Sigurnost sustava pametnih kuća

Mikelić, Toni

Istarsko veleučilište
Università Istriana
di scienze applicate

Toni Mikelić

Sigurnost sustava pametnih kuća

Završni rad

Pula, Rujan 2024.

Istarsko veleučilište
Università Istriana
di scienze applicate

Toni Mikelić

Sigurnost sustava pametnih kuća

Završni rad

JMBAG:0303040909

Studijski smjer: Preddiplomski stručni studij Mehatronike

Predmet: Završni rad

Profesor: Marko Turk, pred.

Pula, Rujan 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Toni Mikelić, kandidat za prvostupnika inženjera mehatronike, izjavljujem da je ovaj Završni rad rezultat isključivo mog vlastitog rada. Temelji se na mojim istraživanjima i oslanja na objavljenu literaturu, što je dokumentirano korištenim bilješkama i bibliografijom. Također, izjavljujem da nijedan dio Završnog rada nije prepisan iz necitiranih izvora i da rad ne krši autorska prava drugih autora. Osim toga, potvrđujem da nijedan dio ovog rada nije korišten u bilo kojem drugom radu ili instituciji, bilo visokoškolskoj, znanstvenoj ili radnoj.

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, Toni Mikelić dajem odobrenje Istarskom veleučilištu – Universita Istriana di scienze applicate, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom Ugrađeni sustav za praćenje prometa i kontrolu prometnih nezgoda koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____

Sažetak

U ovome radu obradit će se tema sigurnosti sustava pametnih kuća. Sistemi pametnih kuća su se zadnjih godina jako razvili i više nisu toliko rijetka pojava. U početku će biti obrađeni sigurnosni sistemi kuća kao što su videonadzor,alarmni sustav, zaključavanje vrata i upravljanje rasvjetom. Cilj samog rada je analizirati sigurnost samog sustava u slučajevima kao što padovi napona, upadi hakera i fizičke sigurnosti server sobe. Provest će se analiza sistema pametnih kuća koje se trenutno nalaze na tržištu i usporediti njihove zaštite sustava. Na temelju prikupljenih podataka donijet će se zaključak o tome koji sustav predstavlja najbolje rješenje, uz preporuke za poboljšanje sigurnosti u određenim situacijama. Primjeri iz privatnog i profesionalnog života poslužit će kao smjernice za primjenu konkretnih mjera, tamo gdje je to moguće, kako bi se povećala ukupna razina sigurnosti.

Ključne riječi: pametna kuća, sigurnost, zaštita, mreža, sustavi

Summary

This final thesis will be focused on the topic of smart home system security. Smart home systems have greatly advanced in recent years and are no longer such a rare occurrence. Initially, the focus will be on home security systems such as video surveillance, alarm systems, door locking mechanisms, and lighting control. The aim of the thesis is to analyze the security of these systems in situations such as power outages, hacker attacks, and the physical security of server rooms. An analysis will be conducted on smart home systems currently available on the market, comparing their security features. Based on the collected data, a conclusion will be made regarding which system offers the best solution, along with recommendations for improving security in certain situations. Examples from both private and professional life will serve as guidelines for the implementation of specific measures, where applicable, to enhance overall security levels.

Keywords: Smart home, security, protection, network, systems

Sadržaj

1. UVOD

Pametna kuća je skup uređaja i senzora koji nam služe za upravljanje kućom. Sam pojam pametne kuće odnosi se na prikladno postavljanje kuće gdje se uređajima i aparatima može upravljati iz daljine putem mobilnog ili nekog drugog umreženog uređaja, zvukovima kao što su glas i pljesak i postavljanjem profila. Pametna kuća također i potencijalno pruža sigurnost, kao i poboljšanu ekološku održivost *(Lin & Bergmann, 2016).*

Uređaji pametne kuće međusobno su povezani i može im se pristupiti preko jedne središnje točke a to može biti pametni telefon, tablet, računalo ili igrača konzola.

Pametna kuća posjeduje i mogućnost samoučenja kako bi mogli naučiti navike vlasnika kuće i prilagoditi postavke kuće da bi vlasniku olakšali svakodnevnu rutinu. Na primjer, pametni klimatizacijski sustav može koristiti široku paletu kućnih senzora i izvora podataka temeljenih na webu za donošenje inteligentnih operativnih odluka, a ne jednostavne sheme ručne ili fiksne kontrole. Pametni klimatizacijski sustav može predvidjeti očekivanu popunjenost kuće praćenjem podataka o lokaciji kako bi se osiguralo da klima uređaj postiže željenu razinu udobnosti kada je kuća nastanjena i štedi energiju kada nije *(Lin & Bergmann, 2016).*

Uz nabrojane mogućnosti još jedan jako bitan dio pametne kuće je i njezina sigurnost. Video nadzor, alarmi sustav, razni senzori pokreta, brave na vratima jedni su od načina kako zaštiti kuću od provala.

S obzirom da je to pametna kuća čiji je sistem ustvari računalo povezano na internet moramo uzeti u obzir sigurnost samog sustava. Sustav moramo zaštiti fizički na način da prostoriju u kojoj nam je centralna jedinica bude pod posebnim ključem, da je mogu otvoriti određene osobe i da bude zaštićena alarmom. Isto tako bitno nam je i napajanje samog sustava i što u slučaju nestanka struje iz mreže. U tom slučaju potrebno je imati baterijski sustav ili UPS (Uninterruptible Power Supply) koji štiti računalo, i ostale komponente koje uključimo preko UPS-a, od oscilacija u strujnoj mreži. Još je jedna stvar jako bitna kad je u pitanju sigurnost sistema a to je software-ska sigurnost. Pošto cijeli sistem funkcionira preko interneta prvo što nam pada na pamet su 'hakeri'. Dosta često nailazimo na razna pisanja i komentare o pametnim kućama i njihovoj sigurnosti i kako 'haker' može doslovno preko rasvjetnog tijela upasti u naš sistem, bilo koji pametni kućni uređaj koji se može povezati s internetom može biti hakiran. Na primjer,

