Naučni članci / Scientific articles

Vrsta rada: Pregledni članak
Primljen: 22. 1. 2021.
Prihvaćen: 28. 1. 2021.
UDK: 004.78:004.35

Problemi u vezi sa procenom pouzdanosti podataka na kojima počiva Internet stvari

Slavko Pokorni[1]*

[1] Visoka škola strukovnih studija za informacione tehnologije ITS-Beograd, Beograd, Srbija; slavko.pokorni@its.edu.rs

Apstrakt: U poslednje vreme beleži se povećano interesovanje za proučavanje Interneta stvari (IoT – Internet of Things). Otkriveni su novi koncepti, a stari su unapređeni ili ispravljeni zahvaljujući inovativnim istraživačkim studijama i razvoju IoT tehnologija u različitim sektorima. Pored toga, fokus je i na bezbednosti i standardima Interneta stvari. IoT aplikacije koje se primenjuju u drugim granama industrije, poput pametnog življenja, Industrije 4.0 i E-zdravlja su i dalje relevantne. Cilj ovog rada jeste da pokaže da se Internet stvari (IoT) mora smatrati pouzdanim, naročito kada se radi o Internetu stvari zasnovanom na podacima. Pouzdanost takvog Interneta stvari je kompleksan problem koji nije lako rešiti, jer podrazumeva hardver, softver, ljudski faktor, podatke, a u današnje vreme i veštačku inteligenciju. Moguće je izračunati pouzdanost IoT sistema pomoću proste jednačine koja će biti predstavljena u ovom radu. Ali osnovni problem jeste kako izračunati pouzdanost podsistema u ovoj jednačini. Pored toga, pouzdanost ima veze sa dostupnošću i pogodnošću održavanja. Sadržaj ovog rada se uglavnom oslanja na dve nedavno objavljene publikacije autora.

Ključne reči: pouzdanost, dostupnost, pogodnost održavanja, Internet stvari, zasnovanost na podacima, podaci.

1. Uvod

Internet stvari (IoT – Internet of Things) ili internet pametnih uređaja nastao je krajem XX veka, dok je teorija i praksa pouzdanosti počela da se javlja 50-ih godina prošlog veka. Međutim, Internet stvari je veoma kompleksan i međuzavisan sistem, zbog čega su obrazovanje i istraživanje pouzdanosti svakodnevno suočeni sa novim zahtevima u vezi sa IoT-om.

Kod Interneta stvari uređaji su međusobno povezani i mogu da komuniciraju između sebe, često bez ikakvog uplitanja ljudi. Budući da Internet stvari počiva na ljudskom faktoru, hardveru i softveru, on mora posedovati visoku pouzdanost, zbog čega je neophodna šira diskusija o ovoj temi.

IoT sistem zasnovan na podacima je kompleksniji od običnog, budući da su podaci sastavni deo ovog sistema. Iz tog razloga, neophodno je razmotriti pouzdanost tih podataka. U [1] primenjena je klasična metoda procene pouzdanosti da bi se istražilo pitanje dostupnosti i pouzdanosti IoT-a. Fokus ovog rada je pouzdanost Interneta stvari zasnovanog na podacima.

2. Internet stvari

Internet stvari će transformisati ljudsko društvo, čineći ga inovativnijim, pristupačnijim i efikasnijim, a tu je i ogroman potencijal za ekonomski i ekološki razvoj. Međutim, jedno od neodložnih pitanja koje se mora rešiti, ukoliko želimo da do ove revolucionarne transformacije dođe, jeste njegova pouzdanost [2].

Internet stvari je trenutno jedna od najpopularnijih tema. Elektronske komponente postaju sve manje i sve jeftinije, a bežične komunikacije sve rasprostranjenije. Upravo ova tri faktora imaju najveći uticaj na Internet stvari.

Internet stvari će transformisati aplikacije poput elektronskog zdravstva, kućne automatizacije i senzora za praćenje parametara životne sredine. Čak je i ekonomija deo ove rasprave. Aktuelni razvoj internet veza i pametnih računara je Internet stvari, njegove aplikacije i prateće hardverske platforme učinio glavnom temom u akademskoj i stručnoj javnosti. IoT sistemi se mogu primeniti u najrazličitijim scenarijima, od malih prenosivih uređaja, pa sve do infrastrukture čitavih gradova [3, 1].

Internet stvari je neosporno vrlo složen koncept. IoT sistemi podrazumevaju hardverske i softverske komponente, ali povremeno i ljudski faktor [1]. Upravo zato što Internet stvari počiva na hardveru, softveru i ljudskom faktoru, na njegovu pouzdanost utiču sva tri. Dostupnost i pogodnost održavanja takođe imaju veze sa pouzdanošću. Prvi korak u ovoj diskusiji biće definisanje pouzdanosti, dostupnosti i pogodnosti održavanja.

3. Pouzdanost, dostupnost i pogodnost održavanja

Oblast teorije i prakse pouzdanosti počela je da se razvija tek 50-ih godina prošlog veka. Ukoliko se od predmeta/koncepta/stavke očekuje da ispuni određene standarde učinka i da proizvede željene rezultate u određenom vremenskom periodu, onda se govori o njegovoj/njenoj pouzdanosti.

Pouzdanost komponenti i održavanje sistema su dva faktora koja određuju dostupnost računarskog sistema. Međutim, različiti ljudi različito definišu i izračunavaju dostupnost.

Na primer, trenutna dostupnost (takođe poznata i kao dostupnost) definiše se kao verovatnoća da će sistem (ili komponenta) biti u funkciji u određenom trenutku.

U slučaju neispravne komponente ili sistema, pouzdanost i dostupnost su jednake, međutim dostupnost je značajnija od pouzdanosti kada govorimo o ispravnim komponentama i sistemima [4].

I pouzdanost i dostupnost imaju veze sa održavanjem. Stoga, da bi troškovi IoT-a bili što niži, faza projektovanja IoT-a mora da uključi analizu i procenu održavanja.

Pogodnost održavanja podrazumeva da se pametni sistem može lako isključiti, popraviti i prepraviti bez značajnog ugrožavanja normalnog funkcionisanja sistema ili njegovih funkcija. Da bi se osiguralo da se IoT sistem može lako popraviti ili zameniti u slučaju kvara, potrebno je da on sadrži komponente koje se lako menjaju. Lako održivi IoT sistem se može opisati kao sistem koji efikasno i delotvorno izvršava operacije održavanja [5, 1].

Kako izračunati dostupnost sistema ili komponente, može se pronaći u [4].

Zamena IoT uređaja može da smanji njegovu dostupnost ako se od IoT sistema očekuje da radi i tokom zamene baterije, na primer. Zbog toga se IoT sistemi zasnovani na podacima strože i detaljnije kontrolišu, sa fokusom na njihovu pouzdanost u pogledu hardvera, softvera, ljudskog faktora i podataka.

4. Internet stvari je sistem zasnovan na podacima

Izraz „zasnovan na podacima" (data-driven) odnosi se na sve odluke i procese koji zavise od dostupnih informacija. Ovo se najbolje može videti na primeru velikih podataka [6]. Zasnovanost na podacima ima veze sa naukom o podacima, rudarenjem podataka i drugim srodnim oblastima. Mnoga polja, uključujući polje kome pripada Internet stvari, koriste izraz „zasnovan na podacima" da opišu svoje polje delovanja.

Da bi organizacija bila kvalifikovana kao „zasnovana na podacima", ona mora da se bavi prikupljanjem i analizom podataka. Da bi se to postiglo, neophodan je neki oblik komunikacije. Mi danas koristimo različite uređaje, mreže, softver i Internet stvari da to postignemo, a svaki od ovih elemenata može da se pokvari. Međutim, mi želimo da oni funkcionišu i popravljamo ih kada se pokvare, a upravo to je svrha pouzdanosti. Dok budemo govorili o pouzdanosti, kratko ćemo se osvrnuti na Internet stvari.

Heterogenost „end-to-end" IoT sistema donosi određene izazove u vezi sa pouzdanošću. Mnogo veća pažnja se mora posvetiti interfejsima između podsistema kako bi se osigurala kompatibilnost, a to može da utiče na pouzdanost. Najkritičnija tačka IoT-a jeste fizički sistem kod koga može da dođe do nepredviđenih kvarova. Inženjeri i matematičari su dugo analizirali ove sisteme kao element hardverske pouzdanosti kako bi smanjili učestalost kvarova i sačuvali ljudske živote [7].

5. Elementi IoT sistema zasnovanog na podacima

Netačne glasine o praćenju podataka, dugim zastojima, pa čak i gubitku podataka mogu da smanje interesovanje za IoT komunikacije, ali i poverenje u podatke. Internet stvari zahteva visok nivo pouzdanosti kako bi mogao da održi korak sa sopstvenim ubrzanim razvojem [8].

Zbog toga, pouzdanost sistema zasnovanih na IoT-u zavisi od samih komponenti (elemenata) IoT-a i podataka koji čine sistem.

5.1. Pouzdanost IoT hardvera

MIL-HDBK-217 se koristi za utvrđivanje pouzdanosti elektronskih uređaja još od 60-ih godina prošlog veka. Prvobitna verzija ovog proizvoda razvijena je 1961. godine (verzija A). I pored svih njenih nedostataka, više od 80% inženjera i dalje koriste MIL-HDBK-217 za utvrđivanje pouzdanosti. Industrijski i komercijalni sektor, naravno, imaju sopstvene standarde za izračunavanje pouzdanosti. Međutim, RIAC's 217PlusTM metodologija i softverski alat zamenili su MIL-HDBK-217, koji se više ne može besplatno koristiti. Pored toga, novi MIL-HDBK-217 je značajno teži za razumevanje od prethodne verzije [9].

I pored toga što imamo MIL-HDBK-217 na raspolaganju, teško je utvrditi pouzdanost hardvera. Zbog toga što ne postoji standardizovana metoda za predviđanje pouzdanosti hardvera, rezultati mogu drastično da variraju u pogledu metodološke strogosti, kvaliteta podataka i mere u kojoj se analiza i neodređenost uzimaju u obzir [10]. Pored toga, dešava se da nisu svi procesi predviđanja zabeleženi. IEEE standard 1413 je utvrđen 2009. kao odgovor na to (Standard Framework for Hardware Reliability Prediction – Skup standarda za predviđanje pouzdanosti hardvera). Internet stvari obuhvata širok spektar hardverskih komponenti različitog kvaliteta i stepena pouzdanosti. Da bi se precizno izračunala pouzdanost komercijalnog hardvera, neophodno je utvrditi pouzdanost i stopu kvarova, prosečno vreme do kvara (MTTF) ili prosečno vreme između kvarova (MTBF), a takvih podataka nema.

5.2. Pouzdanost IoT softvera

Važan kriterijum koji treba razmotriti jeste kvalitet softvera kao gotovog proizvoda. Postoje različiti modeli za procenu pouzdanosti softvera, ali nijedan nije univerzalno prihvaćen [11, 9]. Uglavnom je teško definisati zahteve koji moraju biti ispunjeni da bi se softver mogao smatrati pouzdanim. Ovo naročito važi za Internet stvari. Pošto se softver suštinski razlikuje od hardvera, problem samim tim postaje još teži. Iako je pouzdanost softvera probabilistička, ona nije i vremenski zavisna funkcija. Važno je napomenuti i da ne postoje standardizovane prakse za predviđanje pouzdanosti softvera. Stručnjaci za pouzdanost i softver moraju se postarati da softver bude uključen u studije slučaja pouzdanosti sistema.

Kada dođe do kvara ključnog elementa/komponente, tada nastaje pravi problem sa softverskom pouzdanošću. „Otporan na kvarove" nije isto što i „nikada se ne kvari". Softverska bezbednost i pouzdanost idu jedno s drugim zato što je njihova zajednička svrha kreiranje bezbednog i pouzdanog softvera. Softverski inženjeri i inženjeri za pouzdanost moraju ponovo da udruže snage. Uprkos tome, mali broj obrazovnih institucija i profesionalaca iz ove industrije se uopšte

trudi da druge nauči osnovama softverske pouzdanosti i bezbednosti [4].

Veliki je izazov unaprediti pouzdanost pomoću redundantnog softvera, jer u svakoj kopiji postoji greška [4].

5.3. Ljudska pouzdanost u IoT-u

Kao što je navedeno u uvodu ovog rada, i ljudi mogu biti deo IoT sistema. Zbog toga je Internet stvari podložan ljudskoj grešci.

Ljudska pouzdanost se može povećati sprečavanjem akcidenata i minimiziranjem štete. Pored rada sa hardverom i softverom, do ovih problema može doći isključivo kod uskladištenih podataka. Ljudski postupci utiču na tehnološke sisteme. Postoji mnogo primera gde su odluke ili postupci jedne ili više osobe tokom korišćenja, održavanja ili popravke tehnološkog sistema izazvale katastrofe ili pad čitavog sistema. Inženjeri za pouzdanost mogu značajno da utiču na ovakve ishode kroz saradnju sa drugima, na primer menadžerima rizika, ekolozima ili inženjerima za bezbednost i zdravlje na radu. Posledice ljudske greške u rukovanju podacima mogu biti prilično ozbiljne. Ljudskoj pouzdanosti se može pristupiti na različite načine i pomoću različitih modela [9]. Procedure, pravila, kodeksi, standardi i zakoni ne mogu da spreče sve kvarove na sistemu, ali mogu da smanje njihovu verovatnoću i učestalost.

Za autora ovog rada pouzdanost, uključujući i ljudsku, oduvek je bila važna tema, zbog čega se pominje u svim njegovim udžbenicima.

5.4. Pouzdanost podataka u IoT-u

Neophodno je da podacu budu pouzdani, a to znači potpuni i tačni, jer se tako gradi poverenje u njih. Iz tog razloga, da bi se održala sigurnost i kvalitet podataka, kao i njihova usklađenost sa propisima, osnovni cilj inicijativa posvećenih integritetu podataka jeste da osiguraju pouzdanost podataka [12].

Kako bi donosili ispravne odluke, biznis liderima su potrebne tačne informacije. Zbog toga je pouzdanost podataka jedan od najvažnijih faktora u organizacijama koje rade sa podacima. Međutim, validnost i pouzdanost podataka nisu ista stvar. Pouzdanost skupa podataka zavisi od validnosti, potpunosti i jedinstvenosti tog skupa podataka. Zbog nepouzdanosti Interneta stvari, neki podaci mogu nedostajati, biti oštećeni ili nepotpuni.

Nažalost, ne postoji adekvatna teorija niti praksa koja nam pomaže da konceptu pouzdanosti podataka pristupimo na pravi način.

5.5. Pouzdanost veštačke inteligencije Interneta stvari

Internet stvari zasnovan na podacima nije izuzetak kada se radi o trendu korišćenja veštačke inteligencije (AI – Artificial Intelligence). Mašinsko učenje (MU) i veštačka inteligencija transformišu različite aspekte ekonomije, obrazovanja i ljudskih života uopšte. Mašinsko učenje postaje sve značajnije u ključnoj oblasti otkrivanja sajbernapada na Internetu stvari. Mašinsko učenje takođe može da otkrije sofisticirane napade pomoću strategija zasnovanih na znanju. Međutim, nedostatak javno dostupnih i redovno ažuriranih skupova podataka predstavlja najozbiljniji problem u vezi sa bezbednošću IoT-a [13].

Veštačka inteligencija je evoluirala od mašinskog učenja, preko dubokog učenja, pa sve do praktičnog AI-ja. AI mašinama omogućava da uče iz sopstvenog iskustva, da se prilagođavaju novim okolnostima i podacima i da izvode određene zadatke bez učešća ljudi. Prepoznavanje lica, glasa i pobede u šahu su već moguće. Trenutno se najviše primenjuje kod IoT podataka, brzog interneta i superračunara i njihovog neprekidnog rasta. Statističke i računarske tehnike se trenutno primenjuju za istraživanje veštačke inteligencije [14].

AI prepoznaje obrasce i abnormalnosti u podacima zahvaljujući pametnim senzorima i uređajima, a pritom mu nisu potrebne nikakve instrukcije, npr. gde da ih traži. Pored toga, algoritmi mašinskog učenja „uče" kako da s vremenom generišu sve tačnije rezultate. Zbog toga je MU nadmašilo tradicionalne alate poslovne inteligencije u pogledu brzine i tačnosti. Duboko učenje, računarski vid, obrada prirodnih jezika i primena MU za proveru optimizacije i predviđanja su AI tehnologije koje upotpunjuju Internet stvari [15].

Čak i veštačka inteligencija može da otkaže, i to na isti način kao ljudsko rasuđivanje, ako pokuša da mašinsku inteligenciju zameni ljudskom. Zbog čega onda ljudi donose pogrešne zaključke (odluke)? Da li postoji način da rešimo problem pouzdanosti AI-ja ili da izbegnemo kvarove?

S obzirom na značaj ovog pitanja, ISO/IEC je odlučio da se pozabavi njime. Takozvana pouzdanost AI sistema ispitana je u [16], uključujući sledeće: poverenje u AI sisteme može se uspostaviti kroz transparentnost, upravljivost i druge mehanizme; (2) inženjerske zamke i povezane pretnje i rizici po AI sisteme, zajedno sa mogućim tehnikama i metodama za ublažavanje njihovih posledica; (3) metoda za postizanje dostupnosti, otpornosti, pouzdanosti, tačnosti, bezbednosti i privatnosti AI sistema. Postoji mnogo karakteristika koje nešto čine pouzdanim, uključujući pouzdanost, dostupnost, otpornost, bezbednost, odgovornost, integritet, autentičnost, kvalitet i upotrebljivost. Svi ovi atributi uključeni su u ovu definiciju pouzdanosti. Kao i bilo koji drugi proizvod, AI se mora održavati kako bi i dalje bio upotrebljiv i snažan.

Jedan od faktora za utvrđivanje pouzdanosti IoT-a jeste stopa kvarova hardvera i softvera. Pored nje, tu su i drugi faktori, poput protokola, energetske efikasnosti (zelene energije), standardizacije i drugih uticaja, kao na primer bezbednosti. Kada govorimo o protokolima, pouzdan protokol obaveštava pošiljaoca da li su podaci uspešno isporučeni naznačenom primaocu na mreži [17].

Tip korisnika određuje pouzdanost proizvoda koji koristi. Pouzdanost i dostupnost servisa umnogome zavise od onoga ko ga koristi. To znači da će dizajn IoT sistema zavisiti od tipa korisnika kome je namenjen. Internet stvari je takođe zasnovan na podacima i zavisi od njih.

Ciljevi u vezi sa dostupnošću Gugl servisa uglavnom zavise od njihove funkcije i tržišne pozicije. Međutim, potrebno je uzeti u obzir nekoliko faktora [18]. Ako je pitanje šta kupci mogu da očekuju od kompanije u pogledu korisničke

usluge, onda se na umu moraju imati sledeće stavke: da li kupovina ove usluge od strane korisnika direktno utiče na prihod kompanije; da li je ova uslugakomercijalna; ako na tržištu postoji konkurencija, kakav je njihov nivo usluge; da li ova usluga služi pojedincima ili kompanijama; pouzdanost IoT sistema vođenih podacima je tek na petom mestu.

6. Pouzdanost IoT sistema

IoT sistem zasnovan na podacima je kompleksniji od običnog IoT sistema, koji podrazumeva hardver, softver i ponekad ljudsku i veštačku inteligenciju, koje se mogu smatrati podsistemima IoT sistema, stoga preporučujemo promenu jednačine u [1, 19],

$$R_S(t) = R_{HW}(t)R_{SF}(t)R_H(t)R_D R_{AI} \quad (1)$$

gde R_{HW}, R_{SF}, R_H, R_D i R_{AI} predstavljaju pouzdanost podsistema hardvera, softvera, ljudskog faktora, podataka i veštačke inteligencije, tim redosledom.

Iako prethodna formula deluje jednostavno, ona je validna jedino ako su kvarovi na podsistemu hardvera, softvera i podataka međusobno isključivi. Na blok dijagramu pouzdanosti ovo predstavlja serijski model. Izračunavanje pouzdanosti ovih podsistema predstavlja poseban problem koji zavisi od vrste podsistema.

U jednačini iznad pouzdanost je jednaka verovatnoći. Dakle, ako smatramo da je podsistem pouzdan, onda ćemo u formuli napisati da je verovatnoća za taj podsistem jednaka 1.

Kao što je ranije pomenuto, postoji čitava teorija i praksa u vezi sa izračunavanjem pouzdanosti hardvera i softvera, koja je daleko od jednostavne, naročito ako hardver sadrži veliki broj komponenti (elemenata). Izračunavanje pouzdanosti softvera je poseban problem, a ne postoji ni adekvatna teorija niti praksa u vezi sa izračunavanjem pouzdanosti ljudskog faktora, podataka i AI-ja.

Ne postoji jednostavan način da se izračuna pouzdanost Interneta stvari zbog njegove prividne složenosti. Upravo zbog kompleksnosti IoT-a, preporučujemo da se njegova pouzdanost testira pomoću simulacije. Pokorni i Janković [20] i Pokorni i saradnici [21] izvršili su simulaciju kompleksnih sistema, čiji su rezultati doveli do novih saznanja. Slično drugim podsistemima, i veštačka inteligencija se može tretirati kao podsistem u IoT sistemu zasnovanom na podacima i uključiti u jednačinu (1).

7. Pet pravaca istraživanja pouzdanosti IoT-a

Pouzdanost Interneta stvari zasnovanog na podacima je oblast pogodna za istraživanje. Postoji čitav niz radova posvećenih ovoj temi. Na primer, [22] izdvaja sledećih pet ključnih karakteristika sistema za upravljanje pouzdanošću IoT-a:

1. Merenje po vertikalnoj i vremenskoj osi
   Ukoliko je IoT sistem dizajniran za upravljanje kritičnom infrastrukturom, poput sistema bezbednosti i saobraćaja, neophodno je izmeriti otpornost sistema u realnom vremenu ili približno realnom vremenu. Neophodno je obratiti posebnu pažnju na aplikacije koje upravljaju servisima za hitne slučajeve i koje zahtevaju hitar i pouzdan odgovor. Pored toga, kriterijumi za određivanje pouzdanosti svakog pojedinačnog domena se moraju definisati. Na primer, rešenja instalirana u pametnoj zgradi mogu da tolerišu nekoliko sekundi kašnjenja, dok sa druge strane, proizvodni proces može da toleriše zakašnjenje od nekoliko mikrosekundi. Iz tog razloga, istraživanje je ključno za kategorizaciju ovih potreba i izgradnju odgovarajućih rešenja za svaki vertikalni domen.
2. Svi uređaji, svi protokoli
   Veliki broj protokola se povezuje na servise Interneta stvari i koristi ih. Veliki broj istraživačkih grupa radi na dizajniranju laganijih i efikasnijih komunikacionih protokola. Svakog dana, novi IoT uređaji i hardver se pojavljuju na potrošačkom tržištu, zbog čega pouzdana rešenja moraju biti nezavisna od hardvera, softvera i komunikacionih protkola.
3. „Full-stack" svest
   Pregled literature otkrio je da, iako su neki istraživači rešili određeni problem ili grupu problema u vezi sa istraživanjem IoT-a, nijedno istraživanje se nije bavilo „end-to-end" pouzdanošću. Imajući u vidu raspon i kompleksnost IoT implementacija, to ne znači da istraživači treba da kreiraju „univerzalnu" metodu za postizanje pouzdanosti, jer bi to bilo u direktnoj suprotnosti sa prvim istraživačkim ciljem navedenim iznad. Umesto toga, potrebno je predlagati prilagođena rešenja za svaku pojedinačnu IoT vertikalu. Povećanje pouzdanosti IoT-a predstavljalo bi dragocen i inovativan rezultat istraživanja koji bi bio od ogromne koristi za krajnje korisnike IoT-a.
4. Korišćenje anomalija za dobijanje podataka o pouzdanosti
   Anomalije u IoT servisima su česta pojava. Iako je ovaj rad važan i neophodan, on ne mora nužno da poboljša pouzdanost. Anomalija ne upozorava korisnika da je IoT sistem manje pouzdan nego ranije, zbog čega je neophodno sintetisati informacije o pojavi abnormalnosti u IoT sistemima i pretvoriti ih u podatke o pouzdanosti. Na primer, ako senzor u pametnoj kući koji kontroliše parametre okruženja zakaže, to neće dovesti do situacije opasne po život. Međutim, kvar na senzorima za kontrolu temperature u fabrici može da dovede do pregrevanja i opasnih kvarova na zupčanicima.
5. Predviđanje i upravljanje kvarovima
   Ovaj rad se opširno bavi pouzdanošću. Međutim, ukoliko istraživanje ode dalje od toga, moguće je razmotriti prediktivno održavanje. Na primer, da li je moguće odrediti tačan datum održavanja pomoću merljivih parametara pouzdanosti sistema? Da li se ovo može klasifikovati kao dinamički proces zasnovan na pouzdanosti podataka u realnom vremenu umesto kao istorija pređašnjih kvarova pomoću kojih ćemo predvideti buduće? Rešavanje

ovog istraživačkog izazova predstavljalo bi suštinsku prekretnicu u istraživanju pouzdanosti IoT-a.

8. Zaključak

Tradicionalne kompanije koje nisu prisutne na internetu mogle bi da se transformišu u digitalne kompanije zahvaljujući novim industrijama i tehnologijama, poput računarstva u oblaku, veštačke inteligencije i Interneta stvari. Međutim, ovo zahteva reviziju modela poslovanja, ali je i neophodno za kompanije koje žele da opstanu na sve kompetitivnijem tržištu. Elementi Interneta stvari i procena pouzdanosti sistema zahtevaju znanje iz različitih tehničkih i netehničkih oblasti, kao i timski rad.

Internet stvari zasnovan na podacima je višedimenzionalni sistem koji uključuje hardver, softver, ljudski faktor i podatke. Neophodno je razmotriti pouzdanost svakog od ovih podsistema, što je otežano nedostatkom adekvatne teorije i prakse za neke od njih. Otpornost veštačke inteligencije kao potencijalnog podsistema mora biti testirana.

Pouzdanost nije uvek glavni prioritet kada se govori o Internetu stvari zasnovanom na podacima. Međutim, znanje o tome šta treba da tražimo i kako donošenje odluka pomoću nepotpunih ili neispravnih podataka može dovesti do niza negativnih posledica može nam pomoći u slučaju kvara.

Došlo je do dramatične promene u načinu na koji komuniciramo i koristimo tehnologiju zahvaljujući Internetu stvari. Jeftini uređaji mogu da se međusobno povežu na fleksibilniji i pouzdaniji način nego ranije, a ta karakteristika se danas koristi u kritičnim aplikacijama poput saobraćajne infrastrukture, zdravstva i bezbednosti u domu. Mogućnost merenja pouzdanosti ovih IoT uređaja pomoću ograničenih resursa jedna je od njihovih vitalnih funkcija. Nakon detaljne analize trenutnog stanja u merenju pouzdanosti IoT-a, ovo istraživanje se bavi različitim problemima u vezi sa tim poduhvatom. Ključni pravci u istraživanju pouzdanosti IoT-a utvrđeni su nakon detaljnog ispitivanja i analize.

Reference

1. Pokorni S. Reliability and Availability of the Internet of Things. Vojnotehnički glasnik/Military Technical Courier. 2019; 67(3):588-600. Available from: https://doi.org/10.5937/vojtehg67-21363.
2. Xing L. Reliability in Internet of Things: Current Status and Future Perspectives. IEEE Internet of Things Journal. 2020; 7(8). Available from: https://ieeexplore.ieee.org/document/9089244.
3. Zhu Q, Uddin MYS, Venkatasubramanian N, Hsu CH, Hong HJ. Poster abstract: Enhancing reliability of community Internet-of-Things deployments with mobility. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu. [Internet]. 2018 April 15-19. Available from: https://doi.org/10.1109/INFCOMW.2018.8406922.
4. Pokorni S. Reliability of information systems, textbook. Belgrade: Information Technology School (in Serbian); 2014.
5. Thomas MO, Rad BB. Reliability Evaluation Metrics for Internet of Things, Car Tracking System: A Review. International Journal of Information Technology and Computer Science (IJITCS) [Internet]. 2017;9(2):1-10. Available from: https://doi.org/10.5815/ijitcs.2017.02.01.
6. Technopedia [Internet]. Available from https://www.techopedia.com/definition/18687/data-driven (Seen 28.10.2021)
7. Azghiou K, El Mouhib M, Koulali M, Benali A. An End-to-End Reliability Framework of the Internet of Things. Sensors (Basel) 2020 May; 20(9): 2439. Published online 2020 Apr 25. doi: 10.3390/s20092439.
8. Prasad SS, Kumar C. A Green and Reliable Internet of Things. Communications and Network [Internet]. 2013;5(1B):44-48. Available from: https://doi.org/10.4236/cn.2013.51B011.
9. Pokorni S. Reliability prediction of electronic equipment: Problems and experience. In: 7th International Scientific Conference on Defensive Technologies OTEH. Belgrade; 2016;695-700. October 06-07, ISBN 978-86-81123-82-9.
10. Elerath JG, Pecht M. IEEE 1413: A Standard for Reliability Predictions. IEEE Transactions on Reliability [Internet]. 2012;61(1):125-129. Available from: https://doi.org/10.1109/TR.2011.2172030.
11. Kapur KP. Measuring Software Quality (State of the Art). In: 5th DQM International Conference Life Cycle Engineering and Management ICDQM. Belgrade; 2014 June 27-28;3-45.
12. Talend [Internet]. [cited 28.10.2021]. Available from https://www.talend.com/resources/what-is-data-reliability/.
13. Charlesworth A. Absolute Essentials of Digital Marketing; Routledge: London, UK; 2020.
14. Hassanien A, Darwish EH. Machine Learning and Data Mining in Aerospace Technology. Cham, Switzerland: Springer Nature Switzerland AG; 2020.
15. Kuleto V, Ilić M, Dumangiu M, Ranković M, Martins OD, Păun D, Mihoreanu L. Exploring Opportunities and Challenges of Artificial Intelligence and Machine Learning in Higher Education Institutions. Sustainability 2021, 13, 10424. Available from: https://doi.org/10.3390/su131810424.
16. ISO. 2020. ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence [Internet]. Available from: https://www.iso.org/standard/77608.html?browse=tc.
17. Pokorni S. Current State of the Artificial Intelligence in Reliability and Maintainability. Vojnotehnički glasnik/Military Technical Courier. 2021;69(3):578-593, DOI: 10.5937/vojtehg69-30434. Available from: https://doi:10.5937/vojtehg69-30434, ISSN 0042-8469, UDC 623 + 355/359.
18. Alvidrez M. Embracing Risk. [e-book] Sebastopol, CA: O'Reilly Media, Inc.; 2017. Available from: https://landing.google.com/sre/sre-book/chapters/embracing-risk/#risk-management_measuring-service-risk_time-availability-equation.
19. Pokorni S. Reliability of Data-driven Internet of Things Systems. 6th International Conference on Economic Sciences and Business Administration BIG DATA-DRIVEN SMART URBAN ECONOMY. ICESBA 2021. Romania. 2021 26-27 November.
20. Pokorni S, Janković R. Reliability Estimation of a Complex Communication Network by Simulation. In: 19th Telecommunication forum TELFOR. Belgrade; 2011 November 22-24;226-229. IEEE 978-1-4577-1500-6/11.
21. Pokorni S, Ostojić D, Brkić D. Communication network reliability and availability estimation by the simulation method. Vojnotehnički glasnik/Military Technical Courier [Internet]. 2011;59(4):7-14. Available from: https://doi.org/10.5937/vojtehg1104007P.
22. Moore SJ, Nugent CD, Zhang S. et al. IoT reliability: a review leading to 5 key research directions. CCF Trans. Pervasive Comp. Interact. 2020;2:147–163. Available from: https://doi.org/10.1007/s42486-020-00037-z