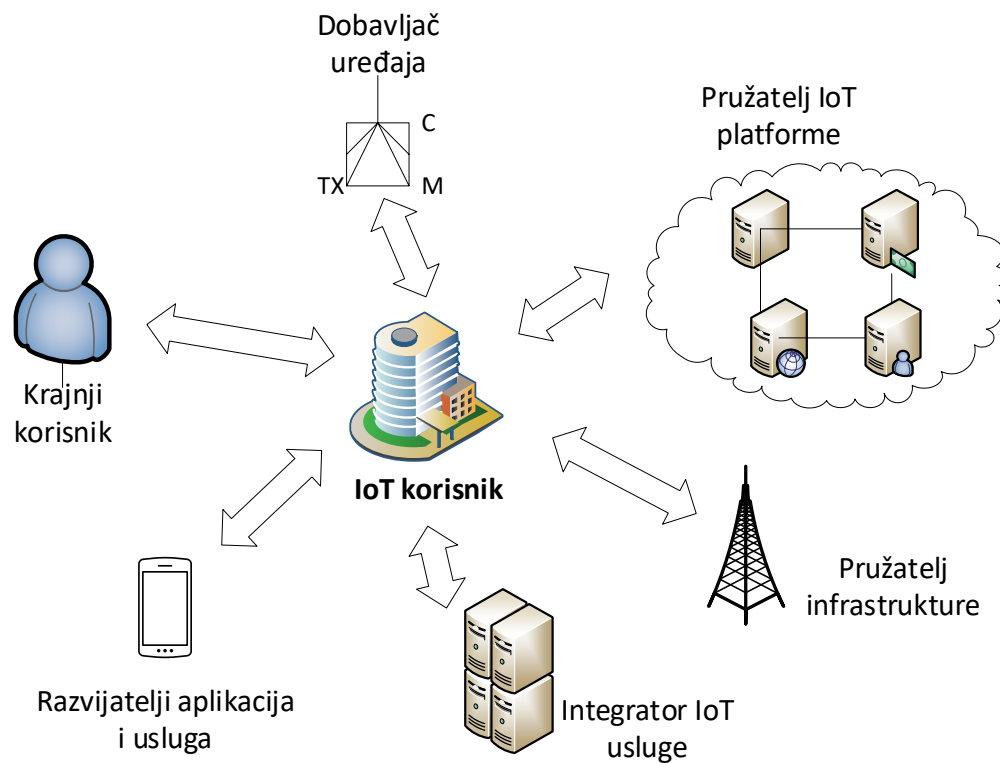


Slika 29: Mogući odnosi integratora IoT usluge

Sljedeća uloga u lancu vrijednosti je IoT korisnik. IoT korisnik je najčešće ključna figura u lancu vrijednosti budući da je on u pravilu i naručitelj same usluge. IoT korisnik je entitet koji uslugu pokušava uključiti u svoje poslovanje kako bi stvorio dodatnu vrijednost. Slika 30 prikazuje moguće odnose IoT korisnika s ostalim ulogama i to:

- Proizvođačem IoT uređaja radi definiranja vrste uređaja i funkcionalnosti.
- Pružateljem infrastrukture radi usluge povezivosti i uređaja.
- Pružateljem IoT platforme radi dohvaćanja podataka s uređaja.
- Integratorom IoT usluge radi dogovora oko funkcionalnosti usluge.
- Razvijateljem aplikacija i usluga radi dogovora oko funkcionalnosti aplikacije.
- Krajnjim korisnikom koji koristi uslugu koja je napravljena na IoT korisnika.

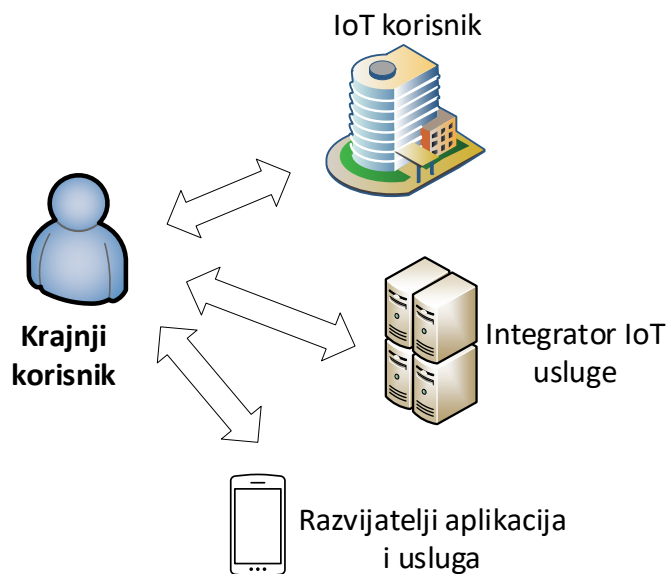
Bez IoT korisnika sam poslovni model za bilo koju ulogu osim povezivosti je vrlo teško postaviti budući da on definira poslovne procese i u njegov postojeći model se treba ugraditi nova usluga koja će dati novu vrijednost ili će u konačnosti stvoriti novi poslovni model za IoT korisnika.



Slika 30: Mogući odnosi IoT korisnika

Konačno na kraju lanca vrijednosti nalazi se krajnji korisnik koji koristi IoT uslugu. U ovisnosti o vrsti usluge krajnji korisnik uslugu može plaćati ili je koristiti besplatno i ujedno može imati odnose s (na slici 31):

- IoT korisnikom vezano uz uslugu koju koristi.
- Integratorom IoT usluge
- Razvijateljem aplikacija i usluga



Slika 31: Mogući odnos krajnjeg korisnika

Sukladno prethodno opisanim odnosima u slučaju izbijanja određenog problema, kvara ili ispada, svatko odgovara za svoj segment i za pojedinu uslugu se gleda tko je odgovoran za što. Dobar primjer kojim se mogu objasniti navedeni odnosi je usluga pametnog parkiranja koja se koristila u prethodnim poglavljima samo za razliku od primjera rađenih sa senzorima uzmimo za primjer da je detekcija slobodnih mjesta implementirana korištenjem kamera. U projektu sudjeluju proizvođač uređaja, proizvođač IoT platforme, integrator IoT usluge, IoT korisnik i krajnji korisnici. U slučaju da dođe do povrede podataka s uređaja gdje se preko slike može direktno identificirati osoba, potrebno je definirati tko je odgovoran. Krajnji korisnik koji je oštećena strana ima ugovor s IoT korisnikom i sve nastale probleme sudskim putem rješava s njime. IoT korisnik tada treba vidjeti gdje je moglo doći do povrede usluge. Naime, podaci se mogu ukrasti direktno s kamere ili nekog od povezanih sustava koji prikupljaju podatke. Nakon provjere u svojoj internoj organizaciji, IoT korisnik radi provjeru s integratorom IoT usluge budući da ima ugovor s njim. Integrator IoT usluge mora provjeriti u svojem sustavu te zatim kontaktirati pružatelja usluge IoT platforme. On ima ugovor s pružateljem IoT uređaja koji ima ugovor s pružateljem IoT povezivost. Proizvođač IoT uređaja na kraju lanca vidi da je proboj došao kod njih i da su slike uzete direktno s kamere zbog nedovoljne sigurnosne zaštite. Zakonski, prema GDPR-u, za podatke je odgovoran IoT korisnik kojeg krajnji korisnik može tužiti, ali on ima pravo na temelju svojih ugovora tužiti za naknadu štete ostale dionike u lancu kako bi naplatio svoju štetu. U ovom slučaju IoT korisnik i integrator IoT usluge nisu imali

direktne ugovore s pružateljem IoT uređaja stoga su morali posredno pitati za odgovornost i tužba ne može ići direktno već prema hijerarhiji u lancu vrijednosti. Ukoliko bi IoT korisnik imao ugovore sa svim ulogama u lancu vrijednosti (što bi mogao), onda bi se i odgovornost mogla drugačije podijeliti, odnosno, mogle bi se izbjeći odgovornosti integratora IoT usluge i pružatelja usluge platforme.

5. POSLOVNI MODEL USLUGA PAMETNIH GRADOVA

Republika Hrvatska gospodarski zaostaje za zapadnom Europom i teško može pronaći sredstva kojima bi financirala ili pomogla razvoj pametnih lokalnih sredina. Gradovi u RH, osim Grada Zagreba, imaju vrlo male i stegnute proračune kojim teško mogu nešto samostalno izgraditi. Upravo iz tog razloga u ovom poglavlju dat će se primjer poslovnog modela za sve uloge u lancu vrijednosti. Predstavljeni poslovni model uključit će regulatorna obilježja objašnjena u prethodnim poglavljima. Zbog količine podataka i tablica prikazat će se jedan primjer na usluzi pametnog parkiranja.

Isto tako predlaže se poslovni model na razini RH kojim se može pojednostaviti i pojeftini implementacija usluga pametnih gradova.

