IoT sigurnosni izazovi

Soldat, Mihaela

Sveučilište Jurja Dobrile u Puli
Tehnički fakultet u Puli

Mihaela Soldat

IOT SIGURNOSNI IZAZOVI

Završni rad

Pula, rujan, 2024. godine

Sveučilište Jurja Dobrile u Puli
Tehnički fakultet u Puli

Mihaela Soldat

IOT SIGURNOSNI IZAZOVI

Završni rad

JMBAG: 0303100973, redoviti student

Studijski smjer: Računarstvo

Predmet: Sustavi temeljeni na znanju

Znanstveno područje: Tehničke znanosti
Znanstveno polje: Računarstvo
Znanstvena grana:
Mentor: izv. prof. dr. sc. Nicoletta Saulig
Komentor: izv. prof. dr. sc. Željka Tomasović

Pula, rujan, 2024 godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Mihaela Soldat, kandidat za prvostupnika računarstva ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljeni način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

Soldat

U Puli, 29.6.2024.

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, Mihaela Soldat dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj Završni rad pod nazivom IoT sigurnosni izazovi

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

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

U Puli, 29.8.2024.

Potpis

Soldat

Zahvala

Želim izraziti duboku zahvalnost svojim mentoricama, izv. prof. dr. sc. Nicoletti Saulig i izv. prof. dr. sc. Željki Tomasović, koje su me svojim savjetima i podrškom vodile kroz izradu ovog rada. Njihova stručnost i strpljenje omogućili su mi da se uspješno nosim s izazovima istraživanja.

Posebno se zahvaljujem organizatorima konferencije SpliTech 2024, koji su prepoznali vrijednost mog rada i omogućili mi priliku da ga predstavim na međunarodnom skupu. Prihvaćanje mog rada na konferenciji bilo je veliko priznanje i poticaj za daljnje istraživanje sigurnosnih izazova u IT tehnologijama. Rad nosi naslov: Security challenges of the Internet of Things, https://splitech.org/assets/programme%20final.pdf

Na kraju, neizmjerno hvala mojoj obitelji i prijateljima na bezuvjetnoj podršci i motivaciji tijekom cijelog mog akademskog puta.

Sadržaj

1. Uvod

Internet stvari (IoT) širok je pojam i kako se tehnologija nastavlja razvijati, postaje još širi. Internet stvari opisuje proširenje internetske povezanosti sa svakodnevnim uređajima koji su opremljeni senzorima, potrebnim softverom i raznim tehnologijama koje su dizajnirane za povezivanje uređaja i sustava koji razmjenjuju podatke putem Interneta, žično ili bežično. Na potrošačkom tržištu, tehnologija IoT-a odnosi se na proizvode koji omogućuju funkcionalnosti pametnog doma (eng. smart home), ali se koristi i u drugim sektorima kao što su zdravstvo, poljoprivreda i dr. Iako IoT stječe sve veću popularnost, sigurnost ostaje značajan problem. Cyber napadi slijede razvoj IoT-a i razvijaju se u skladu s njim, postajući sve sofisticiraniji. Budući da mnogi IoT uređaji nemaju ugrađenu sigurnost, povezivanje milijardi IoT uređaja povećava prijetnju i pruža mogućnost brojnih napada na uređajima. Potrebno je osigurati CIA funkcionalnosti (povjerljivost, integritet i dostupnost) putem enkripcije, redovitih ažuriranja uređaja i drugih sigurnosnih mjera [1]. Drugi izvori [2], navode da se CIA Trijada pokazala nedostatnom u kontekstu kibernetičke sigurnosti i da je, kao produžetak CIA-e, osiguravanje pouzdanosti, neporicanja, privatnosti, odgovornosti i mogućnost revizije ključno. Unatoč razvoju višestrukih sigurnosnih postupaka za zaštitu IoT uređaja od kibernetičkih napada, sigurnosni protokoli su još uvijek nekvalitetno dokumentirani, što može dovesti do toga da krajnji korisnici ne primjene sigurnosne mjere protiv napada [3]. Globalni podaci i platforma za poslovnu inteligenciju, Statista, izvijestili su da će broj uređaja povezanih IoT-om doseći približno 15 milijardi diljem svijeta do kraja 2023. Posljedično, svaki povezani uređaj podložan je kibernetičkim napadima bez sveobuhvatnih sigurnosnih protokola. Industrije koje koriste IoT tehnologiju, osobito one koje obrađuju vrlo povjerljive podatke, riskiraju teške posljedice nedovoljne sigurnosti IoT-a. Ovaj rad obrađuje sljedeće teme:

