IoT i pametna kuća

Obadić, Sven

Undergraduate thesis / Završni rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:704524

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-23**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

IoT I PAMETNA KUĆA

Završni rad

Sven Obadić

Osijek, 2017.

Sadržaj

1. UVOD 1
1.1. Zadatak završnog rada 1
2. POJAM IOT – INTERNET OF THINGS 2
2.1. Primjena IoT-a 3
3. PODATKOVNI PROTOKOLI I KOMUNIKACIJSKA TEHNOLOGIJA 5
3.1. Protokoli za prijenos podataka 5
3.1.1. Protokol za komunikaciju između uređaja (DDS) 6
3.1.2. Protokol za prikupljanje podataka od uređaja (MQTT) 7
3.1.3. Protokol za komunikaciju između uređaja i korisnika (XMPP) 9
3.1.4 Protokol za međusobno povezivanje poslužitelja (AMQP) 10
3.2. Komunikacijska tehnologija 11
3.2.1. Radio frekvencijska identifikacija *(RFID)* 11
3.2.2. Bluetooth 13
3.2.3. WIFI 14
3.2.4. ZigBee 14
3.2.5. Ostale značajne komunikacijske tehnologije 16
4. PREDNOSTI I NEDOSTACI IoT-A 18
5. PROJEKT PAMETNE KUĆE – NADGLEDANJE U STVARNOM VREMENU 19
6. ZAKLJUČAK 24
LITERATURA 25
POPIS OZNAKA I KRATICA 26
SAŽETAK 28
ABSTRACT 28
ŽIVOTOPIS 29

1. UVOD

U današnje vrijeme svijet bez interneta je teško zamisliv. Broj uređaja odnosno korisnika spojenih na internet je prešao 20 bilijuna. Do 2020. godine predviđa se kako će taj broj porasti do 50 bilijuna. Upravo zbog toga dosadašnji IPv4 protokol je i zamijenjen novim IPv6 protokolom koji podržava ekstremno mnogo više jedinstvenih IP adresa.

Do prije nekoliko godina bilo je nezamislivo upravljati kućanskim uređajima dok niste kod kuće. Danas postaje normalno primjerice upravljati sustavom grijanja na daljinu, preko mobilnog telefona ili nekog drugog pametnog uređaja.

IoT predstavlja mrežu fizičkih uređaja, vozila, zgrada ili bilo kojih drugih stvari opremljenih sa potrebnom elektronikom, softverom, senzorima i mrežnom povezanošću koja im omogućava međusobnu razmijenu podataka.

U prvome poglavlju ovoga završnog rada govoriti će se o *Internet of things* tehnologiji te kako je nastala. Nakon toga objasniti će se protokoli za razmjenu podataka između senzora i uređaja. Objasniti će se najčešće korištene komunikacijske tehnologije i njihovi nedostaci te koliko je sve to zapravo sigurno za implementaciju. U praktičnom dijelu rada prikazati će se dio osobnog projekta pametne kuće koji trenutno sadržava sustav video nadzora prednje i stražnje strane obiteljske kuće.

1.1. Zadatak završnog rada

Zadatak završnog rada je teoretski obraditi IoT (*Internet of things*) i dati prijedlog za implementaciju tih načela u „pametnoj kući“ sa trenutno dostupnim tehnologijama u Hrvatskoj. U prvom dijelu rada opisani su protokoli, komunikacijska tehnologija i sigurnost sustava. Nakon toga proći će se trenutno dostupne tehnologije i mogućnost njihove implementacije. Na kraju će se prikazati početak osobnog projekta pametne kuće.

2. POJAM IoT – INTERNET OF THINGS

„*Internet of things* – IoT“, pojavio se 1999. godine od strane Kevina Ashtona koji je bio suosnivač Auto-ID centra na institutu za tehnologiju u Massachusetts-u. Tvrtka Gartner koja se bavi istraživanjem novih tehnologija na globalnoj razini objavila je da je IoT jedna od top deset najvažnijih strategijskih tehnologija na svijetu. Istovremeno, tvrtka Cisco je predvidjela preko 50 bilijuna uređaja na internetu do 2020. godine uz enorman porast narednih godina. IoT se temelji na komunikaciji putem mreže ili nekih drugih oblika prijenosa kao što je Bluetooth ili primjerice RFID (Radio-frequency identification) koji radi na principu radijske frekvencije. Danas IoT ima jako puno primjena i primjenjuje se u širokom spektru djelatnosti, a sve u cilju što većeg olakšanja raznoraznih poslova te što veće uštede i iskoristivosti. Pojam Internet of thingsa je veoma teško definirati jer obuhvaća sve uređaje koji se ističu po svojim karakteristikama u domeni povezivanja sa ostalim uređajima u neku cjelinu ili sustav kako bi se omogućila što veća interakcija sa korisnikom.

Sustav može biti veoma jednostavan, ali s druge strane može biti i veoma kompleksan. Sve ovisi o tome koji su korišteni protokoli i što sve čini jedan takav pametan sustav. Najčešće ćemo vidjeti primjenu u pametnim kućama, međutim sve više velikih tvrtki odlučuje se što više automatizirati i olakšati si poslovanje pretvarajući tvornice u tzv. pametne tvornice. Još uvijek su pametni uređaji dosta skupi, ali kroz par godina uz još veći napredak tehnologije cijena će pasti u toj mjeri da će si pametne uređaje moći priuštiti gotovo svako kućanstvo.

Cijeli sustav se zasniva na odnosu senzor-mikroupravljač-softver-korisnik. Primjerice, želimo upravljati sa rasvjetnim tijelom u kući. Na instalaciju prije rasvjetnog tijela priključuje se mikrokontroler preko kojega korisnik šalje komandu. Kontroler može biti Wireless, Bluetooth, žično spojen na mrežu ili pak komunikacija može biti ostvarena na neki drugi način. Ovisno o vrsti komunikacije, korisnik uspostavlja komunikaciju putem sučelja odnosno upravljačkog programa na računalu ili pametnom telefonu. Ako je komunikacija ostvarena preko kućne lokalne mreže koja ima izlaz na internet, onda korisnik može upravljati sustavom od bilo kuda gdje ima izlaz na internet. Ako je pak komunikacija ostvarena preko Bluetootha ili neke slične tehnologije, onda je uvijek potrebno biti u neposrednoj blizini kako bi se uspostavila veza sa kontrolerom.

U ovisnosti o željama i potrebama koristi se ona tehnologija koja će najbolje odgovarati traženim zahtijevima.

2.1. Primjena IoT-a

IoT je našao svoju primjenu u gotovo svim sferama modernog života. Koristi se u industriji, medicini, logistici, privatnim kućama itd. Postoji puno primjera implementacije, ali ovo su neki od najčešćih.

U industriji se koristi u obliku RFID (Radio-frequency identification) identifikacijskih oznaka bilo za praćenje samih proizvoda ili za praćenje zaposlenika. Pod praćenje zaposlenika podrazumijeva se dolazak i odlazak sa radnog mjesta. Na taj način mnogo je lakše voditi evidenciju o proizvodima kao i samim ulascima i izlascima radnika. Slijedeća primjena je u samoj proizvodnji upotrebom senzora, bar kod čitaća i na kraju kompleksnih robota koji su daleko efikasniji nego ljudi. Nastaje problem što se što većim stupnjem modernizacije drastično smanjuje potreba za lošije obrazovanim zaposlenicima odnosno tzv. „malim radnicima“. Povećava se potreba za inženjerima i visokoobrazovanim radnicima iz tehničkih područja.

U logistici se IoT koristi za praćenje i identifikaciju tereta. Što za određivanje pozicije vozila za prijevoz pa do praćenja pozicije i identifikaciju samog tereta. Ovakav način distribucije uvelike olakšava usklađenost i organizaciju između dobavljača i kupca. Cijeli logistički lanac postaje puno efikasniji. Najveća prednost je što se razvojem tehnologije sve može pratiti u realnom vremenu pomoću GPS sustava.

IoT je najrašireniji kod privatnih potrošaća koji čine najveći udio u ukupnom broju uređaja koji su trenutno na mreži. Pojam „smart home“ odnosno pametna kuća godinama se sve češće i češće spominje. Moguće je gotovo svaki uređaj povezati na mrežu i upravljati njime pomoću jedinstvenog sučelja. Upotrebom brojnih senzora, elektromotora, mikrokontrolera i mnoge druge elektronike moguće je upravljati gotovo svakim uređajem. U pametnoj kući IoT je najčešće implementiran u obliku video nadzora, senzora pokreta i otvaranja prozora/vrata te upravljanjem sustavom centralnog grijanja i rasvjete. Prilikom svake detekcije pokreta kada je sustav uključen, ovisno o odabranom načinu komunikacije, obavještava se korisnik sustava. Najveća prednost je što korisnik osim što može iz udobnosti vlastitog doma upravljati uređajima i sustavima, ako je sustav dovoljno dobro tehnički izvedem može to raditi i izvan doma. Primjerice poveća sobnu temperaturu prije nego što dođe s posla ili pak upali svijetlo ako je vani mračno.

IoT se sve više počeo koristiti i u medicini. Najveći dio primjene odnosi se na pacijente. Doktori mogu pratiti pacijenta na daljinu putem pametnih uređaja koji mjere broj otkucaja srca ili krvni tlak. Ostatak implementacije vezan je uz bolnicu kao ustanovu. Unutar bolnice se upotrebom uređaja koji su međusobno povezani olakšava rad doktorima i uspostavlja se veća

efikasnost između različitih odjela. Samim time smanjuje se red čekanja pacijenta. Znanstvenici su otišli korak dalje te je osmišljen prvi pametni pejsmejker. Ali upitna je njegova realna primijena prvenstveno zbog mogućnosti upada hakera, a to može završiti sa smrtnim ishodom kod pacijenta.

