IZAZOVI SIGURNOSTI I PRIVATNOSTI MEDICINSKIH INTERNET STVARI

Muhamed Ćosić, Internacionalni Univerzitet Travnik u Travniku, drmuhamedcosic@gmail.com
Nešad Krnjić, Internacionalni Univerzitet Travnik u Travniku, prof.nesad@gmail.com
Rudolf Petrušić, Internacionalni Univerzitet Travnik u Travniku, rudolfpetrusic@gmail.com

Pregledni članak

Rezime: *Internet stvari, ili skraćeno "IoT" predstavljaju savremeni koncept koji se odnosi na proširenje mogućnosti interneta izvan svog prirodnog okruženja računara na široki spektar drugih procesa i okruženja. Internet medicinskih stvari (IoMT) je poseban dio IoT-a koji kontinuirano dobiva na snazi i popularnosti. Internet medicinskih stvari pruža podršku tradicionalnim zdravstenim sistemima poboljšavajući njihovu performantnost kroz povećanje efikasnosti, efektivnosti, pouzdanosti i skalabilnosti. Ovaj rad se bavi pitanjima sigurnosti i privatnosti internet stvari prvenstveno u domenu medicinskih internet stvari. Prvo se predstavljaju glavne prijetnje po sigurnost, a potom i prijetnje vezane za privatnost medicinskih internet stvari. Fokus rada je usmjeren na predstavljanje glavnih modela za zaštitu sigurnosti i privatnosti medicinskih internet stvari.*

***Ključne riječi**: IoMT, internet, sigurnost, privatnost..*

SECURITY AND PRIVACY CHALLENGES OF THE MEDICAL INTERNET OF THINGS

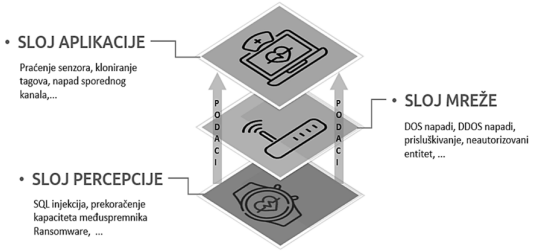
Summary: *The Internet of Things, or "IoT" for short, is a modern concept that refers to extending the possibilities of the Internet beyond its natural computer environment to a wide range of other processes and environments. The Internet of Medical Things (IoMT) is a special part of the IoT that is continuously gaining in strength and popularity. The Internet of Medical Things supports traditional health systems by improving their performance by increasing efficiency, effectiveness, reliability and scalability. This paper deals with issues of security and privacy of Internet of Things primarily in the field of medical Internet of Things. The main threats to security are presented first, followed by threats to the privacy of medical Internet of Things. The focus of the paper is on presenting the main models for protecting the security and privacy of medical internet of things.*

***Keywords**: IoMT, internet, security, privacy.*

1 UVOD

Internet, krucijalna tehnologija informacijskog doba u kome živimo, sve više se temelji na platformama bežične komunikacije. Od svoje pojave pa do danas, kroz proizvodnju i distribuciju digitalnih informacija, internet predstavlja ogroman potencijal za povećanje performantnosti svih oblika ljudskih aktivnosti. Donedavno su se umrežavali samo stolni ili prenosivi računari, pametni telefoni i njima slični uređaji. Današnji stepen razvoja interneta usmjeren je na razvoj složene automatizacije kroz umrežavanje različitih vrsta uređaja opremljenih senzorima poput brojnih kućanskih aparata, pametnih samovozećih automobila, različitih mjernih uređaja, medicinske opreme i uređaja i sl. Nabrojani uređaji se ne povezuju samo na širokopojasnu mrežu nego se povezuju i međusobno što im omogućava razmjenu informacija npr. putem M2M (machine to machine) tehnologije. Komunikacijsku mrežu nastalu na ovaj način nazivamo Internet stvari ili kraće IoT. Nastanak IoT-a je omogućen zahvaljujući pojavi jeftinih računarskih čipova koji su zbog svoje pristupačnosti ugrađeni u mnoštvo stavri, od jednostavnih mjernih instrumenata do komplikovanih medicinskih uređaja, automobila, brodova i aviona. Sve pomenute stvari uz pomoć digitalne inteligencije postaju „pametne“ što im omogućava razmjenu velike količine podataka bez intervencije ljudi. Dakle svaki fizički entitet je moguće pretvoriti u IoT ukoliko se tom entitetu omogući spajanje na internet.

Na samom početku razvoja IoT-a primarni cilj bio je poboljšanje performantnosti proizvodnje i poslovanja. U novije vrijeme naglasak u razvoju IoT-a je na razvijanu „pametnih kuća“ ili „pametnih gradova“. Koncept IoT-a je sveprisutan u svim segmentima ljudskog djelovanja pa tako svoju primjenu nalazi i u medicini kroz poseban segment IoT-a nazvan Internet medicinskih stvari ili kraće IoMT. IoMT igra ključnu ulogu u daljinskoj zdravstvenoj zaštiti i nadzoru za povećanje učinkovitosti medicinskih uređaja, te brzini i dostupnosti medicinskih usluga.(5) IoMT označavaju širok dijapazon medicinskih uređaja i aplikacija koje se koristeći računarske mreže povezuju sa zdravstvenim informacionim sistemima (ZIS). Čim se pojavio IoMT je pokazao značajan potencijal u smislu poboljšanja zdravstvene zaštite kroz omogućavanje daljinskog praćenja stanja pacijenata. IoMT omogućavaju implementaciju velikog broja aplikacija od implantabilnih medicinskih uređaja do bežične mreže tijela (WBAN). Zbog toga se IoMT naširoko koristi za poboljšanje zdravstvene zaštite i smatra se stupom novih sveprisutnih zdravstvenih usluga (4). Shema 1 prikazuje da strukturu IoMT-a čine sloj percepcije, mrežni sloj i sloj aplikacija.



Shema 1: IoMT struktura i vrdste napada

Svaki od navedenih slojeva im specifičan zadatak pa je tako sloj percepcije zadužen za pribavljanje zdravstvenih podataka putem različitih IoMT uređaja (npr. uređaji za praćenje EKG-a). Mrežni sloj obrađuje i putem transportnih protokola prenosi prikupljene podatke. Zadatak sloja aplikacija je da dobivene informacije koristi za pružanje adekvatnih medicinskih usluga i potreba pacijenata.