- pregled arhitekture Interneta stvari i izazova koje ona nosi
- pregled ranjivosti i cyber napada specifičnih za IoT
- sigurnosne preporuke za zaštitu IoT-a
- inovativni pristupi za unaprjeđenje IoT sigurnosti

2. Arhitektura Interneta stvari

Iako ne postoji standardizirana i dogovorena arhitektura, troslojna arhitektura je općeprihvaćena arhitektura u IoT-u, a uvedena je u inicijalnim fazama istraživanja [4].

Sastoji se od sljedećih slojeva, a svaki od slojeva podložan je sigurnosnim prijetnjama ,koje mogu iskoristiti povezanost slojeva i informacije koje one dijele [4]:

- perceptivni sloj (eng. Perception layer) - fizički sloj opremljen senzorima i aktuatorima za prikupljanje podataka
    - najčešće prijetnje uključuju [5]: prisluškivanje, spoofing napad, malware, prijetnje tijekom prijenosa
- mrežni sloj (eng. Network layer) - opremljen ruterima, služi za povezivanje s drugim uređajima ili serverima
    - često na meti Denial of Service (DoS) napada, povrede podataka, exploit napada, Man in the Middle (MitM) napada [5]
- aplikacijski sloj (eng. Application layer) - sloj koji komunicira s korisnikom
    - ranjiv na prijetnje poput malwarea i dr. [5]

3. Sigurnosni izazovi

Ovo poglavlje detaljno će objasniti ranjivosti Interneta stvari, prijetnje i napade specifične za IoT.

3.1 Ranjivosti Interneta stvari

Prema Nacionalnom Institutu Standarda i Tehnologija (NIST), ranjivost je slabost u informacijskom sustavu, koju prijetnje mogu iskoristiti kako bi naštetili sustavu. Najčešće IoT ranjivosti možemo podijeliti u četiri kategorije [6]: ranjivosti uzrokovane korisničkim rukovanjem, komunikacijske ranjivosti, ranjivosti firmwarea i softwarea te fizičke ranjivosti uređaja.

3.1.1 Ranjivosti uzrokovane korisničkim rukovanjem

Slabe lozinke i zanemarivanje ažuriranja

Mnogi IoT uređaji koriste prethodno zadane (default) i jednostavne lozinke [5]. Promjena lozinke uobičajena je praksa, ali korisnici često zanemaruju upute ili lozinku zamijene s lako pamtljivom. Ova navika povećava mogućnost preuzimanja kontrole nad uređajem od strane neautoriziranih osoba ili uređaja.

U slučajevima redovnih ažuriranja, korisnici ih ponekad ignoriraju. Problem nastaje kad se ažuriranja iznova i iznova zanemaruju jer sigurnosna ažuriranja za napade i viruse nisu primijenjena.

3.1.2 Komunikacijske ranjivosti

Uporaba nesigurnih komunikacijskih protokola

U IoT mrežama, uređaji su često povezani preko iste mreže, što znači da, u slučaju napada, napad može lako zahvatiti i druge uređaje unutar iste mreže. Ranjivi protokoli mogu biti odabrani zbog svojih boljih performansi i manjeg zahtjeva za procesorskom snagom u usporedbi s sigurnijim protokolima. Potrebno je uspostaviti ravnotežu između potrošnje resursa, koji su često ograničeni, i kvalitetnog sigurnosnog dizajna [5].

