UNIVERZITET CRNE GORE

ELEKTROTEHNIČKI FAKULTET

Amina Pirović

PRIMJENA PAMETNIH UGOVORA ZA OČUVANJE BEZBJEDNOSTI I PRIVATNOSTI U PAMETNIM KUĆAMA

MASTER RAD

Podgorica, 2024.

PODACI I INFORMACIJE O KANDITATU:

Ime i prezime: Amina Pirović

Datum i mjesto rodjenja: 10.07.1999. godine, Plav, Crna Gora

Naziv završenog osnovnog studijskog programa i godina završetka studija: Primjenjeno računarstvo, 2023. godine

INFORMACIJE O MASTER RADU:

Naziv master studija: Master studije Primijenjenog računarstva

Naslov rada: Primjena pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama

Fakultet/Akademija na kojem je rad odbranje: Elektrotehnički fakultet, Podgorica

UDK, OCJENA I ODBRANA MASTER RADA

Datum prijave master rada: 13.06.2023. godine

Datum sjednice Vijeća na kojoj je prihvaćena tema: 22.09.2023. godine

Mentor: Prof. dr Nikola Žarić

Komisija za ocjenu/odbranu rada:

1. prof. dr Milutin Radonjić, ETF Podgorica, predsjednik
2. prof. dr Nikola Žarić, ETF Podgorica, mentor
3. prof. dr Vesna Popović - Bugarin, ETF Podgorica, član

Datum odbrane: 16.02.2024

Datum promocije: _____

Ime i prezime autora: Amina Pirović, BApp

E T I Č K A I Z J A V A

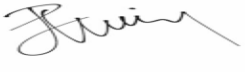
U skladu sa članom 22 Zakona o akademskom integritetu i članom 18 Pravila studiranja na master studijama, pod krivičnom i materijalnom odgovornošću, izjavljujem da je master rad pod naslovom

"Primjena pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama"

moje originalno djelo.

Podnosilac izjave,

Amina Pirović, BApp



U Podgorici, dana 12.12.2023. godine

APSTRAKT

Istraživanje o jačanju sigurnosti pametnih kuća kroz decentralizovanu arhitekturu baziranu na blockchain-u postavlja se kao odgovor na sveprisutnost pametnih tehnologija u domaćinstvima. Sa sve većim brojem povezanih uređaja i rizicima od sajber prijetnji, istraživanje se bavi ključnim pitanjima privatnosti, bezbjednosti podataka i integriteta sistema, pružajući doprinos u smislu razumjevanja i implementacije rješenja koja unaprjeđuju ove ključne aspekte svakodnevnog života. Predmet istraživanja je primjena pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama.

U tom kontekstu sprovedena je kvalitativna studija slučaja, kroz pregled relevantne literature, analizu postojećih radova stručnjaka i implementaciju sigurnih transakcija korišćenjem Ethereum pametnih ugovora. Pristup je interdisciplinaran, kombinujući elemente informacione tehnologije, sigurnosti podataka, i primjenjenog inženjeringa. Kroz opsežnu analizu i eksperimentalne implementacije, istraživači su stvorili temelj za zaključke o efikasnosti predloženih rešenja. Vršena je analiza predloženih modela, kako bi se uočile njihove prednosti i nedostaci, i ukazale mogućnosti poboljšanja.

Najvažniji rezultati ovog istraživanja ukazuju na potrebu za decentralizovanom arhitekturom u pametnim kućama, posebno koristeći blockchain tehnologiju. Ova arhitektura pruža više opcija privatnosti i bezbjednosti u poređenju s centralizovanim sistemima. Implementacija pametnih ugovora na Ethereum platformi pokazuje prednosti, ali i izazove, uključujući ograničenja u realnom vremenu i potrebu za rješenjima koja integrišu blockchain s rubnim računarstvom.

Doprinos ovog istraživanja ogleda se u činjenici da je analizom primjera utvrđeno koji su izazovi i nedostaci sa kojima se suočavaju postojeća rješenja, i šta bi trebalo unaprijediti. Sem primjene u praksi, naučni doprinos istraživanja ogleda se u činjenici da rezultati dobijeni istraživanjem mogu biti dobra polazna osnova za buduća naučna istraživanja na ovu temu. Istovremeno, istraživanje može biti polazna osnova za buduća istraživanja na slične teme, odnosno na primjenjivanje pametnih ugovora u drugim oblastima.

Ključne riječi: bezbjednost, blockchain, Ethereum, pametni ugovori, pametne kuće, privatnost

ABSTRACT

Research on strengthening smart home security through a decentralized blockchain-based architecture is being put forward as a response to the ubiquity of smart technologies in households. With the growing number of connected devices and the risks of cyber threats, the research addresses the key issues of privacy, data security and system integrity, contributing to the understanding and implementation of solutions that improve these key aspects of everyday life. The subject of research is the application of smart contracts to preserve security and privacy in smart homes.

In this context, a qualitative case study was conducted, through a review of relevant literature, analysis of existing works by experts and the implementation of secure transactions using Ethereum smart contracts. The approach is interdisciplinary, combining elements of information technology, data security, and applied engineering. Through extensive analysis and experimental implementations, researchers have created a foundation for conclusions about the effectiveness of the proposed solutions. An analysis of the proposed models was carried out, in order to identify their advantages and disadvantages, and to point out the possibilities of improvement.

The most important results of this research indicate the need for a decentralized architecture in smart homes, especially using blockchain technology. This architecture provides more privacy and security options compared to centralized systems. Implementing smart contracts on the Ethereum platform presents advantages as well as challenges, including real-time limitations and the need for solutions that integrate blockchain with edge computing.

The contribution of this research is reflected in the fact that the analysis of the examples determined the challenges and shortcomings faced by the existing solutions, and what should be improved. Apart from application in practice, the scientific contribution of the research is reflected in the fact that the results obtained from the research can be a good starting point for future scientific research on this topic. At the same time, the research can be a starting point for future research on similar topics, that is, on the application of smart contracts in other areas.

Keywords: security, blockchain, Ethereum, smart contracts, smart homes, privacy

Spisak slika:

Spisak tabela:

SADRŽAJ

1. UVOD

Pametni ugovori su programabilni računarski kodovi koji omogućavaju automatsko izvršavanje ugovora bez učešća treće strane. Pametni ugovori mogu biti korisni za očuvanje bezbjednosti i privatnosti u pametnim kućama na više načina. Oni omogućavaju automatsko izvršavanje bezbjednosnih procedura, kontrolu pristupa, upozorenja o aktivnostima, zaštitu privatnosti i nadzor nad sistemima. Primjena pametnih ugovora u pametnim kućama može doprinijeti poboljšanju bezbjednosti i privatnosti, automatskom upravljanju i smanjenju potrebe za ljudskim intervencijama, što bi omogućilo da se vlasnici kuća fokusiraju na druge stvari. Međutim, kao i uvijek, važno je da se sprovode bezbjednosne mjere i pažljivo razmatraju sve prednosti i nedostaci prije primjene pametnih ugovora u pametnim kućama.

Uz brzi napredak tehnologije automatizacije, sistemi kućne automatizacije poboljšavaju svoju tehnologiju kako bi iskoristili prednosti revolucije industrije 4.0, koja je trenutni trend u proizvodnim tehnologijama za automatizaciju i razmjenu podataka. Termin automatizacija odnosi se na niz kontrolnih sistema koji ne zahtijevaju interakciju ljudi. To podrazumijeva kontrolu i rad širokog spektra opreme, mašina i industrijskih mehanizama. On će voditi upravljanje i praćenje kućnih aparata u realnom vremenu putem Interneta spajanjem aplikacija Interneta stvari/Interneta inteligentnih uređaja (IoT). Svaki dan, IoT raste od malih mašina do ogromnih mašina koje mogu dijeliti podatke i obavljati zadatke dok su ljudi zaokupljeni drugim aktivnostima (Jenal et al., 2022).

Termin kućna automatizacija ili pametna kuća odnosi se na životni prostor koji je opremljen tehnologijom za praćenje i podršku dobrobiti svojih stanovnika. Drugim riječima, to je proces automatskog upravljanja kućnim aparatima korišćenjem raznih kontrolnih sistema. Posljednjih godina se koriste različite tehnike upravljačkog sistema za rad i nadzor električnih kućnih aparata i različitih tipova senzora kao što su svjetla, ventilatori, senzori pokreta, temperaturni senzori i drugi (Sharif et al., 2022). Prema Taivu i saradnicima (Taiwo et al., 2022), primarna funkcija pametne kuće je da ima inteligentniji nadzor i daljinsko upravljanje, tako da se svakodnevne aktivnosti automatizuju bez intervencije korisnika ili sa korisnikovim daljinskim upravljanjem na praktičniji, efikasniji, sigurniji i jeftiniji način.

Ekosistem pametne kuće IoT prolazi kroz tranziciju koju pokreće napredak informacionih i komunikacionih tehnologija. Održavanje povjerljivosti, integriteta i autentičnosti podataka je neophodno kada je u pitanju IoT. Stoga je od ključne važnosti

ispuniti bezbjednosna pitanja pametne kućne mreže. IoT se odnosi na integraciju uređaja sa internetom. Takvi uređaji se nazivaju IoT uređaji i podržavaju proširenje internetske veze izvan uobičajenih standardnih uređaja kao što su računari, laptopi, pametni telefoni, itd. Neki uobičajeni primjeri IoT uređaja uključuju:

- Pametno osvjetljenje – Pametno osvjetljenje se može koristiti za uštedu energije prilagođavanjem osvjetljenja uslovima ambijenta i uključivanjem/isključivanjem svjetla prema potrebama korisnika. Ovo može u velikoj mjeri smanjiti upotrebu energije. Ušteda energije takođe pomaže u smanjenju troškova;
- Pametno zaključavanje vrata – Krivična djela poput provale i krađe mogu se dogoditi svakome u bilo koje vrijeme. Pametne brave na vratima omogućavaju vam da zaključate svoj dom ili omogućite pristup bilo kome sa bilo kojeg mjesta pomoću aplikacije za pametne telefone;
- Detekcija dima – Ova aplikacija se može koristiti za otkrivanje okruženja pametne kuće za zdrav život. U slučaju požara može podići uzbunu obližnjoj vatrogasnoj stanici i korisniku putem e-pošte/SMS-a, obavještavajući ih o situaciji.

Sve veći broj uređaja će vjerovatno postati dio IoT-a u budućnosti, od kojih je svaki dizajniran da prikuplja, skladišti i komunicira ogromnu količinu podataka. Ovi podaci se mogu koristiti za pružanje informacija u stvarnom vremenu o zdravlju i finansijama osobe, kao i o njihovoj lokaciji, kontaktima, navikama, ponašanju i aktivnostima. Konačno, IoT uređaji pružaju okruženje u kojem se informacije o svakom pojedincu mogu čuvati, analizirati, pratiti, učiniti dostupnim i dijeliti sa drugim umreženim uređajima i eventualno drugim korisnicima.

Prednosti koje pružaju pametne kuće su brojne, ali nisu široko prihvaćene ni od strane opšte populacije niti od strane starijih ljudi. Ovo se može pripisati činjenici da su različite tehnologije, koje funkcionišu kao jezgro pružanja ovih usluga, još uvijek u fazi razvoja ili čekaju na komercijalizaciju. Drugi razlog je da se većina istraživanja o pametnim kućama fokusira na osnovne tehnologije, senzore, aktuatore i razne druge usluge koje oni mogu pružiti (Taiwo et al., 2022).

Jedan od ključnih izazova u aplikacijama za pametne kuće je osigurati bezbjednost i privatnost. Bezbjednost sistema pametnih kuća je jedan od najznačajnijih aspekata za zaštitu privatnosti potrošača pametnih kuća (Hammami et al., 2022). Komunikacija između stvarnih objekata stvara značajne izazove u pogledu povjerenja, bezbjednosti i privatnosti. Trenutno

postoje mnoge bezbjednosne prijetnje i napadi za IoT. Zbog ogromne veličine prenosa podataka, protivnici kao što su napadi čovekom u sredini (MiM) i napadi uskraćivanjem usluge (DoS) i distribuirani napadi uskraćivanjem usluge (DDoS) mogu ciljati važne prenose podataka u mreži. Zaštita ličnih podataka korisnika je primarni fokus zaštite privatnosti. To može biti ime osobe, lokacija, kretanje ili bilo koja druga informacija o pojedincu (koje osoba ne želi dijeliti s drugima). Lične fotografije, filmovi i drugi digitalni podaci skladišteni su u pametnim kućama. Kamere na pametnim uređajima mogu se aktivirati daljinski, a fotografijama i video zapisima se može pristupiti sa bilo kojeg mjesta. Osim toga, mikrofoni na raznim uređajima mogu primati privatne telefonske pozive i tekstualne poruke (Aloraini et al., 2022).

Blockchain se odnosi na distribuiranu i decentralizovanu javnu knjigu koja drži sve transakcije izvršene u peer-to-peer mreži i dijeljene među učesnicima. Mehanizam konsenzusa se koristi za verifikaciju svake transakcije u lancu. Ove decentralizovane informacije smanjuju mogućnost mijenjanja podataka (Madjid & Defvyanto, 2022).

Usvajanje osnovnih tehnologija se obično dešava u različitim fazama. Svaka faza je definisana novostima aplikacija i složenošću koordinacionih napora potrebnih da bi se one učinile izvodljivim. Blockchain aplikacije su u ranoj fazi (Zheng & Lu, 2022). Blockchain tehnologija se može smatrati jednim od glavnih pokretača za postizanje značajne uštede troškova. Stoga, uprkos trenutnoj visokoj cijeni implementacije Ethereuma za pametne kuće, vjerovatno je da će se ovaj trošak smanjiti nakon što tehnologija vremenom sazrije. U ovom istraživanju uglavnom su istraživani aspekti bezbjednosti i privatnosti protoka podataka između različitih entiteta koristeći šemu zasnovanu na blockchainu za aplikaciju pametne kuće.

U nastavku je izvršeno prikazivanje uvodnih razmatranja, kao i predmeta istraživanja, motiva i cilja istraživanja, istraživačkih pitanja, naučnih metoda korišćenih u istraživanju, doprinosa istraživanja i ograničenja istraživanja.

Predmet istraživanja

Predmet istraživanja je primjena pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama. U tom kontekstu, pametni ugovori se mogu koristiti na razne načine: za upravljanje bezbjednosnim sistemima, za obezbjeđivanje privatnosti, za kontrolu pristupa i za automatizaciju. U kontekstu bezbjednosnih sistema pametni ugovori mogu biti

programirani da upravljaju bezbjednosnim sistemima u pametnoj kući, kao što su sigurnosne kamere, senzori pokreta, senzori dima i slično. Na primjer, pametni ugovor može biti programiran da automatski uključi kamere i alarm u slučaju da senzor pokreta registruje neovlašćeni ulazak u kuću. U kontekstu privatnosti, pametni ugovori mogu biti programirani da obezbijede privatnost u pametnoj kući. Na primjer, blokirajući pristup podacima o korišćenju energije od strane trećih lica ili automatski brišući privatne podatke nakon isteka određenog vremena. U kontekstu kontrole pristupa pametni ugovori se mogu koristiti za kontrolu pristupa u pametnoj kući. Na primjer, odobravanjem pristupa samo za određene osobe u određenom vremenskom periodu. Na taj način se sprečava neovlašćeni pristup nekome ko ne bi trebalo da bude u kući.

Motiv i cilj istraživanja

IoT pametni kućni uređaji, iako pružaju prednosti korisnicima, donose i mnoge prijetnje zbog loše ili nedosljedne implementacije bezbjednosnih protokola i protokola privatnosti. IoT uređaji trenutno dostupni na tržištu se oslanjaju na klijent-server model i kanalizovanu arhitekturu sa ogromnim kapacitetima za računanje i skladištenje. Centralizovana arhitektura ima različite slabosti kao što su jedna tačka neuspjeha, centralni autoritet i ograničena transparentnost. Stoga je postojeći pristup skup zbog visokih troškova infrastrukture servera u oblaku, mrežne opreme i pratećeg održavanja. Nadalje, nijedna postojeća platforma ne podržava komunikaciju između svih pametnih kućnih uređaja niti garantuje interoperabilnost usluga koje nude različiti proizvođači u oblaku. Dakle, korišćenje standardnog peer-to-peer decentralizovanog pristupa može prevladati i smanjiti troškove koji odgovaraju održavanju i infrastrukturi klijent-server modela i podijeliti zahtjeve za obradu na pametnoj kućnoj mreži. Blockchain arhitektura može pružiti adekvatno rješenje koje odgovara potrebama za takvom platformom.

Međutim, nedostatak privatnosti korisnika kao rezultat široke adaptacije i implementacije blockchain-a ostaje glavna briga. Povjerljivost podataka se kasnije pojavila kao pitanje od primarne važnosti, jer podaci generisani u pametnoj kući sadrže osjetljiv sadržaj uključujući informacije o zdravlju korisnika i detalje o lokaciji. Glavna zabrinutost oko integriteta blockchain-a odnosi se na napade koji se odnose na privatnost korisnika, kao što su napadi na povezivanje. Takvi napadi koriste dostupne podatke snimljene u blokovima

kako bi dobili pristup privatnim informacijama povezujući informacije sa alternativnim skupovima podataka ili relevantnim pozadinskim znanjem.

Postojeća literatura o blockchain arhitekturi prvenstveno ukazuje na mogućnosti i izazove korišćenja blockchain-a uopšteno. Međutim, samo nekoliko istraživača je istraživalo aplikacije pametnih ugovora; većina trenutnih istraživanja se provodi u bitkoin okruženju, a ne u pametnim ugovorima (Vacca et al., 2021).

Nadalje, dok se blockchain smatra budućnošću skladištenja podataka zbog svoje decentralizovane strukture, još uvijek treba riješiti nekoliko problema prije nego što se implementira u scenarije svakodnevnog života. Značajan parametar u blockchain aplikacijama koji treba dalje razvijati je očuvanje podataka i privatnost transakcija. Odnosno, distribuirana priroda blockchain-a znači da identitet ili lični podaci pojedinca mogu procuriti tokom transakcija ukoliko nisu kodirani na odgovarajući način.

Prvi cilj istraživanja je analiza ključnih pojmova koji se odnose na predmet istraživanja, kako bi se bolje razumijela suština problema privatnosti i bezbjednosti u kontekstu pametnih kuća. Drugi cilj je istražiti mogućnost postizanja bezbjedne i privatne komunikacije IoT uređaja unutar pametne kuće primjenom Ethereum pametnog ugovora. Dakle rad ima za cilj razumijevanje primjene pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama.

Istraživačka pitanja

Postavljena su tri istraživačka pitanja:

- Da li korišćenje pristupa zasnovanih na blockchain-u može doprinijeti očuvanju bezbjednosti i privatnosti u pametnim kućama?

Odgovor na ovo pitanje dobiće se pregledom literature datom u drugom poglavlju o glavnim temama – pametne kuće, blockchain tehnologija, infrastruktura u oblaku i podrška za pametne kuće, bezbjednosni mehanizmi i tehnike očuvanja privatnosti zasnovane na blockchain-u, prijetnje i napadi.

- Kako se Ethereum pametni ugovori mogu koristiti za osiguranje pristupa pametnim kućnim uređajima?

Polazna pretpostavka je činjenica da su pametni ugovori sigurni i pouzdani u skladu sa činjenicom da je riječ o programabilnim ugovorima koji se izvršavaju na blockchain-u.

Samim tim, pametni ugovori se mogu koristiti za automatsko izvršavanje uslova ugovora, uključujući pristup pametnim kućnim uređajima. Odgovor na ovo istraživačko pitanje dobiće se pregledom literature i odabranog primjera u okviru trećeg dijela rada – arhitektura pametne kuće zasnovana na Ethereum-u.

- Koje se prednosti postižu korišćenjem šeme zasnovane na blockchain-u i koliko je ona efikasna protiv sajber pretnji?

Odgovor na ovo istraživačko pitanje dobiće se analizom odabranog primjera šeme kontrole pristupa zasnovane na atributima u okviru četvrtog dijela rada – implementacija bezbjednosti i privatnosti u pametnim kućama: kontrola pristupa zasnovana na atributima i pametnim ugovorima.

Naučne metode

Naučne metode istraživanja su sistematični i objektivni postupci koji se koriste u naučnom istraživanju kako bi se dobili pouzdani i valjani podaci. Svaka od naučnih metoda ima svoje prednosti i nedostatke, i stoga je u ovom radu korišćena kombinacija metoda kako bi se dobili što precizniji i pouzdaniji podaci.

Hipotetičko-deduktivna metoda primjenivana je za ciljem provjeravanja postavljenih hipoteza. Prednost ove metode ogleda se u činjenici da daje velike rezultate ukoliko su hipoteze koje će biti provjeravane međusobno povezane. Nedostatak ove metode ogleda se u izrazitoj parcijalnosti.

Metoda analize sadržaja primjenjivana je sa ciljem analize što većeg broja dostupnih pisanih tragova koji su povezani sa predmetom istraživanja. Prednost ove metode ogleda se u mogućnosti primjene dostupnih podataka o pametnim kućama, blokchain tehnologiji, infrastrukturi u oblaku i podršci za pametne kuće, bezbjednosnim mehanizmima i tehnikama očuvanja privatnosti zasnovanim na blockchain-u, kao i prijetnjama i napadima. Sa druge strane, nedostatak je mali izvor podataka koji su direktno povezani za primjenom pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama.

Metoda sinteze primjenjivana je kako bi bila obezbijeđena sistematizacija znanja u skladu sa zakonitostima formalne logike, u vidu procesa izgradnje teorijskog znanja u smjeru od posebnog ka opštem.

Metoda indukcije primjenjivana je kako bi se na osnovu analize pojedinačnih činjenica došlo do opšteg zaključka. Prednost ove metode ogleda se u mogućnosti analiziranja različitih činjenica koje se odnose na prijetnje i napade i na osnovu toga izvođenju zaključaka o mogućnosti prevencije istih. Nedostatak ove metode ogleda se u činjenici da postoji veliki broj pojedinačnih slučajeva i da je značajno odabrati prave, kako bi se izveli adekvatni zaključci.

Metoda dedukcije primjenjivana je kako bi se dobio način zaključivanja u kome su iz opštih pretpostavki izvedeni posebni i pojedinačni zaključci. Pomoću ove metode su izvedeni zaključci vezano za primjenu pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama. Nedostatak ove metode ogleda se u činjenici da u slučaju pogrešnih pretpostavki postoji mogućnost izvođenja pogrešnih zaključaka.

Metoda apstrakcije primjenjivana je prilikom odvajanja bitnih od nebitnih elemenata predmeta istraživanja. Prednost ovog metoda ogleda se u mogućnosti da budu odvojene činjenice koje su značajne za samo istraživanje od nebitnih činjenica. Nedostatak se ogleda u mogućnosti da prilikom odabira dođe do izostavljanja nekog od bitnih elemenata.

Metoda generalizacije primjenjivana je u radu tako što će od pojedinačnih zapažanja biti izvođeni uopšteni zaključci, koji su realni, uzevši u obzir činjenicu da imaju oslonac u stvarnosti. Prednost ove metode ogleda se u mogućnosti da uz pomoć pojedinačnog zapažanja, budu izvedeni zaključci o tome da li primjena pametnih ugovora može doprinijeti očuvanju bezbjednosti i privatnosti u pametnim kućama. Nedostatak se ogleda u mogućnosti da dođe do greške prilikom izvođenja zaključaka, usled pogrešnih zapažanja.

Doprinos istraživanja

Uz razumijevanje prijetnji i napada, kao i značaja očuvanja bezbjednosti i privatnosti u pametnim kućama, sproveden je veliki broj istraživanja koja su se ovom problematikom bavila. Nasuprot tome, nije sproveden veliki broj istraživanja koja su se bavila primjenom pametnih ugovora u cilju očuvanja bezbjednosti i privatnosti u pametnim kućama. Samim tim, to je predstavljao motiv i povod za sprovođenje ovog istraživanja.

Očekivani rezultati istraživanja obezbjediće uvid, ne samo u pametne kuće, blokchain tehnologiju, infrastrukturu u oblaku i podršku za pametne kuće, bezbjednosne mehanizmime i tehnike očuvanja privatnosti zasnovanim na blockchain-u, prijetnje i napade, već i u

mogućnost primjene pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama. Istraživanje prikazuje okvir bezbjednosti i privatnosti zasnovan na blockchain-u za rješavanje izazova u vezi sa IoT uređajima u sistemima pametnih kuća. Kroz rad će biti prikazano kako se blockchain tehnologija može koristiti kao knjiga kako bi korisnicima i IoT uređajima u pametnim kućama omogućila laku autentifikaciju bez oslanjanja na poznati autoritet.

Naime, biće prikazano kako se pametni ugovor može koristiti za osiguranje pristupa pametnim kućnim uređajima. U radu će prikazano generisanje tokena ERC-20 i mehanizam kontrole pristupa zasnovan na atributima koji koristi Ethereum pametne ugovore integrisane sa rubnim računarstvom (serverima) za autentifikaciju pristupa korisnika IoT pametnim kućnim uređajima. Biće prikazana primjena blockchain-a i rubnog računarstva radi postavljanja decentralizovanog sistema za poboljšanje računarskih sposobnosti prepuštanjem poslova rudarenja i skladištenja na rubne servere. U skladu sa tim, rezultati istraživanja mogu biti izuzetno korisni i primjenjivi u praksi u cilju očuvanja bezbjednosti i privatnosti u pametnim kućama.

Sem primjene u praksi, naučni doprinos istraživanja ogleda se u činjenici da rezultati dobijeni istraživanjem mogu biti dobra polazna osnova za buduća naučna istraživanja na ovu temu. Istovremeno, istraživanje može biti polazna osnova za buduća istraživanja na slične teme, odnosno na primjenjivanje pametnih ugovora u drugim oblastima.

2. PREGLED LITERATURE

Ovo poglavlje predstavlja pregled literature o glavnim temama rada, i u njemu se daje pregled pametnih kuća, blokchain tehnologije, govori o infrastrukturi u oblaku i podršci za pametne kuće, detaljno opisuju bezbjednosni mehanizmi i tehnike očuvanja privatnosti zasnovane na blockchain-u i razmatraju prijetnje i napadi.

2.1. Pametna kuća

2.1.1. Šta je pametna kuća?

Početak informacione i komunikacijske tehnologije povezan je sa pojavom Interneta. Od tada, internetske usluge razvijale su se zadivljujućom brzinom, do te mjere da su stručnjaci za tehnologiju morali stvoriti novu terminologiju koja objašnjava kako se u potpunosti mogu iskoristiti revolucionarne karakteristike ovih usluga. Ova terminologija je IoT i uključuje niz aplikacija, kao što su pametne kuće, koje zavise od Interneta (Babangida et al., 2022).

Shodno tome, ideja o obogaćivanju postojeće literature novim istraživačkim pristupima predloženim u posljednjih deset godina u vezi sa različitim obrascima podataka koji se koriste u sistemima pametnih kuća uglavnom se pripisuje eksponencijalnom rastu samih podataka, a to se samo po sebi pokazalo više od dovoljnog da izazove revolucionarnu transformaciju u odnosu na to kako su pametne kuće dizajnirane i dalje razvijene (Balasingam, Zapiee & Mohana, 2022).

Da bismo razumijeli kako pametne kuće funkcionišu, prvo treba shvatiti suštinu jedinstvene integrativne i komunikacijske mreže koju stvara pametna kuća, unutar koje se više uređaja i aplikacija može koristiti, kontrolisati i regulisati na daljinu, a da ne spominjemo mogućnost svakog uređaja da šalje i prima poruke sa drugih uređaja na tako prepoznatljiv način da pomognu stanovnicima ovih kuća da stvore personalizovano okruženje koje odgovara njihovom životnom stilu (Hammami et al., 2022).

U tom smislu, istraživači definišu pametnu kuću kao onu u kojoj komunikaciona mreža povezuje senzore, uređaje, kontrole i druge aparate koji omogućavaju daljinsko praćenje i kontrolu od strane stanara i drugih kako bi se pružile česte i redovne usluge stanarima i električnom sistemu (Nemec Zlatolas, Feher & Hölbl, 2022).

Stoga, čini se da se ključni tehnički atribut sistema pametne kuće vrti oko stvaranja centralnog kontrolnog čvorišta koje je uglavnom odgovorno za igranje uloge posredničkog elementa između nekoliko drugih uređaja i predmeta za domaćinstvo i vlasnika pametne kuće koji upravlja ovim aparatima i alatima. Ovo centralno kontrolno čvorište se zove *Home Gateway*, i koristi niz komunikacijskih protokola koji, zauzvrat, povezuju spoljnu mrežu sa kućnom mrežom (Chi & Chi, 2022).

Autori navode da pametne kuće zahtijevaju dobro programiran sigurnosni sistem koji sprečava druge da provale u kuću ili hakuju njene uređaje i koriste ih u nepoželjne svrhe (Tchagna Kouanou et al., 2022). Bezbjednost je važna, ali to ne znači da se automatski podrazumijeva. Takođe je važno imati na umu da ovi sistemi moraju biti prilagođeni korisniku, sa interfejsom koji omogućava skoro svakome da efikasno i brzo koristi svoje funkcije.

Prema mišljenju stručnjaka, pametne kuće zahtijevaju prisustvo niza elemenata, uključujući (Philip, Luu & Carte, 2023):

- glavni sistem koji uključuje komunikacione mreže, servere i radne stanice;
- interaktivni terminal koji se lako koristi za članove porodice koji im omogućava kontrolu i upravljanje svom pametnom kućnom opremom i uređajima;
- pametne utičnice koje se mogu instalirati na način koji povezuje uređaje na strujne utičnice;
- pametne uređaje, uključujući televizijske jedinice, frižidere, klima-uređaje, šporete i mašine za pranje veša koji su programirani da šalju/primaju podatke do/od glavnog sistema pametne kuće;
- bezbjednosne sisteme pametne kuće koji sprečavaju hakere i uljeze da naruše privatnost domaćinstva ili koriste njegove pametne uređaje i druge predmete bez dozvole. Ovi sistemi uključuju pametne kamere, senzore za curenje dima i gasa i tastere za hitne slučajeve.

2.1.2. Centralizovana arhitektura pametne kuće

Uopšteno govoreći, tradicionalni sistemi pametne kuće su pod kontrolom centralizovane arhitekture. Ovaj oblik arhitekture smješta sve vrste uređaja i opreme za domaćinstvo u jednu mrežu koja se kontroliše preko kućnog mrežnog prolaza, koji zauzvrat

može koristiti vlasnik pametne kuće da dođe do ovih uređaja i opreme iz jednog centralnog kontrolnog čvorišta (Budi et al., 2022).

Ovaj kućni sistem mrežnog prolaza služi kao jedini element koji omogućava svakom uređaju unutar kućne mreže da uspostavi neku vrstu komunikacije sa spoljnom mrežom. Mrežni prolazi za pametne kuće takođe su namijenjeni obavljanju specifičnih funkcija kao što su prikupljanje informacija o potrošnji energije, obrada podataka vlasnika pametne kuće, kao i precizno praćenje njegove/njene lokacije (Corno & Mannella, 2023).

Dakle, glavna ideja korišćenja centralizovane arhitekture vezana je za postojanje jednog centralnog prolaza za obradu koji je odgovoran za primanje, upravljanje, analizu i obradu podataka koje će kasnije koristiti krajnji korisnici da preduzmu akciju (Budi et al., 2022). Stoga je, ne samo daljinski pristup, već i centralizacija tog pristupa važna za razumijevanje mogućih načina na koje se mogu iskoristiti prednosti pametne tehnologije.

Sanaej (Sanaei, Haghifarm & Safdarian, 2022) sugerišu da centralizovane arhitekture zahtijevaju centralni kontroler čija je glavna funkcija prikupljanje informacija koje se odnose na uređaje i opremu za domaćinstvo za dalju obradu ovih informacija. Ovaj kontroler se smatra najvitalnijim elementom u procesu obrade, jer upravlja svim aparatima i kućnim potrepštinama, kao i podacima o pametnoj mreži s obzirom na količinu energije koju su ti uređaji i predmeti namijenjeni da potroše (Sanaei, Haghifarm & Safdarian, 2022). Upotreba ovih podataka ključna je za prednosti određenih vrsta tehnologije pametnih kuća.

Stoga je centralizovana arhitektura pametne kuće vrsta programirane kontrolne šeme koja se može instalirati u kompjuterski sistem. Koristi brojne izlaze i izvore iz kojih prikuplja različite obrasce informacija. Ovi izlazi i izvori obuhvataju korisnički interfejs, aktuatore, senzore i kontrolne proračune, što centralizovanu arhitekturu pametne kuće čini jasno različitom od tipa arhitekture poznate kao distribuirana arhitektura pametne kuće (Bhuyan et al., 2022).

2.1.3. Pitanja bezbjednosti i privatnosti u vezi sa centralizovanom arhitekturom

Centralizovana arhitektura se smatra glavnim sistemom preko kojeg rade IoT aplikacije. Međutim, naišla je na velike kritike što se tiče pitanja bezbjednosti i privatnosti, zbog svog krutog i ranjivog programiranja u koji se lako mogu infiltrirati hakeri i zlonamjerni softver, što ugrožava sve informacije skladištene u sistemu i uzrokuje da korisnici mogu

postati žrtva eksploatacije (Xihua & Goyal, 2022). Namjeravamo da razmotrimo da li su ove kritike opravdane.

Istraživači ukazuju da hakeri obično smatraju da su sistemi programirani koristeći centralizovanu arhitekturu savršeno okruženje za praktikovanje svojih podlih aktivnosti protiv korisnika pametnih kuća (Farooq et al., 2022). Do upada dolazi prvo neovlaščenim pristupom podacima kućnog mrežnog prolaza, a zatim napadaču postaje lakše da počne koristiti kućne predmete i uređaje, ili čak ukrade kritične informacije o samim korisnicima pametne kuće.