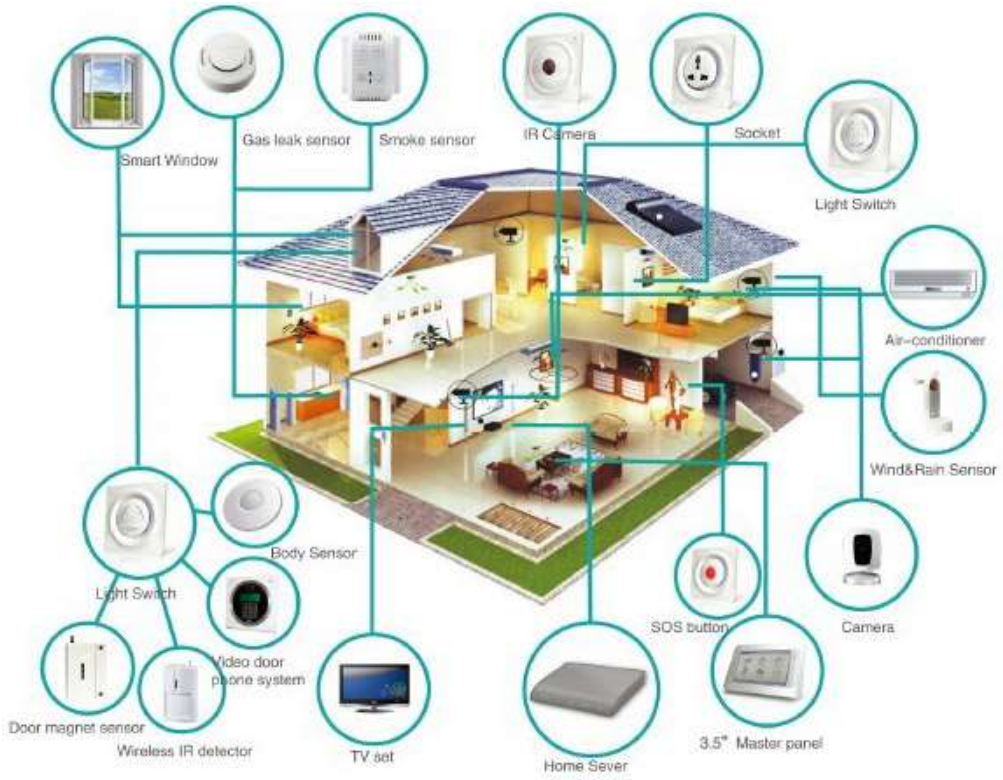
ako je pametni zvučnik povezan s Wi-Fi ruterom, koji je također povezan s pametnim televizorom, video zvonom i pametnim termostatom, tada bilo koji od tih uređaja može proslijediti ranjivosti na drugi. Ako je jedan uređaj hakiran, i ostatak je vjerojatno osjetljiv na hakiranje. Stoga nam je potreban plan kako zaštititi ne samo jedan uređaj, već i sve stavke u pametnom sustavu tj. kući. Prva stvar koja je i najjednostavnija je stvoriti jaku i sigurnu lozinku za WiFi mrežu. Druga bitna stavka je vatrozid a da bi nas vatrozid štitio mora biti kvalitetan i od licenciranog davatelja usluge kojeg je potrebno ga podesiti i redovno ažurirati. Još je dosta načina zaštite sustava koje ćemo obraditi u samom radu.

2. PAMETNE KUĆE

Da bi pametna kuća funkcionirala, potrebno je nekoliko ključnih komponenti i tehnologija koje omogućavaju međusobnu komunikaciju uređaja, automatsko upravljanje i centralizirano kontroliranje sustava. Prvo što je bitno navesti su pametni uređaji. Pametni uređaji su uređaji povezani na mrežu koji mogu i ne moraju komunicirati jedni s drugima i s korisnicima putem mobilnih aplikacija ili glasovnih asistenata. Obraditi ćemo par uređaja, a to su pametni termostati, pametni prekidači i žarulje, pametne brave, pametni senzori, pametne kamere i sigurnosni sustavi te pametni kućanski uređaji *(Young*, 2019).

Da bi svi ti uređaji mogli komunicirati potreban nam je centralni sustav upravljanja, često nazvan "hub" ili "kontroler" koji služi kao središnja točka koja omogućuje povezivanje i kontrolu svih pametnih uređaja u kući. Njegova glavna funkcija je omogućiti komunikaciju između različitih uređaja i protokola, centralizirati kontrolu nad kućnim sustavima te olakšati automatizaciju. Moguće je imati pametnu kuću i bez centralnog sustava upravljanja. Ovo se naziva decentralizirani ili distribuirani sustav pametne kuće. U takvom sustavu svaki pametni uređaj funkcionira neovisno, a upravljanje se često vrši izravno putem mobilnih aplikacija ili glasovnih asistenata, umjesto da se svi uređaji povežu na jedan centralizirani kontroler. Nedostatak je što u ovome slučaju ne možemo imati potpuno automatizirani sustav koji prepoznaje naše rutine nego mi kao korisnik putem raznih aplikacija sami kontroliramo dobivene podatke i upravljamo uređajima (Athom B.V., 2024)

Uz sve navedeno još je jedna bitna stavka a to je stabilna i pouzdana mrežna infrastruktura koja može podržati različite vrste uređaja i komunikacijskih protokola. Postoje tri vrste mreže a to su bežična mreža (Wi-Fi), žičana mreža (ethernet) ili mesh mreža. Ovisno o složenosti pametne kuće i broju povezanih uređaja, mreža mora biti sposobna pružiti dovoljno propusnosti, raspon pokrivenosti i sigurnost kako bi se osigurao nesmetan rad svih pametnih sustava.



Slika 1*:Prikaz pametne kuće i njezinih uređaja*

(Izvor: https://three-s.co/solutions/smarthome-solutions/)

2.1. ELEMENTI SUSTAVA PAMETNIH KUĆA

2.1.1. Videonadzor

Sustavi videonadzora pružit će nam mir jer omogućuju brzo i jednostavno postavljanje i zaštitu vaše kuće i dvorišta. Većina setova za kućni videonadzor koji se nalaze na tržištu jednostavno i dobro se integriraju u postavke pametne kuće, što znači da je nevjerojatno lako postaviti kamere i detektore u dom, dolaze s aplikacijama za pametne telefone koje vam omogućuju nadziranje imovine bez obzira gdje se mi nalazili. Mnogi od tih setovi dolaze s kamerama i senzorima kao dio paketa, što olakšava postavljanje odmah, dok su drugi modularniji, što vam omogućuje kupnju dodatnih kamera i senzora ovisno o veličini vašeg doma.

Videonadzor pokreće mobilna aplikacija za nadzor koja nam omogućuje nadzor i upravljanje našim sigurnosnim kamerama pomoću pametnog telefona ili tableta. Takva aplikacija bogata je značajkama koje nam pružaju potpunu kontrolu nad kućnom sigurnošću. Također aplikacije za video nadzor omogućuju nam upravljanje s više

kamera odjednom, spremanje video materija nekoliko dana unazad ovisno o memoriji, slanje obavijesti na mobilni uređaj čim je kretnja u području nadzora aktivna pa čak i aktiviranje alarma (ProTech Security, 2021)

Slika 2*: Kontrola videonadzora putem pametnog telefona*

(Izvor: https://protechsecurity.com/mobile-control-and-video-surveillance-for-smart-home-security-systems/)

2.1.2. Alarmni sustav

Za alarmi sustav pametne kuće koriste se razni senzori kao što su senzori detekcije pokreta, senzori za dim i plin, senzor poplave. Takvi uređaji spojeni su WiFi signalom sa centralnom upravljačkom jedinicom koja očitanja senzora prikazuje na smartphone-u. Ovaj sustav prati sve prostorije u kući i u njima mjeri razinu ugljičnog monoksida i temperaturu. Na taj način može ne samo otkriti požar, već i točnu lokaciju na kojoj je požar izbio i automatski proslijediti tu informaciju vatrogascima (CIS FER, 2012) Za razliku od starih alarmnih sustava gdje se moralo na centralnu jedinicu upisivati razne kodove na smart home dovoljno je samo izgovoriti glasovnu naredbe ili pljesak i alarm se gasi. Također ako se alarm ne ugasi u određenom vremenu smart home automatski alarmira odgovarajuće hitne službe.