U ovom poglavlju koristi se platno poslovnog modela (engl. *Business Model Canvas*)[81] kako bi se definirali poslovni modeli svakog dionika u lancu vrijednosti. Poslovni modeli omogućuju stvaranje vrijednosti iz novih ideja. Sama ideja za novi proizvod ili uslugu nije dovoljna ukoliko se ne može odgovoriti na neka osnovna pitanja kako razviti uslugu. Isto tako, altruizam nije osnova za stvaranje platforme na kojoj se mogu pružati važne usluge, posebno u sektorima kao što su razvoj i socijalno poduzetništvo.

Platno poslovnog modela nudi precizne alate koji navode na razmišljanje o poslu, a istovremeno drži vrlo vidljivima ključne točke kako za onoga koji model definira, tako i za cijeli tim i sve ostale dionike. Najjednostavnije rečeno, platno poslovnog modela pruža okvir za dobivanje najvećih vrijednosti iz novih ideja uz istovremeno objektivno sagledanje svih potencijalnih rizika i pretpostavki koje one donose.

Za postavljanje poslovnog modela potrebno je odgovoriti na neka osnovna pitanja koja se tiču svih dionika u projektu. Pitanja su zajednička i možemo ih podijeliti u nekoliko skupina:

- Ključni partneri: koji su ključni partneri u projektu? Koji su glavni dobavljači? Koje glavne resurse trebamo od partnera? Koje ključne aktivnosti partner provodi?
- Ključne aktivnosti: koje ključne aktivnosti su potrebne za provođenje našeg prijedloga rješenja? Distribucijski kanali? Odnos s kupcima? Prihodi?

- Ključni resursi: koji su ključni resursi potrebni za naše rješenje? Koji distribucijski kanali? Kakvi odnosi s kupcima? I kakvi prihodi?
- Prijedlog vrijednosti: koje vrijednosti se donose kupcu? Koje probleme mu našim vrijednostima rješavamo? Koji skup proizvoda ili usluga nudimo? Koje potrebe kupca ispunjavamo našim rješenjem?
- Odnosi s kupcima: kakve odnose svaki segment našeg kupca očekuje da ostvarimo s njima? Koje smo već ostvarili? Kako je to uključeno u naš poslovni model? Koliko nas to košta?
- Kanali: kroz kakve kanale naš kupac želi biti kontaktiran? Kako sad dolazimo do njih? Kako su naši kanali integrirani? Koji pokazuje najbolje rezultate? Koji je cjenovno najpovoljniji? Kako ih integriramo s rutinom kupca?
- Segment kupca: za koga stvaramo novu vrijednost? Koji su naši najvažniji kupci?
- Struktura troškova: koji su najznačajniji troškovi u našem poslovnom modelu? Koji su ključni resursi najskuplji? Koje su ključne aktivnosti najskuplje?
- Izvori prihoda: koliko su kupci spremni platiti proizvod? Koliko trenutačno plaćaju? Kako trenutačno plaćaju? Kako bi željeli plaćati? Kako svaki od izvora prihoda doprinosi ukupnim prihodima?

Navedene stavke mogu se predložiti u tablici koja čini platno poslovnog modela i daje vrlo jasan pregled svih rizika, aktivnosti i resursa uz potrebne izvore prihoda kako bi projekt bio uspješan. Slika 32 prikazuje primjer jednog takvog platna poslovnog modela.

 Ključni partneri Koji su naši ključni partneri? Koji su naši ključni dobavljači? Koje ključne resurse trebamo od partnera? Koje ključne aktivnosti rade naši partneri? •	 Ključne aktivnosti Koje ključne aktivnosti naša ideja treba? Distribucijski kanali? Odnosi s kupcima? Izvori prihoda? •	 Prijedlog vrijednosti Koje vrijednosti donosimo kupcu? Koje probleme kupca rješavamo? Koje skupove proizvoda ili usluga nudimo pojedinim segmentima kupca? Koje potrebe kupca ispunjavamo? •	 Odnosi s kupcima Kakve odnose svaki segment našeg kupca očekuje da ostvarimo s njima? Koje smo uspostavili? Kako su integrirani u naš poslovni model? Koliki je to trošak? •	 Segment kupaca Za koga stvaramo vrijednost? Tko su naši najvažniji kupci? •
 Struktura troškova Koji su najznačajniji troškovi u našem poslovnom modelu? Koji su ključni resursi najskuplji? Koje su ključne aktivnosti najskuplje? •		 Izvori prihoda Koliko su kupci spremni platiti proizvod ili uslugu? Koliko trenutno plaćaju? Kako trenutno plaćaju? Kako bi voljeli plaćati? Koliko svaki od izvora prihoda doprinosi ukupnim prihodima? •		

Slika 32: Primjer platna poslovnog modela

5.1. Poslovni model usluge pametnog parkiranja

Gradovi diljem svijeta koji započinju preobrazbu iz tradicionalnog grada u inteligentni, samoodrživi gradovi obično započinju s uslugama koje će riješiti njihova uska grla, odnosno probleme koji trenutno predstavljaju najveći izazov za grad. Prometne gužve u većini velikih gradova svijeta predstavljaju velik problem koji najčešće nastaje zbog spore vožnje vozača koji traže parkirno mjesto. Jedan od načina kako riješiti navedeni problem je korištenje usluge pametnog parkiranja. Na taj način vozači više ne bi trebali tražiti parkirno mjesto već bi dolazili na unaprijed definirana parkirna mjesta što bi smanjilo gužve u gradovima i do 70%[76].

Kod izrade modela usluge potrebno je uzeti u obzir sve aspekte, odnosno, svaka uloga u lancu vrijednosti ima svoj poslovni model i za svaku od njih potrebno je izraditi platno poslovnog modela. Jedino kod krajnjeg korisnika se ne radi platno poslovnog modela jer on uslugu kupuje i konzumira je te je kao dionik u lancu vrijednosti u stvari potrošač. Jedino kod usluga internetskog društva gdje i krajnji korisnici sudjeluju u generiranju podataka, same usluge su u pravilu besplatne, ali i dalje poslovni model za krajnjeg korisnika je zanemariv i stoga se u ovom radu neće obrađivati poslovni model sa strane krajnjeg korisnika.

Kod izrade poslovnog modela bitno je znati koji su ključni kupci, a to se može vidjeti iz odnosa dionika u lancu vrijednosti koje je navedeno u poglavlju 4.3. Naša usluga pametnog parkiranja sastoji se od sljedećih dionika:

- IoT korisnika
- Pružatelja IoT platforme
- Integratora IoT usluge
- Proizvođača uređaja
- Pružatelja povezivosti
- Razvijatelj aplikacija i usluga
- Krajnjeg korisnika

U našem slučaju za krajnjeg korisnika se poslovni model neće raditi budući da je on potrošač i kao takav ne generira neku dodatnu vrijednost u lancu vrijednosti. IoT korisnik je centralna uloga i on definira procese i nove vrijednosti koje mu u projektu trebaju. IoT korisnik bi u našem slučaju bilo poduzeće koja nadzire, održava i naplaćuje parkirna mjesta u gradu (na

primjer ZagrebParking ili iz prethodnog primjera SplitParking). U našem primjeru želi se omogućiti kroz jednostavnu mobilnu aplikaciju pregled svih parkirnih mjesta u gradu, navigaciju do njih te mogućnost rezervacije parkirnog mjesta podizanjem parkirnog stupića. Također, kroz aplikaciju se želi dati mogućnost prijave pogrešno parkiranih vozila čime bi se ubrzalo uklanjanje nepropisno parkiranih vozila, ali i smanjila potreba za stalnim izlaskom na teren pauk vozila što bi dovelo do uštede.

Proizvođač uređaja će ponuditi opremu, tj. senzore, rampe i sve što je potrebno kako bi se moglo detektirati slobodno i rezervirati parkirno mjesto.

Pružatelj povezivosti daje konekciju prema internetu i to je u pravilu pružatelj elektroničke komunikacijske infrastrukture koji uslugu povezivosti može pružiti putem mreža nepokretnih komunikacija ili upotrebom nekog vida bežične tehnologije kao što je LTE, 5G, LoraWAN, Sigfox, Wifi i slično.

Pružatelj IoT platforme pruža platformu koja je poveznica između uređaja i aplikacije, odnosno, IoT usluge te služi za povezivanje svih drugih bilo budućih ili postojećih usluga preko iste platforme kako bi se podaci mogli dijeliti između usluga i time dodavati nove vrijednosti većini usluga. Osim toga, jedan od ključnih zadataka pružatelja IoT platforme je upravljanje i nadgledanje postavljenih umreženih uređaja.

Integrator IoT usluga mora sve procese uklopiti u poslovni model IoT korisnika, dok razvijatelj aplikacija i IoT usluga na temelju podataka primljenih od integratora izrađuje aplikaciju za mobilni uređaj preko koje će se vršiti pregled slobodnih mjesta, rezervacija i plaćanje.

Na sljedećim stranicama dan je pregled platna poslovnog modela za sve uloge osim pružatelja povezivosti koji je zakonski reguliran i njegov poslovni model je jasno propisan te ga nema potrebe posebno razrađivati. Specifičnost je upotreba tehnologija koje koriste nelicencirani spektar koji nije štićen od strane države te time nije niti reguliran i ovakav poslovni model nije posebno razrađen u ovoj disertaciji.

