Анализа безбедносних модела детекције упада у дистрибуиране системе, оптимизацијом хибридних алгоритама неуронских мрежа

By Nikola Savanović

WORD COUNT	36283	TIME SUBMITTED	08-JUL-2024 09:21AM
		PAPER ID	110105207

Универзитет Сингидунум
Београд
Департман за последипломске студије

Докторска дисертација

Анализа безбедносних модела детекције упада у дистрибуиране системе, оптимизацијом хибридних алгоритама неуронских мрежа

Ментор

Проф. др Марко Шарац

Студент

Никола Г. Савановић
2015460068

Београд, 2024. године

Ментор и чланови комисије

Ментор:	Проф. др Марко Шарац, Универзитет Сингидунум
Чланови комисије:	Проф. др Небојша Бачанин-Џакула, Универзитет Сингидунум
	Проф. др Бошко Николић, Универзитет у Београду
Датум одбране:	… … 2024.

Сажетак

У овом раду представља се анализа, евалуација и компаративна анализа вишеструког броја алгоритама за класификацију података, у виду здравствених података. Експерименти су изведени над бинарним и вишекласним скуповима података, при чему су коришћене метрике као што су Коенов коефицијент капе, *PR* криве, и *ROC* криве за процену перформанси и друго. Резултати експеримента показују да оптимизовани предложени алгоритам *XG-MFA* остварује и постиже најбоље перформансе у већини случајева. Један од експерименталних резултата показује да предложени алгоритам остварује просечну прецизност од 0.993 над бинарним скуповима података и 0.997 над вишекласним скуповима података, што представља значајно боље перформансе у поређењу са другим анализираним алгоритмима. Овај алгоритам такође постиже највише вредности у *PR* и *ROC* кривама, што указује на његов сврсисходан потенцијал приликом побољшања класификације података. Такође, посебан акценат стављен је на важност детекције и превенције упада у дистрибуиране системе, што је од критичног значаја за заштиту осетљивих здравствених података у ери здравства 4.0. Ефикасна класификација и заштита података осигурава, не само тачне дијагностичке и аналитичке процесе, већ и сигурност података од свих савремених потенцијалних безбедносних претњи по такав систем.

Abstract

This paper presents an analysis, evaluation, and comparative analysis of multiple algorithms for data classification, focusing on healthcare data. Experiments were conducted on binary and multi-class datasets, utilizing metrics such as Cohen's kappa coefficient, PR curves, and ROC curves for performance assessment, among others. The experimental results indicate that the optimized proposed XG-MFA algorithm achieves the best performance in most cases. One of the experimental results shows that the proposed algorithm achieves an average precision of 0.993 on binary datasets and 0.997 on multi-class datasets, representing significantly better performance compared to other analyzed algorithms. This algorithm also achieves the highest values in PR and ROC curves, indicating its purposeful potential for improving data classification. Additionally, special emphasis is placed on the importance of intrusion detection and prevention in distributed systems, which is critically important for protecting sensitive healthcare data in the era of Healthcare 4.0. Effective data classification and protection ensure not only accurate diagnostic and analytical processes but also the security of data from all contemporary potential security threats to such systems.

Захваљујем се својој породици, мојим родитељима и брату, за њихову безусловну подршку током свих година мог академског образовања. Без њихове подршке овај успех никада не би био могућ.

Желим да се захвалим свом ментору, професору др Марку Шарцу, чија су упорност, истрајност, стручност, искуство и мотивација биле од непроцењиве користи током реализације и писања докторске дисертације.

Изражавам посебну захвалност и исказујем изразито дубоко поштовање према Универзитету Сингидунум, на челу са власником и председником проф. др Милованом Станишићем, који су ми омогућили да целокупан наставни процес докторских студија успешно реализујем.

Захваљујем се свим својим пријатељима и колегама који су ми протеклих година пружали несебичну подршку и мотивисали ме да довршим давно постављене циљеве.

Хвала вам.

Садржај

1. Увод 7
1.1. Значај теме и предмет истраживања 15
1.2. Циљ истраживања и полазне хипотезе 16
1.3. Структура докторске дисертације 18
2. Теоријске основе 20
2.1. Карактеристике дистрибуираног система 20
2.2. Савремени изазови у дистрибуираним системима 22
2.2. Архитектура дистрибуираних система 22
2.3. Типови архитектуре 24
2.4. Дистрибуирано рачунарство 27
2.4. Рачунарство у облаку и у дистрибуираним системима 28
2.5. Дистрибуирани системи у пракси и њихове рањивости 29
2.6. Интернет ствари у дистрибуираним системима 30
2.8. Пример коришћења уређаја интернет ствари у концепту *Healthcare* 4.0 31
2.8.1 Рањивости концепта *Healthcare* 4.0 35
3. Наука и преглед литературе 38
4. Дистрибуирани системи и машинско учење 45
4.1. Изазови дистрибуираних система, проблеми и циљеви истраживања 46
4.2. Рањивости инфраструктуре дистрибуираних система 47
5. Машинско учење и алгоритми неуронских мрежа 47
6. Проблеми оптимизације алгоритама машинског учења 50
6.1. Примена алгоритама машинског учења у експерименталним окружењима 52
6.2. Алгоритми машинског учења 52
6.3. Алгоритам *XGBoost* 53
7. Дубоко учење 53
7.1. Дубоке неуронске мреже 54
7.2. Конволуцијске неуронске мреже 54
7.3. Вештачке неуронске мреже - *ANN* 55
8. Метахеуристике – поступци високог нивоа 55
8.1. Механизми заштите ИДС ИПС 57
8.2. Постизање перформанси, прецизности и тачности применом имплементираних алгоритама 58

9. Предложени експериментални алгоритам.....59
10. Експериментални скуп података.....60
10.1. Поставка експеримента и очекивани исходи.....67
10.2. Метрика перформанси експерименталног решења.....69
11. Резултати евалуације експеримента и компаративна анализа резултата.....72
11.1. Резултати експеримента и исходи.....72
11.2 Статистички модел као механизам потврде достигнутих резултата.....125
12. Анализа обављених експеримената.....141
12.1. Закључна разматрања докторске дисертације.....142
12.2 Будући рад и будућа истраживања.....148
13. Литература.....150

Садржај слика

Слика 1 Дијаграмски приказ дистрибуираног система 24
Слика 2 Графичка илустрација клијент-сервер архитектуре 25
Слика 3 Графичка илустрација система равноправних чворова 26
Слика 4 . Графичка илустрација система трослојне архитектуре 27
Слика 5 Илустрација повезивања корисника на дистрибуирани систем уз коришћење технологије Healthcare 4.0 32
Слика 6 Илустрација заштите осетљивих података у Healthcare 4.0 концепту 33
Слика 7 Илустрација повезивања технологија интернет ствари са Healthcare 4.0 концептом 34
Слика 8 8 Графичка илустрација реаговања концепта Healthcare 4.0 на релевантне аларме 35
Слика 9 9 Принцип напада човек у средини 36
Слика 10 Илустрација линеарне регресије представљена линијом нагиба 48
Слика 11 Илустрација логистичке регресије и формиране сигмоидне криве 49
Слика 12 Илустрација класификационог регресионог стабла 50
Слика 13 Класификација метахеуристичких алгоритама [32] 56
Слика 14 Графичка илустрација НП-тешких проблема 57
Слика 15 Графичка илустрација бинарног скупа података за дистрибуцију ознака [13] 64
Слика 16 Графичка илустрација вишекласних безбедносних скупа података [13] 64
Слика 17 Графичка илустрација безбедносног бинарног скупа података [13] 65
Слика 18 Графичка илустрација дистрибуција класа [13] 66
Слика 19 Графичка илустрација корелација карактеристика приказано кроз топлотну мапу [13] 67
Слика 20 Графикон дијаграма циља за бинарни скуп података [13] 80
Слика 21 Графикон циља конвергенције за бинарни скуп података [13] 81
Слика 22 Графикон криве PR предложеног XG-MFA алгоритма [13] 82
Слика 23 Графикон макро и микро просека ROC криве за бинарни скуп података [13] 83
Слика 24 Графичка илустрација расподеле различитости појева у бинарном скупу података [13] 84
Слика 25 Графичка илустрација бинарног скупа података XG-MFA алгоритма и матрица конфузије [13] 85

Слика 26 Графичка илустрација дијаграма циља за максималне вредности Коеновог коефицијента капе [13] 93
Слика 27 Графикон конвергенције, где се приказују максималне вредности Коеновог коефицијента капе [13] 94
Слика 28 Графичка илустрација PR криве над бинарним скупом података, помоћу максималних вредности Коеновог коефицијента капе [13].....95
Слика 29 Графичка илустрација макро-микро просека за бинарни скуп података XG-MFA алгоритма [13].....96
Слика 30 Графичка илустрација расподеле различитости појева, помоћу максималних вредности Коеновог коефицијента капе [13] 97
Слика 31 Графичка илустрација матрице конфузије за максималне вредности бинарног скупа података помоћу Коеновог коефицијента капе [13] 98
Слика 32 Дијаграм вишекласног скупа података, где се илуструје дијаграм циља [13] 108
Слика 33 Графикон конвергенције објективне функције током итерација за различите алгоритме, показујући како се перформансе мењају током времена [13].....109
Слика 34 Површина испод криве PR (Precision-Recall) за XG-MFA алгоритам, која илуструје однос између прецизности и одзива у сценаријима са неуравнотеженим класама [13] 110
Слика 35 Површина испод криве ROC (енгл. Receiver Operating Characteristic) са макро и микро просецима за XG-MFA алгоритам, омогућавајући процену перформанси у различитим праговима класификације [13].....111
Слика 36 Дијаграм различитости појева за објективне вредности, који визуализује густину и расподелу резултата међу различитим алгоритмима [13].....112
Слика 37 Матрица конфузије за XG-MFA алгоритам, која приказује тачна и нетачна предвиђања за различите класе, помажући тиме идентификације области где модел најчешће греши [13].....113
Слика 38 Дијаграм циља за вредности вишекласног скупа података различитих алгоритама, који помоћу Коеновог коефицијента капе [13].....114
Слика 39 Графикон конвергенције вишекласног скупа података током итерација, илуструјући како се резултати мењају кроз више итерација [13].....115

Слика 40 Површина испод криве Precision-Recall, која приказује однос прецизности и одзива за XG-MFA алгоритам, важан за процену модела са неуравнотеженим класама [13] 116
Слика 41 Површина испод криве (енгл. Receiver Operating Characteristic - ROC), приказујући како алгоритам балансира између истинито позитивних и лажних позитивних предвиђања при различитим праговима [13] 117
Слика 42 Дијаграм вишекласног скупа података где се помоћу Коеновог коефицијента капе визуализује густину резултата и распон перформанси различитих алгоритама [13] 118
Слика 43 Матрица конфузије за која приказује детаљне тачне и нетачне класификације за сваку класу [13]....119
Слика 44 Интерпретација важности карактеристика у бинарној и вишекласној класификацији помоћу XGBoost-a [13] 130
Слика 45 Интерпретација важности карактеристика у бинарној и вишекласној класификацији помоћу XGBoost-a [13] 131
Слика 46 SHAP анализа утицаја карактеристика у бинарној и вишекласна класификацији помоћу XGBoost-a [13] 132
Слика 47 SHAP анализа утицаја карактеристика у бинарној и вишекласној класификацији помоћу XGBoost-a [13] 133
Слика 48 nSHAP анализа 10. реда за бинарну и вишекласну класификацију са приказом интеракција карактеристика [13]....135
Слика 49 nSHAP анализа 10. реда за бинарну и вишекласну класификацију са приказом интеракција карактеристика [13]....136
Слика 50 Шапли–Тејлор анализа карактеристика бинарна класификација [13] 138
Слика 51 Шапли–Тејлор анализа карактеристика вишекласна класификација [13]....139
Слика 52 nSHAP анализа другог реда за бинарну и вишекласну класификацију - Бинарна nSHAP анализа [13] 140
Слика 53 nSHAP анализа другог реда за вишекласну класификацију - вишекласна nSHAP анализа [13]....141

Садржај табела

Табела 1 Збирни резултати бинарне класификације - експеримент минимизације грешке [13] 74
Табела 2 Добијени резултати експеримента минимизације према дефинисаним класама [13] 77
Табела 3 Најбољи добијени хиперпараметри од стране модела помоћу бинарне класификације [13] 79
Табела 4 Резултати експеримента максимизације коефицијента Коенове капе дате бинарне класификације [13] 87
Табела 5 Резултати експеримента максимизације коефицијента Коенове према класама 0 и 1 89
Табела 6 Поставке хиперпараметара за моделе бинарне класификације експеримента [13] 92
Табела 7 Приказ општих резултата класификације вишеструких класа [13] 99
Табела 8 Резултати вишекласне класификације приликом експеримента минимизације грешке [13] 101
Табела 9 Најбољи хиперпараметри добијени од стране модела за вишекласну класификацију у експерименталном поступку минимизације грешке [13] 103
Табела 10 Резултати вишекласне класификације у експерименту максимизације Коеновог капа коефицијента [13] 105
Табела 11 Детаљни резултати по класама за најбоље извођење модела вишекласне класификације - симулација максимизације Коеновог капа коефицијента [13] 122
Табела 12 Најбоље добијени модели хиперпараметара за вишекласну класификацију у оквиру експеримента за максимизацију Коеновог капа коефицијента [13] 124
Табела 13 Резултати Шапиро-Вилкових тестова нормалности за различите XGBoost алгоритме у различитим сценаријима [13] 128
Табела 14 Резултати Вилкоксоновог теста са рангирањем за процену статистичке значајности перформанси XG-MFA методе у односу на конкурентске методе у различитим сценаријима [13] 129
Табела 15 Поређење перформанси различитих модела машинског учења на IoT-Flock здравственом скупу података за предвиђање малициозног и нормалног саобраћаја [13] 137

1. Увод

Експоненцијалним растом измештања мрежне инфраструктуре организација у комплексне дистрибуиране системе (енгл. *Distributed System*), где је од важности сачувати интегритет и непорецивост осетљивих информационих података, повећава се и број потенцијалних рањивости услед њихове хетерогености. Докторска дисертација се бави анализом, унапређењем и предлагањем новог модела механизма заштите рањивости сложених дистрибуираних система у погледу детекције упада. Стога, предложеним оптимизованим моделом прецизније се може утврдити да ли је мрежни саобраћај валидан или се може сматрати потенцијално сумњивим, тј. рањивим и малициозан по један такав систем. Побољшава се детекција класификације потенцијалног напада на дистрибуирани систем. Постојећи механизми се унапређују оптимизацијом хибридних алгоритама, помоћу неуронских мрежа (енгл. *Neural network*), те се предлаже нови модели који могу прецизније и на време препознати претњу или утврдити да ли се посматрани мрежни саобраћај може класификовати као *нормалан*, тј. исправан мрежни саобраћај. Неуронске мреже, често називане и вештачке неуронске мреже (енгл. *Artificial Neural Networks - ANN*), могу се представити као део области машинског учења, а засновани су на идеји људског мозга, где се опонашају биолошки неурони који међусобно могу слати и размењивати сигнале.

Дистрибуирани системи представљају међусобно повезану мрежу чији је след оперативних активности координисан у напред предефинисаним акцијама и догађајима. Такође, представљају колекцију високо софистицираних физички раздвојених серверских уређаја (машина), као и колекцију за складиштење података (енгл. *Storage server*). Сервери за складиштење података представљају мрежну локацију са огромним потенцијалом за чување различитог дигиталног садржаја (документи, аудио/видео садржај, софтвери итд.) једне организације. Серверима за складиштење података може се приступати локално или путем јавне мреже (интернета). Такође, може се имплементирати таква конфигурација да им се може приступати искључиво из јасно уређеног, тј. дефинисаног ИП опсега (нпр. из седишта организације) користећи одговарајуће софтвере путем којих се може обезбедити сигурнија конекција, а у циљу постизања очувању интегритета података.

Иза сложеног дистрибуираног система, као таквог, може стајати изграђена (или изнајмљена) сложена инфраструктура која је, заправо, одговорна за имплементацију решења. Склад између компоненти дистрибуираног система и пратеће софтверске имплементације у директној је корелацији, како би се приликом међусобних интеракција створио релевантан режим у којем се може одговорити заједничком акцијом, тј. постизањем јединственог исхода (нпр. остваривање приступа мрежном ресурсу, софтверу итд.). Фактор свеукупног побољшања механизма детекције упада у један сложен дистрибуирани систем може се побољшати оптимизацијом хибридних алгоритама, помоћу неуронских мрежа.

Област рачунарских наука дистрибуиране системе препознаје као механизам рачунарства у облаку (енгл. *Cloud computing*). У савременом дигиталном свету

рачунарство у облаку представља централизован систем; користе се различите технике за приступање дељеном ресурсу (садржају, документу, медију итд.) путем глобалне мреже, стога се у дистрибуиране системе може уврстити наведени систем. Према организацији Националног института за стандарде и технологију - *NIST* (енгл. *National Institute of Standards and Technology*) и специјалној публикацији издатој у те сврхе (под бројем 800-145), рачунарство у облаку представља модел за који се каже да је свеприсутан, практичан и доступан на захтев; омогућава брз приступ и интеракцију ресурсима, са минималним управљањем према страни пружаоца услуге [1]. Оно представља испоруку различитих типова услуга путем јавне глобалне мреже. Услуге рачунарства у облаку могу бити услуге коришћења различитог софтвера, складиштења података, услуге изнајмљивања сервера, различитих мрежних ресурса и друго. Генерално, такав дељени ресурс се може крајњим корисницима испоручивати на захтев (енгл. *On-demand*). Дељени ресурси могу бити доступни путем софтверског решења (нпр. веб апликације), у виду мрежних дељених фолдера и друго. У дистрибуираном рачунарству (енгл. *Distributed Computing*), многобројне услуге могу испоручивати садржај према различитим специфичним условима. У контексту значења пружања услуга, првенствено се сматра испоручивање захтеваног садржаја према задатом критеријуму од стране тражиоца одговарајуће услуге. То може бити захтев за приступ одговарајућем директоријуму, упућивања различитих захтева ка дистрибуираном систему и друго. Упућени захтеви могу бити стандардни, тј. захтеви за преузимање (GET), уписивање (POST), брисање (DELETE), затим, за изменом постојећег ресурса (PUT) итд.

Како се услед глобалних и савремених трендова јавља потреба за све већом интеграцијом дистрибуираних система, многе светске организације изместиле су своје пословање у облак, тј. у дистрибуиране системе. Тиме је постигнуто значајно умањење трошкова у погледу интеграције сопствених решења, у виду опремања организације физичким серверима и другом пратећом сложеном мрежном опремом. Физичким измештањем серверске инфраструктуре, услед измештања пословања из физичких просторија организације, јавили су се проблеми рањивости и чувања интегритета измештених података на удаљене сервере. Могу се дефинисати различите претње за сваки систем, као ентитет. Свака нестабилност у раду негативно се може одразити на пословање организације. Неке добро познате безбедносне рањивости [81] јесу напади *DDoS* (енгл. *Distributed Denial of service*) [58][92] - ускраћивање услуге и ометање нормалног функционисања система, затим, напад на успоставу везе, линкове рутирања и сесије, *SQL* инјекције, напади уметања скрипт кодова - *XSS* (енгл. *Cross-Site Scripting*), напади на механизме и системи аутентикације и ауторизације. Од важности је напоменути да наведени напади представљају само најосновније добро познате нападе. Такође, нивои претњи од малициозног софтвера и рањивих кодова може значајно разликовати у зависности од типа дистрибуираног система који трпи напад. Поред интеграције савремене физичке опреме, важно је исправно извршити конфигурацију дистрибуираног система, исправна имплементација безбедносних механизама и

протокола заштите, као и редовност у погледу ажурирања система и софтвера. Дистрибуирани системи се могу штити на различите начине, а то је:

- Имплементација сложених механизама аутентикације и ауторизације уз фактор двоструке провере,
- Шифровањем података, мрежног саобраћаја и коришћење сложених алгоритама који могу бити од користи приликом приступања удаљеном ресурсу,
- Праћење логова, анализа прикупљеног саобраћаја и детекција безбедносних инцидената, интеграција сложених система попут IDS/IPS (енгл. *Intrusion Detection System*/*Intrusion Prevention System*) [90],
- Подизање свеукупне свести и едукација запослених о имплементираним пословним принципима безбедносних механизама.

Интернет ствари (енгл. *Internet of Things*) према националном институту за стандарде и технологију, према публикацијама *NIST SP 800-172* и *NIST SP 800-172A*, представља рачунарску мрежу уређаја која у себи садржи скуп хардвера, софтвера, фирмвера и актуатора, који омогућавају међусобну интерактивност и повезивање са другим уређајима, те се на тај начин могу размењивати подаци путем интернета [2]. Уређаји интернет ствари могу бити различитих намена, те се могу наћи у кућним апаратима, аутомобилској индустрији [70][84], у различитим медицинским уређајима и друго. Идеја лежи у томе да се омогућава међумрежна комуникацију, тј. размена података између различитих физичких уређаја, те се таквом интеграцијом постиже имплементација паметних уређаја. Многобројни изазови су постављени пред овај тир рачунарске мреже у погледу свеобухватне сигурности, с обзиром на то да се може управљати изузетно великом количином података. Од важности је имплементација јаких, сложених и адекватних безбедносних мера, како би се умањио ризик од *цурења* података. Рањивост интернет ствари суштински одговара рањивостима дистрибуираних система, с тим да постоје специфичне разлике. Наиме, различити физички уређаји имају различите нивое заштите; некомпатибилност доводи до проблема слабих сигурносних механизама. Такође јавља се проблем нередовности ажурирања уређаја интернет ствари, те нове верзије напада могу значајно угрозити старије верзије физичких уређаја. Може се јавити рањивост у погледу небезбедних бежичних мрежа, с обзиром на то да многи уређаји користе механизме за бежично повезивање уређаја, са слабом безбедношћу (нпр. конекција која користи *bluetooth* везу, тј. стандард). Некомпатибилност и недостатак стандарда значајно доприноси свеопштој рањивости уређаја интернет ствари који припадају једној дистрибуираној мрежи. Изазов у погледу безбедности дистрибуиране мреже, где равноправне чланове мреже чине уређаји интернет ствари, представља уједначавање стандарда и компатибилност између уређаја. Такође, јачање и имплементирање снажних механизама аутентикације и сложене ауторизације може се сматрати једним од најважнијих фактора у доприносу безбедности. Стога, неопходно је утврђивати идентитет сваког корисника који има тенденцију пријаве или се представља равноправним чланом мреже, где је приликом сваке аутентикације неопходно извршити одговарајуће додељивање права приступа. Истовремено, од важности је безбедно управљање уређајима (коришћењем сложених лозинки за приступ), имплементација

софтверских и хардверских решења заштитног зида (енгл. *Firewall*), као имплементација система за детекцију и превенцију упада у мрежу - *IDS*/*IPS*.