Slika 3*: Senzor dima*

(Izvor: https://medium.com/@dave.wechsler/how-the-smart-home-and-the-internet-of-things-iot-may-materially-impact-non-catastrophic-peril-66e7fdbedb21)

2.1.3 Pametni prekidači

Pametni prekidači omogućuju korisnicima upravljanje rasvjetom iz bilo kojeg mjesta putem pametnih telefona ili tableta, pod uvjetom da imaju internetsku vezu, što pruža praktično upravljanje rasvjetom čak i kad nisu kod kuće. Većina pametnih prekidača koristi bežične komunikacijske protokole poput Wi-Fi-ja, Zigbeeja, Z-Wavea ili Bluetootha kako bi se povezali s kućnom mrežom, omogućujući nesmetanu komunikaciju između prekidača, pametnih uređaja i drugih kompatibilnih uređaja unutar pametnog doma.

Integracija s glasovno kontroliranim asistentima poput Amazon Alexe, Google Assistanta ili Appleove Siri omogućuje korisnicima da upravljaju svjetlima glasovnim naredbama, pružajući potpuno hands-free iskustvo. Pametni prekidači također omogućuju postavljanje rasporeda za automatsko uključivanje ili isključivanje svjetla u određeno vrijeme, što pomaže simulirati prisutnost dok ste odsutni, poboljšava sigurnost doma i optimizira potrošnju energije.

Mnogi pametni prekidači nude mogućnost prigušivanja svjetla, što omogućuje prilagodbu razine svjetline za različite aktivnosti ili raspoloženja. Uz to, korisnici mogu

kreirati prilagođene scenarije osvjetljenja za posebne prilike poput filmskih večeri, večera ili opuštanja. Napredniji modeli dolaze s opcijom praćenja potrošnje energije, pružajući korisnicima uvid u obrasce potrošnje i omogućujući im donošenje odluka o energetski učinkovitim opcijama osvjetljenja, što može smanjiti račune za struju.

Pametni prekidači često se integriraju s popularnim platformama za pametne domove poput Amazon Alexe, Google Assistanta, Apple HomeKita ili Samsung SmartThingsa, omogućujući jednostavnu interakciju s drugim pametnim uređajima unutar istog ekosustava (Digital Home Systems Pty Ltd, *2023*).

2.1.4 Pametni klima uređaji

Pametna klima u sustavu pametne kuće odnosi se na sustav grijanja, ventilacije i klimatizacije (HVAC) koji se može daljinski upravljati, automatizirati i prilagođavati prema potrebama korisnika. Ovaj sustav koristi naprednu tehnologiju za optimizaciju udobnosti i energetske učinkovitosti unutar doma.

Jedna od ključnih značajki pametne klime je mogućnost daljinskog upravljanja putem aplikacija na pametnim telefonima ili tabletima. To omogućuje korisnicima da prilagode temperaturu, raspored grijanja ili hlađenja, čak i kada nisu kod kuće. Na primjer, može se programirati klima uređaj da se uključuje neposredno prije nego što se vratite iz posla, čime osiguravate ugodnu temperaturu kada stignete.

Pametna klima se također može integrirati s drugim pametnim uređajima u kućanstvu. Na primjer, sustav može automatski prilagođavati temperaturu na temelju prisutnosti ili odsutnosti osoba u prostoriji, koristeći senzore pokreta ili pametne prekidače. Također, neki sustavi koriste podatke o vremenskim uvjetima i prognozama kako bi optimizirali radni učinak. Osim udobnosti, pametna klima pomaže i u štednji energije. Uz mogućnost praćenja potrošnje energije putem aplikacija, korisnici mogu osigurati da njihovi sustavi rade efikasnije i smanjiti tako troškove grijanja i hlađenja. Pametni termostati, koji su često dio ovog sustava, omogućavaju precizno upravljanje temperaturom i pravilno postavljanje rasporeda.

Sve u svemu, pametna klima u sustavu pametne kuće značajno doprinosi poboljšanju kvalitete života, pružajući udobnost i energetsku učinkovitost putem sofisticiranih tehnologija (Athom B.V., 2022).

2.1.5 Pametni prozori

Pametni prozori su inovativni dijelovi pametnog doma koji poboljšavaju udobnost, sigurnost i energetsku učinkovitost u kućanstvima. Ovi prozori integriraju različite funkcionalnosti koje omogućuju automatsko ili daljinsko upravljanje, a mogu se koristiti u sklopu šireg sustava pametne kuće.

Neke od prednosti pametnih prozora su njihova sposobnost regulacije svjetlosti. Na primjer, neki pametni prozori koriste tehnologiju koja omogućuje promjenu prozirnosti stakla, čime se kontrolira količina sunčeve svjetlosti koja ulazi u prostoriju. Ova funkcionalnost pomaže u smanjenju potrebe za umjetnom rasvjetom i, istovremeno, održava udobnu temperaturu unutar doma.

Pametni prozori također mogu biti opremljeni senzorima koji prate vanjske uvjete, kao što su temperatura i vlažnost, te na temelju tih informacija prilagođavaju svoj položaj ili razinu privatnosti. Na primjer, ako se temperatura u prostoriji poveća zbog sunčeve izloženosti, pametni prozor može automatski zatamniti staklo ili otvoriti prozore radi poboljšanja ventilacije. Osim regulacije svjetlosti i temperature, pametni prozori često su povezani s sustavima sigurnosti. Mogu se integrirati s alarmima ili kamerama, što omogućuje praćenje i zaštitu doma. Korisnici također mogu daljinski zaključati ili otključati prozore putem aplikacije, što dodatno povećava sigurnost (Dunleavy, 2024).

3. SIGURNOST SUSTAVA

Identificirana su četiri široka područja u kojima pametni kućni uređaji mogu pružiti značajne koristi korisnicima: zdravstvene koristi, ekološke koristi, financijske koristi te psihološko blagostanje i socijalna uključenost. Ove koristi odražavaju najvažnije aspekte koje su identificirali Sovacool i Furszyfer Del Rio u svojoj studiji temeljenoj na intervjuima s ekspertima, pri čemu ti autori također ističu važnost "ugodnosti i kontrolabilnosti" koje nude pametne kuće *(Buil-Gil et al, 2023).*

No, osim potencijalnih prednosti, važno je razumjeti i rizike te izazove povezane s korištenjem tehnologija pametnih domova.

Potrošački IoT (Internet of Things) može se na više načina zloupotrijebiti u kriminalne svrhe, a lako je pronaći primjere napada koji uključuju pametne kućne uređaje. Među najpoznatijim slučajevima je botnet Mirai, koji iskorištava slabosti u sigurnosti IoT uređaja i koji je korišten u brojnim disruptivnim DDoS (Distributed Denial-of-Service) napadima diljem svijeta.

Autori prvih napada 2016. godine objavili su izvorni kod za Mirai, što je omogućilo njegovo ponovno korištenje i prodaju kao uslugu DDoS-a "na iznajmljivanje". Godine 2017., programeri Mirai zlonamjernog softvera također su proglašeni krivima za infekciju IoT uređaja i kućnih usmjerivača, stvarajući time još jedan botnet koji je korišten u prijevari klikova za generiranje nezakonitih prihoda od oglašavanja.

Osim toga, drugi poznati napadi uključivali su hakiranje kućnih kamera koje se koriste za sigurnost i nadzor doma i ukućana, čime je omogućeno slobodno pregledavanje privatnih videa na internetu. Ovakvi incidenti dodatno naglašavaju potrebu za jačanjem sigurnosti i privatnosti u svijetu pametnih domova.