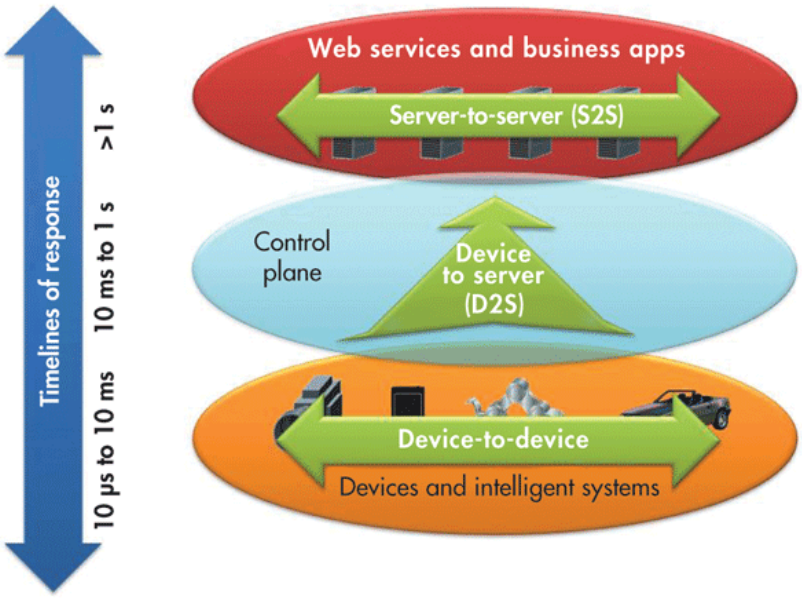
IoT se u prodaji koristi na način da se pomoću tableta ili nekih drugih uređaja korisnicima omogući pregled trenutne ponude u realnom vremenu. Time se postiže veća interakcija između trgovine i kupca te kupac ima bolji uvid u ponudu i trenutne akcije. Jedan od najvećih trgovačkih lanaca u SAD-u Walmart već neko vrijeme ima na košarama za kupnju ugrađen pametni uređaj sa bar kod čitačem koji omogućava kupcu skeniranje proizvoda te se na ekranu prikazuje ukupna cijena proizvoda u košari. Istovremeno je omogućen i prikaz trenutnih cijena i akcija.

3. PODATKOVNI PROTOKOLI I KOMUNIKACIJSKA TEHNOLOGIJA

Najvažniji dio jednog IoT sustava su podatkovni protokoli za razmjenu podataka između uređaja odnosno poslužitelja sa tim uređajima. Povezivanjem uređaja koji koriste podatkovne protokole sa nekom od dostupnih komunikacijskih tehnika možemo učiniti da neki uređaj bude pametan uređaj.

3.1. Protokoli za prijenos podataka

Za komunikaciju između uređaja postoje razni podatkovni protokoli za prijenos podataka i informacija. Oni osiguravaju pravoremenu i točnu razmjenu podataka i informacija između povezanih uređaja. IoT trenutno podržava mnogo raznih protokola i zato je važno razumijeti koji protokol ima koju namjenu te kako pojedini protokol vrši adresiranje podataka. Prikaz vremena odaziva u različitim odnosima prikazan je na slici 3.1.



Slika 3.1. Primjer vremena odaziva kod adresiranja podataka

Uređaji moraju komunicirati jedni s drugima D2D (*Device to Device*). Nakon toga podaci sa uređaja moraju biti prikupljeni i poslani na poslužitelj D2S *(Device to Server*). Infrastruktura poslužitelja dijeli podatke prikupljenih od uređaja (S2S), eventualno ga pružajući nazad

uređajima, programima za analizu ili ljudima. Protokoli se mogu ugrubo podijeliti na njih nekoliko od kojih svaki kasnije ima i do nekoliko desetaka pod vrsta.

• MQTT *(eng. Message Queue Telemetry Transport*): protokol za prikupljanje podataka od uređaja i transfer tih podataka na poslužitelj (D2S)

• XMPP (eng. *Extensible Messaging and Presence Protocol*): protokol najprikladniji za komunikaciju uređaja i korisnika, poseban slučaj D2S načina zbog toga što su korisnici spojeni na poslužitelje.

• DDS (eng. *Data-Distribution Service)*: služi za brzu komunikaciju između uređaja (D2D)

• AMQP (eng. *Advanced Message Queuing Protocol)*: Sustav čekanja koji služi za međusobno povezivanje poslužitelja (S2S)

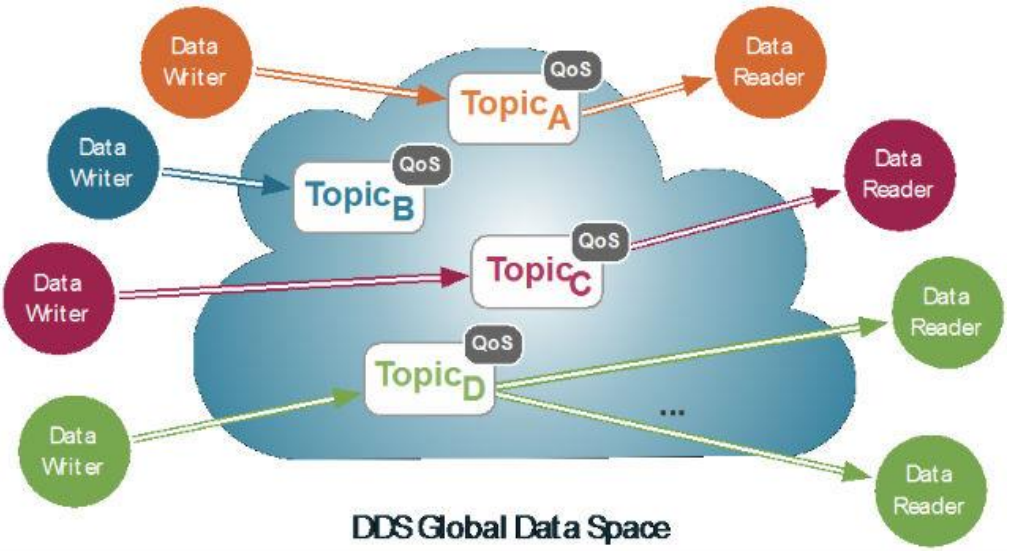
3.1.1. Protokol za komunikaciju između uređaja (DDS)

Koristi se u stvarnovremenskim sustavima za uređaj-uređaj komunikaciju te omogućava skalabilnost,stvarnovremenski pouzdan prijenos podataka sa velikim brzinama prijenosa. DDS se primjenjuje tamo gdje se koristi velika količina podataka. U prijenosnom sustavu postoji programski sloj koji glumi most između operacijskog sustava i aplikacije. Time se omogućava raznim komponentama sustava da lakše međusobno komuniciraju i razmijenjuju podatke. Takva usmjerenost podataka omogućava da sve poruke koje sadržavaju bitne podatkovne informacije budu shvaćene od strane aplikacije

U suštini DDS u svakom trenutku zna koje podatke treba pohraniti i kontrolirati, a koje dijeliti. Glavna namjena je spojiti jedan uređaj sa drugim i osigurati njihovu komunikaciju odnosno razmjenu podataka između njih. Može efikasno dostaviti milijune poruka u sekundi za mnogo istovremenih primatelja. Uređaji zahtijevaju podatke mnogo brže nego što to zahtijeva IT infrastruktura. Nešto što je stvarnovremenski se obično izražava u mikrosekundama. Uređaji imaju potrebu za komuniciranjem sa mnogo uređaja odjednom što može biti veoma složeno. Zbog toga je korištenje TCP protokola previše ograničavajuće. DDS nudi veliku kvalitetu distribucije podataka i pouzdanost. Također nudi veoma efikasno filtriranje i odabiranje točno određenih podataka koji trebaju biti preusmjereni na točno određeno mjesto, a to može biti i tisuće istovremenih odredišta. Za male uređaje postoje i drugačije verzije DDS-a, koje mogu efikasnije raditi u takvom okruženjima.

DDS ima veliku primijenu u vojnim sustavima, vjetroelektranama, bolnicama i automobilizmu.

DDS je odličan protokol za razmjenu podataka između uređaja gdje je važno da se podatak prenese u točno određenom odnosno zatraženom vremenu . Omogućava pravovremen dolazak podataka do točno određenog odredišta u točno definiranom vremenskom periodu. Podaci uvijek moraju biti dostupni u pravo vrijeme te se također razlikuju po prioritetu, vremenu i ostalim svojstvima kao što je to slučaj i kod RTP protokola.



Slika 3.2. Prikaz razmjene podataka između pošiljatelja i primatelja zasnovan na odnosu objava-pretplata

3.1.2. Protokol za prikupljanje podataka od uređaja (MQTT)

MQTT prikuplja podatke od uređaja. Kao što i sam naziv govori, glavna namjena je telemetrija odnosno nadgledanje na daljinu. Cilj je prikupiti podatke sa svih uređaja i prenijeti ih do IT infrastrukture. Protokol prvenstveno cilja na veliku mrežu malih uređaja koji trebaju biti nadgledani ili kontrolirani sa oblaka odnosno na daljinu.