Nedostatak enkripcije tijekom prijenosa podataka

Sigurnost IoT sustava ovisi o zaštiti podataka prikupljenih od strane brojnih senzora na sloju percepcije. Enkripcijom se može osigurati sigurnost podatkovnih paketa i osjetljivih informacija od neovlaštenog pristupa. Međutim, većina IoT uređaja koristi manje pouzdane bežične medije ili, rjeđe, prenose podatke u obliku običnog teksta zbog ograničenih resursa za robusnije kriptografske algoritme. Ovi uređaji su skloniji curenju podataka, napadima ili presretanju podataka [2].

3.1.3 Ranjivosti firmwarea i softwarea

Firmware je programska podrška i podatci trajno zapisani u ROM-u, a predstavlja kombinaciju softverske podrške i sklopovlja. Omogućava osnovne strojne upute i komunikaciju između hardvera i softvera na uređaju.

Nedostatak redovnih softverskih ažuriranja

Za razliku od drugih tehnologija, IoT ne dobivaju ažuriranja tako često [7]. Nedostatak čestih ažuriranja softvera može ugroziti sigurnost i funkcionalnost IoT uređaja i podataka koje obrađuju.

Nesigurni mehanizmi ažuriranja

Uređaji s nesigurnim mehanizmima ažuriranja u većem su riziku od instaliranja zlonamjenrih komponenti. IoT uređaji mogu biti kompromitirani korumpiranim i neprovjerenim ažuriranjima, što može negativno utjecati na poslovne subjekte i individualne korisnike. Sav software treba biti verificiran i odobren, a ažuriranja poslana preko sigurnih i enkriptiranih kanala.

Nesigurna web sučelja (eng. *interface*)

Nesigurna web sučelja mogu biti uzrok kompromitiranja IoT uređaja i njihovih komponenti.Primjeri ove ranjivosti uključuju slabu autentifikaciju i autorizaciju, što može dovesti do neovlaštenog pristupa sučelju, nedostatak korištenja HTTPS-a, što omogućuje presretanje i izmjenu informacija koje se šalju i primaju putem tog sučelja, te nesigurnu konfiguraciju bez zaštite od napada grube sile [6].

3.1.4 Fizičke ranjivosti uređaja

Veliki broj IoT uređaja u upotrebi

U 2023. godini u svijetu je u uporabi oko 15 milijardi IoT uređaja. Sve veći broj IoT uređaja povećava sigurnosne ranjivosti i predstavlja sve veći izazov za sigurnosne stručnjake. Veliki broj uređaja unutar organizacije otežava ručno prepoznavanje i mapiranje svakog uređaja.

Problemi koji se odnose na sigurnost IoT-a, poput slabih lozinki nedostatka enkripcije tijekom prijenosa i nesigurnih mehanizama ažuriranja, relevantne su i kritične teme od početka IoT-a do danas. Ovo ukazuje na upornu i evoluirajuću prirodu problema sigurnosti.

3.2 Razlikovanje pojmova kibernetičkih prijetnji i kibernetičkih napada

Kao što je definirano NIST rječniku, cyber prijetnja[1] je svaki događaj s potencijalnim negativnim utjecajem na organizacije ili pojedince i potencijalom da izvor prijetnje iskoristi ranjivosti Interneta stvari navedenih u prethodnom poglavlju ovoga rada.

S druge strane, cyber napad[2] je bilo koja vrsta zlonamjerne aktivnosti koja pokušava prikupiti, poremetiti, kontrolirati ili uništiti resurse sustava ili same informacije.

Glavna razlika između ova dva pojma je namjernost. Prijetnja može biti namjerna ili nenamjerna. Najčešće nenamjerne prijetnje su prirodne katastrofe. Napadi su, s druge strane, uvijek namjerne radnje na sustavu ili uređaju. Svaka IoT domena ili sloj arhitekture podložni su mogućem cyber napadu [1].

3.3 Cyber napadi na Internet stvari

Kategorizacija korištena u ovome dijelu data je prethodno od strane autora u članku [8] o sigurnosnim i problemima privatnosti u IoT-u. Članak opisuje jedanaest kategorija, a ovaj rad izdvaja četiri najbitnije.