IoT uređaji rade slanjem, primanjem i analizom sirovih podataka iz stvarnog svijeta, a zatim se koriste, djelomično ili potpuno, za izvršavanje unaprijed programiranih ili korisnički definiranih radnji. Procjenjuje se da će do 2030. godine u svijetu postojati 25,44 milijardi aktivnih IoT uređaja, što znači otprilike tri IoT uređaja za svaku osobu na ovoj planeti. Ovoliki broj svakako pridaje značajnu težinu njihovoj prisutnosti, a možemo s pouzdanjem pretpostaviti da će se broj IoT uređaja nastaviti povećavati svake godine, dok neprestano pronalazimo nove praktične primjene u raznim područjima, uključujući, ali ne ograničavajući se na, zdravstvenu skrb, nosive

tehnologije, kućnu zabavu, sigurnost, poljoprivredu, isporuku i praćenje, prijevoz, infrastrukturu gradova, proizvodnju energije te maloprodaju i industriju.

Nažalost, zbog nedostatka adekvatnih sigurnosnih mjera, IoT uređaji su često ranjivi na razne sigurnosne prijetnje. To uključuje korištenje zadanih lozinki koje su lako kompromitirane od strane napadača, što im omogućuje da iskoriste te uređaje za pokretanje napada na druge povezane uređaje ili mreže. Također, mnogi uređaji koriste zastarjeli firmware koji može biti podložan poznatim ranjivostima, nemaju sigurnosne mehanizme prilikom pokretanja te ne koriste enkripciju.

Osim toga, zapanjujućih 98% prometa koji se sastoji od korisničkih podataka, komandi i očitanja senzora često se prenosi kroz otvorene internetske kanale bez ikakve enkripcije, što ih čini izuzetno ranjivima na najosnovnije oblike napada „čovjeka u sredini“(„man in the middle“). Ovi napadi omogućavaju napadačima da presretnu, pročitaju ili čak modificiraju osjetljive podatke u običnom tekstu, bez znanja pošiljatelja ili primatelja. Izvještaji također pokazuju da je do 57% svih povezanih IoT uređaja danas još uvijek ranjivo na većinu napada umjerene do visoke ozbiljnosti, o kojima će biti riječi u nadolazećim dijelovima ovog rada. Nažalost, situaciju dodatno komplicira to što većina korisnika obično ostavlja svoje uređaje nezaštićenima upotrebom zadnjih korisničkih podataka i tvorničkih postavki *(Kabir et al, 2023).*

Napade dijelimo prema cilju štete na nekoliko vrsta.

Cyber-dependent harm odnosi se na štetu koja proizlazi iz kriminalnih aktivnosti koje se mogu izvršiti isključivo putem digitalnih tehnologija, poput računala, mreža i interneta. Ovi zločini ovise o tehnologiji kako bi se dogodili, te bez digitalnih sustava ne bi bili mogući.

Primjeri cyber-dependent štete uključuju hakerske napade, gdje se neovlašteno pristupa računalima i mrežama, malware napade koji koriste zlonamjerni softver za uništavanje ili kontrolu sustava, te DDoS napade koji preopterećuju mreže kako bi usluge postale nedostupne.

Jedan od njih je i cyber-enabled harm. To su kriminalne radnje koje su se mogle dogoditi i bez tehnologije, ali se sada izvode brže, šire ili učinkovitije uz pomoć interneta.

Primjeri cyber-enabled štete uključuju prijevare kao što su online financijske prijevare, gdje kriminalci koriste internet za krađu novca ili podataka. Krađa identiteta je također olakšana internetom, jer se osobni podaci lakše prikupljaju putem društvenih mreža ili hakiranih baza podataka. Online uznemiravanje i zlostavljanje, poput cyberbullyinga ili doxxinga, gdje su osobne informacije objavljene kako bi se nekoga naštetilo, još je jedan oblik cyber-enabled štete *(Buil-Gil et al, 2023).*

Iako su pametni domovi jedinstvena okruženja, sigurnosne prijetnje s kojima se suočavaju vrlo su slične onima u drugim područjima. Jedna od glavnih briga su prijetnje povjerljivosti, koje uključuju neplanirano otkrivanje osjetljivih informacija. Na primjer, povrede sigurnosti u sustavima za nadzor doma mogu otkriti osjetljive podatke, poput medicinskih informacija. Čak i naizgled bezopasni podaci, poput unutarnje temperature doma, mogu se iskoristiti za utvrđivanje je li kuća zauzeta, što može dovesti do provale. Gubitak povjerljivosti ključeva ili lozinki također može omogućiti neovlašten pristup sustavu.

Prijetnje autentifikacije odnose se na rizik od neovlaštenog mijenjanja podataka o senzorima ili kontrolama. Na primjer, ako obavijesti o statusu sustava nisu ispravno autentificirane, mogu pokrenuti pogrešne radnje, poput toga da sustav za upravljanje domom pogrešno otvori vrata i prozore zbog lažne hitne situacije, omogućujući tako nezakonit ulaz. Problemi se mogu pojaviti i kod automatskih softverskih ažuriranja ako nisu pravilno autentificirana.

Najveći rizik predstavljaju prijetnje pristupa, gdje neovlašteni pristup, osobito na administratorskoj razini, kompromitira cijeli sustav. To se može dogoditi zbog lošeg upravljanja lozinkama ili ključevima ili povezivanjem neovlaštenih uređaja na mrežu. Čak i bez potpune kontrole, neovlašteni pristup može ukrasti propusnost ili uzrokovati uskraćivanje usluge legitimnim korisnicima. Pametni kućni uređaji, koji su često na baterije i povezani bežično, također su ranjivi na napade iscrpljivanja energije, gdje preplavljivanje mreže zahtjevima troši energiju uređaja i tako ih onesposobljava *(Lin & Bergmann, 2016)*.

3.1. Zaštita sustava prilikom nestanka električne energije

Prilikom nevremena često zna doći do nestanka električne energije, ali što to znači za našu pametnu kuću? Neki uređaji u sebi imaju integrirane baterije koje ih u slučaju nestanka električne energije održavaju na životu još neko vrijeme ali većina uređaja nema tu mogućnost.

Upravo zbog takvih situacija pametno je u kući imati UPS sustav. UPS (Uninterrupted Power Supply) je rezervna baterija koja služi kao zaštita od prenapona. Kad god UPS primijeti nestanak struje, zaštitit će vaš uređaj od bilo kakvog povratnog udara, a njegova baterija služi za napajanje uređaja sve dok se ne vrati napajanje iz mreže. Pomoću njega smart home i u slučaju nestanka električne energije i dalje ima uključenu zaštitu i ostaje sigurna kuća.

4. SIGURNOST KOMUNIKACIJE

Kao što je već navedeno pametne kuće za povezivanje koriste internetski protokol i svi su uređaji povezani putem čvorišta. Uređaji koji su spojeni na internet prikupljaju i pohranjuju podatke o našoj upotrebi, navikama i sklonostima - bilo na uređaju ili na mreži. Svi ti podaci čine pametni dom potencijalnim rizikom za našu privatnost, a svaki uređaj koji dodate u mrežu dodaje novu zabrinutost.