Glavni problem sa centralizovanom arhitekturom po pitanju privatnosti i bezbjednosti leži u činjenici da koristi jedno kontrolno čvorište koje usmjerava svaku pojedinu naredbu, što bi moglo omogućiti da se cijeli sistem pametne kuće sruši u bilo kojem trenutku ako se dogodi samo jedan mali kvar. Takođe, napadačima olakšava zadatak hakovanja, jer sve što treba da urade jeste da hakuju kućni mrežni prolaz da bi dobili pristup cijelom sistemu (Jin et al., 2022).

Jedan od načina upada u centralizovani sistem arhitekture pametne kuće je jednostavno korišćenje mamca prerušenog u uređaj člana unutar mreže pametne kuće, što može lako omogućiti napadaču da kontaminira kućnu mrežu mrežnog prolaza i dobije podatke koje ona sadrži, što otkriva sistem za dalje rizike privatnosti i bezbjednosti (Kumar et al., 2022).

2.1.4. Decentralizovana arhitektura pametne kuće

Decentralizovana arhitektura pametne kuće se odnosi na dizajn i organizaciju pametnih uređaja i sistema u kući tako da se odvijaju bez centralnog upravljanja ili kontrole. Umjesto toga, svaki uređaj ili podsistem ima svoju autonomiju i sposobnost donošenja odluka, uz mogućnost komunikacije i saradnje sa drugim uređajima kroz mrežu.

Ovaj pristup decentralizaciji ima nekoliko prednosti (Lee et al., 2020):

- Pouzdanost – Budući da svaki uređaj može raditi nezavisno, kvarovi ili problemi na jednom uređaju neće uticati na rad drugih dijelova sistema;
- Brzina – Brza i direktna komunikacija između uređaja može dovesti do bržeg odziva sistema;

- Skalabilnost– Dodavanje ili uklanjanje uređaja iz sistema može biti lakše jer ne zahtijeva promjenu centralnog upravljanja;
- Bezbjednost – Decentralizovani sistem može biti otporniji na pojedinačne tačke otkaza, dok je istovremeno teže napasti centralnu tačku kontrole;
- Autonomija – Uređaji mogu donositi lokalne odluke i reagovati na promjene okoline bez potrebe za stalnim upravljanjem sa centralne tačke.

Ključ za uspješnu decentralizovanu arhitekturu pametne kuće je dobra komunikacija između uređaja putem standardizovanih protokola i interfejsa kako bi se omogućila saradnja između njih. Takođe, korisnik može koristiti pametne uređaje i aplikacije za upravljanje i nadzor sistema, ali sami uređaji takođe donose odluke na osnovu programiranih pravila ili senzorskih informacija.

Decentralizovane pametne kuće su sve popularnije, jer nude veću autonomiju i prilagodljivost korisnicima i smanjuju zavisnost od centralnih serverima ili upravljanja, što može biti sigurnosni rizik i tačka otkaza u tradicionalnim centralizovanim sistemima pametnih kuća.

Decentralizovana arhitektura pametne kuće konstruisana je drugačije od centralizovane arhitekture. Kako Grunert (Grunert, 2022) ističe, sistemi decentralizovane arhitekture postaju bolja alternativa koja nudi mnogo efikasnije šeme zaštite od drugih centralizovanih sistema arhitekture pametne kuće. Decentralizovana arhitektura se takođe smatra korisnom u omogućavanju vlasnicima da uživaju u suverenitetu podataka, kao i u očuvanju povjerljivosti podataka.

Neki istraživači ukazuju da bi se decentralizovana arhitektura mogla nazvati i distribuiranom arhitekturom koja je evidentna kroz aktuelizovan sistem kontrole i adresirana i korišćena kao okvir za obradu koji se distribuira, koji dalje ugrađuje sve softverske komponente u jednu kućnu automatizovanu mrežu (Tchagna et al., 2022).

2.1.5. Pitanja bezbjednosti i privatnosti u vezi sa decentralizovanom arhitekturom

Sistemi zasnovani na decentralizovanoj arhitekturi smatraju se efikasnim rješenjem koje bi se moglo koristiti kao alternativa centralizovanim sistemima, zbog njihove snažne sposobnosti da obezbijede privatnost i bezbjednosti za korisnike sistema. Ovo daje sistemima decentralizovane arhitekture ogromnu prednost u odnosu na sisteme centralizovane

arhitekture kada je u pitanju stvaranje sigurnijeg okruženja koje održava privatnost korisnika (Far & Rad, 2022).

Liang i Ji (Liang & Ji, 2022) takođe pojašnjavaju da stručnjaci u oblasti programiranja i IoT-a uvijek imaju tendenciju da koriste sisteme decentralizovane arhitekture kao savršene arhitekture koja ima za cilj postizanje visokog nivoa privatnosti i bezbjednosti za sve korisnike u stambenim okruženjima.

Iako bi decentralizovana arhitektura pametne kuće trebala biti sigurnija i sa više zaštite i privatnosti od centralizovane arhitekture, i dalje se suočava s nekoliko problema kada se primjenjuje u većim mrežama. U tom trenutku, sistem decentralizovane arhitekture postaje izložen brojnim prijetećim rizicima vezanim za bezbjednost i privatnost. Ovi problemi se mogu navesti na sljedeći način (Harper, 2006):

- Problemi iteracije – Decentralizovana arhitektura pruža mrežnim agentima mogućnost da međusobno komuniciraju direktno bez upotrebe centralnog kontrolnog čvorišta kao posrednika. Iako bi se ovo moglo pokazati sigurnim, obavezni iterativni pokušaji komunikacije mogu predstavljati određene prijetnje, ostavljajući sistem ranjivim na frontu bezbjednosti i privatnosti;
- Problemi nedosljednosti – Sistemi zasnovani na decentralizovanoj arhitekturi su donekle nedosljedni kada je u pitanju njihov ukupni nivo performansi, što može stvoriti otvor za napadače unutar ovog nedosljednog vremenskog okvira performansi, dovodeći privatnost i bezbjednost korisnika u opasnost;
- Problemi sa distribucijom – Decentralizovani sistemi zasnovani na arhitekturi uvijek su podržani šemom distribucije koji omogućava višestrukim korisnicima da dobiju pristup skladištenim podacima, što stvara okruženje u kojem se neovlašćeni korisnici mogu infiltrirati kao administratori i ukrasti onoliko podataka koliko žele.

Stoga je važno uzeti u obzir ideju da bezbjednosne prednosti decentralizacije nisu otvoren i zatvoren slučaj.

2.2. Blockchain tehnologija

2.2.1. Blockchain pregled

Blockchain je oblik tehnologije koji se koristi za skladištenje podataka na decentralizovan način, što znači da se podaci ne čuvaju na jednom centralnom serveru, već se

distribuiraju na mnogo računara (čvorova) širom mreže. To omogućava veću sigurnost i otpornost na napade, jer hakovanje jednog čvora neće dovesti do kompromitovanja celokupnog sistema. Takođe, blockchain tehnologija često koristi kriptografiju za obezbjeđivanje nepromjenjivosti podataka. Nepromjenjivost podataka je ključna karakteristika blockchain-a. Kada se podaci jednom unesu u blockchain, teško ih je izmjeniti ili izbrisati, što doprinosi integritetu podataka. Blockchain je dobro poznat po svojoj pouzdanoj infrastrukturi baze podataka i može se koristiti u različitim poljima i kontekstima (Shrimali, Patel, 2022).

Blockchain je nastao po prvi put kao novi tehnološki pristup, tokom 1980-ih i 1990-ih, a zatim je bio svjedok revolucionarnog pomaka 2008. godine kada je priznat i primijenjen u području kriptovaluta (Padmavathi & Rajagopalan, 2023).

Blockchain se obično sastoji od niza blokova strukturiranih na uzastopni način (Vashisht et al., 2022; Padmavathi & Rajagopalan, 2023). Svaki od ovih blokova je dizajniran i programiran da sadrži osnovne podatke datog sistema i grupisan u dva dijela. Gornji dio, poznat kao *header*, uključuje heševe trenutnih i prethodnih blokova, vremenske oznake i druge relevantne informacije, dok donji dio, poznat kao *body*, sadrži glavne podatke sistema. Tehnička terminologija se može dalje opisati na sljedeći način (Thakare & Pund, 2022):

- Glavni podaci – Ovo se odnosi na bilo koji oblik podataka koji se odnosi na osnovnu uslugu koju pruža blockchain aplikacija. Ovi podaci mogu uključivati na primjer IoT ili bankovne podatke;
- Heš – Ovo se odnosi na najvažnije faktore u bilo kojem blockchain-u. Heš je funkcija koja zadovoljava šifrovane zahtjeve potrebne za rješavanje proračuna blockchain-a i razvijena na osnovu informacija prisutnih u gornjem dijelu bloka;
- Vremenska oznaka – Ovo se odnosi na to koliko je vremena potrebno da se blok generiše, tj. vremenska linija svakog bloka od pokretanja do završetka;
- Ostale informacije – Ovo se odnosi na bilo koju drugu srodnu informaciju koja ima neke veze s glavnim podacima blockchain aplikacije, kojima upravlja i koje koristi korisnik.

Sa druge strane, funkcija konsenzusa blockchain-a ukazuje na stanje kompatibilnosti među svim čvorovima povezanim s blockchain-om, što znači da je svaki čvor uređen na organizovan način jedan s drugim čvorom, osiguravajući da svi podaci koji se prenose s

jednog čvora na drugi ostanu isti, a da oblik ili forma nisu promjenjeni ili hakovani na bilo koji način (Saraji, 2023).

Blockchain-ovi se dijele na sljedeća tri tipa (Singh, Kumar & Kathuria, 2022):

- Javni blockchain-ovi – Ova vrsta blokchain-a je javno dostupna za bilo koga da vidi, preuzme, uporedi sa drugim blockchain-ovima, pa čak i konstruiše nove block-ove koji se dodaju prethodnom lancu blokova;
- Privatni blockchain-ovi – Za razliku od prvog tipa, privatni blokchain-ovi su centralizovaniji i zahtijevaju nekoliko ovlašćenih korisnika da ih kontrolišu i pregledaju. To je zato što samo mala grupa učesnika kontroliše mrežu. Svi drugi koji žele vidjeti ili uređivati blockchain trebaju zatražiti dozvolu administratora blockchin-a;
- Blochain-ovi konzorcijuma – Ovaj karakterističan tip blockchain-a je veoma favorizovan od strane izvršnih menadžera u različitim institucijama, zahvaljujući svojim jedinstvenim karakteristikama privatnosti i bezbjednosti koje omogućavaju samo onima koji rade i komuniciraju sa institucijom da vide i koriste blockchain.

Blockchain je stoga očigledno tehnologija prikladna kada je privatnost potrebna, stoga joj pridajemo veliku pažnju.

2.2.2. Blockchain tehnologija za bezbjednost i privatnost pametne kuće

Brojni vlasnici pametnih kuća nedavno su odabrali blockchain tehnologiju kao najsigurniji način za osiguranje visokog nivoa privatnosti i zaštitu svojih pametnih kućnih uređaja od manipulacije i zloupotrebe. Blockchain tehnologija omogućava vlasnicima pametnih kuća da bezbjedno pošalju svoje kritične informacije drugim institucijama kao što su banke i internetska tržišta, a da pri tom ne naruše njihovu privatnost od strane bilo koje treće strane pružaoca usluga (Vashisht et al., 2022).

U skladu sa tim, blockchain postaje sve popularniji u pametnim kućama, a na ovu temu su objavljeni brojni noviji istraživački radovi. U nastavku će biti analizirani noviji radovi o blockchain-u i pametnim kućama. Samo par radova govori o bezbjednosti i privatnosti njihovih predloženih arhitektura, pokazujući vrijednost razmatranja ovog pitanja.

Rad Lazaroiuoa i Roskia (Lazaroiu & Roscia, 2017) opisuju model pametnog okruga koji kombinuje IoT sa blockchain-om zajedno sa korisničkim pristupom električnoj mreži. Ovaj prototip modela omogućava korisnicima da interaguju sa električnom mrežom putem

blockchain-a. Korisnici sa konfiguracijom solarnih panela mogu koristiti mrežu i njene blokchain mehanizme za kupovinu i/ili prodaju energije. Ovo ilustruje kako se IoT aplikacije koje koriste blockchain mogu izvoditi i replicirati u stvarnim situacijama (Lazaroiu & Roscia, 2017).

Jedan rad opisuje dizajn energetskog lanca koji je sigurna šema za trgovanje energijom za automatizovane kuće koje koristi blockchain u ekosistemu pametne mreže. Šema pruža sveobuhvatne procjene bezbjednosti okvira u vezi sa komunikacijom, troškovima i vremenom računanja (Bhattacharya et al., 2022).

Šakarami i saradnici (Shakarami, Benson & Sandhu, 2022) su predložili sistem pametnog zaključavanja vrata baziran na blockchain-u. Sistem je uključivao obične blockchain procese u kojima tri korisnika funkcionišu kao čvor za izvođenje dokaza o radu. Tri senzora su ugrađena u sistem za detekciju kretanja i udaljenosti čvorova. Međutim, o vlasnicima pojedinačnih kuća (tj. pojedinačnih čvorova) tek treba razgovarati kao o dijelu rješenja. Pojedinačni čvorovi izazivaju zabrinutost u vezi s procesom kojim vrata zasnovana na blockchain-u verifikuju transakcije koje proizvodi jedan čvor (Shakarami, Benson & Sandhu, 2022).

Mohanti i saradnici (Mohanty et al., 2020) izvještavaju o svom dizajnu efikasnog lakog integrirsanog blockchain (ELIB) modela koji koristi javni blockchain, oblak i pametne ugovore za IoT sisteme. Njihov model je primijenjen u pametnim kućama za procjenu njenih performansi i iako je smanjio vrijeme obrade i pokazao zadovoljavajuće rezultate, korišćenje oblaka dovodi do rizika povećanja ukupne cijene sistema.

U jednom radu predlaže se rješenje pametne kuće bazirano na Ethereum-u kako bi se minimizovali problemi povjerljivosti, integriteta i autentifikacije sa IoT uređajima. Dizajn se takođe bavi problemima centralizovanog mrežnog prolaza, ali ne i dodatnim računarskim složenostima koje stvara blockchain (Lee et al., 2020).

Osim toga, predložena je sigurna i lagana arhitektura za pametne kuće zasnovana na blockchain-u. Arhitektura omogućava centralizovani nadzor lokalnog blockchain-a od strane vlasnika pametne kuće. Sva komunikacija sa lokalnim uređajem i čvorom preklapanja koristi zajednički ključ koji obezbjeđuje rudar za podršku bezbjednosti komunikacije. Autori navode da su koristili lagano heširanje kako bi otkrili transakcijske anomalije; povjerljivost podataka, integritet i dostupnost su osigurani zajedno sa mjerama zaštite od DDoS napada. Arhitektura

koristi prednosti skladištenja u oblaku kako bi izbjegla probleme sa memorijom kod pametnih kućnih uređaja (Wang et al., 2022a).

Moin i saradnici (Moin et al., 2019) naglašavaju opsežnost i teškoće vezane za upravljanje bezbjednosnim aspektima implementacije blockchain-a u IoT postavkama. Autori predlažu petoslojni najsavremeniji okvir za razvoj sigurnijih i efikasnijih IoT sistema zasnovanih na blockchain-u. Okvir uključuje osnovne IoT slojeve kao dodatak sloju za skladištenje kako bi podržao poboljšani prenos podataka u mreži sa dozvolom baziranom na blockchain-u. Oni takođe koriste oblak za skladištenje zapisa IoT senzora kao odgovor na ograničen kapacitet skladištenja senzorskih uređaja. Ovo poboljšava bezbjednosne karakteristike vezane za transakcije kao što su minimalno vrijeme kreiranja bloka, integritet, pristupačnost, dostupnost, skalabilnost i nepromjenjivost. Konkretno, blockchain se kreira u sloju za skladištenje kada se pojave varijacije bloka dok se izvode konsenzusni algoritmi i funkcije rudarenja. Dizajn modela takođe ima dovoljnu prilagodljivost da se dopadne vlasnicima pametnih kuća, preduzećima, školama i pametnim gradovima (Moin et al., 2019).

IoT kućni uređaji nemaju veliku računarsku snagu ili kapacitet skladištenja. Osim toga, mogu imati visoke troškove i visok utrošak vremena prilikom prenosa podataka. Predložena je nova lagana blockchain i hijerarhijska arhitektura zasnovana na ugovoru za poboljšanje nivoa bezbjednosti u pametnim kućama (Farooq et al., 2022). Konkretno, pametni ugovori su skripte ugrađene u privatni blockchain i aktiviraju ih IoT uređaj kada se ispune specifični uslovi.

Predstavljena je arhitektura koja podržava lokalno skladištenje distribuirane knjige od strane svakog IoT uređaja. Lokalni rudar se koristi od strane pametne kuće za obradu transakcija u privatnim i javnim blockchain-ima. Ovaj lokalni rudar takođe može skladištiti podatke na uređaju, dodati druge uređaje u privatni blockchain i umetnuti IoT uređaje sa pametnim ugovorima. Kao odgovor na ograničene računarske i skladišne mogućnosti IoT uređaja, autori su postavili vremenska ograničenja u kome lokalni rudari učitavaju privatne blockchain podatke. Autori tvrde da bi lokalni rudari privatne blockchain podatke trebali učitavati svakih deset dana i da bi samo posljednjih pet blokova trebalo održavati za naredne transakcije (Zhou et al., 2018).

Hu i saradnici (Xu, Bao & Zhu, 2020) izvještavaju o dizajnu i implementaciji sistema decentralizovanog pametnog doma zasnovanog na Ethereum-u. Kao softverska platforma, Ethereum izlazi iz blockchain tehnologije kako bi podržao programere da sastavljaju i

implementiraju decentralizovane aplikacije. Koristili su Ethereum za razvoj pametnih ugovora za skladištenje podataka senzora. Upotreba Ethereum-a za pametne ugovore omogućila je autorima da dizajniraju prototip sistema za simulaciju aplikacije za pametnu kuću. Model je dizajniran da automatski ažurira senzore vlažnosti i temperature u realnom vremenu u pametnim kućama kada ih pokreću određeni događaji, demonstrirajući prednosti koje podupiru ono što želimo učiniti (Xu, Bao & Zhu, 2020). Autori, međutim, ne pominju da je njihov sistem skup za vođenje i da neki elementi dizajna zahtijevaju dalja poboljšanja.

Sajngh i saradnici (Singh et al., 2019) izvještavaju kako su spojili blockchain konzorcijum sa računarstvom u oblaku u arhitekturi svog sistema kako bi poboljšali povjerljivost podataka, integritet, skalabilnost i pristupačnost, a time i sigurnost i bezbjednost pametne kuće. Njihov sistem pokazuje kako pametne kućne mreže zasnovane na blockchain-u mogu upravljati transakcijama koristeći računarstvo u zelenom oblaku. Zeleni broker se koristi za smanjenje spoljnih uticaja na okolinu (Singh et al., 2019).

Konačno, Aung i Tantidham (Aung & Tantidham, 2018) su prijavili uticaj Ethereum-a na sistem pametne kuće i razvijenu arhitekturu pametne kuće uključujući privatni blockchain, pametni kućni rudar, senzore povezane s lokalnim skladištenjem i aktuatorske uređaje. Njihova arhitektura je modifikovani oblik dizajna koji su razvili Dori i saradnici 2017. godine, ali sa dodatim Ethereum aplikacijama i pametnim ugovorima. Sistem može generisati politike za rukovanje transakcijama koje uključuju navođenje pojedinaca ovlašćenih za pristup i praćenje podataka. Ovi autori dalje tvrde da blockchain baziran na Ethereum-u može biti manje efikasan u vremenski osjetljivim situacijama s obzirom na to da mu je potrebno oko 20 sekundi da se završi transakcija, što je predugo za situacije u kojima je potreban hitan odgovor (Aung & Tantidham, 2017).

Rad Alzoubija (Alzoubi, 2022) predstavlja novu paradigmu u kojoj su mobilni agenti, uključujući podatke koji se automatski i autonomno migriraju između dva različita kućna uređaja, zaštićeni i održavani u bezbjednoj seriji hešova unutar arhitekture ojačane blockchain tehnologijom, koja štiti sistem pametne kuće od mogućih prijetnji i napada (Alzoubi, 2022). Paradigma se pokazala uspješnom i lako se primjenjuje u drugim obrascima IoT sistema.

Sa druge strane, postoji izvještaj o razvoju nove šeme poznate kao privatna bezbjedna kontrola pristupa zasnovana na blockchain-u kao savršeno siguran sistem za kontrolu kućnih predmeta i uređaja u sistemima pametnih kuća (Xue, Xu & Zhang, 2018). Šema služi kao štit

koji blokira i unutrašnje i spoljne napade i prijetnje. Funkcioniše na jedinstven, ali jednostavan način, budući da blockchain tehnologija privatno skladišti pristupne zapise dok minimizira komunikacione i računske troškove

2.2.3. Izazovi integracije blockchain tehnologije u sisteme pametne kuće

Blockchain tehnologija je korišćena kao osnovno rješenje za osiguranje bezbjednosti i održavanje privatnosti podataka za svoje korisnike. Međutim, ne može se previdjeti nekoliko kritičnih pitanja koja dovode do sljedećih izazova u vezi sa korišćenjem blockchain tehnologije u IoT aplikacijama (Liang & Ji, 2022):

- rudarenje podataka zahtijeva intenzivnu količinu računarske snage;
- IoT uređaji uključuju resurse koji su jako ograničeni;
- rudarenje blokova traje dugo;
- slaba skalabilnost, a time i slaba sposobnost da se nosi sa sve većim brojem čvorova u mreži;
- tendencija stvaranja zapanjujuće količine saobraćaja zbog osnovnih protokola koji se odnose na blockchain tehnologiju.

Drugi autori su takođe identifikovali sljedeće izazove s kojima se suočava blockchain tehnologija (Shakarami, Benson & Sandhu, 2022):

- Skladištenje – Podaci imaju tendenciju da zauzimaju veliku količinu prostora zbog sve većeg broja čvorova tokom vremena, što dovodi do povećanja veličine knjige;
- Skalabilnost – Skaliranje bi na kraju moglo promijeniti osnovnu karakteristiku blockchain-a, pomjerajući njegov pristup u centralizovaniji stil kontrole;
- Loše operativne vještine – Nažalost, samo relativno mali broj ljudi je stvarno opremljeno i kvalifikovano za vješto korišćenje aplikacija blockchain tehnologije;
- Dugotrajnost – Iako blockchain tehnologija pruža veliku bezbjednost i privatnost, njen proces enkripcije može potrajati mnogo vremena.

Kada su u pitanju pametni kućni sistemi, istraživači ukazuju da blockchain tehnologija nije savršena i da bi zapravo mogla dovesti do sljedećih prepreka za korisnike (Vashisht et al., 2022):

- Potrebna je ogromna računarska snaga kako bi se uspostavio konsenzus između svih čvorova unutar njihovih blokova u integrativnoj mreži tako da se određene zlonamjerne prijetnje protiv pametnih kućnih jedinica mogu otkriti i spriječiti;
- Prelivanje protoka podataka od čvora do čvora i bloka do bloka može lako uzrokovati neke probleme i zaustaviti cijeli proces komunikacije, a za ove podatke je potrebna uravnotežena računska šema koja koristi veliku procesorsku snagu i munjevitu brzinu, što nije uvijek slučaj sa svakom aplikacijom blockchain tehnologije;
- Unutar kućnih mreža, kad god se broj čvorova poveća, skalabilnost blockchain-a primjetno opada, što utiče na efikasnost prenosa podataka i njihovo čuvanje privatnim;
- Iako se blockchain sistemi pokazuju da su sigurni i decentralizovani, količina komunikacije i saradnje između kućne opreme i uređaja može dovesti do curenja podataka, što sisteme pametnih kuća čini ranjivijim na sajber napade i prijetnje.

2.3. Infrastruktura u oblaku i podrška za pametne kuće

2.3.1. Pregled računarstva u oblaku

Autori pokazuju da računarstvo u oblaku nudi korisnicima metodologije obrade koje se odlikuju i fleksibilnošću i praktičnošću, što omogućava dijeljenje i spoljne usluge različitih količina podataka povezanih s određenim kontekstima (Jamsa, 2022). Godla i saradnici (Godla, Fikadu & Adema, 2022) su istakli da računarstvo u oblaku uključuje bitan broj komponenti koje obuhvataju sljedeća tri faktora:

- Klijenti – Prva komponenta predstavlja alat krajnjih korisnika koji im omogućava da upravljaju mnoštvom informacijskih paketa koji se drže u oblaku. Ovi alati mogu biti bilo koji tip računarskog uređaja kao što su mobilni telefoni, laptopovi ili desktop računari;
- Distribuirani serveri – Druga komponenta predstavlja servere koji su odgovorni za pružanje visokokvalitetnih usluga bezbjednosti i pristupačnosti, kojima se upravlja sa različitih geografskih lokacija;
- Centar podataka – Treća komponenta predstavlja servere preko kojih se mogu dobiti informacije korišćenjem procesa virtuelizacije fizičkih servera za virtuelno hostovanje servisa.

Ponuđeno je pojednostavljenje koncepta računarstva u oblaku, objašnjavajući pristup koji integriše brojne resurse i stavlja ih u virtuelizovanu platformu na mreži, koja korisnicima Interneta omogućava pristup široko artikulisanoj biblioteci informacija o svim poljima istraživanja, bez ograničenja bilo kakvim prostornim ili vremenskim faktorima ili upotrebom čvrstih diskova koji koštaju korisnika ili operatera ogromnu svotu novca i zahtjevaju periodično održavanje, što se pokazuje kao zamoran proces (Sriram, 2022).

2.3.2. Integracija blockchain tehnologije sa računarstvom u oblaku

Efikasni dobici koji se mogu postići integracijom blockchain tehnologije sa računarstvom u oblaku potvrđeni su u literaturi, jer ovaj nivo integracije može lako poboljšati ukupne performanse računara, izbjeći sve izazove vezane za curenje podataka, povećati procesorsku snagu operativnih blokova jer prenosi eksponencijalno rastuću količinu protoka podataka od čvora do čvora (Alzoubi, Al-Ahmad, & Kahtan, 2022).

Kako ističu istraživači, kada se računarstvo u oblaku spoji sa blockchain tehnologijom, poboljšava se sposobnost zaštite sistema i podataka koje sadrži od različitih prijetnji, budući da je manipulaciju podacima mnogo teže obraditi kada se podaci skladište u više blokova i čuvaju na različitim mjestima i različitim lokacijama (Gong & Navimipour, 2022). Taranum i Abidin (Tarannum & Abidin, 2023) ističu da se zajedničko korišćenje blockchain tehnologije i računarstva u oblaku smatra inherentno korisnim u brojnim profesionalnim i akademskim kontekstima, uključujući zdravstveni sektor, obrazovni sektor kao što je e-učenje i logistiku.

Ngujen i saradnici (Nquyen et al., 2020) su sproveli studiju koja ukazuje na to koliko je sigurno i efikasno integrisati aplikacije blockchain tehnologije sa računarstvom u oblaku. Studija uvodi novo dostignuće u kontekstu blockchain tehnologije, računarstva u oblaku i IoT-a pod nazivom blockchain cloud internet-of-things (BCoT). Ova nova tehnologija omogućava bezbjedno i konzistentno dijeljenje i prenos podataka na IoT-u u oblaku za mnoge aplikacije koje funkcionišu u nizu usluga kao što je zdravstveni sistem (Nquyen et al., 2020.).

Pored gore navedenih studija, studija koju su sproveli Habib i saradnici (Habib et al., 2022) naglašava značaj korišćenja računarstva u oblaku kao skele za aplikacije blockchain tehnologije, posebno u postavkama pametnih kuća, a to se pripisuje tome što računarstvo u

oblaku omogućava korisnicima da dođu i koriste podatke iz oblaka na mreži, koji održava stabilan protok podataka i poboljšava skalabilnost blockchain-a i ukupnu snagu obrade.

2.4. Bezbjednosni mehanizmi zasnovani na blockchain-u

2.4.1. CIA trijada

CIA (*Confidentiality, Integrity, Availability*) triada je skraćenica koja označava tri ključna principa informacione sigurnosti. Pun naziv je Confidentiality, Integrity, Availability, što bi se moglo prevesti kao povjerljivost, integritet, dostupnost. Ovi principi čine osnovu za razumijevanje i implementaciju zaštite informacija i sistema, kako u informatičkoj sigurnosti tako i u drugim kontekstima gdje je sigurnost informacija važna. Kako bi se stekao bolji uvid u interakcije CIA trijade, sva tri principa su dalje i odvojeno razrađena na sljedeći način (Hiza, 2022):

- Povjerljivost – Princip povjerljivosti uključuje čuvanje podataka korisnika, uključujući njihove profesije, identitete i druge povezane informacije. Ovo se dešava i kroz uspostavljanje ograničenja i šifrovanje podataka koji se odnose na kritične detalje njihovih života i finansijskih transakcija;
- Integritet – Princip integriteta koristi karakterističnu bezbjednosnu mjeru koja uključuje bezbjednosni parametar preko kojeg se može otkriti nivo tačnosti informacija, čime se daje autorizacija na osnovu toga koliko su te informacije tačne. Ovo takođe pomaže u održavanju konzistentnosti podataka i nudi korisniku, i nikome drugom, mogućnost da u potpunosti kontroliše i reguliše svoje informacije;
- Dostupnost – Na princip dostupnosti se redovno gleda kao na mač sa dve oštrice. U svojoj srži, pruža mogućnost pristupa svim vrstama informacija kako korisnik smatra prikladnim. Međutim, ovo često dolazi sa visokom cijenom za plaćanje, jer se od bezbjednosnih stručnjaka traži da dodaju više ograničenja, ojačaju mrežu i ponude više opcija privatnosti za korisnike kako bi pravilno i sigurno osigurali informacije kojima se pristupa.

I organizacije i pojedinci koji obavljaju svoje profesionalne i dnevne zadatke na mreži dijele i primaju ogromnu količinu podataka koji potiču iz različitih izvora i koji se skladište ili na diskove u oblaku ili na tradicionalne diskove. Imajući ovo na umu, istraživači su tvrdili da se skup bezbjednosnih principa mora objaviti kako bi se zaštitila privatnost korisnika podataka i održalo optimalno bezbjedno okruženje na mreži (Samuel et al., 2022). Jedan od

najefikasnijih modela koji se koristi za osiguranje bezbjednosti i privatnosti za korisnike je CIA trijada, koja uključuje principe povjerljivosti, integriteta i dostupnosti.

Ukoliko se prekrši bilo koji od ova tri principa, informacije korisnika postaju izložene velikoj opasnosti. Međutim, intenzitet ove opasnosti može biti (Hiza, 2022):

- niska i ograničena, sa malim ili bez efekta;
- srednja, sa primjetnim kritičnim oštećenjima;
- visoka, što izaziva opasan uticaj za korisnike sa teškim štetnim dejstvom.

Stoga, blockchain tehnologija treba tražiti potpunu upotrebu CIA trijade kako bi integrisala svoje principe povjerljivosti, integriteta i dostupnosti u svoje aplikacije, što zauzvrat može omogućiti pristup raznim mjerama privatnosti i bezbjednosti, kao što su šifrovanje, transparentnost, otpornost i revizija (Septiani et al., 2022).

2.4.2. Kontrola pristupa

U kontekstu IoT sistema, kontrola pristupa se pokazala kao jedan od najefikasnijih modaliteta za osiguranje bezbjednosti i privatnosti korisnika. Ovi korisnici uključuju pojedince, institucije i poslovne organizacije (Ragothaman et al., 2023). Kontrola pristupa se svodi na kontrolnu tačku koja ili odbija ili dozvoljava korisnicima pristup određenom korpusu informacija. Sa druge strane, blockchain tehnologija može lako koristiti kontrolu pristupa kako bi pomogla u uspostavljanju sistema koji je više decentralizovan i nudi arhitekturu koja je u stanju da prevaziđe kvarove u jednoj tački (Namane & Ben Dhaou, 2022).