[1] https://csrc.nist.gov/glossary/term/cyber_threat
[2] https://csrc.nist.gov/glossary/term/cyber_attack

3.3.1 Fizički napadi

Ubacivanje lažnih čvorova

Ovaj je napad jedan od najrazornijih za IoT uređaje. Napadači postavljaju zlonamjerne čvorove u IoT mrežu ili koriste lažne čvorove kako bi s lažnim identitetom ostvarili pristup mreži. Cilj ovakvih napada kontrola je protoka podataka, pristup povjerljivim informacijama i pokretanje dodatnih napada [9]. U najgorem slučaju, lažni čvor može uništiti cijelu mrežu ili omogućiti napadaču potpunu kontrolu nad mrežom.

3.3.2 Mrežni napadi

RFID spoofing

RFID (Radio Frequency Identification) spoofing varijanta je kloniranja gdje RFID oznaka nije fizički replicirana. Napadači koriste uređaje za praćenje i oponašanje važećih oznaka kako bi maskirali napadačev identitet [9]. Pristup sustavu omogućen je lažnim predstavljanjem kao originalni izvor [10]. Kako bi napad bilo moguće izvesti, uređaji napadača moraju imati potpun pristup protokolima i tajnama korištenima u svakoj autentifikaciji u IoT mreži.

Botnet napad

Botneti mreže su kompromitiranih računala ili IoT uređaja s aktivnim botovima koje napadači kontroliraju bez znanja vlasnika. Koriste se za zlonamjerne aktivnosti ili preusmjeravanje mrežnih resursa. Napadač daljinski može kontrolirati međusobno povezane uređaje. Botneti su opasniji od pojedinačnih malwarea jer mogu zaraziti tisuće uređaja.

DoS i DDoS napadi

Kod DoS (Denial of Service) napada, napadač preopterećuje uređaj s prevelikim brojem nepotrebnih zahtjeva za uslugom [4] što može dovesti do kašnjenja ili blokiranja usluge stvarnim korisnicima. S druge strane, DDoS (Distributed Denial of Service) koristi botove za pokretanje koordiniranih napada na metu, onemogućavaju usluge stvarnom korisniku.

MitM napad

Tijekom MitM (Man in the Middle) napada, napadači koriste zlonamjerni čvor, postavljen između dva originalna čvora u mreži, radi presretanja komunikacije bez pristanka ili znanja originalnih čvorova. Na ovaj način napadač ima kontrolu nad cijelom komunikacijom; može

prisluškivati i slati izmijenjene informacije primatelju. MitM napad mogu pokrenuti kompromitirani IoT uređaji korištenjem metoda poput SSH otimanja (eng. hijacking), DNS spoofinga ili sidejackinga.

Wormhole napad

Ovaj napad može biti izveden na dva načina. Napadači pridobiju kontrolu nad dva ili više čvorova u IoT mreži i kreiraju transmisiju, odnosno svojevrstan tunel, između njih. Drugi način je ubacivanje zlonamjernog koda u mrežu kako bi se promjenio originalni put prijenosa. Rezultat je narušen mrežni promet i topologija te kršenje povjerljivosti podataka.

3.3.3 Softverski napadi

Phishing

Phishing je tip prijevare kod koje se počinitelj pretvara da je pouzdan izvor i korisnika navede da otkrije povjerljive podatke poput lozinki ili instaliranja zlonamjerne aplikacije na IoT uređaj [8]. Kod IoT-a phishing je usmjeren na prijevaru korisnika, a ne samog uređaja.

Brute force napad

Ovo je jedan od najstarijih tipova napada, ali je još uvijek čest i učinkovit. Koristi se tehnikom pokušaja i pogreške (eng. trial-and-error) kako bi provalio sigurnosne mehanizme i vjerodajnice za prijavu [8]. Napadači često koriste poseban software dizajniran za testiranje velikog broja kombinacija dok ona ne bude pogođena.

3.3.4 Napadi na firmware

Prisluškivanje

Prisluškivanje je pasivan napad krađe informacija iz loše osiguranog prijenosa između IoT uređaja [8]. Ne ometa performanse uređaja ili mreže, pa ga je teško detektirati.