Protokol veoma malo sudjeluje u prijenosu podataka sa uređaja na uređaj i najviše je fokusiran na prijenos podataka na više uređaja. Upravo zbog toga što ima jasnu samo jednu primjenu, MQTT je veoma jednostavan protokol koji nudi samo nekoliko mogućnosti kontrole. Ne zahtjeva brz prijenos podataka i zbog toga je stvarnovremenski prijenos najčešće izražen u sekundama. Za MQTT protokol je normalno da jedan integracijski poslužitelj ili čvorište,

obrađuje razmjenu informacija i transformaciju za veoma mnogo aplikacija ili podatka. Svi uređaji se spajaju na podatkovni poslužitelj. Koristi najviši sloj TCP protokola.

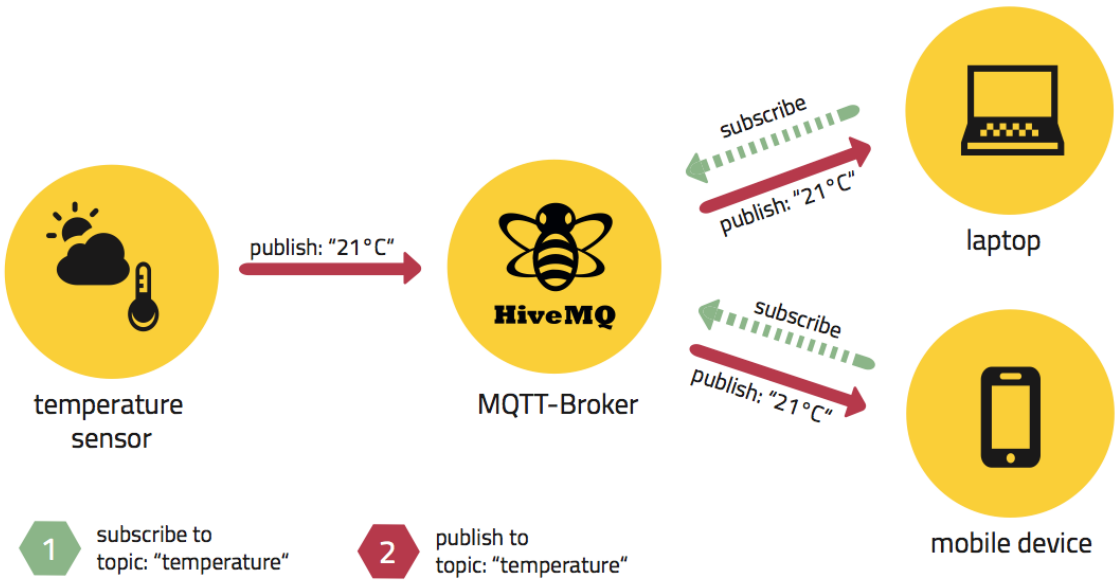
MQTT definira nekoliko glavnih metoda koje definiraju traženu akciju da bude izvedena od strane identifikacijskog resursa. Što taj resurs predstavlja, bilo da se radi o postojećim podacima ili podacima koji će se generirati dinamički ovisi o implementaciji na samom poslužitelju. Često resurs odgovara na datoteku ili izlaz iz izvorišnog prebivališta na poslužitelju.

Definirane metode zasnovane na odnosu „*publish-subscribe*“ :

- Spajanje – čeka da se ostvari konekcija sa poslužiteljem
- Odjava – čeka da MQTT klijent odradi posao koji ima za odraditi i TCP/IP sesiju za odjavu
- Pretplata – čeka se završetak postupka pretplate ili odjave sa pretplate
- Odjava pretplate – zahtjeva od poslužitelja odjavu klijenta sa jedne ili više pretplaćenih tema
- Objava - odmah se vraća tema aplikaciji nakon zahtjeva od strane MQTT klijenta

MQTT je dizajniran da podržava bežične mreže sa različitim razinama latencije zbog povremenih bandwidth ograničenja ili nepouzdanosti veze.

Na slici 3.3 dan je primjer jednog temperaturnog senzora sa kojeg se očitavaju podaci na mobilni uređaj i prijenosno računalo putem MQTT podatkovnog protokola.



Slika 3.3. Prikaz odnosa objava - pretplata na kojoj je zasnovan MQTT protokol

3.1.3. Protokol za komunikaciju između uređaja i korisnika (XMPP)

XMPP je komunikacijski protokol zasnovan na slanju i primanju poruka između različitih sustava na mreži i baziran je na XML jeziku. Omogućava blizu stvarnovremensku razmjenu strukturiranih podataka između dvije ili više osoba. Protokol je izvorno bio nazvan „Jabber“ što bi se moglo prevesti kao brbljati ili razgovarati, osmišljen od strane Jabber zajednice 1999. godine i služio je za razmjenu instant poruka u stvarnom vremenu. Protokol je također korišten za publish-subscribe sustave, razmjenu podataka, VoIP i IoT kod kojega je korišten u pametnim električnim mrežama .

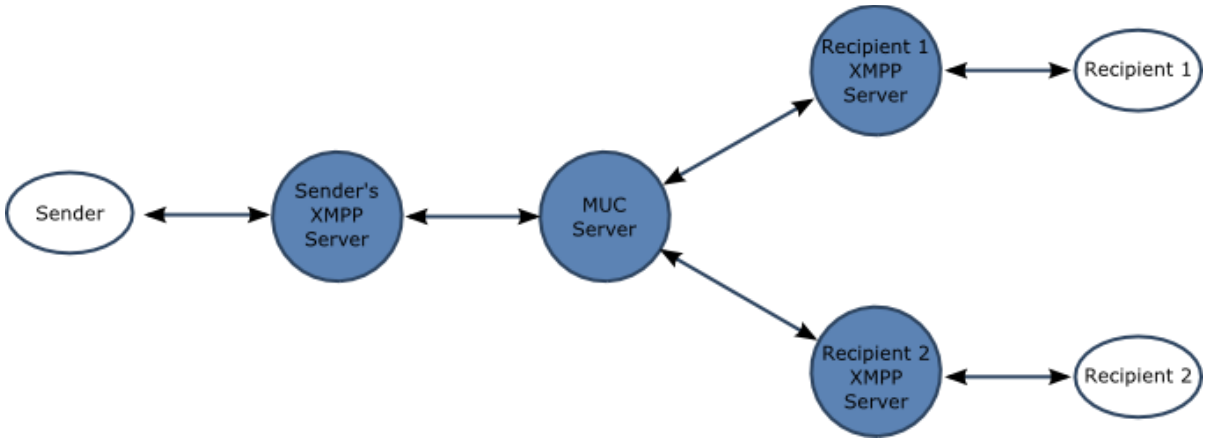
Kao i MQTT protokol, radi preko TCP protokola. Njegova ključna prednost je u tome što koristi naziv@domena.com shemu adresiranja koja uvelike pomaže spojiti male uređaje u ogromnoj mreži. U kontekstu IoT-a predstavlja najlakši i najjednostavniji način adresiranja uređaja. Osobito je pogodan kod prijenosa podataka sa većih udaljenosti i nepristupačnih točaka baš kao što je to slučaj u osoba-osoba komunikaciji. Brzine prijenosa poruka ostvaruju se u sekundama.

XMPP mreža koristi klijent-poslužitelj arhitekturu gdje klijenti nemoraju direktno odgovarati jedni drugima. XMPP je decentraliziran odnosno svatko može pokrenuti svoj vlastiti XMPP poslužitelj. Podržava sigurnu autorizaciju (SASL) i enkripciju (TLS) koji su ugrađeni u njegovu jezgru.

Nedostatak ovog protokola je to što nema efikasnu kontrolu nad prijenosom podataka.

XMPP je jedan od najčešće korištenih komunikacijskih protokola za razmjenu poruka. Otvorenog je koda za razliku od većine ostalih protokola za slanje instant poruka. Kod IoT-a je osobito pogodan za povezivanje potrošački orjentiranih sustava u pametnoj kući, primjerice sustava grijanja tako što bi se termostat dodao na poslužitelj na koji bi se pristupalo preko računala ili mobilnog telefona.

Na slici 3.4 opisan je jedan primjer slanja informacije. Informacija se najprije šalje na pošiljateljev XMPP poslužitelj, nakon toga zahtjev prima MUC(Multi user chat) poslužitelj koji vrši daljnju komunikaciju i razmijenu informacija sa primateljima.



Slika 3.4. Primjer razmjene poruka preko XMPP protokola

3.1.4 Protokol za međusobno povezivanje poslužitelja (AMQP)

AMQP je binarni protokol otvorenog standarda u aplikacijskom sloju dizajniran tako da podržava široku paletu aplikacija i komunikacijskih obrazaca Nudi kontorlirani protok komunikacijskih poruka te garantira isporuku najmanje jednom, najviše jednom ili točno jednom. Također osigurava potvrdu autentičnosti i/ili enkripicju baziranu na SASL ili TLS protokolima. Definirana AMQP obilježja su slanje i primanje, čekanje, usmjeravanje od točke do točke, pouzdanost i sigurnost.

AMQP se ponekad smatra i IoT protokolom. On šalje transakcijske poruke između poslužitelja. Možemo ga poistovjetiti sa bankarstvom jer može pouzdano procesuirati tisuće transakcija na čekanju. Protokol je fokusiran na točnu isporuku podataka. Koristi se TCP protokol koji pruža veoma pouzdanu point to point vezu. Krajnje točke moraju znati prihvatiti svaku poruku. AMQP koji se u početku koristio samo u bankarstvu fokusira se na praćenje

svih poruka i osiguravanje svake poruke isporučenom bez obzira na eventualne kvarove ili ponovno podizanje sustava. Uglavnom se koristi u poslovnom svijetu. U kontekstu IoT-a, AMQP je najprikladniji za upravljački mehanizam i analizu funkcija baziranih na poslužitelju.