Kontrola pristupa obuhvata tri glavna tipa poznata kao:

- Kontrola pristupa zasnovana na povjerenju – se u osnovi oslanja na različite faktore ili parametre povjerenja kako bi procijenio nivo povjerenja koje korisnici imaju. Ovaj pristup mjeri koliko korisnici vjeruju sistemu, uzimajući u obzir ograničenja u vezi sa dostupnim podacima i vrstom informacija koja može biti ili otkrivena ili zaključana za njih. Drugim rječima, sistem koristi različite faktore kako bi odredio koliko korisnicima može biti dozvoljeno pristupiti određenim podacima ili funkcionalnostima, uzimajući u obzir nivo povjerenja koji im se pridaje (Salji et al., 2022);

- Kontrola pristupa zasnovana na ulozi – sa okvirom za kontrolu pristupa koji nudi mehanizam koji omogućava organizacijama da komuniciraju različite nizove podataka na osnovu uloge svakog korisnika unutar svake organizacije, i iako se ne koristi u kompjuterskim mrežama, kontrola pristupa zasnovana na ulozi se i dalje koristi u mrežama direktnih komunikacija (Alrahili, 2022);
- Kontrola pristupa zasnovana na koaliciji – je metoda kontrole pristupa koja prisiljava korisnike koji žele da dobiju pristup određenim skupovima podataka da prvo posjeduju neku vrstu autoriteta akreditiva kao način poboljšanja mjera privatnosti i bezbjednosti (Ardagna et al., 2010). Kontrola pristupa zasnovana na koaliciji dalje je podijeljena na dva tipa, kontrolu pristupa zasnovanu na atributima i kontrolu pristupa zasnovanu na mogućnostima:
  - Kontrola pristupa zasnovana na atributima – istraživači su zaključili da je kontrola pristupa zasnovana na atributima – *ABAC (Attribute-Based Access Control*) efikasno rješenje koje pomaže u ublažavanju problema uzrokovanih drugim tradicionalnim okvirima kontrole pristupa, zbog svoje jedinstvene arhitekture koja omogućava korisnicima da dobiju pristup skupovima podataka skladištenim u sistemu na osnovu njihovih atributa, a ne njihove uloge ili bezbjednosne oznake koje su im dali administratori sistema (Shammar, Zahary, & Al-Shargabi, 2023). Ovo je očigledno korisno u stvaranju autonomnog sistema koji ne zahtjeva nikakav oblik administratorske intervencije;
  - Kontrola pristupa zasnovana na mogućnostima – je još jedan okvir kontrole pristupa, koji omogućava korisnicima da dobiju pristup različitim skupovima podataka u zavisnosti od potpisa ključnih figura i faktora zaduženih za rad i uticaj na sistem, kao što su vlasnik autorskih prava, pružaoci usluga, i pristupni periodi. To bi se lako moglo postići generisanjem i zatim provjerom tokena kako bi se pomoglo korisnicima da dobiju pristup podacima (Deepthi & Khandwekar, 2023).

2.5. Tehnike očuvanja privatnosti zasnovane na blockchain-u

2.5.1. Tehnike očuvanja privatnosti

Aplikacije blockchain tehnologije suočavaju se sa nekoliko izazova u pogledu očuvanja privatnosti korisnika zbog mogućeg curenja podataka do kojeg može doći kada se

broj čvorova u bloku progresivno povećava. Stoga se neke od sljedećih tehnika za očuvanje privatnosti mogu implementirati u blockchain tehnologiju kako bi se ublažio ozbiljan uticaj ovih incidenata. Istraživači su naveli sljedeće glavne vrste tehnika očuvanja privatnosti (Ejaz et al., 2019; Hassan, Rehmani, Chen, 2019):

- Šifrovanje – Ova strategija je uobičajena u blockchain mrežama za osiguranje transakcija i prenosa podataka. Svakom korisniku u blockchain mreži dodijeljena su dva ključa: javni ključ za korišćenje sa drugim blockchain korisnicima i prenos poruka do određenog čvora i privatni ključ za dešifrovanje poruka samo za čitanje. Pristup šifrovanja/dešifrovanja štiti poruke i održava privatnost blockchain transakcija. Funkcije za očuvanje privatnosti zasnovane na enkripciji, međutim, povećavaju zahtjeve za računanjem i komunikacijom na IoT mreži (Ejaz et al., 2019). Na primjer, čvorovi podržani enkripcijom i dešifrovanjem imaju visoke računarske troškove za proizvodnju i isporuku ključeva, što značajno povećava zahtjeve za računanjem. Nadalje, strategije šifrovanja mogu imati propuste u svojim matematičkim formulama, što rezultira kompromitovanim kapacitetom za isporuku potpune privatnosti podataka (Chen, 2019);
- Anonimizacija – Ovu strategiju za očuvanje privatnosti sistema IoT-a primijenili su istraživači u IoT aplikacijama zasnovanim na blockchain-u, kao što su elektronski zdravstveni kartoni, finansijske platforme, mreže vozila i energetski sistemi. Istraživači su predložili povećanje strategija anonimizacije uključujući anonimnost, blizinu i raznolikost (Chen, 2019). Iako anonimizacija pruža snažne garancije privatnosti većini IoT sistema baziranih na blockchain-u, oni su skloni kompromisima, kao što su napadi na povezivanje, gdje se podaci iz spoljnih izvora kombinuju sa zaštićenim anonimizovanim podacima za pristup privatnim podacima korisnika IoT-a (Ejaz et al., 2019). Dodatno, anonimizacija može ograničiti obim do kojeg se može pristupiti detaljima zapisa, ostavljajući analitičaru/primaocu nemogućnost da pristupi potencijalno potrebnim detaljima iz anonimnog skupa podataka;
- Miješanje – Protokoli za miješanje coin-a podržavaju anonimnost korisnika prilikom uključivanja u finansijske transakcije koristeći IoT sisteme zasnovane na blockchain-u. Tradicionalne metode miješanja nisu u potpunosti decentralizovane, što znači da je za prenos transakcija često potreban pouzdani server treće strane. Ove usluge uglavnom preuzimaju transakcije od nekoliko korisnika i miješaju ih kako bi zaštitile

identitet transakcije od protivnika. U transakcijama miješanja, svaki korisnik blockchain-a u IoT sistemu prenosi šifrovanu novu adresu trećem licu (mikseru) koja se zatim dešifruje i miješa između ostalih adresa prije nego što se vrati u čvorove predajnika (Ejaz et al., 2019). Trenutne strategije miješanja, međutim, ne koriste treće strane za miješanje. Istraživači su razvili *coin-shaffle* i *mix-coin* protokole za zaštitu privatnosti korisnika tokom finansijskih IoT blockchain transakcija. Kombinovani pristupi dobro funkcionišu u finansijskim transakcijama, ali nivo anonimnosti ostaje nizak i može biti ugrožen zbog njihove ranjivosti na presretanje i sajber napade (Chen, 2019). Nadalje, potpuna privatnost se ne može osigurati korišćenjem pristupa miješanja jer se transakcija može pratiti analizom transakcionih grafova;

- Diferencijalna privatnost – Diferencijalna privatnost je tehnika očuvanja privatnosti koja se koristi za osiguranje informacija i ličnih podataka učesnika kada su ove osjetljive informacije uključene u statistički skup podataka, što zauzvrat omogućava operaterima i analitičarima da pregledaju sve informacije potrebne za njihov rad bez otkrivanja ličnih podataka učesnika. Diferencijalna privatnost je učvrstila svoj značaj kao jedna od najpoznatijih tehnika očuvanja privatnosti koja garantuje da će lični podaci korisnika i učesnika biti osigurani i zaštićeni od kršenja pravila privatnosti ili krađe. To se događa u okruženju u kojem se specifični relevantni podaci mogu statistički analizirati u svrhu istraživanja, a da se pritom ne moraju ugroziti osjetljivi podaci korisnika (Ejaz et al., 2019). Istraživači definišu diferencijalnu privatnost kao precizno matematičko ograničenje koje ima za cilj da osigura privatnost pojedinačnih informacija u bazi podataka čak i dok se odgovara na upite o agregatu. Ovo ukazuje na to da diferencijalna privatnost nije ništa drugo nego metoda za određene analitičare koji koriste skupove podataka samo da pregledaju i uređuju podatke koji odgovaraju njihovom istraživanju, bez da dođu do ličnih podataka učesnika, dodavanjem šuma tim skupovima podataka. Ovaj šum je napravljen od nasumičnih fragmenata podataka kako bi se stvorile lažne informacije koje nemaju nikakvog značenja ili veze s originalnim skupom podataka, čime se štite vitalne i lične informacije korisnika. Razlog zašto je diferencijalna privatnost najprikladnija tehnika za aplikacije blockchain tehnologije je taj što otkriva samo informacije koje se koriste da pomognu stručnjacima i korisnicima da izvrše određene zadatke, bez ugrožavanja bilo koje njihove kritične informacije ili potkopavanja privatnosti njihovih mreža. Ovo omogućava aplikacijama i sistemima blockchain tehnologije da funkcionišu na efikasniji način i eliminiše negativan uticaj problema privatnosti koji bi mogli biti

povezani sa ovim aplikacijama (Chen, 2019). Dinamičnost diferencijalne privatnosti znači da je pogodna za upotrebu u blokchain scenarijima. Na primjer, tehnike diferencijalne privatnosti perturbacije podataka u tački mogu unijeti šum u podatke bez narušavanja nivoa tačnosti u realnom vremenu i emitovati ih koristeći blockchain aplikacije. Mehanizmi koji se koriste u perturbaciji podataka u tačkama prvo izračunavaju stope greške, a zatim izračunavaju vrijednost šuma na osnovu stope greške. Šum se zatim dodaje na osnovu izračunate vrijednosti kako bi se podržala zaštita privatnosti. Zabilježena vrijednost šuma je različito privatna, tako da potencijalni protivnici posmatrači ne mogu precizno odrediti stvarnu vrijednost ili postojanje/odsustvo korisnika u decentralizovanoj bazi podataka (Huang et al., 2022). Prije analize statistike iz blockchain baza podataka od strane treće strane, moguće je osigurati zaštitu korisnika primjenom diferencijalne privatnosti. Konkretno, diferencijalna privatnost čini aspekte statističkih podataka blockchain-a nerazlučivim. Kao rezultat toga, analitičar nije u mogućnosti da sa sigurnošću predvidi dostupnost određenih blokchain čvorova u skupu podataka. Diferencijalna privatnost stoga može pružiti kontrolu privatnosti za važne podatke, što znači da njena primjena u blockchain-ima može pružiti mnogo pozitivnih rezultata privatnosti. Stoga nije iznenađujuće da je blockchain s različitom privatnošću naširoko istražen u nekoliko polja uključujući zdravstvo (de Moraes Rossetto, Sega & Leithardt, 2022; El Azzaoui et al., 2022), računarstvo u oblaku (Morawiec & Sołtysik-Piorunkiewicz, 2022), i pametne mreže (William et al., 2022).

2.6. Prijetnje i napadi

2.6.1 Napad uskraćivanja usluge (DoS) napad

DoS je jedan od najpoznatijih oblika napada u sajber carstvu. Jednostavno je baziran oko ideje promjene normalnih karakteristika određenog skupa funkcija koje izvršavaju korisnici sistema, čineći ih nedostupnima i potpuno neispravnim, tako da korisnik više nije u mogućnosti koristiti usluge ili funkcije ovog sistema (Jazzar & Hamad, 2022).

Napadači koji se oslanjaju na DoS napade kao svoje oružje po izboru uvijek izgledaju kao da slijede određenu i organizovanu putanju, koja uključuje slanje vještački i zlonamjerno kreiranih lažnih poruka na server, što uzrokuje zaustavljanje cijelog sistema i prekida bilo kakav oblik komunikacije između servera i korisnika (Aziz, Abdulqadder & Jawad, 2022).

2.6.2. Napadi modikacije

Napadi modifikacije funkcionišu kroz specifičnu tehniku u kojoj napadač teži da izmijeni, doda ili eliminiše podatke u skupu podataka žrtve. Podaci se takođe mogu miješati, proces koji se zove manipulisanje. Ovaj napad takođe uključuje još jednu često korišćenu tehniku koja uključuje ubacivanje lažnih i netačnih podataka, u procesu poznatom kao *fuzzing*, koji omogućava napadaču da slobodno krivotvori informacije dok je cijelo vrijeme ispod radara detekcije. Napadači to obično rade tako što prikrivaju mašinski program da luta u skupu podataka (Tian & Nogale, 2023). Autori takođe ističu da je glavni cilj svakog modifikacionog napada da se iskoristi prednost bilo kog oblika komunikacije koji se odvija između napadača i žrtve, da se dobije privilegija da se mjenjaju paketi podataka (Soni & Singh, 2022).

2.6.3. Napad povezivanja

Napadi povezivanja su prilično jedinstveni po tome što ne zahtjevaju nikakve vještine programiranja ili složenog kodiranja. Sve što napadač treba da uradi da bi izvršio ovaj napad je da prikupi fragmente podataka koji se odnose na anonimnog korisnika kako bi ih povezao u jedno tijelo informacija, koje više ne drži korisnika anonimnim. To je jednostavno pitanje traženja podataka i povezivanja svih zajedno (Nomoto et al., 2022).

Shodno tome, ovo se odnosi na podatke koji se obično objavljuju na internetu za javnost. Međutim, isti podaci mogu biti razbacani po cijelom internetu ili u različitim skupovima podataka. Stoga će napadačima trebati znatan napor da povežu ove podatke kako bi na kraju mogli stvoriti jedinstvenu sliku osjetljivih informacija o korisnicima (Civitarese, 2023).

2.6.4. Napadi zaključivanja

Svrha pokretanja napada zaključivanjem je prikupljanje korisnih informacija o korisnicima sistema. Ove informacije obično ne otkrivaju sami korisnici. Međutim, oni mogu dodati fragmente svojih ličnih podataka u različite sisteme. Na primjer, napad zaključivanjem uključuje dobijanje podataka o korisnikovim aktivnostima koje se odnose na njegovu/njenu dnevnu rutinu i navike. Ovi podaci, iako na prvi pogled djeluju nevažno, mogu biti od izuzetne koristi za napadača, jer omogućavaju otkrivanje drugih važnih detalja, kao što su

informacije o sobnoj temperaturi koje bi mogle biti hakovane i promjenjene (Yi et al., 2022). Klimatizaciju razmatramo u kontekstu pametne kuće, stoga je evidentno da je snimanje podataka o temperaturi relevantno. Tačan status kuće i preferencije stanara omogućavaju napadaču da izvuče zaključke o njihovoj prisutnosti.

Stoga su istraživači ukazali da se napadi zaključivanjem uglavnom zasnivaju na praksi i tehnikama rudarenja podataka, tako da napadač može dobiti i u potpunosti otkriti vrijedne informacije o žrtvi, koristeći bitove i dijelove drugih trivijalnih informacija koje se inače ne bi pokazale monumentalno kritičnim za korisnika (Xiao et al., 2022).

3. ARHITEKTURA PAMETNE KUĆE ZASNOVANA NA ETHEREUM-U

U modernom svijetu, IoT uređaji kao što su senzori igraju ključnu ulogu u prikupljanju privatnih ličnih i organizacionih podataka, što može postaviti izazove u vezi sa privatnošću, bezbjednošću i etikom (Karale, 2021). Da bi se prevazišli potencijalni problemi, potrebni su dobro definisani i fleksibilni mehanizmi zaštite. Mnogi pristupi bezbjednosti i privatnosti su ispitani u IoT okruženju, ali obično su neprimjenjivi i mogu predstavljati ograničenja zbog prirode decentralizovane topologije i ograničenja resursa uobičajenih uređaja (Dorri et al., 2017a). Stoga je jedno od predloženih rješenja za očuvanje bezbjednosti i privatnosti u IoT okruženju korišćenje pristupa zasnovanih na blockchain-u, koji bi mogli pružiti decentralizovane, sigurne ravnopravne mreže. Blockchain omogućava članovima da komuniciraju jedni sa drugima bez pouzdane posredničke strane i bez potrebe da jedan drugome daju pristup pisanju. Integracija pristupa zasnovanih na blockchainu sa IoT uređajima može proizvesti distribuiranu i pouzdanu kontrolu pristupa za IoT (Geneiatakis et al., 2017).

Dolaskom četvrte industrijske revolucije i razvojem tehnologije mreže uređaja, u pametnim kućama se povećava nadzor i kontrola različitih uređaja. Preneseni podaci mogu sadržati lične osjetljive informacije kada uređaj komunicira putem pametne kućne mreže. Stoga se bezbjednost u komunikaciji pojavljuje kao važno pitanje. Autentifikacija i autorizacija uređaja su od suštinskog značaja za osiguranje bezbjednosti cijele mreže pametnih kuća. Park i Čang (Park & Chang, 2023) su predstavili model koji predstavlja metod za upravljanje pametnim uređajima u kući zasnovan na Ethereum blockchain-u sa poboljšanjem sigurnosti uz primjenu tehnologije dokaza nultog znanja (engl. *zero-knowledge proof*). Ovaj model predstavlja dva ključna koraka. Prvi korak je autentifikacija, koja se vrši čuvanjem heša javnog ključa pouzdanih uređaja na osnovu pametnih ugovora. Ovaj postupak obezbjeđuje tačnost autentifikacije tokom komunikacije sa uređajem i sprečava napade na uređaj, kao što je lažno predstavljanje. Drugi korak modela podrazumijeva potvrdu autentičnosti uređaja putem tehnologije nultog znanja tokom komunikacije sa uređajem, a zatim dijeljenje posebnog ključa sa javnim ključem kriptosistema. Obično, uređaji komuniciraju putem razmjene javnih ključeva u kriptosistemu, ali otkrivanje javnog ključa može ugroziti bezbjednost uređaja. Kada je javni ključ uređaja izložen, uređaj postaje lako identifikovan, što može pomoći napadačima da prikupe informacije o kućnoj mreži.

Prije par godina objavljeno je veliko istraživanje koje koristi blockchain kao rješenje za aplikacije zasnovane na IoT-u, od kojih većina nudi samo dokaz koncepta sa mogućim scenarijima. U svom radu Oudah i saradnici (Ouaddah, Abou Elkala & Ait Ouahman, 2016) uvode fer pristup kao potpuno decentralizovani okvir za upravljanje autorizacijom koji zadovoljava zahtjeve korisnika da kontrolišu i ovladaju sopstvenom privatnošću. UTXO model blockchain-a je korišćen kao baza podataka ili tačka za pronalaženje politike gdje se sve politike kontrole pristupa čuvaju kao transakcije. Tokeni autorizacije su definisani kao digitalni potpisi koji predstavljaju prava pristupa određenim resursima. Međutim, glavno ograničenje njihovog modela je potrebna dugotrajna konfirmacija, što nije prikladno za aplikacije koje zahtjevaju visok integritet.

Predložena lagana arhitektura pametne kuće zasnovana na blockchain-u, koju su razvili Dori i saradnici (Dorri, Kanher & Jurdak, 2017), ima za cilj poboljšati bezbjednost i privatnost pametnih kuća. Ova arhitektura koristi hibridni pristup koji se sastoji od tri osnovna nivoa: pametne kuće, mreže sa preklapanjem i skladištenja u oblaku. Nivo pametne kuće predstavlja samu pametnu kuću i sve uređaje (IoT uređaje) unutar nje. Svaki uređaj ima svoju ulogu u kući, kao što su senzori, termostati, kamere, i drugi uređaji. Kako bi se povećala bezbjednost, svaki uređaj koristi privatnu nepromjenjivu knjigu, što znači da se svaka interakcija i transakcija koja se dešava sa uređajem evidentira i čuva na način koji ne može biti promjenjen. Mreža sa preklapanjem je bitna komponenta ove arhitekture. Ona omogućava uređajima unutar kuće da komuniciraju bezbjedno i pouzdano. Ova mreža omogućava da se informacije dijele između uređaja i održava visok nivo sigurnosti i privatnosti u komunikaciji među uređajima. Takođe, omogućava centralno smanjenje troškova obrade podataka. Nivo skladištenja u oblaku uključuje skladištenje podataka u oblaku, gdje se čuvaju važni podaci i informacije koje su relevantne za pametnu kuću. Ovi podaci se takođe mogu povezati sa javnim blockchain-om. Dodatno, javni blockchain se koristi za uključivanje uređaja sa većim resursima, koji su spojeni zajedno kako bi stvorili distribuirani lanac povjerenja. Ovaj lanac povjerenja se koristi za olakšavanje procesa validacije novih transakcija i blokova. To pomaže u smanjenju procesa i dodatnih troškova u validaciji novih podataka. Na kraju, različiti entiteti u pametnoj kući komuniciraju na različitim nivoima putem transakcija koje se zatim grupišu u blokove, slično kao u tradicionalnom blockchain sistemu. Ova arhitektura omogućava bolju sigurnost, privatnost i efikasnost u upravljanju IoT uređajima u pametnoj kući.

U radu Hašemija i saradnika (Hashemi et al., 2016), blockchain je iskorišćen kao osnovna baza podataka za skladištenje informacija. Autori su razvili distribuirani i decentralizovani mehanizam koji se oslanja na tehnologiju blockchain-a, posebno koristeći pretplatu na publikacije kao ključni element. Ovaj mehanizam omogućava efikasno upravljanje pristupom informacijama, koristeći liste pristupa i politike kontrole prava pristupa. U ovom sistemu usmjerenom na korisnika, različite uloge ili entiteti mogu međusobno sarađivati i komunicirati na način koji je siguran i privatniji. Ovo se postiže kroz skalabilne usluge razmjene poruka koje se baziraju na modelu objavljivanja-pretplate. Ovaj model omogućava entitetima da primaju samo one informacije koje su relevantne za njih i na koje imaju pravo pristupa. Osim toga, podaci se čuvaju i upravljaju putem blockchain tehnologije, što obezbeđuje integritet i nepromenjivost podataka. Ovakva arhitektura pruža siguran, efikasan i privatniji način komunikacije i razmjene informacija među korisnicima i entitetima u sistemu. Blockchain se koristi kao centralno skladište podataka koje osigurava transparentnost i pouzdanost u upravljanju informacijama.

3.1. Arhitektura pametne kuće, bezbjednost i blockchain

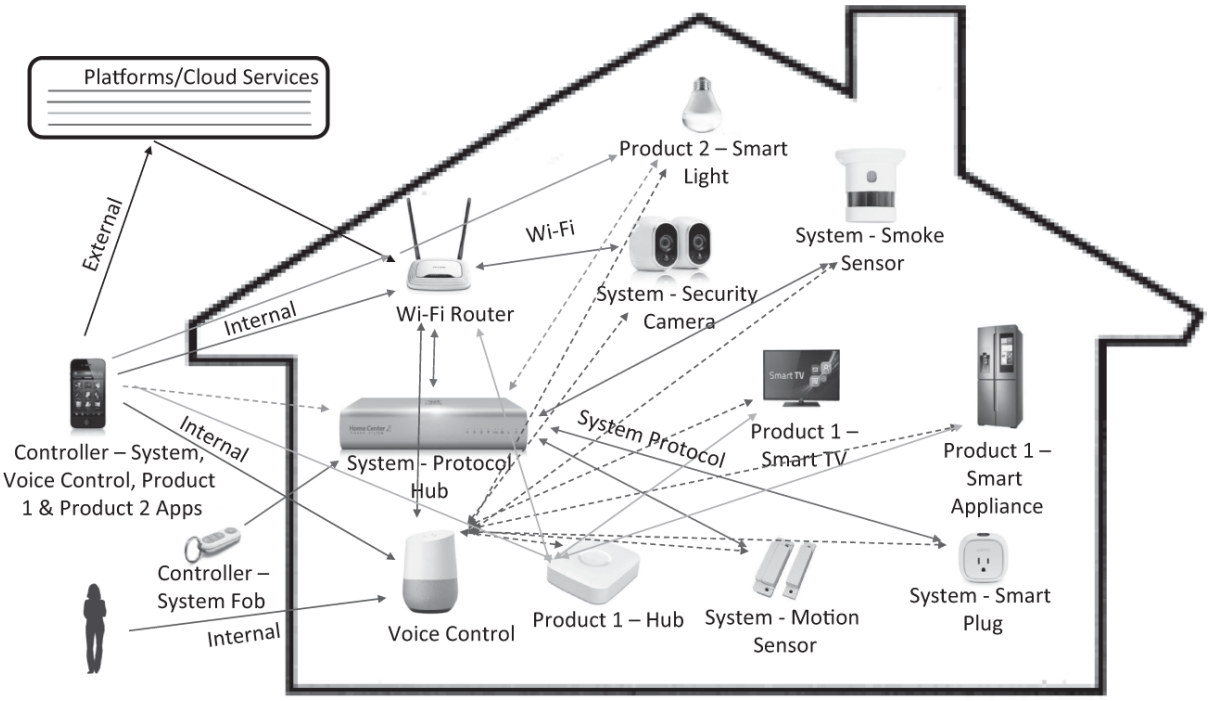
U okviru ovog dijela rada prikazani su tradicionalna arhitektura pametne kuće i bezbjednost i blockchain u kontekstu pametne kuće.

3.1.1. Tradicionalna arhitektura pametne kuće

Arhitektura pametne kuće podrazumijeva integraciju naprednih tehnoloških sistema i komponenti kako bi se stvorila kuća koja je pametnija, energetski učinkovitija i udobnija za stanovanje (Aliero et al., 2021). Slika 1 prikazuje primjer pametne kuće. U nastavku je prikazano nekoliko ključnih elemenata i koncepta arhitekture pametne kuće.

Automatizacija je ključna komponenta pametne kuće koja omogućava korisnicima da stvore udobno, energetski učinkovito i sigurno okruženje. Pametne kuće koriste različite sisteme za automatizaciju kako bi olakšale upravljanje različitim aspektima kuće (Stolojescu-Crisan, Crisan & Butunoi, 2021). Pametna rasvjeta je jedan od ključnih elemenata automatizacije. Ona omogućava prilagođavanje svjetlosnih postavki prema potrebi i preferencijama. Korisnici mogu postaviti raspored svjetla, prilagoditi intenzitet svjetla, promijeniti boje ili koristiti senzore svjetla kako bi se automatski prilagodila osvjetljenost zavisno od vremenskih uslova i prisutnosti u prostoriji. Takođe, automatizacija se proteže na upravljanje grijanjem i hlađenjem putem pametnih termostata. Ti termostati omogućavaju

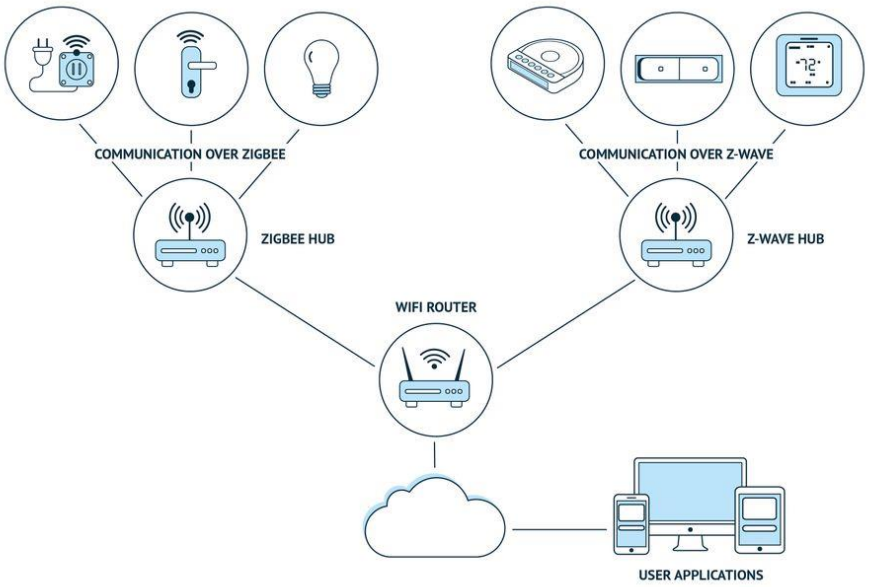
precizno upravljanje temperaturom u kući, što može rezultirati uštedom energije. Oni se mogu programirati prema rasporedu korisnika ili prilagoditi prema stvarnim vremenskim uslovima i prisutnosti u kući. Pametna sigurnost je takođe ključni aspekt automatizacije. To uključuje nadzor sigurnosnih sistema pomoću kamera, senzora pokreta, senzora dima i plina, sistema zaštite od provala. Kada se otkrije nepravilnost, sistem može automatski aktivirati alarme ili obavijestiti vlasnike putem mobilnih aplikacija. U području zabave, automatizacija omogućava jednostavno upravljanje audio i video sistemima. Korisnici mogu kontrolisati muziku, filmove i televiziju putem pametnih uređaja ili glasovnih naredbi. Integracija glasovnih asistenata omogućava korisnicima upravljanje različitim uređajima i sistemima glasom. Sve ove tehnološke mogućnosti obično su dostupne korisnicima putem mobilnih aplikacija koje omogućavaju praćenje i upravljanje svojim kućama izvan nje, čime se olakšava svakodnevno upravljanje i prilagođavanje okoline prema vlastitim željama i potrebama. Automatizacija pametne kuće pruža praktičnost i udobnost dok istovremeno doprinosi energetskoj učinkovitosti i sigurnosti doma (Gunge & Yalagi, 2016).



Slika 1 ***Pametna kuća (Burdon, 2020)***

Povezivost je takođe ključna karakteristika pametnih kuća. Svi uređaji i komponente u kući mogu biti povezani putem različitih bežičnih tehnologija, kao što su ***Wi-Fi***, *Bluetooth, Zigbee* i *Z-wave*. Ova povezivost omogućava korisnicima daljinsko nadziranje i upravljanje svojim domom putem Interneta. *Wi-Fi* je jedna od najčešće korišćenih tehnologija za povezivanje uređaja u pametnoj kući. Omogućava brzu i stabilnu vezu za uređaje kao što su

pametni telefoni, tableti, računari i pametni uređaji za kuću. *Wi-Fi* omogućava daljinsku kontrolu uređaja putem Internet pristupa. Bluetooth se često koristi za povezivanje uređaja na kratke udaljenosti, kao što su pametni zvučnici, slušalice i mobilni uređaji. To omogućava jednostavno povezivanje i bežičnu reprodukciju zvuka. *Zigbee* je bežična tehnologija dizajnirana posebno za pametne kuće. Omogućava nisku potrošnju energije i pouzdano povezivanje između pametnih uređaja kao što su senzori, pametni prekidači i brave. *Zigbee* takođe podržava mrežu s niskom latencijom koja je važna za brzu reakciju pametnih uređaja. *Z-Wave* je bežični protokol specijalizovan za povezivanje i komunikaciju pametnih uređaja u pametnim kućama. Ova tehnologija se ističe po svojoj niskoj potrošnji energije, interoperabilnosti između različitih proizvođača i sposobnosti stvaranja pouzdane mreže uređaja koji se međusobno kontrolišu putem radiofrekvencijskih signala. *Z-Wave* tehnologija omogućava korisnicima jednostavnu i pouzdanu kontrolu nad svojim pametnim uređajima, doprinoseći udobnosti i energetskoj učinkovitosti u pametnim kućama (Savin, 2017; Danbatta & Varol, 2019). Povezivost omogućava korisnicima da nadziru i upravljaju svojim kućama izvan nje putem interneta. To znači da možete daljinski upravljati svjetlima, termostatom, sigurnosnim kamerama i drugim uređajima putem mobilnih aplikacija ili Internet pregledača. Ova daljinska kontrola korisnicima omogućava pristup njihovom domu čak i kada nisu fizički prisutni. Osim toga, povezivost omogućava pametnim uređajima u kući da komuniciraju međusobno, što rezultira boljom koordinacijom i automatizacijom (Pradeep et al., 2016). Na primjer, senzor pokreta može aktivirati rasvjetu ili termostat može prilagoditi temperaturu u sobi na osnovu podataka s drugih uređaja. Povezivost je temeljni element pametnih kuća i omogućava korisnicima da stvore pametno, integrisano i praktično okruženje za život.



Slika 2 *Arhitektura pametne kuće koja sadrži čvorišta za različite protokole (Odunlade, 2022)*

Sigurnost igra izuzetno važnu ulogu u zaštiti doma, imovine i sigurnosti stanara. Pametne kuće obično imaju sisteme sigurnosti koji uključuju kamere za nadzor okoline i unutrašnjih prostora, senzore pokreta za detekciju aktivnosti, senzore dima i plina za rano upozorenje na opasnosti i mogućnosti daljinskog nadzora i upravljanja ovim sistemima. Pametne kuće često su opremljene sigurnosnim kamerama koje omogućavaju nadzor nad spoljnim i unutrašnjim prostorima. Kamere se mogu postaviti na ključnim tačkama kako bi se snimale aktivnosti oko kuće. Mnoge pametne kamere podržavaju visoku rezoluciju i mogu snimati video zapise uživo ili ih skladištiti u oblaku. Senzori pokreta detektiraju kretanje u kući i oko nje. Kada se aktiviraju, mogu pokrenuti različite akcije, kao što su uključivanje svjetla, slanje obaviještenja vlasnicima ili pokretanje snimanja na sigurnosnim kamerama. Pametni senzori dima i plina prate prisutnost dima i plina u kući. Ako se otkrije prisutnost, sistem će obavijestiti vlasnike, aktivirati alarm i pomoći u prevenciji požara ili trovanja plinom. Ova kombinacija sigurnosnih komponenti omogućava vlasnicima kuća i stanarima da budu svjesni događaja u i oko svoje kuće i da brzo reaguju na potencijalne prijetnje (Gazis & Katsiri, 2021). Daljinski nadzor i upravljanje putem mobilnih aplikacija čini ovaj proces praktičnim i omogućava korisnicima da ostanu povezani sa svojim domom, čak i kad nisu prisutni. Naime, korisnici mogu daljinski nadzirati i upravljati sigurnosnim sistemima putem mobilnih aplikacija. To znači da mogu provjeravati stanje kamere, primati obaviještenja i kontrolisati senzore čak i kad nisu kod kuće. Pametni sistemi zaštite od provala uključuju

senzore na vratima i prozorima, pametne brave i alarmne sisteme. Sistemi zaštite od provala mogu se integrisati s drugim sigurnosnim komponentama za potpuniju zaštitu kuće. Integracija različitih aspekata sigurnosti pruža korisnicima veći osjećaj sigurnosti i kontrole nad njihovim okruženjem. Osim toga, ovi sistemi često pružaju mogućnost snimanja događaja, što može biti od pomoći u slučaju potrebe za istraživanjem ili praćenjem događaja koji su se dogodili unutar ili oko doma (Chitnis, Deshpande & Shaligram, 2016).