Вештачка интелигенција (енгл. *Artificial Intelligence*) представља глобални тренд који значајно доприноси унапређењу постојећих друштвених и индустријских решења, омогућавајући већу подршку аутономији уређаја (у свим гранама индустрије), разноликом спектру иновација, повезујући уређаје интернет ствари у организацијама, индустрији, паметним кућама и друго [3]. Значајан су фактор, готово, сваком аспекту данашњег друштвеног и пословног света. Истовремено, јавља се проблем рањивости оваквих система у погледу неправилног тренирања над великим скуповима подацима, где грешке, услед погрешне донесене одлуке, могу проузроковати имплементацију лоших резултата. Самим тим, јавља се рањивост која се може огледати у манипулацији над скуповима података, те се један аутономни или дистрибуирани систем може обмањивати. Имплементација вештачке интелигенције се могу користити на нивоу организације, где такви системи постају циљана мета нападача који умећу злонамеран код [94]. Као исход таквих случајева, малициозни код се може преносити *по дубини*, кроз целокупан дистрибуирани систем ка уређајима који су директно повезани на имплементиран систем вештачке интелигенције. Вештачка интелигенција може бити веома сложена за заштиту, те се мора водити рачуна о шифровању скупова података, њиховом заштићеном преносу и коришћењем безбедносних протокола током њиховог преноса. Неопходно је на уму имати интеграцију сложених механизама заштите над моделима, а са циљем заштите интегритета тренираних скупова података. Такође, реаговању на инциденте услед откривених аномалија, потенцијалних и евентуалних неправилности у раду, вештачка интелигенција може значајно допринети побољшавањем механизама за детекцију и превенцију упада.

Као грана вештачке интелигенције машинско учење (енгл. *Machine learning*) [65] акценат ставља на коришћење података и употребу алгоритама [4]. Фокус и циљ јесте људско опонашање учења, постепено остварујући боље, тачније и прецизније резултате у односу на претходно остварено искуство, тј. претходно постигнуте резултате учења. Традиционални механизми за детекцију упада, често се фокусирају и изолују у појединачном, тј. засебном сегменту организације. Скалабилност и проширивост представљају изузетно сложен процес приликом имплементације нових развојних трендова у погледу шифровања података, конекције, протокола [57], као и самог система *по дубини*. Услед појаве савремених метода унапређења исхода тренирања модела машинским учењем, коришћењем савремених алгоритама машинског учења, од важности је унапредити постојећи оквир за детекцију и превенцију упада, који може идентификовати повезане претње. Добро познати и актуелни проблеми који представљају високе и сложене рањивости систему јесу уцењивачки злонамерни софтвери (енгл. *Ransomware*), као и напади напредне трајне претње (енгл. *Advanced Persistent Threat - APT*) који се могу карактерисати као шпијунажа или саботажа једне мреже дистрибуираних система [5]. Машинским учењем, односно, побољшањем и оптимизацијом алгоритама за детекцију и превенцију упада се може постићи

свеобухватно унапређење заштите интегритета инфраструктуре организације [103]. Такође, оптимизацијом алгоритама машинског учења може се остварити виша прецизност у погледу детекције упада у један дистрибуирани систем.

Алгоритми машинског учења представљају математичке моделе путем којих је могуће направити след догађаја који су способни да на основу претходно стеченог искуства (знања) донесу одговарајућу одлуку. Уређаји који користе овакве интегрисане алгоритме у својим логичким операцијама, могу користити кодове машинског учења за препознавање патерна (образаца), затим, помоћу истих је могуће доношење различитих одлука у зависности од типа података који су добијени на улазу (енгл. *Input*), као и током процеса учења.

Оптимизацијом алгоритама машинског учења може се окарактерисати као поступак проналаска што идеалнијих параметара или најадекватнијих карактеристика модела. Проналаском одговарајућих вредности постижу се боље перформансе у оквиру датог сценарија, тј. задатка. Као исход оптимизације може се сматрати унапређење алгоритма у погледу побољшања способности модела, где се на основу улазних података тачније предвиђају или класификују излази. Добијањем бољих и тачнијих резултата постиже се ефикасност у погледу примене машинског учења. Један од начина оптимизације алгоритама машинског учења јесте оптимизација хиперпараметара, што уједно представља и кључни метод који се примењује у овој докторској дисертацији. Хиперпараметри могу имати изузетно висок нивоу утицаја на перформансе модела, те се свеукупна употребљивост модела у практичној примени може значајно унапредити. Такође, у експерименталном делу докторске дисертације, коришћене су метахеуристичке оптимизације за проналазак доброг решења у посматраном простору података, као подршка оптимизацији хиперпараметрима; временски фактор је подразумевано прихватљив приликом претраге.

Алгоритми машинског учења нису имуни на рањивости различитог типа које могу бити традиционални напади или манипулацијом података, нарушавајући тачност модела, као и утицај приликом доношења одлука. Добро познати напад на алгоритме машинског учења представљају *преварантски напади* (енгл. *Adversarial attacks*), где нападач директно може утицати на улазне податке, тј. информације модела. Тиме се може у потпуности нарушити интегритет модела, као и његова непорецивост у погледу генерисања излаза података, односно, доношења одлука модела.

Неуронске мреже представљају тип вештачких неуронских мрежа за решавање изузетно сложених и комплексних проблема [66]. Ова област заснована је на принципима и идеји људског мозга, где више вештачких неурона заједно извршавају сложене задатке (класификација скупова података [67], различита предвиђања [59], препознавање објеката итд.). Допринос неуронских мрежа у процесима доношења одлука предвиђања има за циљ минимизације грешке. Таква минимизација може се постићи на основу балансирања тежина веза између међусобно повезаних неурона. У погледу рањивости,

неуронске мреже подложне су одређеним нападима, који могу угрозити прецизност модела. Такође, услед непрецизности модели могу претрпети значајну количину погрешно унесених вредности, те се могу генерисати нетачна предвиђања. Важно је истаћи да напади оваквог типа за људске посматраче изгледају готово идентично и непромењено [6]. Како би модел у потпуности био рањив, нападач мора познавати унутрашњост и структуру скупова унутар модела или нападач мора имати сазнања у вези са тренирани подацима [6]. Могуће је имплементирати већу сигурност неуронских мрежа различитим стратегијама попут регуларизације, развијањем редудантних модела, вишеструке провере улазних података (пре почетка тренирања модела) и друго.

Дубоко учење представља специфичну грану машинског учења са акцентом на обучавање (вештачких) неуронских мрежа [68]. Фокус дубоког учења усмерен је на специфичну област [60] - дубоке неуронске мреже (енгл. *Deep neural networks - DNNs*). Дубоке неуронске мреже имају висок степен ефикасности [95] у широком задатом спектру постављених задатака машинског учења; засноване су на концепту учења људског мозга. Дубоке неуронске мреже у својој имплементацији могу имати најмање један скривени слој, који се, заправо, смешта између улазних и излазних слојева. Скривени слој, састављен од скривених неурона, има фунцкију сложених операција над улазним подацима у циљу постизања нових и апрстракнијих излазних резултата, а приликом разрешавања комплексних проблема. Примарно се омогућава представљање података кроз више нивоа, те се тиме постиже решавање комплексних проблема [7]. Како неуронске мреже представљају изузетно снажан механизам и моћан алат за разрешавање комплексних проблема, оне су потпомогнуте дубоким учењем које могу значајно допринети у различитим сферама; то може бити подршка аутономним уређајима, могу значајно допринети области препознавању графичких илустрација, облика, визуализација итд. Као и друге области овог поља, дубоко учење није у потпуности непробојно и није немогуће извршити нарушавање свеукупне безбедности података. Постоје различити типови рањивости које могу утицати на интегритет улазних и излазних података. Као и код алгоритама машинског учења, све се чешће указује на проблем *преварантских напада* где нападач може извршити измене у виду погрешне класификације уз улазне податке.

Постоје механизми заштите дубоког учења које за циљ имају умањење штете узроковане услед напада на интегритет и непорецивост улазних података. Различите рањивости могу бити разрешене или пак умањене користећи се релевантним техникама за дате сценарије, те се могу користити технике регуларизације, затим, употребом валидационих сукопова, адекватним подацима тренинга и друго. Одбрамбеним механизмима могу се створити значајно поузданији модели дубоког учења, те се уједно и свеобухватни интегритет дистрибуираног система може побољшати.

Сходно претходно наведеним претпоставкама, спрега и међусобна веза између машинског учења, дубоког учења и неуронских мрежа евидентно указује да се може направити корелација између датих грана и области. Будући да се наведене технике

користе наизмечно, у датом тренутку, може се рећи и да постоје основне разлике и нијансе између њих. Наиме, област вештачке интелигенције, као дисциплина, у себи садржи своје под-области, тј. машинско и дубоко учење, као и неуронске мреже. Но, неуронске мреже представљају под-област машинског учења, а дубоко учење представља под-област неуронских мрежа [4].

У експерименталном делу докторске дисертације доказује се и постиже се научни допринос у побољшању заштите дистрибуираног система. Примењују се технике оптимизације машинског учења метахеуристиком и хиперпараметрима, како би се постигао виши степен заштите интегритета података и целокупног дистрибуираног система као виталног дела једне организације, унапређивањем техника детекције упада у мрежу. Предложени алгоритам комбинује *XGBoost* са модификованим алгоритмом свитаца (XG-MFA) како би се побољшала тачност и поузданост модела у задацима вишекласне и бинарне класификације. Анализа је спроведена коришћењем *IoT-Flock* генерисаног скупа података из здравствених *IoT* уређаја, са фокусом на откривање малициозних и нормалних саобраћајних патерна, тј. образаца. Овај рад има за циљ да покаже супериорност предложеног *XG-MFA* алгоритма у односу на постојеће методе, истовремено пружајући концизан, детаљан и јасан оквир за разумевање и побољшање свеукупне безбедности у дистрибуираним системима који користе уређаје интернет ствари. Приликом извођења експеримената добијени резултати, упоређују се са другим иновативним и најновијим метахеуристичким методима у идентичном експерименталном окружењу; доказују супериорну прецизност и тачност над посматраним скупом података. Тиме се може рећи да предложени модел постиже инфериорну тачност у поређењу са другим високопрецизним добијеним резултатима. Резултати указују на значајне предности у прецизности и стабилности модела, чиме се отвара пут за будућа истраживања и примене у многобројним доменима савремене дигиталне ере.

Током експерименталних поступака у овој докторској дисертацији представља се анализа, евалуација и компаративна анализа више алгоритама за класификацију скупа здравствених података. Услед раста обима и комплексности здравствених података [102] у ери *Healthcare* 4.0 [107] [108], од важности су алгоритми који могу ефикасно обрађивати и класификовати скупове података, док се истовремено обезбеђује висок ниво заштите података услед потенцијалних напада. У датом контексту, предложени *XG-MFA* алгоритам показује предности у поређењу са постојећим поредбеним методима.

Експерименти су изведени на бинарним и вишекласним скуповима података, при чему су коришћене метрике као што су Коенов коефицијент капе [105], *PR* криве [106], и *ROC* криве [104] за процену перформанси. Резултати показују да алгоритам *XG-MFA* остварује и постиже најбоље перформансе у већини случајева, са просечном прецизношћу од 0.993 на бинарним и 0.997 на вишекласним скуповима података. *PR* и *ROC* криве показују да предложени алгоритам *XG-MFA* постиже највише вредности

прецизности и одзива у поређењу са другим алгоритмима, што га чини супериорним избором за класификацију података. Алгоритам достиже највише резултате у метрици Коеновог коефицијента капе, указујући на високу стопу приликом предвиђања и постижући стабилност остварених резултата.

Поред постигнутих високих перформанси приликом класификације података, предложени модел *XG-MFA* алгоритам интегрише напредне методе заштите података у своју архитектуру, укључујући напредне методе шифровања и аутентикације. Захваљујући механизму за рано откривање аномалија (детекција упада) [77], алгоритам омогућава брзо реаговање на потенцијалне претње, а самим тим значајно смањује ризик од упада у дистрибуиране системе. У експерименталним поступцима показао је високу отпорност на различите типове напада, укључујући *DoS* и *DDoS* нападе, са способношћу да идентификује и спречи 99.9% симулираних напада.

Системи који користе предложени оптимизовани алгоритам *XG-MFA* приказују смањен број лажних позитивних и лажних негативних детекција, што побољшава поузданост и тачност система за детекцију упада. Ефикасна класификација података постиже сигурност података од свих савремених потенцијалних безбедносних претњи на дистрибуиран систем. Увођење предложеног алгоритма у здравствене системе може значајно допринети побољшању заштити осетљивих података пацијената. Предложени модел такође омогућава скалабилност и прилагодљивост различитим окружењима, што га може чинити од значајне користи у реалним ситуацијама у пракси. Узимајући у обзир све постигнуте резултате, може се закључити да *XG-MFA* алгоритам у експерименталним поступцима постиже одличне перформансе [78] приликом класификације и заштите података у дистрибуираним системима концепта *Healthcare* 4.0.

1.1. Значај теме и предмет истраживања

Услед велике разноликости и сложености дистрибуираних система, ни за један систем се не може дефинисати униформно решење које може представљати полазну тачку или бити полазни модел, на основу ког се могу градити решења за ма који специфичан сценарио. Четврта дигитална индустријска револуција, позната под називом *Индустрија 4.0,* донела је дигиталном друштву и глобалној индустрији многобројне погодности у погледу аутоматизације посла. Комбинујући различите хардверске технологије, омогућавајући софтверску подршку за постављање адреса интернет протокола (верзије 4 и верзије 6) на дате уређаје, омогућена је синтеза различитих типова уређаја. Овакви уређаји потпадају под опште дефинисани и усаглашени појам - интернет ствари (IoT). Сходно њиховој хардверској разноликости, јавиле су се многобројне рањивости уређаја интернет ствари, те је неопходна и њихова боља и ефикаснија заштита. Предмет истраживања докторске дисертације тежи унапређењу модела детекције упада у мрежу. Наиме, јављају се значајни проблеми приликом филтрирања и анализирања мрежног саобраћаја, а који пристиже са удаљене локације до физичког уређаја (интернет ствари).

Стога, акценат се ставља на унапређење детектовања стварних напада, у односу на потенцијално рањиве или на одговарајуће сумњиве активности. Како се целокупан пристигли мрежни саобраћај не би засебно анализирао и филтрирао, алгоритми машинског учења значајно могу допринети ефикаснијој провери, умањујући стопе тзв. лажних позитивних (енгл. *False positive*) стања. Дато стање представља резултат утврђивања да је, заправо, једно стање тачно (true) онда када је то стање суштински нетачно (false). Овакав мрежни саобраћај се сматра исправним, али у великом броју механизми за детекцију упада (IDS) означавају га потенцијално рањивим по систем, блокирајући валидан упит, тј. захтев према дељеној мрежној локацији (нпр. сервер, мрежни ресурс, мрежни софтвер итд.). Аларми који се оглашавају приликом активације детекције представљају уједно и лажне аларме [8]. Такође, уједначено је неопходно водити рачуна и о супротном стању које може бити лажно негативно (енг. *False negative*) које се сматра најопаснијим и најштетнијим по један дистрибуирани систем, где се стварни напад (или рањивост) сматра исправним мрежним саобраћајем, тј. валидним упитом.

Над системима детекције упада у дистрибуиран систем, у овој докторској дисертацији, постојећа решења се оптимизују помоћу неуронских мрежа, где се вишеструким понављањем експеримената подиже боља класификација мрежног саобраћаја. За оптимизацију метахеуристикама коришћен је *алгоритам синус косинус* (енгл. *Sine Cosine Algorithm - SCA*). Добијени резултати извршених експеримената поређени су са релевантним резултатима дате области. У сврхе експеримената коришћени су добро познати скупови података (енгл. *Datasets*) за детекцију и превенцију упада.

1.2. Циљ истраживања и полазне хипотезе

Импликације остварених резултата у значајној мери доказују постављене теоријске тврдње приликом општих разматрања овог научног истраживања. Експерименталним истраживањем и доказивањем се процењује класификација мрежних података, тј. мрежног саобраћаја. На основу извршене класификације перформансе и ефикасност се побољшавају хибридним алгоритмом неуронских мрежа. Робусним алгоритмом машинског учења *XGboost* врши се класификација мрежних напада. Експеримент се врши над скуповима података генерисаних помоћу *IoT-Flock* алата [36], који може симулирати здравствене сценарије са нормалним и малициозним уређајима.

Компаративним методама са радовима релевантне области резултати се пореде, те се успоставља нови модел високих и супериорних перформанси. Циљ истраживања, на основу низа обављених експеримената, манифестује се као утврђивање и побољшање ефикасности система за откривање упада у дистрибуирани систем.

Савремени дистрибуирани системи немају универзално и оптимално решење у погледу заштите инфраструктуре. Свака организација која користи услуге дистрибуираних система може интегрисати и имплементирати своја сопствена решења, те је услед њихових специфичности неопходно анализирати и утврдити експериментима која врста оптимизације највише одговара датом сценарију. Наиме, у те сврхе се могу користити хибридни алгоритми у циљу оптимизације и побољшања постојећих модела, а који знатно могу допринети очувању интегритета једног дистрибуираног система.

Докторска дисертација предлаже ефикаснији модел постојећих система заштите дистрибуираног система, засновано на оптимизованом алгоритму, са акцентом на унапређење механизма детекције упада у такав сложени и измештени систем организације. Идеја научног истраживања у докторској дисертацији ослања се на извођење различитих експерименталних поступака, како би се дошло до баланса између што прецизнијег модела и што оптималнијег решења. Услед експерименталних анализа, утврђују се и недостаци оваквих система, како њихових механизмима за детекцију упада тако и у имплементираним постојећим решењима. На основу прикупљеног корпуса мрежног саобраћаја побољшава се детекција потенцијално рањивог саобраћаја у мрежној инфраструктури дистрибуираног система.
Полазне и појединачне хипотезе овог научног истраживања могу се представити као:

- Адаптивним методима утврђује се степен рањивости дистрибуираног система.
- Машинско учење доприноси повећању перформанси у погледу ефикасне размене података између великог броја сервера (и сервиса) и корисника.
- Методи машинског учења могу побољшати постојеће алгоритме детекције и превенције упада; свеукупно, може повећати ефикасност и прецизност приликом доношења одлука за умањење сумњивих активности у дистрибуираном систему.
- Оптимизацијом хиперпараметрима и метахеуристиком врши се високопрецизнија претрага за што оптималнијим решењем.

- Неуронске мреже доприносе поузданости модела за детекцију и превенцију упада. Емпиријским истраживањем установљен је след фаза експеримената, на основу корпуса информација.
- На бази извршених експеримената утврђују се коначне разлике посматраних скупова података са упоредивим научним доприносима из области, те се покреће процес дедукције о употребљивости предложеног модела.
- Комбиновањем хибридних алгоритама машинског учења, као и побољшањем истих, може се постићи се унапређење детекције упада у дистрибуирани систем без значајног утицаја на перформансе система.

1.3. Структура докторске дисертације

Уводни део садржи теоријске претпоставке, циљеве, исходе, као и спрегу са релевантним научним доприносима из области.

Друго поглавље садржи детаљнији опис теоријских основа из области научног истраживања.

Треће поглавље тезе представља преглед научних радова, истраживања и значајних доприноса у погледу хибридне заштите дистрибуираних система. У овом делу поглавља приказују се досадашњи остварени резултати унапређених заштитних механизама у дистрибуираним системима, као и у њиховој инфраструктури. Акценат трећег дела представља анализу унапређених и предложених нових модела хибридних алгоритама детекције и превенције упада у мрежну инфраструктуру. Остварени резултати из научне области манифестују се као оквир и основ за теоријско поткрепљење тврдњи и експерименталних оквира ове дисертације.

Четврти део садржи детаљан преглед архитектуре рачунарства у облаку, специфичне сервисе и протоколе. Дефинише се преглед области машинског учења и вештачке интелигенције. Такође, дефинише се оквир за општа разматрања и начин примене наведених технологија над дефинисаном експертизом. Наведени оквир подразумева дефинисање проблема рањивости детекције и превенције упада у мрежну инфраструктуру организације. У оквиру истог дела описује се утицај метахеуристике. Посебна пажња усмерава се на корелацију између машинског учења и препознавања различитих активности које се одвијају у клијент-сервер архитектури.

Пети део дисертације садржи теоријске основе проблема оптимизације алгоритама машинског учења и вештачке интелигенције, као и предложене методе разрешења постављених проблема претходног дела.

Шести део састоји се од теоријских претпоставки проблема оптимизације машинског учења, као и дефинисања рањивости инфраструктуре дистрибуираних система. У наведеном поглављу детаљно се описују проблеми, рањивости у савременом пословном окружењу организација, а које користе дату имплементацију мрежног приступа ресурсима применом алгоритама машинског учења.

Седмо поглавље докторске дисертације садржи преглед у области дубоког учења, са посебним акцентом на алгоритме машинског учења, неуронских мрежа, као и разматрања могућности њихове хибридне оптимизације, користећи и метахеуристике.

У осмом поглављу описује се шта, заправо, представља суштину разрешења проблема приликом унапређења оптимизације алгоритама машинског учења. Посебан осврт ставља се на важност баланса метахеуристика, перформанси и тачности података, као и на постигнутом времену извршавања задатих операција у оквиру механизама заштите детекције упада у дистрибуиране системе.

У деветом делу дисертације истиче се предложени експериментални поступак, класификација анализираног мрежног саобраћаја, са свим аномалијама, који се може карактерисати као упад у дистрибуиран систем. Из свега тога даје се оквир одабира релевантног решења, користећи алгоритме машинског учења.

Десети део дисертације садржи опис експеримента, где се над свим обављеним сетовима података примењује и имплементира одабрани унапређени, тј. оптимизовани алгоритам машинског учења, у погледу детекције упада у дистрибуиран систем. Посебна пажња ставља се на процес обављених експеримената, са циљем постизања тачности резултата, постизању високе стопе заштите интегритета података.

Једанаесто поглавље састоји се од приказа и евалуације резултата експерименталног дела обрађеног скупа података. Посебан осврт је на неуравнотежености података, њихова нормализација, тј. одстрањивање нетачних података из скупова података.

Дванаесто поглавље представља анализу обављених експеримената над скуповима података, као и закључна разматрања. Дефинише се коначан исход у погледу постигнутих резултата, са посебним акцентом на то да ли су остварени резултати експеримента заиста унапредили заштиту дистрибуираних система. Исход и циљ рада представља научни допринос у погледу унапређења механизама детекције и превенције упада, а самим тим заштите од нарушавања интегритета информационих података дистрибуираних система. У наведеном поглављу даје се предлог за наставак будућа истраживања.

У тринаестом поглављу ове дисертације представља се списак целокупне литературе, научних и других извора коришћених у сврхе достизања нових научних остварења.

2. Теоријске основе

Експанзијом дигиталног доба, константним експоненцијалним растом захтева привреде за брзим и ефикасним добијањем услуга или пружањем информација, од користи је крајњим корисницима где дистрибуирани системи могу представљају значајан ослонац. Кохерентан систем који је састављен од колекције међусобно повезаних уређаја (физичких машина) представља један дистрибуиран систем. Физичке машине, које могу бити различити сервери, рачунари и друго, могу комуницирати међусобно. Оне се могу наћи на истој физичкој локацији, те се исто тако могу распоредити и на више физички међусобно повезаних (директно или посредно) локација или региона. У погледу перформанси, а тако у погледу доступности и поузданости [87], дистрибуирани системи значајно превазилазе аспекте перформанси засебног рачунарског система. Поред дељења ресурса неког система, дистрибуирани систем може делити процесорску моћ вишеструког броја радних станица (енгл. *Workstations*) путем механизама дистрибуираног рачунарства.

2.1. Карактеристике дистрибуираног система

Може се поставити основна претпоставка да се један дистрибуиран систем састоји од децентрализованих компоненти система. Такве децентрализоване компоненте представљају физичке машине (или виртуалне), те се могу дефинисати и као мрежа чворова. Распоређивање оваквих компоненти може бити геостацирано на истим, различитим физичким или на виртуалним локацијама. На дијаграмском приказу може се уочити да путем мрежне инфраструктуре уређаји могу остваривати међусобну конекцију у циљу постизања извршавања корисничких задатака. Разноврсност дистрибуираних система самим тим укључује и кључне карактеристике које они садрже. Наиме, може се истаћи неколико кључних карактеристика:

- Транспарентност,
- Хетерогеност,
- Отвореност,
- Скалабилност,
- Отпорност на грешке,
- Конкурентност,
- Ефикасност.