	DDS	AMQP	MQTT	XMPP
TRANSPORT	UDP/IP (unicast + multicast) TCP/IP	TCP/IP	TCP/IP	TCP/IP
INTERACTION MODEL	Publish-and-Subscribe, Request-Reply	Point-to-Point Message Exchange	Publish-and-Subscribe	Point-to-Point Message Exchange
SCOPE	Device-to-Device Device-to-Cloud Cloud-to-Cloud	Device-to-Device Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud
AUTOMATIC DISCOVERY	✓	-	-	-
CONTENT AWARENESS	Content-based Routing Queries	-	-	-
QoS	Extensive (20+)	Limited	Limited	-
INTEROPERABILITY LEVEL	Semantic	Structural	Foundational	Structural
SECURITY	TLS, DTLS, DDS Security	TLS + SASL	TLS	TLS + SASL
DATA PRIORITIZATION	Transport Priorities	-	-	-
FAULT TOLERANCE	Decentralized	Implementation-Specific	Broker is SPoF	Server is SPoF

Tablica 3.1. Usporedba protokola za prijenos podataka

3.2. Komunikacijska tehnologija

3.2.1. Radio frekvencijska identifikacija *(RFID)*

RFID koristi elektromagnetska polja da identificira i prati oznake (*eng. tags*) pričvršćene na neki objekt. Svaka oznaka sadrži elektronički upisane podatke. Pasivne oznale prikupljaju energiju iz obližnjih RFID čitača pomoću radio valova. Aktivne oznake imaju svoj vlastiti izvor napajanja i mogu djelovati i više stotina metara udaljeni od RFID čitača.

Koriste se u mnogim industrijama, primjerice prilikom proizvodnje automobila gdje se u toku proizvodnje postavi tag na automobil i prati se daljnji tijek proizvodnje. Mogu se primjerice pratiti kutije sa dijelovima u velikim skladištima itd.

Velika prednost RFID oznaka je u tome što se mogu implementirati u bilo kakav fizički oblik. Postoje oznake u obliku privjeska za ključeve, oznake u obliku kartica, pa čak i implatantne oznake u obliku malih ampula koji su gotovo veličine zrna riže.

Band	Regulations	Range	Data speed
120–150 kHz (LF)	Unregulated	10 cm	Low
13.56 MHz (HF)	ISM band worldwide	10 cm–1 m	Low to moderate
433 MHz (UHF)	Short Range Devices	1–100 m	Moderate
865-868 MHz (Europe) 902-928 MHz (North America) UHF	ISM band	1–12 m	Moderate to high
2450-5800 MHz (microwave)	ISM band	1–2 m	High
3.1–10 GHz (microwave)	Ultra wide band	up to 200 m	High

Tablica 3.2. Frekvencije korištene u RFID oznakama

Također, oznake mogu biti samo za čitanje što znači da imaju tvornički zapisan serijski broj u sebi ili mogu biti za čitanje/pisanje odnosno pomoću posebnih uređaja se može promijeniti već zapisan identifikacijski broj. Oznake u sebi sadržavaju mali integrirani krug u koji je zapisana informacija odnosno serijski broj i antenu koja služi za primanje i odašiljanje signala.

RFID čitači odašilju signal istovremeno ispitujući signal sa taga. Oznaka dobiva poruku sa čitača i zatim reagira šaljući svoje informacije. Informacija može biti serijski broj ili može biti bilo koji drugi niz brojeva koji nešto označavaju. Kao i kod oznaka, postoji više vrsta čitača koji također mogu biti aktivni ili pasivni.

U primjeru pametne kuće RFID se najčešće implementira kao sustav ulaska u prostoriju bez potrebe za ključem. Oznaka se prisloni na čitač i sustav dobiva impuls da se vrata mogu otvoriti. Kod ove vrste komunikacije postoji problem što se RFID tagovi mogu kopirati što predstavlja velik i ozbiljan problem sigurnosti i narušavanja privatnosti. Ovaj problem se može riješiti takozvanim mjenjajućim kodovima koji se koriste u daljinskom zaključavanju automobila ili garaža.

3.2.2. Bluetooth

Bluetooth predstavlja bežičnu razmjenu podataka na male udaljenosti između dva ili više uređaja. Izumljen je od strane tvrtke Ericsson i bio je originalno zamišljen kao alternativa RS-232 kabelu. Koristi kratkovalne radio valove frekvencija od 2.4 do 2.485 Ghz.

Prilikom prijenosa podataka Bluetooth dijeli prenesene podatke u pakete i prenosi svaki paket na jedan od 79 određenih Bluetooth kanala. Svaki kanal ima propusnost od 1Mhz.

Bluetooth je komunikacijski protokol primarno dizajniran za malu potrošnju energije na kojoj radi, sa kratkim dometom i sa veoma niskom cijenom mikročipova korištenih u uređajima. Zbog toga što se za komunikaciju koristi radijska frekvencija, uređaji ne moraju biti vizualno dostupni jedni drugima kao što je to bio slučaj kod nekad popularnog IR prijenosa.

Postoji nekoliko verzija Bluetootha, svaka ima drugačiji maksimalni domet i brzinu prijenosa, ovisno o tome kako su napredovale verzije kroz godine. Verzije su opisane u tablici 3.2.

Bluetooth version	Maximum speed	Maximum range
3.0	25 Mbit/s	10 meters (33 ft)
4.0	25 Mbit/s	60 meters (200 ft)
5	50 Mbit/s	240 meters (800 ft)

Tablica 3.3. Usporedba Bluetooth verzija

Bluetooth verzija 4.2 koja je postala dostupna 2014. godine bila je uvod Bluetootha u IoT. Najbitnije poboljšanje je bio *Internet Protocol Support Profile* (IPSP) verzija 6 koja je bila spremna za Bluetooth pametne stvari u podršci za spajanje u pametnoj kući. Bluetooth verzija 5 koja je izašla 2016. godine ima značajke koje su uglavnom fokusirane na IoT tehnologiju. Pruža duplo veću brzinu prijenosa, četiri puta veći domet i 8 puta veći kapacitet prijenosa podataka nego što je to imala verzija 4.

Bluetooth je najčešće primjenjivan kod mobilnih uređaja, a u posljednje vrijeme sve se češće primjenjuje u slušalicama, zvučnicima, tipkovnicama i miševima. Pojavljuje se također u mikrokontrolerima za upravljanje rasvjetom,utičnicama i prekidačima.

3.2.3. WIFI

WIFI je tehnologija za mrežnu komunikaciju između uređaja bazirana na IEEE 802.11 standardu. WIFI je našao primjenu u gotovo svim modernim uređajima današnjice počevši od računala, mobitela, printera i mnogih drugih. WIFI kompatibilni uređaji spajaju se na internet putem WLAN-a i bežičnih pristupnih točaka. Unutar zatvorenog prostora domet pristupne točke je dvadesetak metara, a to sve zavisi od prepreka odnosno zidova. Što se tiče dometa u otvorenom, on može biti par stotina metara odnosno nekoliko kilometara. Sve ovisi o optičkoj vidljivosti, kvaliteti i vrsti antene te broju pristupnih točaka.

WIFI koristi frekvencije od 2.4 i 5GHz gdje se frekvencija od 2.4GHz najčešće koristi kod malih udaljenosti i spajanje mobitela na pristupnu točku. Frekvencija od 5Ghz se koristi za spajanje pristupnih točaka koje se nalaze na većim udaljenostima.

Jedna je od trenutno najkorištenijih tehnologija za mrežnu komunikaciju. Svaka wifi mreža ima svoj SSID odnosno jedinstveni naziv. Također kod postavljanja mreže može se odabrati najpogodniji kanal odnosno kanal na kojemu će kvaliteta veze biti najbolja. Dvije najbitnije stvari u WIFI mreži su adapter i usmjerivači (*eng. router*). Adapteri omogučavaju uređajima spajanje na mrežu, a mogu biti spojeni preko USB, PCI ili neke druge podatkovne sabirnice. Usmjerivači koji su najčešće i pristupna točka omogučavaju izlaz na internet.

Postoji nekoliko sigurnosnih metoda odnosno protokola. Najčešći i najvažniji su WEP, WPA i WPA2. Danas se sve više izbjegava WEP jer ga je veoma lako probiti. Najpogodnija je WPA2 zaštita u što boljoj kombinaciji velikih i malih slova, brojeva te simbola. Dodatni način sigurnosti izvodi se iz samog sučelja gdje se vrši filriranje IP ili MAC adresa te se time mreža može još bolje osigurati od potencijalnog upada.