 <i>Ključni partneri</i> • Proizvođač IoT platforme • Integrator IoT usluge • Pružatelj usluge povezivosti • Proizvođači elektroničkih komponenti • Proizvođači kutija	 <i>Ključne aktivnosti</i> • Proizvodnja uređaja • Ugradnja senzora • Postavljanje stupića • Razvoj cjenovnog modela • Razvoj API-ja za dohvat podataka  <i>Ključni resursi</i> • Elektroničke komponente za izradu uređaja • Stručnjaci za HW • Stručnjaci za SW • Alat za programiranje mikrokontrolera i API-ja.	 <i>Prijedlog vrijednosti</i> • Putem jednostavnih standardiziranih sučelja dostupno: • Obavijesti o zauzeću parkirnih mjesta • Jednostavno podizanje i spuštanje rampi	 <i>Odnosi s kupcima</i> • Korisnička podrška u slučaju grešaka • Brza reakcija kod kvarova uređaja  <i>Kanali</i> • Direktna prodaja pružateljima platforme, integratoru usluga ili IoT korisniku • Digitalni marketing	 <i>Segment kupaca</i> • Pružatelji usluge platforme • Integratori IoT usluga • IoT korisnik
 <i>Struktura troškova</i> • Razvoj hardvera i softvera • Licence za softver • Prodaja, marketing • Usluga montaže uređaja, održavanje		 <i>Izvori prihoda</i> • Postotno povećanje u odnosu na troškove proizvodnje • Naplata usluge montaže (50% na RUC) • Godišnje održavanje (% vrijednosti projekta)		

Slika 33: Platno poslovnog modela za **proizvođača uređaja**

 Ključni partneri - IoT korisnik - Integrator IoT usluge - Proizvođač IoT uređaja - Razvijatelj aplikacija i usluga	 Ključne aktivnosti - Razvoj platforme - Rješavanje sigurnosnih pitanja - Interoperabilnost i otvorenost prema aplikacijama - Cjenovni model	 Prijedlog vrijednosti - Za IoT korisnika Multifunkcionalna platforma otvorenog tipa; interoperabilna s mogućnošću jednostavne integracije s drugim sustavima ili uslugama - Za IoT integratora Integracija svih uređaja dostupnih na platformi kroz standardizirana sučelja. - Dobavljanje podataka s uređaja	 Odnosi s kupcima - Korisnička podrška 24 sata - Brza reakcija na ispade, kvarove ili sigurnosne propuste - Pouzdan partner	 Segment kupaca - IoT integrator - IoT korisnik
 Struktura troškova - Razvoj, hosting i licence - Prodaja, marketing - Održavanje			 Izvori prihoda - Surge pricing kod prodaje platforme - Naplata prema broju korisnika (uređaja) ili količini generiranih podataka - Godišnje održavanje (% od cijene projekta)	

Slika 34: Platno poslovnog modela za **pružatelja usluge platforme**

 Ključni partneri • Pružatelj IoT platforme • IoT korisnik • Razvijatelj aplikacija i usluga • Pružatelj usluge naplate	 Ključne aktivnosti • Integracija usluge u postojeće procese • Rješavanje regulatornih problema (sigurnost, privatnost) • Jasno definirani zahtjevi i procesi  Ključni resursi • Tehnološka platforma • Stručnjak za razvoj na platformi • Alat za razvoj na platformi • SW arhitekt	 Prijedlog vrijednosti • Integracija postojećih procesa s novim vrijednostima kako bi se razvila nova usluga • Integracija mobilne aplikacije sa službom za odvoz vozila kako bi mogli zaprimati obavijesti od korisnika	 Odnosi s kupcima • Korisnička podrška • Prema IoT korisniku transparentno, sigurno, odgovorno i pouzdano • Prema platformi pouzdan i siguran partner  Kanali • Direktna prodaja • Digitalni marketing • Javna nabava	 Segment kupaca • IoT korisnik • Pružatelj IoT platforme
 Struktura troškova • Razvoj – trošak plaća ljudi • Licence za razvojnu okolinu • Prodaja, marketing • Trošak smještaja (deployment) usluge		 Izvori prihoda • Iznos uvećan od svih rashoda za x% • Godišnje održavanje 20% vrijednosti ugovorenog posla		

Slika 35: Platno poslovnog modela za **integratora IoT usluge**

 <i>Ključni partneri</i> • Pružatelj IoT platforme • Integrator IoT usluge • IoT korisnike • Pružatelj karata za mobilnu aplikaciju • Pružatelj navigacijske usluge za mobilnu platformu	 <i>Ključne aktivnosti</i> • Razvoj mobilne aplikacije • UX dizajn • Integracija karata i sustava za navigaciju • Rješavanje sigurnosnih pitanja	 <i>Prijedlog vrijednosti</i> • Mobilna aplikacija ima jednostavno sučelje za: Traženje parkirnog mjesta Plaćanje p.m. Rezervaciju p.m. Navigaciju • Jednostavno sučelje za prijavu krivo parkiranih vozila od strane korisnika	 <i>Odnosi s kupcima</i> • Korisnička podrška za mobilnu aplikaciju • Pouzdan i siguran partner prema svim ključnim partnerima	 <i>Segment kupaca</i> • IoT korisnik • Integrator IoT usluge • Pružatelj IoT platforme
 <i>Struktura troškova</i> • Trošak razvoja • Licenca za mobilne platforme • marketing		 <i>Izvori prihoda</i> • Prodaja usluge razvoja i odžavanja mobilne aplikacije.		

Slika 36: Platno poslovnog modela za **razvijatelja aplikacija i usluga**

 <i>Ključni partneri</i> • Pružatelj IoT platforme • Integrator IoT usluge • Razvijatelj aplikacija i usluga	 <i>Ključne aktivnosti</i> • Definiranje svih funkcijskih i nefunkcijskih zahtjeva usluge • Implementacija regulatornih problema (sigurnost)	 <i>Prijedlog vrijednosti</i> • Za krajnje korisnike: Mogućnost traženja parkirnog mjesta. Mogućnost rezervacije. Mogućnost plaćanja. Mogućnost slanja obavijesti o krivom parkiranju. • Za ostale: Pouzdan partner	 <i>Odnosi s kupcima</i> • Služba za korisnike	 <i>Segment kupaca</i> • Krajnji korisnici
 <i>Struktura troškova</i> • Nabava platforme, integracija, nabava mobilne aplikacije (ugovor direktno s IoT integratorom koji rješava sve navedeno) • Osoba za definiranje procesa i vođenje projekta • Marketing		 <i>Izvori prihoda</i> • Naplata parkirnog mjesta po satu • Naplata dnevnih karata		

Slika 37: Platno poslovnog modela za **IoT korisnika**

Iz platna poslovnih modela za pojedine korisnike (slike 33-37) vidljivo je što svaka uloga u projektu vidi kao aktivnosti i koji je njen poslovni model. Također, za svaku od usluga su uzete u obzir i regulatorne mjere definirane u preporukama (tablica 5) iz prethodnog poglavlja.

Na temelju preporuka i predložka platna poslovnog modela lako se može uvidjeti ima li pojedina usluga prostora za uspjeh, odnosno imaju li svi dionici u lancu uspješan poslovni model na kojem bi temeljili svoj poslovanje.