Транспарентност (енгл. *Transparency*) представља основну карактеристику дистрибуираног система. Представља систем у целини кориснику. Омогућава механизам где корисници могу остваривати интеракцију целокупним садржајем и свим подацима система.

Хетерогеност (енгл. *Heterogeneity*) представља карактеристику рада са разноликим хардверским и софтверским компонентама дистрибуираног система. Унутар

хетерогености система, могуће је интерпретирање различитих програмских позива како би се покренуто процесирање дистрибуираног система успешно извршило.

Отвореност (енгл. *Openness*) дистрибуираног система је од важности за његово функционисање. Наиме, тиме се постиже могућност проширења или унапређење постојећег система. Од важности је прецизно и исправно дефинисати интерфејсе, те је неопходно водити рачуна о стандардизацији интерфејса компоненти, односно, о њиховој компатибилности. Тиме се постиже једноставнија интеграција и усклађивање нових са постојећим компонентама система.

Скалабилност (енгл. *Scalability*) значајно доприноси подизању свеобухватне ефикасности система, те знатно може допринети рапидном броју корисника система. Услед остваривања комуникације међу чворовима дистрибуираног система, уколико се имплементира централизовани систем, може се изазвати уско грло, те се то може јавити као проблем централизованог система.

Отпорност на грешке (енгл. *Fault Tolerance*), као носећи ступ архитектуре дистрибуираних система може значајно допринети поузданости рада свих апликација, сервиса и других активности у оквиру самог система. Снага једног система огледа се у њеној могућности да се може носити са многобројним изазовима. Нарушавање перформанси система услед пада једног или више чворова система не сме утицати негативно. Такође, доступност података се услед сличних активности не сме десити унутар једног таквог система. Проблем се може превазићи редундантношћу, одговарајућим партиционисањем, евентуалним репликацијама система са циљем подизања отпорности на грешке. Механизам који знатно може утицати и повећати отпорност на грешке јесу обнова система и редундантност одговарајуће компоненте.

Конкурентност (енгл. *Concurrency*) дистрибуираног система представља механизам где је одговарајући систем може приступати и користити дељене ресурсе. У пракси овај принцип се може примењивати у системима и на местима где је од важности извршавање вишеструких операција истовремено. Конкурентно извршавање операција у дистрибуираном систему представља механизам који се извршава у засебним компонентама, а које се физички налазе на одвојеним физичким машинама.

Ефикасност (енгл. *Efficiency*) значајно доприноси механизму и способношћу система приликом коришћења сопствених ресурса у циљу извршења покренутих задатака. Архитектура, дизајн и оптерећење система, тако и хардверска и софтверска имплементација представљају кључан фактор ефикасности једног дистрибуираног система. Оптимизација у виду дизајнирања система може значајно смањити број корака који је потребно остварити међу компонентама једног система; тиме се може постићи свеукупно умањење потрошње енергије. Балансирање приликом постизања уравнотеженог рада у погледу оптерећења система може позитивно утицати на свеобухватну оптерећеност активних компоненти. Уравнотежен рад у значајној мери доприноси ефикасном коришћењу сопствених ресурса.

2.2. Савремени изазови у дистрибуираним системима

Комуникација између компоненти дистрибуираног система заснива се на могућој међусобној комуникацији, путем мрежних протокола. Стандардни протоколи се користе у сврхе размене порука, попут *HTTP*, *TCP/IP* и друго. Коришћењем оваквих протокола омогућава се компонентама дистрибуираног система размена (слање и примање) порука и података.

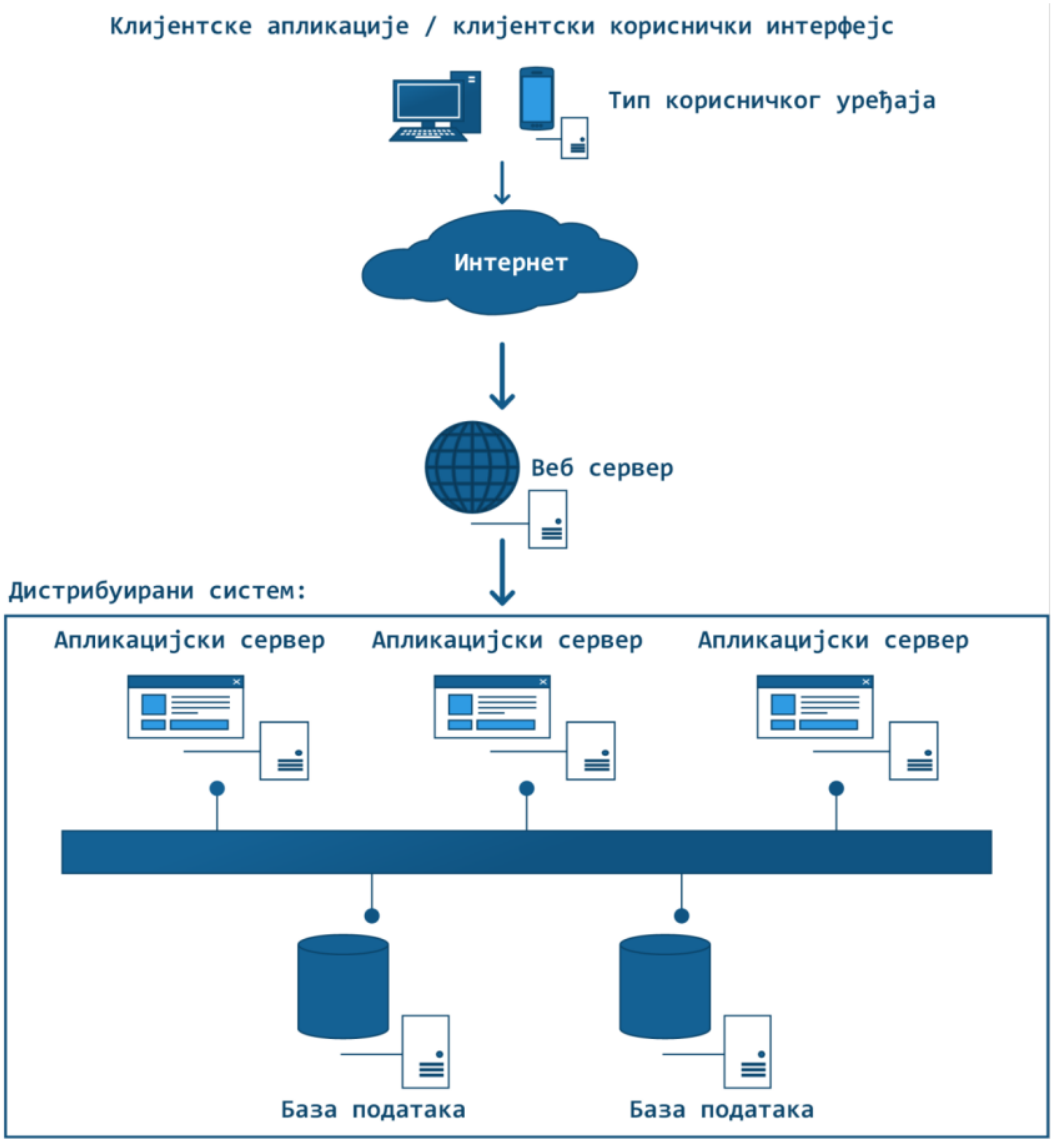
Услед повећања броја захтева према једном систему организације, уједно, измештањем једног целокупног система организације у дистрибуиран систем, једноставније се извршава хардверска надоградња целокупног система који се може налазити у функцији. Током свог рада, услед доброг дизајнирања система и упркос отказивању једног или неколико чворова система, без значајној утицаја на перформансе система, дистрибуирани систем може опслужити све захтеве, без осетног утицаја у погледу перформанси система. У супротном случају, у монолитним системима престанак рада једног (или више) чворова узрокује нарушавање, односно, пад целокупног система. Дистрибуирани системи могу прихватати велики број конекција, али свакако тај број може представљати значајно оптерећење на перформансе система у погледу испоруке података. У сврхе постизања високих перформанси у погледу испоруке услед великог броја захтева (конекција) од изузетно великог значаја може бити скалабилност дистрибуираних база података. Геолокација је важан фактор, те се дистрибуирана испорука на основу географске дистрибуције података може сматрати интуитивним за корисника, а где дистрибуирани системи могу ефикасније опслуживати у том погледу кориснике.

Као главни недостатак дистрибуираног система може се истаћи, заправо, изостанак јединственог софтверског решења које може бити универзално за различите захтеве организација. Дисбаланс у погледу сигурности и општој безбедности података, представља један од основних полазних тачака усаглашавања заштите података; услед хетерогености ових система, подаци могу *цурети* (енгл. *Leak*), те им се неовлашћено може приступати. Будући да дистрибуирани системи могу садржати изузетно обимне, сложене и комплексне базе података, а које се користе за опслуживање изузетно великог броја корисника, јављају се изазови у погледу њиховог одржавања управљања

2.2. Архитектура дистрибуираних система

Дистрибуирани системи имају неколико важних сегмената, те се посебно истичу вишеструки чворови (енгл. *Nodes*) ентитета, затим, механизми комуникационих линкова, одговарајући посредни софтвер (енгл. *Middleware*) задужен за одржавање тока и контроле комуникације између чворова дистрибуираног система; може бити од користи слоју на ком се користе софтвери ради постизања хетерогености. Чворови у дистрибуираном систему представљају мање или више сложене рачунарске ентитете. Они могу остваривати међусобну међумрежно повезивање. Посредни софтвери

смештају се као спрега између софтверских апликација дистрибуираног система и мрежене архитектуре; задужени су за координацију и управљање ресурсима, а у циљу постизања ефикасности и поузданости. Имплементација вишеструких чворова може утицати на значајно умањење или генералну отпорност у погледу грешака система, те је самим тим расположива и боља скалабилност, као и доступност мрежног ресурса. Услед упућивања захтева за извршењем задтака од стране клијента, у оваквим системима захтеви се деле на мање задатке. Путем мрежне инфраструктуре врши се њихова расподела на чворове. Приликом обављања задатака чворови међусобно могу размењивати неопходне информације у циљу завршетка задатка. Такође, уколико је задатак сложеније природе, чворови могу међусобно сарађивати у циљу постизања што оптималнијег решења. Дијаграмски приказ дистрибуираног система се може представити као на слици испод.



Слика 1 Дијаграмски приказ дистрибуираног система

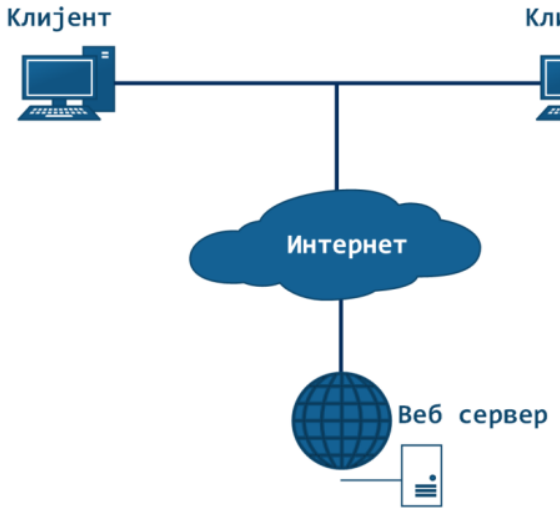
2.3. Типови архитектуре

Апликације и софтверска имплементација дистрибуираних система најчешће користи неку од стандардизованих типова архитектуре. Уједно, типови архитектуре дистрибуираних система могу бити:

- Клијент-сервер архитектура,
- Архитектура система равноправних чворова/чланова,
- Архитектура трослојног система,

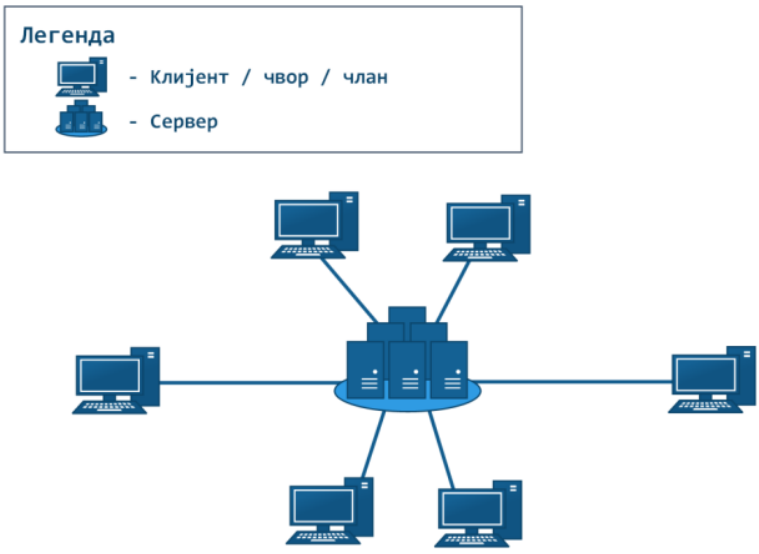
- Архитектура вишеслојног (*N*-слојног) система.

Системи клијент-сервер архитектуре (енгл. *Client*/*Server*) представљају стандардни и најосновнији тип који се може користити приликом имплементације серверских решења. Клијент упућује одговарајући захтев серверу; сервер одговара одговарајућом поруком (нпр. испоручује захтевани ресурс или га може одбити). Клијент може иницирати извршавање неког задатка на серверској страни; сервер може обрађивати захтев, те извршити одговарајуће алокације ка ресурсима и кончано га може извршити. Клијент добија одговарајући резултат у виду релевантног излаза сервера. Овакав тип система, заправо, могуће је имплементирати и у другачије архитектуре и системе.



Слика 2 Графичка илустрација клијент-сервер архитектуре

Архитектура система равноправних чворова (енгл. *Peer-to-Peer*) омогућава систему да сваки чвор засебно извршава сопствени задатак у својој интерној меморији. Путем одговарајућих линкова може прослеђивати обрађене податке. Линк или медиј за пренос података може бити било ког типа, а од важности је да за исти постоји подршка у релевантном систему. Рачунарске мреже могу користити овакав вид међумрежног повезивања, где су рачунари, тј. хостови равноправни чланови мреже и који међусобно могу остваривати комуникацију, а да при томе сваки хост за себе има сопствену и независну базу података. Оваква архитектура не садржи у себи централизован, нити монолитни систем, а ни засебан уређај који може извршавати захтевније процесе. Одлучивање, приликом доношења различитих одлука, остају на физичким машинама која су део архитектуре равноправних чворова, а где у сваком тренутку свака машина може преузети улогу или клијента или сервера.

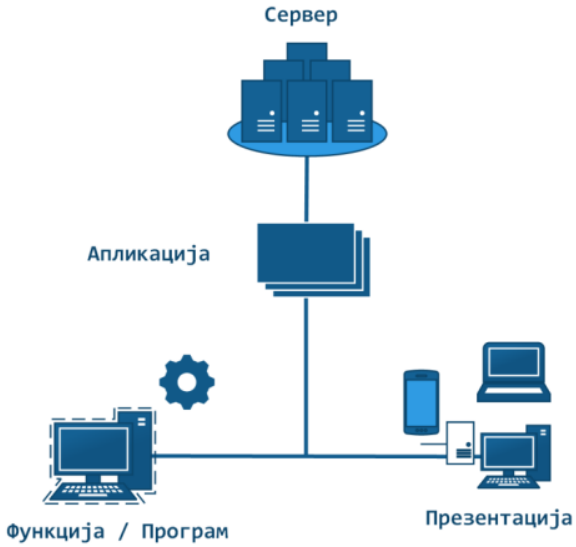


Слика 3 Графичка илустрација система равноправних чворова

Архитектура трослојног система (енгл. *Three-tier*) представља специфичну структуру где се могу користити различити слојеви за сваку функционалност (или засебну функцију) програма. Слојеви система могу бити:

- Слој апликације,
- Слој података,
- Слој презентације.

У систему трослојне архитектуре подаци клијента се чувају у оквиру средњег слоја, тј. у слоју података. Овакав механизам се данас може сусрести најчешће у савременим веб апликацијама. Клијентске апликације у трослојном систему могу се ослањати на функционалности слоја података, те он може након одговарајућих захтева обрађивати и извршавати захтеве, а на крају их прослеђивати одговарајућим серверима.



Слика 4 . Графичка илустрација система трослојне архитектуре

Вишеслојна архитектура (енгл. *N-tier*) позната под термином као вишеслојни дистрибуиран систем. Слично трослојном систему, оваква архитектура технички може у себи имати и садржати неограничене број функција. По том погледу је веома сличан трослојном систему, с разликом у примени, где се оваква архитектура чешће користи у пословним решењима организације, где је кроз веб апликације неопходно управљати подацима апликације (или софтверског решења). Услед овакве примене, сервери који се могу сматрати апликацијским и који у себи садрже имплементирану пословну логику, могу комуницирати са оба преостала слоја - са слојем података и слојем презентације.

2.4. Дистрибуирано рачунарство

Окружење дистрибуираног рачунарства (енгл. *Distributed Computing*) представља специфичну категорију дистрибуираних система. Превасходно користи механизме и ресурсе дистрибуираних система за извршавање одговарајућих задатака. Потреба за дистрибуираним рачунарством јавља се услед многобројних недостатака, некада одличних, централизованих система, попут ИБМ мејнфрејм (енгл. *IBM Mainframe*) решења. Централизовани системи су сврсисходни уколико могу обављати и радити са малом количином података и малим бројем корисника, али услед великог раста корисника на интернету, које је потребно опслужити истовремено, они постају неефикасни. Овај проблем је постао основ и оквир за прелазак у област дистрибуираног рачунарства и сличних технологија.

Током коришћења дистрибуираних система, а где може постојати мноштво различитих система, дистрибуирано рачунарство представља важну спрегу у њиховом међусобном

повезивању. Овим се постиже расподела извршавања одговарајућих делова програма покренутих у дистрибуираном рачунарству, а који се извршавају на различитим системима који су саставни део једне рачунарске мреже. Приликом повезивања аутономних уређаја преко централизоване рачунарске мреже, у циљу постизања јединственог циља, дистрибуираним рачунарством се постиже поједностављенији вид интеракције уређаја путем мреже. Самим тим, постиже се међусобно интерреаговање у погледу реализације датог проблема (задатка), али на више различитих уређаја.

У циљу постизања бољих резултата у погледу извршавања комплексних задатака, увођењем разноврсних рачунарских система постиже се већа снага. Као и код дистрибуираних система [56], дистрибуирано рачунарство суштински има иста основна својства, а која су скалабилност, отпорност на грешке, дељење ресурса и транспарентност [9]. У погледу предности коришћења дистрибуирано рачунарство се сматра високо поузданим, такође, у финансијској пројекцији овакво окружење је знатно јефтиније од централизованих система. Као савремени изазов сматра се извршавање задатака паралелно, где су задаци разврстани на засебне делове, а које је потребно извршити на различитим системима.

Дистрибуирано рачунарство је пронашло широку примену у свакодневном животу. Може се користити у различитим мобилним уређајима (системима), исто тако, може се пронаћи у апликацијама за праћење временске прогнозе, у системима електронских продавница и друго. Пример алата са доступним изворним кодом представља алат *Apache Hadoop* [10] који се користи за дистрибуирано рачунарство и обраду.

2.4. Рачунарство у облаку и у дистрибуираним системима

Претходних година (и деценија) дошло је до значајног унапређења техонологија, како самих перформанси рачунара, тако и свеукупног побољшања рачунарских мрежа. Интернет, као данашња неизоставна карика сваког пословања, доживљава свакодневни напредак, те су се уз рачунарске мреже појавиле нове могућности попут дистрибуираног рачунарства и рачунарства у облаку. Технички гледано, наведени појмови се у потпуности односе на различите субјекте, с тим да је аксиом њиховог међусобног повезивања, заправо, идентичан. Примери који најбоље илуструју коришћење рачунарства у облуку представљају услуге компанија Гугл (енгл. *Google*) и Амазона (енгл. *Amazon*) [11]. Друштвене мреже могу такође бити пример таквог коришћења, с обзиром на то да се текстуалне поруке, различити аудио-визуални садржај складиште у облаку.

У рачунарству у облаку постоје основне карактеристике који су од важности а то су [1]:

- Услуга на захтев,
- Широки мрежни приступ,
- Дељење (удруживање) ресурса,
- Брза еластичност (могућност),

- Измерена услуга.

Услуга на захтев (енгл. *On-demand self-service*) представља механизам где корисник самостално може приступати аутоматски одговарајућим услугама на серверу, без претходне потврде од стране људског фактора, а у међусобној спрези са пружаоцем услуга (енгл. *Service provider*).

Широки приступ мрежи (енгл. *Broad network access*) представља могућности које су доступне путем мреже, а које омогућавају коришћење различитих уређаја на хетерогеним системима (нпр. радне станице, лаптопови, рачунари, мобилни телефони и друго).

Дељење (удруживање) ресурса (енгл. *Resource pooling*) представља карактеристику где рачунарским ресурсима може приступати вишеструки број корисника. Ова карактеристика се огледа у могућности за складиштењем података, различитом обрадом података, коришћењем меморије и мрежног пропусног опсега. Ресурси се могу делити према геолокацији. У пракси, корисник најчешће нема сазнање о локацији датих података нити исту може контролисати. Кориснику се потенцијално може омогућити додатни вид постављања локације на вишем нивоу, те може одредити државу, покрајину, град, дата центар или неки други доступан опсег.

Брза еластичност (енгл. *Rapid elasticity*) омогућава корисницима како би се у складу са релевантном потражњом услуге брзо проширивале, односно, смањивале. Корисник у таквом окружењу може имати осећај обезбеђен неограничени број могућности у било ком тренутку потражње.

Измерена услуга (енгл. *Measured service*) представља систем у облаку где се могу аутоматизовано пратити и контролисати ресурси. Оваква услуга односи се на мерење дељених ресурса у погледу пропусног опсега, складиштења података, обрада података и друго. Концепт измерене услуге односи се на то да се свака употреба дељеног ресурса може приказивати, пратити или контролисати.

2.5. Дистрибуирани системи у пракси и њихове рањивости

CPS (енгл. *Cyber Physical System*) сајбер-физички системи представљају интеграцију рачунарских и физичких интеракција и процеса где хостови (рачунари) врше мониторинг и контролишу физичке процесе кроз петље дате повратне информације. Такви системи могу бити од значаја унутар критичних инфраструктура као што су паметне мреже, медицински уређаји и индустријска аутоматизација. Такође, подложни су разноликим врстама напада због своје комплексности и хетерогености. Ови системи омогућавају ефикасно управљање и размену података међу различитим уређајима и сервисима, али такође могу представљати значајне безбедносне изазове. Рањивости у дистрибуираним системима могу довести до озбиљних последица, укључујући губитак

осетљивих података, нарушавање приватности интегритета података и компромитовање функционисања критичних инфраструктура.

Генеративне супарничке мреже (енгл. *Generative Adversarial Network* – GAN) користе два конкурентна модела: генератор и дискриминатор [86]. Дискриминатор у генеративној супарничкој мрежи је класификатор. Генератор прави лажне податке укључујући и повратну информацију од стране дискриминатора [12]. Самим тим функционише према принципу као класификатор који покушава да разликује стварне од генерисаних података, чиме се побољшава способност обе стране кроз процесе учења.

Напад ускраћивањем услуге (енгл. *Denial-of-service - DoS*) представља напад на рачунарски систем или мрежу који може узроковати кратак или трајан прекид, а некада може произвести значајно смањење доступности сервиса свим корисницима. Такви напади могу озбиљно нарушити функционисање дистрибуираних система, ометајући нормалне операције и изазивајући бројне пословне и оперативне губитке.