Primjena internet stvari u medicini je napravila veliku promjenu jer je sve donedavno dominantno sredstvo za evidentiranje podataka o stanju pacijenata bila olovka i papir. Informaciono komunikacione tehnologije su naravno i prije pojave IoT-a omogućile da se uz

pomoć računara i zdravstvenih informacionih sistema način evidentiranja podataka o pacijentima radikalno unaprijedi. Ali pojavom IoT-a dešava se još značajniji i radikalniji pomak nabolje budući da se otvaraju sasvim nove mogućnosti poput razmjene podataka između medicinskih uređaja bez intervencije ljekara i drugog medicinskog osoblja. Na ovaj način se omogućava daljinsko praćenje bitnih parametara vezanih za zdravlje pacijenata. Međutim, cyber kriminalci često koriste slabo zaštićeni IoMT za različite oblike cyber napada, dovodeći u opasnost privatnost i sigurnost podataka. Ovo je moguće zbog toga što IoMT, kao i drugi IoT uređaji imaju nedostatak u vidu nedovoljno standardizovanih sigurnosnih kontrola.

Veliki broj IoMT uređaja ima nepouzdane provjere autentičnosti što dovodi do povećanog rizika neovlaštenog pristupa tim uređajima. Da bi se smanjili rizici od cyber napada prilikom razvoja medicinskih sigurnosnih sistema treba uzeti u obzir nekoliko ključnih zahtjeva. Prvi od tih zahtjeva je integritet podataka, a odnosi se na činjenicu da sve vrijednosti zadovoljavaju semantičke standarde i uključuje dvije razine tačnosti i pouzdanosti. Integritet podataka može se podijeliti u četiri kategorije, odnosno integritet entiteta, integritet domene, referentni integritet i korisnički definirani integritet, koji se može održavati od stranih ključeva, ograničenja, pravila i propisa.

Sljedeći zahtjev je upotrebljivost podataka koja je potrebna kako bi se osiguralo da podatke ili podatkovne sisteme mogu koristiti samo ovlašteni korisnici. Veliki podaci ne nude samo velike prednosti već i kritične izazove, kao što su prljavi podaci i nestandardni podaci. Osim toga, oštećenje podataka ili gubitak podataka uzrokovan neovlaštenim pristupom također dodatno uništava iskoristivost podataka. Također, svaka organizacija treba strategiju kontinuiteta poslovanja i oporavka od katastrofalnih gubljenja podataka.(8)

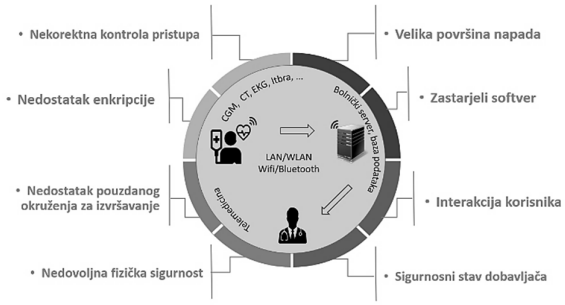
Kontrola podataka u vidu kontrole pristupa medicinskim podacima treći je od ključnih zahtjeva sigurnosti i predstavlja učinkovito sredstvo za praćenje korištenja resursa, zajedničku mjeru nalaza i praćenje abnormalnih događaja. Kontrolni sadržaj općenito uključuje korisnike, davatelje usluga u oblaku kao i pristupne i operativne datoteke. Četvrti zahtjev se odnosi na povjerljivost podataka o pacijentu. Podaci o pacijentu mogu se podijeliti u dvije kategorije: opća evidencija i osjetljivi podaci. Osjetljivi podaci, također se mogu nazvati podaci privatnosti pacijenata, uključuju psihičko stanje, seksualnu orijentaciju, seksualnu funkciju, zarazne bolesti, status plodnosti, ovisnost o drogama i informacije o identitetu. Potrebno je osigurati da osjetljivi podaci neće procuriti do neovlaštenih korisnika. Čak i ako su podaci presretnuti potrebno je osigurati da izražene informacije budu nerazumljive neovlaštenim korisnicima.

2 SIGURNOSNI IZAZOVI MEDICINSKIH INTERNET STVARI

Iako primjena IoMT tehnologija zdravstvu donosi mnoge pogodnosti također donosi i velike sigurnosne izazove. I drugi IoT uređaji su izloženi sigurnosnim prijetnjama ali posljedice koje mogu proisteći mnogo su veće kod napada na IoMT uređaje obzirom da mogu prouzrokovati i gubitke ljudskih života. Primjetno je da je u zadnjih nekoliko godina zdravstveni sektor u samom vrhu po broju hakerskih napada. „Pametni“ IoMT uređaji su dizajnirani da korektno obavljaju određene zadatke, ali zbog nedostatka potrebnih sigurnosnih funkcija, podložni su kibernetičkim napadima što je pogotovo izraženo kada su spojeni na nezaštićene mreže, ili čak na istu mrežu kao i ostatak infrastrukture organizacije. Sigurnost je jedan od aspekata koji se najviše tiču

područja IoMT-a (1). Postoji veliki broj sigurnosnih problema (Shema 2) kojima su izloženi IoMT uređaji među kojima su najvažniji sljedeći problemi:

- Nekorektna kontrola pristupa- sigurnosni sistem uređaja često dozvoljava da usluge koje nudi IoMT uređaj budu dostupne ne samo vlasniku uređaja nego i drugim osobama. Takođe, u velikom broju slučajeva uređaji istog modela se isporučuju sa jednakom predefiniranom lozinkom;
- Jako velika površina napada-IoT uređaji nude veliki broj usluga putem interneta. Što je broj takvih usluga veći veća je i moguća površina napada;
- Zastarjeli softver-IoMT uređaji se često isporučuju s neažuriranim softverom. Povećanje rizika od neželjenih napada je proporcionalno dužini vremena koje prođe od momenta proizvodnje IoMT uređaja do njegove implementacije u nekom informacionom sistemu;
- Nedostatak enkripcije-ima za posljedicu da se na mrežnom putu između uređaja i njegove krajnje tačke može pregledati mrežni promet i imati pristup osjetljivim podacima Čest je slučaj da se API tokeni pohranjuju na uređaju putem običnog teksta ili da se koriste slabi kriptografski algoritmi;
- Nedostatak pouzdanog okruženja za izvršavanje- velika većina IoMT uređaja su u osnovi računari opće namjene koja mogu pokretati određeni softver. Tu činjenicu cyber kriminalci koriste da instaliraju vlastiti softver koji može uzrokovati razne vrste sigurnosnih problema i onemogućiti pravilno funkcionisanje uređaja;
- Sigurnosni stav dobavljača- u nekim slučajevima dobavljač nema uspostavljen proces za rješavanje sigurnosnih problema;
- Nedovoljna fizička sigurnost- U mnogim slučajevima ne pridaje se potrebna pažnja fizičkom osiguranju uređaja. Zbog toga se može desiti da neovlaštene osobe koje posjeduju odgovarajući nivo informatičkog znanja imaju pristup hardveru uređaja;
- Interakcija korisnika- ogleda se u činjenici da se ne poklanja dovoljna pažnja izradi adekvatne dokumentacije o uređaju kao i pažnje u smislu dizajna i upotrebljivosti što rezultira da korisnici nisu motivisani ili su onemogućeni da sami konfiguriraju sigurnosne postavke.