3.2.4. ZigBee

[1]ZigBee je bežični komunikacijski protokol namjenjem osobnim mrežama s malom propusnošću i malom potrošnjom energije. Ciljane primjene ZigBee-a su aplikacije koje zahtijevaju umrežavanje velikog broja uređaja, prijenos male količine podataka, malu potrošnju

[1] https://hr.wikipedia.org/wiki/ZigBee

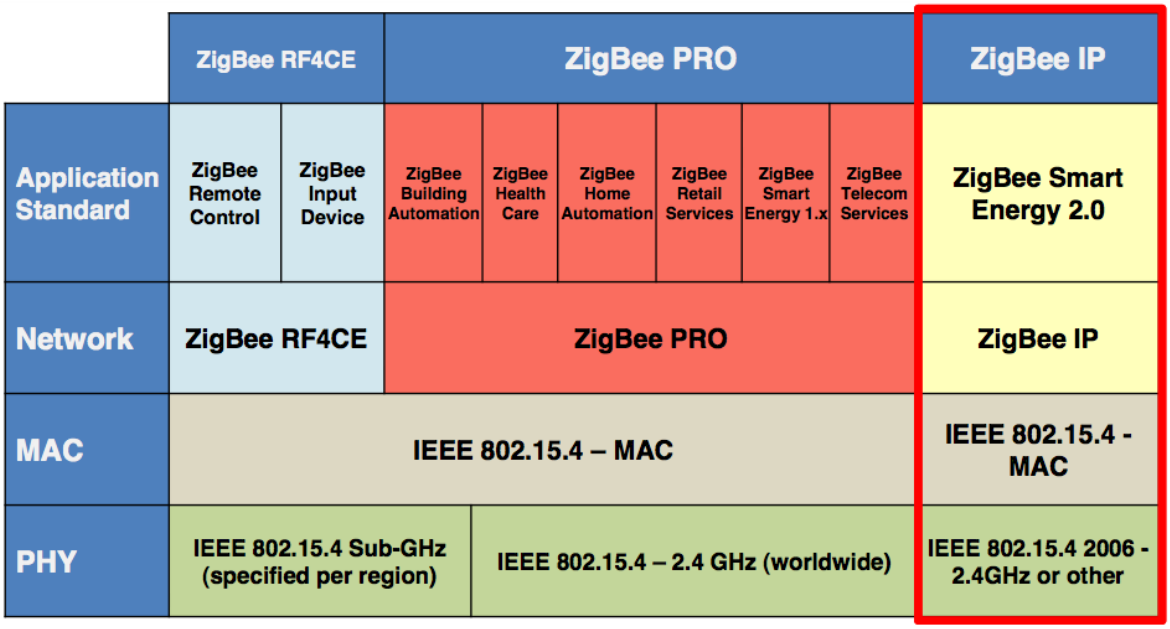
energije te visoku sigurnost prijenosa. ZigBee se temelji na IEEE normi 802.15.4, ali se često ova dva pojma poistovjećuju.

Protokol je nastao zbog potrebe umrežavanja uređaja kod kojih se razmijenjuje mala količina podataka, a aplikacije zahtijevaju veliku autonomiju uređaja, a samim time i veoma malu potrošnju energije. Ovaj protokol se najčešće koristi u mreži senzora kao što su senzori pokreta, senzori otvaranja vrata i prozora, senzori za detekciju dima i mnogi drugi. Sve češće ga se može susresti kao glavni komunikacijski protokol u sustavima pametnih kuća.

Po razini funkcionalnosti dijeli se na dvije osnovne klase uređaja, a to su *FFD (eng. Fully Functional Device)* i RFD *(eng. Reduced Functional Device).* FFD je potpuno funkcionalan uređaj i obično je spojen na stalni izvor napajanja te je energetski neovisan dok je RFD uređaj sa ograničenom funkcionalnošću te ima svoj vlastiti izvor napajanja naprimjer baterije. Protokol definira uređaje po njihovoj funkciji. Tri glavne stavke u sustavu su koordinator, usmjerivač i uređaj. Koordinator dodjeljuje mrežne adrese i vodi brigu o komunikaciji između uređaja. Usmjerivač služi za povećanje dometa mreži i mogućnost spajanja velikog broja uređaja u mrežu. Dok su uređaji obično senzori ili uređaji za kontrolu. Domet je od 10 do 100 metara. Brzina prijenosa 250kbps.

Arhitekturu ugrubo možemo podijeliti na 4 sloja, a to su fizički sloj, sloj za pristup mediju, mrežni i aplikacijski sloj. Fizički sloj aktivira i deaktivira predajnik, mjeri razinu energije signala i kvalitetu veze. Također vrši provjeru oslobođenosti i odabir kanala te šalje podatke. Sloj za pristup mediju (MAC*)* pristupa fizičkom sloju, poreće mrežni koordinator i generira PAN id (*Personal area Network Identifier*). Uspostavlja vezu MAC adresa između različitih čvorova i ostvaruje komunikaciju između susjednih čvorova u mreži. Mrežni sloj je zadužen za cjelokupnu kontrolu mreže. Prima podatke od MAC i aplikacijskog sloja. Pravilno adresira poruke između čvorova. Uključuje i isključuje uređaje s mreže, konfiguracija uređaja itd. Aplikacijski sloj je zadužen samo za komunikaciju između aplikacija koje koristi ZigBee protokol kao način komunikacije.

Postoji nekoliko pod vrsta ovog protokola, sve ovisno o tome za koju namjenu se koristi. Prikaz nekih od podprotokola možemo vidjeti u Tablici 3.3.



Tablica 3.4 Usporedba slojeva kod nekoliko podvrsta ZigBee protokola

Postoje sigurnosni mehanizmi koji omogučavaju filtriranje MAC adresa pa dodatno doprinose sigurnosti.

3.2.5. Ostale značajne komunikacijske tehnologije

- **NFC (*Near field communication*)** - komunikacija bliskog polja je bežična tehnologija sa veoma malim dometom najčešće od par centimetara gdje se komunikacija ostvaruje dodirom dvaju uređaja. Baziran je na RFID komunikaciji. Koristi se elektromagnetska indukcija za razmjenu podataka između antena svakog uređaja. Zastupljena je najčešće u mobilnim uređajima. Radi na frekvenciji od 13.56Mhz. Brzine prijenosa od 100–420kbps.

- **Mobilne mreže** - čine veliki dio komunikacije danas. U IoTu se za komunikaciju na velike udaljenosti koristi prednost GSM/3G/4G mobilnih mreža. Radi na različitim frekvencijama u ovisnosti koji standard se koristi. Maksimalni domet za GSM je oko 35km, dok je za HSPA do 200km. Naravno, sve to ovisno o udaljenosti od odašiljača do odašiljača. Brzina prijenosa podataka primjerice za 3G u prosjeku iznosi do 10 Mbps

- **6LowPAN (*IPv6 Low-power wireless Personal Area Network*)** – komunikacijski protokol baziran na Ipv6 protokolu niske potrošnje energije. Za razliku od drugih protokola 6LowPAN protokol definira mehanizme za enkapsulaciju i sažimanje

zaglavlja. Ključna prednost je što se koristi Ipv6 protokol koji je veoma važan za budućnost IoT tehnologije. Dizajniran je za automatizaciju kuća i zgrada omogućujući složenu kontrolu sustava i komunikaciju sa uređajima preko bežične mreže niske potrošnje energije.

- **Sigfox** – alternativa širokopojasnim mrežama, svojim opsegom nalazi se između WIFI i mobilnih mreža. Koriste ISM frekvencije koje su namijenjene u industrijske,znanstvene i medicinske svrhe u telekomunikacijama. Imaju veoma ograničen frekvencijski spektar te za njihovo korištenje nije potrebno imati nikakve dozvole i licence. Nastala je kao alternativna tehnologija WIFI tehnologiji koja ima relativno kratak domet, a s druge strane komunikacija putem mobilnim mreža je veoma skupa i troši puno energije. Sigfox koristi takozvanu Ultra narrow Band tehnologiju čija potrošnja iznosi 50 uW za razliku od primjerice mobilnih mreža koje troše 5000uW. Omogućava gotovo stotinu puta veću autonomiju nego komunikacija putem mobilnih mreža. U nenaseljenom području ima domet od 30-50km, dok se u naseljenom području može ostvariti domet od 3-10km. Brzina prijenosa podataka kreće se u rasponu od 10-1000bps. U Europi se koriste frekvencije od 868.0 do 868.6 Mhz.

4. PREDNOSTI I NEDOSTACI IoT-A

Kao što svaki sustav ima svoje prednosti i nedostatke tako ih ima i sustav IoT-a. Niti jedan sustav nikad neće biti u potpunosti siguran od potencijalnih upada. Trenutno najveći problem ovog sustava je velika mogućnost za upad ako je sustav loše dizajniran. Najviše se to odnosi na nacionalnu i industrijsku špijunažu. Provedeno je istraživanje gdje su znanstvenici probali hakirati sustav u pametnom automobilu i u tome uspjeli. Uspjeli su upravljati osvjetljenjem automobila te sustavom kočenja bez da vozač može išta učiniti. Provedeno je još jedno testiranje gdje su znanstvenici uspjeli hakirati GPS sustav jedne jahte koji je korišten za navigaciju. Upad je moguć u bilo koji sustav. Sve dok nije ostvaren fizički pristup nekom uređaju možemo reći da je korisnik siguran. Kada se ostvari fizički kontakt na uređaj sigurnost drastično pada. Pod fizički kontakt misli se na pristup uređaju pomoću njegovih serijskih brojeva ili MAC adrese. Samo prestretanje podataka nije toliko kritično koliko fizički upad. Najčešće se uspiju presresti samo neki podaci.