Дистрибуирани *DoS* (енгл. *Distributed denial-of-service – DdoS*) напад представља сложенију варијанту *DoS* напада. У свој напад може укључивати више компромитованих уређаја. Такви уређаји су често распоређени широм глобалне рачунарске мреже, а који могу истовремено нападати исти циљ. Ови напади могу брзо преоптеретити мрежне ресурсе и сервере, а тиме постижући да услуге постану недоступни корисницима.

Напад сондирањем (енгл. *Probe Attack – PA*) представља методичко скенирање мреже са циљем идентификације рањивих тачака и прикупљања информација о мрежној инфраструктури. Овај тип напада омогућава нападачима да пронађу слабе тачке у систему које могу касније искористити за сложеније и штетније нападе.

U2R (енгл. *User to Root*) и *R2L* (енгл. *Root to Local*) напади омогућавају кориснику са ограниченим привилегијама прибављање администраторских (root) чиме нападач стиче потпуну над нападнутим хостом (или системом). *R2L* напади могу укључивати изузетно високу злоупотребу мрежних сервиса, а са циљем прибављања локалних привилегија мрежне инфраструктуре. Тиме се омогућавају наредни напади и осетљивим или затвореним деловима једног дистрибуираног система. Оба типа напада у пракси представљају значајну претњу по безбедност дистрибуираних система.

2.6. Интернет ствари у дистрибуираним системима

Интернет ствари (енгл. *Internet of Things - IoT*) укључује мрежу физичких уређаја који могу остваривати конекцију према глобалној мрежи, који могу размењивати податке међусобно, као и са централизованим (дистрибуираним) системима. Могу укључивати различита хардверска решења попут уређаја паметних кућа, затим, уређаје за различите индустријске гране, као и многе друге компоненте које омогућавају бројне аутоматизације једне организације. Такође, њиховим међусобним повезивањем

остварује се ефикасније надгледање, односно, мониторинг различитих интерреаговања међу наведеним уређајима.

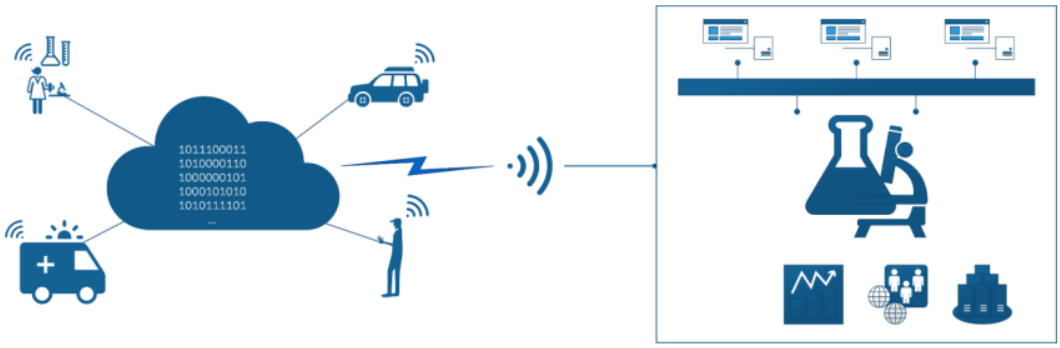
IoT уређаји се користе у различитим индустријским браншама попут здравства, паметним инфраструктурама градова, као и у бројним пословним аутоматизацијама. У здравству, на пример, IoT уређаји могу вршити удаљено надгледање пацијената, аутоматизовану комуникацију са међусобно повезаним здравственим службама, контролу медицинских препарата и лекова и друго.

Велике препреке у савременој дигиталној ери пословања *IoT* технологија представља недостатак универзалних стандарда и протокола. То може довести до значајних проблема интероперабилности између различитих уређаја, што представља директан фактор интеграције и контроле целокупних система подржаних од стране *IoT* уређаја на глобалном нивоу.

Ови уређаји су врло често мета злонамерних напада, управо због недостатка стандарда, чиме се повећава њихова рањивост. Такође, јавља се и огроман недостатак одговарајућих протокола безбедности таквих система. Стога, ови уређаји представљају потенцијалне тачке уласка за злонамерне приступе који могу компромитовати целокупне рачунарске мреже, који могу неовлашћено приступати и прикупљати осетљиве податке. Самим тим, нападачи могу изазвати прекид у функционисању критичних инфраструктура и дистрибуираних система.

2.8. Пример коришћења уређаја интернет ствари у концепту *Healthcare* 4.0

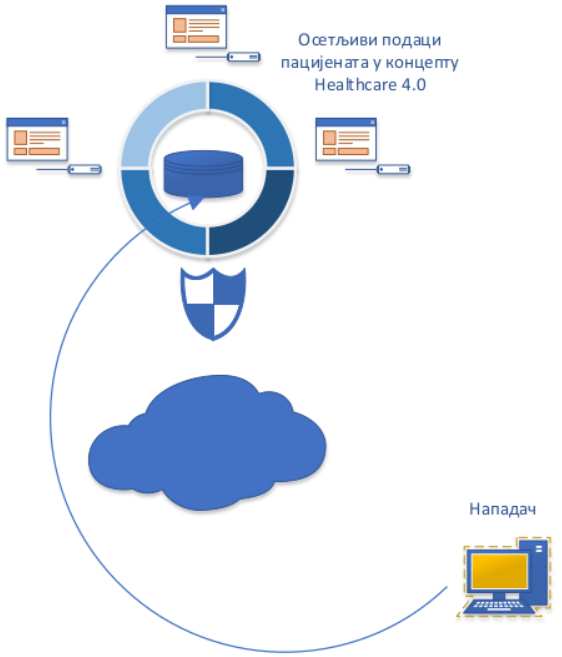
Концепт *Healthcare* 4.0 представља напредни систем бриге и неге о корисницима услуге, тј. пацијентима уз коришћење софистицираних технологија, помоћу интернет ствари. У својој основи овај концепт припада четвртој индустријској револуцији. Може имплементирати различите технологије попут вештачке интелигенције, интернет ствари, сложеније технологије за аналитику и праћење података и друго.



Слика 5 Илустрација повезивања корисника на дистрибуирани систем уз коришћење технологије Healthcare 4.0

Наведени концепт може унапредити свеукупан систем здравствене индустрије у погледу остваривања доступности, побољшања квалитета, те може омогућити бржи одзив, тј. вишу ефикасност у погледу унапређења здравственог третмана корисника услуге.

Помоћу наведеног концепта може се постићи имплементација персонализоване медицине. Такође, концепт се може имплементирати у паметне уређаје за негу пацијената, где се може извршити одговарајућа интеграција овог решења, путем којег се кориснику услуге може омогућити здравствена нега са удаљене локације. Као и у свакој технологији која је у свом технолошком напретку, током свог развоја и свакодневног унапређења концепт *Healthcare 4.0* може имати одређене проблеме. Они се огледају у погледу безбедности, сигурности и приватности података, што значајно може утицати на перформансе самог система, тј. на брзину адаптације. Наиме, примарни проблем концепта јесте заштита података корисника услуге, услед доступних података о кориснику услуге. Подаци могу бити изузетно осетљиве природе, те се исти могу односити на личне информације о различитим важним информацијама, попут генетског кода корисника, многобројни приватни подаци корисника, историјат болести корисника концепта и друго.



Слика 6 Илустрација заштите осетљивих података у Healthcare 4.0 концепту

Услед недостатака стандарда *Healthcare* 4.0 концепта могу се јавити многобројни проблеми приликом интеграције са различитим системима. Перспектива концепта огледа се у увођењу и дефинисању стандарда, те се тиме може значајно унапредити механизам размене података између уређаја различитих нивоа. Такође, значајно се може побољшати размена информација и ресурса између различитих и релевантних здравствених установа које могу пружати негу са удаљене локације.



Слика 7 Илустрација повезивања технологија интернет ствари са Healthcare 4.0 концептом

Истиче се значајан чинилац *Healthcare* 4.0 концепта, који, заправо, може емитовати и преносити информације у реалном времену (енгл. *real-time*). Тиме се остварује императив у погледу бржег и ефикаснијег реаговања ангажованог особља приликом пружања одговарајуће неге према корисницима услуге. Осим бржег реаговања може се постизати ефикаснија дијагностика корисника, тј. пацијената.

Приликом дијагностиковања стања корисника услуге, витални параметри и фактори који се могу пратити уживо, у реалном времену. Услед уочавања постојања аномалија код корисника услуге, тј. одступање од оквира који су претходно постављени, може се приступати неопходним корацима за изменом текуће терапије. Након тога, одабрани лекар и релевантно медицинско особље наједном могу извршити потребну дијагностику над новим медицинским третманом, те се могу прикупити нове анализе текуће терапије. Овај концепт омогућава високи ниво ефикасности у погледу детекције хитних интервенција код корисника услуге, као што је нпр. срчани удар корисника услуге. Релеватне установе које могу пратити здравствено стање корисника могу предузети све одговарајуће мере у погледу спасавања живота корисника са удаљене локације.



Слика 8 8 Графичка илустрација реаговања концепта Healthcare 4.0 на релевантне аларме

Концепт технологије *Healthcare* 4.0 може значајно допринети у погледу ефикасности консултовања са медицинским особљем релевантних области медицинске струке, те се могу много брже и ефикасније разменити потребне информације са релевантним медицинским установама. Таквим корацима може се повећати и побољшати ефикасност приликом доношења одлука, а добијених на основу дијагностике корисника услуге у реалном времену.

2.8.1 Рањивости концепта *Healthcare* 4.0

Горепоменута технологија има својих недостатака у виду рањивости. Услед комбиновања технологија интернет ствари са *Healthcare* 4.0 концептом могу се јавити проблеми у виду заштите, интегритета и непорецивости података. Свеопште присутна техника напада на концепт *Healthcare* 4.0 јесте напад *човек у средини* (енгл. *Man-in-the-middle*), где се могу пресретати различити осетљиви лични подаци о кориснику услуге [13].

Напад *човек у средини* представља механизам где се нападач смешта између две стране које покушавају остваривати интеракцију или приликом њихове размене релевантних података. Суштина напада се огледа у томе где обе стране могу стичу утисак да се комуникација одвија директно, те да целокупна комуникација сигурна.



Слика 9 9 Принцип напада човек у средини

Проблем неовлашћеног приступа осетљивим и личним информацијама пацијента може се јавити услед коришћења слабијих техника шифровања (енгл. *Encryption*) података. Приликом остваривања интеракције са релевантним установама, уз коришћење уређаја интернет ствари, а услед значајног недостатака механизама за детекцију злонамерних упада, може доћи до високе рањивости корисничких података.

Рањивост се може јавити у системима и рачунарским мрежама где су повезани уређаји интернет ствари, а где, заправо, може бити интегрисан концепт *Healthcare* 4.0. Наиме, напади могу уследити на целокупну мрежну инфраструктуру где нападачи могу намерно ометати или онеспособљавати (корисницима) доступне и активне сервисе, а који су од значаја за рад са корисницима услуге. Такође, овакви напади могу у потпуности зауставити нормалан и неометан ток рада, тј. могу га у потпуности онеспособити.

Након извршеног напада наведених типова, могуће је у трагу оставити и убризгати злонамеран и нежељен софтвер, са одредишним циљем ка уређајима интернет ствари. Последица може бити велика, с обзиром на то да уређаји који остварују различите интеракције са крајњим корисницима имају приступ осетљивим информацијама корисника (тј. пацијената). Самим тим, може доћи до значајног *цурења* поверљивих података, те се може нарушити интегритет.

Људски фактор може значајно допринети многобројним пропустима, поред значајне разноликости у стандардима уређаја интернет ствари, интеграција и имплементација како хардверских, тако и софтверских решења детекције (IDS) и превенције (IPS) упада у дистрибуиране системе може бити од изузетне важности. Такође, хардверска и софтверска имплементација решења заштитног зида (енгл. *Firewall*) може значајно допринети свеукупној заштити интегритета података. Интеграцијом ових решења значајно доприноси благовременом реаговању на (потенцијално) сумњиве активности у дистрибуираним системима, а која на било који начин може нарушити стабилност дистрибуираног система, а који у себи садржи концепт *Healthcare* 4.0.

Услед поменутих рањивости и потенцијалних проблема, концепту *Healthcare 4.0* потребно је унапредити механизме заштите, те се у такве сврхе, а поред наведених система за детекцију и превенцију упада (IDS/IPS), могу се користити и системи за:

- Аутоматизацију одговора на инциденте (енгл. *Automated Incident Response Systems*),
- Безбедносна анализа система (енгл. *Security Analytics Systems*),
- Идентитет и управљање приступом (енгл. *Access Management Systems – IAM*).

Поред наведених система, значајно може допринети систем за управљање рањивостима (енгл. *Vulnerability Management Systems*).

Значајна и велика подршка, а самим тим и огроман потенцијал лежи у области вештачке интелигенције, која може бити фактор решавању сложених и многобројних проблема рањивости са којом се сусреће концепт *Healthcare* 4.0 у оквиру свог окружења, тј. дистрибуираног система. Услед изузетно великог скока у области *интелигнетног учења* специфичних алгоритама, изузетно сложени и напредни алгоритми машинског учења могу бити од важности приликом прикупљања и анализирања великих скупова података. На основу добијених резултата, могу се анализирати и изводити многобројни закључци; указује се на то ко, заправо, потенцијално представља фактор претње или ко може произвести напад на дистрибуирани систем.

Вештачка интелигенција пружа огроман потенцијал приликом унапређења рањивих делова система концепту *Healthcare* 4.0. Такође, значајно може допринети отклањању претходно научених проблема. У оквиру наведене области, многобројни напредни и добро познати алгоритми машинског учења могу се користити као инструмент, тј. механизам анализирања скупова података. Услед добијених резултата, у зависности према потреби, може се довести до закључака који сегмент нежељеног мрежног саобраћаја може указивати на потенцијални напад, односно, на претњу. У свему томе, вештачка интелигенција има за циљ да потпомогне у вишем степену ефикасности приликом детекције нових надолазећих рањивости према дистрибуираном систему, где модели машинског учења на основу улаза могу да произведу нетачан излаз [88]. Тиме се ствара таква рањивост да нападач може обучити сопствени модел и извршити адверсаријалне нападе. Овакав исход се може постићи, односно, може се напад предвидети на основу претходно научених (или добро познатих) напада, тј. стања.

Приликом унапређења свеобухватне заштите дистрибуираног система, алгоритми машинског учења имају изузетну способност да помогну приликом предвиђања и предузимања значајних и корисних превентивних мера, пре него што се, заправо, деси нови инцидент у мрежној инфраструктури једне организације.

Услед функционалне аутоматизације процеса са циљем постизања високе и сложене ефикасности у погледу заштитних мера, могу се значајно унапредити и одговори на уочене, односно, детектоване инциденте у мрежној инфраструктури. Област вештачке интелигенције у значајној мери може допринети приликом препознавања шаблона

напада, како непознатих, тако и познатих, те самим тим може и одреаговати на исте. Наведена област умногоме чему рапидно доприноси наредним и сложеним механизмима шифровања, а који се могу применити на постојеће алгоритме.

Прогресивним побољшањем постојећих цифарских система квалитативно се могу унапредити механизми и сложени системи за детекцију рањивости, а уз подршку дубоког учења. Тиме се може произвести свеукупно бољи и модернији системи који имплементирају сложеније механизме шифровања података.

3. Наука и преглед литературе

Дистрибуирани системи често су изложени сложеним претњама споља услед злонамерних нападача на сервере једне организације, ради неовлашћеног прибављања и прикупљања информација или потпуног ометања функционисања доступних услуга сервера. Заштити оваквих система значајно доприносе системи за детекцију (откривање) упада, а уједно и системи за превенцију упада. Често у пракси није довољно користити основни заштитни зид (firewall) или основне уграђене механизме за детекцију и превенцију упада. Веома често је сврсисходно унапредити њихове могућности.

Аутори рада [14] установили су да је неопходност система за детекцију упада у паметне мреже електроенергетског система, потпомогнуто од стране машинског учења, од круцијалне важности за разрешавање њене мрежне рањивости. Фактори који су узети у обзир јесу примена машинског учења на системе за детекцију упада, процеси генерисања скупова података, разноликост система за детекцију упада заснованих на моделима машинског учења, различите метрике, специфичне сложености система, као и научени (тренирани) модели током свеобухватних фаза испитивања.

Резултати анализа научног истраживања [14] огледају се у томе да детекција упада у један систем може бити високо ефикасан само уколико систем ради у потпуности у складу, односно, синхронизовано и уједначено. Предмет истраживања овог рада је био CPS (енгл. *Cyber Physical System*) који, заправо, представља високо софистицирани интелигентни дигитални систем нове генерације, који се може у потпуности пратити и контролисати помоћу релевантних алгоритама. Систем омогућава потпуно праћење и контролу рачунарске мреже, те омогућава и апсолутно контролу над свим уграђеним физички процесима [15]. У резултатима рада наводи се да минимална, тј. свакојака сметња на такав систем може узроковати дисбаланс рада система и може изазивати одговарајућа оштећења. Примарни ослонац безбедности дистрибуираног система заснован је на брзом реаговању система за детекцију упада, где машинско учење својим методима процењује факторе различитих утицаја. Како паметна електроенергетска мрежа очекује ефикасан и брз одзив у решавању уочених аномалија, истраживачи су дошли до неколико важних закључака. За стабилнији и ефикаснији рад неопходни су напреднији системи за детекцију упада који се заснивају на претходно наученим аномалијама. Такође, приликом имплементације алгоритама машинског учења у такав

систем, циљ унапређења система за детекцију упада огледа се у томе да се исти систем унапреди наученим карактеристикама рањивости. Аутори наводе неопходност развоја специфичне и засебне метрике сваког паметног дистрибуираног система, ради откривања потенцијалних и стварних упада у исти. Такође, у раду се наводи неопходност испитивања у другим смеровима, како је установљено да су бежичне мреже (енгл. *WMN - Wireless Mesh Network*, *AMI - Advanced Metering Infrastructure*, *WSN - Wireless Sensor Network*) увелико инхерентне у оваквим паметним системима.

Истраживање аутора у научном раду [16] бави се сличним проблемима као и истраживања докторске дисертације. Аутори наводе да системи за детекцију упада у рачунарску мрежу и дистрибуирани систем користе шаблоне и стандардне обрасце. Нападачи, приликом потенцијалних напада покушавају прикрити своје трагове, заобилазећи стандардне обрасце. Услед тога, аутори рада истичу да је то довело до новог развоја система за детекцију упада у дистрибуирани систем, те да је као такав заснован на алгоритмима машинског учења. Аутори су развили генеративну супарничку мрежу - GAN (енгл. *Generative Adversarial Network*). Поменута мрежа представља модел машинског учења, где се две неуронске мреже такмиче једна са другом, помоћу метода дубоког учења, како би постале значајно прецизније у њиховим предвиђањима [17]. У наведеном истраживању аутори су помоћу ове мреже стварали генеративне моделе, како би потенцијално заобишли механизме за детекцију упада у дистрибуиран систем, а самим тиме и побољшали перформансе истог. Резултати истраживања доказују да приликом генерисаног мрежног саобраћаја од стране генеративне супарничке мреже може значајно допринети побољшању перформанси система детекције упада. Такође, аутори доказују у раду високу успешност у погледу избегавања детекције упада у систем помоћу исте мреже (GAN). Резултати рада [16] огледају се у имплементацији крајњег решења за генерисање супарничког мрежног саобраћаја, те и за тестирање злонамерних потенцијала помоћу исте мреже. Циљ и исход научног рада своди се на свеобухватно избегавање система за детекцију злонамерног приступа једном систему. У резултатима се наводи да су све функционалне карактеристике релевантних напада у потпуности задржане. За обучавање и генерисање модела генеративне супарничке мреже (GAN) осмишљено је више модела машинског учења, попут алгоритма случајне шуме (енгл. *RFA - Random Forest Algorithm*) и алгоритма вештачке неуронске мреже (енгл. *ANN - Artificial Neural Network*). Аутори наводе да се тиме могу добити стабилни класификатори који се користе приликом процеса обучавања алгоритма, заједно са моделима генеративних супарничких мрежа. Истраживање показује да перформансе система за детекцију упада у мрежу високо ефикасно детектују напад намерног ометања доступности (енгл. *DoS - Denial of Service*). Поред овог напада истраживачи за тестирање способности детекције упада уједно користе и нападе испитивање саобраћаја PA (енгл. *Probe attack*), *U2R* (енгл. *User to Root*) и *R2L* (енгл. *Root to Local*). Истраживачи тврде да су *DoS* и *PA* показали високу успешност у избегавању детекције упада (уз све функционалне карактеристике напада). Занимљив податак овог истраживања потврђује да се помоћу генератора компоненте архитектуре генеративне супарнике мреже (GAN) и дискриминатор заједно могу користити у циљу подизања перформанси за детекцију

упада. Прецизније, аутори указују на то да комбиновањем наведених система, потпомогнути машинским учењем, уносом излаза из генератора у дискриминатор, заправо се ефикасније се детектује злонамерно понашање у дистрибуираном систему.

Интересантан допринос и научне резултате доносе аутори у раду [18] у виду нове хибридне методе [72] за детекцију упада у рачунарску мрежу. У раду се класификује мрежни саобраћај, те се приказују у два различита стања, тј. системи за детекцију упада се помоћу алгоритама машинског учења унапређују функционалностима тако да могу да класификују да ли је мрежни саобраћај нормалан или ненормалан. Аутори су приказали нову хибридну методу којом се може детектовати упад у мрежну инфраструктуру где се обављају две фазе. Прва фаза је окарактерисана као селекција карактеристика, док је друга фаза представљена као детекција напада на мрежну инфраструктуру. Прва фаза (селекција карактеристика) користи технику обмотавања (енгл. *Wrapper technique*) која носи назив *MGA-SVM*. Као таква, ова имплементација састављена је од комбинације различитих карактеристика; једна карактеристика је метода за подршка вектору (енгл. *SVM - Support Vector Machines*), док се друга односи на методу генетског алгоритма, који има укључено вишеструко родитељско укрштање са родитељском мутацијом (енгл. *MGA - Multi-parent Mutation*). Такође, аутори су се определили да за детекцију напада, тј. упада у рачунарску мрежу користе (вештачку) неуронску мрежу. Истраживачи су подигли перформансе свом систему хибридном комбинацијом два алгоритма машинског учења. Суштински, комбинују се алгоритми гравитационог претраге (енгл. *HGS - Gravitational Search Algorithm*) и веома често коришћен - оптимизацијаројем честица (енгл. *PSO - Particle Swarm Optimization*), те је добијена хибридна метода *MGA-SVM-HGS-PSO-ANN* заснована на еволутивним алгоритмима.