Zapravo, mnogi stručnjaci vjeruju da s takvim uređajima ne biste trebali razmišljati o tome što će se dogoditi 'ako' su hakirani, nego 'kada' jer ih je lako hakirati i nude malo zaštite. Ako nam je Smart home sustav povezan na glavni i jedini ruter u kući onda nisu ugroženi samo podaci s naših smart home uređaja. Svaki bi upad u sustav mogao ugroziti naše privatne podatke, uključujući e -poštu, naše račune na društvenim medijima, pa čak i naše bankovne račune. Nažalost, treba zapamtiti da ne postoji IT infrastruktura koja je 100% sigurna. Jedino što možemo učiniti je nastojati smanjiti rizik zato, kod projektiranja i povezivanja uređaja i sustava pametne kućne, vrijedi analizirati što nam je važno i koji je rizik. Postoje razni načini kojima bismo mogli poboljšati sigurnost naše kuće, te ćemo u nastavku navesti neke od njih *(White et al, 1995).*

4.1. Različite kućne mreže

Prvi korak u rješavanju kućne sigurnosti je izoliranje vaše pametne kućne mreže od drugih mreža. To je relativno jednostavno učiniti postavljanjem mreže za goste za kućne uređaje. Na primjer, u tom slučaju hladnjak bi se još uvijek mogao hakirati kako bi postao dio botneta koji šalje neželjenu poštu ili rudari kriptovalute. Međutim, budući da zauzima vlastitu mrežu, neće moći pristupiti e-pošti ili bankovnom računu. Za aktivaciju opcije mreža za goste moramo ući u postavke rutera i potražiti referencu za pristup gostu ili gostujuću mrežu. Da bismo pristupili tim postavkama, moramo znati administrativno korisničko ime i lozinku za ruter, kojima se može pristupiti putem web preglednika ili aplikacije ako je dostupna za naš uređaj. Ako ruter ima opciju koja dopušta gostima pristup lokalnim mrežnim resursima, najbolje je isključiti ju. U nekim slučajevima uređaj može koristiti izraz "Izoliraj" koji postiže istu stvar, a to je da zadrži sve što je povezano s gostujućom mrežom za pristup bilo čemu osim Internetu.

Druga mogućnost je imati dvije zasebne internetske veze od kojih svaka koristi svoj ruter. To je najsigurniji i najjeftiniji pristup. Možemo ostati na istoj mreži i ugovoriti drugu vezu ili u drugoj mreži ugovoriti još jednu dodatnu internet vezu.

Treća mogućnost je ujedno i najkompliciranija a to je koristiti jednu internetsku vezu, ali dva odvojena rutera koji su pravilno povezani i konfigurirani. Nepravilno povezivanje neće postići sigurnosni cilj izolacije uređaja. Ovo nije nešto što bih preporučio, osim ukoliko se osoba koja to postavlja i konfigurira, ili netko tko pomaže razumije u mrežu. Većina rutera ili nije zaštićena ili koristi tvorničku lozinku poput "admin", što svakako puno olakšava pristup uređajima pametnog doma koji su spojeni na ruter. Prvo što trebamo napraviti je zamijeniti postavljenu lozinku snažnom i jedinstvenom. Način na koji ćemo to napraviti razlikuje se ovisno o uređaju, ali je u osnovi isto. Moramo razmisliti i o promjeni SSID-a (Identifikator skupa usluga), koji je samo naziv naše Wi-Fi mreže, pošto dosta proizvođača koristi naziv specifičan za određeni model pa ga hakeri mogu lako probiti (*Data Doctors*, 2019).

4.2 PROTOKOLI SPAJANJA NA MREŽU

4.2.1. WiFi

Wi-Fi je jedan od najčešće korištenih protokola za bežično povezivanje u pametnim kućama zbog svoje široke kompatibilnosti i fleksibilnosti. Wi-Fi radi na principu bežičnog prijenosa podataka koristeći radiovalove. Najčešće korištene frekvencije su 2.4 GHz i 5 GHz, ove frekvencije su nelicencirane i dostupne za opću uporabu. Sigurnost Wi-Fi-a je snažna, osobito s novijim standardima poput WPA3. Međutim, Wi-Fi mreže su česta meta napada, pa je važno osigurati snažnu autentifikaciju i zaštitu lozinkama.

Prednosti spajanja putem Wi-Fi-a uključuju široku kompatibilnost s različitim uređajima, što omogućava jednostavno povezivanje bez obzira na vrstu uređaja koji koristite. Također, instalacija i konfiguracija Wi-Fi mreže su vrlo jednostavne, što čini postupak postavljanja pristupačnim i brzim za korisnike. Uz to, Wi-Fi pruža veliku fleksibilnost u postavljanju uređaja, jer nije ograničen fizičkim kablovima, što omogućava slobodnije raspoređivanje uređaja unutar prostora.

Nedostatci spajanja putem Wi-Fi-a uključuju nekoliko važnih aspekata. Prvo, Wi-Fi mreže mogu biti osjetljiva na smetnje koje dolaze od drugih Wi-Fi mreža ili elektroničkih uređaja, što može utjecati na stabilnost veze. Drugo, sigurnosni rizici su prisutni ako mreža nije pravilno zaštićena, što može dovesti do neautoriziranog pristupa i potencijalnih prijetnji privatnosti. Treće, neki ruteri imaju ograničen broj istovremenih veza, što može uzrokovati probleme u slučajevima kada je potrebno povezati veliki

broj uređaja. Ovi nedostatci mogu utjecati na ukupno iskustvo korištenja Wi-Fi mreže, pa je važno biti svjestan tih izazova i poduzeti odgovarajuće mjere kako bi se minimizirali njihovi učinci.

4.2.2. Zigbee

Zigbee je popularan bežični komunikacijski protokol dizajniran za aplikacije s niskom potrošnjom energije, kao što su pametne kuće, IoT (Internet of Things) uređaji i industrijska automatizacija.

Zigbee uređaji troše vrlo malo energije, što omogućava dugotrajan rad na baterije. Ovo je idealno za senzore, pametne prekidače i druge uređaje koji ne zahtijevaju stalno napajanje.

Također, Zigbee koristi mrežnu topologiju (mesh network), što znači da svaki uređaj u mreži može djelovati kao čvor koji prenosi podatke drugim uređajima. To povećava domet i pouzdanost mreže, jer podaci mogu pronaći alternativni put do odredišta ako neki čvor nije dostupan. Zigbee koristi AES-128 enkripciju za zaštitu komunikacije između uređaja, što pruža solidnu razinu sigurnosti, osobito u kućnim i IoT aplikacijama.

4.2.3. Bluetooth

Bluetooth je dobar izbor za pametne uređaje s niskom potrošnjom energije i niskim zahtjevima za propusnost podataka, poput senzora, brava i prekidača. Bluetooth Low Energy (BLE) je posebno koristan zbog dugotrajne baterije. Bluetooth koristi nekoliko slojeva sigurnosnih mehanizama, uključujući AES-128 enkripciju, također koristi mehanizme za uparivanje i autentifikaciju, čime se povećava razina sigurnosti. Međutim, zbog ograničenog dometa i niske propusnosti, nije idealan za uređaje koji trebaju konstantan i visokopropusni prijenos podataka, kao što su sigurnosne kamere ili multimedijalni sustavi, uglavnom se koristi za jednostavne uređaje poput senzora, brava, termostata ili osvjetljenja.