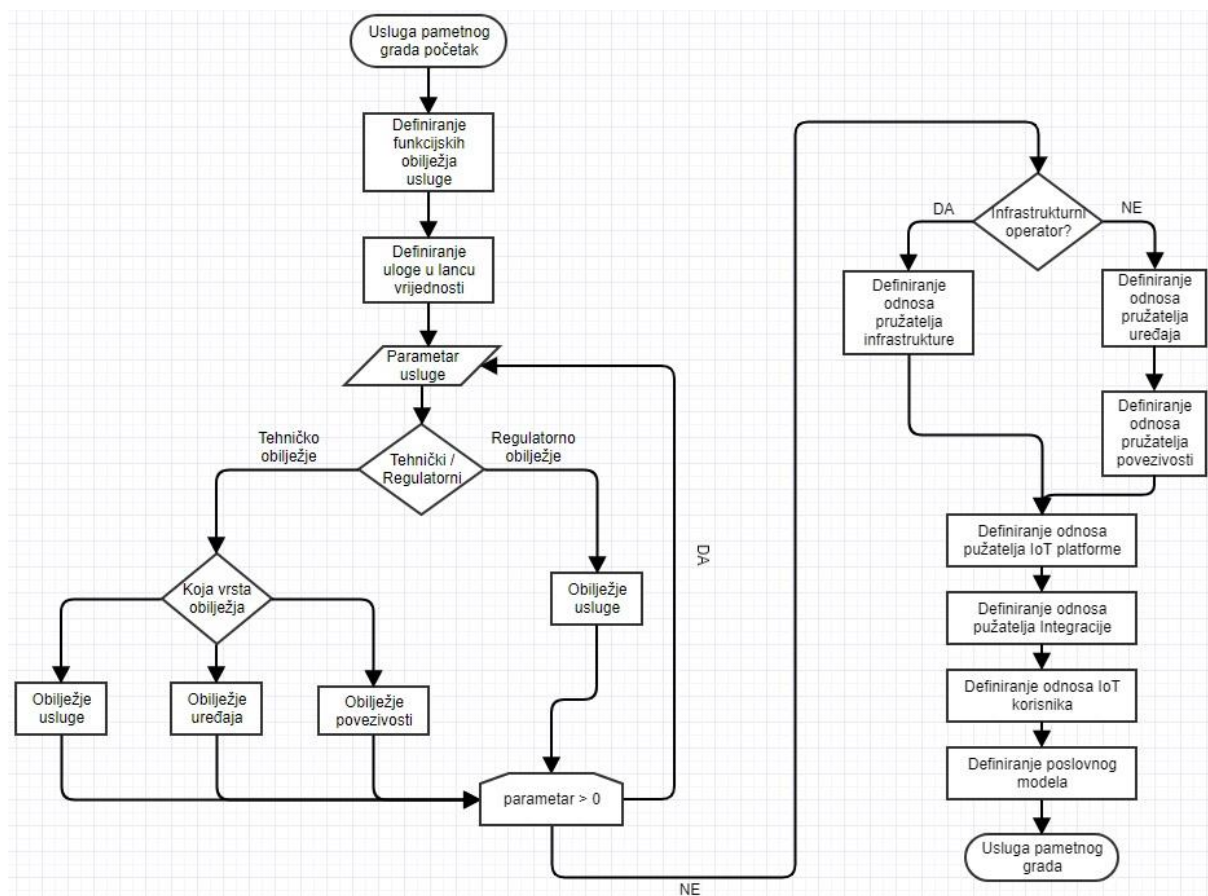
5.2. Metoda za definiranje regulatornih zahtjeva i analiza njihovog utjecaja na usluge Interneta stvari u području pametnih gradova

Prilikom dizajniranja usluge pametnih gradova potrebno je precizno definirati funkcijske zahtjeve, te ostaviti mogućnost za njihova proširenja. S problemima koje usluga pametnih gradova treba riješiti najviše su upoznati stručnjaci u gradskim odjelima i sektorima gdje se problemi i javljaju. Međutim, ti isti ljudi najčešće nisu dovoljno samostalni da bi definirali zahtjeve usluge koja će riješiti njihov problem. Stoga se moraju pouzdati u vanjske konzultantske kuće ili direktno surađuju s integratorskim poduzećima koje taj posao odrađuju za njih.

Kako bi se taj dio olakšao, odnosno, kako bi ljudi u gradskim službama mogli na jednostavan način dizajnirati uslugu pametnih gradova, predstavljena je metoda za definiranje regulatornih zahtjeva i analiza utjecaja na usluge Interneta stvari u području pametnih gradova.

Na slici 38 prikazan je algoritam koji prati korake opisane u ovoj disertaciji, a kojim se na jednostavan način može identificirati obilježja usluge pametnih gradova te izraditi dizajn same usluge.

Algoritam započinje pitanjem koje probleme usluga treba riješiti, odnosno, definiranjem funkcijskih zahtjeva usluge. Ovdje se obično radi popis svih procesa i njihovih funkcija koje su obuhvaćene uslugom pametnih gradova i analizira koji dio može biti unaprijed upotrebom IKT-a i usluga pametnih gradova. Nakon definiranja svih zahtjeva nad uslugom, potrebno je definirati uloge u lancu vrijednosti budući da različite uloge u lancu vrijednosti imaju i različite obveze vezane uz regulatorna obilježja predstavljena u poglavlju 4.



Slika 38: Algoritam za definiranje usluge pametnog grada

Utvrđivanjem uloge u lancu vrijednosti, a na temelju prethodno definirane taksonomije, mogu se za pojedinu uslugu pametnih gradova odrediti za nju svojstvena obilježja. Za svaki parametar usluge određuje se je li tehnički ili regulatorni parametar, te za tehničke parametre se određuje jedna od tri vrste obilježja: obilježje usluge, obilježje uređaja ili obilježje povezivosti. Ovaj proces se ponavlja dokle god postoje dostupni parametri usluge pametnog grada. Završetkom ovog procesa definirana su obilježja usluge pametnog grada čime se započinje postupak definiranja odnosa između dionika u lancu vrijednosti.

Temeljem predložene metode gradovi će moći brže definirati usluge i sve zahtjeve koje usluga pametnog grada koju žele uvesti treba ispuniti.

5.3. Prijedlog poslovnog modela za države male i srednje veličine poput RH

Velik broj gradova u svijetu krenuo je u proces digitalne transformacije u pametne gradove, međutim još uvijek velik broj njih razmišlja kako i na koji način napraviti takvu transformaciju. Stariji gradovi većinom imaju dotrajale infrastrukture i pitanje je kako započeti proces transformacije.

Koncept pametnog grada omogućava efikasnije vođenje grada, te pružanje kvalitetnije usluge po povoljnijoj cijeni uz istovremeno stvaranje privlačnijeg mjesta za život i rad građana. Cilj je integrirati najvažnija područja primjene, odnosno, usluge grada. Na taj način se omogućava integrirano upravljanje gradom. Unaprjeđuje se pružanje usluga svim dionicima i povećava se kvaliteta života, kompetitivnosti i održivost.

Kako bi se ubrzao koncept rješenja pametnog grada, potrebno je dodatno stimulirati tržište, a jedan od načina je svakako standardizirana i otvorena gradska platforma. Takva platforma predstavlja centralno mjesto za prikupljanje podataka koji se proslijeđuju odgovarajućoj službi, a ujedno nudi i otvorena sučelja za treću stranu ukoliko želi raditi nove vrijednosti na temelju otvorenih podataka.

Kod digitalne transformacije, najveći izazov gradovima uz nedostatak znanja i kadrova koji bi transformaciju proveli, svakako je pronalazak financijskih sredstava za realizaciju projekata. Usluge pametnih gradova mogu biti u vlasništvu grada i gradskih tvrtki ili mogu biti putem koncesija dodijeljene privatnim tvrtkama koje će realizirati uslugu.

Od financijskih izazova najveći izazov za gradove predstavlja nabava IoT platforme preko koje prolaze svi podaci i na kojoj se podaci čuvaju i obrađuju predstavlja jedan od najvećih financijskih izdataka za jedinice lokalne samouprave.

Slijedom navedenog bez pomoći države razvoj pametnih gradova u RH ostat će tek na pojedinačnim istupima nekih gradova u pojedine tehnološki napredne usluge ili će ovisiti o zakonskim uredbama koje će propisati implementaciju pojedine pametne usluge, poput elektroničkog praćenja odvoza otpada koje su svi gradovi već trebali implementirati.

Također postavlja se i pitanje usluga koje se protežu kroz više sektora i/ili više domena. Na primjer usluge vezane uz cestovni promet zadiru u nadležnost i gradskih cesta, županijskih cesta i državnih cesta. Ukoliko se želi napraviti aplikacija koja će funkcionirati, potrebno je povezati sve tri domene (gradsku, županijsku, državnu) pod jednu uslugu. Stoga bi država na nacionalnoj razini mogla postaviti IoT platformu (Slika 39) kojoj će ciljani korisnici biti

jedinice lokalne samouprave (gradovi) uz mogućnost proširenja usluge na vatrogasce, policiju, hitnu pomoć i sve ostale javne službe. Svaki grad bi imao svoj pristup i na platformi bi mogao graditi svoje usluge. Također, usluge na nacionalnoj razini bile bi dostupne svim korisnicima usluge. Gradovi bi na temelju svojih mogućnosti proširivali skup usluga koje bi nudili građanima u ovisnosti o razvoju infrastrukture (širokopojasni pristup, senzori).

Razvoj usluga trebao bi biti jednostavan, odnosno, sam pristup platformi trebao bi biti što jednostavniji s otvorenim sučeljem. Tvrtke ili fizičke osobe koje se bave razvojem usluga bi mogle imati mogućnost pristupa senzorima i aktuatorima za potrebe razvoja usluga. Isti bi morali biti registrirani kod pružatelja usluge platforme uz odobrenje jedinica lokalne samouprave za koje se radi razvoj. Radi bržeg razvoja, sam proces registracije trebao bi biti jednostavan.

U modelu bi postojale tri razine usluga:

1. Usluga koristi svoje senzore/aktuatore i svoju aplikaciju
2. Usluga koristi postojeću infrastrukturu, npr. podatke s postojećih senzora dostupnih putem platforme, i na temelju njih se pruža usluga
3. Ne koriste se senzori/aktuatori već na temelju dostupnih podataka se pruža usluga ili platforma služi za prikupljanje podataka s pametnih uređaja (tableti, mobiteli) na temelju čega se pruža usluga.

Ovakvim poslovnim modelom, jedinice lokalne samouprave dobile bi brži i jednostavniji pristup implementaciji usluga pametnih gradova te bi uklonili veliku prepreku, a to je IoT platforma, počevši od same nabave, konfiguracije do održavanja.