Истраживање ове докторске дисертације обухвата и анализе рањивости и над уређајима интернет ствари, као део дистрибуираног система. Интересантан допринос и сврсисходан резултат доносе аутори научног рада [19] у ком се баве рањивошћу уређаја интернет ствари, као и превенцијом напада на њих. Аутори су установили да је несклад међу стандардима, као и несигуран приступ уређајима интернет ствари, заправо, круцијални проблем њихове рањивости. Наводи се у раду да је кључна компонента, технички гледано, систем за детекцију упада у дистрибуирани систем, као и за сваку *IoT* платформу. Истиче се да компонента система за детекцију упада у почетку може бити изузетно јака, али да током времена слаби и тиме постаје *слаба карика* једног дистрибуираног система. Допринос механизмима заштите овог истраживања заснива се на дубоком учењу, са циљем заштите рачунарске мреже од потенцијалног напада дистрибуираног ускраћивања услуге (енгл. *DDoS - Distributed Denial of Service*). Истраживање се заснива на превенцији напада на ободу (енгл. *Edge*) интелигентне мрежне инфраструктуре, а засновано је на принципу од тачке до тачке (енгл. *End-to-end*). Творци овог решења своје системе су постављали на различите *edge* локација, те се нису одлучили да тренирају моделе засноване на хосту. У раду се различити модели дубоког учења, заправо, користе у датом моменту случаја, односно, приликом специфичног

сценарија. Аутори су, технички, направили специфичне профиле за превенцију упада, а који су засновани на великој моћи алгоритама дубоког учења вештачких неуронских мрежа, те дуге краткорочне меморије (енгл. *Long short-term memory*) [69] [100], затим, помоћу алгоритама *GRU-D* и истог алгоритма (GRU-D) заједно са алгоритмом обичне неуронске диференцијалне једначине (енгл. *Neural ODE - Neural Ordinary Differential Equation*).

Истраживачи су тиме постигли:

- Класификацију карактеристика,
- Детекцију свих уочених аномалија у рачунарској мрежи и
- Генерисање карактеристичних и специфичних профила за детекцију упада у мрежу.

Оно што резултат чини корисним, нови предложени модел се може обучавати и у режиму *offline* на свакој *edge* локацији. Добијени резултати локалног обучавања могу унапредити и допринети ефикасности перформансама глобалног модела. Тиме су аутори развили сопствени дистрибуирани систем за детекцију упада, заједно са превенцијом упада који може извршавати задатке успешно у раним фазама напада, у реалном времену.

Наредна истраживачка студија бави се, као и њени претходници, системима за детекцију и превенцију упада у мрежне инфраструктуре које користе уређаје интернет ствари [20]. Рад се бави анализом међусобно повезаних уређаја интернет ствари, где се подаци могу размењивати и прикупљати путем различитих сензора, те је исте могуће преносити путем јавних линкова без било какве подршке од стране људског фактора. У научном истраживању се наводи да услед раста потребе за уређајима интернет ствари, јавља се све већи тренд њихове примене у паметним организацијама, кућама, зградама, улицама и друго, чинећи их напреднијим, тј. *паметнијим*. Аутори научног рада се баве многим отвореним питањима рањивости ових уређаја, а за које је од изузетне важности, како и због поузданости, усавршавање система за детекцију и превенцију упада (IDS/IPS). Истраживањем над посматраним скуповима података, аутори су обавили експерименталне анализе, те је установљено да је за сваку интеграцију интернет ствари у дистрибуирани систем неопходна строга еваулуација, са циљем подизања перформанси система за детекцију упада. Евалуација и све потребне фазе тестова над посматраним скуповима података (datasets) нопходни су да буду, како наводе аутори, стриктно везани за уређаје интернет ствари.

Аутори научно-истраживачког рада [21] дају значајан експериментални допринос приликом повезивања конволуцијске неуронске мреже (енгл. *CNN - Convolutional Neural Network*) [71][73] и прикупљања просторних карактеристика (енгл. *spatial features*). Такође, истраживачи помоћу исте конволуцијске неуронске мреже прикупљају из дугорочне и краткорочне меморије (енгл. *Long Short-Term Memory*) временске карактеристике, са циљем стварања модела хибридног система за детекцију упада у систем. Ради повећавања перформанси предложеног модела, аутори су додали моделу и

одговарајуће слојеве (енгл. *Layers*) нормализације и слојеве искључивања (енгл. *Dropout*). Модел је обучен на основу бинарне и вишекласне класификације, а коришћена су три скупа података (*CIC-IDS 2017*, *UNSW-NB15* и *WSN-DS*). Матрица конфузије (енгл. *Confusion Matrix*) у овом научном раду задужена је да одреди коначну ефикасност система.

Посматрана ограничења и критеријуми евалуације истраживача јесу:

- Тачност,
- Прецизност,
- Стопа детекције,
- Метрику за прецизност модела, тј. Ф1-резултат (енгл. *F1-score*) и
- Стопа лажних аларма (енгл. *FAR - False Alarm Rate*).

Аутори наводе да се у резултатима рада и експерименталним исходима [21] на овај начин остварује изузетно висока стопа детекција упада, висока тачност и веома ниска стопа лажних аларма. Резултати су са 5 епоха постигнути су резултати бинарне класификације од 99,64%, 94,53% и 99,67%, за посматране скупове података (редом) *CIC-IDS2017, UNSW-NB* и *WSN-DS*. Аутори истичу да за нападе црва (енгл. *Worms*) и нападе на вебу - детекције нису биле високо ефикасне за неке од посматраних скупова података. Такође, истраживачи су установили испитивањем утицаја унакрсне валидације (енгл. *K-Fold Cross Validation*) и укупним повећањем броја епоха да се превасходно перформансе побољшавају, пре него што заиста постану стабилне.

Истраживачки рад на тему модела детекције упада у систем, заснованог на конволуцијској неуронској мрежи с механизмима пажње (енгл. *Attention Mechanisms*) [22]. Рад доноси значајне резултате у погледу система за детекцију упада помоћу конволуцијских неуронских мрежа, где је кључни посматрани фактор, заправо, успостављање механизма за потпуно праћење мрежног саобраћаја једног дистрибуираног система. Акценат овог истраживања је нешто другачије природе, те у себи садржи и методе генерисања слика. Идеја лежи у томе да се побољша свеукупна рачунарска ефикасност датог модела организовањем релевантне структуре слике, где механизам пажње, заправо, утиче на свеобухватно побољшање система за детекцију упада у један систем.

У експерименталном делу аутори су се ослањали на структурну организацију слика које могу сачувати веома корисну информацију, а уз важну напомену да се исте чувају у оригиналном скупу података. Приликом обраде слика, већи број пиксела је добио вредност 0 током процеса израчунавања, што директно утиче на ефикасност обрађивања слика. Тиме се ближе појашњава већа брзина извршавања коју модели могу заиста приказати приликом процесуирања података. За предложени модел аутори наводе да ради веома добро из аспекта прецизности класификације и брзине извршавања. Тачност класификације већинског броја модела досеже вредност изнад 0,96; тиме су аутори указују да је довољна количина информација датог оригиналног скупа података заиста сачувано у сликама. Генерално, сви модели су успели да обраде више од 350 узорака по секунди, где је већи број чак премашио 500 узорака по секунди. Аутори наводе да су два модела помоћу хардверске подршке графичке картице успела да обраде 2500 узорака у секунди.

Резултати овог експеримента, како наводе аутори, огледају се у томе да су прикупљени резултати веома подесни за различите врсте модела за обраду слика, како би у наставку могли да изврше релевантне прорачуне. Евалуација метрика за предложени модел доказује да се висока тачност веома добро понаша у класификацији слика, те предложени модел ефикасно може обрадити различите узорке података, а при том, не умањујући високу тачност класификације.

Научно-истраживачки рад заснован на новом моделу дубоког учења доноси нешто другачији приступ за детекцију мрежних упада у систем [23]. Како истичу аутори, многобројни методи машинског и дубоког учења увелико су распрострањени приликом процена система за детекцију упада. Такви системи би требало да имају способности за ефикасно препознавање сајбер напада на систем рачунарске мреже (као и на хост уређаје унутар њега), те га могу и класификовати и аутоматски препознати као валидан напад. У раду се испитује интересантан сегмент где аутори указују на то да се претходна истраживања нису у великом броју фокусирала на испитивање перформанси модела над различитим јавним доступним скуповима података (datasets). Такође, аутори наводе да услед брзо променљивих техника упада у дистрибуиране системе, јавни скупови података морају бити веома често тестирани и често се ажурирати у циљу остваривања што валиднијих резултата. Истраживање наведеног рада се своди на проучавању дубоких и и конволуцијских неуронских мрежа, као врсте модела дубоког учења које се могу користити за стварање високо ефикасног, а уједно и флексибилног система за детекцију пада. Циљ таквог модела за детекцију упада јесте боље и ефикасније препознавање сајбер напада, те и њихова класификација. У раду је предложена нова двостепена техника дубоког учења, која, заправо, врши хибридизацију *дуге краткорочне меморије* (LTSM) и *аутокодовања* (енгл. *Autoencoders - AE*) за детекцију напада. Аутори су за анализу и одређивање оптималних мрежних параметара користили скупове података *CICIDS2017* и *CSE-CICDIS2018*, те из експерименталних резултата произилази *LSTM-AE* модел. Аутори овог истраживања наводе да је предложени хибридни модел применљив на реалне сценарије. Такође, предложено решење новим предложеним хибридним моделом, како аутори наводе, може се користити у другим дисциплинама, попут медицине, пољопривреде и превођења језика. Резултати у тим областима показују да је стопа губитака значајно побољшана током обуке, услед чишћења података. Аутори су приликом оцењивања перформанси предложеног хибридног модела, заправо, поредили две функције грешке - средња квадратна грешка (енгл. *MSE - Mean Squared Error*) и средња апсолутна грешка (енгл. *MAE - Mean Absolute Error*), где је период обучавања дефинисан у пет епоха. Приликом експерименталних тестова MAE функција је показала боље резултате у домену тачности перформанси предложеног модела. Аутори наводе, поред добрих резултата да није најподесније користити увек *MSE* за све моделе (или скупове података), с обзиром на његову високу осетљивост на значајна одступања, тј. на велике грешке. Систем за детекцију упада боље процењује грешку помоћу функције *MAE*. Истраживачи су за предложени хибридни модел обавили тридесет епоха, те је као такав постигао изузето високу тачност приликом детекције упада у мрежу, неовлашћеном приступању података и друго. Резултати експеримента указују на то да је предложено хибридно решење

приликом фаза детекције већег броја класа постигао детекцију од 99,99% над посматраним скупом података *CICIDS2017*. У раду се наводи да предложени модел *LSTM-AE* има изузетно светлу будућност и значајан потенцијал који може допринети различитим постојећим и алтернативним архитектурама. Експерименти су оставили будућим ауторима простор за будуће доприносе у погледу употребе, односно, комбиновања предложеног модела заједно са трансферним учењем. Такође, предлажу да се изврше нови тестови над новијим скуповима података у области сигурности рачунарских мрежа, где се свакодневно појављују нови типови и механизми високотехнолошких напада, а са циљем експерименталног тестирања детекције злонамерних активности помоћу предложеног модела.

4. Дистрибуирани системи и машинско учење

Услед неопходности (уједно и услед све веће потражње) високо софистицираних метода система за детекцију безбедносних проблема и рањивости, доприноси овог рада заснивају се и огледају на предлозима нових решења, приликом детекције упада и одбрамбених механизама у робусним системима.

Дистрибуирани системи представљају колекцију независних рачунарских хост машина (рачунара) међусобно повезаних, који заједничким деловањем у мрежи постижу заједнички циљ. Такви системи могу омогућавати свеукупно повећање ефикасности, поузданости и скалабилности, а самим тим могу на сврсисходан начин обрађивати скупове података. Машинско учење у оквиру дистрибуираних система може играти улогу приликом обраде масивних количина података [61], уједно може помоћи приликом аутоматизације сложених задатака, као што су детекција и превенција упада у дистрибуирани систем од свих безбедносних претњи по исти.

Дистрибуирани системи могу имати неколико типова, као што су хетерогени системи, системи засновани на кластерима, као и варијанта система базирана на микросервисима. Хетерогени системи могу укључивати различите типове уређаја, више различитих међусобно повезаних рачунарских мрежа. Системи засновани на кластеру обично садрже скуп међусобно повезаних рачунара који могу радити, заправо, као један систем. Системи засновани на микросервисима могу користити независне компоненте које могу међусобно комуницирати помоћу предефинисаних интерфејса.

Један од највећих изазова дистрибуираних система савремене дигиталне ере јесте очување интегритета података, а који се могу компромитовати приликом њиховог преноса кроз мрежу. Дистрибуирани системи често су подложни рањивостима и нападима који нарушавају стабилност система (нападима *DoS* и *DDoS*).

Напредне технике машинског учења могу значајно допринети свеукупној безбедности и ефикасности дистрибуираних система. Самим тим, указује се на потребу за увођењем и применом хибридних алгоритама и неуронских мрежа. Такви алгоритми се могу

користити како би се установила и омогућила ефикаснија детекција упада у систем. Такође, може постићи и боље предвиђање безбедносних изазова и претњи по један дистрибуиран систем. Стога, бројна унапређења оптимизацијом алгоритама машинског учења и интеграцијом са постојећим системима могу унапредити целокупну скалабилност и поузданост дистрибуираних система, што може представљати фактор њихове примене у критичним окружењима попут здравства.

4.1. Изазови дистрибуираних система, проблеми и циљеви истраживања

У овој докторској дисертацији истражују се различити концепти, где се и дају предлози модификоване метахеуристике, која је развијена за потребе истраживања [24] где се акценат ставља на свеукупно побољшање безбедности уређаја интернет ствари. Такође, поред тога истражују се и дају се нове стратегије које могу допринети заштитним системима и одбрамбеним механизмима од високо-технолошких напада на мрежну инфраструктуру. Такође, акценат се ставља и на одбрамбене механизме физичких уређаја интернет ствари међусобно повезаних са удаљеним дистрибуираним системом. У датим истраживањима, са циљем достизања високих тачности метода користе се различити типови података, тј. реални и симулирани. Таквим приступом може се постићи прецизнија и ефикаснија процена примене развијеног решења у реалном окружењу.

Услед многобројних рањивости, проблема у конфигурацији у разноликим системима интернет ствари, а приде се могу појавити и грешке. Услед таквог сценарија користе се напредни алгоритми који значајно доприносе унапређењу и који могу допринети свеукупном побољшању након што се обави евалуација процене безбедносних рањивости у реалном окружењу, приликом интеракције са корисницима.

У фокус великих дистрибуираних система у будућности може бити императив у постизању баланса између високих перформанси и безбедносних механизама, а услед све већег броја коришћења уређаја интернет ствари, где је примаран проблем неусаглашеност стандарда. Многобројни дистрибуирани системи имају значајних потешкоћа приликом опслуживања значајног броја различитих доступних сервиса, попут разноликости података, власништво и обим података, те потенцијалне претње и друго [24]. Свеукупним побољшањем и подршком алгоритмима машинског учења, безбедност дистрибуираних система и безбедносни модели заједно представљају потенцијал за будућност. Услед високог протока информација кроз различите физичке уређаје, посебан приоритет се ставља на:

- Интегритет података,
- Тајност података,
- Аутентикацију корисника и
- Гарантованих овлашћења корисницима.

Услед горе наведених проблема, тј. рањивости, а на основу веома велике разноврсности физичких уређаја интернет ствари, популарна техника за пресретање информација између крајњег корисника и дистрибуираног система јесте *човек у средини*. Подаци се могу тим нападом пресретати [13], те се као такви могу злоупотребити са циљем прибављања осетљивих и личних информација крајњих корисника услуга. Једно од истраживања овог рада представља испитивање безбедносних механизама у концепту *Healthcare* 4.0, где се могу пресретати високо осетљиви подаци о пацијенту (као што је историја болести пацијента) који је активан корисник ове услуге, тј. концепта. Такође, до цурења података може доћи и приликом размене информација, тј. размене података између пацијента (као корисника уређаја интернет ствари) и одговарајућих установа путем комуникационих линкова [13].

Организације које користе у својим дистрибуираним системима овакве технологије у свом рачунарству *у облаку,* често су изложени нападима [83] на мрежну инфраструктуру. Такође, нападач може намерно ометати комуникационе линкове, активне сервисе и услуге, те за последицу напада један систем може имати потпуно обустављање, тј. прекид сервиса на нивоу њихове доступности, а самим тим и последицу нарушеног интегритета.

4.2. Рањивости инфраструктуре дистрибуираних система

Рањивост инфраструктуре дистрибуираних система лежи у њиховој комплексности и великом броју компоненти које могу бити мета напада. Овакви системи често обрађују значајне количине података у реалном времену, што их чини подложним различитим безбедносним претњама и изазовима. Напади на дистрибуиране системе могу угрозити интегритет, поверљивост и доступност података, што може довести до значајних губитака и прекида у функционисању услуга. У концепту *Healthcare 4.0*, интеграција *IoT* уређаја повећава ризик од напада, с обзиром на то да сваки уређај може представљати потенцијалну тачку уласка за нападаче, услед неусаглашености у стандардима. Стога је важно примењивати напредне технике детекције упада и оптимизоване моделе машинског учења како би се побољшала безбедност и отпорност ових система.

5. Машинско учење и алгоритми неуронских мрежа

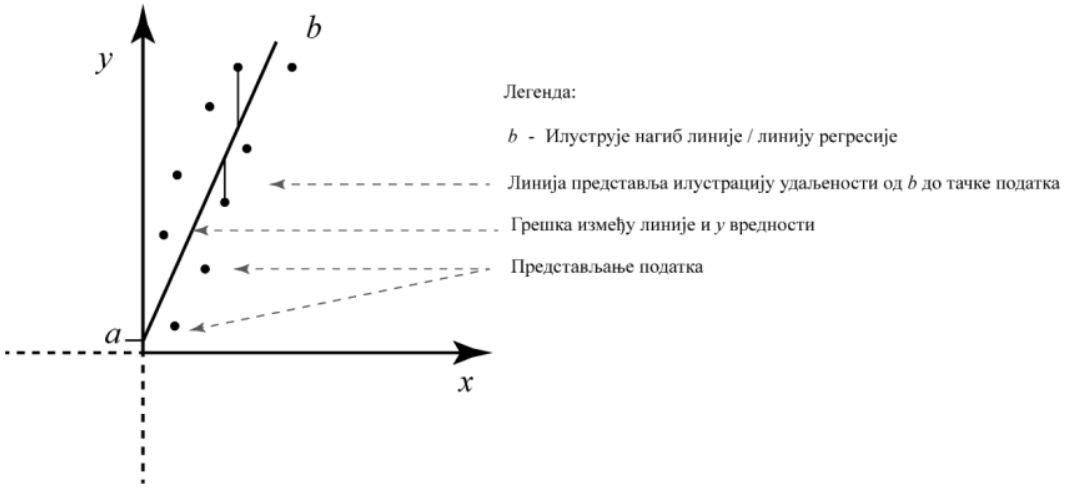
Комбиновањем две снажне и савремене гране, где друга својим математичким моделима и опонашањем природних стања потпомаже прву, заједно могу значајно могу допринети проналажењу и предвиђању догађаја. Задаци који се могу поставити испред њих заснивају се на концепту учења на основу предочених података, те се (потенцијално) из тога може донети одлука - нова, оптималнија, бржа и унапређена. Машинско учење у својој имплементацији може користити различите сложене напредне и хибридне алгоритме; примери могу бити класификатори, регресија [85], неуронске мреже,

градијентско спуштање или појачавање и многе друге. Тиме се може постићи ново моделовање шаблона понашања над подацима.

Линеарна регресија у машинском учењу може имати скуп променљивих. Оне се означавају словом □. На основу улазних променљивих може се одредити излазна променљива □. Квантификовање јесте циљ машинског учења, те се улазне и излазне променљиве могу довести у везу.
Наведена веза [25] између улазних и излазних променљивих у линеарној регресији [26][27] може се изразити помоћу једначине [28]:

$$\square = \square + \square\square ,$$

где □ и □ представљају вредности коефицијената које је потребно пронаћи.



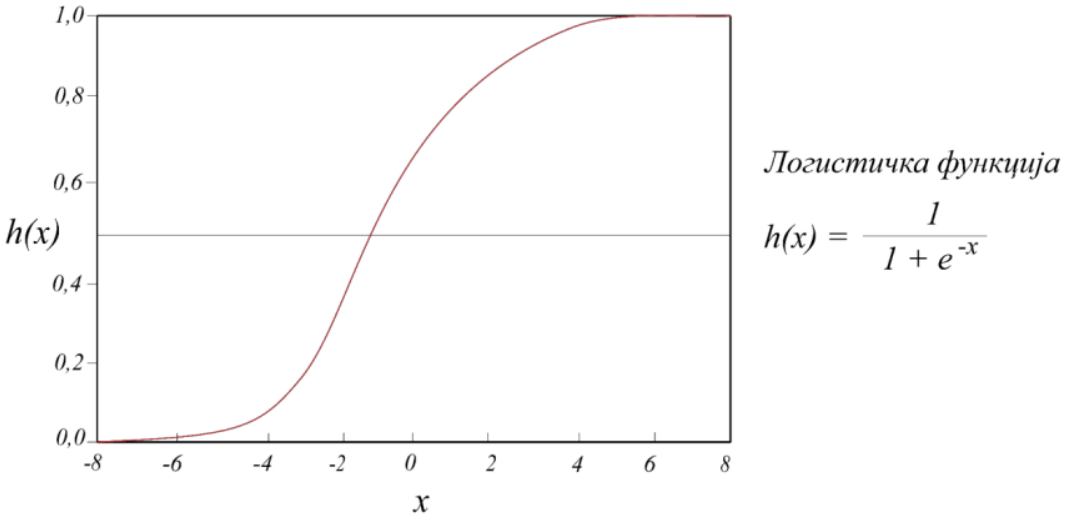
Слика 10 Илустрација линеарне регресије представљена линијом нагиба

Логистичка регресија у машинском учењу може се ослањати на прогнозе линеарне регресије које се огледају у специфичним континуираним вредностима. Поред прогнозе линеарне, која за свој резултат има континуиране вредности, очекивани исход логистичке регресије јесу дискретне вредности. Оне се могу приказати и добити тек након што се примене трансформационе функције. Идеална је за коришћење бинарне класификације, тј. за скупове података (datasets) где се □ = *0* или □ = *1*. Уколико је вредност 1, у том случају она се односи на подразумевану класу у посматраном догађају предвиђања. Случај се може довести у везу са концептом *Healthcare* 4.0 путем ког се може пратити стање пацијента, где постоје, заправо, две могућности. Прва могућност је да је пацијент у добром здравственом стању (вредност 0), док се друга вредност може повезати са неким догађајем (вредност се поставља на 1), те се предвиђање стања пацијента може означавати у посматраном скупу података са вредношћу 1. Из претходно

наведеног, логистичка регресија, која настаје услед трансформационе функције, носи назив *логистичка функција* [29]:

$$h(\square) = 1/(1 + e^{\wedge} - \square).$$

Функција дефинише сигмоидну криву (тј. *S* криву).



Слика 11 Илустрација логистичке регресије и формиране сигмоидне криве

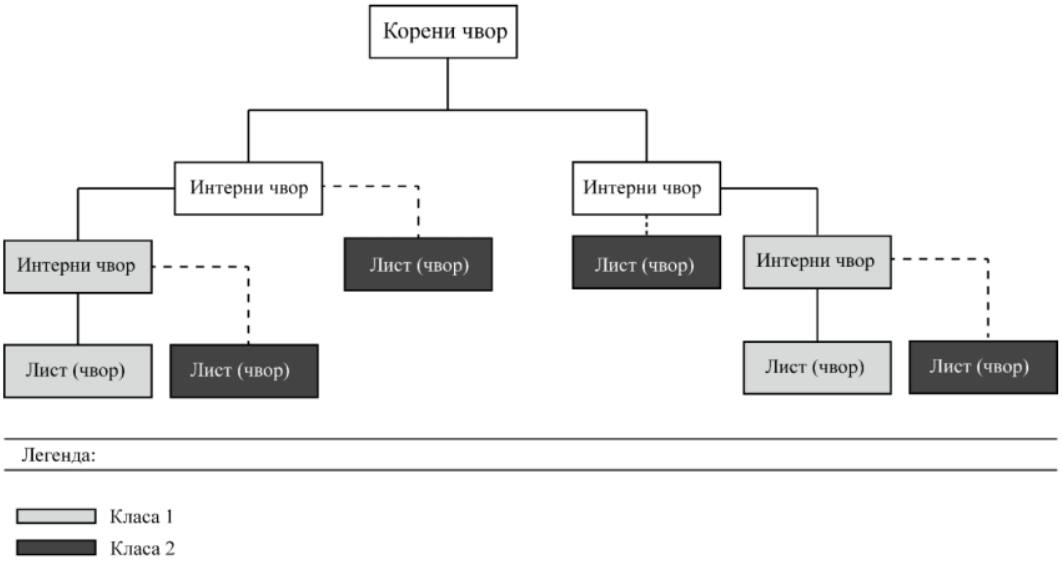
Резултат логистичке регресије огледа се у формату вероватноће претходно дефинисане подразумеване класе. Разлика између логистичке и линеарне регресије управо лежи у излазу функције, где наспрот овој, у линеарној регресији резултат (излаз) јесте директан исход функције. С обзиром на то да резултат може бити у распону (опсегу) од 0 до 1, вероватноћа исхода се може пронаћи само између наведених посматраних вредности. Тако се, на пример, може надовезати претходно наведени пример концепта *Healthcare* 4.0. Наиме, уколико резултат вероватноће (тј. оцене) износи 0,97, алгоритам може за свој исход приказати да је пацијент врло вероватно у лошијем здравственом стању.