4.2.4. Ethernet

Ethernet je jedan od najstarijih i najpouzdanijih protokola za povezivanje uređaja na mrežu i također može igrati ključnu ulogu u pametnim kućama. Iako je Ethernet tradicionalno žičani protokol koji koristi kablove za povezivanje uređaja, ima nekoliko specifičnih prednosti i primjena u pametnim kućama. Što se prednosti tiče tu možemo

definitivno navesti da je pouzdani stabilan u komunikaciji. Budući da je veza fizički ostvarena putem kabela, nema smetnji kao kod bežičnih protokola (Wi-Fi, Zigbee, Bluetooth) koje mogu biti ometene zidovima, namještajem ili drugim uređajima. Također je imun na smetnje iz bežičnih mreža ili drugih uređaja koji emitiraju na sličnim frekvencijama, što ga čini vrlo stabilnim za rad s kritičnim uređajima poput sigurnosnih kamera ili sustava za kućnu automatizaciju. Omogućava vrlo visoku brzinu prijenosa podataka, često puno veću nego Wi-Fi ili drugi bežični protokoli, što ga čini idealnim za uređaje koji zahtijevaju velike količine podataka, kao što su pametne sigurnosne kamere, video sustavi ili kućni medijski serveri. Što se sigurnosti tiče**,** ethernet veze su inherentno sigurnije jer su fizički ograničene na žičanu vezu, što ih čini manje podložnima napadima poput presretanja ili neovlaštenog. Uz dodatne sigurnosne mjere poput firewall-ova i enkripcije, Ethernet pruža visoku razinu zaštite podataka. Ethernet uređaji obično se napajaju putem mrežnog napajanja ili putem tehnologije Power over Ethernet (PoE), koja omogućava prijenos i podataka i energije preko istog mrežnog kabela. To znači da uređaji poput pametnih kamera, senzora ili sustava za kućnu automatizaciju mogu raditi neprekidno bez potrebe za zamjenom baterija.

Što se nedostataka tiče to je sigurno fizička instalacija. Ethernet zahtijeva postavljanje kabela kroz kuću, što može biti složeno, osobito u postojećim objektima. Postavljanje dodatnih kabela za povezivanje svih pametnih uređaja može biti skupo i zahtjevno. Za nove gradnje ili renovacije, Ethernet je odličan izbor, ali u postojećim kućama Wi-Fi ili bežične mreže često su jednostavnija opcija. Uređaji koji se povezuju putem Ethernet kabela nisu mobilni i ne mogu se lako premještati, što je suprotno bežičnim uređajima koji mogu biti postavljeni bilo gdje u kući (*Patrick*, 2017).

4.2 WiFi lozinka

Prilikom postavljanja WiFi mreže i rutera ili ako nismo ažurirali zadane postavke, vrlo je važno stvoriti snažnu, jedinstvenu lozinku za našu Wi-Fi mrežu. Zadana lozinka, na primjer, ona koja je postavljena na našem ruteru ili ju je postavio davatelj usluga, može biti rizična. Treba odabrati jedinstvenu lozinku koja se ne koristi niti na jednom našem drugom uređaju ili računu te koju koristimo samo za svoju mrežu. Također, preporučeno je koristiti šifriranje WPA2 ili više (nalazi se u postavkama rutera) i omogućiti bilo koji vatrozid koji je dostupan.

Detaljnije upute proizvođača trebali bi pronaći u informacijama o proizvodu koje smo dobili s Wi-Fi ruterom kada je kupljen. Ako je potrebna pomoć u pristupu postavkama rutera, osim podataka o proizvodu, možemo i posjetiti web stranicu proizvođača. Web stranica davatelja usluga također može biti dobar izvor potrebnih informacija.

Osim toga, treba razmisliti o suradnji s pružateljem usluge ili proizvođačem rutera kako biste saznali kako ažurirati ruter s najnovijim sigurnosnim ažuriranjima.

4.3 Javne WiFi mreže

Javne tj. otvorene Wi-Fi mreže nisu sigurne zato što haker može nadzirati naš promet i tako slati virus. Sve aktivnosti na javnoj mreži su rizične, uključujući i kontroliranje uređaja pametne kuće.

Za brze naredbe, poput paljenja svjetla ili zaključavanja pametne brave, koje ne koriste puno mobilnih podataka, bolje je koristiti svoje mobilne podatke koje plaćamo pružatelju usluge umjesto javne mreže.

Za zahtjevnije zadatke i one koji zahtijevaju korištenje veće količine mobilnih podataka poput streaminga sa sigurnosnih kamera i video zvona, pronalaženje sigurne Wi-Fi mreže idealno je ako nemate neograničeno mobilnih podataka.

Ako morate koristiti nezaštićenu javnu Wi-Fi mrežu, upotrijebite virtualnu privatnu mrežu (VPN) za šifriranje svojih podataka kako ih drugi promatrači ne bi mogli pročitati. Više informacija o VPN-u na sljedećim stranicama.

4.4 Autentifikacija u dva koraka

Autentifikacijska provjera može biti višestruka ali najčešće se koristi autentifikacija u dva koraka (2FA). To dodatni je stupanj sigurnosti koji nije samo lozinka. S autentifikacijom u dva koraka, svaki put kad se netko pokuša prijaviti na naš smart home uređaj, mora pružiti dodatni dokaz identiteta.

Taj dokaz može biti u obliku jednokratnog PIN-a (OTP) ili kontrolnog koda poslanog na naš telefon ili adresu e-pošte koji potvrđuje da ste osoba koja se prijavljuje doista vi.

Većina pametnih uređaja prema zadanim postavkama ima značajku provjere autentičnosti u dva koraka, ali neki uređaji nemaju. U tom slučaju možete omogućiti 2FA s pomoću aplikacija trećih strana, poput Google autentifikatora. Čak i ako naš smart home uređaj ima višestruku autentifikaciju s pripadajućom mobilnom

aplikacijom, dodatni sloj sigurnosti putem pouzdane usluge treće strane može pružit će nam dodatni mir *(Kabir et al, 2023)*

4.5 Vatrozid

Vatrozid je mrežni sigurnosni uređaj koji prati dolazni i odlazni mrežni promet te dopušta ili blokira podatkovne pakete na temelju sigurnosnih pravila. Njegova je svrha uspostaviti barijeru između vaše interne mreže i dolaznog prometa iz vanjskih izvora kako bi se blokirao zlonamjerni promet poput virusa i hakera.

Vatrozidi pažljivo analiziraju dolazni promet na temelju unaprijed utvrđenih pravila i filtriraju promet koji dolazi iz nesigurnih ili sumnjivih izvora kako bi spriječili napade. Vatrozidi štite promet na ulaznoj točki računala, zvanoj portovi, gdje se razmjenjuju informacije s vanjskim uređajima *(Zubović, 2022).*

Na primjer, "Izvornoj adresi 182.17.2.1 dopušteno je doći do odredišta 182.17.2.1 preko porta 14." Možemo zamisliti IP adrese kao disko klubove, a brojeve portova kao ljude koji žele uči u te klubove, vatrozid bi u ovom slučaju bio izbacivač na ulazu u klub. Izbacivač ima svoja pravila koja morate ispuniti da bi ušli u klub kao što su recimo godine, garderoba i slično. Samo osobama koje zadovoljavaju pravila (izvorne adrese) je dopušteno ući u klub (odredišna adresa) - tada se to dodatno filtrira tako da ljudi unutar kluba mogu pristupiti samo određenim dijelovima kluba (odredišni portovi), ovisno o tome jesu li vip gosti, imaju li rezerviran stol ili običan gost. Vip gostu je dopušteno u bilo koju prostoriju u klubu (bilo koji port), dok je drugim gostima dopušten ulazak u određene dijelove kluba (određene portove).