Ukoliko bi platforma bila ponuđena na državnoj razini svim gradovima, početna investicija, odnosno mjesečni najam i samo održavanje platforme, za gradove bi bila značajno povoljnija, tj. takav trošak bi si gradovi mogli priuštiti.

Takva platforma mogla bi biti smještena u neko od državnih poduzeća koje se bavi područjem djelovanja elektroničkih komunikacija. Primjerice, poduzeće Odašiljači i veze d.o.o., koje je u vlasništvu RH, objedinjuje svu svjetlovodnu infrastrukturu svih trgovačkih društava u vlasništvu RH stoga bi bilo logično da oni ujedno budu vlasnik takve platforme. U ovisnosti o različitim poslovnim modelima Odašiljači i veze d.o.o. ujedno mogu biti i pružatelj povezivosti davanjem LoRaWAN ili WiFi tehnologije koja može biti smještena na njihovim lokacijama i odašiljačima u RH.

Sukladno gore navedenom modelu na jednostavnom primjeru usluge pametnog parkinga uloge u modelu su sljedeće:

Proizvođač senzora: privatno poduzeće

Pružatelj povezivosti: HT, A1 Hrvatska ili Tele2 preko LTE ili neko privatno poduzeće ukoliko koristi WiFi ili LoraWan tehnologiju.

Pružatelj IoT platforme: Odašiljači i veze d.o.o. (OiV)

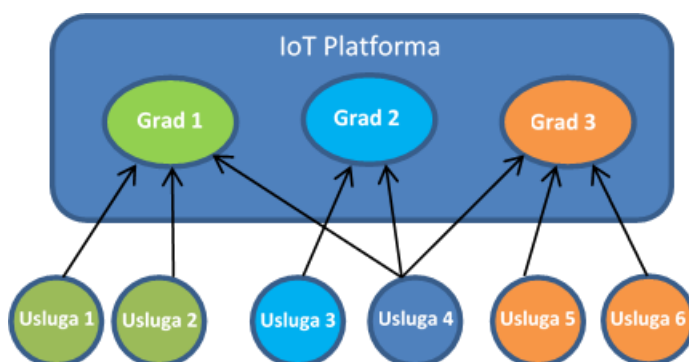
Integrator IoT usluge: Privatno poduzeće koja se bavi integracijom

IoT korisnik: npr. Zagreb parking

Razvijatelj aplikacija i usluga: Privatno poduzeće koje se bavi razvojem mobilnih aplikacija

Krajnji korisnik: građani

Poslovni model za OiV: OiV za korištenje svoje platforme od gradova uzima naknadu. IoT korisnici također plaćaju naknadu OiV-u (osim ukoliko je to drugačije dogovoreno s gradovima). Prema modelu OiV bi mogao ući i u izgradnju same infrastrukture (širokopojasni pristup, senzori).



Slika 39: Model IoT platforme za usluge pametnih gradova

Slika 39 daje prikaz predloženog poslovnog modela za države male i srednje veličine poput RH gdje postoji jedna platforma na razini države, a županije, gradovi i općine mogu za svoje potrebe u najam uzimati usluge po vertikali. Tako se mogu i jednostavno replicirati usluge za različite gradove, ali i usluge koje prelaze više sektora i dimenzija mogu se korištenjem ovakvog poslovnog modela jednostavno implementirati i time smanjiti probleme međusobnih odnosa u lancu vrijednosti kroz više sektora.

Mnogi gradovi već imaju vertikalno razvijene usluge koje su preteča današnjih digitalnih usluga te koje rade i mogu se koristiti samo na platformama specijaliziranim za

pojedina područja. Stoga, ukoliko je potrebno, može se uzeti u obzir neka od platformi koje služe za interoperabilnost različitih sustava kako bi se međusobno povezali. Primjer jednog takvog programskog rješenja za integraciju i interoperabilnost je symbIoTe. Kroz takvu platformu moguće je pristupati senzorima, aktuatorima i drugim IoT uređajima koji se nalaze na drugim IoT platformama.

6. ZAKLJUČAK

Ubrzani porast populacije u gradovima diljem svijeta stvara konstantan pritisak na postojeću infrastrukturu u gradovima koja više nije adekvatna. U većini gradova infrastruktura je dotrajala. Primjerice, vodovodne cijevi pod pritiskom često pucaju te su načete brojnim pukotinama što dovodi do velikih financijskih gubitaka. Komunalna poduzeća mogu uštedjeti između 7,1 i 12,5 milijarde dolara godišnje korištenjem rješenja pametnog korištenja voda¹⁰.

Zbog navedenog gradski oci su primorani raditi promjene iz tradicionalnih gradova u digitalne, pametne i samoodržive gradove kroz dugoročne strategije i planove za razvoj gradova u sljedećih 20-30 godina. Također, tehnologija se vrlo brzo mijenja, a istovremeno tehnologiju ne prati zakonski okvir kako bi se prilagodio svim inovacijama i tehnološkim promjenama. Kao rezultat imamo potencijalne nove usluge koje mogu donijeti gradovima značajne uštede u svim segmentima, ali ne mogu biti implementirane jer su u suprotnosti s nekim zakonskim odredbama. Iz toga razloga, vlade u svijetu pokušavaju postaviti pravila u skladu s današnjom tehnologijom. Glavni fokus je kako približiti tehnologiju građanima podizanjem svijesti i povjerenja u tehnologiju. Primjer promjene zakonskih okvira kako bi se prilagodio promjenama u tehnologiji može se vidjeti u obrazovanju. Krajem 2018. godine u RH je donesen zakon kojim se po prvi put spominju digitalni udžbenici čime napokon i obrazovanje ulazi u digitalnu sferu.

Tehnologija je ključna komponenta digitalne transformacije bez koje sigurno ne bi bilo napretka i upravo iz tog razloga postoje brojna istraživanja koja su usmjerena na tehničke aspekte usluga pametnih gradova. Za razliku od njih, u ovoj disertaciji u analizu su uzeti i tehnološki i regulatorni aspekti usluga pametnih gradova kako bi mogli gradskim službama, razvijateljima usluga, ali i svim ostalim dionicima u lancu vrijednosti IoT usluga predložiti preporuke koje su važne za njihove obveze i zaduženja u ekosustavu usluga pametnih gradova.

U ovoj disertaciji predložena je taksonomija koja je pobrojala i napravila kategorizaciju relevantnih tehnoloških i regulatornih obilježja usluga pametnih gradova. Odabrana su četiri studijska slučaja na kojima je napravljena analiza na temelju predložene taksonomije. Od usluga pametnih gradova odabrane su usluge pametnog parkiranja, pametnog brojila električne energije, suradnog opažanja okoline u pokretnu za nadgledanje kvalitete zraka i usluga pametne javne ulične rasvjete. Na temelju ovog modela za svaku od uloga u lancu vrijednosti Interneta

¹⁰ SAM Study, Water: a market of the future 2010

stvari dana je specifična preporuka vezana uz regulatorna obilježja koja utječu na poslovanje i koja trebaju biti ispunjena kako bi se ostvario uspješan projekt usluge pametnog grada. Postoje mnoga tehnička i regulatorna obilježja za usluge pametnih gradova, međutim, ne mora se svaka uloga u IoT lancu vrijednosti fokusirati na sva obilježja. Stoga ovakav pristup, kroz regulatorne preporuke pojednostavljuje i ubrzava njihove poslovne analize.

Osim toga u disertaciji su prikazani odnosi u lancu vrijednosti iz kojih je vidljivo tko s kim može komunicirati ukoliko ima potrebe u ovisnosti o usluzi. Na temelju međusobnih odnosa dan je primjer usluge gdje je došlo do povrede osobnih podataka. Iz navedenog primjera vidi se tko je odgovoran za koji segment, odnosno što se događa ukoliko krajnji korisnik prijavi neovlašteno korištenje svojih osobnih podataka.

Zadnji segment disertacije daje općeniti prikaz poslovnih modela kroz primjer platna poslovnog modela. Opisana su sva obilježja takvog modela i kako se na njemu mogu unaprijed definirati svi poslovni aspekti i predvidjeti ključni partneri, aktivnosti, potrebni resursi, svi troškovi, ali i mogući prihodi. Usluga pametnog parkiranja uzeta je kao primjer na kojem je napravljena analiza poslovnog modela za sve uloge u lancu vrijednosti iz kojih je vidljivo da svaka od uloga u lancu vrijednosti može pronaći svoj uspješan poslovni model. Izuzet je jedino krajnji korisnik koji nema nikakve prihode.

Treći doprinos u disertaciji je metoda za definiranje tehničkih i regulatornih obilježja. Proces dizajniranja usluga pametnih gradova potrebno je pojednostaviti što je više moguće kako bi ljudi u gradskim službama lakše mogli pristupiti izradi zahtjeva za usluge pametnih gradova. Stoga je predstavljena metoda za definiranje regulatornih zahtjeva i analiza utjecaja na usluge Interneta stvari u području pametnih gradova.