Стога, вредност □ може се генерисати логаритмовањем □ вредности, помоћу горе наведене формуле логистичке функције. Потом се примењује праг из ког се може форсирати добијена вредност вероватноће у релевантну бинарну класификацију.

Класификациона регресиона стабла (енгл. *Classification and Regression Trees - CART*) може се представити као једна имплементација одлуке дрвећа (енгл. *Decision Trees*) [30], те се може користити у сврхе предвиђања догађаја. Корени и унутрашњи чворови јесу нетермални чворови како класификационих, тако и регресионих стабала. Стога, терминални чворови се представљају као листови. Тако се може дефинисати структура

да (сваки) нетерминални чвор може представљати појединачну улазну променљиву (означава се са □), а уједно може представљати и тачку раздвајања на датој променљивој. Самим тим, листови могу представљати променљиву излаза (означава се са □). Логика модела може се огледати у поступку предвиђања:

1. Пролази се кроз сва раздвајања стабла (са циљем досега до листова),
2. Исписује се вредност датог листа



Слика 12 Илустрација класификационог регресионог стабла

Наивни Бајесов класификатор (енгл. *Naïve Bayes*) имплементира и користи Бајесову теорему приликом прорачуна вероватноће да ће се један догађај догодити, уз претходни услов да се претходно десио један догађај. У настав се, приликом прорачуна, користе:

- Тачна вероватноћа хипотезе, дефинише се као h,
- Претходно знање (о догађају) , дефинише се као □.

6. Проблеми оптимизације алгоритама машинског учења

Како је машинско учење неопходно у савременој ери обучавања модерних алгоритама машинског учења, истраживачи се сусрећу са многобројним потешкоћама приликом имплементације оваквих сложених алгоритама.

Током испитивања скупа података може се десити *проблем препроучавања* (енгл. *Overfitting*). Алгоритам може развити специфичан модел који је исувише усклађен са посматраним скупом података, те исход може произвести лош капацитет података, тј. прегенерисане податке. Такво понашање огледа се у резултату где током обучавања података добијају тачни подаци, а изостају резултати за нове податке.

Поред прегенерисаних података, може се десити, а услед једноставности предложеног модела, заправо, проблем недовољног учења (енгл. *Underfitting*). Исход оваквих проблема огледа се у томе да обучени модел није у могућности да јасно дефинише и одреди спрегу између дефинисаних улазних и посматраних излазних променљивих. Епилог таквог сценарија може се огледати у генерисању великог броја грешака.

Алгоритми се значајно могу унапредити оптимизацијом хиперпараметара, што представља уједно и сржистраживања у докторској дисертацији. Такође, од велике је важности одабир исправних хиперпараметара. На коначни исход предложеног решења, односно, на предложени модел значајно може утицати и одабир хиперпараметара. Неадекватан избор хиперпараметара, заправо, може генерисати и производити лошије, односно, слабије резултате од очекиваних.

Функције алгоритама машинског учења суштински би требало да представљају баланс и конзистентност система [89]. С тим у вези, коришћење неподударајућих функција усмерености (енгл. *Mismatched Objective Function*) често доводи до резултата који нису очекивани (и уједно могу бити лошији, тј. слабијих од очекиваних). Такође, услед несклада могу се произвести и генерализована решења, што свакако не представља позитиван исход.

Током обрађивања посматраних података, може се јавити несклад резултата, те се такав исход огледа над квалитетом предложеног модела. Узрок томе може бити у неправилном претпроцесуирању података. Проблем се може јавити услед исувише великог броја уметних података, нетачно или неодговарајуће праћење модела, уклањање неодговарајућег шума и слично.

Посебан осврт се може указати на недовољно великој количини скупа података (енгл. *Small Training Set*). Како је претходно дефинисан *проблем препроучавања*, а приликом коришћења слабијег скупа података, може се десити да модел може веома лако запамтити целокупан скуп података (током своје обуке), те самим тим може доћи до претходно дефинисаног проблема.

Услед значајно велике разлике у погледу броја података међу класама које се посматрају над датим моделом, може се десити несиметричност података (енгл. *Imbalanced Data*). У таквом сценарију проблем се огледа у томе да модел може извршити бољу класификацију ону класу која је, заправо, већа. Несиметрични подаци се могу наћи у типовима скупова података где посматрана класа добија дисбалансирану, тј. неравномерну дистрибуцију опажања. Технички посматрано, ознака једне класе има изузетно висок степен броја опажања, док друга има изузетно низак број.

Комбиновањем машинског и дубоког учења за циљ има постизање бољих резултата у сваком сегменту обучавања алгоритама, њихове оптимизације, као и постизања бољих резултата у сваком сегменту податка. Чести проблеми који се могу сусрети приликом

дубоког учења јесте, заправо, предугачко дубоко претренирање (енгл. *Deep Learning Pitfalls*), где предугачак ток и процес обуке може представљати велики проблем.

6.1. Примена алгоритама машинског учења у експерименталним окружењима

Како се алгоритми машинског учења могу интегрисати у сваку пословну логику савременог друштва, оно, заправо, има оквир и след ствари који се може у основи применити на такву интеграцију. Наиме, у експерименталним окружењима машинско учење значајно може допринети предвиђању резултата обављеног експеримента. Новодобијени резултати се могу добити само уколико постоје постојећи подаци различитих активности у окружењу. Приликом обављања и вршења експеримената алгоритми машинског учења могу значајно допринети оптимизацији експеримента, односно, његовом структурном дизајнирању. У контексту наведеног, исход може дати претпоставке или оквир у погледу оптималних предлога за минимизацију или пак за максимизацију релевантног исхода. Класификација података важан је поступак за одговарајућу идентификацију различитости или сличности, а заснованим на карактеритикама посматраног догађаја. Из наведеног, може се извести аутоматизовано учење на основу спроведених експеримената, те се претходно стечено знање (прикупљене информације) могу открити различитости. Тако, на пример, у случају где је потребно побољшати оптимизацију једног дистрибуираног система, односно, његових делова уопште, на основу претходно обављених експеримената могу се открити законитости добијених променљивих вредности приликом обављања сложених математичких операција.

6.2. Алгоритми машинског учења

Алгоритми машинског учења представљају претпоставку и саставну компоненту савремених дистрибуираних система. С обзиром на њихове способности, ови алгоритми способни су за извршавање комплексних задатака. То може укључивати и оперативност над системима који повезују уређаје интернет ствари (IoT), омогућавајући тиме сложену аналитику и аутоматизацију комплексних задатака које они могу обављати. Алгоритми могу користити различите механизме приступа, као што су надгледано, ненадгледано и појачано учење, са циљем моделовања и предвиђања стања дистрибуираног система. Надгледано учење може укључивати коришћење означених података за обучавање модела. Ненадгледано учење способно је да ради са неозначеним подацима, са циљем откривања скривених структура. Појачано учење омогућава учење остварујући интеракцију са окружењем [82].

Неуронске мреже, а самим тим укључујући дубоке неуронске мреже (DNN), конволуцијске неуронске мреже (CNN) и рекурентне неуронске мреже (RNN), од значаја су приликом решавања бројних проблема машинског учења, омогућавајући да заштите

рачунарске ресурсе од спољних напада [91][93]. Поменуте дисциплине, поред побољшавања тачности и ефикасност система, могу допринети збирном побољшању свеукупне безбедности и робусности дистрибуираних система.

6.3. Алгоритам *XGBoost*

Многобројни алгоритми машинског учења у себи садрже специфичне савремене методе које се могу имплементирати, односно, путем којих се може постићи оптималнији резултат над тренираним моделом. Самим тим, наведени алгоритам има сопствене специфичне параметре који се могу оптимизовати у зависности од специфичних случајева.

Овакви алгоритми заснивају се на поставци и претпоставци датог проблема који је потребно разрешити. Такође, модерним методама којима се могу оптимизовати и прилагођавати параметри посматраног модела, резултат се може огледати у сложеној и прецизној контроли приликом процеса машинског учења, као и над обрадом скупова података. Самим тим, свака карактеристика модела се подешава и оптимизује засебно, те се за посердну и непосредну последицу резултат осликава у виду разноликости оптимизације у *XGBoost* алгоритму.

Добијање кохерентности међу различитим факторима представља срж овог алгоритма. Посматрани различити фактори јесу [24]:

- Прецизност,
- Брзина и
- Генерализација модела.

Како би се остварили бољи резултату, а самим тим се постижу реалистичнији и адекватнији резултати, може се спроводити специфичан итеративни процес у ком се параметри алгоритма итеративно подешавају. Циљ таквог подешавања јесте боља евалуација података, који се могу поредити са својим претходним стањима, тј. обављеним претходним анализама.

Подударност између *XGBoost* алгоритма и концепта *Healthcare* 4.0 може се илустровати као процес прикупљања, анализе и предвиђања догађаја. Резултат ове корелације може се осликати у виду побољшања механизама одлучивања у процесима које користи *Healthcare 4.0* концепт.

7. Дубоко учење

Представља грану машинског учења која се примарно ослања на неуронске мреже [97] [98] са више слојева (дубоким неуронским мрежама), а са циљем анализе и интерпретације комплексних података [96]. Омогућава изузетно високе перформансе у различитим имплементацијама као што су препознавање говора, обрада података, као и

детекција безбедносних претњи у *IoT* системима. Формуле које се користе у дубоком учењу углавном обухватају различите функције активације, функције губитака (енгл. *Loss functions*) и алгоритама оптимизације. С обзиром на то да се неуронске мреже састоје од вишеструких слојева, како би се остварио резултат врши се трансформација података; у ове сврхе користе се улазни, скривени и излазни слојеви. Они обављају процес трансформације података. Формула која ближе описује овај ток гласи:

$$y = f(W_3 \cdot f(W_2 \cdot f(W_1 \cdot x + b_1) + b_2) + b_3)$$, где је

- *W* - тежине,
- *b* бајас, а
- *f* функција активације.

7.1. Дубоке неуронске мреже

Дубоке неуронске мреже (енгл. *Deep Neural Network - DNN*) састоје се од више скривених слојева између улазног и излазног слоја. Ови модели су способни да науче сложене функције и обрасце у подацима захваљујући својој дубокој архитектури. Основна формула [31] која описује *DNN* укључује:

$$[y = f(W_n \cdot f(W_{n-1} \cdot \dots f(W_1 \cdot x + b_1) \dots + b_{n-1}) + b_n)]$$, где је

- x – представља улазни вектор (енгл. *input vector*) у мрежу. Наведени параметар представља податке који се уносе у неуронску мрежу за даљу обраду истих.
- W_i- Тежинска матрица (енгл. *Weight matrix*) за дати слој i. Задужене су за одређивање снаге између посматраних неурона у слоју $i-1$ и неурона у слоју i, дате везе.
- b_i: Пристрасност (енгл. *Bias*) за слој i. Користи се као додатни параметар моделу омогућавајући бољу и оптималнију прилагодљивост.
- *f*: Активациона функција (енгл. *Activation function*). Представља нелинеарну функцију која се може применити на излаз сваког посматраног слоја. Након његове примене моделу се тиме омогућава уење сложених образаца.
- *y*: Излазни вектор (енгл. *Output vector*) мреже представља предвиђање или класификацију коју мрежа може давати услед улазних података у исту.

7.2. Конволуцијске неуронске мреже

Конволуцијске неуронске мреже (енгл. *Convolutional neural network - CNN*) представљају посебан процес које имају намену обраде података [75] [101] са мрежном структуром. Сложена структуре мреже може бити слика. Основни елемент *CNN* је конволуцијски слој који може примењивати филтере над улазним подацима како би исход резултовао

карактеристикама. Општа формула [31] за конволуцијски слој може бити представљена као:

$$y_{i,j} = \sum_{m,n} x_{i+m,j+n} \cdot w_{m,n} + b, \text{ где}$$

- x представља улазне податке,
- w представља филтере и
- b бајас.

7.3. Вештачке неуронске мреже - *ANN*

Вештачке неуронске мреже (енгл. *Artificial Neural Network ANN*) представљају како општи, тако и основни тип неуронских мрежа које се могу састојати од више слојева и то: улазног, једног или више скривених и излазног слоја. У пракси користе функције активације услед генерисања и моделовања сложених образаца; те се може користити и за анализу сирових пиксела [76], односно, сложених задатака. Општа формула [31] за један неурон у вештачкој неуронској мрежи гласи:

$$y = f(W \cdot x + b), \text{где су}$$

- W представља тежине,
- x представа улазне податке,
- b представља бајас и
- f представља функцију активације.

Аутоенкодери (енгл. *Autoencoders AE*) представљају врсту неуронских вештачких мрежа *ANN* која има способност да научи ефикасно представљање података. У пракси се често може користити за проналажење и откривање аномалија, као и за димензионо смањење.

8. Метахеуристике – поступци високог нивоа

Представља и обухвата процес високог нивоа рачунарске оптимизације алгоритама, које имају за циљ да унапреде и побољшају резултат алгоритма, тј. да покушају да пронађу најбоље могуће решење проблема дате оптимизације. Метахеуристике користе специфичне класе које у себи садрже механизме за проналажење оптималних решења логичког проблема.



Слика 13 Класификација метахеуристичких алгоритама [32]

Заснивају се на природним процесима и појавама, који у својој основи могу бити представљени корз природне феномене. Познати метахеуристички алгоритми могу се представити као:

- Генетски алгоритми,
- Алгоритми роjева,
- Роjеви пчела,
- и други.

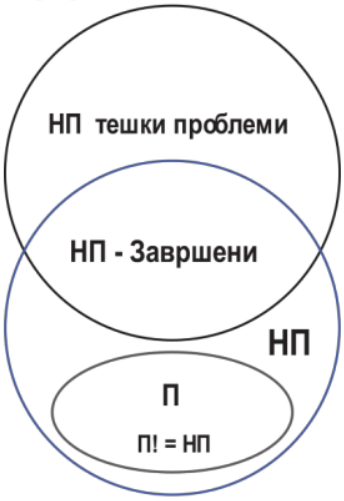
Област теорије комплексности је од великог значаја за рад са метахеуристикама. Оне (метахеуристике) као такве подесне су решавање комплексних и компликованих проблема. Време проналаска решења може се дефинисати полиномијалним временом, према теорији комплексности; оно се односи на укупно време прерачунавања датог проблема. Услед оваквог приступа, полиномијални временски алгоритми могу се представити изузетно ефикасним. Наиме, у таквом поступку време не може бити више полиномијалне функције величине проблема [33]. Формула се може представити у математичкој нотацији великог *O*:

$$O(m(n)) = O(n^k), \text{ где}$$

m(n) - представља време израчунавања датог логичког/алгоритамског проблема,
n - представља полиномилајлну функцију величине посматраног проблема,
k - представља константу која може бити у директној зависности са датим проблемом.

С тим у вези, метахеуристике могу значајно допринети решавању НП-тешких проблема [13]. Подесне су за њихово решавање у прихватљивом и разумном временском

интервалу. За НП-тешки проблеми (недетерминистички у полиномијалном времену) представљају проблем који може бити решен у полиномијалном времену и ако и само ако постоји НП-комплетан проблем [34]. Метахеуристике са својим могућностима не могу сигурно обезбедити успех решавања датих проблема, али могу представити и пружити боље или довољно добро решење.



Слика 14 Графичка илустрација НП-тешких проблема

Из претходног се може закључити да не постоји јединствен, као ни изузетно ефикасан алгоритам који има способност решавања свих проблема. Као подршка и превазилажењу проблема може се увести *NFL* (енгл. *No Free Lunch*) теорема, где се дефинише правило такво да уколико су, заправо, функције оптимизације једнако вероватне, самим тим су и сви алгоритми оптимизације једнако ефикасни, односно, неефикасни [35].

Комбиновањем наведеног доказује се теорема да унапређењем или потенцијалним побољшањем алгоритма за разрешавање датог проблема, из тога произилази (врло вероватно) погоршан исход приликом решавања неког другог проблема. Самим тим, може се извести јединствен закључак да метахеуристике немају могућност проналаска јединственог решења за сваки проблем; оне омогућавају да се итеративним процесима постигну и остваре задовољавајућа или прихватљива решења у разумном временском периоду. Обједињавањем са *NFL* теоремом остварује се, заправо, позитиван компромис током процеса тражења што оптималнијег решења. У овом случају евалуације је од високе важности број извршених експеримената са циљем добијања задовољавајућих (или прихватљивих) исхода решења.

8.1. Механизми заштите ИДС ИПС

Механизми заштите у дистрибуираним системима за детекцију упада (IDS) [62] и системима за превенцију упада (IPS), у савременој ери могу играти кључну улогу

приликом интеграције и имплементације безбедносних механизама унутар дистрибуираних система, а самим тим и *IoT* уређаја. Системи за детекцију упада могу надгледати мрежне активности, анализирајући мрежни саобраћај са циљем откривања потенцијалних претњи и евентуалних напада. С друге стране, системи за превенцију упада делују проактивно, блокирајући сумњиве активности, а све то у реалном времену. Напредни алгоритми машинског учења омогућавају наведеним механизмима да идентификују савремене сложене, укључујући и нове претње, а које је систем научио на основу претходно стечених догађаја. Имплементацијом ових решења, користе се технике као што су класификација, кластеровање и дубоко учење [63][64].

У овом раду комбинује се *XGBoost* алгоритам, оптимизован модификованим алгоритмом свитаца (XG-MFA), показује високу ефикасност приликом детекције безбедносних и сигурносних проблема приликом коришћења *IoT* уређаја у дистрибуираним системима. Анализа *SHAP* коришћена је за сврсисходније разумевање утицаја различитих карактеристика над донесеним одлукама модела, што омогућава побољшање тачности и поузданости *IDS* и *IPS* система. Овакав приступ збирно унапређује детекцију и превенцију упада и доприноси унапређењу целокупне безбедносне архитектуре дистрибуираних система.

8.2. Постизање перформанси, прецизности и тачности применом имплементираних алгоритама

На основу свеобухватне анализе и свих спроведених експеримената, у овој докторској дисертацији, а на основу објављеног научног истраживања [13] предлаже се употреба хибридног алгоритма *XG-MFA* за унапређење постојећих оквира за детекцију упада у дистрибуиране системе. Овај алгоритам, који комбинује *XGBoost* са модификованим алгоритмом светлосних мушица, показао је изузетну прецизност и робусност у различитим сценаријима класификације.

Са просечном тачношћу од 99.99% у задацима вишекласне класификације, *XG-MFA* је показао способност да прецизно детектује сложене безбедносне претње у *IoT* уређајима у здравственом сектору. Додатно, употреба *SHAP* анализе омогућава дубље и поузданије разумевање додатних фактора који могу допринети претњама, што омогућава знатно бољу превенцију и дизајн сигурнијих и безбеднијих дистрибуираних система.

У поређењу са другим методама, *XG-MFA* је постигао најбоље резултате у готово свим кључним метрикама; највиши резултат није постигао само приликом одзива, а где је постигнуто изузетно високо друго место. Ови резултати могу указивати на то да је *XG-MFA* не само прецизан, већ доследан и моћан у својим перформансама. Применом овог алгоритма у постојеће оквире за детекцију упада у дистрибуиране системе могу се значајно повећати ефикасност и сигурност система. Стога, препоручује се интеграција *XG-MFA* у постојеће инфраструктуре за побољшање безбедности и смањење ризика од

упада у исте. Овај приступ може омогућити боље управљање и заштиту података у реалном времену, чиме се доприноси општој безбедности дистрибуираних система.

9. Предложени експериментални алгоритам

Представља се предложени експериментални алгоритам, на основу научно-истраживачког рада [13], који је развијен да анализира безбедносне претње у дистрибуираним системима кроз употребу *IoT* уређаја у здравству. За потребе експеримента, користи се *XG-MFA* - хибридни алгоритам *XGBoost*-а и модификованог алгоритма свитаца (енгл. *Frefly algorithm*), као основни метод за детекцију упада. Експериментални поступак обухвата анализу и представљање скупа података, поставку серверске инфраструктуре, коришћење специфичних протокола који се користе за симулације и понављање експеримената, као и детаљну поставку експеримента.

Скуп података је генерисан помоћу *IoT-Flock* алата [36], који симулира здравствене сценарије са нормалним и малициозним уређајима. Два најзначајнија скупа података, *CICIDS2017* и *CSE-CICIDS2018*, користе се за тренирање и тестирање модела. Сваки скуп података садржи детаљне информације о мрежном саобраћају и идентификационим параметрима који су битни за откривање безбедносних претњи.

Поставку експеримента чине дистрибуирани сервери на којима су постављени *MQTT* брокери и *COAP* сервери, који симулирају реалне услове рада *IoT* уређаја. Током експеримента, ови сервери обрађују и анализирају податке у реалном времену, омогућавајући алгоритму да идентификује и класификује различите типове напада. Основни протоколи који се користе за комуникацију су *MQTT* (енгл. *Message Queuing Telemetry Transport*) и COAP (енгл. *Constrained Application Protocol*), који, технички гледано, омогућавају размену података између међусобно повезаних уређаја.

Експериментална поставка обухвата неколико корака:

- иницијалну припрему података,
- тренирање модела,
- тестирање и
- евалуацију резултата.

За сваку фазу спроведена је детаљна анализа како би се осигурала висока тачност и поузданост резултата. Посебан осврт посвећен је оптимизацији хиперпараметара, како би се постигле што више и боље перформансе модела.

Резултати експеримента су оцењени, односно, евалуирани помоћу стандардних метрика као што су прецизност, одзив, Ф1-резултат и Коенов коефицијент капе (енгл. *Cohen's kappa coefficient*). Резултати се, затим, пореде са другим најчешће коришћеним техникама машинског учења, а са циљем потврде ефикасности предложеног алгоритма. Предложени експериментални алгоритам пружа свеобухватно унапређење

безбедносних оквира у здравственим системима који користе технологију *IoT*, чиме се може допринозити бољој заштити података и сигурности дистрибуираног система.

10. Експериментални скуп података

Током истраживачког поступка, а на основу прикупљених научних резултата, за референти оквир одређен је скуп података за анализу сигурности уређаја у здравству [37] заснованих на принципима *IoT*. Важно је поменути податак да у време писања ове докторске дисертације не постоји много алата који пружају или имају могућност симулација напада на један дистрибуирани систем, у оваквом оквиру и окружењу.