Shema 2: IoMT okruženje i najčešće sigurnosne prijetnje

Jedan od nedostataka IoMT uređaja u pogledu sigurnosti je taj što se prilikom njihovog dizajniranja više pažnje posvećuje upotrebljivosti a ne sigurnosti. Zbog pomenutog nedostatka IoMT uređaji vrlo osjetljivi na cyber napade. Slaba otpornost na cyber napade predstavlja ozbiljan problem imajući u vidu posljedice koje mogu nastupiti, a koje u krajnjijem slučaju mogu rezultirati gubitkom ljudskih života. Stoga je imperativ da pacijenti, ljekari, bolnice i druge zdravstvene ustanove razumiju potencijalne IoMT prijetnje kako bi se smanjili budući napadi (2).

3 IZAZOVI PRIVATNOSTI MEDICINSKIH INTERNET STVARI

Zloupotreba i neovlašten pristup IoMT uređajima takođe može ugroziti privatnost pacijenata što može imati dalekosežne posljedice. Neke od mogućih posljedica su nanošenje duševne boli i emocionalne štete zbog zloupotrebe medicinske

dokumentacije. IoMT je tehnološka paradigma koja se razvija velikom brzinom, čemu doprinosi i sve brži razvoj informaciono komunikacionih tehnologija, što otežava pravovremeno rješavanje mnogih problema privatnosti pacijenata koji se javljaju prilikom korištenja ove tehnologije. U narednim godinama očekuje se dolazak velikog broja IoMT uređaja koji mogu sadržavati komponente koje će dovesti do problema interoperabilnosti i problema povezanih s privatnošću (6). Postoji veliki broj problema narušavanja privatnosti pacijenata kojima su izloženi prilikom korištenja IoMT uređaja među kojima su najvažniji sljedeći problemi:

- Nedovoljno razvijena svijest pacijenata o metodama, količini i vrsti podataka koje IoMT uređaji prikupljaju što posljedično dovodi do manje opreznosti i veće izloženosti hakerskim napadima;
- Okruženje u kojem se koriste IoMT uređaji koje podrazumijeva više korisnika koji koriste iste uređaje;
- IoMT uređaji uglavnom imaju nizak nivo kontrole te pacijenti koji koriste ove uređaje nemaju mogućnost upravljanja svojom privatnošću i podacima koji se prikupljaju;
- Za umrežavanje IoMT uređaja i prenos i razmjenu podataka koji oni prikupljaju koriste se bežične komunikacijskih mreže što se često može zloupotrijebiti na način da se te mreže "prisluškuju" u cilju dobivanja povjerljivih podataka o pacijentima;
- Pohranjivanje podataka o pacijentu u „oblaku" stvara dodatne mogućnosti cyber kriminalcima da pristupe i zloupotrijebe pohranjene podatke;
- Nedovoljna zaštita privatnosti-brojne su mogućnosti za zloupotrebu IoMT uređaja koje mogu rezultirati narušavanjem privatnosti osobama koje koriste takve uređaje. Jedan od primjera je da se IoMT uređaji koji posjeduju ugrađenu kameru mogu iskoristiti za neovlašteno snimanje audio i video zapisa;
- Ranjivosti aplikacija-propusti programera mogu dovesti do toga da napadač pokrene vlastiti kod na uređaju, što mu onda dozvoljava prikupljanje osjetljivih informacija;
- IoMT uređaji u svome radu prikupljaju i obrađuju jako velike količine podataka što dobro obučenim kriminalcima može omogućiti da na osnovu njih zaključuju različite osjetljive informacije;
- Nedostatak globalne standardizacije stvara dodatni prostor za zloupotrebu podataka i narušavanje privatnosti pacijenata.

Obzirom da se upotreba IoMT uređaja nastavlja širiti velikom brzinom, problem zaštite privatnosti korisnika tih uređaja postaje sve veći. Takođe količina podataka koji se obrađuju i generišu MIoT uređajima eksponencijalno raste što u konačnici dovodi do veće izloženosti povjerljivim medicinskim podacima. Pacijentove informacije o privatnosti postoje u svim fazama tj. prilikom prikupljanja podataka, prijenosa podataka, pohrane u oblaku i republikacije podataka (7). Dalji razvoj IoMT uređaja morat će osigurati adekvatne mehanizme zaštite sigurnosti i privatnosti korisnika tih uređaja.

4 MODELI ZAŠTITE

Postoje različiti oblici prijetnji po sigurnost IoMT uređaja koje se prema obliku napada mogu razvrstati u tri grupe. U prvu grupu spadaju prijetnje čija je manifestacija napada hardver, drugu grupu čine prijetnje koje napade vrše putem zlonamjernog softvera, a u treću grupu spadaju prijetnje koje napadaju podatke u toku njihovog prijenosa. Kao odgovor na pomenute prijetnje koriste se različite zaštitne mjere IoMT uređaja a neke od njih su sljedeće:

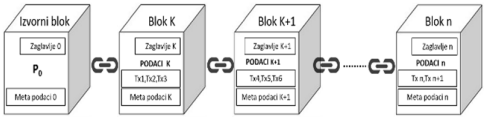
- Zaštitne mjere za nosive IoMT uređaje;
- Zaštitne mjere za mobilne IoMT uređaje;

- Zaštitne mjere za progutave IoMT uređaje;
- Zaštitne mjere za stacionarne IoMT uređaje;
- Zaštitne mjere za ambijentalne IoMT uređaje;
- Zaštitne mjere za implantabilne IoMT uređaje;
- Zaštitne mjere za IoMT komunikacijske uređaje;
- Zaštitne mjere za IoMT uređaje za elektronsko vođenje zdravstvenih zapisa.

Kao i u slučaju bilo kojeg IoT okruženja, sigurnosni mehanizmi su podijeljeni u dvije vrste, sigurnosni mehanizmi bazirani na softveru i sigurnosni mehanizmi bazirani na hardveru. Sigurnosni mehanizmi koji su softverskog tipa imaju ugrađene matematičke metode koje omogućavaju softversku zaštitu sistema. Sigurnosni mehanizmi koji su hardverskog tipa bazirani su na enkripciji poput infrastrukture javnih ključeva, naprednih standarda šifriranja, i kriptografije eliptične krivulje. Softverski bazirani mehanizmi zahtijevaju dijeljene temeljne parametre sa serverom ili s drugim uređajima. Prednost ove vrste sigurnosnih mehanizama ogleda se u činjenici što oni zahtijevaju relativno malu računarsku kompleksnost u smislu snage i pohrane uz istovremeno nuđenje visokog nivoa efikasnosti. Treba napomenuti da dijeljeni temeljni parametri nisu potrebni za asimetrične protokole.