4. Sigurnosne preporuke

4.1 Postojeća rješenja

1. **Osvještavanje korisnika o sigurnosti**

Nedovoljno poznavanje i briga o sigurnosti može rezultirati izlaganjem IoT uređaja potencijalnim napadima. Nužno je da korisnik bude upoznat s ranjivostima i rizicima svojih uređaja. Sigurno ponašanje je potrebno promovirati. Kad su korisnici upućeni u to što je sigurno ponašanje i koje su najbolje prakse, smanjuje se mogućnost da postanu žrtve napada socijalnog inžinjeringa ili da su im uređaji nezaštićeni.

2. **Autentifikacija**

Velik broj ranjivosti i napada naglašava potrebu za snažnim mehanizmima autorizacije i autentifikacije. Ovaj pristup, u kombinaciji s razvijenom svijesti o sigurnosti, smanjuje mogućnost neautoriziranog pristupa i osigurava da samo autorizirani korisnici i IoT uređaji mogu pristupiti mreži i sustavima [6].

3. **Redovna ažuriranja**

Ako se ažuriranja zanemaruju i IoT uređaj koristi zastario software, postoji značajan rizik od neispravljenih sigurnosnih propusta. Ranjivosti mogu dopustiti iskorištavanje IoT uređaja i njegovih podataka dostupnih napadačima. Uz redovita ažuriranja, poznate ranjivosti mogu se pravilno riješiti i uređaj se može bolje zaštititi od prijetnji.

4. **Podjela mreže u segmente**

Ako se, usprkos preporukama, napad dogodi, segmentacija zahvaćenih IoT uređaja može ograničiti napad u segmentu gdje se uređaji nalaze, sprečavajući tako širenje napada cijelom mrežom [6].

5. **Zaštita dizajnirana specifično za IoT uređaje**

Budući da IoT uređaji imaju karakteristično dizajnirane sustave, tradicionalna IT sigurnosna rješenja nisu uvijek prikladna ili primjenjiva za njih, stoga je potrebno razviti samo posebno izrađenu zaštitu [14]. Među strategijama koje predlažu autori [15] su i lagani algoritmi šifriranja. Razvoj i implementacija lakih algoritama šifriranja prikladnih za IoT uređaje su ključni. Ovi su algoritmi dizajnirani za učinkovit rad na IoT uređajima s ograničenim računalnim resursima te za pružanje visoke razine zaštite i privatnosti podataka.

4.2 Prijedlog za razvoj protokola sigurne komunikacije

1. **Mehanizmi sigurne autentifikacije**

Metode kao što su dvofaktorska autentifikacija (2FA), autentifikacija tokenom, autentifikacija temeljena na certifikatima i druge metode osiguravaju IoT uređaje od lažnog identifikacije i neovlaštenog pristupa.

2. **Provjera integriteta podataka**

Provjera integriteta podataka daje informacije o tome je li podacima koje šalju IoT uređaji manipulirano od strane neovlaštenih osoba ili programa. Kontinuirano praćenje integriteta podataka zamijenilo bi jednokratnu provjeru i učinilo ju pouzdanijom.

3. **Sustav upravljanja ključevima**

Upravljanje ključevima je ključni sigurnosni problem za IoT uređaje zbog ograničenih resursa i njihove osjetljivosti na prijetnje. Prijedlog je nadogradnja zamjenom postojećih protokola za predistribuciju nasumičnih ključeva metodom koja generira simetrične tajne ključeve između svakog IoT čvora, čime se učinkovito rješavaju problemi povezani s potrošnjom i raznim sigurnosnim prijetnjama, budući da se ključevi ne prenose između uređaja.

4. **End-to-End enkripcija (E2EE)**

S E2EE (enkripcija s kraja na kraj), komunikacija između IoT uređaja bila bi zaštićena od trećih strana koje bi mogle pristupiti i mijenjati podatke koji se prenose s jednog uređaja na drugi.