U disertaciji je zbog svojih specifičnosti dan i poseban poslovni model za manje i srednje države veličine Republike Hrvatske. Naime, jedinice lokalne samouprave u državama slabijeg gospodarstva vrlo teško mogu financirati početak digitalne transformacije. Čak je i Europska komisija u [12] prepoznala da države s nižim BDP-om treba podržati te pokušati pronaći drugačiji pristup za pronalazak financijskih sredstava. Za razliku od gradova zapadne Europe koji sami financiraju projekte ili povlače sredstava iz EU fondova uz repliciranje rješenja koja su već implementirana u nekim gradovima, gradovi država s nižim BDP-om vrlo teško mogu financirati transformaciju pa čak i postotak koji trebaju izdvojiti ukoliko sredstva

povlače iz fondova. Upravo iz tog razloga EK predlaže da se takve države međusobno udruže i između sebe podjele rješenja i usluge koje su same razvile. Među uslugama koje su obuhvaćene ovim prijedlogom Europske Komisije, svakako su usluge koje uključuju više domena i više sektora, poput primjerice usluge u transportu.

U takvim uslugama koje uključuju više domena i sektora ključna uloga u lancu je pružatelj usluge platforme koji predstavlja središnju točku. Svi uređaji i sve usluge su distribuirane preko te točke te se različite nove vrijednosti mogu stvarati korištenjem istih podataka u različitim uslugama. Povezivanjem javnih tijela na nacionalnoj razini na istu platformu mogu se razviti vrlo kompleksne i zahtjevne usluge koje pojednostavljaju procese koji su danas nezamislivi u digitalnom obliku.

Na temelju navedenih zahtjeva predložen je poslovni model za države slabijeg gospodarstva poput RH gdje se kroz jedno državo tijelo može ponuditi integrativna platforma koja će ispuniti zahtjeve na nacionalnoj razini, ali ujedno i vertikalno gradovima može ponuditi pristup za njihove usluge. Time se rješava najskuplji segment usluga pametnih gradova, a to je pružatelj usluga IoT platforme za pametne gradove te se jedinice lokalne samouprave mogu orijentirati na druge segmente kod izrade usluga uz istovremeno iskorištavanje podataka s nacionalne razine.

Usluge pametnih gradova u narednom periodu ubrzano će se razvijati i to ne samo zbog entuzijazma gradonačelnika već i zbog same potrebe gradova koji više neće moći funkcionirati na klasičan način zbog sve većeg priljeva populacije.

LITERATURA

- [1] „ITU Internet Reports 2005: The Internet of Things“, International Telecommunication Union
- [2] A. AntoniĆ, „Platforme za obradu podataka u stvarnom vremenu u području Internet objekata“, izvještaj za kvalifikacijski doktorski ispit, 2013.
- [3] John Soldatos, Nikos Kefalakis, Manfred Hauswirth, Martin Serrano, Jean-Paul Calbimonte, Mehdi Riahi, Karl Aberer, Prem Prakash Jayaraman⁴, Arkady Zaslavsky, Ivana Podnar Žarko, Lea Skorin-Kapov and Reinhard Herzog. OpenIoT: Open Source Internet-of-Things in the Cloud, Invited paper, to appear in Lecture Notes in Computer Science, vol. 9001, 2015.
- [4] “World Urbanization Prospects: The 2018 Revision”, United Nations, Department of Economic and Social Affairs, svibanj 2018
- [5] The White House. FACT SHEET: Administration Announces New “Smart Cities” Initiative to Help Communities Tackle Local Challenges and Improve City Services; Office of the Press Secretary: Washington, USA, 2015.
- [6] President’s Council of Advisors on Science and Technology. Technology and the Future of Cities; President’s Council of Advisors on Science and Technology: Washington, DC, USA, 2016.
- [7] Lučić, D.; Boban, M.; Mileta, D. An Impact of General Data Protection Regulation on a Smart City Concept. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018.
- [8] Eckhoff, D.; Wagner, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. IEEE Commun. Surv. Tutor. 2018, 20, 489–516.
- [9] Anthopoulos, L.; Giannakidis, G. Task-Based Process Modeling for Policy Making in Smart Cities. In Proceedings of the ITU Kaleidoscope Academic Conference, Bangkok, Thailand, 14–16 November 2016.
- [10] Benjelloun, A.; Crainic, T.G.; Bigras, Y. Toward a Taxonomy of City Logistics Projects. Procedia Soc. Behav. Sci. 2010, 2, 6217–6228.
- [11] Perboli, G.; De Marco, A.; Perfetti, F.; Marone, M. A New Taxonomy of Smart City Projects. Transp. Res. Procedia 2014, 3, 470–478.
- [12] European Commission, EU Smart Cities Information System (SCIS). The Making of a Smart City: Policy Recommendation. Available online: www.smartcities-infosystem.eu (accessed on 12 December 2018).
- [13] “Establishing Smart City Technical Standards and Guidance: A Way Forward”, Stephen Cohen, William Money, International World Wide Web Conference Committee (IW3C2), 2017
- [14] “Smart cities. Ranking of European medium-sized cities, Final Report”, Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E., Centre of Regional Science, Vienna UT, 2007
- [15] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, „Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions“, Future Generation Computer Systems, 2013.

- [16] J. Belissent, „Getting Clever About Smart Cities: New Opportunities Require New BusinessModels“, Forrester Research, 2010.
- [17] CERP-IoT, „Vision and Challenges for Realising the Internet of Things“, Ožujak 2010
- [18] Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac, „A Survey on Sensor-based Threats toInternet-of-Things (IoT) Devices and Applications“, 2017.
- [19] International Telecommunication Union, Telecommunication sector (ITU-T), „Overview of the Internet of things“, lipanj. 2012.
- [20] Joachim W. Walewski and Authors, „Inital Architectural Reference Model for IoT“, lipanj 2011.
- [21] Francois Carrez and Authors, „Final architectural reference model for the IoT v 3.0“, srpanj 2013.
- [22] Making Sense of Interoperability: Protocols and Standardization Initiatives in IoT“, (2013) Sutaria. R. and Govindachari, R. The 2nd ComNeT-IoT workshop in the 14th International Conference on Distributed Computing and Networking (ICDCN 2013), TIFR, Mumbai.
- [23] Toby Jaffey, „MQTT and COAP, IoT Protocols“, Eclipse Newsletter, veljača 2014.
- [24] Paul Duffy, „Beyond MQTT: A Cisco view on IoT Protocols“, Cisco Blog, travanj 2013.
- [25] XMPP Standards Foundation, <http://xmpp.org/about-xmpp/technology-overview/>
- [26] Stan Schneider, „Understanding The Protocols Behind The Internet Of Things“, Electronic Design, listopad 2013.
- [27] IBM, IBM Smarter Cities: Creating Opportunities through Leadership and Innovation, Whitepaper, IBM Corporation, 2014. Retrieved 11/20/14, http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/index.html
- [28] International Telecommunications Union, listopad 2015, <https://www.itu.int/en/ITU-T/ssc/Pages/info-ssc.aspx>
- [29] US Department of Transportation, <https://www.transportation.gov/smartercity>
- [30] International Organization for Standardization (ISO), „Smart Cities, Preliminary Report 2014“, 2014
- [31] „Forecast: The Internet of Things, Worldwide, 2013.“, Gartner, 2013.
- [32] D.Evans, “ The Internet of Things How the Next Evolution of the Internet Is Changing Everything”, White Paper, Cisco, travanj 2011.
- [33] Miguel Blockstrand, Tomas Holm, Lars-Örjan Kling, Robert Skog and Berndt Wallin, „Operator opportunities in the internet of things“, Ericsson review, 2011
- [34] Rooney, B. “Internet of Things Poses Big Questions.” Wall Street Journal Online, July 3, 2013.
- [35] International Data Corporation (IDC) Press Release. “The Internet of Things Is Poised to Change Everything, Says IDC.” October, 2013.
- [36] Grand View Research, „Smart City Report“, <https://www.grandviewresearch.com/press-release/global-smart-cities-market>, veljača 2018.
- [37] Forbes, „Smart Citites – A 1.5\$ Trillion Market Opportunity“, <https://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/#5b24c57d6053>, lipanj 2014.
- [38] European Innovation Partnership on Smart Cities and Communities EIP-SCC, „The Marketplace of the European Innovation Partenrship on Smart Cities and Communities