Kao što je to slučaj i sa drugim IoT uređajima, IoMT uređaji se suočavaju sa izazovom brzog plasiranja novih proizvoda na tržište, zbog čega se zahtjevi sigurnosni često stavljaju u drugi plan. IoMT uređaji često u radu razmjenjuju osjetljive i povjerljive podatke čijom bi se zloupotrebom mogla ugroziti sigurnost i privatnost korisnika tih uređaja. Pomenuti izazovi nameću potrebu za iznalaženjem rješenja odnosno modaliteta zaštite sigurnosti i privatnosti korisnika IoMT uređaja, a u nastavku rada ukratko će biti predstavljeni neki od tih modela.

- **Blockchain model** podrazumijeva implementaciju metoda šifriranja fokusiranim na atributima i njihovog kombinovanja s blockchainom tehnologijom za dijeljenje i pohranu medicinskih podataka između aktera uključenih u korištenje IoMT uređaja. Koristeći enkripciju baziranu na atributima politike ključa kao i enkripciju baziranu politici šifriranog teksta omogućava se sigurno dijeljenje i pohranjivanje podataka. Snaga ovog modela je u omogućavanju pouzdanog upravljanja ključevima za „cloud-servere“ kao i medicinske implantabilne uređaje kao i posjedovanje ugrađenih mehanizama kojima se dozvoljava pristup podacima isključivo autorizovanim korisnicima. Pomenuti mehanizmi osiguravaju uspostavljanje sigurne veze između IoMT uređaja uz istovremeno reduciranje troškova prijenosa i drugih troškova te ukupnog računarskog opterećenja.



Shema 3: Pojednostavljena shema Blockchain-a

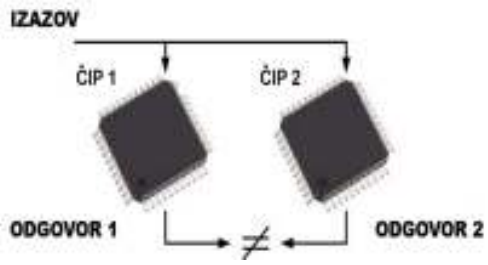
Jedan od nedostataka ovog modela je u tome što se podaci koji su već pohranjeni u blokchain-u ne mogu naknadno mijenjati kao i činjenica da model zanemaruje „napade iznutra“. Takođe model zahtjeva korištenje pouzdanog autoriteta treće strane te u slučaju da je treća strana pretrpjela napade cyber kriminala, podaci korisnika IoMT uređaja mogu biti ugroženi.

Model autentifikacije - autentifikacija je postupak utvrđivanja je li tvrdnja istinita, obično tvrdnja o nečijem identitetu. Model autentifikacije

osigurava vjerodostojan potpis za prijenos kriptiranih okvirova između komunikacijskih čvorova i nudi veći nivo sigurnosti prijenosa podataka između korisnika IoMT uređaja i ljekara. Zdravstveni informacioni sistemi moraju biti otporni na sigurnosne prijetnje kao što su krivotvorenje i otkrivanje zdravstvenih izvještaja, lažiranje servera, a također i otporni na neovlašteni pristup IoMT uređajima. Zbog toga je vrlo važno da takvi sistemi posjeduju adekvatne mehanizme za autentifikaciju korisnika.

Postoji nekoliko načina za osiguravanje mehanizama za autentifikaciju koji su se pokazali kao prihvatljivi u smislu pouzdanosti. Jedan od hardverski baziranih mehanizama zaštite je autentifikacijski sistem koji koristi fizičke neklonirane funkcije (engl. Physical Unclonable Functions-PUFs). Umjesto da koriste jedan kriptografski ključ, PUF-ovi implementiraju mehanizam "provjere autentičnosti izazov-odgovor". Kada se na strukturu primijeni električni podražaj, ona reagira na nepredvidiv (ali ponovljiv način) zbog složene interakcije podražaja s fizičkom mikrostrukturom uređaja. (3) PUF je fizički objekt koji odašilje izlaz (odgovor) za određeni unos (izazov) koji služi kao jedinstveni identifikator. Zbog integralne fizičke varijabilnosti u integrisanim krugovima, može pružiti mehanizam izazov-odgovor za sigurnosne aplikacije. Kao što naziv govori, PUF je jedinstven i ne može se klonirati zbog proizvoljnih i nepopravljivih učinaka procesa proizvodnje IC-a. Svaki PUF je drugačiji (Shema 4).

Jedinstvenost, pouzdanost i slučajnost glavne su karakteristike PUF-a. Postoje dvije vrste PUF-ova: jaki i slabi. Razlika je povezana s brojem odgovora koji se mogu generisati.



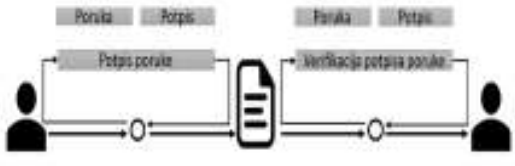
Shema 4: PUF generira izlaze specifične za svaki pojedini VLSI čip

Drugi mehanizam za zaštitu SNP-a naziva se umrežavanje imenovanih podataka (engl. Named data networking-NDN). Umrežavanje imenovanih podataka koristi usmjeravanje temeljeno na imenu i predmemoriranje unutar mreže za podršku učinkovite isporuke sadržaja, što ga čini pouzdanom mrežnom tehnologijom koja može povećati efikasnost i sigurnost isporuke podataka u lancu blokova.

Jedan od nedostataka na koji treba ukazati odnosi se na otežanu integraciju IoMT-a sa Blockchain-om. To se prije svega odnosi na nekompatibilnost u smislu potrebnih resursa za rad. Proces rudarenja blockchainu zahtijevaju složenije računarske resurse kao i veću potrošnju energije za razliku od IoMT uređaja.

Modeli privatnosti – proučavajući istraživanja koja su rađena na temu zaštite privatnosti korisnika IoMT uređaja može se uočiti nekoliko modela. Uz zahtjev zaštite privatnosti modeli također uzimaju za cilj očuvanje transparentnosti, aktuelnosti i dostupnosti zdravstvenih podataka. Najvažniji modeli privatnosti su nabrojani u nastavku. Reverzibilna tehnika skrivanja podataka s dvostrukim okvirom je model koji omogućava perceptivnu kvalitetu podataka sa IoMT uređaja na visokom nivou i računarsku efikasnost, što je omogućilo njegovo

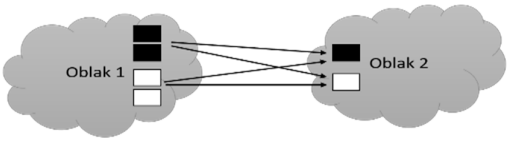
korištenje u IoMT mreži. Drugi značajan model je dvostruki potpis u algoritmu digitalnog potpisa eliptične krivulje koji je usmjeren na čuvanje povjerljivost podataka koji se prenose iz IoMT uređaja u oblak.