Energetska učinkovitost je još jedan ključan aspekt pametnih kuća. Ove kuće često su opremljene sistemima za upravljanje potrošnjom energije kako bi smanjile troškove i smanjile ekološki otisak. Pametni termostati omogućavaju precizno upravljanje grijanjem i hlađenjem prema potrebi, čime se sprečava nepotrebno rasipanje energije (Ayan & Turkay, 2020). LED rasvjeta je energetski učinkovita alternativa tradicionalnim sijalicama i omogućava smanjenje potrošnje električne energije za osvjetljavanje kuće. Osim toga, pametni sistemi za osvjetljenje omogućavaju prilagođavanje svjetlosnih postavki prema potrebama i preferencijama korisnika (Byun et al., 2013). Solarna energija igra važnu ulogu u energetskoj učinkovitosti pametnih kuća. Instalacija solarnih panela na krovu omogućava kući da proizvodi vlastitu električnu energiju iz obnovljivog izvora, što smanjuje troškove energije i doprinosi očuvanju okoline (Zhou et al., 2016). Praćenje potrošnje energije omogućava korisnicima da bolje razumiju kako i gdje se troši energija u njihovoj kući. To ih postiče na razumnu potrošnju i omogućava identifikovanje načina na koje mogu dodatno uštedjeti energiju (Salman et al., 2016). Kombinacija ovih energetski učinkovitih sistema i komponenti čini pametne kuće ekološki prihvatljivijima i omogućava korisnicima da smanje svoj račun za energiju, doprinoseći istovremeno očuvanju okoline. Energetska učinkovitost je važan aspekt savremenih domova, a pametne kuće nude rješenja koja pomažu postizanje ovog cilja.

Integracija zabave je još jedan važan aspekt pametnih kuća koji omogućava korisnicima potpunije iskustvo u njihovom domu. Ove kuće nude integrisane sisteme za zabavu, uključujući pametne televizore, visokokvalitetne zvučnike i sisteme za streaming muzike. Pametni televizori omogućavaju korisnicima pristup različitim medijskim sadržajima putem Internet povezivanja. Mogu se povezati s drugim pametnim uređajima u kući i koristiti za gledanje televizije, filmova, streaming usluga, igranje videoigara i druge medijske aktivnosti. Zvučnici su također važan dio integracije zabave u pametnim kućama. Pametni zvučnici s glasovnim asistentima omogućavaju korisnicima da upravljaju svojim kućama glasovnim naredbama, uključujući kontrolu osvjetljenja, termostata, sigurnosnih sistema i

drugih pametnih uređaja. Sistemi za streaming muzike omogućavaju korisnicima da pristupe svojoj omiljenoj muzici iz različitih izvora. Muzika se može reprodukovati u cijeloj kući pomoću pametnih zvučnika i bežičnih audio sistema. Integracija zabave u pametnim kućama pruža korisnicima praktičnost i raznolikost opcija za uživanje u svojim omiljenim medijskim sadržajima (Vandome, 2018). Korisnici mogu prilagoditi svoje iskustvo zabave prema sopstvenim preferencijama i lako upravljati svim aspektima zabave u svojem domu putem mobilnih aplikacija ili glasovnih naredbi. To stvara okruženje koje je prilagođeno njihovim željama i potrebama za uživanje u slobodnom vremenu i opuštanje.

Pametne kuće omogućavaju **glasovnu kontrolu**. Naime, korisnici često koriste glasovne asistente kao što su Amazon Alexa, *Google Assistant* ili *Apple Siri* kako bi upravljali uređajima i sistemima u svojoj kući. Ovi glasovni asistenti omogućavaju korisnicima da jednostavno izdaju glasovne naredbe kako bi kontrolisali različite aspekte pametnog doma. Na primjer, korisnik može reći "Alexa, uključi svjetla u dnevnoj sobi" ili "Hey Google, smanji temperaturu na termostatu". Glasovna kontrola čini upravljanje pametnim uređajima jednostavnim i praktičnim, a korisnici se mogu osloniti na ove asistente kako bi obavili različite zadatke, uključujući promjenu postavki, dobijanje informacija i upravljanje zabavnim sadržajem. Ova tehnologija čini pametne kuće još pristupačnijima i prikladnijima za korisnike svih starosnih grupa (Isyanto, Arifin & Suryanegara, 2020).

Prilagodljivost je važna karakteristika pametnih kuća. Ove kuće su dizajnirane s ciljem da se lako prilagode potrebama i preferencijama korisnika. To znači da korisnici imaju fleksibilnost u promjeni postavki i funkcionalnosti kako bi stvorili okruženje koje odgovara njihovom načinu života. Jedan od primjera prilagodljivosti je kontrola svjetla. Korisnici mogu prilagoditi intenzitet svjetla, boju svjetla i raspored osvjetljenja u skladu s trenutnim potrebama i atmosferom koju žele stvoriti. Ovo se može učiniti putem mobilnih aplikacija, daljinskih upravljača ili glasovnim naredbama. Pametni termostati također nude prilagodljivost u upravljanju temperaturom u kući. Korisnici mogu programirati termostat prema sopstvenom rasporedu i preferencijama, a također ga mogu prilagoditi na daljinu putem mobilnih aplikacija. Osim toga, prilagodljivost uključuje mogućnost integracije različitih pametnih uređaja i sistema kako bi se stvorilo cjelovito iskustvo. Korisnici mogu odabrati koje uređaje žele uključiti u svoj pametni dom i kako žele da ti uređaji međusobno komuniciraju (Vandome, 2018). Prilagodljivost pametnih kuća omogućava korisnicima da stvore okruženje koje odražava njihov stil života i potrebe. To je posebno važno jer se

potrebe i preferencije korisnika mogu mijenjati tokom vremena, pa je prilagodljivost ključna za održavanje udobnosti i funkcionalnosti pametne kuće.

Sistemi pametnog osvjetljenja predstavljaju ključnu komponentu modernih pametnih kuća. Njihova prednost leži u sposobnosti korisnika da prilagode osvjetljenje u svojoj kući prema vlastitim preferencijama i trenutnim potrebama. Ovo prilagođavanje uključuje kontrolu jačine svjetla, pa čak i promjenu boje svjetla kako bi se stvorila određena atmosfera. Na primjer, korisnici mogu smanjiti svjetlinu za stvaranje intimnih večeri ili odabrati hladniju bijelu svjetlost za bolju koncentraciju tokom radnih zadataka. Osim toga, pametni sistemi osvjetljenja omogućavaju stvaranje različitih atmosfera u različitim dijelovima kuće. Na taj način, korisnik može postaviti romantičnu svjetlost u dnevnoj sobi, energičniju svjetlost u radnoj sobi ili nježnu svjetlost u spavaćoj sobi, sve prema svojim potrebama i trenutnom raspoloženju. Jedna od ključnih prednosti ovih sistema je mogućnost daljinskog upravljanja. Putem pametnih telefona, tableta ili daljinskih upravljača, korisnici mogu prilagoditi osvjetljenje iz udobnosti svojih fotelja ili čak izvan kuće. Ovo je ne samo praktično, već i doprinosi sigurnosti jer korisnici mogu simulirati prisutnost čak i kad nisu kod kuće. Sistemi pametnog osvjetljenja također mogu reagirati na vremenske i senzorske uslove (Khoa et al., 2020). Na primjer, mogu automatski prilagoditi svjetlost zavisno od dnevnog svjetla ili ugasiti svjetla kad nema prisutnosti u prostoriji. Ova funkcionalnost doprinosi energetskoj učinkovitosti i smanjenju troškova električne energije. Naposletku, sistemi pametnog osvjetljenja nisu samo funkcionalni, već i doprinose udobnosti i estetici doma, stvarajući prilagodljivo i ugodno okruženje koje se lako prilagođava potrebama i željama korisnika.

Pametni uređaji za kuću predstavljaju važnu komponentu pametnih domova, koja transformiše način na koji komuniciramo sa svojim okruženjem. Pametne kuće često koriste različite pametne uređaje kako bi poboljšale udobnost, energetsku učinkovitost, sigurnost i funkcionalnost doma. Pametni frižideri su jedan od primjera pametnih uređaja. Ovi frižideri su opremljeni ekranima osjetljivim na dodir, kamerama i Wi-Fi povezanošću. Korisnici mogu pregledati unutrašnjost frižidera putem mobilnih aplikacija kako bi provjerili sadržaj bez otvaranja vrata. Osim toga, pametni frižideri mogu pratiti datume isteka hrane, stvarati popise za kupovinu i čak predlagati recepte na osnovu dostupnih namirnica. Pametne mašine za pranje i sušenje veša nude praktičnost i uštedu energije. Korisnici njima mogu upravljati putem mobilnih aplikacija kako bi postavili raspored pranja, pratili status ciklusa pranja i sušenja te primili obaviještenja kada je veš spreman (Kang, Moon & Park, 2017). Pametne

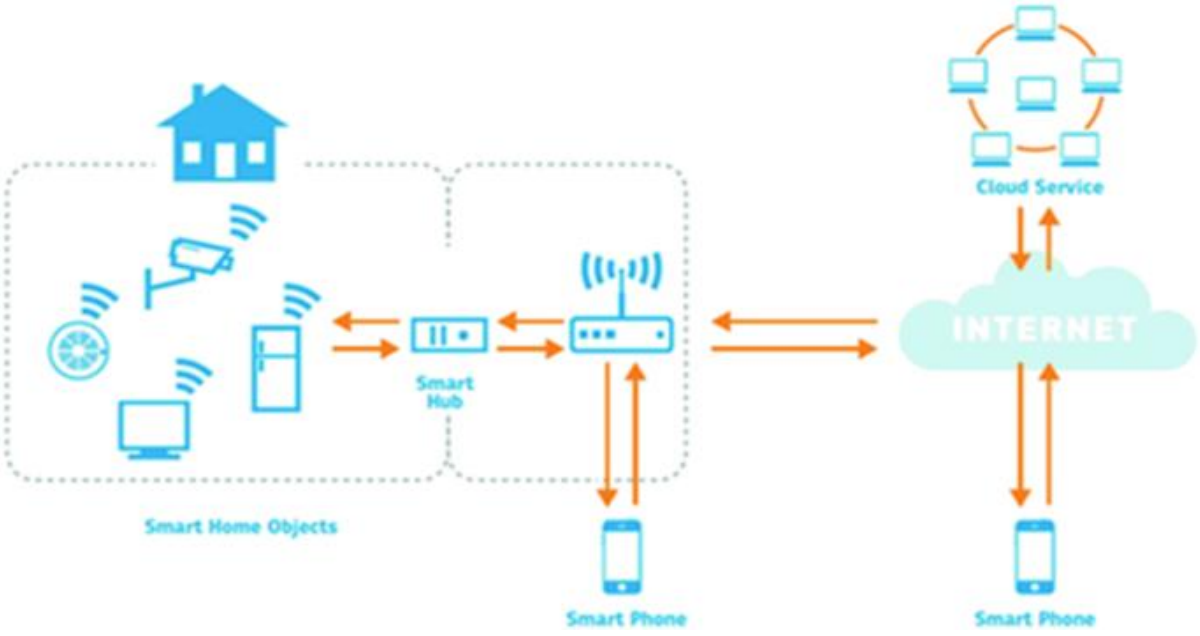
brave omogućavaju korisnicima da kontrolišu pristup svojoj kući putem mobilnih aplikacija. To znači da mogu zaključavati i otključavati vrata daljinski, omogućiti pristup gostima, pratiti ko ulazi i izlazi iz kuće, i stvarati privremene digitalne ključeve za goste (Williams et al., 2020). Pametni termostati su ključni za upravljanje grijanjem i hlađenjem u kući. Oni omogućavaju precizno postavljanje temperature prema rasporedu i preferencijama korisnika, a takođe se prilagođavaju uslovima poput vremena i prisutnosti u kući kako bi smanjili potrošnju energije (Özgür et al., 2018) Ovi pametni uređaji čine život u pametnoj kući praktičnijim, energetski učinkovitijim i sigurnijim. Omogućavaju korisnicima bolju kontrolu nad različitim aspektima njihovog doma, a integracijom ovih uređaja u jedinstven ekosistem, korisnici mogu postići veću koordinaciju i automatizaciju, čineći svoj život još udobnijim i praktičnijim.

Nadzor kvaliteta vazduha je komponenta pametnih kuća koja doprinosi udobnosti i zdravlju stanara. Ovo uključuje upotrebu senzora za praćenje kvaliteta vazduha i sistema za pročišćavanje vazduha kako bi se osiguralo čisto i zdravo okruženje u kući. Senzori za praćenje kvaliteta vazduha mjere različite parametre kao što su koncentracija čestica, nivo vlage, prisutnost gasova, uključujući one štetne po zdravlje. Ti senzori prate promjene u kvalitetu vazduha i omogućavaju korisnicima da budu svjesni potencijalnih problema. Sistemi za pročišćavanje vazduha uključuju različite tehnologije, poput HEPA filtera, aktivnog ugljenika i UV-C sterilizacije. Ovi sistemi uklanjaju čestice, alergene, bakterije i viruse iz vazduha, poboljšavajući kvalitet vazduha u kući. Pametni sistemi za nadzor kvaliteta vazduha često omogućavaju korisnicima da prate i kontrolišu kvalitet vazduha putem mobilnih aplikacija. Ovo pruža korisnicima informacije o trenutnom stanju vazduha i omogućava im da preduzmu odgovarajuće mjere kako bi osigurali da vazduh u njihovom domu bude čist i siguran za disanje (Vandome, 2018). Nadzor kvaliteta vazduha postaje sve važniji aspekt pametnih kuća, posebno s obzirom na rastuću zabrinutost za kvalitet vazduha u unutrašnjim prostorima i njegov utjicaj na zdravlje. Integracija ovih tehnologija u pametne kuće omogućava korisnicima da stvore zdravo i ugodno okruženje za sebe i svoje porodice.

Važno je napomenuti da arhitektura pametne kuće zahtijeva integraciju ovih tehnoloških komponenata u samoj fazi projektovanja kuće. To uključuje postavljanje kablova, senzora i pametnih uređaja kako bi se osigurala glatka funkcionalnost sistema. Takođe je potrebno razmotriti sigurnosne aspekte kako bi se zaštitila kuća od potencijalnih napada na sisteme pametne kuće.

Komponente pametne kuće se mogu dodati u postojeću kuću naknadno, iako će to možda zahtijevati nešto dodatnog truda i prilagođavanja u poređenju s integracijom tih komponenata u fazu projektovanja kuće. U svakom slučaju, dodavanje pametnih komponenti u postojeću kuću je moguće, i mnogi ljudi to uspješno čine kako bi poboljšali funkcionalnost, sigurnost i energetsku učinkovitost svojih domova.

Koncept pametne kuće uključuje integraciju sistema i pametnih uređaja u ljudsko okruženje kako bi se ljudima olakšao svakodnevni život. Pametna kuća ima širok spektar rješenja kao što su brojila, senzori i mikrosistemi koji su izgrađeni na osnovu niza tehnologija, standarda i uređaja. Ova rješenja se mogu koristiti za izvještavanje o potrebnim informacijama o okolini na dnevnoj bazi. Na primjer, pametni uređaji u pametnoj kući mogu pružiti informacije o nivou temperature ili potrošnji energije (Omran et al., 2022).



Slika 3 ***Tradicionalna arhitektura pametne kuće (Qashlan, Nanda & He, 2020)***

Tradicionalne pametne kuće, kao što je primjer prikazan na slici 3, zasnovane su na centralizovanoj arhitekturi u kojoj su kućni uređaji povezani na srednje čvorište koje obezbjeđuje direktnu internet konekciju (Qashlan, Nanda & He, 2020). Središnji uređaj pruža direktnu Internet konekciju za povezane uređaje u kući. Bežični protokoli poput *Zigbee* ili *Z-Wave* često se koriste za komunikaciju između uređaja i središnjeg čvorišta, što omogućava različitim uređajima da komuniciraju i budu upravljani na daljinu. Nakon toga, centralna kontrolna jedinica se povezuje sa kućnim ruterom kako bi omogućila uređajima da budu povezani sa spoljnim svetom, pristupaju Internetu i da mogu komunicirati sa cloud uslugama

ili udaljenim serverima. Ova arhitektura ima svoje prednosti, poput lakoće upravljanja različitim uređajima iz jednog centralnog mjesta, ali takođe ima i izazove, uključujući sigurnosne aspekte i potencijalne tačke kvara. Kako bi se osigurala sigurnost i stabilnost takvih sistema, važno je da se koriste odgovarajući sigurnosni mehanizmi i da se ažuriraju uređaji i softveri kako bi se sprečili potencijalni sigurnosni rizici.

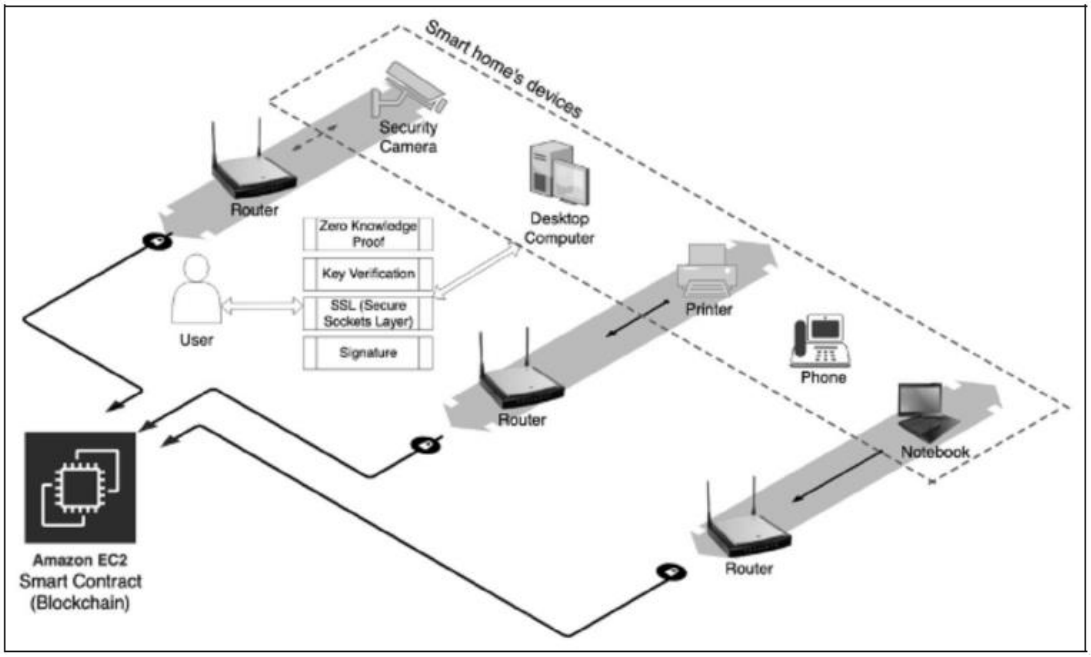
Integracija između svih uređaja rezultira povećanom bezbjednošću i problemima privatnosti u okruženju pametne kuće (Al-Turjman et al., 2022). Istraživanja i prethodni rad su obavljeni kako bi se identifikovale i razumijele potencijalne prijetnje i postojeće tehnike koje su prilagođene okruženju pametne kuće. Na primjer, Ili i saradnici (Illy et al., 2020) predložili su pristup usmjeren na mrežu koji prati mrežne aktivnosti kako bi se otkrilo sumnjivo ponašanje i korišćenje softverski definisane tehnologije umrežavanja u kontekstu pametne kuće za dinamičko blokiranje uređaja na osnovu njihovih mrežnih aktivnosti. Istraživanje koje su sproveli Dos Santos i saradnici (Dos Santos et al., 2022) opisuje praktičnu metodu oblikovanja saobraćaja koja efikasno štiti privatnost pametne kuće od pasivnog mrežnog protivnika bez značajnog povećanja troškova podataka ili smanjenja performansi mreže. Istraživanje koje su sproveli Sivarman i saradnici (Sivaraman et al., 2015) primjenjuje novu laganu metodu provjere identiteta šifrovanja/dešifrirovanja među senzorskim čvorovima koristeći dinamički varijabilni bezbjednosni certifikat šifrovanja. Međutim, tradicionalni pristupi bezbjednosti su uglavnom centralizovani i skupi. Potrošnja energije i režijski troškovi obrade su visoki, a postoji i poteškoća sa razmjerom. Stoga pametni kućni uređaji zahtijevaju skalabilan i decentralizovan pristup kako bi se prevazišao ovaj izazov (Nasir et al., 2022).

3.1.2. Bezbjednost i blockchain

Svaki bezbjednosni dizajn treba da se bavi trijadom CIA-e: povjerljivost, integritet i funkcije dostupnosti povezane s podacima i sistemima. Povjerljivost sprečava neovlašćene korisnike da pristupe privatnim podacima, istovremeno osiguravajući da ih primaju samo ispravni korisnici.

Integritet održava konzistentnost i tačnost podataka osiguravajući da se preneseni podaci primaju nepromijenjeni. Dostupnost garantuje pristup podacima kada su korisnicima potrebni (Ratkovic, 2022). U blockchain-u, povjerljivost se može riješiti korišćenjem para privatnih i javnih ključeva koje svaki čvor mora posjedovati. Čvor pošiljaoca koristi privatni

ključ za potpisivanje digitalnog potpisa i emitiovanje transakcije kroz cijelu mrežu. Čvor primaoca potvrđuje transakciju koristeći javni ključ čvora pošiljaoca. Na ovaj način, samo važeće transakcije se skladšte i dodaju u blockchain (Bhawana et al., 2022). Iako se tvrdi da je povjerljivost i privatnost u blockchain-u teško postići zbog vidljivosti cjelokupnog sadržaja transakcije svakom čvoru na mreži, predložene su mnoge metode za rješavanje ovog problema (Guo & Yu, 2022). Dokazi bez znanja i homomorfna enkripcija su dvije različite metode o kojima se raspravlja u literaturi (Steffen et al., 2022). Proces transakcije podataka zasnovan na blockchain-u u pametnoj kući prikazan je na slici 4.



Slika 4 *Proces transakcije podataka zasnovan na blockchain-u u pametnoj kući (Park & Chang, 2023, 551)*

Osim toga, kako bi se osigurao integritet podataka, koristi se nekoliko kriptografskih alata i odgovarajućih strategija replikacije podataka (Knacef et al., 2023). U arhitekturi zasnovanoj na blockchain-u, pune replikacije blockchain-a postoje na velikom broju čvorova, gdje svi čvorovi imaju istu kopiju blokova. Štaviše, mnoge kriptografske tehnike se koriste u blockchain-u uključujući heš funkciju, digitalne potpise i Merkle stablo. Niz funkcija heširanja SHA-256 sprovodi proces rudarenja za pisanje novih transakcija, njihovo vremensko označavanje i dodavanje u blok. Kada blok postane dio lanca, svi rudari moraju potvrditi i dogovoriti njegov sadržaj. Stoga je praktično nemoguće poništiti transakciju zbog jednosmjerne prirode funkcije heširanja i ogromne računarske snage koja je potrebna za neovlašćeno djelovanje u blockchain-u. Algoritam digitalnog potpisa zasnovan na eliptičnim

krivim koristi se u blockchainu za generisanje digitalnog potpisa kako bi se osiguralo da sve transakcije obavlja samo pravi čvor. Takođe, blockchain koristi strukturu Merkle stabla koja omogućava sigurnu verifikaciju sadržaja velikih podataka slanjem samo heš podataka: čvor primaoca provjerava heš u odnosu na korijen Merkle stabla. Svaka promjena u bilo kojoj transakciji na dnu će rezultirati promjenom heša čvora iznad i tako dalje do korijena stabla, što znači da će heš bloka biti drugačiji i da će postati nevažeći blok (Thakur, 2017).

Što se tiče dostupnosti, blockchain je potpuno decentralizovana arhitektura koja osigurava da ne postoji jedna tačka kvara i da se podaci distribuiraju na više čvorova. Svaki čvor u mreži ima kopiju cjelokupne istorije transakcija koja se može provjeriti i pratiti do prve transakcije. Ovo rezultira distribuiranom arhitekturom otpornom na greške (Thakur, 2017). Autori pretpostavljaju da je blockchain infrastruktura mnogo otpornija na prijetnje dostupnosti kao što su lažno predstavljanje ili DoS od druge centralizovane arhitekture IoT-a (Shah et al., 2022).

Stoga, kriptografsko heširanje u blockchain-u i njegov konsenzus protokol, koji provjerava da li se heš poklapa s njegovim blokom ili ne, čine blockchain teoretski otpornim na neovlašćeno korišćenje. Heš zahtjeva mnogo vremena i energije za računanje za generisanje i služi kao dokaz rada kako bi se osiguralo da svaki čvor preduzima računski rad za dodavanje novog bloka u lanac bez mijenjanja sadržaja bloka. Takođe, hešovi povezuju svaki blok sa jedinstvenim hešom prethodnog bloka. Dakle, svaka promjena u jednom bloku će zahtijevati izračunavanje novog heša za taj blok i takođe za svaki sljedeći blok ili će blok biti u sukobu sa postojećim blokovima i drugi čvorovi će odbiti promjenu. To je ono što blockchain čini nepromjenjivim.

3.2. Primjer kreiranja pametnih ugovora i evaluacija prikazanog prototipa

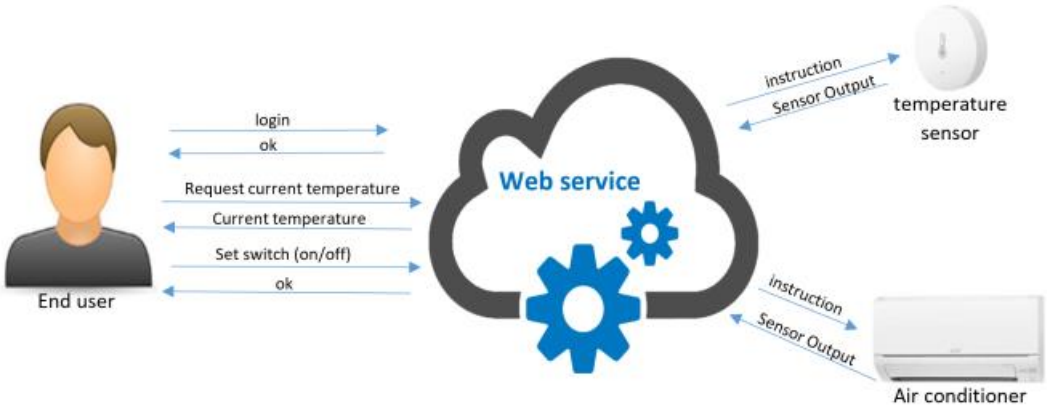
U poređenju sa drugim blockchain tehnologijama, Ethereum koji je predložio Vatalik Buterin 2013. godine je javno distribuirana blockchain tehnologija koju izvodi Ethereum VirtualMachine (EVM) (Zhao, 2022) koja omogućava korisnicima da kreiraju sopstvene programe željene složenosti koristeći pametni ugovor. Ova karakteristika omogućava da Ethereum koriste različite decentralizovane aplikacije, ne ograničavajući se na kriptovalute. Pogodan je za aplikacije koje zahtjevaju automatsku interakciju između članova na mreži (Mehedi et al., 2019).

Najjednostavnije rečeno, vrijeme transakcije za Ethereum je 12 sekundi u odnosu na Bitcoin koji ima vrijeme bloka od 10 minuta, s obzirom da se koristi za širok spektar aplikacija. Nedavno su mnoge organizacije i industrije pokušale izgraditi sopstvene slučajeve upotrebe za Ethereum (Arslanian, 2022).

3.2.1. Primjer arhitekture pametne kuće zasnovana na Ethereum-u

U scenariju pametne kuće, pametni uređaji mogu međusobno komunicirati direktno kako bi zatražili podatke za pružanje određenih usluga. Na primjer, pametni klima uređaj traži trenutnu sobnu temperaturu od temperaturnog senzora kako bi automatski uključio klima uređaj kada temperatura poraste do određene vrijednosti ili uključio grijač ako temperatura padne ispod određene vrijednosti. Oba uređaja takođe mogu slati upozorenja ili obavještenja korisniku o njihovom stanju.

Možemo početi razmatranjem trenutnih pametnih rješenja i provjerom kako ona funkcionišu putem konvencionalnih metoda, kao što je prikazano na slici 5. Ako neko želi daljinski upravljati pametnim klima uređajem, tada bi mu obično bila potrebna (nadamo se) sigurna web usluga koja omogućava pristup tek nakon što unesete login i lozinku. Tada je moguće poslati naredbu, a web servis će naložiti hardveru da aktivira ili deaktivira klima uređaj.

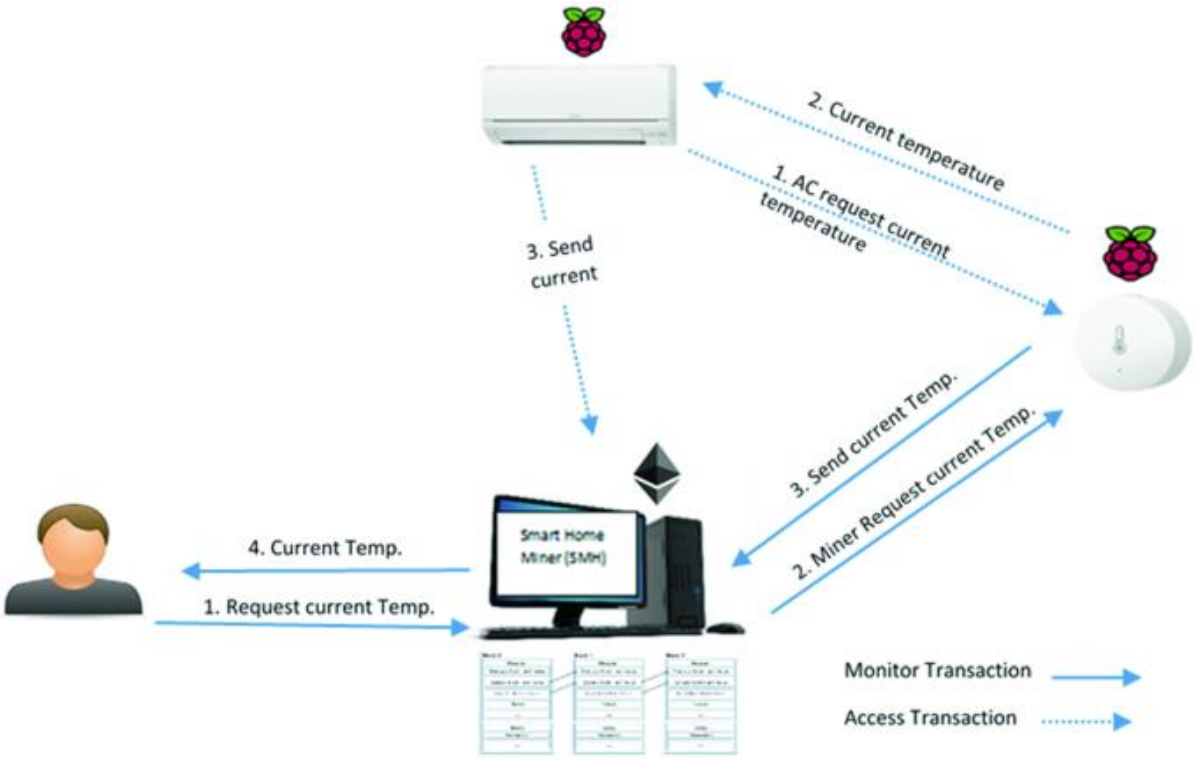


Slika 5 *Tradicionalni način kontrole povezanog pametnog uređaja (Qashlan, Nanda & He, 2020*)

Problem je u tome što web usluge pružaju ono što se naziva pristup za pisanje. Poslate instrukcije web servis prevodi u hardverske instrukcije, a zatim ih izvršava priključeni uređaj, u ovom slučaju klima uređaj. Po definiciji, nije sigurno dozvoliti pristup pisanju. Nijedan web

servis nije neprobojan. Odobrenje pristupa uređaju spolja uvijek povećava mogućnost da će neko moći hakovati ovaj pristup do krajnjih korisnika, čime ugrožava njihovu sigurnost i privatnost. Ova ranjivost je posljedica jedne tačke neuspjeha, tačke u kojoj se provjerava autentičnost i gdje se prihvataju dolazne instrukcije.

Kašlan i saradnici (Qashlan, Nanda & He, 2020) predložili su prototip, prikazan na slici 6, izgrađen na blockchain-u koji koristi pametni ugovor za kontrolu dozvola za promjenu stanja klima uređaja. Arhitektura njihovog prototipa, prikazana na slici 6, zasniva se na Ethereum pametnom ugovoru i sastoji se od pametnog kućnog rudara povezanog na privatni blockchain, temperaturnog senzora i klima uređaj. Koristi se Raspberry Pi za simulaciju IoT uređaja (Qashlan, Nanda & He, 2020).



Slika 6 ***Eksperimentalni prototip (Qashlan, Nanda & He, 2020)***

3.2.2. Primjer procesa kreiranja pametnog ugovora

U svom eksperimentu Kašlan i saradnici (Qashlan, Nanda & He, 2020) kreirali su dva pametna ugovora. Prvi je ugovor monitora za provjeru očitavanja temperaturnog senzora postavljenog u prvom Raspberry Pi-u. Drugi pametni ugovor je raspoređen u drugom

Raspberry Pi-jevom pristupnom ugovoru, koji omogućava klima uređaju da zatraži vrijednost očitavanja temperature iz ugovora o monitoru (Qashlan, Nanda & He, 2020).

Ugovor o monitoru – Ovaj ugovor omogućava vlasniku kuće da provjeri trenutnu vrijednost temperature. Samo vlasnik može podesiti i mijenjati vrijednost temperature, navodeći adresu vlasnika koji ima dozvolu za postavljanje vrijednosti u ugovornom tijelu. Ugovor može slati upozorenja vlasniku u određeno vrijeme kako bi se prikazala trenutna sobna temperatura (Qashlan, Nanda & He, 2020).