- (EIP-SCC)“, <https://eu-smartcities.eu/sites/default/files/2018-04/EIPSCC-Brochure.pdf>, travanj 2014.
- [39] “Internet of Things – From Research and Innovation to Market Deployment”, Ovidiu Vermesan, Peter Friess, River Publisher, 2014.
- [40] Weber, M., Lučić, D. Lovrek, I., “Internet of Things Context of the Smart City”, 2017 International Conference on Smart Systems and Technologies (SST), 2017.
- [41] Vermesan, O.; Friess, P. Internet of Things—From Research and Innovation to Market Deployment; River Publisher: Gistrup, Denmark, 2014.
- [42] van der Veer, H.; Wiles, A. ETSI White paper No. 3 Achieving Technical Interoperability—The ETSI Approach; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2018.
- [43] Brutti, A.; de sabbata, P.; Frascella, A.; Gessa, N.; Ianniello, R.; Novelli, C.; Pizzuti, S.; Ponti, G. Smart City Platform Specification: A Modular Approach to Achieve Interoperability in Smart Cities: Technology, Communications and Computing. In The Internet of Things for Smart Urban Ecosystems; Springer: Cham, Switzerland, 2019; doi:10.1007/978-3-319-96550-5_2.
- [44] H2020 Project symbIoTe Web Site. Available online: <https://www.symbiote-h2020.eu/> (zadnje pristupan 10.12.2018).
- [45] Podnar Zarko, I.; Soursos, S.; Gojmerac, I.; Ostermann, E.G.; Insolubile, G.; Plociennik, M.; Reichl, P.; Bianchi, G. Towards an IoT framework for semantic and organizational interoperability. In Proceedings of the 2017 Global Internet of Things Summit (GloTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6.
- [46] G. Santucci, “1.1 The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects”, Vision and Challenges for Realising the Internet of Things, March 2010.
- [47] European Commission. “Communication on future networks and the internet.” Brisel, Rujan, 2008.
- [48] European Commission, „Internet of Things: A 14-point Action Plan“, Brisel, lipanj 2009.
- [49] T. Wachtel, “10th Meeting of the Internet of Things Expert Group Meeting Minutes” Brisel, studeni 2012.
- [50] RAND Europe, “Europe’s policy options for a dynamic and trustworthy development of the Internet of Things.”, SMART 2012/0053, kolovoz 2013
- [51] National Institute for Standards and Technology (NIST), “NIST Releases Final Smart Grid 'Framework 2.0' Document”, veljača 2012.
- [52] Department of Homeland Security, <http://www.dhs.gov/st-snapshot-detect-protect>, rujan 2013
- [53] IN-Q-TEL Press Release, “IN-Q-TEL ANNOUNCES STRATEGIC INVESTMENTS IN WIRELESS SENSOR NETWORKING”, listopad 2005.
- [54] Federal Trade Commission, “Public Comments: # 484; FTC Seeks Input on Privacy and Security Implications of the Internet of Things; FTC Project No. P135405; Commission Staff to Conduct Workshop on November 21, 2013 in Washington, DC“, srpanj 2013
- [55] Federal Trade Commission, Internet of Things Workshop, Washington DC, <http://ftc.gov/bcp/workshops/internet-of-things/>, studeni, 2013
- [56] http://europa.eu/rapid/press-release_IP-13-534_en.htm, zadnje pristupano: 25.01.2019
- [57] <https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018>, zadnje pristupano: 25.01.2019

- [58] Direktiva o energetskej učinkovitosti u krajnjoj potrošnji I energetskeim uslugama te o stavljanju izvan snage Direktive Vijeća 93/76/EEZ, travanj 2006, <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32006L0032&from=EN>
- [59] Direktiva o energetskej učinkovitosti, izmjeni directive 2009/125/EZ I 2010/30/EU I stavljanju izvan snage direktiva 2004/8/EZ I 2006/32/EZ, listopad 2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1399375464230&uri=CELEX:32012L0027>.
- [60] <https://ec.europa.eu/energy/en/topics/market-and-consumers/smart-grids-and-meters>, zadnje pristupano: 25.01.2019.
- [61] Uredba o roamingu u javnim pokretnim telefonskim mrežama u Zajednici i izmjeni Direktive 2002/21/EZ, lipanj 2007, <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32007R0717&from=EN>
- [62] European Commission. REGULATION (EU) No 531/2012 on Roaming on Public Mobile Communications Networks within the Union; European Commission: Brussels, Belgium, 2015.
- [63] European Comission. Digital Single Market Strategy. May 2015. Dostupno online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN> (pristupano 10.12.2018).
- [64] A Digital Agenda for Europe. European Commission, 2010. Dostupno online: [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R\(01\)](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01)) (pristupano 12.12.2018).
- [65] Uredba o utvrđivanju mjera u vezi s pristupom otvorenom internetu te o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama i Uredbe (EU) br. 531/2012 o roamingu u javnim pokretnim komunikacijskim mrežama u Uniji, studeni 2015, <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32015R2120&from=EN>
- [66] Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation); REGULATION (EU) 2016/679; Official Journal of the European; 2016; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
- [67] Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA; DIRECTIVE (EU) 2016/680; Official Journal of the European; 2016; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG
- [68] Direktiva o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), srpnja 2002, <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32002L0058&from=EN>
- [69] S. Soursos, I. Podnar Zarko, P. Zwickl, I. Gojmerac, G. Bianchi and G. Carrozzo, "Towards the Cross-Domain Interoperability of IoT Platforms", in the Proceedings of the European Conference on Networks and Communications (EUCNC) 2016, 27-30 June, Athens, Greece.
- [70] H2020 project symbIoTe web site: <https://www.symbiote-h2020.eu/> (accessed on 10.12.2018)
- [71] IoT-EPI whitepaper, Advancing IoT Platforms Interoperability, 2018.

- [72] Hafiz Husnain Raza Sherazi, Luigi Alfredo Grieco, and Gennaro Boggia, "A Comprehensive Review on Energy Harvesting MAC protocols in WSNs: Challenges and Tradeoffs," *Ad Hoc Networks*, vol. 71, pp. 117 - 134, 2018. doi: 10.1016/j.adhoc.2018.01.004.
- [73] „REGULATION (EU) 2016/2286 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment“, European Commission, December 2016.
- [74] Confidentiality, integrity, and availability (CIA triad), <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>, zadnje pristupano: 25.01.2019
- [75] European Commission, EU Smart Cities Information System (SCIS). The Making of a Smart City: Policy Recommendation. Available online: www.smartcities-infosystem.eu (accessed on 12 December 2018).
- [76] Donald C. Shoup, "Cruising for parking", *Transport Policy* 13 (2006) 479–486, July 2006
- [77] A. Antić, V. Bilas, M. Marjanović, M. Matijašević, D. Oletić, M. Pavelić, I. Podnar Žarko, K. Pripužić and L. Skorin-Kapov, „Urban Crowd Sensing Demonstrator: Sense the Zagreb Air“, *Proceedings of the 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 2014
- [78] M. Marjanović, L. Skorin-Kapov, K. Pripužić, A. Antić and I. Podnar Žarko, „Energy-Aware and Quality-Driven Sensor Management for Green Mobile Crowd Sensing“, *Journal of network and computer applications*, 59 (2016), pp. 95-108.
- [79] „Enabling the Internet of Things“, Report, BEREC – Body of European Regulators for Electronic Communications, BoR (16) 39, 12 February 2016.
- [80] European Commission, "Lighting the Cities: Accelerating the Deployment of Innovative Lighting in European Cities", June 2013.
- [81] "Business Model Canvas: A Simple Tool For Designing Innovative Business Models", siječanj 2012, Forbes, <https://www.forbes.com/sites/tedgreenwald/2012/01/31/business-model-canvas-a-simple-tool-for-designing-innovative-business-models/#3cc7990416a7>, zadnje pristupano: 25.01.2019

POPIS SLIKA

Slika 1: Postotak urbanizacije 1970. godine [4]	4
Slika 2: Postotak urbanizacije 1990. godine [4]	4
Slika 3: postotak urbanizacije 2018. godine [4]	5
Slika 4: Postotak urbanizacije 2030. godine [4]	5
Slika 5: Urbanizacija RH u odnosu na Europu.....	6
Slika 6: Prikaz podjele pametnih gradova u 6 područja interesa	11
Slika 7: Pojednostavljeni prikaz arhitekture IoT-a	13
Slika 8: Referentni model arhitekture Interneta stvari IoT-A	15
Slika 9: IoT referentni model Y.2060.....	17
Slika 10: Usporedni prikaz tradicionalnih i IoT protokola [22]	21
Slika 11: Funkcijska arhitektura oneM2M-a.....	22
Slika 12: Pojednostavljena arhitektura pametnih gradova	26
Slika 13: Broj povezanih uređaja na Internet do 2020. godine	29
Slika 14: broj instaliranih povezanih uređaja	29
Slika 15: Tržišni potencijal prema Statistici.....	30
Slika 16: Udjel pojedinih segmenata IoT-a na tržištu	31
Slika 17: Potencijal tržišta prema područjima ²	32
Slika 18: lanac vrijednosti IoT modela.....	35
Slika 19: Aktivacija eCall sustava prilikom nesreće [57]	44
Slika 20: Različiti standardi na svim razinama [71].....	60
Slika 21: Prikaz atributa pouzdanosti i poveznica sa sigurnošću	65
Slika 22: Osnovna načela informacijske sigurnosti.....	66
Slika 23: Prijetnje načelima informacijske sigurnosti	67
Slika 24: Predložena taksonomija IoT usluga	72
Slika 25: primjer aplikacije na kojoj su prikazane rute dvije biciklističke rute, najkraća i alternativna „zelena“ ruta s boljom kvalitetom zraka	76
Slika 26a: Odnosi pružatelja uređaja i povezivosti infrastrukture	Slika 26b: Pružatelj
Slika 27: Mogući odnosi pružatelja infrastrukture	85
Slika 28: Mogući odnosi pružatelja IoT platforme.....	86
	87