Vatrozidi mogu biti softverski ili hardverski, iako je najbolje imati oboje. Softverski vatrozid je program instaliran na svakom računalu i regulira promet putem brojeva portova i aplikacija, dok je fizički vatrozid dio opreme instalirane između vaše mreže i pristupnika *(Jakolić, 2020).*

Slika 4: Hardverski vatrozid

(Izvor: https://www.digitaltrends.com/home/smart-home-defense-against-hackers/)

4.6 Virtual Private Network (VPN)

Virtual Private Network (VPN) stvara privatnu mrežu uređaja na javnom internetu. Uobičajena je namjena da se zaposlenici sigurno povežu s korporativnim internetom od kuće ili u pokretu. VPN radi tako što šifrira sve naše podatke na mreži, a zatim ih prosljeđuje kroz vanjski server kako bi ih anonimizirao prije nego što ti podaci krenu prema predviđenom odredištu.

VPN radi stvaranjem šifriranog tunela od točke do točke kako bi se podaci mogli sigurno dijeliti. Na primjer, recimo da radnik u tvrtki za osobna ulaganja odluči raditi u jednom gradskom kafiću. Dok pristupa osjetljivim podacima o svojim klijentima iz sustava svoje tvrtke, ne bi htio da ti podaci kruže, nešifrirani, na WiFi-u kafića, gdje bi ih bilo tko mogao ukrasti. Dakle, povezuje se putem VPN -a s korporativnom mrežom preko WiFi mreže kafića.

Ali i u ovome slučaju postoje situacije koje nisu 100% sigurne. Radnik će koristiti VPN za usmjeravanje šifriranog prometa s laptopa na VPN kontroler. To znači da je zaštićen samo promet poslan s tog laptopa, najčešće je to samo djelomičan promet povezan s

poslom. Zbog velikih troškova prebacivanja tog prometa natrag u kontroler, pregledavanje weba i pristup platformama za pohranu podataka poput Salesforcea, Google diska i Dropboxa nisu zaštićeni.

Čak i ako sav promet s laptopa prolazi kroz VPN, postoje određena ograničenja koja treba uzeti u obzir. Prvo, VPN neće zaštititi dolazni promet koji ide prema laptopu ili bilo kojem drugom uređaju na mreži. Također, VPN neće spriječiti razmjenu podataka između uređaja koji su spojeni na kućnu mrežu, što znači da, ako je pametni zvučnik zaražen, može napasti laptop. Pored toga, ako se na kućnoj mreži primi e-mail s namjerom krađe identiteta i otvori se, VPN neće spriječiti virus u njegovom napadu ili pristupu uslugama u oblaku.

Pri odabiru VPN davatelja usluga, važno je obratiti pažnju na nekoliko ključnih čimbenika. Kompatibilnost rutera je ključna – VPN mora biti kompatibilan s ruterom kako bi mogao zaštititi cijelu pametnu kuću. Dok većina VPN-ova danas nudi ovu mogućnost, neki još uvijek nisu kompatibilni, a neki pružaju bolje smjernice za instalaciju. Snaga i sigurnost enkripcije također su važni, jer svrha VPN-a jest zaštita podataka, pa je važno odabrati VPN s najjačom enkripcijom. Učinkovita pravila o privatnosti su ključna kako bi se osiguralo da podaci ostanu privatni i da ih davatelj VPN-a ne otkriva. Brzina veze je također bitna, jer neki VPN-ovi mogu usporiti internetsku brzinu, što može značajno utjecati na kućni Wi-Fi s više povezanih uređaja. Stoga je važno odabrati VPN s visokom brzinom veze. Na kraju, važno je provjeriti ima li davatelj VPN-a ograničenja u vezi s obradom podataka, jer neki besplatni VPN-ovi mogu imati ograničenja koja nisu pogodna za vlasnike pametnih domova. VPN zasigurno nije rješenje za sve rizike povezane sa sigurnosti sustava pametnih kuća, ali osigurava da su svi podaci koje uređaji prenose šifrirani i sigurni. Također osigurava da se svi presretnuti podaci ne mogu izravno pratiti na našu fizičku lokaciju. Korištenjem VPN-a, prijetnja koju hakeri predstavljaju IoT uređajima značajno se smanjuje i to je sjajan način za osiguravanje sigurnosti pametnog doma (*Spencer, 2024).*

Slika 5 : VPN mreža

(Izvor: https://smartnutter.com/vpn-for-smart-home-here-is-why-you-need-it/

5. POHRANA PODATAKA

5.1. Vrste pohrane podataka

Imamo dvije vrste pohrane podataka, lokalnu i pohrana u oblaku. Kao prvu obradit će se lokalna pohrana. Podaci se pohranjuju izravno na uređaj ili unutar lokalne mreže kuće, često na ili u samim uređajima koji imaju ugrađenu memoriju.

Lokalna pohrana podataka pruža nekoliko značajnih prednosti. Vlasnici kuće imaju potpunu kontrolu nad svojim podacima, što značajno povećava privatnost i sigurnost. Uređaji povezani na lokalnu mrežu mogu raditi neovisno o internetskoj vezi, jer su svi podaci pohranjeni unutar kuće, što omogućava brži pristup bez kašnjenja povezanih s prijenosom na udaljene servere. Međutim, lokalna pohrana ima i svoje nedostatke. Kapacitet za pohranu je ograničen veličinom diska ili memorije, a fizičko oštećenje, poput požara ili krađe, može dovesti do nepovratnog gubitka podataka ako se ne poduzmu odgovarajuće mjere zaštite.

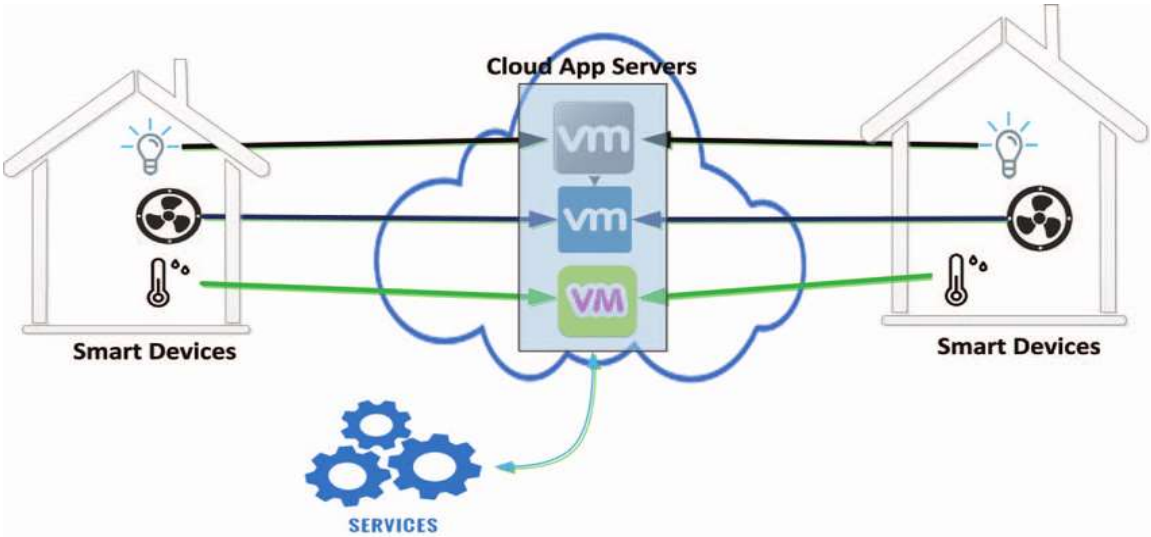
S druge strane, pohrana u oblaku nudi značajne prednosti poput praktično neograničenog prostora za pohranu podataka, ovisno o planu usluge. Korisnici mogu pristupiti svojim podacima s bilo kojeg mjesta uz internetsku vezu, a mnogi cloud sustavi pružaju automatske sigurnosne kopije podataka, što smanjuje rizik od gubitka podataka. No, pohrana u oblaku također ima svoje nedostatke. Podaci se nalaze na udaljenim serverima, što može otvoriti potencijalne sigurnosne prijetnje poput hakiranja ili neovlaštenog pristupa. Također, pristup podacima ovisi o dostupnosti internetske veze; bez nje, pristup podacima može biti onemogućen.