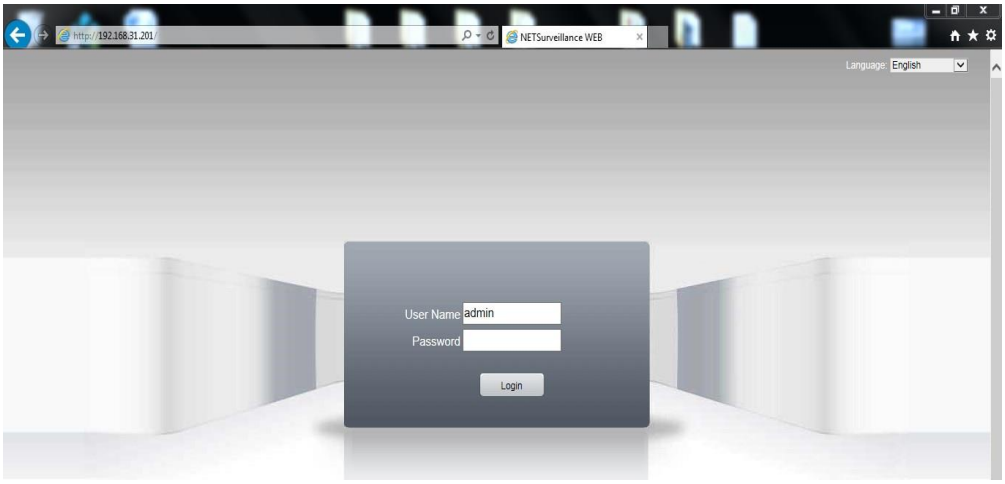
Kod automatizacije u pametnim kućama gdje se ne koristi upravljanje i nadgledanje na daljinu, izlaz na internet nije toliko bitan, pa se ovaj nedostatak u ovom slučaju ne osjeti. Bilo da su uređaji spojeni na lokalnu LAN mrežu ili da su spojeni na neki kontroler preko nekog drugog komunikacijskog protokola kao što je Bluetooth ili RFID.

Pojavljuje se problem zaštite privatnosti. Što više razne tehnologije i uređaja se koristi, razina sigurnosti pada i veća je mogućnost za narušavanje privatnosti. Moguće je da će privatni podaci procuriti na ostatak mreže što je idealno za internet kriminal i krađu identiteta. Kao što je to slučaj sa pametnim telefonima, tako će za koju godinu ovo biti slučaj i kod ovog sustava. Sve što je na mreži može biti praćeno i ugroženo. Najveći izazov kod unaprijeđenja ovog sustava svakako će biti povećanje sigurnosti i zaštite privatnosti korisnika. Uvođenjem temeljitih sigurnosnih provjera vjerodostojnosti i boljih enkripcija biti će moguće ostvariti i bolju zaštitu.

Sa trenutnim sigurnosnim sustavima i mehanizmima ugrađenim u pojedine protokole može se reći da je sustav siguran te nema većih sigurnosnih prijetnji za korisnike.

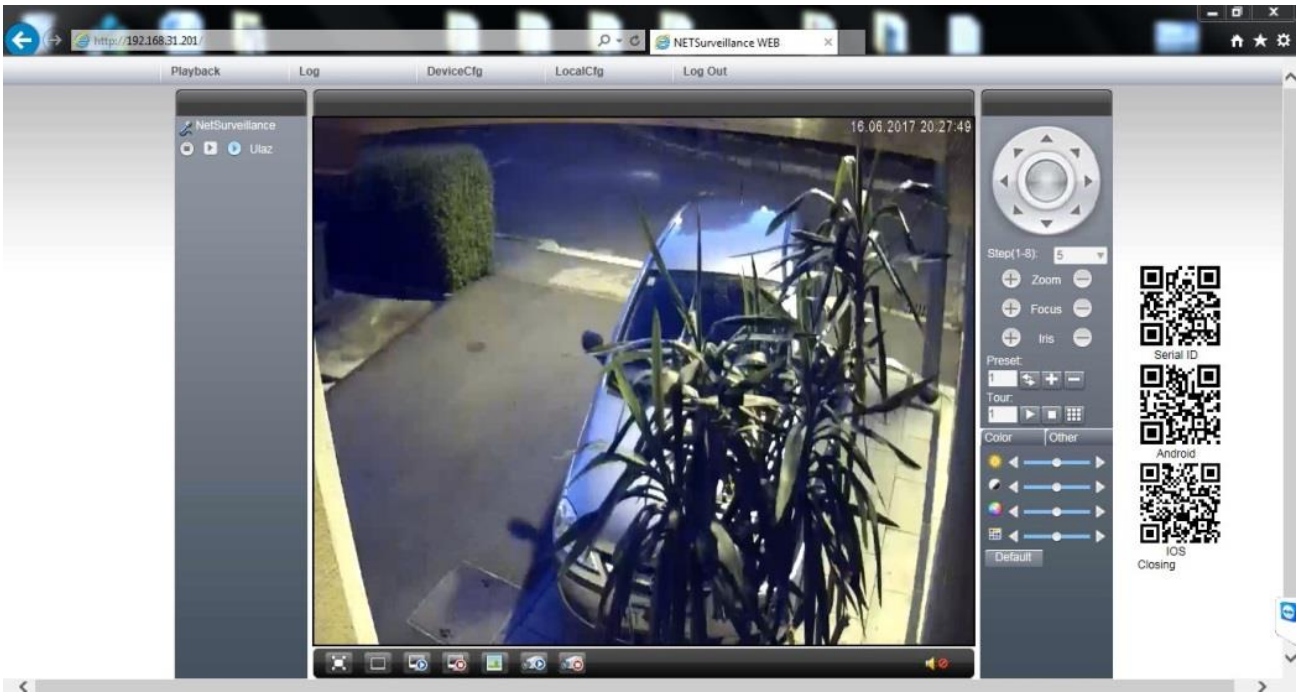
5. PROJEKT PAMETNE KUĆE – NADGLEDANJE U STVARNOM VREMENU

Za potrebe ovog rada i vlastitog interesa u modernu tehnologiju i pametne sustave, nabavljene su dvije jeftinije IP kamere proizvođača ESCAM. Prilično jeftine kamere koje imaju dosta dobre specifikacije. Korištene kamere su ESCAM QF001 koje su se pokazale kao odličan odabir za jednostavniju upotrebu te odličan omjer uloženo-dobiveno. Namijena ove dvije kamere je nadzor glavnog i sporednog ulaza u obiteljsku kuću. Softver korišten u kamerama ne nudi previše opcija jer je besplatan, ali nudi sve najbitnije stavke kao što su reakcija odnosno alarm na detekciju pokreta ili nestanak konekcije. Trenutno je u upotrebi samo direktan prijenos videa sa dojavom detekcije pokreta. Kamere se mogu jednostavno pregledavati na daljinu jer su također povezane i na Cloud. Sučelju se pristupa putem lokalne mreže na koju su kamere spojene. U preglednik se unese IP adresa te se otvara prozor za prijavu kao što se vidi na slici 5.1.



Slika 5.1. Prikaz prozora za prijavu na upravljačko sučelje

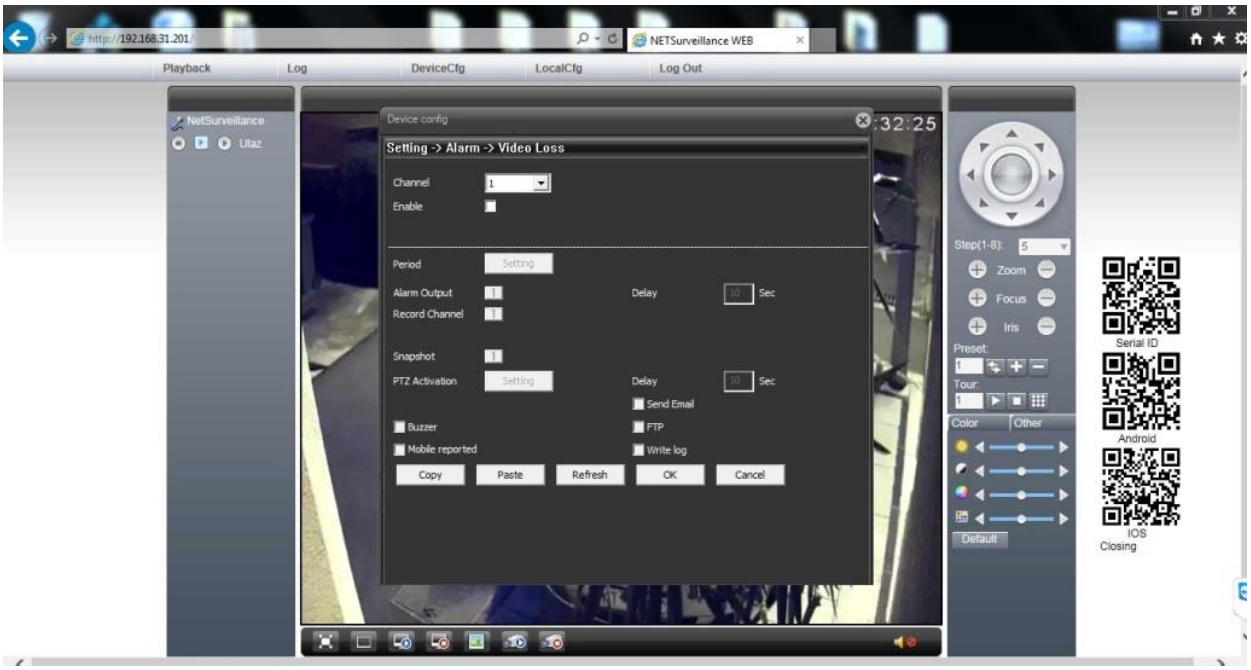
Kameri se pristupa preko njezine jedinstvene IP adrese te podataka za prijavu. Korisničko ime u ovom slučaju je admin te on ujedno služi za pristup sučelju koje ima puna administratorska prava. Može se dodati još korisnika kojima se po izboru mogu dodjeliti prava. Nakon popunjavanja podataka za prijavu otvara se mali prozorčić u kojem biramo kvalitetu prijenosa, postoje dva tipa prijenosa. Glavni prijenos (*eng. main stream*) te sporedni prijenos koji se pokreće kada je lošija internet veza. Odabirom vrste prijenosa pojavljuje se trenutna slika na kameri te sučelje sa svim mogućim postavkama kao što se vidi na slici 5.2.