Ugovor o pristupu – Ovaj ugovor može zahtijevati vrijednosti očitavanja temperature pozivanjem vrijednosti iz ugovora o monitoru. Zatim će, na osnovu vrijednosti, ugovor ili uključiti ili isključiti klima uređaj i poslati obaviještenje vlasniku o njegovom trenutnom stanju (Qashlan, Nanda & He, 2020).

Eksperiment koji su izveli Kašlan i saradnici (Qashlan, Nanda & He, 2020) donosi nekoliko pitanja i izazova u vezi sa implementacijom pametnih ugovora u okruženju pametnih kuća. Prvo, iako se čini da su pametni ugovori o monitoru i pristupu korisni za kontrolu temperature u kući, postavlja se pitanje praktične primjene ovakvih ugovora. Da li je zaista neophodno koristiti Ethereum blockchain i pametne ugovore za ovakve osnovne funkcionalnosti, kao što je praćenje temperature i upravljanje klima uređajima? Ovo može stvoriti nepotrebnu složenost i troškove za prosečnog korisnika pametne kuće.

Drugo, problem se pojavljuje u vezi sa skalabilnošću. Ethereum blockchain, iako pruža sigurnost i neporecivost, suočava se sa ograničenjima u brzini i kapacitetu obrade transakcija. U slučaju velikog broja pametnih kuća i uređaja, ovo može dovesti do kašnjenja i visokih troškova transakcija. To postavlja pitanje da li je Ethereum uvijek najbolje rješenje za ovakve primjene.

Kritičko razmatranje praktičnosti, skalabilnosti i stvarnih potreba korisnika je od suštinskog značaja kada se implementiraju pametni ugovori u okruženju pametnih kuća kako bi se osigurala optimalna funkcionalnost i korisničko iskustvo.

3.2.2.1. Hardver i softver

Kašlan i saradnici (Qashlan, Nanda & He, 2020) su izgradili slučaj korišćenjem jednog laptopa (Dell XPS) i dva računara sa jednom pločicom (Raspberry Pi 3 model B). Na svaki uređaj instaliran je geth klijent (interfejs komandne linije implementiran u Go-Ethereum) koji prenosi uređaje na Ethereum čvorove. Za svaki čvor kreiran je Ethereum

račun i konfigurisani su i čvorovi da formiraju privatnu blockchain mrežu, gdje laptop igra ulogu dva rudara jer ima veliku sposobnost računanja i skladištenja. Raspberry Pi funkcioniše kao lagani Ethereum čvor za implementaciju ugovora o nadzoru i ugovora o pristupu (Qashlan, Nanda & He, 2020).

Za pisanje i sastavljanje ugovora korišćen je Remix integrisani razvoj. Ovo je Remix integrisani razvoj zasnovan na pretraživaču za Solidity, koji je jezik koji se koristi za pisanje pametnih ugovora. Za implementaciju i kompajliranje ugovora, kao i praćenje stanja ugovora, Web3.js je prilagođen za interakciju sa odgovarajućim geth klijentom putem HTTP veze. Jednostavna HTML web stranica je napravljena da olakša interakciju između vlasnika kuće i uređaja (Qashlan, Nanda & He, 2020).

Eksperiment koji su Kašlan i saradnici izveli, iako obećava implementaciju pametnih ugovora za pametne kuće, nosi sa sobom nekoliko kritičkih aspekata. Prvo, korišćenje Raspberry Pi uređaja kao Ethereum čvorova i rudara može biti ograničavajuće u stvarnom svijetu. Iako su oni korisni za eksperimentalne svrhe, njihova ograničena procesorska moć i kapacitet skladištenja mogu biti prepreka za skalabilnost i performanse u stvarnim pametnim kućama sa većim brojem uređaja i zahtjevima.

Drugo, upotreba Remixa i Web3.js za pisanje, kompajliranje i interakciju s pametnim ugovorima može biti previše tehnički za prosečnog korisnika pametne kuće. Većina korisnika želi jednostavna rešenja koja ne zahtjevaju duboko razumijevanje blockchain tehnologije ili programiranja. Implementacija složenih alatki može dodatno otežati usvajanje ove tehnologije.

Takođe, eksperiment se izvodi u kontrolisanom okruženju, a stvarni svijet pametnih kuća može doneti dodatne izazove kao što su sigurnost, interoperabilnost i podrška za različite uređaje i protokole. Ovo ukazuje na potrebu za daljim istraživanjem i razvojem kako bi se ovi koncepti prilagodili praktičnim i svakodnevnim zahtjevima korisnika pametnih kuća.

3.2.2.2. Implementacija

Na osnovu smjernica o kojima se raspravlja u bijeloj knjizi Ethereuma, Kašlan i saradnici (Qashlan, Nanda & He, 2020) su konfigurisali privatni blockchain sa nekim modifikacijama:

- Za preuzimanje i instalaciju bira se kompatibilna verzija Ethereum klijenta za svaki uređaj;
- Windows power shell se koristi za pokretanje geth-a izvršavanjem naredbe geth;
- U prikazanom privatnom blockchain-u, svaki čvor mora ispuniti zahtjeve da bi se mogao pridružiti istom blockchain-u; ovi zahtjevi uključuju:
  - isti genesis fajl (Test.json) mora biti inicijalizovan od strane svakog čvora. Inicijalizacija stvara blok geneze, koji je prvi blok blockchain-a i ne odnosi se ni na jedan blok;
  - isti mrežni identifikator sesije mora koristiti svaki čvor za povezivanje na isti blockchain. Bilo koji identifikator sesije se može dodijeliti osim 1, 2 i 3 jer su rezervisani za glavni lanac. Za svoju konfiguraciju dodjelili su mrežni ID 4224 kako sledi:

```
{
  "config": {
    "chainId": 4224,
    "homesteadBlock": 1,
    "eip150Block": 2,
    "eip150Hash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
    "eip155Block": 3,
    "eip158Block": 3,
    "byzantiumBlock": 4,
    "ethash": {}
  },
  "nonce": "0x0",
  "timestamp": "0x5b41b451",
  "extraData": "0x0000000000000000000000000000000000000000",
  "gasLimit": "0x47b760",
  "difficulty": "0x80000",
  "mixHash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
```

```
"coinbase": "0x0000000000000000000000000000000000000000",
"alloc": {
  "0000000000000000000000000000000000000000": {
    "balance": "0x1"
  },
  "0000000000000000000000000000000000000001": {
    "balance": "0x1"
  }
},
"number": "0x0",
"gasUsed": "0x0",
"parentHash": "0x0000000000000000000000000000000000000000"
}
```


- za inicijalizaciju privatnog blockchaina, izvršava se geth naredba:
  geth --datadir /user/Amjad/Test/miner1 init Test.json
- zatim se kreira nalog za svaki čvor gdje svaki nalog ima privatni i javni ključ i indeksiran je svojom adresom, koja je izvedena iz poslednjih 20 bajtova javnog ključa:
  geth --datadir /user/Amjad/Test/miner1 account new
- da bi se pokrenuo geth na svakom čvoru, izvršava se naredba koja uključuje različite zastavice za različite funkcionalnosti:
  geth --networkid 4224 --mine --minerthreads 2 --datadir "." --nodiscover --rpc --rpcport "8543" --port "30304" --ipcdisable --rpccorsdomain "*" --nat "any" --rpcapi admin,eth,web3,personal,net --unlock 0 --password ./password.sec
- zbog ograničenog broja čvorova koji se koriste u prikazanom okviru, nema potrebe za korišićenjem mehanizma otkrivanja za uparivanje čvorova. Datoteka static-nodes.json se koristi za uparivanje čvorova:
  admin.addPeer("enode://5f1d23c79a9bd7505469ed524047d276ad3a5964db763ae4e5c13a53326b9f492e7a02367f8e5c350a960e08bed1604e6860262b9013cf7c0c70aad9f91c1094$@[::]:30303?discport=0")
- posljednji korak se ponavlja da se dodaju dva Raspberry Pi-ja kao čvorovi kako bi se dobio privatni blockchain sa potpuno sinhronizovanim čvorovima.

Eksperiment koji su Kašlan i saradnici sproveli za konfiguraciju privatnog blockchain-a sa Raspberry Pi uređajima i Windows računarima sadrži nekoliko kritičkih aspekata. Prvo, upotreba Raspberry Pi uređaja kao Ethereum čvorova i rudara može doneti izazove u pogledu performansi i kapaciteta. Raspberry Pi uređaji su poznati po svojoj ograničenoj procesorskoj moći, memoriji i skladištenju, što može uticati na brzinu i efikasnost izvršavanja transakcija i rudarenja.

Drugo, konfiguracija i postavljanje čvorova putem Windows PowerShell komandi, izrada naloga i povezivanje čvorova putem JSON datoteka može biti tehnički zahtjevno i zahtijevati duboko razumijevanje Ethereum platforme. Ovo može predstavljati prepreku za prosečnog korisnika koji želi implementirati blockchain rešenja u okruženju pametnih kuća.

Takođe, eksperiment se izvodi u kontrolisanom okruženju sa malim brojem čvorova. U stvarnom svijetu, gde bi se koristila veća mreža čvorova i uređaja, administracija i upravljanje takvim privatnim blockchain-om može postati znatno složenija i zahtijevati dodatne mjere zaštite, uparivanje i održavanje.

Ovo istraživanje naglašava potrebu za daljim radom kako bi se otklonili tehnički izazovi i pojednostavila implementacija blockchain rješenja u okruženju pametnih kuća, kako bi se omogućila praktična primjena i upotreba.

3.2.2.3. Razvoj i implementacija pametnog ugovora

Kašlan i saradnici (Qashlan, Nanda & He, 2020) koristili su Remix pretraživač. Za ugovor o nadzoru definisane su dvije glavne funkcije: *setValue()* i *getValue()*. Samo vlasnik kuće može postaviti vrijednost temperature, tako da se modifikator koristi za ograničavanje upotrebe funkcije za postavljanje na adresu vlasnika kuće. Bilo koji drugi čvorovi mogu zatražiti vrijednost temperature pozivanjem funkcije get, koja će vratiti vrijednost temperature:

```
pragma solidity ^0.4.18;
contract Test {
   string public Sensor;
   address owner;
   function Test() public {
      owner = msg.sender;
   }
```

```
    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }
    event Value(string sensor);
    function setValue(string _Sensor) onlyOwner public {
        Sensor = _Sensor;
        Value(_Sensor);
    }
    function getValue() public constant returns (string) {
        return (Sensor);
    }
}
```

Ugovor o pristupu je razvijen da omogući svakom čvoru da pročita trenutnu vrijednost temperature. Ima samo jednu funkciju, koja poziva funkciju *getValue()* iz ugovora monitora na osnovu njene adrese. Stoga je nemoguće promijeniti vrijednost jer će se čitati samo sa specifične adrese ugovora o monitoru (Qashlan, Nanda & He, 2020):

```
pragma solidity ^0.4.18;
contract Access {
    function getSensorValue(address addr) returns (string) {
        Test T = Test(addr);
        return T.getValue();
    }
}
contract Test {
    function getValue() returns (string);
}
```

Konačno, napravljen je jednostavan HTML korisnički interfejs za interakciju sa pametnim ugovorom koristeći web3.js. Prva korisnička interakcija se sastoji od preuzimanja vrijednosti temperature iz funkcije getValue() i formira jedno polje za unos vrijednosti koja će biti postavljena putem jQueryja iz polja za unos teksta (Qashlan, Nanda & He, 2020).

U oznaci head, Web3.js biblioteka je uvezena za povezivanje sa privatnim blockchain čvorovima. Zatim se u oznaci skripte upisuje kod za rad sa pametnim ugovorom. Web provajder je postavljen na lokalni host 8543. Metoda web3.eth.contract() je korišćena za kreiranje ugovora, prihvatajući parametar binarnog interfejsa aplikacije (ABI), koji omogućava da pozivamo funkcije i primamo podatke iz pametnog ugovora. ABI je kopiran iz Remix pretraživača gdje je napisan pametni ugovor. Zatim se stvarna adresa ugovora definiše na osnovu pridružene adrese ugovora u Remix-u (Qashlan, Nanda & He, 2020).

Drugi korisnički interfejs izrađen je kako bi simulirao stanje klima uređaja. On preuzima trenutnu temperaturu iz ugovora o pristupu koji poziva getValue() iz ugovora o monitoru. Svakih 5 sekundi očitavanje temperature se ažurira pozivanjem nove vrijednosti temperature. Na osnovu vrijednosti, biće poslano obavještenje o trenutnoj temperaturi i stanju AC (uključeno/isključeno) (Qashlan, Nanda & He, 2020).

Kašlan i saradnici su izveli eksperiment koji uključuje implementaciju pametnih ugovora za praćenje temperature u pametnim kućama i interakciju s njima putem korisničkog interfejsa. Iako je njihova metodologija valjana i eksperiment je koristan za demonstraciju osnovnih principa rada pametnih ugovora, postoje neki kritički aspekti koji se mogu istaći.

Prvo, eksperiment se zasniva na Solidity programskom jeziku za pisanje pametnih ugovora, što zahtjeva od korisnika duboko tehničko razumijevanje i znanje programiranja. Ovo ograničava širu upotrebu i usvajanje blockchain tehnologije u okruženju pametnih kuća, jer prosječni korisnici nisu obavezno tehnički vješti.

Drugo, eksperiment se izvodio u kontrolisanom okruženju s malim brojem čvorova i uređaja. U stvarnim pametnim kućama, koje mogu imati mnogo više uređaja i čvorova, postoji potreba za skalabilnošću i efikasnom administracijom. Takođe, bezbjednost i privatnost podataka korisnika predstavljaju važne izazove koji nisu detaljno razmatrani u eksperimentu.

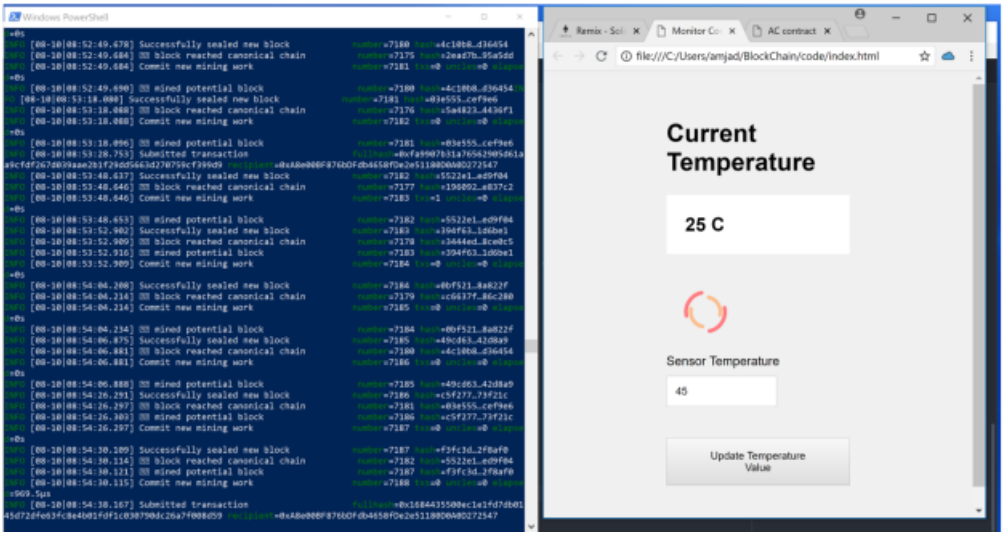
Naposletku, korisnički interfejs i način interakcije s pametnim ugovorima možda nisu intuitivni za prosečnog korisnika pametnih kuća. Ovo može predstavljati prepreku za usvajanje tehnologije. Stoga je važno da se nastavi sa istraživanjem kako bi se razvili korisnički prijateljski alati i rješenja koja bi olakšala upotrebu pametnih ugovora u stvarnom svijetu pametnih kuća.

3.2.3. Evaluacija prototipa

3.2.3.1 Primjeri za korisnički interfejs

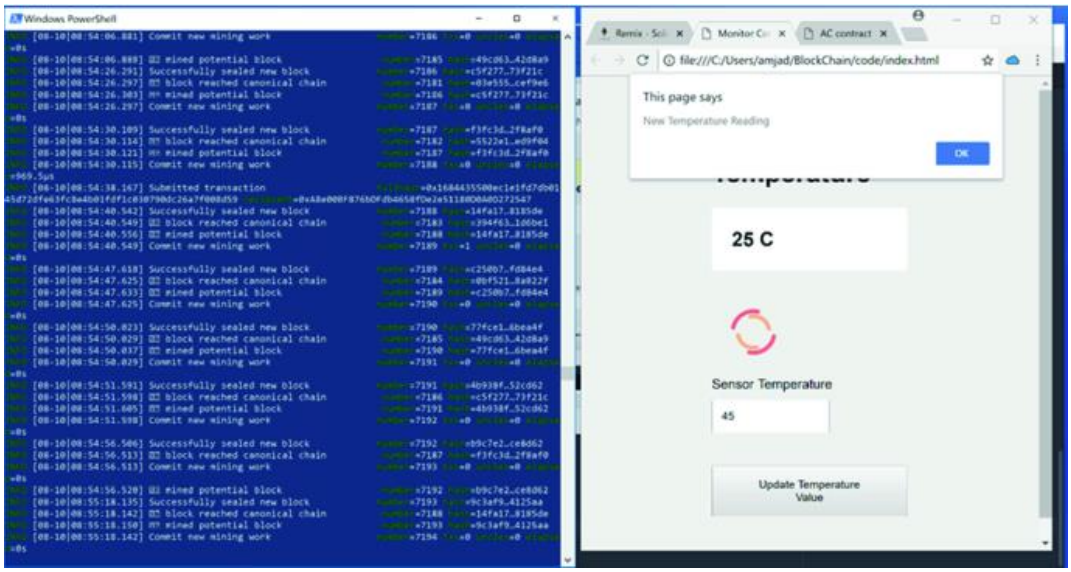
U nastavku su prikazani primjeri za korisnički interfejs (Qashlan, Nanda & He, 2020):

- Ugovor o monitoru prikazuje trenutnu vrijednost i minimum koji omogućava vlasniku kuće da postavi vrijednost. Kada se pritisne dugme Ažuriraj vrijednost temperature, rudar prima transakciju i počinje rudarenje, kao što je prikazano na slici 7;

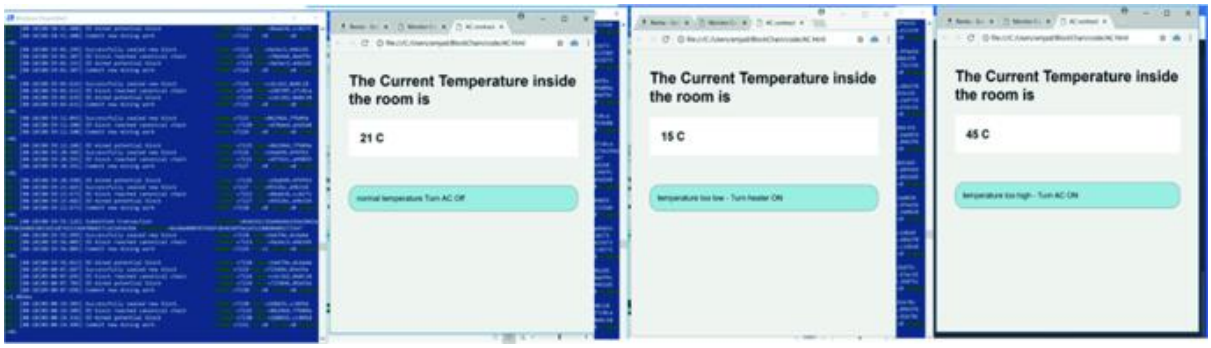


Slika 7 ***Vlasnik postavlja novu vrijednost temperature (Qashlan, Nanda & He, 2020)***

- Kada je transakcija rudarena, pojavljuje se upozorenje koje pokazuje da je vrijednost temperature promijenjena i da postoji novo očitavanje temperature;
- Korisnički interfejs ugovora o pristupu prikazuje trenutne temperature prostorije i stanje naizmjenične struje, kao što je prikazano na slici 8. Ažurira se svakih pet sekundi. Postavljaju se tri različita obavještenja na osnovu očitavanja temperature, kao što je prikazano na slici 9: ako je očitavanje temperature više od 30 ˚C klima uređaj će se će se uključiti u sistemu hlađenja; ako je manja od 20 ˚C, klima uređaj će se uključiti u režimu grijanja; u suprotnom, temperatura će biti normalna i klima uređaj će biti isključen.



Slika 8 ***Nova obavještenja o temperaturi (Qashlan, Nanda & He, 2020)***



Slika 9 *Trenutna temperatura u sobi (temeratura u prostoriji je normalna, temperatura u prostoriji je manja od 20 ˚C, temperatura u sobi je veća 20 ˚C od 30 ˚C (Qashlan, Nanda & He, 2020)*

Prikazani korisnički interfejsi i funkcionalnosti sistema djeluju obećavajuće, ali postoje određeni aspekti koji se moraju kritički razmotriti kako bi se osigurala praktična primjenjivost i efikasnost sistema.

Prvo, kada se govori o korisničkom interfejsu za ugovor o monitoru, čini se da je ovaj korak prilično tehnički orijentisan, gde korisnik treba da zna šta znači rudarenje i kako da ažurira vrijednost temperature. Ovakav interfejs može biti konfuzan za prosječne korisnike koji nisu upoznati sa blockchain tehnologijom i pametnim ugovorima. Jedan od ključnih izazova bio bi kako olakšati korišćenje ovih interfejsa za širu publiku. Istovremeno, interakcija s pametnim ugovorima putem dugmadi i obavještenja može biti neprecizna i manje efikasna u stvarnom svijetu. Korisnici pametnih kuća mogu zahtijevati praktičnije i

brže načine interakcije s uređajima, što može obuhvatiti upotrebu glasovnih asistenata, mobilnih aplikacija ili senzora za automatsko prilagođavanje postavki.

Drugo, korisnički interfejs za ugovor o pristupu ima složen proces ažuriranja temperature i upravljanja klima uređajem. Postavke za aktivaciju sistema hlađenja ili grijanja na osnovu očitavanja temperature možda zahtijevaju visok nivo tehničkog razumijevanja od strane korisnika. Poželjno bi bilo obezbjediti intuitivnije i jednostavnije korisničke interfejse kako bi se korisnicima olakšalo kontrolisanje njihovih uređaja i sistema.

Istovremeno, ažuriranje informacija svakih pet sekundi može opteretiti mrežu i resurse, naročito ako se radi o velikom broju pametnih uređaja u kući. Treba pažljivo razmotriti kako ovakva učestala ažuriranja utiču na performanse sistema, posebno u stvarnim kućnim okruženjima sa velikim brojem uređaja. Optimizacija za efikasnu komunikaciju između uređaja i sistema je ključna kako bi se izbjegli preopterećenje i kašnjenja u reakcijama na promjene u temperaturi.

Naposletku, korisnički interfejs ne uzima u obzir bezbjednost i privatnost podataka korisnika. Praćenje temperature i upravljanje uređajima u pametnoj kući zahtjeva pažljivu zaštitu podataka kako bi se sprečilo neovlašćeno pristupanje i zloupotreba informacija. Ovi aspekti trebaju biti bolje istraženi i implementirani u okviru pametnih kuća kako bi se osigurala sigurna i privatna upotreba tehnologije.

3.2.3.2. Evaluacija bezbjednosti

Tabela 1 sumira kako okvir koji su predložili Kašlan i saradnici (Qashlan, Nanda & He, 2020) postiže bezbjednosne zahtjeve o kojima se govorilo. Okvir koji su predložili Kašlan i saradnici (Qashlan, Nanda & He, 2020) oslanja se na Ethereum blockchain. Validirane transakcije smatraju se sigurnim i pretpostavlja se da korisnik čuva svoj privatni ključ sigurno.

Prema tome, samo vlasnik kuće ima kontrolu nad podacima blockchain-a. Potpisana digitalna transakcija i decentralizovana priroda blockchain-a garantuju da napadači ne mogu pristupiti mreži ili lažno predstavljati pravog korisnika. Napadači moraju steći kontrolu nad većinom mrežnih resursa ili lažirati digitalni potpis vlasnika kako bi kontrolisali čvorove. Osim toga, rudar u okviru sistema prihvata transakcije samo od čvorova kojima su dodjeljeni i privatni i javni ključ kada su dodani u privatnu mrežu (Qashlan, Nanda & He, 2020).

Uslov	Odbrana
Povjerljivost	Upotreba para privatnih i javnih ključeva
Integritet	Heš funkcija, algoritam digitalnog potpisa zasnovan na eliptičnim krivim i Merkle stablo
Dostupnost	Prihvataju se samo validirane transakcije rudara

Tabela 1 *Dostignuća u procjeni sigurnosti*

Blockchain kao što je Ethereum obično zahtjeva određeni broj potvrda od drugih čvorova. Ovo osigurava da je transakcija minirana i ispravno ugrađena u blockchain, stvarajući više svjedoka trećih strana kako bi se osigurala autentičnost transakcije. Čak i ako haker na neki način otme jedan čvor ili presretne instrukcije, pokazaće se nemogućim oteti sve to istovremeno i navesti mrežu da povjeruje da je uređaj isključen kada bi trebao biti uključen (Qashlan, Nanda & He, 2020).

Zbog pametnog ugovora koji djeluje kao vozilo za komandu, a radi to tek nakon višestrukih potvrda trećih strana, klima uređaj kojim se upravlja u ovom primjeru više ne zahijeva nikakvu eksternu pristupačnost, to može biti čvor samo za čitanje sa samo odlaznom vezom i da sinhronizira sa drugim blockchain čvorovima. Bezbjednost je postignuta provjerenim kriptografskim metodama, pri čemu privatni ključ omogućava kreiranje potpisa koji se ne može krivotvoriti, koji potom može provjeriti bilo koja treća strana kao originalan bez potrebe za pristupom privatnom ključu. Dakle, blockchain je zapravo sigurna baza podataka spojena s nizom programskih opcija, koje se nazivaju pametni ugovori. Pametni ugovor je jednostavno nekomplikovan kompjuterski program. Ovi kompjuterski programi se mogu podesiti da vjeruju samo instrukcijama od ovlašćenog čvora. Ovaj čvor se autentifikuje potpisom iz njihovog privatnog ključa, nešto što se može čuvati u potpunoj tajnosti. Dakle, slanje instrukcija u blockchain ne može ugroziti bezbjednost. Trenutno ne postoji dokazan način da napadač ometa poruku koja se šalje pametnom ugovoru, za razliku od klijent-server sistema sa centralnom bazom podataka i mnoštvom bezbjednosnih slojeva, svih potrebnih da se odbrani od napadača (Qashlan, Nanda & He, 2020).

Jedna dodatna bezbjednosna prednost je razdvajanje pisanja i čitanja od hardverskog prekidača. Staromodni sistem klijent-server mora uvijek zaštititi svoju bazu podataka koristeći slojeve bezbjednosti. Blockchain, naprotiv, širi svoje informacije po mreži. U

sistemu klijent-server može se napasti jedan čvor da bi se promjenilo stanje sistema. Da bi se isto postiglo u blockchain sistemu, bilo bi potrebno napasti i srušiti svaki pojedinačni čvor, što je praktično nemoguće (Qashlan, Nanda & He, 2020).

Tako su kućni IoT uređaji zaštićeni od zlonamjernih zahtjeva i DDOS napada. U stvari, DDOS napadi su jedan od kritičnih tipova napada koji su generalno relevantni za pametne kuće (Yakubu et al., 2023), što je tačka koju okvir koji su predložili Kašlan i saradnici (Qashlan, Nanda & He, 2020) efikasno rješava.

Prikazana sigurnosna analiza okvira koji su predložili Kašlan i saradnici (Qashlan, Nanda & He, 2020) ukazuje na njihovu sveobuhvatnu strategiju zaštite podataka i IoT uređaja korišćenjem Ethereum blockchain tehnologije. Njihova upotreba para privatnih i javnih ključeva za obezbjeđenje povjerljivosti, i implementacija heš funkcija, digitalnih potpisa i Merkle stabala za osiguranje integriteta podataka ukazuju na dobar nivo zaštite.

Istovremeno, mehanizmi za kontrolu pristupa i prihvatanje samo validiranih transakcija od strane rudara dodatno pojačavaju sigurnost sistema. Osim što se oslanjaju na provjerene kriptografske metode, oni koriste decentralizovani model koji otežava zlonamjernim akterima pristup mreži ili lažno predstavljanje korisnika. Čak i u slučaju napadača koji bi uspio oteti jedan čvor, okvir zahtijeva kontrolu nad većinom mrežnih resursa kako bi se ugrozila funkcionalnost sistema. To ukazuje na dobru sigurnosnu arhitekturu koja se ne oslanja samo na jedan sloj odbrane.

Osim toga, upotreba pametnih ugovora kao vozila za komandu, koji se aktiviraju tek nakon višestrukih potvrda trećih strana, povećava sigurnost upravljanja uređajima. Implementacija blockchain-a omogućava razdvajanje pisanja i čitanja podataka, što dodatno doprinosi bezbjednosti sistema. Dodatno, rješavanje problema DDOS napada koji su kritični za pametne kuće predstavlja važan aspekt zaštite.

Iako ovo predstavlja snažan okvir za sigurnost, važno je napomenuti da nijedan sistem nije potpuno neprobojan. Zahtijeva se neprekidno praćenje i ažuriranje sigurnosnih mjera kako bi se održala bezbjednost sistema u promjenjivom okruženju. Naime, iako predloženi okvir pruža efikasnu zaštitu od bezbjednosnih pretnji, postoji nekoliko ključnih aspekata koji se moraju kritički razmotriti kako bi se osigurala njegova praktična primjena.

Prvo, okvir se oslanja na korisnike da čuvaju svoje privatne ključeve sigurno, što može predstavljati izazov, jer se sigurnost privatnih ključeva može narušiti zbog nepažnje ili

napada. Iako se pretpostavlja da samo vlasnik kuće ima kontrolu nad podacima blockchain-a, potrebno je obratiti posebnu pažnju na edukaciju korisnika o sigurnom čuvanju privatnih ključeva.

Drugo, uprkos prednostima decentralizacije i potvrda od strane trećih strana u blockchain tehnologiji, potrebno je razmotriti situacije u kojima je neophodan brz pristup uređajima ili sistemima, naročito u hitnim situacijama. Prikazani okvir ističe da su neovlašćeni pristupi nemogući, ali može doći do problema u slučajevima kada je potrebna trenutna reakcija.

Naposletku, iako se okvir Kašlana i saradnika efikasno bavi DDOS napadima i pruža dodatnu bezbjednost putem pametnih ugovora, važno je konstantno ažurirati i nadograditi sistem kako bi se prilagodio novim bezbjednosnim pretnjama koje mogu nastati tokom vremena.

Zaključno, analizirani okvir za bezbjednost u pametnim kućama nudi značajne prednosti, ali zahtijeva pažljivo upravljanje privatnim ključevima, razmatranje hitnih situacija i kontinuirano praćenje bezbjednosnih pretnji kako bi se održala njegova efikasnost u stvarnom svetu.

4. IMPLEMENTACIJA BEZBJEDNOSTI I PRIVATNOSTI U PAMETNIM KUĆAMA: KONTROLA PRISTUPA ZASNOVANA NA ATRIBUTIMA I PAMETNI UGOVORI

Izgradnja pametne kuće sa integrisanom IoT mrežom pruža vlasnicima kuća rezultate kao što su povećana udobnost, bezbjednost i kvalitet života. Mreža pametne kuće je utemeljena na IoT infrastrukturi koja povezuje heterogene pametne uređaje (npr. pametne telefone, pametna brojila, nosive uređaje itd.). Sistemi pametne kuće mogu omogućiti i poboljšati sposobnost ljudi da žive samostalno. Oni uključuju skup neprocjenjivih tehnologija uključujući i one za praćenje i procjenu zdravlja, što ih čini privlačnim korisnicima i dizajnerima uređaja. Iako su prednosti pametnih kuća za vlasnike kuća i aktere (zainteresovane strane) dobro dokumentovane, nekoliko rizika se takođe mora uzeti u obzir, uključujući sajber napade i prijetnje bezbjednosti podataka i privatnosti korisnika (Philip, Luu & Carte, 2023).

Tradicionalni pristupi rješavanju takvih rizika oslanjaju se na centralizovane okvire koji su podložni sajber napadima. Stoga je funkcija kontrole pristupa važna za sprečavanje pristupa neovlašćenim korisnicima putem eksplicitnih ili impliciranih specifikacija i dozvoljavanje pristupa resursima samo ovlašćenim stranama. Kontrole pristupa su tradicionalno bile podržane centralizovanim sistemom kojim je relativno jednostavno upravljati. To znači da se centralni server koristi za obradu svih kontrola pristupa: naime, dodjeljivanje prava pristupa, upravljanje pristupom (npr. ažuriranja, opoziva) i provjere pristupa. Međutim, postoje rizici oko toga da server bude tačka kvara zbog prirodnih (funkcionalnih) ili eksternih (sajber napad) sila i potencijalnog kompromitovanja sistema kontrole pristupa. Nadalje, velika i distribuirana priroda IoT sistema znači da postoje poteškoće u vezi s kontrolom zahtjeva centralizovanim šemama za pristup željenom resursu (Al-Turjman, Zahmatkesh & Shahroze, 2022).

Distribuirane mreže kontrole pristupa mogu se suprotstaviti nekim od gore navedenih ograničenja centralizovanih mreža. Ove mreže obavljaju procese vezane za kontrolu pristupa koristeći više čvorova, a ne jedan server. Čvorovi se slažu o pravima koja će im se dodijeliti, politikama za pružanje pristupa i rezultatima verifikacije za pružanje čvrstih i pouzdanih kontrola pristupa koje mogu odoljeti zlonamjernim napadima. Kao rezultat toga, sve je veći

interes za korišćenje nove blockchain tehnologije za distribuiranu i pouzdanu kontrolu pristupa.