Shema 5: Dizajn sheme dvostrukog potpisa korištenjem ECDSA

Online skupovi podataka je model koji se koristi se za procjenu i validaciju i efikasnosti sistema koji koriste IoMT uređaje. Nedostatak ovog modela izražen je u pogledu nedovoljne skalabilnosti u odnosu na cyber napade. Model slijepe serijske enkripcije jedan je od modela koji nudi zaštitu privatnosti korisnika IoMT uređaja uz istovremenu efikasnost za uređaje sa ograničenim resursima.

Modeli bazirani na vještačkoj inteligenciji- proučavajući istraživanja koja su rađena na temu zaštite sigurnosti i privatnosti korisnika IoMT uređaja mogu se izdvojiti dva ključna modela a to su model mašinskog učenja i model velikih podataka. Mašinsko učenje kao moćan alat vještačke inteligencije ima veoma važnu ulogu u poboljšanju mnogih performansi IoMT uređaja pa tako i u domenu zaštite sigurnosti i privatnosti. Reprezentativni modeli bazirani na mašinskom učenju su model za otkrivanje anomalija u mreži za IoT aplikacije te algoritamski model mreže dubokih uvjerenja. Jedan od modela baziranih na tehnikama velikih podataka je model automatizacije koji je usmjeren na ograničavanje otkrivanja ličnih podataka zanemarivanjem ugrožavajućih podataka putem metoda koje zahtijevaju uklanjanje određenih identifikatora.



Shema 6: Model hibridnog izvršavanja-podjela rada u javnom i privatnom oblaku

Drugi model iz ove grupe je model hibridnog izvršavanja koji štiti integritet podataka kroz podjelu rada u javnom i privatnom oblaku.

ZAKLJUČAK

Internet medicinskih stvari podskup je tehnologija interneta stvari koji se sastoji od medicinskih uređaja povezanih na mrežu zdravstvene zaštite. IoMT uređaji omogućuju praćenje zdravstvenog stanja pacijenata bez ljudske intervencije integracijom automatizacije, međufaznih senzora i vještačke inteligencije temeljene na mašinskom učenju. IoMT tehnologija povezuje pacijente s ljekarima i drugim zdravstvenim radnicima putem medicinskih uređaja, omogućujući udaljeni pristup prikupljanju, obradi i prijenosu medicinskih podataka preko zaštićene mreže. Međutim, cyber kriminalci često koriste slabo zaštićeni IoMT za različite oblike cyber napada, dovodeći u opasnost privatnost i sigurnost podataka. Ovo je moguće zbog toga što IoMT, kao i druge IoT imaju nedostatak u vidu nedovoljno standardizovanih sigurnosnih kontrola.

Veliki broj IoMT uređaja imaju nepouzdane provjere autentičnosti što dovodi do povećanog rizika neovlaštenog pristupa tim uređajima. I drugi IoT uređaji su izloženi sigurnsonim prijetnjama ali posljedice koje mogu proisteći mnogo su veće kod napada na IoMT uređaje obzirom da mogu prouzrokovati i gubitke ljudskih života. Doprinos ovog rada ogleda se u ukazivanju na prijetnje po sigurnost i privatnost korisnika IoMT uređaja a u tom pogledu se

najviše fokusirao na predstavljanje modela zaštite sigurnosti i privatnosti tih uređaja. Obzirom da je primjena IoMT uređaja u ekspanziji očekivati je da će se srazmjerno povećanju broja uređaja povećavati i hakerski napadi što će u budućnosti predstavljati veliki izazov u pogledu zaštite sigurnosti i privatnosti podataka o pacijentima.

Dalji razvoj IoMT uređaja morat će osigurati adekvatne mehanizme zaštite sigurnosti i privatnosti korisnika tih uređaja.

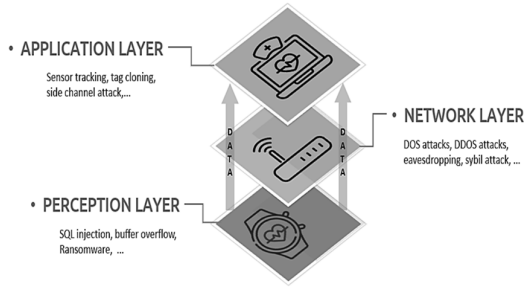
LITERATURA

1. Alonso Virgos, L., et all., (2021). Internet of Medical Things: Current and Future Trends, by Cardona, M., Solanki, V., Cena, G.C. (Eds.): Internet of Medical Things-Paradigm of Wearable Devices, CRC Press, p. 19-35.
2. Anandarajan, M., Malik S., Schumacher, U. (2018). Protecting the Internet of medical things: A situational crime-prevention approach, Cogent Medicine ,Volume 5, 2018, Issue 1
3. Chatterjee, U., Chakraborty, R.S., Mukhopadhyay, D (2017). A PUF-Based Secure Communication Protocol for IoT, ACM Transactions on Embedded Computing Systems, Volume 16, Issue 3, Article No.: 67pp 1–25., https://doi.org/10.1145/3005715
4. Guarda T., Augusto M.F., Barrionuevo O., Pinto F.M. (2018). Next-Generation Mobile and Pervasive Healthcare Solutions. IGI Global; Hershey, PA, USA. Internet of Things in pervasive healthcare systems; pp. 22–31.
5. Guntur, S.R., Gorrepati, R., Dirisala, V.R. (2018). Internet of Medical Things: Remote Healthcare and Health Monitoring Perspective by Hassanien, A., Dey, N., & Borra, S. (Eds.): Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications, CRC Press, p. 271-298.https://unvi.edu.ba/Files/zbornici/SKEI/Zbornik_radova_skei_2019v3.pdf
6. Keerthana, A., Karthiga (2022). Performance Assessment of IoMT Services and Protocols, by R. J. Hemalatha, D. Akila, D. Balaganesh , Anand Paul (Eds.): The Internet of Medical Things (IoMT): Healthcare Transformation (Advances in Learning Analytics for Intelligent Cloud-IoT Systems), Wiley-Scrivener; 1st edition, p. 173-185.
7. Sun,W., et. all. (2017). Security and Privacy in the Medical Internet of Things: A Review, Security and Communication Networks Volume 2018, Article ID 5978636, https://doi.org/10.1155/2018/5978636
8. Šimić, O., Ćosić, M. (2019). Backup system of server data based on Microsoft Data Protection Manager 2012 R2, Conference proceedings of the 4th International Student Conference of Economics and Informatics "SKEI 2018", University "Vitez", BiH, May 2019, p. 503-512.,

1 INTRODUCTION

The Internet, a crucial technology of the information age in which we live, is increasingly based on wireless communication platforms. From its emergence until today, through the production and distribution of digital information, the Internet represents a huge potential for increasing the performance of all forms of human activities. Until recently, only desktop or laptop computers, smartphones and similar devices were networked. Today's level of Internet development is focused on the development of complex automation through the networking of various types of devices equipped with sensors, such as numerous household appliances, smart self-driving cars, various measuring devices, medical equipment and devices, etc. The listed devices are not only connected to the broadband network, but also connect to each other, which enables them to exchange information, for example. through M2M (machine to machine) technology. We call the communication network created in this way the Internet of Things or IoT for short. The emergence of IoT was made possible thanks to the appearance of cheap computer chips that, due to their affordability, are embedded in many things, from simple measuring instruments to complicated medical devices, cars, ships and airplanes. All the mentioned things become "smart" with the help of digital intelligence, which enables them to exchange a large amount of data without human intervention. Therefore, any physical entity can be turned into IoT if that entity is enabled to connect to the Internet.