Slika 5.2. Prikaz prijenosa uživo sa pripadajućim postavkama kamere

Kao što se može vidjeti (Sl. 5.2) sučelje je vrlo jednostavno. Kamera podržava takozvani PTZ (pan, tilt, zoom) što omogućava naknadnu promjenu smjera nadgledanja uređaja. Na početnom ekranu se nalaze opcije za podešavanje same slike kao što su kontrast,svjetlina i udio boje.

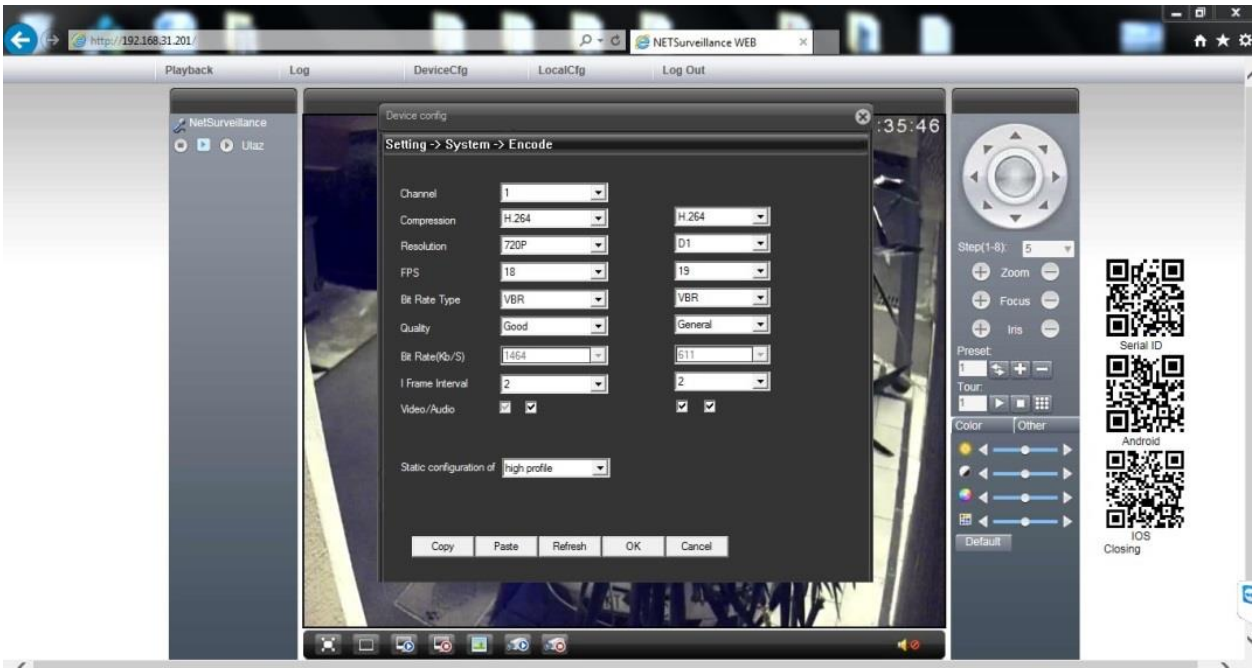
U izborniku „Log“ se nalaze logovi detekcije pokreta koji sadržavaju datum i vrijeme pokreta te naziv uređaja. Kamera naravno ima funkciju snimanja koja se trenutno ne koristi zbog nedostatnog uređaja za pohranu. Snimanje je moguće namjestiti u određenim vremenskim intervalima u tjednu. Moguće je postaviti da se snimanje uključuje na detekciju pokreta i alarm, čak je moguće postaviti neko vrijeme pred snimanja. Kako je sve moguće nadgledati i preko udaljenog servisa u „oblaku“, postoje opcije dojave pokreta preko email-a, zvučnog alarma ili recimo samog loga koji ostaje zapisan u samom sučelju na internoj memoriji. Omogućena je dojava kada video bude izgubljen.



Slika 5.3. Prikaz postavki detekcije gubitka slike

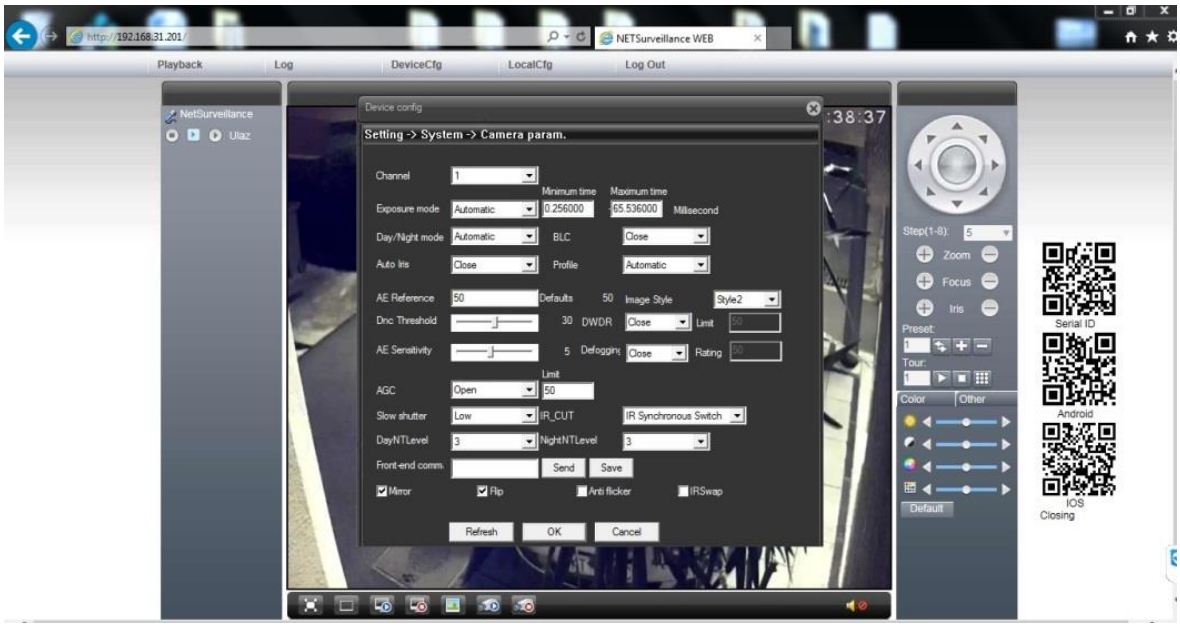
Kamera podržava još nekoliko dojava o promjenama kao što su nedostatak prostora za pohranu, nedostatak uređaja za pohranu i konflikt IP adresa na mreži.

Kao i svaki uređaj, može se namjestiti datum i vrijeme što je kod ovakvog sustava presudno jer je najčešće potrebno znati točno vrijeme ukoliko se snimka naknadno pregledava te je veoma bitno da bude točno unešeno. Mogućnost podešavanja u kojem formatu će biti zapisani datum i vrijeme, te je omogućeno dodavanje imena uređaja na samu sliku. Odabir video standarda omogućen je kao PAL ili NTSC. U djelu postavki koji se odnosi na kvalitetu videa može se podesiti željena kvaliteta glavnog i sporednog video streama kao što je tip kompresije, rezolucija, broj sličica u sekundi i kvaliteta. Ovisno o odabranom načinu kvalitete moguće je odabrati prikaz videa sa zvukom ili bez.



Slika 5.4. Prikaz postavki za određivanje kvalitete videozapisa

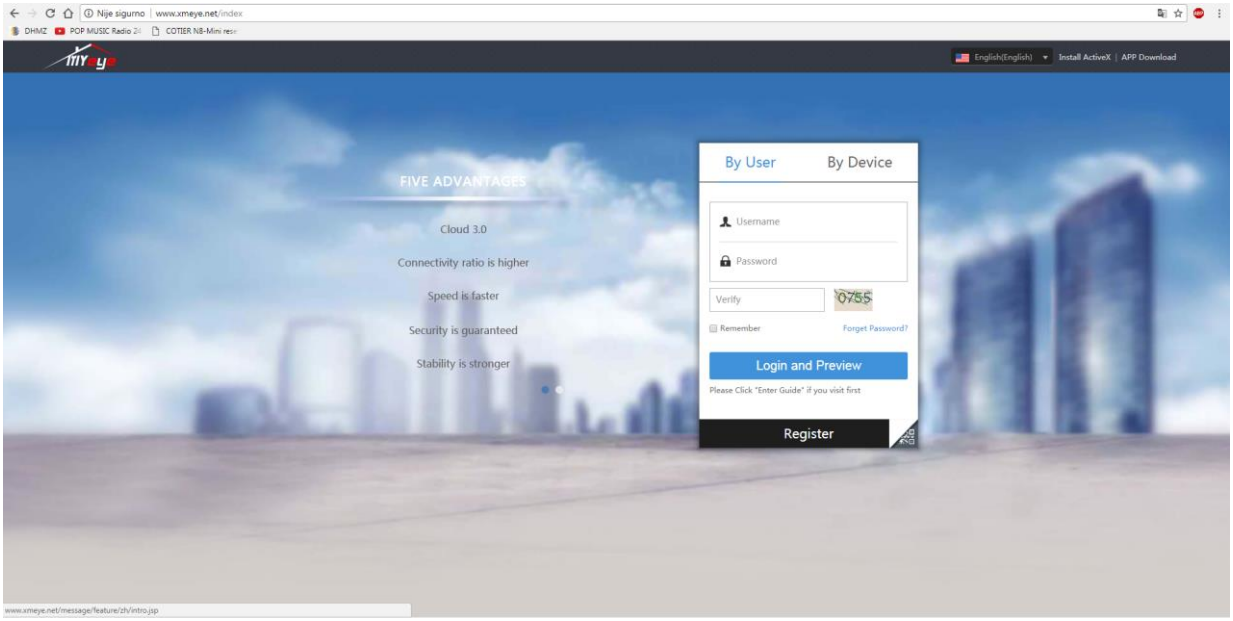
Kod mrežnih postavki nudi se ručno podešavanje IP adrese i DNS servera, kao i samog porta za konekciju. Kamera podržava nekoliko protokola, trenutno se koristi najviše kao P2P (peer to peer) uređaj.