Slika 29: Mogući odnosi integratora IoT usluge	88
Slika 30: Mogući odnosi IoT korisnika	89
Slika 31: Mogući odnos krajnjeg korisnika.....	90
Slika 32: Primjer platna poslovnog modela.....	94
Slika 33: Platno poslovnog modela za proizvođača uređaja	97
Slika 34: Platno poslovnog modela za pružatelja usluge platforme	98
Slika 35: Platno poslovnog modela za integratora IoT usluge	99
Slika 36: Platno poslovnog modela za razvijatelja aplikacija i usluga	100
Slika 37: Platno poslovnog modela za IoT korisnika	101
Slika 38: Algoritam za definiranje usluge pametnog grada	103
Slika 39: Model IoT platforme za usluge pametnih gradova	106

ŽIVOTOPIS

Mario Weber rođen je u Zagrebu 1980. godine gdje je završio osnovnu i srednju školu. Godine 1998. upisao je Fakultet elektrotehnike i računarstva koji je završio 2004. godine s temom Personalizirani virtualni likovi u mobilnoj mreži gdje je radio napredne algoritme za prepoznavanje karakterističnih točaka lica na pametnim telefonima te transformaciju 2D slike u 3D model virtualnog lika.

2004. godine upisuje magistarski studij na Fakultetu elektrotehnike i računarstva u Zagrebu kojeg završava 2008. godine s temom Sustavi naplate za uslugu telefonije u paketski komutiranim mrežama. Rad je bio vezan uz projekt kompleksnog rješenja sustava naplate u realnom vremenu unutar multimedijalnog podsustava temeljenog na IP-u (*engl. IP Multimedia Subsystem - IMS*) u mrežama nove generacije (*engl. Next Generation Network - NGN*).

2011. godine upisao je doktorski studij na Fakultetu elektrotehnike i računarstva u području Interneta stvari s posebnim osvrtom na regulaciju tržišta Interneta stvari u segmentu pametnih gradova.

Tijekom diplomskog studija dobio je Rektorovu nagradu Sveučilišta u Zagrebu za studentski rad „Osobni virtualni likovi u pokretnoj mreži“.

Kao mladi razvojni inženjer započeo je raditi 2004. godine, ali ubrzo preuzima ulogu voditelja projekta na vrlo izazovnom i zahtjevnom projektu naplate u realnom vremenu u mrežama pokretnih komunikacija u Pakistanu i Bahreinu.

Od 2009. godine radi u Hrvatskoj regulatornoj agenciji za mrežne djelatnosti (HAKOM) kao stručnjak za komunikacijske mreže. 2011. godine postavljen je na mjesto rukovoditelja odjela komunikacijskih usluga, a u lipnju 2013. godine imenovan je ravnateljem HAKOM-a gdje je vodio poslovanje agencije te je bio odgovoran za upravljanje stručnom službom. Dužnost ravnatelja HAKOM-a obnašao je do lipnja 2018.

Od listopada 2018. godine direktor je poduzeća Lamaro digital d.o.o.

Za vrijeme svojeg školovanja i radnog vijeka kao koautor sudjelovao je u pisanju knjige „IP Multimedia Subsystem (IMS) Handbok“ u izdanju Taylor&Francis grupacije. Autor je brojnih znanstvenih članaka i sudionik brojnih okruglih stolova te je gostujući predavač na Diplomskom sveučilišnom studiju forenzike u Splitu na modulu Forenzika i nacionalna sigurnost. Bio je predstavnik Republike Hrvatske u Future Internet Forumu (FIF) pri Europskoj komisiji te član Nacionalnog vijeća za kibernetičku sigurnost imenovan od vlade RH.

Radovi objavljeni u časopisima i na međunarodnim konferencijama:

- Weber, Mario, Podnar Žarko, Ivana, „A Regulatory view on Smart City Services“, Sensors 2019
- Mario Weber, Marija Boban, “Security challenges of the Internet of Things”, Mipro 2016, str. 638-643
- V. Švedek, G. Jurin, M. Weber, “Increasing availability of broadband access over copper network infrastructure”, Mipro 2011, str. 407- 412
- M. Weber, Z. Žunko, S. Herceg, “Methodology for telecommunication service component distribution”, MIPRO 2005
- M. Boban, M. Weber, “Internet of things, legal and regulatory framework in digital transformation from smart to intelligent cities”, Mipro 2018
- M. Weber, R. Vulas, V. Švedek, “Regulatory Challenges of the Internet of Things”, Contel 2015, Workshop on Regulatory Challenges in the Electronic Communications Market
- M. Weber, V. Švedek, Z. Jukić, I. Golub, T. Žuljević, “Can HAKOMetar be Used to Increase Transparency in the Context of Network Neutrality?”, Contel 2013
- Z. Jukić, M. Weber, V. Švedek, M. Vuković, D. Katušić, G. Ježić, “Technical aspects of network neutrality”, Contel 2011, str. 405- 410
- S. Herceg, M. Weber, T. Macan, “Challenges in Implementing a SIP-Based Application Server”, Contel 2007, str. 333 - 338
- M. Weber, I. Andrišek, I. Pandžić, “Mobile entertainment using personal avatars”, Contel 2005, str. 341 - 346
- D. Katušić, M. Weber, I. Bojić, G. Ježić, M. Kušek, “Market, Standardization and Regulatory Development in Machine-to- Machine Communications”, Softcom 2012, str. 1-7
- Z. Jukić, A. Budimir, M. Weber, “Current Approach to Preserving the Open and Neutral Character of the Internet in Croatia”, Softcom 2012,
- M. Ljubić Karanović, G. Kulišić, M. Weber, “Measures for preventive Consumer protection in electronic communications”, Softcom 2012
- Z. Jukić, M. Weber, M. Matijašević, “Findings of the Public Consultation on Network Neutrality in Croatia: Report and Analysis”, Softcom 2011, str. 43-51

- M. Weber, G. Ježić, M. Krvišek, “Overview of Looking to the Future Project”, Softcom 2011, str. 1-8
- V. Švedek, M. Weber, „Analysis of the Next Generation Network Regulatory Framework“, Softcom 2010
- M. Vuković, D. Katušić, R. Šoić, M. Weber, “Rule-Based System for Data Leak Threat Estimation”, Softcom 2017
- D. Lučić, M. Weber, I. Lovrek, “Electronic Communications as Smart City Enablers”, SST 2016, str. 241-247
- M. Weber, D. Lučić, I. Lovrek, “Internet of Things Context of the Smart City”, SST 2017, str 187-193 Journal of Mobile Information Systems
- T. Košutić, M. Mošmondor, I. Andrišek, M. Weber, M. Matijašević, I. Pandžić, “Personalized avatars for mobile entertainment”, Hindawi 2006, str. 95 - 110

BIOGRAPHICAL NOTE

Mario Weber was born in Zagreb in 1980 where he finished elementary and high school. In 1998 he started his academic education on the Faculty of Electrical Engineering and Computing, which finished in 2004 with the thesis of Personalized Virtual Characters in the Mobile Network, where he worked on advanced algorithms for recognizing facial characteristic points on smartphones and transforming 2D images into a 3D virtual character model.

In 2004 he enrolled in a Master's degree at the Faculty of Electrical Engineering and Computing in Zagreb, which ends in 2008 with the master thesis "Billing systems for the telephony service in packet switched networks". This work is related to a complex solution of the real time billing system within a IP multimedia subsystem (IMS) in Next Generation Network (NGN) networks.

In 2011 he started his Phd study at the Faculty of Electrical Engineering and Computing in the field of Internet of Things with a special focus on regulation of the IoT market in the segment of Smart Cities.

During his graduation he received Rector's Award from the University of Zagreb for the student work "Personal virtual characters in the mobile network".

As a young development engineer he started working in 2004 but soon takes the role of the project leader on a very challenging and demanding project of real-time billing in the mobile communications networks in Pakistan and Bahrain.

Since 2009, he has been working in the Croatian Networking Regulatory Agency (HAKOM) as a communications network specialist. In 2011, he was appointed as the Head of Communications Services Department, to be appointed as Director of HAKOM in June 2013, which he held until June 2018. As the director of HAKOM he was leading the agency and was responsible for the management of the expert service and for the financial results.

Since October 2018 he is director of Lamaro digital ltd.

He participated as a co-author in writing the book "IP Multimedia Subsystem (IMS) Handbok" published by the Taylor & Francis group during his education and working life. He is the author of numerous scientific articles and a participant of numerous round tables. He is a visiting lecturer at the graduate university study of forensics in Split on the Forensic and National Security Module. He was a representative of the Republic of Croatia at the Future

Internet Forum (FIF) at the European Commission and a member of the National Cyber Security Council appointed by the Government of the Republic of Croatia.