5.2 Sigurnost pohrane podataka

Pametna kuća pohranjuje različite vrste podataka koji doprinose njenom funkcionalnosti i sigurnosti. Podaci o korištenju bilježe sve aktivnosti unutar kuće, uključujući upotrebu svjetala, termostata, pametnih uređaja i kamera, omogućujući tako praćenje i optimizaciju svakodnevnih funkcija. Osobni podaci obuhvaćaju informacije o korisničkim profilima, preferencijama, rutinama i obrascima kretanja unutar kuće, čime se prilagođavaju funkcionalnosti kuće individualnim potrebama korisnika. Sigurnosni podaci uključuju zapisnike s nadzornih kamera, senzore pokreta i alarmne sustave koji pohranjuju snimke i detekcije pokreta, ulazaka i izlazaka, osiguravajući zaštitu i nadzor. Na kraju, podaci o povezanim uređajima pružaju informacije o statusu i funkcijama pametnih uređaja unutar mreže, uključujući razine

baterije, postavke uređaja i eventualne greške u radu, što omogućava pravovremeno održavanje i ispravke.

Naravno da se i kod pohrane podataka treba obratiti pažnju na sigurnost**.** Pohrana osobnih podataka, poput video zapisa s kamera ili podataka o navikama stanara, nosi rizik da takvi podaci mogu biti neovlašteno prikupljani, prodavani ili korišteni od strane trećih strana. Pravilno upravljanje privatnošću zahtijeva jasan pristup zaštiti podataka, uključujući enkripciju, anonimizaciju i jasne politike privatnosti od strane proizvođača pametnih uređaja. Pametne kuće mogu postati mete hakerskih napada, osobito ako sigurnosni protokoli nisu pravilno implementirani. Da bi se zaštitili važno je koristiti enkripciju podataka tijekom prijenosa i pohrane podataka, redovno ažurirati firmware uređaja te primjenjivati sigurnosne zakrpe. Potrebno je uspostaviti jasne kontrole pristupa kako bi se osiguralo da samo autorizirani korisnici mogu pristupiti osjetljivim podacima. Uvođenje dvofaktorske autentifikacije (2FA) i drugih metoda autentifikacije smanjuje rizik od neovlaštenog pristupa.



Slika 6: Spremanje podataka u oblak

(Izvor: https://www.researchgate.net/figure/Cloud-Based-Smart-Home-Architecture-for-controlling-Smart-Devices_fig1_312576520)

6. ZAKLJUČAK

Pametne kuće nisu samo vizija budućnosti, već su dio našeg modernog načina života. To će se samo povećavati kako se tehnologija bude razvijala. Svidjelo se to nama ili ne, pametne kuće ostaju ovdje i od vitalnog je značaja poduzeti potrebne korake kako bi zaštitili svoju sigurnost i privatnost dok ih koristimo. Najbolji način za to je kombinacija više načina zaštite kao što su VPN i vatrozid te snažne lozinke s dvofaktorskom autentikacijom koje sam naveo u ovome radu. Uvijek će postoji način na koji će hakeri ući u naš sistem ako to žele ali bitno je probati se što više zaštiti i ako se upad već i dogodi, pravovremeno to otkriti i reagirati.

LITERATURA

Cathy Young (2019) *Smart Home: Digital Assistants, Home Automation, and the Internet of Things,* Independently published

CIS FER (2012) *Sigurnost pametnih kuća.* Laboratorij za sustave i signale, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu. https://www.cis.hr/files/dokumenti/CIS-DOC-2012-04-045.pdf pristupljeno 19.7.2024.

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., Nicholson, J. (2023) : *Computers in Human Behavior*145 (2023) 10770

White, G., Fisch, E., Pooch, W. (1995): *Computer System and Network Security,* CRC Press

Lin, H., & Bergmann, N. (2016). *IoT privacy and security challenges for smart home environments*. Information, *7*(3), str. 44. https://doi.org/10.3390/info7030044

Jakolić, K. (2020) *Informacijski kriminalitet*. https://repozitorij.bak.hr/islandora/object/bak:91

Zubović, A. (2022) *Sigurnost informacijskih sustava*.

https://repository.pfri.uniri.hr/islandora/object/pfri:3338

Patrick, J. (2017): *Home Attitude: Everything You Need To Know To Make Your Home Smart*, CreateSpace Independent Publishing Platform

Kabir, M., Elmedany, W., & Sharif, M. S. (2023). *Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques.* Journal of Cyber Security Technology, 7(4), 199–223. https://doi.org/10.1080/23742917.2023.2228053

Athom B.V. (2024.) *What is a Smart Home Hub and when do you need one?* (n.d.). https://homey.app/en-us/wiki/smart-home-hub/ pristupljeno 1.9.2024.

Smart Light Switches: Understanding How They Work (2023). https://digitalhomesystems.com.au/how-smart-light-switches-work/ pristupljeno 23.8.2024.

Dunleavy, A. (2024) *How Smart Windows Are Changing Home Automation* https://www.windaes.co.uk/how-smart-windows-are-changing-home-automation/ pristupljeno 10.9.2024.

Pra AirConditioning (2022) *What is Smart Air Conditioning & How Does it Work?*

https://www.praairconditioning.co.uk/smart-air-conditioning/

pristupljeno 10.9.2024.

Smarthome solutions (n.d.) https://three-s.co/solutions/smarthome-solutions/ pristupljeno 20.8.2024. Pametne kuće

Protech Security (n.d.) *Mobile control and video surveillance for smart home security systems* https://protechsecurity.com/mobile-control-and-video-surveillance-for-smart-home-security-systems/ pristupljeno 17.8.2024.

Wechsler, D. (2018) *How the smart home will impact non catastrophic insurance losses* https://medium.com/@dave.wechsler/how-the-smart-home-and-the-

internet-of-things-iot-may-materially-impact-non-catastrophic-peril-66e7fdbedb21 pristupljeno 17.8.2024.

Data Doctors (2019*) Here's how to create a separate network for smart home devices. KTAR.com. https://ktar.com/story/2898083/heres-how-to-create-a-separate-network-for-smart-home-devices/* pristupljeno 17.8.2024.

Velasco, J. (2013) *Without a firewall, the door to your smart home is left wide open* (2013) https://www.digitaltrends.com/home/smart-home-defense-against-hackers/ pristupljeno 18.8.2024.

Spencer, D. (2024) *Why smart homes need a VPN: 4 reasons to get one* https://www.addictivetips.com/vpn/smart-homes-need-vpn/ pristupljeno 18.8.2024.

POPIS SLIKA: