

# Klaidingų iškvietimų identifikavimas

Eimantas Zaranka, Rūta Juozaitienė, Tomas Krilavičius

Vytauto Didžiojo Universitetas,  
Universiteto g. 10, 53361 Akademija, Kauno r.  
Center of Applied Research and Development (CARD),  
Universiteto g. 10, 53361 Akademija, Kauno r.  
[eimantas.zaranka@vdu.lt](mailto:eimantas.zaranka@vdu.lt)

**Santrauka.** Reagavimas į klaidingus iškvietimus trikdo ne tik sklandų saugos paslaugų veikimą, bet ir eikvoja energijos išteklius, didina išmetamų ŠESD emisiją bei transporto atliekų susidarymą. Šio tyrimo tikslas sukurti klaidingų iškvietimų aptikimo modelį, kuris leistų efektyviau valdyti reagavimo į iškvietimus procesą. Pasiūlyta modeliavimo strategija remiasi ansamblinio mašininio mokymosi metodais bei pasižymi gana aukštu tikslumu,  $F_1$  įverčio reikšmė lygi 0,887. Imituojant realias aplinkos sąlygas buvo atliktas eksperimentinis pasiūlytos metodikos testavimas, tokiu būdu patvirtinant jos efektyvumą bei prognozavimo tikslumą.

**Raktiniai žodžiai:** XGBoost, ansamblinis modelis, klasifikavimas, klaidingi iškvietimai, objektų sauga

## 1 Įvadas

Klaidingas iškvietimas nusako situaciją, kai atliekamas iškvietimas į manomai pavojingą ar nukrypstančią nuo standartų situaciją, tačiau išsiuntus reagavimo ekipažą pastebima, kad poreikis į reagavimą nėra reikalingas. Su klaidingais iškvietimais dažniausiai susiduriama apsaugos ir saugumo sistemose, kuriose naudojami judesio, įsilaužimo davikliai ir stebėjimo kameros, kurios reaguodamos į įvairius aplinkos veiksnius perduoda iškvietimo signalą į operacijų centrą. Tačiau galimi sistemos gedimai, gyvūnų elgesys ar kiti veiksniai gali sąlygoti klaidingus iškvietimus, kurie trikdo sklandų saugos paslaugų veikimą, turi neigiamą įtaką efektyviam resursų naudojimui bei mažina pasitikėjimą saugos sistemomis.

Siekiant gerinti siūlomų saugos paslaugų kokybę, atsiranda poreikis diegti klaidingų iškvietimų analizės sistemas. Tokio pobūdžio sistemos yra naudingos saugos tarnyboms, viešosios tvarkos tarnyboms, specialiosioms bei panašaus pobūdžio tarnyboms kadangi padeda efektyviai valdyti reagavimo į iškvietimus procesą, bei ženkliai sumažinti transporto naudojimą –

taupyti energijos išteklius (kurą, elektros energiją), mažinti išmetamų ŠESD emisiją, mažinti transporto atliekų susidarymą.

Šiame straipsnyje pristatomi eksperimentiniai tyrimai, kurių tikslas remiantis iškvietimų į objektus istoriniais duomenimis, sudaryti tikimybinį klaidingų iškvietimų aptikimo modelį. Atlikta analizė apima problemos analizę, duomenų paruošimą ir pradinę analizę, svarbių požymių identifikavimą bei eksperimentus su skirtingais klasifikavimo modeliais. Remiantis eksperimentų metu gautais rezultatais, sukurtas klaidingų iškvietimų aptikimo modulio maketas.

## 2 Literatūros apžvalga

Straipsnyje [1] pristatomas hibridinis iškvietimų (angl. *alarm*) vertinimas. Autorių teigimu, siūlomas sprendimas sugeba įvertinti 30 tūkst. iškvietimų per sekundę, taip sprendžiant sistemos perkrovos ir patikimumo gerinimo užduotis. Tyrime [1] naudojami *Sitasys, London* ir *San Francisko* tikrų iškvietimų duomenų rinkiniai. Dirbtinio intelekto modeliui kurti naudoti keturi algoritmai: atsitiktiniai medžiai (angl. *random forest*), logistinė regresija (angl. *logistic regression*), atraminių vektorių mašina (angl. *support vector machine*) ir neuroninis tinklas. Atlikus eksperimentus pastebėta, kad geriausiai veikia atsitiktinių medžių klasifikatorius, kuriuo pasiekiamas 92 % tikslumas. Tyrime pabrėžiama, kad mašininio mokymosi modeliai turėtų būti kuo paprastesni, siekiant efektyviai dirbti su didelio srauto duomenimis.

Straipsnyje [2] pristatomas įsilaužimų į pastatus aptikimas, naudojant *Wi-Fi* kanalų būsenos (angl. *channel state*) informaciją. Autoriai atlieka klasifikavimą naudojant atraminių vektorių klasifikatorių, kurio pagalba nustatoma ar buvo įsilaužta pro langą ar pro duris. Sudarytas modelis buvo ištestuotas atliekant daugiau nei 200 eksperimentų, kurių metu nustatyta, kad jeigu namie nėra pašalinio judesio, sukurtas modelis veikia 94,5 % tikslumu, jeigu juda vienas pašalinis asmuo sistema veikia 84 %, kur 1,7 % yra klaidingi iškvietimai, atvejais kai užfiksuojamas dviejų asmenų judėjimas modelis veikia 69 % tikslumu.

Straipsnyje [3] pristatomas klaidingų skubios pagalbos iškvietimų nustatymas, analizuojant skambinančiojo elgseną ir vietą. Tyrime pristatomas ribine verte paremtas vertinimas, siekiant išskirti klaidingus iškvietimus. Kiekvienam objektui priskiriamas patikimumo koeficientas  $f$ , kuris atnaujinamas, po kiekvieno atlikto iškvietimo pagal tai ar tas iškvietimas pasitvirtino, ar ne. Inicializuojama  $f$  reikšmė lygi 0. Atveju, kada iškvietimas yra klaidingas

$f$  reikšmė padidinama 1. Šis koeficientas yra lyginamas su dviem slenkstinėmis ribomis  $f_1$  ir  $f_2$ , kurios naudojamos skambinančiojo patikimumo įvertinimui. Patikimi skambinantieji laikomi tie, kuriems  $f \leq f_1$ , ir įtartini, kurie  $f_1 \leq f \leq f_2$ , o ignoruojami, tie kuriems  $f \geq f_2$ . Sistema veikia pasitikėjimo principu, todėl patikimi skambinantieji nėra analizuojami.

Straipsnyje [4] pristatomas klaidingų išskvietimų aptikimas naudojant statistinius metodus. Tyrime, taikomiems algoritmams įvertinti naudojama klaidingai teigiamų rezultatų dažnis (angl. *false positive rate*), tikslumas (angl. *precision*), teisingumas (angl. *accuracy*), jautrumas (angl. *sensitivity*) ir specifiskumas (angl. *specificity*). Modelių kūrimui naudojama trijų etapų strategija: sensorių istorinių duomenų, kurie veikia normaliomis sąlygomis, surinkimas ir statistinio modelio sudarymas, kontrolinės ribos nustatymas sudarytam modeliui ir gyvo srauto stebėjimas. Straipsnyje pastebima, kad nors ir egzistuoja nemažai tyrimų analizuojančių klaidingų išskvietimų aptikimą, tačiau optimalus sprendimas, kuris leistų praktikoje identifikuoti tokius išskvietimus, nerastas.

Straipsnyje [5] pristatomas išskvietimų požymių aptikimas, dideliame išskvietimų duomenų sraute. Anot autorių dideli srautai yra viena pagrindinių priežasčių, kodėl išskvietimų sistemos pasižymi prastu efektyvumu ir duoda mažai naudos. Autoriai naudoja uždary asociatyvinių taisyklių išskyrimą (angl. *closed association rule mining, CHARM*). Siūlomas sprendimas veikia trimis etapais: didelio srauto nustatymas, uždary šablonų (angl. *patterns*) nustatymas ir atitinkamų šablonų nustatymas. Vidutinis algoritmo veikimo laikas 2 minutės. Autoriai teigia, kad siūlomas sprendimas yra veiksmingas ieškant pavojaus signalų šablonų bei padeda sumažinti srauto perteklių.

### 3 Tyrimo metodai

Tyrime naudoti logistinės regresijos, Gauso maišos, SGD, artimiausių kaimynų, sprendimų ir atsitiktinių medžių miško, gradientinio didinimo, LGBM, XGBoost klasifikatoriai ir ansamblinis modelių junginys.

XGB metodas yra vienas iš dažniausiai naudojamų gradiento didinimo sprendimų medžių algoritmų. Jo atveju prognozės tikslumas patobulinamas kuriant daugybę modelių ir akcentuojant tuos mokymo atvejus, kurie yra sunkiai įvertinami. Taip generuojami pradiniai modeliai skirstomi į dvi grupes: silpnus ir stiprius. Silpnas modelis yra algoritmas, kuris veikia tik šiek tiek geriau nei atsitiktinis spėjimas, tuo tarpu stiprus modelis yra tikslesnis prognozavimo ar klasifikavimo algoritmas, kuris yra stipriai koreliuotas su

sprendžiama problema. *XGB* modeliuose silpnaisiais modeliais laikomi pradiniai sprendimų medžiai. Kiekvienas medis bando sumažinti ankstesniojo klaidas. Nors augantys medžiai yra silpnai besimokantys, tačiau pridėdant daug medžių iš eilės ir kiekviename iš jų atsižvelgiant į praeitų medžių klaidas, padidėja efektyvumas ir modelio tikslumas. Kadangi medžiai yra pridėdami nuosekliai, mokymosi algoritmas yra lėtas, tačiau tikslus.

Sudarytų klientų atmetimo prognozavimo modelių tikslumui įvertinti buvo pasirinkti plačiai taikomi tikslumo matai: tikslumas (angl. *precision*), išsamumas (angl. *recall*) ir  $F_1$  kriterijus. Šie matai apskaičiuojami naudojant maišaties matricą (angl. *confusion matrix*), kuri apibendrina klasifikavimo algoritmų efektyvumą ir yra sudaryta iš teisingų teigiamų (angl. *true positive, TP*), teisingų neigiamų (angl. *true negative, TN*), klaidingų teigiamų (angl. *false positive, FP*) ir klaidingų neigiamų (angl. *false negative, FN*) atvejų skaičių. Tikslumas gali būti apibrėžtas kaip modelio klasifikavimo kokybės matas apskaičiuojamas remiantis formule:

$$precision = \frac{TP}{TP+FP}$$

Išsamumas apibrėžiamas kaip santykis tarp teisingai suklasifikuotų teigiamų atvejų skaičiaus ir visų teigiamų atvejų skaičiaus:

$$recall = \frac{TP}{FN+TP}$$

$F_1$  matas yra tikslumo ir išsamumo matų harmoninis vidurkis. Apskaičiuojant  $F_1$  įvertį yra įtraukiamos neteisingai suklasifikuotos reikšmės, todėl šis matas nusako, kiek tikslus ir griežtas yra klasifikatorius atsižvelgdamas ne tik į teisingai suklasifikuotus atvejus, bet ir į blogai suklasifikuotus.  $F_1$  matas gali būti apskaičiuojamas remiantis formule:

$$F1 = 2 * \frac{precision*recall}{precision+recall}$$

## 4 Tyrimo duomenys

Šiame tyrime analizuojami istoriniai saugos tarnybos iškvietimų duomenys. Duomenų aibę sudaro informacija apie 12 598 objektus stebimus 2019 gruodžio 1 d. – 2021 lapkričio 30 d. laikotarpiu. Analizuojami duomenys apima: informaciją apie iškvietimus ir stebimus objektus, meteorologinę informaciją bei nusikalstamas veiklas analizuojamoje lokacijoje.

Pirmojoje kategorijoje fiksuojama informacija apie atliktų iškvietimų laiko žymes (angl. *timestamp*) ir reagavimą į gautą iškvietimą, reaguojamo

objekto miestą, adresą, rajoną, geografines koordinates ir objekto paskirtį. Antroje kategorijoje pateikiama oro temperatūra, matuojama Celsijais, vėjo greitis, metrais per sekundę ir kritulių kiekis milimetrais. Trečiojoje kategorijoje pateikiama informacija apie nusikalstamų veikų pasiskirstymą pagal lokacijas. Šie duomenys gaunami iš nusikalstamų veikų žinybinio registro duomenų žemėlapiu<sup>1</sup>. Šiame tyrime naudojami duomenys apima nusikaltimo datą, nusikalstamos veikos tipą ir užfiksuotos veikos lokaciją (koordinates), pagal kurią apskaičiuojamas nusikaltimų skaičius analizuojamo objekto aplinkoje.

## 5 Pradinė duomenų analizė

Siekiant susipažinti su turimu duomenų rinkiniu, įgauti įžvalgų apie duomenų pasiskirstymą bei sąryšius tarp požymių, buvo atlikta pradinė duomenų analizė. Duomenys gaunami iš trijų srautų, todėl pradinės duomenų analizė pradėta nuo pateiktų duomenų apjungimo. Apjungtą duomenų rinkinį sudaro 289 337 stebiniai (iškvietimai), užfiksuoti 12 598 objektams. Kiekvieną stebėjimą apibūdina 11 požymių, kurie priklauso keturioms anksčiau pristatytoms kategorijoms.

Pradinė duomenų analizė pradėta nuo priklausomojo kintamojo pasiskirstymo analizės, žr. 1 lentelėje. Nesunku pastebėti, kad analizuojama duomenų imtis yra subalansuota, t. y. reagavimo į iškvietimus požymis pasiskirstęs tolygiai.

**1 lentelė.** Duomenų rinkinio stebėjimų pasiskirstymas

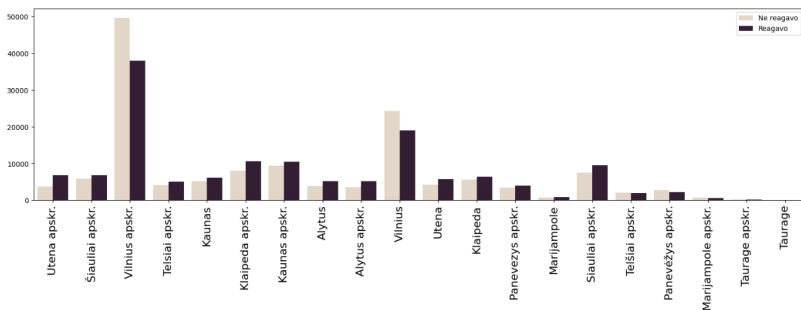
<b>Bendras stebėjimų skaičius</b>	<b>Klaidingų iškvietimų skaičius</b>	<b>Tikrų iškvietimų skaičius</b>
289337	144685	144652

Iškvietimų pasiskirstymo analizė Lietuvos rajonuose pateikta 1 pav. Pastebima, kad Vilnius ir Vilniaus rajonas turi žymiai daugiau fiksuojamų iškvietimų. Be to, šiuose regionuose, klaidingų iškvietimų yra užfiksuojama daugiau negu reaguotinių. Panaši tendencija taip pat pastebima Telšių, Panevėžio ir Marijampolės regionuose.

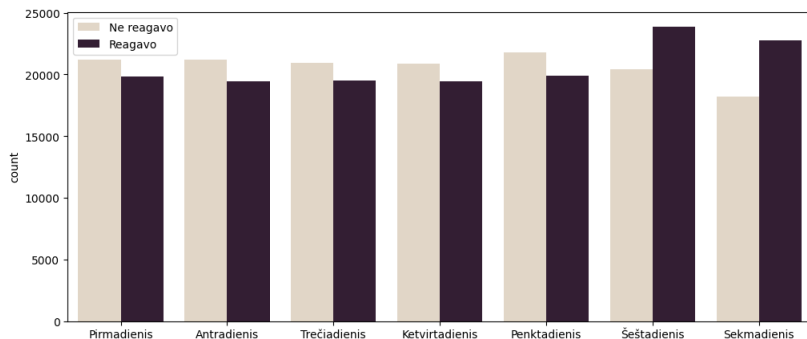
Tyrimo metu taip pat buvo analizuojama savaitės/paros laiko įtaka reagavimui į iškvietimus. Atlikus iškvietimų skaičiaus pasiskirstymo savaitėje

<sup>1</sup> <https://maps.ird.lt/map/>

analizę, kuri pateikta 2 pav., pastebėta, kad darbo dienomis, t. y. pirmadienį-penktadienį, į iškvietimus reaguojama rečiau, be to, bendras iškvietimų skaičius yra mažesnis, negu savaitgaliais. Šeštadieniais pastebimas bendras iškvietimų suaktyvėjimas, tiek klaidingų, tiek tų kuriems saugos tarnybos skiria didesnę dėmesį. Tuo tarpu sekmadieniais sumažėja klaidingų iškvietimų ir padidėja reaguotinų iškvietimų skaičius lyginant su darbo dienomis.

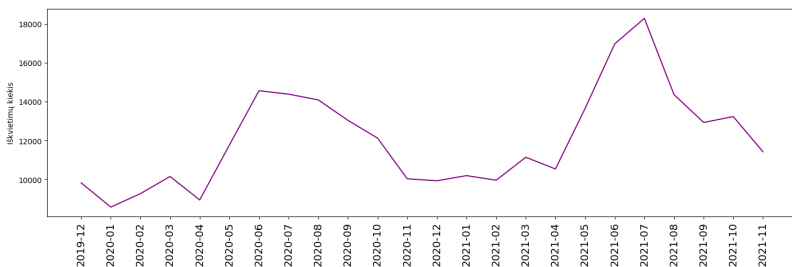


1 pav. Reagavimo į iškvietimus pasiskirstymas, pagal savivaldybes



2 pav. Reagavimo į iškvietimus pasiskirstymas, pagal savaitės dienas

Analizuojant iškvietimų dažnumą (žr. 3 pav.) pastebima, kad mažiausias iškvietimų skaičius yra fiksuojamas žiemą, pirmoje metų pusėje, t. y. sausio ir vasario mėnesiais. Pavasarį iškvietimų skaičius pradeda staigiai augti ir piką pasiekia vasarą, t. y. birželio-liepos mėnesiais, po to pradeda vėl palaipsniui mažėti. Toks tendencingumas būdingas tiek 2020 metais, tiek 2021.



3 pav. Išskvietimų dažnumas

## 6 Duomenų paruošimas

Tyrimo metu, buvo atlikti šie duomenų paruošimo žingsniai: skirtingų duomenų šaltinių apjungimas, naujų požymių kūrimas, treniravimo ir testavimo imties sudarymas ir požymių reikšmių normalizavimas.

Tyrimo naudoti duomenys gaunami iš trijų šaltinių, buvo apjungti remiantis ilgumos ir platumos koordinatėmis. Siekiant analizę papildyti nuskalstamų veikų duomenimis kiekvienam objektui buvo priskirtas nuskalstamų veikų lygis užfiksuotas 1 km spindulio atstumu. Taip pat buvo sukurti nauji kintamieji nusakantys ar gauto išskvietimo lokacija yra miesto centre, ar išskvietimas buvo gautas šventinę dieną, ar išskvietimas buvo gautas savaitgalį, taip pat metų bei paros laiką nusakantys kintamieji, suminio išskvietimų skaičiaus kintamieji, reagavimo dažnumo kintamieji bei laiko tarpus tarp išskvietimų nusakantys kintamieji.

Ansambliniui (angl. *ensemble*) modeliui apmokyti kurtos treniravimo, testavimo ir tikrinimo (angl. *validation*) duomenų aibės. Treniravimo duomenų aibę sudarė 50 %, testavimo ir tikrinimo aibes po 25 % procentus duomenų rinkinio.

## 7 Rezultatai

Siekiant įvertinti bei palyginti klasifikavimo metodų rezultatus buvo taikomas kryžminio patikrinimo metodas su parametru  $k=5$  (angl. *5 fold cross-validation*). Šiuo atveju, duomenų imtis yra dalinama į penkias dalis, kur viena iš dalių yra naudojama testavimui, o likusios modelio apmokymui. Modelių galutiniai rezultatai yra šių 5 testavimo imčių vidurkia. Gauti rezultatai pateikiami 2 lentelėje.

**2 lentelė.** DI modelių rezultatai gauti kryžminio patikrinimo metodu (angl. cross-validation)

Modelis	$F_1$	Tikslumas	Išsamumas
LogisticRegression	0,718	0,718	0,718
GaussianNB	0,682	0,691	0,674
SGDClassifier	0,726	0,744	0,723
KNeighborsClassifier	0,680	0,720	0,720
DecisionTreeClassifier	0,652	0,654	0,642
RandomForestClassifier	0,727	0,735	0,716
GradientBoostingClassifier	0,734	0,724	0,724
LGBMClassifier	0,736	0,741	0,719
XGBClassifier	<b>0,737</b>	<b>0,748</b>	<b>0,727</b>

Pastebėta, kad „XGBoost“ klasifikatorius pasižymi ne tik didžiausia išsamumo įverčio reikšme, tačiau ir didžiausiomis kitų tikslumo metrikų reikšmėmis. Todėl sekančiame etape pasirinkta atlikti šio modelio tinkamiausių hiperparametrų paiešką. Hiperparametrų paieškai naudoti treniravimo ir tikrinimo (angl. *validation*) duomenų aibės. Remiantis naujai gautu hiperparametrų rinkiniu ir testavimo imtimi buvo atliktas „XGBoost“ klasifikatoriaus testavimas, kurio rezultatai parodė, kad modelis pasiekia 0,792 teisingumą (angl. *accuracy*), tikslumą (angl. *precision*) ir išsamumą (angl. *recall*) ir  $F_1$  įvertį, t.y. atlikta hiperparametrų paieška turėjo teigiamą įtaką rezultatų kokybei.

Siekiant padidinti klaidingų iškvietimų aptikimo modelio efektyvumą, pasirinkta apmokyti ansamblinį modelį, sudarytą iš keturių modelių, t. y. sprendimų medžio klasifikatoriaus, artimiausių kaimynų klasifikatoriaus, atraminių vektorių mašinos klasifikatoriaus ir „XGBoost“ klasifikatoriaus, su rastu geriausiu hiperparametrų rinkiniu.

Mašininio mokymosi modeliai, pasirinkti siekiant užtikrinti dvi esmines ansamblinių modelių sudarymo taisykles: modeliai turi būti skirtingi ir modeliai turi pasižymėti geru tikslumu.

Vidiniai ansamblio modeliai mokinti naudojant treniravimo duomenų aibę. Pasinaudojant tikrinimo duomenų aibe atlikti prognozavimai ir gauti procentiniai tikro iškvietimo įverčiai pateikti pagrindiniam „XGBoost“ modeliui apmokyti. Naudojantis testavimo imtimi, atlikti pilno ansamblinio modelio prognozavimai ir gauti tyrimo rezultatai.



Gauti rezultatai rodo, kad šiuo atveju pasiekiamos teisingumo (angl. *accuracy*), tikslumo (angl. *precision*), išsamumo (angl. *recall*) ir  $F_1$  įverčio reikšmės yra lygios 0,887, t. y. sudarytas klaidingų iškvietimų aptikimo modelis pasižymi aukštu tikslumu.

## 8 Išvados

Tyrimo metu analizuojami saugos tarnybų duomenys siekiant sukurti klaidingų iškvietimų aptikimo metodiką. Pirmiausia buvo atliktas duomenų apjungimas, pradinė duomenų analizė, duomenų paruošimas ir modelių kūrimo eksperimentai. Skirtingų šaltinių duomenys apjungiami, siekiant gauti kiek įmanoma daugiau įžvalgų apie iškvietimo patikimumą. Duomenų analizės metu buvo nustatyti tikrų ir klaidingų iškvietimo tendencingumai, į kuriuos atsižvelgus buvo kuriami nauji požymiai.

Remiantis atliktų eksperimentų su skirtingais modeliavimo metodais rezultatais, klaidingų iškvietimų aptikimui rekomenduojama taikyti „XGBoost“ klasifikatorių, kadangi šis metodas pasižymėjo didžiausiu tikslumu. Siekiant pagerinti modelio efektyvumą, buvo atlikta hiperparametrų paieška. Rezultate modelio kokybės rodikliai, apimantys teisingumo, tikslumo, išsamumo ir  $F_1$  įverčius pagerėjo iki 0,792. Norint pasiekti aukštesnį prognozavimo tikslumą buvo sukurtas ansamblinis modelis, kurį sudarė „XGBoost“, sprendimų medžių, atsitiktinių kaimynų ir atraminių vektorių klasifikatoriai. Panaudojant ansamblinio modelio rezultatus, buvo apmokytas galutinis „XGBoost“ klasifikatorius, kuriuo pasiekiamas 0,886 tikslumas ir išsamumas.

## Literatūra

- [1] A. C. Sima, K. Stockinger, K. Affolter, M. Braschler, P. Monte, & L. Kaiser. (2018). A hybrid approach for alarm verification using stream processing, machine learning and text analytics. *EDBT 2018*, 26-29.
- [2] M. A. A. Al-Qaness, F. Li, X. Ma, & G. Liu. (2016). Device-free home intruder detection and alarm system using wi-fi channel state information. *International Journal of Future Computer and Communication*, 5(4), 180.
- [3] M. D. Firoozjaei, J. Park, & H. Kim. (2016). Detecting false emergency requests using callers' reporting behaviors and locations. 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, 243-247.
- [4] A. M. Peco Chacon, & F. P. Garcia Marquez. (2019). False alarms management by data science. *Data science and digital business*, 301-316.
- [5] W. Hu, T. Chen, & S. L. Shah. (2018). Detection of frequent alarm patterns in industrial alarm floods using itemset mining methods. *IEEE Transactions on Industrial Electronics*, 65(9), 7290-7300.