Pojava distribuiranih i otpornih na napade glavnih knjiga blockchain tehnika za zaštitu podataka otvorila je novu mogućnost za izazove privatnosti, sigurnosti i integriteta podataka u pametnoj kući. Blockchain se sastoji od digitalne knjige koja bilježi i dijeli informacije o transakcijama u mreži. Svaki korisnik ima pristup sigurnim kriptografskim javnim i privatnim ključevima za interakciju sa sistemom. Jedan korisnik može pokrenuti transakciju svojim ključevima, a ostali korisnici u mreži mogu je prihvatiti svojim ključevima. Jednom kada se čvorovi slože da izvorni korisnik posjeduje podatke koje traži, transakcija je prihvaćena; inače se odbija (Ratkovic, 2022).

Blockchain tehnologija postiže snažne performanse u nizu aplikacija za pametne kuće uključujući kontrolu pristupa domu, dijeljenje podataka i tako dalje. Implementacija blockchain-a u pametnim kućnim mrežama je opravdana i na osnovu toga što postoji nezavisno od trenutnih heterogenih protokola koji se često primjenjuju u pametnim kućama (npr. Z-Wave, Zigbee, Bluetooth i Thread) (Albany et al., 2022). Ipak, zbog visokog nivoa resursa koji se troše tokom rudarskih i konsenzusnih procedura i ograničenja resursa čvorova u pametnim kućnim uređajima, izazovno je koristiti blockchain direktno u pametnoj kući.

Blockchain radi kao okosnica predložene arhitekture. Krajnji korisnik pristupa uređaju kao čvoru blockchain-a. Funkcije kontrole pristupa spomenute u pametnim ugovorima koriste se za autentifikaciju čvorova. Sve ovo čini dio blockchain-a koji su Kašlan i saradnici (Qashlan, Nanda & He, 2020) istraživali i koji je detaljno predstavljen u prethodnom poglavlju, zajedno sa nivoom bezbjednosne podrške kroz implementaciju blockchain-a.

Rubno računarstvo nudi alternativnu i komplementarnu metodu za upravljanje PoW (*engl. Proof of Work*) zagonetkama i podršku blockchain aplikacijama u pametnoj kući. Rubno računarstvo se odvija na krajevima mreže (ivicama) proširenjem distribucije resursa i usluga zasnovanih na oblaku. Podržava sistem višestrukog pristupa za korisnike da pristupe uslugama sličnim oblaku za poboljšano računarstvo, aplikacije i skladištenje. Pametni kućni uređaji sa ograničenim resursima mogu posljedično povećati svoje računarske sposobnosti prenošenjem rudarskih i skladišnih poslova na rubne servere. Inkorporacija blockchain-a i rubnog računarstva postavlja decentralizovani sistem za autsorsing računanja i bezbjednost

skladištenja koja se odnosi na skalabilne i bezbjednosno dokazane operacije (Xue et al., 2023).

4.1. Kontrola pristupa, ERC-20 token i rubno računarstvo

4.2.1 Šema kontrole pristupa

Sistemi kontrole pristupa se tradicionalno zasnivaju na listama kontrole pristupa, koje korisnicima daju dozvole za pristup. Kada se poveća broj korisnika koji traže resurse, listama kontrole pristupa postaje teže upravljati. Kao rješenje za ovo ograničenje sistema liste kontrole pristupa, dizajneri su kreirali sisteme kontrole pristupa zasnovanog na ulogama koji dodaju međusloj u proces distribucije dozvola za uloge umjesto da ih direktno daju korisnicima i zatim im dodijele svoje uloge. Ova strategija može značajno smanjiti vrijeme i trud potreban za praćenje pravila kontrole pristupa. Ovo važi čak i kada se poveća broj uloga i resursa subjekta, ili kada sistem sadrži mnogo administrativnih polja (Gai et al., 2022). Sistemi kontrole pristupa zasnovani na atributima pokušavaju da riješe probleme povezane sa povećanjem broja uloga dozvoljavajući korisnicima da direktno primjene atribute subjekta, kao i svojstva resursa i okoline. Ovo se može učiniti kako bi se opisale politike pristupa i, kao rezultat, smanjiti broj pravila ili ažuriranja pravila. Sa druge strane, kontrola pristupa zasnovanu na atributima još uvijek treba pristupiti dosljednom opisu atributa polja i definiciji atributa u mnogim poljima (Liang et al., 2022).

Istraživanje koje su sproveli Vang i saradnici (Wang et al., 2022b) je pokazalo primjenjivost šifrovanja zasnovanog na atributima za dijeljenje informacija iz dnevnika revizije i šifrirovanja emitovanja. U ovom scenariju, podaci se skladište na serveru u šifrovanom obliku dok je različitim korisnicima i dalje dozvoljeno da dešifruju različite dijelove podataka u skladu sa svojom bezbjednosnom politikom. Ovo efektivno eliminiše potrebu da se oslanjate na server za skladištenje da biste sprečili neovlašćeni pristup podacima (Wang et al., 2022b). Štaviše, Hu i saradnici (Hu et al., 2023) su objavili vodič za kontrolu pristupa atributima sa definicijom kontrole pristupa zasnovane na atributima i 149 opisa funkcionalnih komponenti kontrole pristupa zasnovane na atributima. Takođe, vodič pruža razmatranja planiranja, dizajna, implementacije i rada za korišćenje kontrole pristupa zasnovane na atributima u velikom preduzeću sa ciljem poboljšanja razmjene informacija uz zadržavanje kontrole nad tim informacijama (Hu et al., 2023). Nadalje, kontrola pristupa zasnovana na atributima je korišćena u blockchain arhitekturi. Autori su predstavili novu platformu za upravljanje digitalnom imovinom, nazvanu DAM-Chain, sa kontrolom pristupa

zasnovanom na povjerenju koja integriše distributivni model kontrole pristupa zasnovane na atributima i blockchain tehnologiju (Sajid Ullah et al., 2023). Oni uzimaju transakcije kao most za integraciju kontrole pristupa zasnovane na atributima i blockchain-a u novu platformu za distribuciju i dijeljenje resursa. Tvrde da njihova predložena platforma podržava fleksibilno i raznoliko upravljanje dozvolama, kao i provjerljiv i transparentan proces autorizacije pristupa u arhitekturi zasnovanoj na blockchain-u.

Drugi predlažu distribuirani sistem kontrole pristupa zasnovane na atributima zasnovan na blockchain-u kako bi se omogućila pouzdana revizija pokušaja pristupa. Pored mogućnosti revizije, ovaj sistem predstavlja nivo transparentnosti od kog mogu imati koristi i podnosioci zahtjeva za pristup i vlasnici resursa. Oni predstavljaju arhitekturu sistema sa implementacijom zasnovanom na Hyperledger Fabric-u, postižući visoku efikasnost i niske računske troškove. Oni su potvrdili svoje rješenje kroz aplikaciju za upravljanje decentralizovanom kontrolom pristupa u digitalnim bibliotekama (Liao, 2022).

Ovo poglavlje posebno ispituje kontrolu pristupa zasnovanu na atributima jer se smatra odgovarajućim decentralizovanim modelom za postavljanje IoT-a i pruža skalabilnost, fleksibilnost i snažnu dinamiku. Šema kontrole pristupa koja će biti detaljno analizirana u poglavlju 4.3. a koju su razvili Kašlan i saradnici (Qashlan et al., 2021) razlikuje se od ostalih prijavljenih radova, u kojima su autori koristili tri vrste procedura za kontrolu pristupa: kontrolu pristupa uređaj-uređaj (D2D), kontrolu pristupa uređaj-korisnik (D2U) i kontrolu pristupa uređaj-server magle (D2FS) kako bi autentifikovali korisnike u Internetu svega (IoE) (Bera et al., 2020). Kontrola pristupa koju su razvili Kašlan i saradnici (Qashlan et al., 2021) zasniva se na različitim politikama koje kombinuju skup subjekata (korisnika), skup objekata (IoT uređaja) i skup radnji koje navode da taj i taj korisnik može izvršiti određenu radnju na IoT uređaju. Politika se poziva kad god postoji zahtjev za pristup od bilo kojeg korisnika ili uređaja u mreži koji koristi pametni ugovor. Štaviše, integrisan je mehanizam tokena za dalje finalizovanje dozvola za pristup IoT uređajima. Pametni ugovor provjerava politike, zatim prati količinu tokena i kome pripada određeni token i koliko"ga treba koristiti za pristup određenom IoT uređaju.

4.2.2. ERC-20 token

ERC-20 je skraćenica od Ethereum Request for Comments, a broj 20 služi kao jedinstveni identifikator koji ga razlikuje od ostalih standarda. Tokeni ERC-20, što znači

Ethereum zahtjev za komentar 20, predstavljaju standard za zamjenjive tokene na Ethereum blockchainu. Zamjenjivi tokeni su međusobno zamjenjivi, što znači da jedna jedinica tokena ima istu vrednost i funkcionalnost kao druga jedinica istog tokena (Shirole, Darisi & Bhirud, 2020).

Standard ERC-20 definiše niz pravila i funkcija koje moraju da se pridržavaju tokeni bazirani na Ethereum-u, što osigurava da različiti tokeni mogu međusobno da komuniciraju i koriste se u različitim decentralizovanim aplikacijama i uslugama na dosledan i predvidljiv način. Kao tehnički standard, ERC-20 je postao jedan od najvažnijih i naširoko korišćenih tokena za sve pametne ugovore na Ethereum blockchain-u. ERC-20 definiše skup od šest funkcionalnosti unutar Ethereum sistema u korist drugih tokena (Bauer, 2022):

- *totalSupply():* da shvatite koliko je tokena kreirano i postoji u sistemu;
- *balanceOf(vlasnik adrese):* da vratite broj tokena na računu za datu adresu;
- *allowance(vlasnik tokena adrese, potrošač adrese):* stanje korisnika je jedan od najkritičnijih podataka potrebnih za završetak transakcije. Da bi izvršio transakciju, korisnik mora imati određeni broj tokena. Ako korisnik nema potreban broj tokena, funkcija *allowance()* koristi se za otkazivanje transakcije;
- *approve(potrošač adrese, tokeni jedinice):* vlasnik ugovora dozvoljava prikupljanje potrebne količine tokena sa adrese ugovora nakon što korisnik ima potreban broj tokena za transakciju i provjerava stanje. Upoređujući transakciju sa ukupnom zalihom tokena, ova funkcija osigurava da nema dodatnih ili nedostajućih tokena;
- *transfer(adresa na, tokeni jedinice):* ova funkcija *transfer()* omogućava vlasniku ugovora da pošalje tokene. Omogućava vlasniku ugovora da prenese određeni broj tokena na druge adrese. Takođe omogućava prenos određenog broja tokena između ukupne ponude i korisničkog računa;
- *transferFrom(adresa od, adresa do, uint256 tokenId*): vlasnik ugovora može prenijeti tokene koristeći *transfer()* funkciju. Ova funkcija omogućava vlasniku ugovora da pošalje iznose tokena na različite adrese. Takođe, omogućava prenos određenog broja tokena iz cjelokupne ponude na korisnički račun.

Važno je napomenuti da, iako tokeni ERC-20 dele zajedničke funkcionalnosti, pojedinačni tokeni mogu imati dodatne karakteristike ili varijacije iznad standarda. Tokeni ERC-20 se ponekad nazivaju kripto sredstvima ili kripto tokenima na Ethereum mreži.

4.2.3. Rubno računarstvo

Sposobnost računarstva u oblaku da obezbijedi neograničenu obradu, skladištenje podataka i resurse sistemske administracije dovela je do razvoja mnogih aplikacija zasnovanih na oblaku i brze ekspanzije internet korporacija, kao što je Amazon, poslednjih godina.

Trend je nedavno bio premještanje funkcija oblaka na rubove mreže. Ovo zavisi od aplikacija koje su osetljive na kašnjenje (na primjer, virtuelna stvarnost) sa strogim zahtjevima za kašnjenje. Rubno računarstvo je izvršilo veći pritisak na resurse i usluge u oblaku kako bi se osigurala mobilnost, otkrivanje lokacije i manje kašnjenje. Kao rezultat ovih prednosti, tehnologija ruba mreže je ključna za realizaciju budućnosti IoT-a (Khanh et al., 2022).

Rubna računarska struktura ima tri nivoa: krajnji uređaj (front-end), rubni server (near-end) i jezgro oblaka (far-end). Hijerarhija na tri nivoa prikazuje računarski kapacitet elemenata kao i njihove karakteristike rubnog računarstva. Senzori i aktuatori na prednjem dijelu pružaju dodatnu i poboljšanu reakciju korisnika. Zahtjevi za resursima moraju biti proslijeđeni serveru, međutim, s obzirom na njihov ograničen kapacitet, serveri na bliskim rubovima upravljaju većinom mrežnog prometa i raznim potrebama za resursima (kao što je obrada podataka u realnom vremenu i rasterećenje računanja). Kao rezultat implementacije rubnih servera, krajnji korisnici imaju koristi od poboljšanih performansi računanja po cijenu povećanog vremenskog kašnjenja. Daleki serveri u oblaku pružaju veću snagu obrade (npr. analitiku velikih podataka) i dodatni prostor za skladištenje podataka. Cilj ove arhitekture sistema je da omogući rubnoj mreži da podrži računarski intenzivne i vremenski kritične aplikacije. Nadalje, određene rubne serverske aplikacije nude sinhronizaciju podataka putem komunikacija u oblaku (Kong et al., 2022).

4.2. Arhitektura pametne kuće zasnovana na blockchain-u

Bezbjednost i privatnost podataka sa IoT uređajima u pametnom domu jedan je od glavnih izazova jer su povezani IoT uređaji ranjivi na razne napade i nedostaju im osnovne bezbjednosne karakteristike. Za rješavanje ovih problema predložena su brojna centralizovana rješenja (Debnath et al., 2022). Istraživači predlažu informaciono orijentisanu mrežnu sistem za usluge pametnih kuća sa trostranom arhitekturom, tačnije udaljeni oblak,

sloj magle sa pametnim kućnim serverima i krajnjim uređajima (Padmanaban et al., 2023). Platforma omogućava implementaciju sistema u realnom vremenu, uključujući aplikacije za pametno praćenje i kontrolu. Drugi okvir predlaže integrisane postojeće komponente IoT arhitekture. Ovi autori su se bavili izazovima i rješenjima IoT pametnih kuća kako bi premostili jaz između trenutnih najmodernijih aplikacija za pametne kuće i mogućnosti njihove integracije u svijet koji je omogućen IoT-om (Philip et al., 2023). San i saradnici (Sun et al., 2016) predstavljaju viziju pametnih i povezanih zajednica. Oni integrišu IoT sa sajber-fizičkim računarstvom u oblaku i Big data za pametni turizam kako bi poboljšali očuvanje zajednice, životnost, revitalizaciju, dostupnost i bezbjednost. Međutim, sav ovaj rad je zasnovan na centralnoj arhitekturi, gdje su glavni izazovi komunikacija i procesiranje, kontrola pristupa i jedna tačka kvara. Stoga su različiti istraživači usmjerili svoju pažnju na distribuirane okvire i predložili popularna rješenja zasnovana na blockchain-u za različite slučajeve upotrebe IoT-a (Sun et al., 2016).

4.2.1 Blockchain autentifikacija, kontrola pristupa i rubno računarstvo u aplikacijama za pametne kuće

Blockchain autentifikacija, kontrola pristupa i rubno računarstvo igraju ključnu ulogu u poboljšanju sigurnosti i funkcionalnosti aplikacija za pametne kuće (Li et al., 2020):

1. Blockchain autentifikacija – Upotreba blockchain tehnologije za autentifikaciju korisnika i uređaja u pametnim kućama pruža visok nivo sigurnosti. Svaki korisnik i pametni uređaj može imati svoj digitalni identitet na blockchain-u, koji se može koristiti za provjeru pristupa i autorizaciju. Ovo osigurava da samo ovlašćeni korisnici i uređaji mogu komunicirati s kućnim sistemima. Blockchain takođe omogućava transparentnost i neporecivost identiteta, sprečavajući potencijalne zloupotrebe;
2. Kontrola pristupa – Pametne kuće često imaju različite zone i uređaje koje treba zaštiti od neovlašćenog pristupa. Blockchain tehnologija može se koristiti za strogu kontrolu pristupa putem pametnih brave, senzora i kamere. Samo korisnici s odgovarajućim ovlašćenjima na blockchain-u mogu otključati vrata ili pristupiti određenim prostorijama. To pruža viši nivo sigurnosti od tradicionalnih ključeva i lozinki;
3. Rubno računarstvo – Rubno računarstvo je ključno za aplikacije pametnih kuća jer omogućava lokalno procesiranje podataka na samim uređajima ili na rubu mreže, umesto slanja svih podataka u oblak. Ovo smanjuje latenciju i povećava brzinu

reakcije sistema za pametne kuće. Blockchain može poslužiti za sigurno skladištenje i razmjenu podataka između uređaja na rubu mreže, čineći ih otpornim na potencijalne napade ili ometanja;

4. Neporecivost podataka – Blockchain pruža neporecivost podataka, što znači da se jednom zapisani podaci ne mogu promjeniti ili izbrisati bez konsenzusa mreže. Ovo je posebno važno u aplikacijama za pametne kuće jer osigurava da podaci o sigurnosti, temperaturi, i drugim aspektima kuće ostanu nepromjenjeni i pouzdani.

Kombinacija blockchain autentifikacije, kontrole pristupa i rubnog računarstva unapređuje sigurnost i efikasnost aplikacija za pametne kuće, omogućavajući korisnicima da upravljaju svojim domovima na pouzdan i inovativan način.

U svom istraživanju, Li i saradnici (Li et al., 2020) bavili su se zabrinutošću oko mrežnih prolaza ili veza između IoT uređaja, tvrdeći da takvi centralizovani aranžmani predstavljaju nekoliko bezbjednosnih rizika kao što su integritet, sertifikacija i dostupnost. Autori su odgovorili tako što su predložili mrežu mrežnih prolaza zasnovanu na blockchain-u koja može da zaštiti od potencijalnih napada mrežnih prolaza. Mreža blockchain tehnologije, koja se sastoji od tri sloja: uređaja, mrežnih prolaza i oblaka, koristi se na sloju mrežnog prolaza da bi se olakšala decentralizacija skladištenjem i razmjenom blokova podataka. Ovo održava integritet podataka kako unutar tako i izvan pametne kuće i dostupnost kroz autentifikaciju i komunikaciju između korisnika mreže. Sa druge strane, njihova arhitektura ima neka ograničenja u smislu složenosti računara nametnuta blockchain operacijama na mrežnim prolazima.

Prednosti upotrebe Ganache, Remix i web3.js arhitekture za pametni kućni IoT blockchain za prevazilaženje poteškoća u pogledu privatnosti podataka, kontrole pristupa povjerenju i mogućnosti proširenja sistema zagovarali su Dang i Ngujen (Dang & Nguyen, 2018). Oni predstavljaju IoT mrežni prolaz za povezivanje klastera IoT uređaja pametne kuće na blockchain mrežu. Njihov rad je komplikovan činjenicom da svaki korisnik i IoT uređaj moraju biti dodijeljeni jednom i samo jednom paru subjekt-objekat zbog činjenice da mrežni prolaz možda nema dovoljno snage računara za rukovanje velikim transakcijama (Dang & Nguyen, 2018).

U svom radu, Xu i saradnici (Xue, Xu & Zhang, 2018) predstavili su privatni pristup kontroli pristupa zasnovan na blockchain-u za rješavanje problema bezbjednosti i privatnosti podataka dok koriste pametne uređaje u sistemima pametnih kuća. U okviru IoT sistema,

predloženi privatni pristup kontroli pristupa zasnovan na blockchain-u pruža „osnovu koja se ne može prevariti i koja se može revidirati“ koja može sprečiti neovlašćeni pristup podacima, zaštititi bezbjednost podataka od prijetnji i omogućiti tačan, robustan i trenutni pristup informacijama. Preporučili su samo jedan internet server kao administrator. Međutim, cio sistem propada ako je administrator neaktivan.

Sajng i saradnici (Singh et al., 2019) su predložili korišćenje pristupa zasnovanog na blockchain-u koji se zasniva na dokazu autoriteta za razvoj mehanizma konsenzusa za bolje upravljanje kućnim aparatima u decentralizovanom okviru. U poređenju sa standardnim sistemom zasnovanim na dokazu o radu, autori su demonstrirali dodatne funkcije za poboljšanje efikasnosti blockchain metode koristeći dokaz o autoritetu kao mehanizam konsenzusa za rešavanje bezbjednosnih problema.

Proučavana je implementacija IoT-a i multi-senzornih okvira zasnovanih na blockchain-u u kontekstu kvaliteta kvaliteta života kod kuće za pacijente kod kojih je nedavno dijagnostifikovan rak. Višestruki medicinski i ambijentalni inteligentni IoT senzori mogu uhvatiti podatke o kvalitetu života iz okruženja pametne kuće i bezbjedno ih podijeliti sa određenom zajednicom od interesa koristeći blockchain i off-chain okvir koji su predložili autori. Bezbjednosni nadzorni sistem kod kuće bilježi podatke o kvalitetu života, kao što su transakcioni zapisi i veliki podaci zasnovani na multimediji (npr. podaci o fiziološkom i mentalnom stanju), kojima autori mogu upravljati korišćenjem analitike podataka zasnovane na blockchain-u (Papachristou et al., 2023).

Dori i saradnici (Dorri et al., 2017b) predlažu IoT arhitekturu baziranu na blockchain-u koja smanjuje uticaj na IoT uređaje uz zadržavanje većine prednosti bezbjednosti i privatnosti tradicionalnog blockchain-a. Mreža sa preklapanjem može se kreirati korišćenjem uređaja s visokim resursima za korišćenje javnog distribuiranog blockchain-a koji osigurava privatnost i bezbjednost u svim fazama procesa transakcije. Nadalje, koristi distribuirano povjerenje kako bi pružila odličnu bezbjednost i privatnost za IoT aplikacije, a minimizira vrijeme potrebno za izvršenje validacije bloka. Međutim, nisu date nikakve informacije o uspostavljanju ovog skalabilnog blockchain-a ili bezbjednosnih certifikata (Dorri et al., 2017b).

U svom radu Ali i saradnici (Ali et al., 2020) implementirali su arhitekturu zasnovanu na IoT-u u tandemu sa *BC* (*Hiperledger Fabric*) da bi procijenili validnost komunikacionih uređaja da li su normalni ili zlonamjerni. Oni su testirali svoju šemu u scenariju pametne

kuće. Međutim, veličina transakcije u *Hiperledger Fabric*-u je veća od druge blockchain platforme jer takođe nose informacije o sertifikatu za odobrenje. Zbog toga se u njihovom scenariju latentnost pogoršava sa povećanjem veličine bloka.

Štaviše, u svom istraživanju Lin i saradnici (Lin et al., 2019) integrišu i blockchain i grupni potpis za anonimnu autentifikaciju članova grupe, kao i kod za autentifikaciju poruke za efikasnu autentifikaciju kućnog mrežnog prolaza bez curenja informacija u scenariju pametne kuće. U HomeChain-u, svi zapisi zahtjeva od članova grupe (ili zahtjevi za opoziv od menadžera grupe) će biti povezani u blockchain. Zbog nepromjenjivosti blockchain-a i sledljivosti grupnog potpisa, ove zapise nije lako manipulisati ili izbrisati, a samim tim i obezbjediti pouzdanu reviziju ponašanja. Međutim, autori izbjegavaju korišćenje bilo kakve politike kontrole pristupa, već samo usvajaju listu opoziva da bi opozvali ovlašćenja zlonamjernih korisnika.

Jutaka i saradnici (Yutaka et al., 2019) predlažu okvir kontrole pristupa zasnovane na atributima za IoT sisteme korišćenjem Ethereum tehnologije pametnih ugovora. Sistem se sastoji od četiri pametna ugovora koji upravljaju pravilima kontrole pristupa zasnovane na atibutima, atributima subjekta i objekta i kontrolom pristupa. Međutim, glavni nedostatak njihovog okvira je to što je prosječno vrijeme za kontrolu pristupa visoko zbog složenih interakcija između ugovora o kontroli pristupa i drugih pametnih ugovora za dohvat atributa i politika (Yutaka et al., 2019).

Zang i saradnici (Zhang et al., 2018) su razvili strukturu pametnog ugovora za distribuirane i pouzdane IoT sisteme kontrole pristupa. Predložena struktura uključuje brojne ugovore o kontroli pristupa, jedan ugovor sa sudijom i jedan ugovor o registru. Međutim, samo jednom kombinacijom subjekt-objekat upravlja jedan ugovor o kontroli pristupa. Veći trošak implementacije implicira sve veći linearni odnos između troškova gasa i broja parova subjekt-objekat sistema (Zhang et al., 2018).

Mora se priznati da je rad koji su predstavili prikazani istraživači ohrabrujući, međutim, postoje određena ograničenja u računskoj složenosti koji pokrivaju parametre kao što su troškovi računanja, vremenski zahtjevi, itd. U nastavku će biti analizirana odabrana šema koju su razvili Kašlan i saradnici (Qashlan et al., 2021) koja integriše šemu kontrole pristupa u okviru dva pametna ugovora raspoređena na serverima sa više ivica kako bi se postigao siguran distribuirani blockchain za opsluživanje pametnih kućnih IoT uređaja. Upotreba servera sa više ivica kao administratora pruža komplementaran način za

prevazilaženje troškova računanja i jedne tačke kvara. Takođe, analizirana je jedna od popularnih blockchain tehnologija, Ethereum pametni ugovor i generisanje tokena ERC-20, za implementaciju simulacije pametnih kućnih uređaja.

4.3. Primjer šeme kontrole pristupa zasnovane na atributima

Osnovne arhitektonske i dizajnerske karakteristike sistema zasnovanog na blockchain-u koji koji koristi Ethereum pametne ugovore za registraciju i upravljanje kućnim korisnikom, IoT pametnim kućnim uređajima i rubnim serverom predloženog od strane Kašlana i saradnika (Qashlan et al., 2021) opisane su u ovom odjeljku i dat je pritički osvrt na njih.

4.3.1. Arhitektura sistema

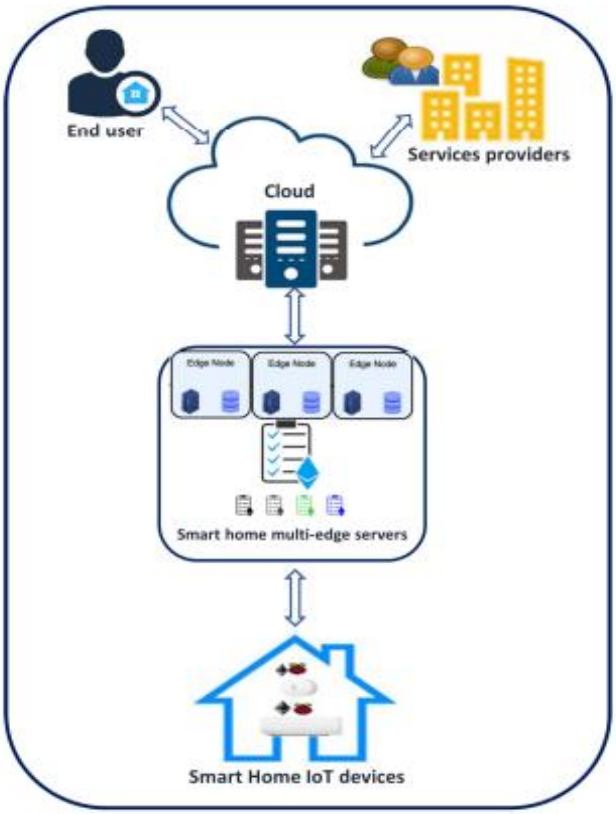
Arhitektura sistema koji su predložili Kašlan i saradnici (Qashlan et al., 2021) prikazana na slici 10 ima četiri osnovna učesnika, a svaki od njih ima pristup Ethereum pametnim ugovorima putem interneta. Ovi učesnici uključuju krajnje korisnike (kao što su kućni korisnici i korisnici usluga), pametne uređaje u kući (IoT uređaje), rubne servere i servere u oblaku. Svaki IoT uređaj u pametnoj kući ima svoju jedinstvenu Ethereum adresu koja uključuje javne i privatne ključeve. Svi drugi učesnici takođe imaju svoje Ethereum adrese i direktno komuniciraju sa pametnim ugovorima. Ova komunikacija se ostvaruje putem Ethereum klijenata za čvorove na rubu i u oblaku ili putem aplikacija/novčanika koje koriste krajnji korisnici. Ključne uloge različitih učesnika u sistemu su sažete u nastavku (Qashlan et al., 2021):

- Krajnji korisnik – Zahtijeva pristupnu dozvolu putem pametnog ugovora za pristup određenim pametnim kućnim uređajima:
    a) kućni korisnik: Korisnički uređaj (npr. računari, laptopi, pametni telefoni) je uređaj koji korisnicima omogućava pristup uslugama koje pružaju serveri (npr. praćenje trenutne temperature njegovog ili njenog doma);
    b) pristupnici usluga: Svi pružaoci usluga kao što su zdravstvena zaštita, policija ili druge strane kojima je potrebno da pristupe podacima pametne kuće kako bi pružili bilo koju vrstu usluge;
- IoT uređaji – Senzori i aktuatori su dva glavna tipa IoT uređaja u sistemu. Senzori mogu prikupiti podatke o sredini (kao što je temperatura) i poslati ih na rubne servere

ili uređaje za skladištenje za kasniju upotrebu. Sa druge strane, aktuatori mogu izvoditi operacije (kao što je uključivanje klima uređaja) kao odgovor na naredbu korisnika;

- Pametni kućni serveri sa više rubova – Rubni čvor je uređaj ili skup uređaja koji mogu komunicirati sa IoT uređajima i uređajima za skladištenje kako bi pružili različite usluge. Primjeri interakcija između servera i drugih kolega uključuju prikupljanje podataka o sredini sa senzora, izdavanje naredbi aktuatorima za obavljanje određenih aktivnosti i pristup ili upisivanje podataka na uređaje za skladištenje. Rubni čvorovi obrađuju sve dolazne i odlazne transakcije i koriste zajednički ključ za lokalnu komunikaciju sa IoT uređajima i lokalnim skladištem. Ovo održava pametne ugovore koji upravljaju registracijom krajnjih korisnika i IoT uređaja i provjerava autentičnost krajnjih korisnika za pristup IoT uređajima. Budući da IoT uređajima nedostaje dovoljna procesorska snaga, samo rubni serveri mogu izvršiti operaciju rudarenja;

  Oblak – Omogućava dugoročnu analizu i skladištenje podataka. Resursi u oblaku se takođe mogu konfigurisati kao čvorovi na blockchain-u kako bi se osigurala privatnost i integritet podataka u sistemu.



Slika 10 *Arhitektura sistema (Qashlan et al., 2021)*

Predložena arhitektura sistema za pametne kuće, iako ambiciozna u svom pristupu, nosi sa sobom nekoliko kritičnih izazova. Prvo, upotreba Ethereum blockchain-a za autentifikaciju i obradu transakcija može dovesti do problema sa skalabilnošću. Ethereum mreža je poznata po svojim ograničenim kapacitetima za obradu transakcija, što može dovesti do kašnjenja i visokih troškova transakcija, posebno u okruženju sa velikim brojem pametnih kuća i uređaja. Ovo ograničenje može negativno uticati na brzinu i performanse sistema. Drugo, kompleksnost arhitekture, sa različitim slojevima uključujući IoT uređaje, rubne servere, servere u oblaku i Ethereum blockchain, može povećati osjetljivost sistema na greške i sigurnosne ranjivosti. Svaki sloj sistema predstavlja potencijalnu tačku greške ili napada, i zahtjeva dodatne mere zaštite i sigurnosti kako bi se osigurala pouzdanost i integritet sistema. Nadalje, implementacija pametnih ugovora na Ethereum blockchain-u može biti složena i zahtijevati dodatne resurse za razvoj i održavanje. Ovo može povećati troškove implementacije i održavanja sistema za pametne kuće. Iako ova arhitektura obećava visok nivo sigurnosti i kontrole nad pametnim kućama, potrebno je pažljivo razmotriti navedene

izazove kako bi se osigurala funkcionalnost i efikasnost sistema. Balansiranje između sigurnosti, performansi i praktičnosti će biti ključno za uspjeh ovakvih kompleksnih sistema.