5. Inovativni pristupi za poboljšanje IoT sigurnosti

5.1 Poboljšavanje sigurnosti uporabom blockchaina

Blockchain tehnologija zajednički je i nepromjenjivi registar koji poboljšava sigurnost IoT-a osiguravajući transparentnost, provjerljivost, pouzdanost i integritet podataka. Informacije su trenutno dostupne, dijele se i potpuno su transparentne te se čuvaju u nepromjenjivom registru kojem mogu pristupiti samo ovlašteni korisnici mreže. Poboljšanje integriteta podataka smatra se jednom od najznačajnijih prednosti blockchain tehnologije [13]. Ovaj je aspekt posebno važan u sektorima koji se bave kritičnim operacijama kao što su zdravstveni i industrijski kontrolni sustavi, gdje je održavanje integriteta podataka unutar IoT mreža najvažnije [12]. Blockchain potencijalno rješava sigurnosne probleme IoT-a kao što su provjera identiteta, sigurna komunikacija, autentifikacija, kontrola pristupa i sigurno pohranjivanje [11]. Također vodi evidenciju incidenata [12], što pomaže u otkrivanju prijetnji i analizi. Učinkovitost blockchaina u poboljšanju sigurnosti IoT-a ovisi o njegovom specifičnom dizajnu i implementaciji.

5.2 Poboljšavanje sigurnosti uporabom strojnog učenja

Strojno učenje primjena je računala i algoritama za inteligentno učenje s ciljem automatizirane detekcije odnosa između podataka. Modeli strojnog učenja testiraju se različitim metodama učenja i mogu se poboljšati na temelju unesenih podataka [11].Modeli strojnog učenja mogu se koristiti za rješavanje sigurnosnih problema kao što su otkrivanje anomalija i upada, profiliranje ponašanja i sigurna autentifikacija.

5.3 Poboljšavanje sigurnosti uporabom umjetne inteligencije

Zbog međusobno povezane prirode IoT uređaja, velika količina podataka se generira i šalje kroz mrežu. Obrada i analiza generiranih podataka može biti priličan izazov u IoT-u, a ovaj problem može se riješiti umjetnom inteligencijom (AI). Algoritmi dizajnirani za analizu podataka mogu detektirati neuobičajene količine senzorskih podataka ili mrežnog prometa koji se prenosi, što je mogući pokazatelj kibernetičke prijetnje. Ostala pitanja koja se mogu riješiti AI su otkrivanje zlonamjernog softvera (malwarea) i očuvanje privatnosti [11]. AI u

kombinaciji s tehnikama strojnog učenja može se koristiti za otkrivanje prijetnji u stvarnom vremenu, povećavajući sigurnost kontinuiranim prilagođavanjem novim prijetnjama. Te algoritme treba uvježbati i testirati kako bi se smanjila mogućnost lažno pozitivnih i lažno negativnih ishoda.

Ovi su pristupi postali relevantni u posljednjih nekoliko godina, a sažetak ovog poglavlja prikazan je u tablici 1. Važno je napomenuti da, iako ovi pristupiti mogu značajno unaprijediti IoT, ne mogu u potpunosti eliminirati sve prijetnje ili spriječiti svaki napad. Također, učinkovitost umjetne inteligencije i strojnog učenja ovisi o kvaliteti i kvantiteti podataka na kojima se obučavaju.

Tablica 1: Sažetak poglavlja Inovativni pristupi za poboljšanje IoT sigurnosti

Pristup	Ključni doprinosi	Prednosti	Nedostaci
Blockchain tehnologija	- osiguravanje transparentnosti, provjerljivost, pouzdanost i redundantnosti podataka	- trenutna dostupnost informacija - pristup dozvoljen samo autoriziranim korisnicima	- visoki troškovi implementacije i održavanja - potreba za velikim brojem obučenih stručnjaka
Umjetna inteligencija	- rješavanje problema otkrivanja anomalija i upada, profiliranja ponašanja i sigurne autentifikacije	- adaptivno otkrivanje prijetnji - poboljšanje sigurnosnih protokola	- zahtijeva velike količine relevantnih podataka za obuku
Strojno učenje	- obrada i analiza velike količine generiranih podataka - otkrivanje neuobičajene količine podataka senzora ili prijenosa mrežnog prometa - poboljšano otkrivanje malwarea	- otkrivanje prijetnji u stvarnom vremenu - poboljšava zaštitu privatnosti - prilagođavanje novim sigurnosnim prijetnjama	- mogućnost lažno pozitivnih i lažno negativnih rezultata - zahtijeva stalno ažuriranje algoritma - zahtijeva velike količine podataka za obuku

6. Zaključak

Internet stvari (IoT) predstavlja mnogo sigurnosnih izazova zbog svoje međusobno povezane prirode. Ranjivosti u IoT-u kreću se od slabih lozinki do nesigurnih komunikacijskih protokola, što dovodi do značajnog porasta kibernetičkih napada. Unatoč razvoju raznih sigurnosnih mjera, protokoli su često neadekvatno dokumentirani, a korisnici ne poduzimaju potrebne mjere opreza. Inovativni pristupi kao što su blockchain, umjetna inteligencija i strojno učenje mogu poboljšati sigurnost IoT-a, ali ne mogu u potpunosti eliminirati sve prijetnje IoT-u. Stoga su kontinuirano istraživanje i razvoj ključni za održavanje sigurnosti IoT uređaja.

7. Literatura

[1] Gelo, D. (2019). Internet of Things (IoT)-Izazovi i mogućnosti cyber sigurnosti povezane s IoT-om (Doctoral dissertation, Algebra University College).

[2] Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. IEEE Access, 8, 168825-168853.

[3] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

[4] Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A., Fartitchou, M. (2020). IoT security: challenges and countermeasures. Procedia Computer Science, 177, 503-508.

[5] Li, S., Da Xu, L. (2017). Securing the internet of things. Syngress.

[6] Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study. Symmetry, 15(11), 1978.

[7] Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. Wireless Personal Communications, 119, 2603-2637.

[8] Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., Auwul, M. R. (2022). A review of security and privacy concerns in the internet of things (IoT). Journal of Sensors, 2022.

[9] Harbi, Y., Aliouat, Z., Harous, S., Bentaleb, A., Refoufi, A. (2019). A review of security in internet of things. Wireless Personal Communications, 108, 325-344.

[10] Mitrokotsa, A., Rieback, M. R., Tanenbaum, A. S. (2010). Classifying RFID attacks and defenses. Information Systems Frontiers, 12, 491-505.

[11] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.

[12] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., Pathan, M. S. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. Journal of King Saud University-Computer and Information Sciences, 101939.

8. Popis tablica

9. Sažetak

Kako ekosustav Interneta stvari (IoT) doživljava eksponencijalni rast, popratni porast kibernetičkih napada predstavlja veliku zabrinutost. Kao odgovor na to, kibernetička sigurnost IoT-a pojavljuje se kao kritičan pothvat usmjeren na ublažavanje ovih rastućih rizika i zaštitu imovine IoT-a. Ovaj rad zadire u višestrani krajolik sigurnosti IoT-a, baveći se izazovima i ranjivostima koje prevladavaju u današnjim IoT sustavima. Istražujući niz potencijalnih rješenja, u rasponu od protokola šifriranja do mehanizama za otkrivanje upada, cilj je opremiti istraživače uvidima u jačanje IoT infrastrukture protiv napada. Nadalje, rasprava se proteže na očekivani napredak u sigurnosti IoT-a, predviđajući budućnost u kojoj će se proaktivne mjere razvijati uz nove prijetnje kako bi se održao integritet i otpornost IoT mreža.

Ključne riječi: Internet stvari, IoT sigurnost, ranjivosti, prijetnje, napadi, izazovi, preporuke

10. Abstract

As the Internet of Things (IoT) ecosystem experiences exponential growth, the accompanying surge in cyberattacks presents a pressing concern. In response, IoT cybersecurity emerges as a critical endeavor aimed at mitigating these escalating risks and protecting IoT assets. This paper delves into the multifaceted landscape of IoT security, addressing challenges and vulnerabilities prevalent in today's IoT systems. By exploring an array of potential solutions, ranging from encryption protocols to intrusion detection mechanisms, it aims to equip researchers with insights into fortifying IoT infrastructures against attacks. Furthermore, the discussion extends to anticipated advancements in IoT security, envisioning a future where proactive measures evolve alongside emerging threats to uphold the integrity and resilience of IoT networks.

Key words: Internet of Things, IoT security, vulnerabilities, threat, attacks, challenges, recommendations, future development