At the very beginning of IoT development, the primary goal was to improve the performance of production and business. Recently, the emphasis in the development of IoT is on the development of "smart houses" or "smart cities". The concept of IoT is ubiquitous in all segments of human activity, so it also finds its application in medicine through a special segment of IoT called the Internet of Medical Things or IoMT for short. IoMT plays a key role in remote health care and monitoring to increase the efficiency of medical devices, and the speed and availability of medical services (5). IoMT refers to a wide range of medical devices and applications that connect to health information systems (HIS) using computer networks. As soon as it appeared, IoMT showed significant potential in terms of improving healthcare by enabling remote monitoring of patients' conditions. IoTs enable the implementation of a wide range of applications from implantable medical devices to wireless body area networks (WBANs). Therefore, IoMT is widely used to improve health care and is considered a pillar of new ubiquitous health services (4). Scheme 1 shows that the structure of IoMT consists of perception layer, network layer and application layer.



Scheme 1: IoMT structure and types of attacks

Each of the mentioned layers has a specific task, so the perception layer is in charge of obtaining health data through various IoMT devices (e.g. ECG monitoring devices). The network layer processes and transmits the collected data through transport protocols. The task of the application layer is to use the obtained information to provide adequate medical services and patient needs.

The application of the Internet of Things in medicine has made a big change because until recently the dominant means of recording data on the patient's condition

was pen and paper. Of course, even before the advent of IoT, information and communication technologies enabled the way of recording patient data to be radically improved with the help of computers and health information systems. But with the advent of IoT, an even more significant and radical shift for the better is taking place, since completely new possibilities are opening up, such as the exchange of data between medical devices without the intervention of doctors and other medical personnel. In this way, it is possible to remotely monitor important parameters related to the health of patients. However, cybercriminals often use weakly protected IoMTs for various forms of cyberattacks, putting privacy and data security at risk. This is possible because IoMT, as well as other IoT devices, lack standardized security controls. A large number of IoMT devices have unreliable authentications leading to an increased risk of unauthorized access to those devices. In order to reduce the risks of cyber attacks when developing medical security systems, several key requirements should be taken into account.

The first of these requirements is data integrity, which refers to the fact that all values meet semantic standards and includes two levels of accuracy and reliability. Data integrity can be divided into four categories, namely entity integrity, domain integrity, referential integrity, and user-defined integrity , which can be maintained against foreign keys, constraints, rules, and regulations. The next requirement is data usability, which is needed to ensure that data or data systems can only be used by authorized users. Big data offers not only great benefits but also critical challenges, such as dirty data and non-standard data. In addition, data corruption or data loss caused by unauthorized access also further destroys data usability. Also, every organization needs a strategy for business continuity and recovery from catastrophic data loss. (8)

Data control in the form of access control to medical data is the third of the key security requirements and is an effective tool for monitoring the use of resources, joint measure of findings and monitoring of abnormal events. Control content generally includes users, cloud service providers, and access and operational files. The fourth requirement relates to the confidentiality of patient data. Patient data can be divided into two categories: general records and sensitive data. Sensitive data, also called patient privacy data, includes mental state, sexual orientation, sexual function, infectious diseases, fertility status, drug addiction and identity information. It is necessary to ensure that sensitive data will not be leaked to unauthorized users. Even if the data is intercepted, it is necessary to ensure that the expressed information is incomprehensible to unauthorized users.

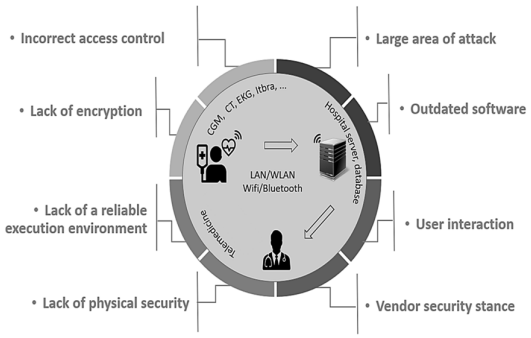
SECURITY CHALLENGES OF THE MEDICAL INTERNET OF THINGS

Although the application of IoMT technologies to healthcare brings many benefits, it also brings great security challenges. Other IoT devices are also exposed to security threats, but the consequences that can arise are much greater in the case of attacks on IoMT devices, since they can also cause loss of human life. It is noticeable that in the last few years the health sector has been at the very top in terms of the number of hacker attacks.

"Smart" IoMT devices are designed to correctly perform certain tasks, but due to the lack of necessary security functions, they are susceptible to cyber attacks, which is especially pronounced when they are connected to unprotected networks, or even to the same network as the rest of the organization's infrastructure. Security is one of the most concerning aspects of the field of IoMT (1). There are a number of security issues (Scheme 2) that IoMT devices are

exposed to, the most important of which are the following:

- Incorrect access control - the security system of the device often allows the services offered by the IoMT device to be available not only to the owner of the device but also to other people. Also, in many cases devices of the same model are delivered with the same predefined password;
- Very large attack surface - IoT devices offer a large number of services over the Internet. The greater the number of such services, the greater the possible attack surface;
- Outdated Software - IoMT devices often ship with out-of-date software. The increase in the risk of unwanted attacks is proportional to the length of time that passes from the moment of production of the IoMT device to its implementation in an information system;
- Lack of encryption has the consequence that on the network path between the device and its endpoint, network traffic can be inspected and sensitive data can be accessed. It is often the case that API tokens are stored on the device in plain text or weak cryptographic algorithms are used;
- Lack of a reliable execution environment - the vast majority of IoMT devices are basically general purpose computers that can run specific software. This fact is used by cybercriminals to install their own software that can cause various types of security problems and disable the proper functioning of the device;
- Vendor Security Attitude - In some cases, the vendor does not have a process in place to address security issues;
- Insufficient physical security - In many cases, the necessary attention is not paid to the physical security of the device. Because of this, it may happen that unauthorized persons who possess the appropriate level of IT knowledge have access to the hardware of the device;
- User interaction - is reflected in the fact that not enough attention is paid to creating adequate documentation about the device, as well as attention in terms of design and usability, which results in users not being motivated or unable to configure security settings themselves.