4.3.2. Kontrola pristupa zasnovana na atributima i pametni ugovori

Da bi pojednostavili kompleksnost jednog pametnog ugovora, predloženi okvir od strane Kašlana i saradnika (Qashlan et al., 2021) sastoji se od dva Ethereum pametna ugovora – ugovora o registru i ugovora o pristupu. Prvi ugovor ima ulogu čuvanja i upravljanja atributima subjekta i objekta, uključujući ažuriranje, dodavanje i brisanje tih atributa, kao i upravljanje politikama. S druge strane, ugovori o pristupu su odgovorni za kontrolu pristupa IoT uređajima. Oni generišu ERC-20 tokene i konačno odobravaju pristup IoT uređajima. Pametni ugovori su opisani na sledeći način (Qashlan et al., 2021):

1. Registrovanje ugovora – Pristupna politika je postavljena na blockchain radi registracije i upravljanja atributima korisnika i IoT uređaja. Samo administrator ima ovlašćenje za izvršenje ovog ugovora, kao što je prikazano u nastavku. Relevantan kod autori su objavili na GitHub-u:

```
pragma solidity ^0.5.0;
contract Add{
struct User {
uint256 id;
string name;
bool set;
}
address owner;
modifier onlyOwner() {
require(owner == msg.sender);
_;
}
mapping(address => User) public users;
function createUser(address _userAddress, uint256 _userId, string memory _userName) public onlyOwner {
User storage user = users[_userAddress];
require(!user.set);
```

```
users[_userAddress] = User({
id: _userId,
name: _userName,
set: true
});
}
function deleteUser(address user) public onlyOwner {
if (user.length < 2)
throw;
else {
uint i = 0;
while (i < user.length) {
if(user[i] == user) {
delete user[i];
userDeleted(user, msg.sender);
}
i++;
}
}
}
}
```

Svaki korisnik i IoT uređaj ima jedinstveni identifikator (Ethereum račun) i više atributa povezanih sa svojim identifikatorom sesije. Ovaj ugovor ima funkcionalnosti za upravljanje atributima subjekta i objekta, uključujući dodavanje, brisanje i ažuriranje. Korisnička struktura je kreirana kako bi sačuvala adresu novog korisnika. Takođe je uvedeno mapiranje. Unutar ugovora se koriste posebni modifikatori koji ograničavaju koje operacije korisnici mogu izvršiti. Na primjer, funkcija brisanja korisnika (*DeleteUser*) omogućava brisanje korisnika iz sistema. Međutim, ugovor će odbiti brisanje ako manje od dva korisnika ostane u sistemu i izbaci izuzetak. Autori su koristili jedan laptop uređaj za simulaciju rubnog servera koji pokreće dva rudara; stoga su najmanje dva korisnika potrebna da bi rudar nastavio sa radom. Ovaj ugovor

takođe definiše politiku koja je povezana sa svakim korisnikom i IoT uređajem na osnovu tipa korisnika, kao što je prikazanou nastavku:

```
contract RequestAccess {
   function checkAttrebute(addressOfUser)
   attribute my_at = attribute(addressOfUser);
   function GetPolicy(address0fUser)
   Policy my_po = Policy(addressofuser);
   if (my_at.checkAttrebute() == true & my_po.GetPolicy() == true)
      return my.sendToken()
   return FAILURE;
}
```

Politika je izjava koja kombinuje skup subjekata (korisnika), skup objekata (IoT uređaja) i skup radnji koje korisnik može izvršiti na IoT uređajima. Primjer politike prikazan je u okviru tabele 2;

Korisnički atributi	IoT atributi	Akcija
UserAddress	IoTAddress	izvršenje
UserType	IoTName	Čitanje
UserName	IoTFun	pisanje

Tabela 2 *Primjer korisničkih atributa, IoT atributa i dozvola*

2. Ugovor o pristupu – Ovaj ugovor upravlja zahtjevima korisnika (subjekta) za pristup IoT uređajima (objektu). Korisnik izvršava ovaj ugovor kako bi zatražio token koji mu omogućava komunikaciju sa objektom, kao što je prikazano u nastavku:

```
contract Attribute is ERC20Interface, Owned (
   string public Symbol;
   string public decimals;
   mapping (address => unit) balance;
   mapping (unit256 => AttributeData) checkAttribute;
   mapping (unit256 => Policy) GetPolicy;
   event Sendtoken (address from, address to, unit tokens)
   struct AttributeData {
```

```
        unit256 AttributeID;
        string Attribute;
        string approve;
    }
    struct Policy {
        unit256 PolicyID;
        string Policy;
        string approve;
    }
    function AttributeToken () public {
        balances [msg. sender]= 100 ;
        totalSupply = 100;
        name = "ACoin";
        decimals = 0;
        symbol = "A";
    }
    function checkAttribute (unit256 AttributeD, string Attribute, string approve) public returns (bool success) {
        checkAttribute[AttributeID]= AttributeData(AttributeID, Attribute, approve);
        return true;
    }
    function GetPolicy (unit256 PolicyID, string Policy, string approve) public returns (bool success) {
        GetPolicy[PolicyID] = Policy (PolicyID , Policy, approve);
        return true;
    }
    function sendToken (address to, unit tokens) public returns (bool success) {
        require (! frozenAccount[to]);
        emit sendtoken (msg. sender, to, tokens);
        return true;
    }
}
```

Ovaj ugovor uključuje funkcije za potvrđivanje atributa subjekta i proveru politike; ugovor o pristupu procenjuje da li subjekt ima pravo da izvrši akciju na objektu na osnovu primljene politike, a zatim šalje token subjektu. Ključne funkcije u ovom ugovoru uključuju *CheckAtribute(), GetPolicy()* i *TransferToken().* Ovaj ugovor takođe generiše ERC-20 tokene. Slika 11 ilustriruje kako koristiti određene funkcionalnosti ugovora o pristupu.Kako bi se sprečilo da važeći korisnik preplavi mrežu zahtevima za pristup, svaki korisnik ima određeni broj važećih tokena u isto vreme, što zavisi od tipa korisnika.

a) funkcija prenosa

b) funkcija potvrde

c) stanje tokena

Slika 11 ***Primjer izvršavanja funkcija ugovora o pristupu (Qashlan et al., 2021)***

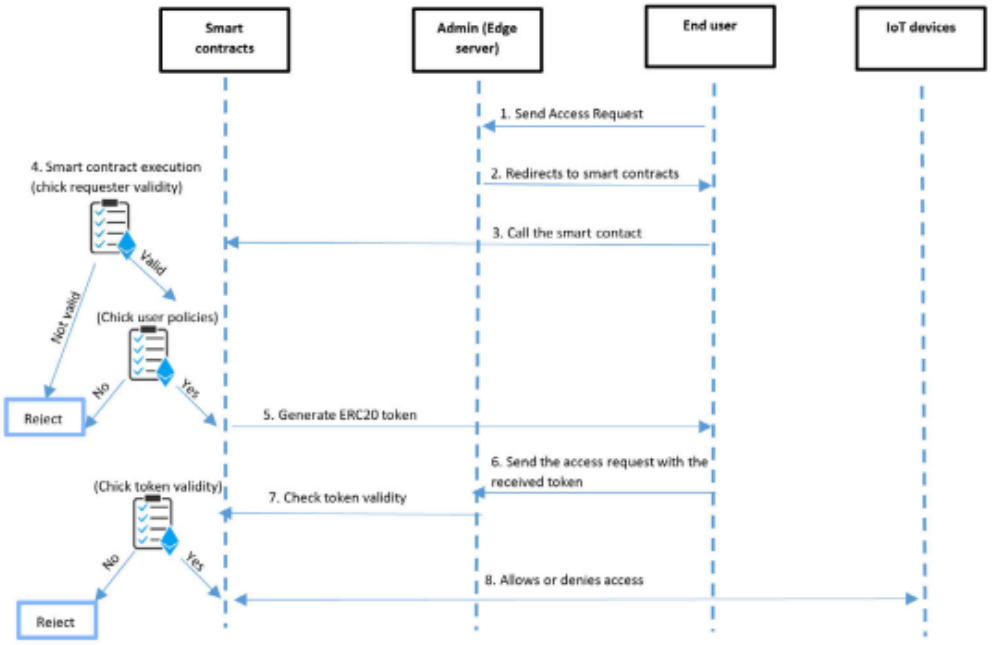
Predloženi okvir sistema za upravljanje atributima i pristupom IoT uređajima koristeći dva Ethereum pametna ugovora, uključujući ugovor o registru i ugovor o pristupu, djeluje kao potencijalno korisno rješenje za složene scenarije upravljanja. Međutim, postoje određeni aspekti ovog okvira koji zahtjevaju kritičku analizu. Prvo, koncept dva pametna ugovora može dodati složenost sistemu. Upravljanje odvojenim ugovorima, kao što je ugovor o registru za atribute i ugovor o pristupu za kontrolu pristupa, može zahtjevati dodatno razumijevanje i praćenje od strane korisnika i razvojnih timova. Ovo povećava potrebu za preciznim dokumentacijama i obukom kako bi se obezbjedilo da korisnici ispravno koriste sistem.

Drugo, ugovor o pristupu određuje broj i vrstu tokena koji su dostupni korisnicima, što se zasniva na tipu korisnika. Iako ovo pruža kontrolu nad pristupom uređajima, može se suočiti sa problemima skaliranja ako je potrebno rukovati sa velikim brojem korisnika sa različitim privilegijama. Trebalo bi pažljivo razmotriti kako se ovaj aspekt može skalirati na način koji održava efikasnost sistema.

Takođe, sistem izgleda kao da ima jake tehničke zahtjeve, uključujući upotrebu Ethereum blockchain-a i pametnih ugovora. To može otežati pristup i korišćenje sistema za korisnike koji nisu upućeni u tehničke aspekte blockchain tehnologije. Razmotriti kako se može pojednostaviti upotreba sistema i smanjiti tehničke prepreke za širi broj korisnika.

4.3.3 Dizajn sistema

Analizirani sistem omogućava korisnicima da se autentifikuju kroz upotrebu atributa i dodjeljivanje tokena. Na slici 12 prikazani su standardni postupci transakcija ugovora o pristupu zasnovanih na atributima uz ovaj sistem autentifikacije. Ovo omogućava korisnicima da na daljinu pristupe ili kontrolišu kućne uređaje pomoću novo generisanih tokena, čime se obezbjeđuje da samo onaj ko podnosi zahtjev može dobiti odgovor od legitimnog kućnog administratora (Qashlan et al., 2021).

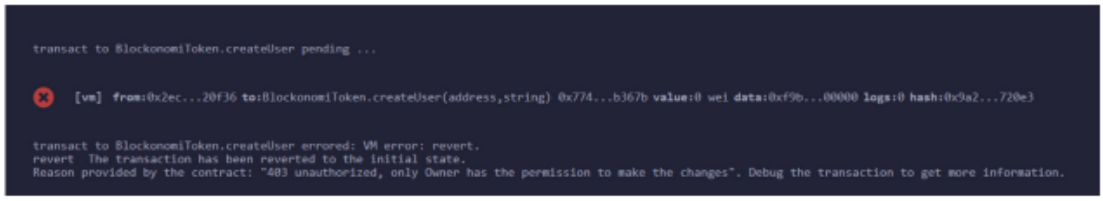


Slika 12 *Tipične transakcije u šemi (Qashlan et al., 2021*

U analiziranom sistemu, kako je opisano u radu Kašlana i saradnika (Qashlan et al., 2021), postoje četiri ključne faze:

1. Inicijalizacija – Početak sistema uključuje odabir administratora unutar porodične grupe kao ilustraciju. Administrator ima zadatak da pozove Register Contracts kako bi dodao ostale korisnike i IoT uređaje u sistem. Svaki korisnik dodjeljuje svoju Ethereum adresu i privatni ključ za potpisivanje transakcija. Ovo znači da svaki kućni administrator čuva grupni javni ključ za verifikaciju transakcija. Da bi se osiguralo da nema tačke kvara, administrator se izvršava na mnogo različitih rubnih čvorova putem rudara koji su povezani sa tim čvorovima;
2. Kontrola zahtjeva – Kada korisnik želi da zatraži pristup ili kontrolu kod kućnog administratora, generiše se token koji važi za određeno vrijeme i tačno vrijeme pristupa. Ovo je predloženi pristup kako bi se sprečili napadi ponavljanja i profilisanja. Nakon što korisnik dobije token pozivajući funkciju *TransferToken()* iz ugovora o pristupu, korisnik konstruiše transakciju prema svojim zahtevima. Na primjer, ako korisnik želi da sazna sobnu temperaturu, transakcija se obračunava nakon što korisnik bude preusmjeren na pametni ugovor i token zahtjeva. U okviru tog ugovora, tri glavne funkcije se pozivaju: *CheckAttribute(), GetPolicy(),* i *TransferToken()*. Korisnik šalje važeći token sa zahtjevom za pristup administratoru, i ako korisnik ima važeći token, pristup mu se odobrava. Slika 13 prikazuje ispravne i neispravne korisničke zahtjeve za pristup informacijama o temperaturi u sobi, kao što je prikazano na snimcima ekrana.

Samo korisnik sa validnim tokenom će biti dozvoljen da provjeri vrijednost senzora



Korisnik bez dovoljno tokena ili ako neregistrovani korisnik zahtjeva da provjeri temperaturu

Slika 13 ***korisnika za podatke o sobnoj temperaturi***

3. Dostava stanja – U ovoj fazi, kućni administrator pažljivo prati pametni ugovor kako bi primjetio nove zahtjeve kada korisnici traže novi pristup ili usluge. Kada se nova transakcija podnese i prođe proces verifikacije, kućni administrator provjerava validnost tokena koji je priložen sa zahtjevom. Na osnovu toga, administrator donosi odluku o odobravanju ili odbijanju pristupa IoT uređajima;
4. Lančana transakcija – U ovoj fazi, administrativni čvorovi, poznati kao rudari, imaju odgovornost da preuzmu transakcije iz pametnog ugovora i takmiče se međusobno kako bi prvi uspješno rešili dokaz rada radi dodavanja bloka u blockchain. Kako bi postigli konsenzus u mreži, rudari objavljuju svoje rješenje na blockchain nakon što uspešno riješe problem dokaza o radu. Nagrada za rudarenje, obično isplaćena u kriptovaluti kao što je Bitcoin, dodjeljuje se prvom rudaru koji uspješno izrudari blok koji zadovoljava konsenzus.

Sistem koji su razvili autori predstavlja značajan korak u obezbjeđivanju autentifikacije korisnika i upravljanju pristupom IoT uređajima putem distribucije tokena. Međutim, njegova složenost i tehnički zahtjevi mogu predstavljati izazove za širu upotrebu. Prvo, sistem je složen i sastoji se od četiri ključne faze sa nizom koraka, što ga čini zahtjevnim za razumijevanje i korišćenje, naročito za korisnike bez tehničkog znanja.

Drugo, korišćenje dokaza o radu za rudarenje blokova može izazvati pitanja skalabilnosti i energetske efikasnosti. Ovaj pristup može dovesti do usporavanja sistema i visokih energetskih troškova, što može otežati primjenu sistema u stvarnim kućnim okruženjima.

Takođe, pitanje skaliranja i sigurnosti mora se pažljivo razmotriti kako bi se zadovoljile potrebe većeg broja korisnika. S obzirom na da se sistem oslanja na Ethereum blockchain, potrebno je razmisliti o tome kako se nositi sa povećanjem broja korisnika i uređaja, a istovremeno održavati njegovu bezbjednost i efikasnost.

Nadalje, inicijalizacija sistema i sam proces dodavanja korisnika može biti složen i ručan, a zahtijeva preciznost i tehničko razumijevanje. Upotreba pametnih ugovora i konstrukcija transakcija može biti izazovna za korisnike koji nisu tehnički obučeni.

Konačno, dok sistem pruža visok nivo sigurnosti i kontrole pristupa, potrebno je pažljivo razmotriti kako se može pojednostaviti za korisnike i učiniti praktičnim za šire mase korisnika.

4.3.4. Implementacija

Prikazani sistem je izgrađen na privatnoj mreži koja koristi Ethereum blockchain. Ovaj model se izvodi na privatnoj Ethereum mreži, koja se sastoji od različitih uređaja i računara. Imamo jedan laptop uređaj tipa Dell XPS koji simulira rubni server, a na njemu su pokrenuta dva rudara. Osim toga, tu su i dva jednostruka računara Raspberry Pi 3 Model B, koji simuliraju temperaturne senzore i LED uređaje. Takođe, postoji još jedan laptop koji predstavlja kućnog korisnika. Rubni server je opremljen sa 4 nezavisna CPU jezgra i 16 GB RAM memorije. Jedno od CPU jezgara je namjenjeno rudarenju, dok se preostala jezgra koriste za podršku rubnom računarskom servisu. Kapacitet rudara uključuje CPU sa brzinom do 3,5 GHz, 8 GB RAM-a i skladišni prostor od 1 TB. Što se tiče Raspberry Pi uređaja, svaki od njih ima CPU brzine 1,2 GHz, 1 GB RAM-a i skladišni prostor od 32 GB, uz dodatne module za senzore temperature i LED uređaje. Laptop koji predstavlja kućnog korisnika raspolaže sa CPU brzine 2,2 GHz, 16 GB RAM-a i 256 GB skladišnog prostora (Qashlan et al., 2021).

U rubnom serveru, za rad s blockchain-om koristi se Go-Ethereum radni okvir, dok se za pisanje pametnih ugovora koristi Solidity programski jezik. Za razvoj pametnih ugovora

koristi se alat Remix integrisani razvoj. Remix takođe koristi Solidity jezik za kreiranje pametnih ugovora. Web3.js, odnosno Ethereum JavaScript API, ima svoju ulogu u modelu, koristi se za implementaciju i kompajliranje ugovora, kao i za praćenje stanja ugovora. Za interakciju s odgovarajućim geth klijentom putem HTTP veze koristi se JavaScript. Da bi omogućila interakciju između kućnih korisnika i uređaja, napravljena je jednostavna HTML web stranica. Na Raspberry Pi uređajima, koristi se lagana verzija Raspbian operativnog sistema, i Go-Ethereum je instaliran, čime je funkcija rudarenja blokova onemogućena. Što se tiče laptopa koji predstavlja kućnog korisnika, koristi se Windows 10 kućna verzija u 64-bitnoj arhitekturi. Na probnom okruženju, prvi laptop obavlja ulogu podrške za dva pružatelja usluga na rubu i rudara koji rješava zagonetku dokaza o radu. Raspberry Pi uređaji i drugi laptopi služe kao klijenti blockchain mreže, generišući i šaljući zahtjeve za resursima prema rubnom serveru. U ovom postavci, rubni server funkcioniše kao potpuni blockchain čvor, gdje čuva sve transakcije, izvršava unaprijed definisane pametne ugovore i kreira nove blokove. S druge strane, IoT uređaji djeluju kao lagani blockchain čvorovi, odgovorni za skladištenje podataka o transakcijama (Qashlan et al., 2021).

Konfiguracija privatnog blockchain-a preduzima niz koraka kako bi se postigao ispravan rad sistema. Prvo, odabire se kompatibilna verzija Ethereum-a. Zatim se koristi Windows PowerShell za pokretanje programa "geth", koji služi za upravljanje Ethereum blockchain-om. Svaki čvor mora zadovoljiti nekoliko zahtjeva prije nego što se može pridružiti blockchain mreži. Ovi zahtjevi uključuju: inicijalizaciju genesis datoteke (Test.json) koja kreira prvi blok u lancu; korištenje ID-a mreže kako bi se povezali s istim blockchain-om, i inicijalizaciju privatnog blockchaina putem "geth" naredbi. Za svaki čvor rudar stvara nalog s privatnim i javnim ključem i indeksira ga prema njegovoj adresi. To omogućava komunikaciju između čvorova i pametnih ugovora. Na svakom čvoru pokreće se "geth" s različitim zastavicama koje definišu različite funkcije. Da bi se sprečilo da spoljni napadači dobiju pristup čvorovima, postavlja se oznaka "no discovery" (bez otkrivanja) na svim čvorovima. Takođe, određene naredbe se koriste za preuzimanje ID-a čvora kako bi se omogućila sinhronizacija. Ovaj postupak se ponavlja kako bi se dodala dva Raspberry Pi uređaja kao čvorovi i laptop kućnog korisnika kako bi se stvorio privatni blockchain sa potpuno sinhronizovanim čvorovima (Qashlan et al., 2021).

U predloženoj arhitekturi, iako rubni server ima potpuni pristup svim funkcionalnostima sistema, ostali korisnici i uređaji IoT-a imaju ograničeno ovlašćenje za korišćenje određenih funkcija, kako je definisano putem pametnih ugovora. Ukoliko korisnik

ili ranjivi uređaji budu kompromitovani i iskorišćeni za izvođenje zlonamjernih aktivnosti, postavka sistema će umanjiti potencijalnu štetu.

Ovaj sistem ima niz izazova i nedostataka koje treba uzeti u obzir. Prvo, sistem se razvio na privatnoj mreži s vrlo specifičnim hardverskim konfiguracijama. Korišćeni uređaji, kao što su Raspberry Pi-jevi i Dell XPS, nisu tipični uređaji koje prosečni kućni korisnik ima na raspolaganju. Ovo čini sistem manje praktičnim za širu upotrebu, jer većina ljudi neće imati pristup ovakvom hardveru.

Drugo, iako je korišćena privatna Ethereum mreža za demonstraciju, nije jasno kako bi se ovaj sistem skalirao na stvarnim javnim Ethereum mrežama s velikim brojem korisnika i IoT uređaja. Kako bi se osigurala praktična primjena, potrebno je razmotriti kako će se sistem ponašati pod opterećenjem i kako će se rješiti problemi skalabilnosti.

Takođe, postavljanje privatnog blockchain-a i njegovo održavanje zahtijeva napredno tehničko razumijevanje, što ga čini manje pristupačnim za prosječne korisnike. Ovo može ograničiti širenje sistema i njegovu uspješnu primjenu u stvarnim kućnim okruženjima.

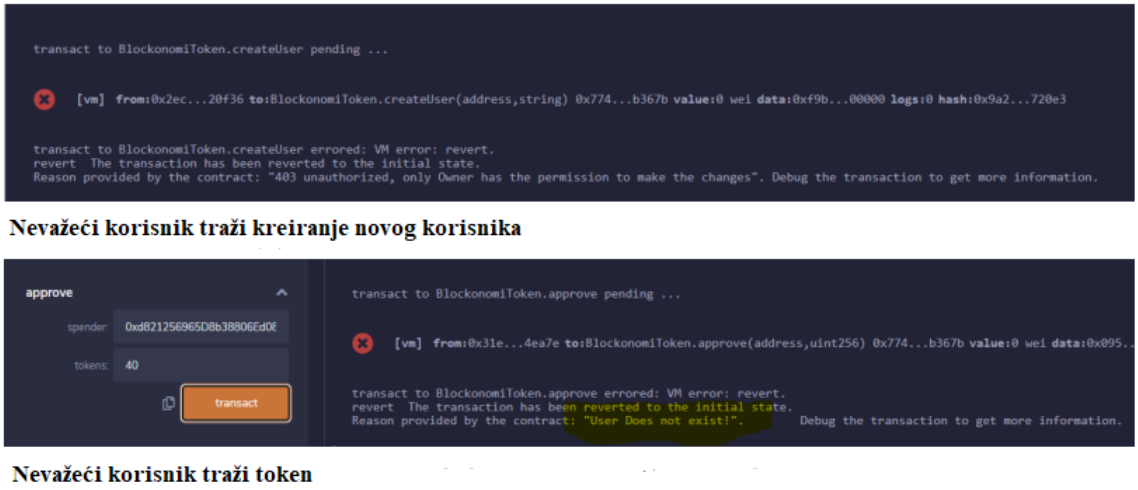
Naposletku, dok se naglašava sigurnost sistema, potrebno je obratiti pažnju na sve potencijalne ranjivosti i rizike vezane za upotrebu pametnih ugovora i distribuciju tokena. Važno je da se sistem neprestano nadgleda i ažurira kako bi se očuvala bezbjednost i zaštita korisnika.

4.3.5. Evaluacija bezbjednosti

Povjerljivost ima za svrhu garantovanje da neovlašćeni korisnici budu sprečeni u pristupu IoT uređajima i njihovim podacima, osiguravajući da se privatni podaci isporučuju isključivo određenim korisnicima. Jedan od načina za postizanje povjerljivosti je šifrovanje poruka putem SSL sesije nakon što korisnik bude uspešno autentifikovan (Yakubu et al., 2023). Kao jedna od snažnih karakteristika blockchain-a, okvir predložen od strane Kašlana i njegovih saradnika (Quashlan et al., 2021) dodjeljuje jedinstvene Ethereum adrese sa dužinom od 20 bajtova direktno ovlašćenim čvorovima, uključujući i IoT uređaje, bez gotovo ikakvih preklapanja. Ethereum adresa ima posebne parove javnih ključeva koji se mogu koristiti za uspostavljanje sigurne SSL sesije radi komunikacije između bilo kojeg autentifikovanog čvora, bilo da se radi o autentifikovanom korisniku ili IoT uređaju. Prilikom formiranja privatne mreže, rudar distribuira privatne i javne ključeve povezane sa Ethereum

adresama za svaki čvor. Senzor temperature ili LED uređaj, kao čvor koji šalje podatke, koristi privatni ključ za stvaranje digitalnog potpisa, omogućavajući da se tražena transakcija emituje preko cijele mreže.

Kad je riječ o dostupnosti, arhitektura koju su Kašlan i saradnici (Quashlan et al., 2021) predložili koristi inherentna svojstva blockchain tehnologije koja obezbjeđuje pouzdanost i robusnost. Zbog decentralizovane prirode blockchain-a i replikacije glavne knjige na više lokacija, rizik od jedne tačke kvara ne postoji, i svi podaci putuju kroz više čvorova. Kopija istorije transakcija čuva se u svakom administrativnom čvoru, što omogućava provjeru i povezivanje sa početnom transakcijom. Štaviše, da bi se povećala dostupnost pametnih kuća, IoT uređaji su zaštićeni od zlonamernih zahtjeva jer prihvataju samo transakcije od korisnika sa validnim tokenima. Dakle, svaka pristigla transakcija prođe autorizaciju od strane administratora prije nego što se proslijedi IoT uređajima.



Slika 14 *Poništi transakciju (Quashlan et al., 2021)*

Takođe, upotreba važećeg tokena povećava nivo bezbjednosti u prikazanoj arhitekturi. To se ogleda u činjenici da samo administratori mogu izdati ispravan token, i samo predviđeni korisnik može koristiti taj token. Slika 14 jasno pokazuje grešku povratka kada bilo ko, osim administratora, pokuša da stvori korisnika ili izda token. Takođe, vlasnik tokena ne može prenijeti taj token na druge korisnike, što znači da ako javni ključ korisnika bude kompromitovan, pametni ugovor sprečava prenos tokena. Administrator će dozvoliti da samo transakcije koje sadrže ispravan token povezan sa odgovarajućim korisnikom budu prihvaćene u mreži (Quashlan et al., 2021).

1. Napad uskraćivanja usluge (DoS) – U ovoj vrsti napada, napadač šalje veliki broj transakcija na cilj kako bi poremetio njegovu dostupnost. Upotreba pametnih ugovora za kontrolu pristupa zasnovanih na atributima u arhitekturi koju su predložili Kašlan i saradnici (Qashlan et al., 2021) smanjuje uticaj ovog napada, jer će biti prihvaćene samo autorizovane transakcije. Administrator mora pažljivo ispitati adresu i politiku za svakog korisnika i uređaj kako bi izdao ispravan token za slanje transakcija. Ukoliko administrator primjeti nekoliko neuspešnih zahteva za pristup od strane neovlašćenih entiteta, može blokirati takve transakcije i odbiti ih. Osim toga, politika se automatski primjenjuje putem pametnih ugovora. U slučaju da zlonamjerni spoljni entiteti kompromituju i preuzmu kontrolu nad IoT uređajima radi izvođenja zlonamjernih aktivnosti, kao što su kontinuirani zahtjevi za resursima ili izvođenje DoS napada, pametni ugovori će automatski sprovoditi predefinisane politike, kao što su ukupna dostava tokena, vrijeme pristupa i trajanje. Na primjer, u scenariju koji su autori predstavili, ukupan broj tokena je ograničen na 100 za svakog korisnika, i ako korisnici ili uređaji zahtijevaju pristup, ugovor za zahtev će izdavati samo određeni broj važećih tokena (jedan po jedan). Ako broj zahtjeva premaši raspoložive tokene, transakcija će biti odbijena (Qashlan et al., 2021).

Kašlan i saradnici (Qashlan et al., 2021) su kreirali prototip za simulaciju scenarija pametne kuće sa samo dva pametna uređaja radi testiranja njihove arhitekture. Međutim, u stvarnom svetu, ovakva mreža će imati više od jednog administratora i mnogo čvorova za rudarenje, iskorišćavajući prednosti distribuirane i nepromjenjive blockchain tehnologije. Prema dizajnu, blockchain je opremljen da se suoči sa i izdrži DDoS napad. Najpre, on eliminiše rizik od pojave jedne tačke kvara. Može održavati listu kompromitovanih IP adresa u svojoj knjizi, što ga čini otpornim na pokušaje ometanja. Čim se server sa listom kompromitovanih adresa napadne, korisnici mogu preći na bilo koji drugi čvor na mreži kako bi pristupili sigurnoj kopiji.

2. Napad modifikacije – U ovom scenariju napada, zlonamjerni napadač može pokušati izmjeniti ili izbrisati sačuvane podatke određenog korisnika ili uređaja. Da bi izveo ovaj napad, napadač mora ugroziti bezbjednost lokalne memorije. Različite varijacije napada modifikacije detaljno su analizirane u okvirima zanovanim na blockchain tehnologiji za razmjenu informacija. Istraživanja tvrde da primjena pametnih ugovora efikasno sprečava napadače da probiju sigurnosne mehanizme njihovih predloženih šema (Rathod et al., 2022). Slično tome, u okviru predloženom od strane Kašlana i saradnika (Qashlan et al., 2021), samo administrator ima ovlašćenje za skladištenje, brisanje ili ažuriranje podataka, u skladu sa

politikama definisanim u pametnim ugovorima. Sve informacije o korisnicima, uređajima i politikama se dijele između rubnih čvorova i oblaka. U slučaju da napadač želi promjeniti ili modifikovati ID korisnika ili bilo kog uređaja, takve promjene će biti brzo otkrivene od strane rubnih čvorova, jer svaki blok sadrži heš vrijednost prethodnog bloka i bilo kakva promjena u jednom bloku rezultiraće prekidom u celokupnom lancu transakcija (Qashlan et al., 2021).

Prijetnja autentifikacije i kontrole pristupa predstavlja ozbiljan bezbjednosni izazov. Prema istraživanju koje su sproveli Alam i saradnici (Alam et al., 2022), napadač može pokušati preuzeti kontrolu nad pametnim kućnim uređajem ili ubaciti lažni uređaj u kućnu mrežu. Kako bi se efikasno zaštitili od ovih pretnji, Kašlan i saradnici (Qashlan et al., 2021) su implementirali hijerarhijski mehanizam odbrane u svom dizajnu. Prva linija odbrane je admin čvor koji centralizovano upravlja svim ulaznim i izlaznim transakcijama (sa ciljem sprečavanja direktnog pristupanja pametnim kučnim uređajima putem Interneta). Sve transakcije se pažljivo nadgledaju od strane administratora, i ako se primjeti bilo kakvo odstupanje od pravila ugovora, transakcija se odbacuje. Drugo, svaki uređaj u kući mora posjedovati jedinstvenu adresu i pratiti istu početnu transakciju u lokalnom blockchain-u. Ovo omogućava uređaju da komunicira sa administratorom i drugim uređajima u mreži. U slučaju da uređaj ne posjeduje jedinstvenu adresu i ne može da prati početnu transakciju, on će biti izolovan iz mreže. Ovaj pristup sprečava napadače da se povežu sa mrežom i instaliraju zlonamerne uređaje, objezbeđujući dodatni nivo bezbjednosti.

Predložena arhitektura sistema za obezbjeđivanje povjerljivosti, dostupnosti i bezbjednosti u kontekstu IoT uređaja i pametnih kuća pruža neke značajne prednosti, ali ima i određene nedostatke i kritične tačke koje treba pažljivo razmotriti.

Prvo, aspekt povjerljivosti sistema, koji se oslanja na upotrebu Ethereum adresa i SSL sesija za komunikaciju, čini se obećavajućim u pogledu osiguravanja privatnosti i bezbjednosti podataka. Međutim, ključno je napomenuti da je uspješnost ovog pristupa značajno zavisna od tačnosti implementacije i upravljanja privatnim ključevima. Gubitak privatnih ključeva ili njihovo kompromitovanje može ozbiljno ugroziti sigurnost sistema. Dakle, potrebno je razmotriti mehanizme za upravljanje i zaštitu privatnih ključeva kako bi se sprečile potencijalne ranjivosti.

Drugo, što se tiče dostupnosti, blockchain tehnologija zaista pruža pouzdanost i robusnost zbog decentralizacije i replikacije podataka. Međutim, treba napomenuti da su

mrežni i energetski zahtjevi blockchain-a i rudarenja dokaza o radu visoki, što može povećati troškove i usporiti sistem u stvarnom svijetu. Osim toga, potrebno je razmotriti kako se sistem skalira sa sve većim brojem uređaja i korisnika kako bi se održala njegova efikasnost.

Kada je riječ o bezbjednosti i prevenciji napada, čini se da su implementirane politike i pametni ugovori efikasni u ograničavanju pristupa i sprečavanju određenih vrsta napada, uključujući DoS napade i pokušaje modifikacije podataka. Međutim, za ovu sigurnost ključno je da se pravilno konfiguriše i održava politika upravljanja atributima subjekta i objekta, a takođe i da se sistem redovno ažurira i održava. U stvarnom okruženju, dinamika IoT uređaja i povećan broj korisnika mogu dodatno otežati ovo upravljanje.

Naposlektu, predložena arhitektura sistema ima potencijal da pruži napredne nivoe sigurnosti, privatnosti i dostupnosti u domenima IoT uređaja i pametnih kuća. Međutim, ključno je razmotriti praktične izazove, uključujući upravljanje privatnim ključevima, skalabilnost, i održavanje sistema kako bi se postigao potencijal ovog rješenja.