Slika 5.5. Napredne postavke za podešavanje snimanja

Postoji još nekoliko opcija kao što su automatski restart u određeno vrijeme te brisanje starih snimaka. Korisna opcija je napredno podešavanje parametara snimanja gdje se nudi

opcija podešavanja osjetljivosti infracrvenog senzora za snimanje noću te za okretanje i zrcaljenje slike. U normalnim uvjetima korištenja sa stabilnom internet konekcijom kamera nije pokazivala nikakve probleme u korištenju, čak kod temperatura nižih od nula stupnjeva. Opcija okretanja u svim smjerovima radi odlično, snimanje funkcionira bez problema iako se trenutno ne koristi. Zbog toga što je kamera nižeg cjenovnog ranga softver nije najbolji, ali služi svrsi. Uređaje koristim i putem „oblaka“ kojemu se može pristupiti putem mobilne aplikacije ili preko internet preglednika na udaljenom računalu. Aplikacija je besplatna. Uređaji su dodani na „oblak“ putem jedinstvenog serijskog koda uređaja te korisničkih podataka za pristup uređaju.



Slika 5.6. Prikaz prijave na „oblak“

Kao i kod prijave na sučelje kamere preko lokalne mreže, prijava preko udaljenog servisa nudi identične postavke. Korisnici se mogu prijaviti putem korisničkog imena kojim se registriraju na servis ili bez registracije samo unošenjem jedinstvenog serijskog broja uređaja i podataka za prijavu. Najjednostavnija metoda za pristup uređajima van lokalne mreže je preko mobilne aplikacije jer ne zahtijeva nikakav dodatan softver niti posebne preglednike kao što je to slučaj kod prijave putem stranice na računalu.

Kamera u potpunosti opravdava svoju cijenu i uz pomoć nekog dobrog softvera može postići svoju maksimalnu iskoristivost u sustavu video nadzora u pametnoj kući.

6. ZAKLJUČAK

Velikim razvojem i napretkom tehnologije na tržištu su sve dostupniji mnogi pametni uređaji. Prvi uređaji koji su postali masovno popularni su bili pametni mobilni uređaji. Njih je nasljedilo tisuće drugih međusobno povezanih uređaja koji olakšavaju svakodnevni život. Mogućnost komuniciranja između raznih uređaja postavila je jednu sasvim novu dimenziju u modernom svijetu. *Internet of things* koji uređajima omogućava međusobnu interakciju na jedan sasvim drugačiji način nego što je to bilo do sad omogućava kontrolu i pristup uređajima sa bilo kojeg mjesta na svijetu. Omogućena je komunikacija između velikog broja uređaja koji su najčešće u obliku neke vrste senzora. Komunikacija može biti ostvarena na više načina kao što je komunikacija uređaja i čovjeka ili komunikacija uređaja i uređaja.

Testiranjem projekta video nadzora za potrebe ovog rada može se zaključiti kako uz dostupnu tehnologiju za malo novca možemo učiniti svoje kućanstvo uvelike produktivnijim i efikasnijim. Započeti projekt pametne kuće se u budućnosti planira dograditi senzorima pokreta, senzorima otvaranja vrata i prozora, temperaturnim senzorima te senzorima za detekciju dima i ugljičnog monoksida.

IoT je svakako jedan od glavnih pojmova budućnosti i to u svim sferama života. Može se očekivati rapidan rast broja uređaja kroz nekoliko godina te drastična promjena komunikacije između ljudi i stvari koja će biti zasnovana upravo na ovom sustavu.

LITERATURA

[1] F. daCosta, *A Scalable* Approach to Connecting Everything,Apress Media, 2013

[2] http://electronics360.globalspec.com/article/8032/20-billion-connected-internet-of-things-devices-in-2017-ihs-markit-says, lipanj 2017.

[3] A. Bassi, M. Bauer, M. Fiedler, T. Kramp: Enabling Things to Talk, Designing IoT solutions with the IoT Architectural Reference Mode,Springer Heidelberg, New York, 2013.

[4] O. Vermesan, P. Friess, Internet of Things – Converging Technologies for Smart Enviroments and Integrated Ecosystems, River Publishers, 2013.

[5] http://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things - 10.6.2017.

[6] https://solace.com/blog/use-cases/understanding-iot-protocols-matching-requirements-right-option - 10.6.2017.

[7] https://en.wikipedia.org/wiki/Data_Distribution_Service - 10.6.2017.

[8] https://en.wikipedia.org/wiki/MQTT - 10.6.2017.

[9] http://www.hivemq.com/blog/how-to-get-started-with-mqtt - 11.6.2017.

[10] https://en.wikipedia.org/wiki/XMPP - 12.6.2017.

[11] https://xmpp.org/about/technology-overview.html - 12.6.2017.

[12] https://en.wikipedia.org/wiki/Advanced_Message_Queuing_Protocol - 14.6.2017.

[13] https://en.wikipedia.org/wiki/Radio-frequency_identification - 14.6.2017.

[14] https://en.wikipedia.org/wiki/Bluetooth - 14.6.2017.

[15] https://en.wikipedia.org/wiki/Wi-Fi - 15.6.2017.

[16] https://hr.wikipedia.org/wiki/ZigBee - 15.6.2017.

[17] http://internetofthingsagenda.techtarget.com/definition/ZigBee - 15.6.2017.

[18] https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about - 16.6.2017.

POPIS OZNAKA I KRATICA

AMQP - Advanced Message Queuing Protocol

D2D – Device to Device

D2S – Device to Server

DDS – Data Distribution Service

DNS – Domain Name System

GPS – Global Positioning System

GSM – Global System for Mobile Communications

HSPA – Hight Speed Packet Access

IoT – Internet of Things

IP – Internet Protocol

IPv4 – Internet Protocol version 4

IPv6 - Internet Protocol version 6

LAN – Local Area Network

MAC – Media Access Control Address

MQTT – Message Queue Telemetry Transport

MUC – Multi-user Chat

NTSC – National Television System Comittee

P2P – Peer to Peer

PAL – Phase Alternation by Line

PAN – Personal Area Network

PCI – Peripheral Component Interconnect

PTZ - Pan, Tilt, Zoom

RFID – Radio Frequency Identification

RTP – Real-time Transport Protocol

S2S – Server to Server

SASL – Simple Authentication and Security Layer

SSID – Service Set Identifier

TCP – Transmission Control Protocol

TLS – Transport Layer Security

USB – Universal Serial Bus

VoIP – Voice over IP

WEP – Wired Equivalent Privacy

WPA – WiFi Protected access

XML – Extensible Markup Language

XMPP - Extensible Messaging and Presence Protocol

SAŽETAK

Internet of Things je koncept budućnosti. Podrazumijeva međusobnu komunikaciju između raznih uređaja,ljudi i stvari. Za razumijevanje sustava važno je razlikovati protokole za razmijenu podataka te protokole koji služe za komunikaciju između uređaja odnosno stvari.

Opisani su najznačajniji protokoli za razmjenu informacija te najkorišteniji komunikacijski protokoli. Učinjen je kratki osvrt na sigurnost ove tehnologije. Na poslijetku je opisan mali projekt sustava videonadzora u pametnoj kući.

Zaključujemo da je tehnologija dovoljno napredovala da se može iskoristiti čak i u privatnim kućama kako bi se olakšao svakodnevni život ljudi.

ABSTRACT

The Internet of Things is the conception of the future. It means mutual communication between different devices, people and things. To understand the Internet of Things important is to distinguish difference between protocols for data exchange and for communication between devices and things.

The most prominent information sharing protocols and the most used communication protocols are described. A brief review was made about security of this technology. At the end, described is my project for video surveillance monitoring in smart house.

We conclude that technology has progressed enough to be able to use it even in private homes to help people's daily lives.

ŽIVOTOPIS

Sven Obadić rođen je 2. kolovoza 1993. godine u Zagrebu. Živi u Kutini. Pohađao je osnovnu školu Stjepana Kefelje te u višim razredima osnovnu školu Mate Lovraka u Kutini. Nakon osnovne škole upisuje smjer tehničar za računalstvo u Tehničkoj Školi Kutina te ju uspješno završava 2012. godine. 2013. godine upisuje preddiplomski stručni studij Elektrotehnike, smjer Informatika na Elektrotehničkom fakultetu u Osijeku. Veoma je zainteresiran za budućnost pametnih tehnologija, sustava i rješenja. U bližoj budućnosti planira se usavršavati na tom području.

Sven Obadić

_____