Scheme 2: The IoMT environment and the most common security threats

One of the shortcomings of IoMT devices in terms of security is that when designing them, more attention is paid to usability than security. Due to the aforementioned lack of IoMT devices are very vulnerable to cyber attacks. Weak resistance to cyber attacks is a serious problem considering the consequences that can occur, which in the worst case can result in the loss of human lives. Therefore, it is imperative that patients, physicians, hospitals, and other healthcare facilities understand the potential IoMT threats in order to reduce future attack and (2).

2 PRIVACY CHALLENGES OF MEDICAL INTERNET OF THINGS

Misuse and unauthorized access to IoMT devices can also compromise patient privacy, which can have far-reaching consequences. Some of the possible consequences are the infliction of mental

pain and emotional damage due to misuse of medical records. IoMT is a technological paradigm that is developing at a high speed, which is contributed to by the increasingly rapid development of information and communication technologies, which makes it difficult to solve many patient privacy problems that arise when using this technology. In the coming years, a large number of IoMT devices are expected to arrive that may contain components that will lead to interoperability and privacy-related issues (6). There are a number of problems of violation of the privacy of patients that they are exposed to when using IoMT devices, among which the following problems are the most important:

- Patients' insufficient awareness of the methods, amount and type of data that IoMT devices collect, which consequently leads to less caution and greater exposure to hacker attacks;
- An environment where IoMT devices are used, which implies multiple users using the same devices;
- IoMT devices generally have a low level of control and patients using these devices do not have the ability to manage their privacy and the data that is collected;
- Wireless communication networks are used to network IoMT devices and transfer and exchange the data they collect, which can often be misused in such a way that these networks are "eavesdropped" in order to obtain confidential patient data;
- Storing patient data in the "cloud" creates additional opportunities for cybercriminals to access and misuse stored data;
- Insufficient privacy protection - there are numerous opportunities for misuse of IoMT devices that can result in the violation of privacy of people using such devices. One example is that IoMT devices that have a built-in camera can be used for unauthorized audio and video recording;
- Application vulnerabilities - developer omissions can allow an attacker to run their own code on a device, which then allows them to collect sensitive information;
- In their work, IoMT devices collect and process very large amounts of data, which can enable well-trained criminals to conclude various sensitive information based on them;
- The lack of global standardization creates additional space for data misuse and violation of patient privacy.

As the use of IoMT devices continues to expand at a rapid pace, the problem of protecting the privacy of users of these devices is becoming greater. Also, the amount of data processed and generated by MIoT devices is growing exponentially, which ultimately leads to greater exposure of confidential medical data. The patient's privacy information exists in all stages, i.e. during data collection, data transfer, cloud storage and data republication (7). Further development of IoMT devices will have to ensure adequate mechanisms to protect the security and privacy of the users of these devices.

3 PROTECTION MODELS

There are different forms of threats to the security of IoMT devices, which can be classified into three groups according to the form of attack. The first group includes threats whose manifestation is hardware attacks, the second group consists of threats that attack through malicious software, and the third group includes threats that attack data during their transmission.

In response to the mentioned threats, various protective measures of IoMT devices are used and some of them are as follows:

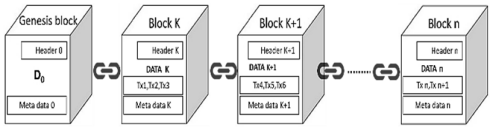
- Safeguards for wearable IoMT devices;

- Safeguards for mobile IoMT devices;
- Safeguards for ingestible IoMT devices;
- Protective measures for stationary IoMT devices;
- Protective measures for ambient IoMT devices;
- Safeguards for implantable IoMT devices;
- Safeguards for IoMT communication devices;
- Safeguards for IoMT electronic health record keeping devices.

As with any IoT environment, security mechanisms are divided into two types, software-based security mechanisms and hardware-based security mechanisms. Security mechanisms that are of the software type have built-in mathematical methods that enable software protection of the system. Hardware-based security mechanisms are based on encryption such as public key infrastructure, advanced encryption standards, and elliptic curve cryptography. Software-based mechanisms require shared underlying parameters with the server or with other devices. The advantage of this type of security mechanisms is reflected in the fact that they require relatively little computational complexity in terms of power and storage while simultaneously offering a high level of efficiency. It should be noted that shared underlying parameters are not required for asymmetric protocols.

As with other IoT devices, IoMT devices face the challenge of bringing new products to market quickly, which often puts security requirements on the back burner. IoMT devices often exchange sensitive and confidential data during operation, the misuse of which could endanger the security and privacy of the users of these devices. The mentioned challenges impose the need to find a solution, that is, a modality to protect the security and privacy of users of IoMT devices, and some of those models will be briefly presented in the continuation of the work.

- **Blockchain model** implies the implementation of attribute-focused encryption methods and their combination with blockchain technology to share and store medical data between actors involved in the use of IoMT devices. Using key policy attribute-based encryption as well as ciphertext policy-based encryption enables secure data sharing and storage. The strength of this model is in enabling reliable key management for "cloud-servers" as well as medical implantable devices, as well as having built-in mechanisms that allow access to data only to authorized users. The mentioned mechanisms ensure the establishment of a secure connection between IoMT devices while at the same time reducing transmission costs and other costs and the overall computing load.

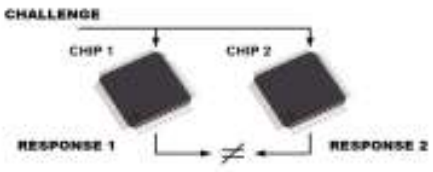


Scheme 3: Simplified scheme of Blockchain

One of the disadvantages of this model is that the data already stored in the blockchain cannot be changed afterwards, as well as the fact that the model ignores "attacks from the inside". Also, the model requires the use of a trusted third-party authority, and in the event that the third party has suffered cybercrime attacks, the data of IoMT device users may be compromised.

- **Authentication model -** authentication is the process of determining whether a claim is true, usually a claim about someone's identity. The authentication model ensures a credible signature for the transfer of encrypted frames between communication nodes and offers a higher level of data transfer

security between the user of the IoMT device and the physician. Health information systems must be resistant to security threats such as forgery and disclosure of health reports, server spoofing, and also resistant to unauthorized access to IoMT devices. That is why it is very important that such systems have adequate mechanisms for user authentication.
There are several ways to ensure authentication mechanisms that have proven to be acceptable in terms of reliability. One of the hardware-based protection mechanisms is an authentication system that uses Physical Unclonable Functions (PUFs). Instead of using a single cryptographic key, PUFs implement a "challenge-response authentication" mechanism. When an electrical stimulus is applied to a structure, it responds in an unpredictable (but reproducible) manner due to the complex interaction of the stimulus with the physical microstructure of the device. (3) A PUF is a physical object that transmits an output (response) for a specific input (challenge) that serves as a unique identifier. Due to the integral physical variability in integrated circuits, it can provide a challenge-response mechanism for security applications. As the name suggests, the PUF is unique and cannot be cloned due to the arbitrary and irreversible effects of the IC manufacturing process. Every PUF is different (Scheme 4).



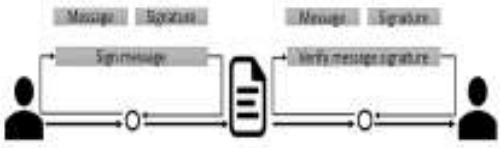
Scheme 4: PUF generates outputs specific to each individual VLSI chip

Uniqueness, reliability and randomness are the main characteristics of PUF. There are two types of PUFs: strong and weak. The difference is related to the number of responses that can be generated.

Another mechanism for SNP protection is called named data networking (NDN). Named Data Networking uses name-based routing and intra-network caching to support efficient content delivery, making it a reliable network technology that can increase the efficiency and security of blockchain data delivery.

One of the shortcomings that should be pointed out is related to the difficult integration of IoMT with Blockchain. This primarily refers to incompatibility in terms of the required resources for work. The blockchain mining process requires more complex computing resources as well as higher energy consumption in contrast to IoMT devices.

- **Privacy models -** studying the research that has been done on the topic of protecting the privacy of users of IoMT devices, several models can be observed. Along with the requirement of privacy protection, the models also aim to preserve the transparency, topicality and availability of health data. The most important privacy models are listed below. A double-frame reversible data hiding technique is an enabling model perceptive quality of data from IoMT devices at a high level and computational efficiency, which enabled its use in the IoMT network. Another notable model is the double signature in the elliptic curve digital signature algorithm, which is aimed at preserving the confidentiality of data transmitted from IoMT devices to the cloud.

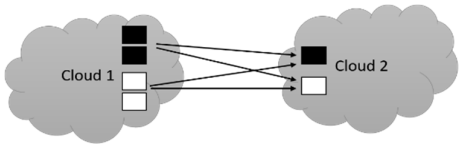


Scheme 5: Design of a dual signature scheme using

Online Datasets is a model used to evaluate and validate the effectiveness of systems using IoMT devices. The lack of this model is expressed in terms of insufficient scalability in relation to cyber attacks. The blind serial encryption model is one of the models that offers privacy protection for IoMT device users while simultaneously being efficient for resource-constrained devices.

- **Models based on artificial intelligence** - studying the research that was done on the topic of protecting the security and privacy of users of IoMT devices, two key models can be distinguished, namely the machine learning model and the big data model. Machine learning as a powerful tool of artificial intelligence has a very important role in improving many performances of IoMT devices and also in the domain of security and privacy protection. Representative models based on machine learning are network anomaly detection model for IoT applications and deep belief network algorithmic model. One of the models based on big data techniques is the automation model, which aims to limit the disclosure of personal data by ignoring compromising data through methods that require the removal of certain identifiers.

  Another model from this group is a hybrid execution model that protects data integrity through the division of labor in the public and private cloud.



Scheme 6: Hybrid execution-

4 CONCLUSION

Medical Internet of Things is a subset of Internet of Things technology consisting of medical devices connected to a healthcare network. IoMT devices enable monitoring of patients' health status without human intervention by integrating automation, interphase sensors and artificial intelligence based on machine learning. IoMT technology connects patients with doctors and other healthcare professionals via medical devices, enabling remote access to the collection, processing and transmission of medical data over a secure network. However, cybercriminals often use weakly protected IoMTs for various forms of cyberattacks, putting privacy and data security at risk. This is possible because IoMT, as well as other IoTs, lack standardized security controls. A large number of IoMT devices have unreliable authentication which leads to an increased risk of unauthorized access to those devices. Other IoT devices are also exposed to security threats, but the consequences that can arise are much greater in the case of attacks on IoMT devices, since they can also cause loss of human life.

The contribution of this paper is reflected in pointing out the threats to the security and privacy of users of IoMT devices, and in this regard it mostly focused on the presentation of the security and privacy protection model of those devices. Considering that the application of IoMT devices is expanding, it is expected that in proportion to the increase in the number of devices, hacker attacks will also increase, which in the future will represent a major challenge in terms of protecting the security

and privacy of patient data. Further development of IoMT devices will have to ensure adequate mechanisms to protect the security and privacy of the users of these devices.

LITERATURE

1. Alonso Virgos, L., et al., (2021). Internet of Medical Things: Current and Future Trends, by Cardona, M., Solanki, V., Cena, GC (Eds.): Internet of Medical Things-Paradigm of Wearable Devices, CRC Press, p. 19-35.
2. Anandarajan , M., Malik S., Schumacher, U. (2018). Protecting the Internet of medical things: A situational crime-prevention approach, Cogent Medicine, Volume 5, 2018, Issue 1
3. Chatterjee, U., Chakraborty, RS, Mukhopadhyay, D (2017). A PUF-Based Secure Communication Protocol for IoT, ACM Transactions on Embedded Computing Systems, Volume 16, Issue 3, Article No.: 67pp 1–25., https://doi.org/10.1145/3005715
4. Guarda T., Augusto MF, Barrionuevo O., Pinto FM (2018). Next-Generation Mobile and Pervasive Healthcare Solutions. IGI Global; Hershey, PA, USA. Internet of Things in pervasive healthcare systems; pp. 22–31.
5. Guntur, SR, Gorrepati, R., Dirisala, VR (2018). Internet of Medical Things: Remote Healthcare and Health Monitoring Perspective by Hassanien, A., Dey, N., & Borra, S. (Eds.): Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications, CRC Press, p. 271-298.
6. https://unvi.edu.ba/Files/zbornici/SKEI/Zbornik_radova_skei_2019v3.pdf
7. Keerthana, A., Karthiga (2022). Performance Assessment of IoMT Services and Protocols, by RJ Hemalatha, D. Akila, D. Balaganesh, Anand Paul (Eds.): The Internet of Medical Things (IoMT): Healthcare Transformation (Advances in Learning Analytics for Intelligent Cloud-IoT Systems) , Wiley-Scrivener; 1st edition, p. 173-185.
8. Sun, W., et. all. (2017). Security and Privacy in the Medical Internet of Things: A Review, Security and Communication Networks Volume 2018, Article ID 5978636, https://doi.org/10.1155/2018/5978636
9. Šimić, O., Ćosić, M. (2019). Backup system of server data based on Microsoft Data Protection Manager 2012 R2, Conference proceedings of the 4th International Student Conference of Economics and Informatics "SKEI 2018", University "Vitez", BiH, May 2019, p. 503-512.,