5. ZAKLJUČAK

Pametne kuće u značajnoj mjeri mijenjaju način na koji upravljamo i živimo u našem domu. Ovi inovativni domovi koriste sisteme automatizacije kako bi olakšali upravljanje različitim aspektima kuće, uključujući rasvjetu, grijanje, hlađenje, sigurnost i zabavu. Sve ove funkcije mogu se kontrolisati putem mobilnih aplikacija ili glasovnih asistenata, čime se korisnicima omogućava potpuna kontrola na njihovim domom, čak i izvan njega putem Interneta. Pametne kuće koriste bežične mreže poput Wi-Fi, Bluetooth i Zigbee kako bi povezale sve uređaje i komponente unutar kuće. Ova povezivost omogućava korisnicima da nadziru i upravljaju svojim domom s udaljenosti. Sigurnost je ključna komponenta pametnih kuća, sa sistemima koji uključuju kamere, senzore pokreta, senzore dima i plina, i mogućnosti daljinskog nadzora i upravljanja. Osim toga, pametne kuće su usmjerene prema energetskoj efikasnosti, koristeći pametne termostate, LED rasvjetu, solarnu energiju i praćenje potrošnje energije kako bi smanjile ekološki otisak. Integrisani sistemi za zabavu, uključujući pametne televizore i zvučnike, pružaju korisnicima beskrajne mogućnosti zabave. Korisnici često koriste glasovne asistente kao Amazon Alexa, Google Assistant ili Apple Siri kako bi jednostavno upravljali svim uređajima i sistemima u svojoj kući. Pametne kuće su prilagodljive potrebama i preferencijama korisnika, omogućavajući promjenu postavki, rasporeda svjetla i temperature prema trenutnim zahtjevima. Sistemi pametnog osvjetljenja omogućuju prilagođavanje boje svjetla i jačine svjetla kako bi se stvorila željena atmosfera. Nadalje, pametne kuće često koriste pametne uređaje kao što su frižideri, mašine i sušilice, brave i uređaji za nadzor kvaliteta vazduha s senzorima za praćenje vazduha i sistemima za prečišćavanje kako bi osigurali zdravo okruženje u kući. Sve ove funkcije čine pametne kuće integralnim dijelom naše svakodnevnice, pružajući nam veću kontrolu i udobnost u našem domu.

Pametne kuće se sastoje od različitih uređaja koji su povezani na Internet. Svi ovi uređaji su povezani na zajedničku mrežu, koja se obično naziva IoT, što omogućava centralizovanu kontrolu svih uređaja u kući putem pametnog telefona, tableta ili računara. To čini život u pametnoj kući praktičnijim i ugodnijim, jer korisnik može kontrolisati sve aspekte svog doma iz jednog mjesta. Međutim, kako pametni uređaji postaju sve popularniji, tako i rizici vezani uz bezbjednost i privatnost postaju sve veći.

Na temelju opsežnog pregleda literature i analize stručnih radova, zaključujemo da decentralizovana arhitektura pametnih kuća zasnovana na blockchain tehnologiji pruža

temeljno razumevanje jačanja sistema, uz primjenu tehnika očuvanja privatnosti. Dok čak i najefikasniji centralizovani sistemi pokazuju ranjivosti poput curenja podataka i krađe identiteta, aplikacije blockchain tehnologije se ističu efikasnošću, pružajući visok nivo privatnosti i bezbjednosti. Ipak, izazovi poput skalabilnosti, upravljanja čvorovima i smanjenja procesorske snage čine važnim razmatranje prilikom implementacije.

U radu se detaljno opisuje implementacija sigurnih transakcija pametnih kuća putem Ethereum pametnih ugovora. Analiza ukazuje na prednosti korišćenja blockchain-a u osiguravanju pristupa pametnim uređajima, dok istovremeno ističe nedostatke, uključujući ograničenja realnog vremena i resursa IoT uređaja. Autori predstavljaju model integracije blockchain-a i rubnog računarstva kao odgovor na izazove skalabilnosti, što doprinosi cjelokupnoj bezbjednosti sistema.

U evaluaciji modela interakcije u stvarnom vremenu između korisnika pametnih kuća i privatnog blockchain čvora, kombinacija blockchain tehnologije, kontrole pristupa zasnovane na atributima i rubnog računarstva pokazuje se kao rješenje problema tradicionalnih metoda kontrole pristupa. Ovaj model uspješno ostvaruje željene bezbjednosne ciljeve, pružajući otpornost na modifikacije i napade, čime se rješava pitanje kontrole pristupa u IoT-u.

U zaključku, istraživanje naglašava prednosti decentralizovane arhitekture pametnih kuća s primjenom blockchain tehnologije, uz istovremeno prepoznavanje tehničkih izazova. Integracija s tehnologijama poput računarstva u oblaku i kontinuirana optimizacija aplikacija blockchain tehnologije predstavljaju ključne korake ka stvaranju snažnih i sigurnih sistema pametnih kuća.

Kao i svaki drugi naučni rad, i ovaj rad se odlikuje određenim ograničenjima. U vidu prvog ograničenja pojavljuje se ograničena dostupnost dokumenata koji analiziraju konkretne primjere primjene pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama. Obim istraživanja ograničen je isključivo koncentrisanjem na mogućnost primjene pametnih ugovora za očuvanje bezbjednosti i privatnosti u pametnim kućama, i njegove druge primjene u kontekstu pametnih kuća nisu bile predmet analize. To bi, međutim, moglo biti ideja za neki drugi istraživački projekat. S obzirom da se istraživanje zasniva na naučnim radovima, postoji mogućnost određenog ograničenja u smislu pristrasnosti materijala, s obzirom da ne postoji mogućnost praktičnog provjeravanja navoda.

U pogledu budućih pravaca istraživanja, ovo istraživanje otvara put za dalje istraživanje u oblasti jačanja sigurnosti pametnih kuća. Razmatranje tehničkih izazova i ograničenja aplikacija blockchain tehnologije pruža osnovu za istraživanje novih tehnoloških inovacija koje bi mogle prevazići ove prepreke. Razvoj skalabilnih rješenja, poboljšanja u upravljanju resursima IoT uređaja i optimizacija procesorske snage mogli bi biti ključni aspekti budućih istraživanja. Praktične primjene proizašle iz ovog rada mogu se fokusirati na implementaciju i integraciju predloženih modela u stvarnom okruženju pametnih kuća. Testiranje ovih modela u praksi omogućilo bi stvaranje konkretnih smjernica i najboljih praksi za implementaciju blockchain tehnologije u cilju poboljšanja bezbjednosti i privatnosti korisnika. Osim toga, dalje istraživanje može se usredsrediti na razvoj alata ili platformi koje olakšavaju implementaciju blockchain tehnologije u pametnim kućama, čime se olakšava širenje ovih inovacija u širem spektru domaćinstava. Sveukupno, ovaj rad pruža osnovu za dalje istraživanje koje može unaprjediti oblast pametnih kuća, dovodeći do praktičnih rješenja koja poboljšavaju sigurnost, privatnost i funkcionalnost ovih sistema u budućnosti.

LITERATURA

1. Alam, T. (2022). Blockchain cities: the futuristic cities driven by Blockchain, big data and internet of things. *GeoJournal*, *87*(6), 5383-5412.
2. Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. (2022). A review: Secure Internet of thing System for Smart Houses. *Procedia Computer Science*, *201*, 437-444.
3. Aliero, M. S., Qureshi, K. N., Pasha, M. F., & Jeon, G. (2021). Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services. *Environmental Technology & Innovation*, *22*, 101443.
4. Alrahili, R. (2022). Towards employing process mining for role based access control analysis: a systematic literature review. In Proceedings of the Future Technologies Conference (FTC) 2021, Volume 1 (pp. 904-927). Springer International Publishing.
5. Ali, J., Ali, T., Musa, S., & Zahrani, A. (2020). Towards secure IoT communication with smart contracts in a blockchain infrastructure. *arXiv preprint arXiv:2001.01837*.
6. Alzoubi, A. (2022). Machine learning for intelligent energy consumption in smart homes. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *2*(1).
7. Alzoubi, Y. I., Al-Ahmad, A., & Kahtan, H. (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. *Computer Communications*, *182*, 129-152.
8. Aloraini, F., Javed, A., Rana, O., & Burnap, P. (2022). Adversarial machine learning in IoT from an insider point of view. *Journal of Information Security and Applications*, *70*, 103341.
9. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3677.
10. Ardagna, C. A., di Vimercati, S. D. C., Neven, G., Paraboschi, S., Preiss, F. S., Samarati, P., & Verdicchio, M. (2010, June). Enabling privacy-preserving credential-based access control with XACML and SAML. In *2010 10th IEEE International Conference on Computer and Information Technology* (pp. 1090-1095). IEEE.

11. Arslanian, H. (2022). Ethereum. In *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets* (pp. 91-98). Cham: Springer International Publishing.
12. Aung, Y. N., & Tantidham, T. (2017, November). Review of Ethereum: Smart home case study. In *2017 2nd International Conference on Information Technology (INCIT)* (pp. 1-4). IEEE.
13. Ayan, O., & Turkay, B. (2020, June). IoT-based energy efficiency in smart homes by smart lighting solutions. In *2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA)* (pp. 1-5). IEEE.
14. Aziz, I. T., Abdulqadder, I. H., & Jawad, T. A. (2022). Distributed Denial of Service Attacks on Cloud Computing Environment. *Cihan University-Erbil Scientific Journal*, *6*(1), 47-52.
15. Babangida, L., Perumal, T., Mustapha, N., & Yaakob, R. (2022). Internet of things (IoT) based activity recognition strategies in smart homes: A review. *IEEE Sensors Journal*.
16. Balasingam, S., Zapiee, M. K., & Mohana, D. (2022). Smart Home Automation System Using IOT. *International Journal of Recent Technology and Applied Science*, *4*(1), 44-53.
17. Bauer, D. P. (2022). ERC-20: Fungible Tokens. In *Getting Started with Ethereum: A Step-by-Step Guide to Becoming a Blockchain Developer* (pp. 17-48). Berkeley, CA: Apress.
18. Bera, B., Das, A. K., Obaidat, M. S., Vijayakumar, P., Hsiao, K. F., & Park, Y. (2020). AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE. *IEEE Consumer Electronics Magazine*, *10*(5), 82-92.
19. Bhattacharya, P., Tanwar, S., Bodkhe, U., Kumar, A., & Kumar, N. (2022). EVBlocks: A blockchain-based secure energy trading scheme for electric vehicles underlying 5G-V2X ecosystems. Wireless Personal Communications, 127(3), 1943-1983.
20. Bhawana, Kumar, S., Rathore, R. S., Mahmud, M., Kaiwartya, O., & Lloret, J. (2022). BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment. *Sensors*, *22*(15), 5733.
21. Bhuyan, M., Kashihara, S., Fall, D., Taenaka, Y., & Kadobayashi, Y. (2022). A survey on blockchain, SDN and NFV for the smart-home security. *Internet of Things*, 100588.

22. Byun, J., Hong, I., Lee, B., & Park, S. (2013). Intelligent household LED lighting system considering energy efficiency and user satisfaction. *IEEE Transactions on Consumer Electronics*, *59*(1), 70-76.
23. Budi, A. S., Fitriyah, H., Setiawan, E., Primananda, R., & Maulana, R. (2022). Distributed rule execution mechanism in smart home system. *International Journal of Electrical and Computer Engineering* (IJECE), *12*(4), 4439-4448.
24. Burdon, M. (2020). The Smart Home: A Collected Target. In *Digital Data Collection and Information Privacy Law* (Cambridge Intellectual Property and Information Law, pp. 39-66). Cambridge: Cambridge University Press.
25. Chi, H., & Chi, Y. (2022). Smart home control and management based on big data analysis. *Computational Intelligence and Neuroscience*, 2022.
26. Chitnis, S., Deshpande, N., & Shaligram, A. (2016). An investigative study for smart home security: Issues, challenges and countermeasures. *Wireless Sensor Network*, *8*(04), 61.
27. Civitarese, G. (2023). Invisible-visual hallucinations in Bion's "Attacks on Linking". *The International Journal of Psychoanalysis*, *104*(2), 197-222.
28. Corno, F., & Mannella, L. (2023, May). A Gateway-based MUD Architecture to Enhance Smart Home Security. In *Proceedings of the 8th International Conference on Smart and Sustainable Technologies–SpliTech 2023* (pp. 1-6). Institute of Electrical and Electronics Engineers (IEEE).
29. Dang, T. L. N., & Nguyen, M. S. (2018). An approach to data privacy in smart home using blockchain technology. In 2018 *International Conference on Advanced Computing and Applications* (ACOMP) (pp. 58-64). IEEE.
30. Danbatta, S. J., & Varol, A. (2019). Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. *In 2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.
31. de Moraes Rossetto, A. G., Sega, C., & Leithardt, V. R. Q. (2022). An Architecture for Managing Data Privacy in Healthcare with Blockchain. *Sensors*, *22*(21), 8292.
32. Debnath, D., Chettri, S. K., & Dutta, A. K. (2022). Security and privacy issues in internet of things. In *ICT Analysis and Applications* (pp. 65-74). Springer Singapore.
33. Deepthi, S., & Khandwekar, S. (2023). Lightweight Capability-Based Access Control for Internet of Things (IoT). In *Applications and Techniques in Information Security: 13th International Conference, ATIS 2022*, Manipal, India, December 30–31, 2022, Revised Selected Papers (pp. 258-266). Singapore: Springer Nature Singapore.

34. Dos Santos, B. V., Vergütz, A., Macedo, R. T., & Nogueira, M. (2022, November). A Dynamic Method to Protect User Privacy Against Traffic-based Attacks on Smart Home. In *2022 IEEE Latin-American Conference on Communications (LATINCOM)* (pp. 1-6). IEEE.
35. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) 2017 Apr 18 (pp. 173-178).
36. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017a). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 *IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.
37. Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 55(12), 119-125.
38. Ejaz, W., Anpalagan, A., Ejaz, W., & Anpalagan, A. (2019). Blockchain technology for security and privacy in internet of things. *Internet of Things for Smart Cities: Technologies, Big Data and Security*, 47-55.
39. El Azzaoui, A., Chen, H., Kim, S. H., Pan, Y., & Park, J. H. (2022). Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems. *Sensors*, *22*(4), 1371.
40. Far, S. B., & Rad, A. I. (2022). Applying digital twins in metaverse: User interface, security and privacy challenges. *Journal of Metaverse*, *2*(1), 8-15.
41. Farooq, M. S., Khan, S., Rehman, A., Abbas, S., Khan, M. A., & Hwang, S. O. (2022). Blockchain-Based Smart Home Networks Security Empowered with Fused Machine Learning. *Sensors*, *22*(12), 4522.
42. Gai, K., She, Y., Zhu, L., Choo, K. K. R., & Wan, Z. (2022). A Blockchain-based Access Control Scheme for Zero Trust Cross-organizational Data Sharing. ACM Transactions on Internet Technology (TOIT).
43. Gazis, A., & Katsiri, E. (2021). Smart home IoT sensors: Principles and applications a review of low-cost and low-power solutions. *International Journal on Engineering Technologies and Informatics*, *2*(1), 19-23.
44. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an IoT based smart home. In 2017 *40th*

International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1292-1297). IEEE.

45. Godla, S. R., Fikadu, G., & Adema, A. (2022). Socket programming-based rmi application for Amazon web services in distributed cloud computing. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021* (pp. 517-526). Singapore: Springer Nature Singapore.
46. Gong, J., & Navimipour, N. J. (2022). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. *Cluster Computing*, *25*(1), 383-400.
47. Grunert, K. (2022). Towards uninterruptible smart home processes. In 2022 *IEEE 24th Conference on Business Informatics (CBI)* (Vol. 2, pp. 80-87). IEEE.
48. Gunge, V. S., & Yalagi, P. S. (2016). Smart home automation: a literature review. *International Journal of Computer Applications*, *975*(8887-8891).
49. Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: research and applications*, *3*(2), 100067.
50. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11), 341.
51. Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: vulnerabilities, risks, and countermeasures. *Computers & Security*, *117*, 102677.
52. Harper, R. (2006). *Inside the smart home*. Springer Science & Business Media.
53. Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512-529.
54. Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of empowered IoT users. In 2016 *IEEE first international conference on internet-of-things design and implementation (IoTDI)* (pp. 13-24). IEEE.
55. Hiza, D. (2022). *Assessig the Significance of Cia Triad Security Model in Establishing ICT Security Controls in The Public Sector (Doctoral dissertation*). Institute of Accountancy Arusha.
56. Huang, H., Yan, Z., Tang, X., Xiao, F., & Li, Q. (2022). Differential privacy protection scheme based on community density aggregation and matrix perturbation. *Information Sciences*, *615*, 167-190.

57. Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, *800*(162), 1-54.
58. Illy, P., Kaddoum, G., Kaur, K., & Garg, S. (2022). ML-based IDPS enhancement with complementary features for home IoT networks. *IEEE Transactions on Network and Service Management*, *19*(2), 772-783.
59. Isyanto, H., Arifin, A. S., & Suryanegara, M. (2020, October). Performance of smart personal assistant applications based on speech recognition technology using IoT-based voice commands. In *2020 International conference on information and communication technology convergence (ICTC)* (pp. 640-645). IEEE.
60. Jamsa, K. (2022). *Cloud computing.* Jones & Bartlett Learning.
61. Jazzar, M., & Hamad, M. (2022). An Analysis Study of IoT and DoS Attack Perspective. In *Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021* (pp. 127-142). Singapore: Springer Nature Singapore.
62. Jenal, M., Omar, A. N., Hisham, M. A. A., Noh, W. N. W. M., & Razali, Z. A. I. (2022). Smart Home Controlling System. *Journal of Electronic Voltage and Application*, *3*(1), 92-104.
63. Jin, H., Liu, G., Hwang, D., Kumar, S., Agarwal, Y., & Hong, J. I. (2022). Peekaboo: A hub-based approach to enable transparency in data processing within smart homes. In 2022 *IEEE Symposium on Security and Privacy (SP)* (pp. 303-320). IEEE.
64. Kang, W. M., Moon, S. Y., & Park, J. H. (2017). An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences*, *7*, 1-12.
65. Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420.
66. Khacef, K., Benbernou, S., Ouziri, M., & Younas, M. (2023). A Dynamic Sharding Model Aware Security and Scalability in Blockchain. *Information Systems Frontiers*, 1-14.
67. Khanh, Q. V., Hoai, N. V., Manh, L. D., Le, A. N., & Jeon, G. (2022). Wireless communication technologies for IoT in 5G: Vision, applications, and challenges. *Wireless Communications and Mobile Computing*, 2022, 1-12.
68. Khoa, T. A., Nhu, L. M. B., Son, H. H., Trong, N. M., Phuc, C. H., Phuong, N. T. H., ... & Duc, D. N. M. (2020). Designing efficient smart home management with IoT

smart lighting: a case study. *Wireless communications and mobile computing*, *2020*, 1-18.

69. Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., ... & Das, S. K. (2022). Edge-Computing-Driven Internet of Things: A Survey. *ACM Computing Surveys*, *55*(8), 1-41.
70. Kumar, A., Upadhyay, A., Mishra, N., Nath, S., Yadav, K. R., & Sharma, G. (2022). Privacy and Security Concerns in Edge Computing-Based Smart Cities. In *Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities (*pp. 89-110). Cham: Springer International Publishing.
71. Lazaroiu, C., & Roscia, M. (2017, November). Smart district through IoT and blockchain. In *2017 IEEE 6th international conference on renewable energy research and applications (ICRERA)* (pp. 454-461). IEEE.
72. Lee, Y., Rathore, S., Park, J. H., & Park, J. H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences*, *10*(1), 1-14.
73. Li, X., Chen, T., Cheng, Q., Ma, S., & Ma, J. (2020). Smart applications in edge computing: Overview on authentication and data security. *IEEE Internet of Things Journal*, *8*(6), 4063-4080.
74. Liang, W., & Ji, N. (2022). Privacy challenges of IoT-based blockchain: a systematic review. *Cluster Computing*, *25*(3), 2203-2221.
75. Liang, X., An, N., Li, D., Zhang, Q., & Wang, R. (2022). A Blockchain and ABAC Based Data Access Control Scheme in Smart Grid. In 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS) (pp. 52-55). IEEE.
76. Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. R. (2019). HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, *7*(2), 818-829.
77. Liao, K. (2022). Design of the Secure Smart Home System Based on the Blockchain and Cloud Service. *Wireless Communications and Mobile Computing*, 2022, 1-12.
78. Lee, Y., Rathore, S., Park, J. H., & Park, J. H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences*, 10(1), 1-14.
79. Madjid, W. P., & Defvyanto, A. R. T. (2022). Cryptocurrency: Opportunities and Challenges in Hungary and Indonesia. *Economic and business trajectory: Indonesia, Asia and Europe*, 198.

80. Mehedi, S. T., Shamim, A. A. M., & Miah, M. B. A. (2019). Blockchain-based security management of IoT infrastructure with Ethereum transactions. *Iran Journal of Computer Science*, *2*(3), 189-195.
81. Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems*, *102*, 1027-1037.
82. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Generation Computer Systems*, *100*, 325-343.
83. Morawiec, P., & Sołtysik-Piorunkiewicz, A. (2022). Cloud computing, Big Data, and blockchain technology adoption in ERP implementation methodology. *Sustainability*, *14*(7), 3714.
84. Namane, S., & Ben Dhaou, I. (2022). Blockchain-Based Access Control Techniques for IoT Applications. *Electronics*, *11*(14), 2225.
85. Nasir, M., Muhammad, K., Ullah, A., Ahmad, J., Baik, S. W., & Sajjad, M. (2022). Enabling automation and edge intelligence over resource constraint IoT devices for smart home. *Neurocomputing*, *491*, 494-506.
86. Nemec Zlatolas, L., Feher, N., & Hölbl, M. (2022). Security perception of IoT devices in smart homes. *Journal of Cybersecurity and Privacy*, *2*(1), 65-73.
87. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications surveys & tutorials, 22(4), 2521-2549.
88. Nomoto, K., Akiyama, M., Eto, M., Inomata, A., & Mori, T. (2022). On the Feasibility of Linking Attack to Google/Apple Exposure Notification Framework. *Proceedings on Privacy Enhancing Technologies*, *4*, 140-161.
89. Odunlade, E. (2022). *What makes a Smart Home smart? A guide to protocols and applications*, https://www.wevolver.com/article/what-makes-a-smart-home-smart-a-guide-to-protocols-and-applications, 22/10/2023.
90. Omran, M. A., Hamza, B. J., & Saad, W. K. (2022). The design and fulfillment of a Smart Home (SH) material powered by the IoT using the Blynk app. *Materials Today: Proceedings*, *60*, 1199-1212.

91. Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and communication networks*, *9*(18), 5943-5964.
92. Özgür, L., Akram, V. K., Challenger, M., & Dağdeviren, O. (2018, May). An IoT based smart thermostat. In *2018 5th International Conference on Electrical and Electronic Engineering (ICEEE)* (pp. 252-256). IEEE.
93. Padmavathi, U., & Rajagopalan, N. (2023). Concept of blockchain technology and its emergence. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 21-36). IGI global.
94. Padmanaban, S., Nasab, M. A., Shiri, M. E., Javadi, H. H. S., Nasab, M. A., Zand, M., & Samavat, T. (2023). The Role of Internet of Things in Smart Homes. Artificial Intelligence-based Smart Power Systems, 259-271.
95. Papachristou, N., Kartsidis, P., Anagnostopoulou, A., Marshall-McKenna, R., Kotronoulas, G., Collantes, G., ... & Bamidis, P. D. (2023, May). A Smart Digital Health Platform to Enable Monitoring of Quality of Life and Frailty in Older Patients with Cancer: A Mixed-Methods, Feasibility Study Protocol. In *Seminars in Oncology Nursing* (p. 151437). WB Saunders.
96. Park, J., & Chang, S. (2023). Secure device control scheme with blockchain in a smart home. *Measurement and Control*, *56*(3-4), 546-557.
97. Philip, S. J., Luu, T. J., & Carte, T. (2023). There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior*, *139*, 107551.
98. Pradeep, S., Kousalya, T., Suresh, K. A., & Edwin, J. (2016). IoT and its connectivity challenges in smart home. *Int. Res. J. Eng. Technol*, *3*, 1040-1043.
99. Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023). Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. *Sensors*, *23*(4), 1805.
100. Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R. A., & Raboaca, M. S. (2022). Blockchain for Future Wireless Networks: A Decade Survey. *Sensors*, *22*(11), 4182.
101. Ratkovic, N. (2022). Improving Home Security Using Blockchain. International *Journal of Computations, Information and Manufacturing* (IJCIM), *2*(1).

102. Samuel, O., Javaid, N., Almogren, A., Javed, M. U., Qasim, U., & Radwan, A. (2022). A secure energy trading system for electric vehicles in smart communities using blockchain. *Sustainable Cities and Society*, *79*, 103678.

103. Sanaei, S., Haghifam, M. R., & Safdarian, A. (2022). Centralized optimal management of a smart distribution system considering the importance of load reduction based on prioritizing smart home appliances. *IET Generation, Transmission & Distribution*, *16*(19), 3874-3893.

104. Saraji, S. (2023). Introduction to Blockchain. In *Sustainable Oil and Gas Using* Blockchain (pp. 57-74). Cham: Springer International Publishing.

105. Sajid Ullah, S., Oleshchuk, V., & Gardiyawasam Pussewalage, H. S. (2023). A Survey on Blockchain Envisioned Attribute Based Access Control for Internet of Things: Overview, Comparative Analysis, and Open Research Challenges. Vladimir and Gardiyawasam Pussewalage, Harsha S., A Survey on Blockchain Envisioned Attribute Based Access Control for Internet of Things: Overview, Comparative Analysis, and Open Research Challenges.

106. Salji, M. R., Udzir, N. I., Ninggal, M. I. H., Sani, N. F. M., & Ibrahim, H. (2022). Trust-based Access Control Model with Quantification Method for Protecting Sensitive Attributes. *International Journal of Advanced Computer Science and Applications*, *13*(2).

107. Salman, L., Salman, S., Jahangirian, S., Abraham, M., German, F., Blair, C., & Krenz, P. (2016, December). Energy efficient IoT-based smart home. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 526-529). IEEE.

108. Savin, R. (2017). Communication protocols for smart home systems. *ProfMarket: Educatin. Language. Success (ProfMarket: Образование. Язык. Успех)*, 174-176.

109. Septiani, N., Lutfiani, N., Oganda, F. P., Salam, R., & Devana, V. T. (2022). Blockchain technology in the public sector by leveraging the triumvirate of security. In *2022 International Conference on Science and Technology (ICOSTECH)* (pp. 1-5). IEEE.

110. Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2022). An attribute-based access control model for Internet of Things using hyperledger fabric blockchain. *Wireless Communications and Mobile Computing*.

111. Sriram, G. S. (2022). Edge computing vs. Cloud computing: an overview of big data challenges and opportunities for large enterprises. *International Research Journal of Modernization in Engineering Technology and Science*, *4*(1), 1331-1337.

112. Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): A survey. *Sensors*, *22*(3), 1094.

113. Shakarami, M., Benson, J., & Sandhu, R. (2022). Blockchain-based administration of access in smart home iot. In *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (pp. 57-66).

114. Sharif, Z., Jung, L. T., Ayaz, M., Yahya, M., & Khan, D. (2022). Smart Home Automation by Internet-of-Things Edge Computing Platform. *International Journal of Advanced Computer Science and Applications*, *13*(4).

115. Singh, S., Kumar, A., & Kathuria, M. (2022). Understanding the public, private and consortium consensus algorithms in blockchain technology. *International Journal of Blockchains and Cryptocurrencies*, *3*(3), 269-288.

116. Shakarami, M., Benson, J., & Sandhu, R. (2022). Blockchain-based administration of access in smart home iot. In *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (pp. 57-66).

117. Shirole, M., Darisi, M., & Bhirud, S. (2020). Cryptocurrency token: An overview. In *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology* (pp. 133-140). Springer Singapore.

118. Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), 6793-6807.

119. Singh, S., Ra, I. H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*, *15*(4), 1550147719844159.

120. Singh, P. K., Singh, R., Nandi, S. K., & Nandi, S. (2019). Managing smart home appliances with proof of authority and blockchain. In *Innovations for Community Services: 19th International Conference, I4CS 2019, Wolfsburg, Germany, June 24-26, 2019, Proceedings* 19 (pp. 221-232). Springer International Publishing.

121. Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015, October). Network-level security and privacy control for smart-home IoT devices. In 2015 IEEE *11th International conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 163-167). IEEE.

122. Soni, M., & Singh, D. K. (2022). LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network. *Wireless Personal Communications*, *127*(2), 1067-1084.

123. Steffen, S., Bichsel, B., Baumgartner, R., & Vechev, M. (2022). Zeestar: Private smart contracts by homomorphic encryption and zero-knowledge proofs. In 2022 *IEEE Symposium on Security and Privacy (SP)* (pp. 179-197). IEEE.

124. Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, *21*(11), 3784.

125. Sun, Y., Song, H., Jara, A. J., & Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. *IEEE access*, *4*, 766-773.

126. Tarannum, W., & Abidin, S. (2023). Integration of Blockchain and Cloud Computing: A Review. In 2023 *10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1623-1628). IEEE.

127. Taiwo, O., Ezugwu, A. E., Oyelade, O. N., & Almutairi, M. S. (2022). Enhanced intelligent smart home control and security system based on deep learning model. *Wireless communications and mobile computing*, 2022, 1-22.

128. Tian, Y., & Nogales, A. F. R. (2023). A Survey on Data Integrity Attacks and DDoS Attacks in Cloud Computing. In 2023 *IEEE 13th Annual Computing and Communication Workshop and Conference* (CCWC) (pp. 0788-0794). IEEE.

129. Tchagna Kouanou, A., Tchito Tchapga, C., Sone Ekonde, M., Monthe, V., Mezatio, B. A., Manga, J., ... & Muhozam, Y. (2022). Securing data in an internet of things network using blockchain technology: smart home case. *SN Computer Science*, *3*(2), 167.

130. Thakur, M. (2017). *Authentication, authorization and accounting with Ethereum blockchain (master thesis).* Helsinki: Department of Computer Science.

131. Thakare, S., & Pund, M. A. (2022). Introduction to Blockchain and Terminologies. In *Blockchain for Smart Systems* (pp. 3-20). Chapman and Hall/CRC.

132. Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2021). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *Journal of Systems and Software*, 174, 110891.

133. Vandome, N. (2018). *Smart homes in easy steps: Master smart technology for your home*. Easy Steps.

134. Vashisht, S., Gaba, S., Dahiya, S., & Kaushik, K. (2022). Security and privacy issues in IoT systems using blockchain. In *Sustainable and Advanced Applications of Blockchain in Smart Computational Technologies* (pp. 113-127). Chapman and Hall/CRC.

135. Xihua, Z., & Goyal, S. (2022). Security and privacy challenges using IoT-blockchain technology in a smart city: critical analysis. *International journal of electrical and electronics research*, *10*, 190-195.

136. Xue, J., Xu, C., & Zhang, Y. (2018). Private blockchain-based secure access control for smart home systems. *KSII Transactions on Internet and Information Systems (TIIS)*, *12*(12), 6057-6078.

137. Xu, L., Bao, T., & Zhu, L. (2020). Blockchain empowered differentially private and auditable data publishing in industrial IoT. *IEEE Transactions on Industrial Informatics*, *17*(11), 7659-7668.

138. Xue, H., Chen, D., Zhang, N., Dai, H. N., & Yu, K. (2023). Integration of blockchain and edge computing in internet of things: A survey. *Future Generation Computer Systems*, *144*, 307-326.

139. Wang, S., Li, H., Chen, J., Wang, J., & Deng, Y. (2022a). DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *Journal of Information Security and Applications*, *66*, 103134.

140. Wang, P., Chen, B., Xiang, T., & Wang, Z. (2022b). Lattice-based public key searchable encryption with fine-grained access control for edge computing. Future Generation Computer Systems, 127, 373-383.

141. William, P., Yogeesh, N., Vimala, S., & Gite, P. (2022). Blockchain Technology for Data Privacy using Contract Mechanism for 5G Networks. In 2022 *3rd International Conference on Intelligent Engineering and Management (ICIEM)* (pp. 461-465). IEEE.

142. Williams, E., Slade, E., Hodges, D., & Morgan, P. (2020). Individual differences in the adoption and secure use of smart home technology. *British Academy of Management Conference: BAM2020 Conference in the Cloud, Online, 2-4 September 2020.*

143. Qashlan, A., Nanda, P., & He, X. (2020). Automated Ethereum Smart Contract for Block Chain Based Smart Home Security. In: Somani, A.K., Shekhawat,

R.S., Mundra, A., Srivastava, S., Verma, V.K. (eds) *Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies*, vol 141 (pp.313-326). Springer.

144. Qashlan, A., Nanda, P., He, X., & Mohanty, M. (2021). Privacy-preserving mechanism in smart home using blockchain. *IEEE Access, 9*, 103651-103669.

145. Yakubu, B. M., Khan, M. I., Khan, A., Jabeen, F., & Jeon, G. (2023). Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home. *Digital Communications and Networks*.

146. Yi, Y., He, J., Zhu, N., & Ma, X. (2022). Social influence-based privacy inference attacks in online social networks. *Security and Privacy*, *5*(2), e194.

147. Yutaka, M., Zhang, Y., Sasabe, M., & Kasahara, S. (2019). Using ethereum blockchain for distributed attribute-based access control in the internet of things. In *2019 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

148. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, *6*(2), 1594-1605.

149. Zhao, Z. (2022). Comparison of Hyperledger Fabric and Ethereum Blockchain. In *2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)* (pp. 584-587). IEEE.

150. Zheng, X. R., & Lu, Y. (2022). Blockchain technology–recent research and future trend. *Enterprise Information Systems*, *16*(12), 1939895.

151. Zhou, B., Li, W., Chan, K. W., Cao, Y., Kuang, Y., Liu, X., & Wang, X. (2016). Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable and Sustainable Energy Reviews*, *61*, 30-40.

152. Zhou, Y., Han, M., Liu, L., Wang, Y., Liang, Y., & Tian, L. (2018). Improving iot services in smart-home using blockchain smart contract. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 81-87). IEEE.