Примарно, овај експериментални поступак као исход има поновно креирање експеримента заснованог на резултатима научног резултата [36], а са циљем постизања полазне тачке за ново идентификовање, односно, поновно упоређивање. Скуп података који садржи нормалан и малициозан саобраћај може се пронаћи на следећој локацији: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset. Саобраћај је заснован према принципу - два медицинска кревета која имају подршку у виду девет уређаја за праћење пацијента. Сви уређаји су базирани на технологији интернет ствари. Подршку уређајима пружа један контролни уређај који носи назив *Bedx-Control-Unit*, где су сви претходно поменути симулациони уређаји креирани помоћу алата под називом *IoT-Flock* [37]. Како би истраживачи [36] постигли тестни догађај, помоћу отвореног флексибилног алата *IoT-Flock* за генерисање симулација, креирано је окружење нормалних и злонамерних уређаја, коме су дефинисане ИП адресе. Тиме се постиже да симулирани саобраћај може остваривати константну међумрежну комуникацију са *IDS* и *IPS* [74] системима дистрибуираног система, а самим тим може се анализирати саобраћај који може бити од изузетног значаја за побољшање превенције и детекције упада у мрежу. Важно је истаћи да су доступна два протокола апликације која се могу користити за генерисање порука и то:

- *MQTT - Message Queuing Telemetry Transport,*
- *COAP - Constrained Application Protocol*.

MQTT представља посредни сервер путем ког је могуће обавити комуникацију између крајњих уређаја који користе *Message Queuing Telemetry Transport* протокол.

За наведени посредни сервер у званичној терминологији се често може сусрести и термин и *MQTT* брокер. Принцип рада *MQTT* брокера је једноставан; прихвата поруке од стране клијентских *IoT* уређаја који користе наведени протокол, а потом их може прослеђивати другим уређајима *IoT* према којима је усмерена порука или сет инструкција, а који имају *претплату* (енгл. *Subscribe*) за праћење одговарајуће теме, тј. комуникационог линка. Подразумевано је да *IoT* уређаји на другој страни користе идентичан протокол за међумрежну комуникацију.

COAP представља специфичан протокол чија је оптимизација прилагођена само уређајима интернет ствари који имају ограничене ресурсе. Под ограничењем ресурса првенствено се мисли на уређаје са сензорима, затим, различите варијанте актуатора и друго. Његова предност огледа се у томе што се примарно користи у комуникационим мрежама где је мноштво међусобно повезаних уређаја. Ефикасан је и изузетно једноставан за имплементацију у једном дистрибуираном систему. Омогућава поуздан и непоуздан пренос података, односно, *TCP* и *UDP* протокол. Има могућност читања, писања и брисања ресурса на уређајима који имају подршку за коришћење овог протокола.

За потребе прибављања информација о самом уређају, *MQTT* протокол је сврсисходан; може прикупити многобројне информације попут ИП адресе, затим корисничког имена и лозинке, различите индикаторе који могу указивати на различите корисничке активности. Други протокол који се може користити, тј. *COAP* експлицитно може захтевати ИП адресу удаљеног сервера, а за његово функционисање овај протокол прослеђује своје тзв. *COAP* команде. Апликација има графички кориснички интерфејс, као и конзолни режим, а омогућавајући тиме приказ резултата у *XML* формату.

Како су аутори истраживачког рада [37] обавили симулацију два медицинска кревета у интензивној нези (ICU). Симулација обухвата, технички гледано, девет сензора и контролном јединицом; означава се са *Bedx-Control-Unit*, где *x* представља број јединице, односно, медицинског кревета. Јединица (*x*) задужена је за конфигурисање времена профила корисника, како би се подесили одговарајући и релевантни временски интервали, затим, садржи у себи симулацију пумпе за дозирање инфузије пацијента, као и симулацију алармног система задуженог за хитна јављања у случају да пацијент не обавља интеракцију са сензорима. Такође, у датом скупу података налази се додатна функционалност у виду одговарајуће јединице за контролу окружења. Овим се постиже контрола симулације експеримента у виду влажности и температуре или потенцијалног дима који се, услед различитих непредвиђених догађаја, може испуштати у просторији. На све ове непредвиђене појаве може реаговати алармна јединица. Такође, оно што је су аутори истраживачког рада укључили то су, заправо, карактеристике које имају профил времена и профил прикупљених података. Механизам имплементације профила података у директној је корелацији са релевантном спецификацијом одговарајућег сензора, а самим тим генерише се резултат у таквом формату. Насупрот томе, профил времена може бити од користи датој симулацији у погледу дефиниције одговарајућег интервала у ком се може обављати размена података између посматраног сензора и контролне јединице.

Резултат у виду генерисања података у симулираној интензивној нези резултује у виду две у потпуности одвојене мреже. Прва генерисана мрежа приказује резултате одговарајуће јединице симулације интензивне неге. Друга генерисана мрежа представља мрежу нападача на исту. Одредишна мрежа састављена је од *MQTT* уређаја који могу

преносити и примати податке од *MQTT* брокера. Више о целокупном скупу података може се видети у референцираном раду [36].

У датом експерименталном поступку *IoT-Flock* генерише се по један виртуални мрежни интерфејс на физичком рачунару. Оперативни систем заснован је на Линукс дистрибуцији. Брокер *MQTT* и *COAP* сервер измештени су на други физички рачунар. Из аспекта испитивања безбедности, рачунарска мрежа нападача садржи у себи десет уређаја који могу изводити четири типа напада и то:

- *MQTT* дистрибуирани *DoS* напад,
- *MQTT* преплављивање (енгл. *publish flood*),
- *Brute force* напад и
- *SlowITE* [38].

Над скупом података примењује се алгоритам за регресију и класификацију са к-најближих суседа, односно, KNN - *K-Nearest-Neighbors* алгортиам [79]. Алгоритам функционише према принципу одређивања класе за све њему непознате инстанце. Одређују се на основу ознака к-најближих суседа. Над скупом података K је постављен на 5, односно, $\square = 5$, где оригинални скуп података садржи укупно 50 дефинисаних карактеристика. Одабир карактеристика је сужен на укупан број 10, ради постизања перфроманси, чиме се уједно постиже максимизација помоћу релевантних предложених метода. Карактеристике су одбаране на бази референцираног рада [36] чиме се додатно поткрепљује ова тврдња. Десет карактеристика је одабрано и то [13]:

- *frame.time_delta*,
- *tcp.time_delta*,
- *tcp.flags.ack*,
- *tcp.flags.push*,
- *tcp.flags.reset*,
- *mqtt.hdrflags*,
- *mqtt.msgtype*,
- *mqtt.qos*,
- *mqtt.retain* и као последња
- *mqtt.ver*.

Приликом анализе мрежног саобраћаја и одговарајућих порука користе се претходно дефинисане карактеристике; опис карактеристика и атрибута дат је у наставку:

- *frame.time_delta*: Измерено време између два узастопна мрежна оквира у датом мрежном саобраћају.
- *tcp.time_delta*: Измерено време између два узастопна мрежна *TCP* пакета у датом мрежном саобраћају.
- *tcp.flags.ack*: Бит који се указује на потврду; *TCP flag* представља ACK бит, а тиме се указује на потврду пријема посматраног сегмента.
- *tcp.flags.push*: Контролна заставица служи као индикатор да је неопходно примаоцу што пре испоручити податак.

- *tcp.flags.reset*: *TCP* контролна заставица захтева прекид текуће *TCP* сесије.
- *mqtt.hdrflags*: Контролна заставица заглавља (енгл. *Header*) у *MQTT* протоколу прецизније одређује информације о специфичности поруке и евентуалном квалитету.
- *mqtt.msgtype*: Представља поруку за *MQTT* протокол.
- *mqtt.qos*: *MQTT* карактеристика представља квалитет услуге (енгл. *Quality of Service*); може се користити да одреди ниво поузданости приликом преноса одговарајуће поруке.
- *mqtt.retain*: Контролна заставица *retain MQTT* протокола указује да ли је посматрана (обична) порука задржана (енгл. Retain) на одговарајућем серверу, тј. постављена на *true*. или је потребно упутити новим клијентима, односно, претплатницима или онда када се претплате на исту.
- *mqtt.ver*: Карактеристика *MQTT* протокола указује на статус верзије која се користи приликом комуникације у мрежи.

Услед коришћења контролне заставице *mqtt.hdrflags* и формата истог, запис се представља у хексадецималном формату. Вредности се, најпре, морају претворити у децимални облик, како би релевантна метода машинског учења била способна да обради ту информацију, тј. податак. Поредбени рад [36], као ослонац овом експерименталном истраживању, у својим поступцима користи искључиво бинарну класификацију над два типа података. Први тип податка илуструје се као у потпуности регуларна међумрежна комуникација (без нападача); представљен је класом нула. Други тип представља напад, а представља се класом један.

У овом научном истраживању проширују се експерименти у односу на претходно посматрану студију [36], која представља ослонац за будућа истраживања. Извршени су и спроведени експерименти у виду три класе [13]:

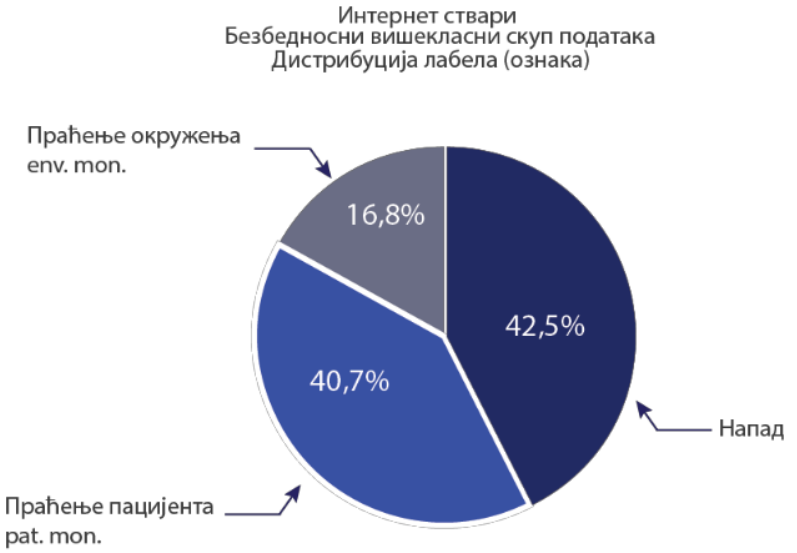
- Класа 0 - Нема напада; врши се мониторинг окружења,
- Класа 1 - Нема напада; врши се мониторинг пацијента и
- Класа 2 - Напад.

Наредна слика приказује дијаграм бинарне класификације, где је 57.5% података означено као позитивно, док 42.5% података чини негативну класу. Дати графикон илуструје расподелу података међу две класе у бинарном експерименту детекције.



Слика 15 Графичка илустрација бинарног скупа података за дистрибуцију ознака [13]

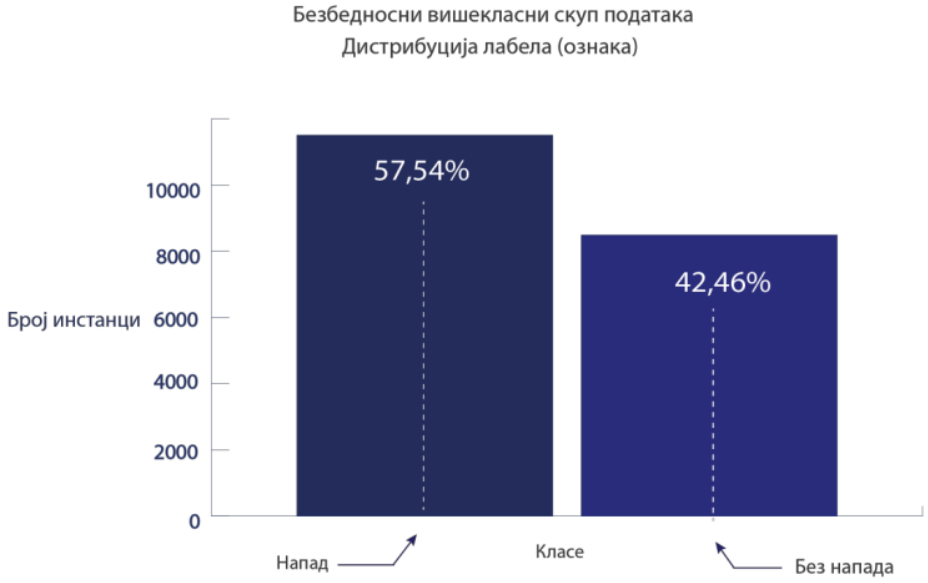
Графикон кругова представља вишекласну класификацију, где 42.5% података припада првој класи, 40.7% другој класи, а 16.8% трећој класи. Графика помаже у једноставнијем разумевању пропорција различитих класа у вишекласном експерименту у домену *Healthcare 4.0*.



Слика 16 Графичка илустрација вишекласних безбедносних скупа података [13]

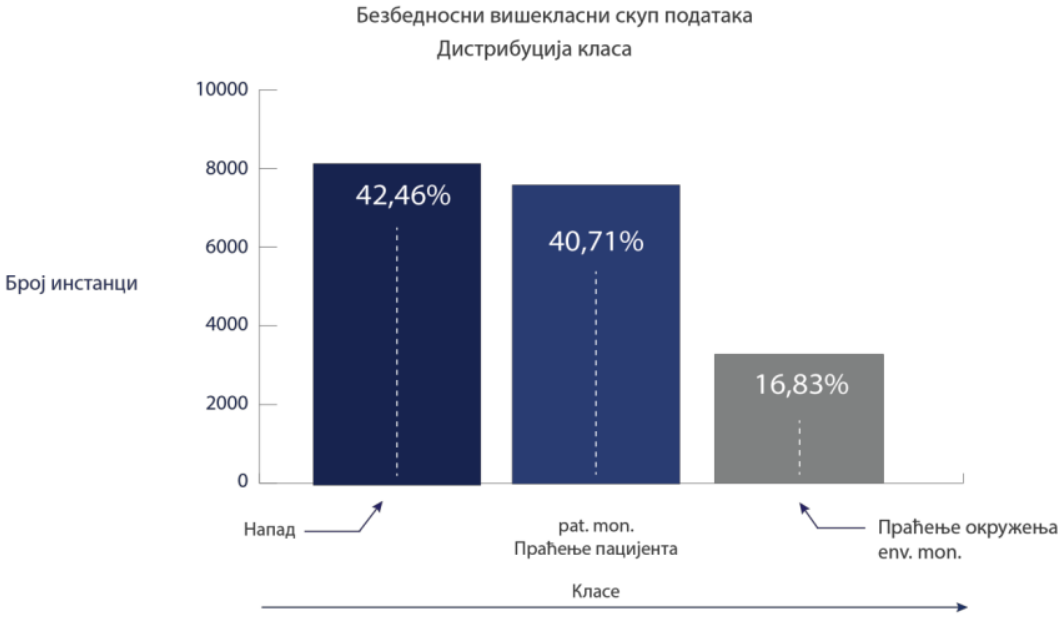
У наставку се може видети графикон који приказује расподелу података у бинарној класификацији. Приказано је да 57.54% података припада позитивној класи, док 42.46%

припада негативној класи. Дати визуелни приказ једноставније приказује расподеле података између две класе.



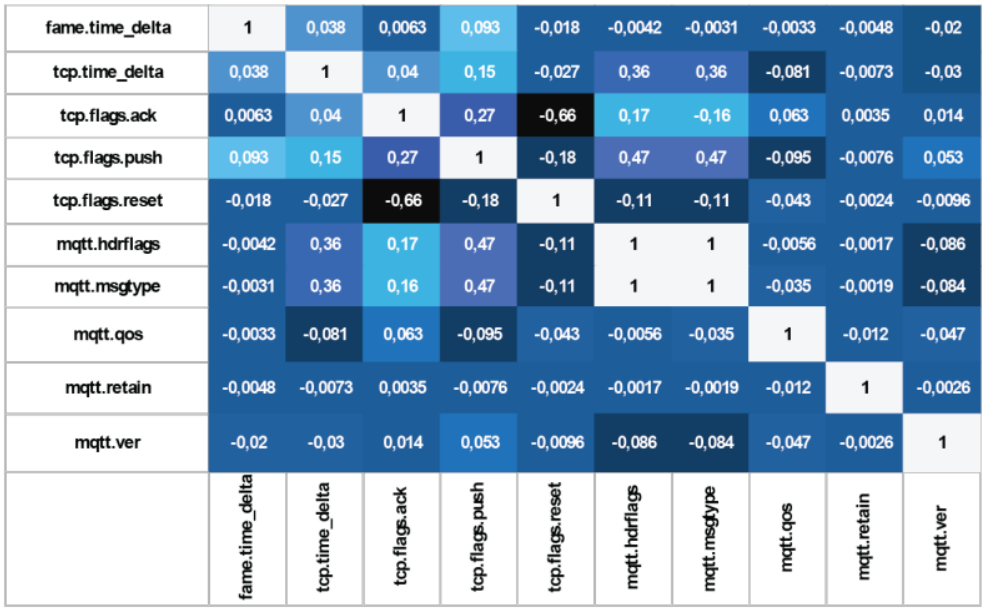
Слика 17 Графичка илустрација безбедносног бинарног скупа података [13]

Слично претходним, наредни графикон илуструје вишекласну класификацију. Графикон приказује информације тако да 42.46% података припада првој класи, 40.71% другој класи, а 16.83% трећој класи. На овај начин може се видети једноставнија расподеле података међу различитим класама над безбедносним вишекласним скупом података за уређаје интернет ствари.



Слика 18 Графичка илустрација дистрибуција класа [13]

Топлотна мапа (енгл. *Heatmap*) приказује корелацију између различитих карактеристика у купу података. Представљене вредности означене су различитим бојама, које омогућавају брзо идентификовање снажних и слабих корелација између карактеристика. Анализа поједностављује разумевање остварених интеракција и потенцијалних утицаја различитих карактеристика на модел у контексту *Healthcare 4.0*.



Слика 19 Графичка илустрација корелација карактеристика приказано кроз топлотну мапу [13]

10.1. Поставка експеримента и очекивани исходи

Како би се постигао виши степен оптимизације хиперпараметара алгоритма *XGBoost*, иста се у експерименталном окружењу спровела помоћу предложеног алгоритма MFA (енгл. *Modified Firefly Algorithm*) [13]. Коришћен је *Intensive Care Unit - ICU* скуп података (dataset) за потребе експерименталног поступка. У научно-истраживачком експерименту извршена је оптимизација хипер параметара; у наставку се може видети њихова оптимизација са својим границама и типовима промењљивих:

- *learning rate* (□), границе претраге: [0,1, 0,9], континуална промењљива,
- □□□_□*h*□□□_□□□□*h*□, границе претраге: [1, 10], континуална промењљива,
- *subsample*, границе претраге: [0,01, 1], континуална промењљива,
- *collsample_bytree*, границе претраге: [0,01, 1], континуална промењљива,
- *max_depth*, границе претраге: [3, 10], целобројна (енгл. *Integer*) промењљива,
- □□□□□, границе претраге: [0, 0,8], континуална промењљива вредност.

Одређене границе у овом експерименту добијене су емпиријски. Коришћени су методи покушаја (енгл. *Trial*) и методи грешке (енгл. *Error method*). За потребе овог експеримента на који се ослања докторска дисертација, предложена метода је извршена помоћу програмског језика Пајтон (енгл. *Python*). Такође, важно је истаћи у овом научном истраживању да су коришћене следеће (стандардне) библиотеке за потребе добијања граница [13]:

- *scipy* - библиотека за нумеричку обраду података, уједно и за статистику, математичке операције (линеарну алгебру, диференцијалне једначине), процесуирање сигнала и друго.
- *numpy* - библиотека за рад са вишедимензионим низовима или матрицама.
- *pandas* - библиотека за манипулацију над подацима, као и за анализу структуираних података, са посебним акцентом на рад са табеларним подацима.

Како би се добио одговарајући резултат, за потребе генерисања модела коришћена је Пајтон библиотека *scikit-learn* [39]. Библиотека је отвореног кода која омогућава многобројне операције машинског учења, а са циљем добијања модела алгоритма *XGBoost*.

У наставку се може видети технички приказ и вредности које се користе приликом оптимизације:

- *I* - користи се како би се дефинисала дужина низа; дужина низа представља кодовано решење,
- *I* - дужина низа носи вредност 6.

Над подацима скупа података није извршена нормализација; извршена је насумична расподела скупа података. Приликом обучавања коришћено је 70% података, док је за потребе тестирања коришћено 30% података [13].

Циљ овог научно-истраживачког рада [13], на који се ослања и сама докторска теза, јесте постизање оптимизације перформанси хибридног *XGBoost MFA* алгоритма. Оптимизација перформанси обавља се поредбеном методом са другим оптимизатора којих је у овом случају укупно 8. Оптимизатори представљају алгоритам или методи који могу пратити и проналазити оптималне вредности релевантних и посматраних параметара датог модела или одговарајућег алгоритма машинског учења. За циљ имају логичке операције попут максимизације или минимизације посматране функције; у том контексту, функције могу бити нпр. функције грешке, затим, функција потрошње електричне енергије и свака друга која може технички мерити квалитет датог решења. У поменутом експерименту, поред 8 посматраних оптимизатора укључен је и оригинални *FA* алгоритам у оквиру истог проблема. Такође, важно је истаћи да су у овом делу експеримента укључени наредни алгоритми за поређење [13]:

- *FA* [40],
- *GA* - Генетски алгоритам [41] [42],
- *PSO* [43],
- Алгоритам вештачког роја пчела (ABC) [44],
- Алгоритам оптимизације шимпанзи (ChOA) [45],
- COLSHADE - Алгоритам диференцијалне еволуције са смањењем величине популације и ограниченим летовима [46],
- SASS - Самоподешаајућа сферна претрага [47].

Над сваким алгоритмом извршен је истоветан тест са сваким индивидуалним претходно наведеним алгоритмом. У питању је исти тест са препорученим вредностима за контролне параметре. Тестови су обављени индивидуално и независно су једни од других тестирани. Такође, идентична поставка експерименталног поступка је обављена за тестирана решења и то са популацијом од 10 решења са преко 10 итерација по покретању теста, са укупно 30 извршавања [13].

10.2. Метрика перформанси експерименталног решења

За потребе научног истраживања на који се примарно ослања истраживање ове докторске дисертације [13], извршена је идентична евалуација као у раду [36]. Наведени поредбени рад је одредио и досегао чврсте темеље у својим резултатима у погледу валидности резултата. Посматрано је неколико параметара:

- Тачност,
- Прецизност,
- Одзив и
- *Ф1*-резултат.

Ф1-резултат представља меру тачности и дефинише се као:

$$Ф1 - \text{резултат} = 2 \cdot \frac{тачност \cdot одзив}{прецизност + одзив}, \text{ где}$$

- Прецизност - дефинише се као вероватноћа тачне класификације позитивне класе,
- Одзив - дефинише вероватноћу свих стварних позитивних случајева.

Овим се може представити хармонијска средина, која представља реципрочну вредност аритметичке средине одговарајућих реципрочних вредности датог скупа, између прецизности (енгл. *Precision*) и одзива (енгл. *Recall*). Помоћу наведене мере тачности ближе се може процењивати перформанса класификационих модела, са посебним освртом на неуравнотеженост међу класа у посматраним подацима.

Резултати посматраних параметара може се извести из матрица забуне (често називана и *матрица конфузије*), која представља снажан алат за анализу у виду предвиђања, тј. предиктивну анализу. Извршава се према шаблону тако што се оригинална табела резултата пореди са добијеним резултатом предвиђаног модела. За циљ има да генерише јаснију слику о томе како се посматрани модел заиста понашао. Самим тим, сви резултати изведени су од сваког поредбеног решења помоћу матрице конфузије. Тачност може бити варијабилна, што технички гледано значи да може бити променљива од случаја до случаја. Променљивост се може јављати услед небалансираног скупа података. Наредне ознаке се користе у стандардној терминологији измерених вредности:

- *TP* - користи се вредност *true positive* за права и лажна предвиђања,

- *FP* - користи се вредност *false positive* за позитивна предвиђања,
- *FN* - користи се вредност *false negative* за негативна предвиђања,
- *TN* - користи се вредност *true negative* такође за негативна предвиђања.

Однос тачног предвиђања у односу на пропуштена предвиђања може се дефинисати као тачност (енгл. *Accurracy*) Циљ оваквог прорачуна огледа се у томе да је неопходно да се утврди колика је, заправо, тачност предвиђања у односу са пропуштеним предвиђањима. Тиме се омогућава, технички гледано, процена тачности модела. Следи формула тачности [49]:

$$Тачност = \frac{\square\square + \square\square}{\square\square + \square\square + \square\square + \square\square}$$

У наставку се дефинише прецизност; суштински се пореде тачна предвиђања у односу на све предвиђане случајеве. Такође, израчунава се прецизност која се може дефинисати као однос тачних предвиђања и укупног броја позитивних предвиђених случајева. Тиме се може постићи процена тачности предвиђања, а за циљ има прорачун поузданости модела приликом идентификације жељених инстанци истог. У наставку се може видети формула [49]:

$$Прецизност = \frac{\square\square}{\square\square + \square\square}$$

У наставку следи формула помоћу које је могуће израчунати успешност колико, заправо, модел може идентификовати све стварне случајеве. Израчунава се као однос тачних предвиђања и позитивних случајева; дефинише се као одзив (енгл. *Recall*) [49]:

$$Одзив = \frac{\square\square}{\square\square + \square\square}$$

У наставку се дефинише формула која одређује *Ф1-резултат*. Одзив (енгл. *Recall*) и прецизност (енгл. *Accuracy*) се комбинују у циљу добијања резултата [49]:

$$\square 1 - резултат = \frac{(2 \cdot прецизност \cdot \text{одзив})}{(прецизност + \text{одзив})}$$

Током процеса истраживања одабрани су различити методи за мерење скупова класификација. Уз помоћ поредбених радова [50] одабрана је метода Коеновог коефицијента капе. Она, у математичком смислу, представља статистичку меру сагласности квантификације између два посматрана скупа класификација у датом примеру. У случају субјективних одлука и номиналних категорија, тј. тамо где не постоји природан редослед, овај метод може бити од значаја. Она се дефинише као:

$$= \frac{(\quad - \quad)}{(1 - \quad)}, \text{ где}$$

- po - представља проценат стварне сагласности,

- pe - представља проценат случајне сагласности.

Математички гледано, вероватноћа догађаја услед неког конкретног фактора који се може поредити са истим догађајем без конкретног фактора представља однос вероватноћа [50]:

$$\frac{(\frac{\square\square}{\square\square})}{(\frac{\square\square}{\square\square})}$$

Како се експериментални поступак даље развија, поредбени резултати други научних достигнућа омогућавају добијање нових резултата. Услед конкретног фактора се може реализовати вероватноћа догађаја [50] приликом поредбеног поступка са вероватноћом истог догађаја. али без датог конкретног фактора. Резултат се може се представити као однос одговарајућих шанси, а који јесте, заправо, резултат у виду коефицијента капе [51].Прорачун се може представити као:

$\square = \frac{\square\square\square\square - \square\square\square\square}{1 - \square\square\square\square}$, где је

- $\square\square\square\square$ - представља посматране сагласности и записује се као и може се записати као израз $(\square\square + \square\square)$,
- $\square\square\square\square$ - представља очекиване сагласности и може се записати као израз [52]: $[(\square\square + \square\square) \times (\square\square + \square\square) + (\square\square + \square\square) \times (\square\square + \square\square)$

Поредбени експеримент садржи одговарајућа ограничења; наиме, вредност K одређена је у опсегу [0, 1]. Све ниже вредности представљају, односно, могу указивати на мању сагласност. Такође, може се истаћи да постоји различити ниво сагласности и висине коефицијента корелације и то [52]:

- Сагласност (енгл. *No agreement*) не постоји уколико је $\square \leq 0$.
- Безначајна сагласност (енгл. *Slight agreement*) за вредности у опсегу $0{,}01 - 0{,}02$.
- Минимална сагласност (енгл. *fair agreement*) за вредности које се крећу у опсегу$0{,}21 - 0{,}40$.
- Умерена сагласност (енгл. *moderate agreement*) за вредности које се крећу у опсегу$0{,}41 - 0{,}60$.
- Значајна сагласност (енгл. *substantial agreement*) за вредности које имају опсег$0{,}61 - 0{,}80$.
- Скоро савршена сагласност (енгл. *near to perfect agreement*) за вредности које се крећу у опсегу од $0{,}81 - 1{,}00$.

Коефицијентима сагласности корелације може се процењивати ниво сагласности између два процењивача, а сходно њиховим класификацијама. Самим тим, могу се доносити одговарајући закључци о поузданости процене. Такође, може се као резултат добити закључак неопходним додатним корацима како би се побољшала сагласност.

11. Резултати евалуације експеримента и компаративна анализа резултата

Експериментални резултати показују да предложени модел заснован на *XG-MFA* алгоритму остварује боље перформансе у поређењу са другим методама. Резултати се мере у погледу тачности, прецизности, одзива и *Ф1*-резултата. Модел је тестиран на више скупова података, укључујући уређаје интернет ствари у здравственом сектору. С тим у вези, модел доказује своје способности за ефикасну детекцију безбедносних претњи. У поређењу са традиционалним алгоритмима, као што су Наивни Бајес (енгл. *Naive Bayes*) и стабло одлучивања (енгл. *Decision Trees*), *XG-MFA* постиже инфериорније резултате, посебно у случајевима где су подаци неуравнотежени. Анализа *SHAP* додатно пружа увид у важност различитих карактеристика, што може омогућити јасније разумевање утицаја сваке од њих на доношење одлука модела. Компаративна анализа са другим техникама оптимизације, као што су генетски алгоритам (енгл. *Genetic Algorithm*) и оптимизација роја честица (енгл. *Particle Swarm Optimization*), такође показује да је предложени модел робуснији и конзистентнији у својим предвиђањима. Резултати представљају значај и практичне примене напредних метода машинског учења и њихове оптимизације у свеукупном побољшању безбедности дистрибуираних система.

11.1. Резултати експеримента и исходи

Докторска теза се бави широким спектром и анализом многобројних резултата, како добијених експерименталним поступком, тако компаративном методом са другим научно-истраживачким резултатима. У наставку се приказује табела у којој се могу видети сумирани резултати бинарне класификације експеримента минимизације грешке [13].

Табела садржи резултате за два примарна мерила и то:

- Грешку класификације и
- Коефицијент Коенове капе (за различитост у методима).

За сваку дату методу посматрају се резултати за обе мере:

- Најбољи,
- Најгори
- Средњи,
- Медијани
- Стандардна девијација и
- Варијанса.

Методе које се користе су:

- *XG-MFA*,
- *XG-FA*,
- *XG-GA*,
- *XG-PSO*,
- *XG-ABC*,
- *XG-SSA*,
- *XG-ChOA*,
- *XG-COLSHADE* и
- *XG-S*

У табели БРОЈ могу се видети одабрани метод, грешка класификације и коефицијент Коенове капе.

Наведени методи који се користе представљају метод оптимизације; сваки има сопствене карактеристике, као и сопствени механизам решавања проблема. У контексту значења, решавање проблема односи се на оптимизацију хиперпараметара датог алгоритма машинског учења *XGBoost*. *Грешка класификације* у табели представља место где се може видети тачност класификације. Наведена колона садржи спектар статистичких метрика које могу одредити резултат у виду тачности. Колона *Коефицијент Коенове капе* састављена је од различитих статистичких метрика. Оне представљају метрике за мерење степена сагласности између два ратера; у пракси, ратер може бити алгоритам или особа која процењује и/или класификује одговарајуће ставке према одговарајућим категоријама. У конкретном случају, врши се класификација *N* ставки у *C* међусобно искључивих категорија. Овим се постиже међусобно упоређивање перформанси сваке дате методе класификације. Важно је истаћи да ниже вредности класификације грешке, заправо, указује на боље перформансе. Такође, *коефицијент Коенове капе* указује на то да све вредности које су ближе вредности 1 за резултат има бољу сагласност, када се мере различите методе. У наставку се могу видети резултати експеримента бинарне класификације. Акценат је стављен на минимизацију грешке. Може се видети закључна евалуација експеримента. Класификација је фокусирана податке који су подељени у две категорије. Посебан акценат је стављен истраживање смањења грешке у класификацији.

Табела 1 Збирни резултати бинарне класификације - експеримент минимизације грешке [13]

	Грешка класификације (циљ)						Коефицијент Коенове капе					
Метод	Најбољи	Најгори	Средњи	Медијан	Стандардна девијација	Варијанса	Најбољи	Најгори	Средњи	Медијан	Стандардна девијација	Варијанса
XG-MFA	0.003	0.003091	0.003036	0.00303	3.24×10−53.24×10−5	1.05×10−91.05×10−9	0.993852	0.993672	0.993785	0.993798	6.63×10−56.63×10−5	4.40×10−94.40×10−9
XG-FA	0.00304	0.003303	0.003153	0.003153	7.85×10−57.85×10−5	6.16×10−96.16×10−9	0.99378	0.993236	0.993545	0.993544	1.81×10−41.81×10−4	2.60×10−82.60×10−8
XG-GA	0.00304	0.003197	0.003096	0.003091	4.82×10−54.82×10−5	2.32×10−92.32×10−9	0.993781	0.993454	0.993662	0.993671	9.87×10−59.87×10−5	9.75×10−99.75×10−9
XG-PSO	0.00307	0.003215	0.003125	0.003109	4.79×10−54.79×10−5	2.30×10−92.30×10−9	0.993708	0.993418	0.993604	0.993635	9.82×10−59.82×10−5	9.64×10−99.64×10−9
XG-ABC	0.00311	0.003374	0.003213	0.003171	8.49×10−58.49×10−5	7.21×10−97.21×10−9	0.993636	0.993092	0.993422	0.993508	1.74×10−41.74×10−4	3.03×10−83.03×10−8
XG-SSA	0.00304	0.003233	0.003138	0.003144	5.99×10−55.99×10−5	3.58×10−93.58×10−9	0.993781	0.993381	0.993576	0.993563	1.23×10−41.23×10−4	1.52×10−81.52×10−8
XG-ChOA	0.00304	0.00318	0.003105	0.0031	4.21×10−54.21×10−5	1.77×10−91.77×10−9	0.99378	0.99349	0.993644	0.993653	8.85×10−58.85×10−5	7.49×10−97.49×10−9
XG-COLSHADE	0.00302	0.003215	0.003102	0.003091	5.85×10−55.85×10−5	3.43×10−93.43×10−9	0.993817	0.993419	0.993649	0.993671	1.19×10−41.19×10−4	1.44×10−81.44×10−8
XG-SASS	0.00302	0.003162	0.003105	0.003118	4.65×10−54.65×10−5	2.16×10−92.16×10−9	0.993815	0.993528	0.993644	0.993616	9.53×10−59.53×10−5	9.09×10−9

У наставку се приказује табела број 2 где се могу видети детаљно добијени резултати. Они су приказани према класама. Такође, приказује се резултат за резултат са најбољим учинком у погледу бинарне класификације. Експеримент се своди на минимизацију грешке. Описују се добијени резултати експерименталне анализе. са посебним освртом на перформансе модела бинарне класификације, по класама. У експерименту минимизације грешке истичу се најбољи модели.

Табела приказује различите метрике за сваку од класа и то:

- Прецизност - *precision,*
- Одзив - *recall,*
- *Ф1*-резултат - *F1-score*.

Посматране класе су:

- 0,
- 1,
- Макро средња вредност - *Macro Avg*,
- Пондерисана средња вредност - *Weighted Avg*.

Класе 0 и 1 често се могу сусрести у оквиру и контексту класификационих проблема, где се подаци могу класификовати у две различите категорије. Ове вредности (0 и 1) моду се доделити управо тим категоријама. Пример из праксе јесте детекција нежељене поште. Наиме, класа 0 може бити за нежељену пошту (енгл. *Spam*), док класа 1 може бити регуларна пошта, те се лакше може извршити експериментална анализа и проблем детекције класе 0 (нежељене поште).

Макро просечна вредност односи се на израчунату просечну вредност и то независно за сваку класу. Затим се тражи средња вредност обе класе. Математички посматрано, свака засебна класа може имати значајан утицај на коначан исход. Може се користити за мерење свеукупних перформанси модела.

Пондерисана просечна вредност, заправо, може дати већу тежину датим класама. Наиме, класе које имају већи број инстанци, могу имати већи утицај на исход. Услед појаве небалансираних класа, ова вредност може бити од користи. Као и макро просечна вредност, у моделу класификације може се користи за мерење прецизности, одзива и *Ф1*-резултат датих класа.

Сваки ред представљене табеле означава једну методу класификације. Колона приказује метрику перформанси за дату класу или њену просечну вредност. Како би се једноставније схватио принцип приказа дате табеле, у наставку се даје опис шаблона. Први ред табеле приказује резултате методе *XG-MFA*; користи вредности прецизност (*precision*), одзив (*recall*) и *Ф1*-резултат, затим, макро и пондерисану просечна вредност. Овакав приступ за циљ има поређење перформанси различитих метода класификације у различитим догађајима, тј. сценаријима.

У табели се користе следећи методи:

- *XG-MFA* (Modified Firefly Algorithm),
- *XG-FA* (Firefly Algorithm),
- *XG-GA* (Genetic Algorithm),
- *XG-PSO* (Particle Swarm Optimization),
- *XG-ABC* (Artificial Bee Colony Algorithm),
- *XG-SSA* (Self-adapting Spherical Search),
- *XG-ChOA* (Chimp Optimization Algorithm),
- *XG-COLSHADE* (Constrained Optimization with Levy Flights and Linear Population Size Reduction),
- *XG-SASS* (Self-adapting Spherical Search).

У наставку се може видети табела детаљних резултата експеримента минимизације грешке.

Табела 2 Добијени резултати експеримента минимизације према дефинисаним класама [13]

Метод	Метрика	0	1	Макро средња вредност	Пондерисана средња вредост
XG-MFA	*прецизност*	0.996567	0.997582	0.997074	**0.996998**
	одзив	0.998219	0.995341	0.99678	**0.996997**
	f1-резултат	**0.997392**	**0.99646**	**0.996926**	**0.996996**
XG-FA	*прецизност*	0.996628	0.997416	0.997022	0.996962
	одзив	0.998096	0.995424	0.99676	0.996962
	f1-резултат	0.997362	0.996419	0.99689	0.996961
XG-GA	*прецизност*	**0.99678**	0.997208	0.996994	0.996962
	одзив	0.997943	0.995632	0.996787	0.996962
	f1-резултат	0.997361	0.99642	0.99689	0.996961
XG-PSO	*прецизност*	0.996536	0.997457	0.996997	0.996927
	одзив	0.998127	0.995299	0.996713	0.996926
	f1-резултат	0.997331	0.996377	0.996854	0.996927
XG-ABC	*прецизност*	0.996506	0.997415	0.99696	0.996892
	одзив	0.998096	0.995258	0.996677	0.996891
	f1-резултат	0.9973	0.996335	0.996818	0.996891
XG-SSA	*прецизност*	0.996841	0.997125	0.996983	0.996962
	одзив	0.997882	**0.995715**	**0.996798**	0.996962
	f1-резултат	0.997361	0.99642	0.99689	0.996961
XG-ChOA	*прецизност*	0.996293	0.997872	**0.997083**	0.996964
	одзив	0.998434	0.994966	0.9967	0.996962
	f1-резултат	0.997362	0.996417	0.99689	0.996961
XG-COLSHADE	*прецизност*	0.996719	0.997333	0.997026	0.99698
	одзив	0.998035	0.995549	0.996792	0.996979

У наставку се подешавају хиперпараметри за одговарајућу бинарну класификацију, са циљем постизања минимизације грешке. Наредна табела приказује најбоље добијене хиперпараметре за дату бинарну класификацију, тј. минимизацију грешке.

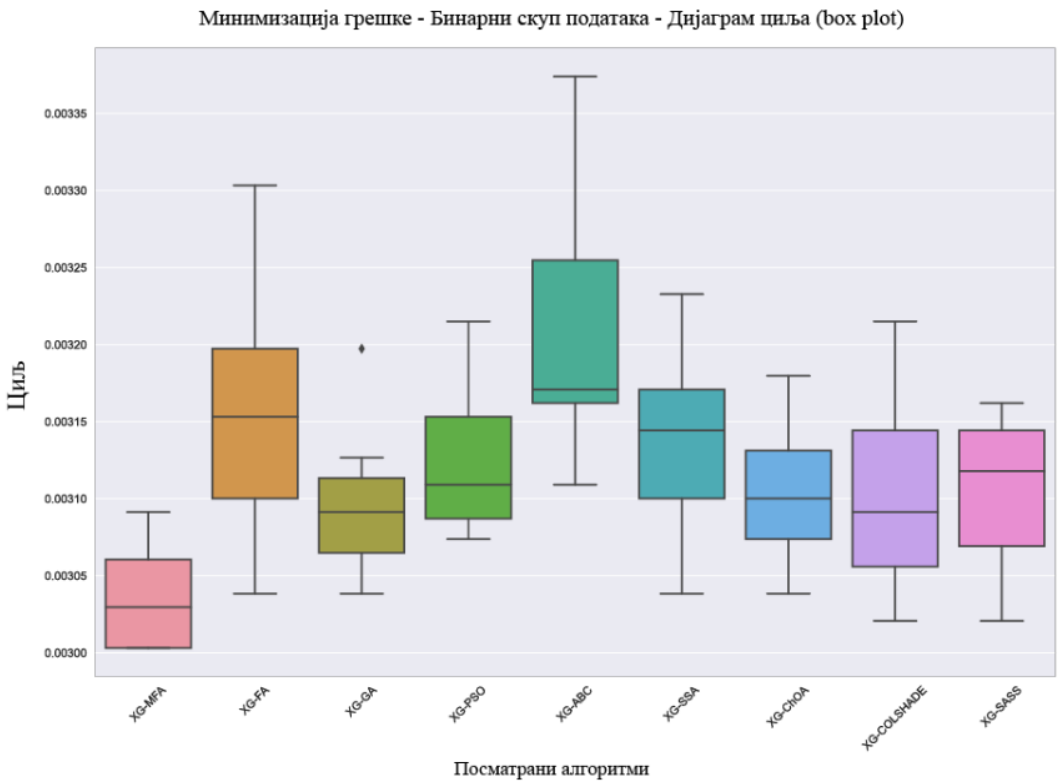
У табели се могу видети поставке хиперпараметара за дефинисане методе; користе се исти методи поменути у претходном експерименталном делу. Поставке хиперпараметара, поред прве већ поменуте колоне су:

- Стопа учења (енгл. *Learning Rate*),
- Минимална тежина детета (енгл. *Min Child Weight*),
- Подузорак (енгл. *Subsample*),
- Број узорака по дрвету (енгл. *Colsample by Tree*),
- Максимална дубина (енгл. *Max Depth*),
- Гама (енгл. *Gamma*).

Табела 3 Најбољи добијени хиперпараметри од стране модела помоћу бинарне класификације [13]

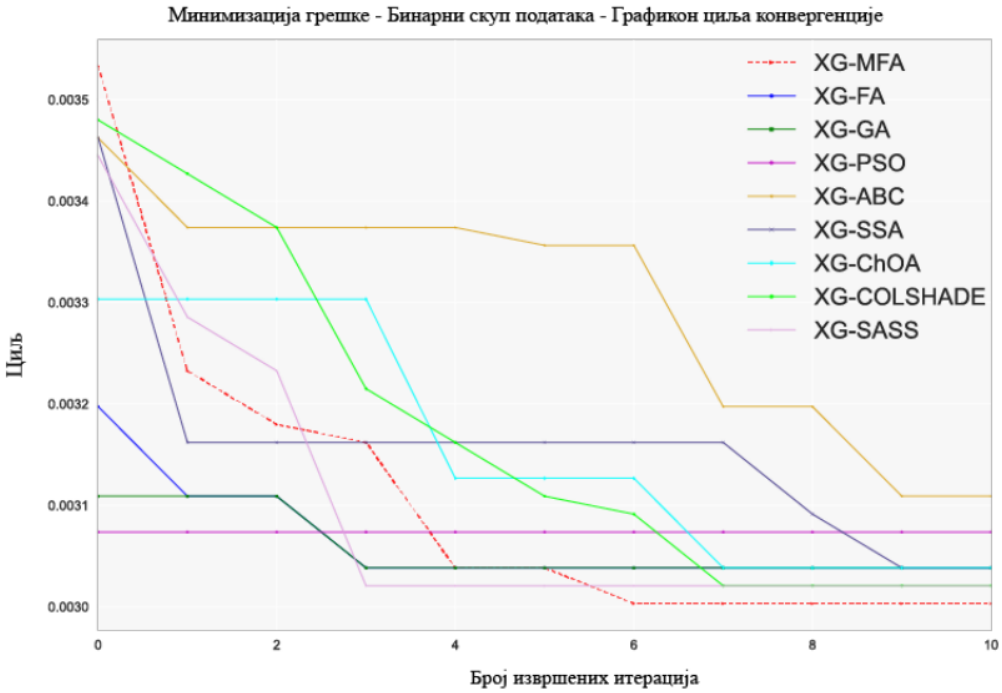
Метод	Стопа учења	Мин. тежина детета	Подузорак	Број узорака по стаблу	Макс. дубина	Гама
XG-MFA	0.826864	1.781749	0.801824	0.663691	10	0.120070
XG-FA	0.900000	1.128921	0.793675	0.871647	10	0.800000
XG-GA	0.788252	1.000000	1.000000	1.000000	10	0.000000
XG-PSO	0.602643	1.000000	0.680449	1.000000	10	0.800000
XG-ABC	0.900000	1.000000	0.673743	1.000000	7	0.323973
XG-SSA	0.748588	1.216229	1.000000	1.000000	10	0.023409
XG-ChOA	0.774825	1.000000	1.000000	1.000000	10	0.567155
XG-COLSHADE	0.900000	2.324410	0.826696	0.781224	10	0.259289
XG-SASS	0.900000	1.000000	0.980985	0.632832	8	0.149104

У наставку се даје графички приказ у виду графикона где се може видети дати експеримент. Приказује се анализа резултата добијена приликом експерименталног поступка [13] бинарне минимизације, током експерименталног поступка. Овим се даје визуализација различитих аспеката перформанси модела. Разноврсност се приказује уз дијаграм ројева за циљ конвергенције и дијаграм циља помоћ, који на јаснији начин приказује графичку расподелу на квартиле, медијане и друге вредности скупа података. Квантили представљају у статистици заједнички назив за перцентиле, деците и квартиле, те се може користити као мера која може поделити једнака перцентилна растојања одговарајућег скупа података.



Слика 20 Графикон дијаграма циља за бинарни скуп података [13]

На наредној слици се приказује графикон циља конвергенције за бинарни скуп података, где се могу видети перформансе различитих алгоритама током времена. Алгоритми *XG-MFA, XG-FA, XG-GA, XG-PSO, XG-ABC, XG-SSA, XG-ChOA, XG-COLSHADE* и *XG-SASS* се пореде у смислу смањења грешке класификације. Вредности по *X* оси представљају број итерација, док *У* оса представља грешку класификације, при чему нижа вредност грешке указује на боље перформансе алгоритма.



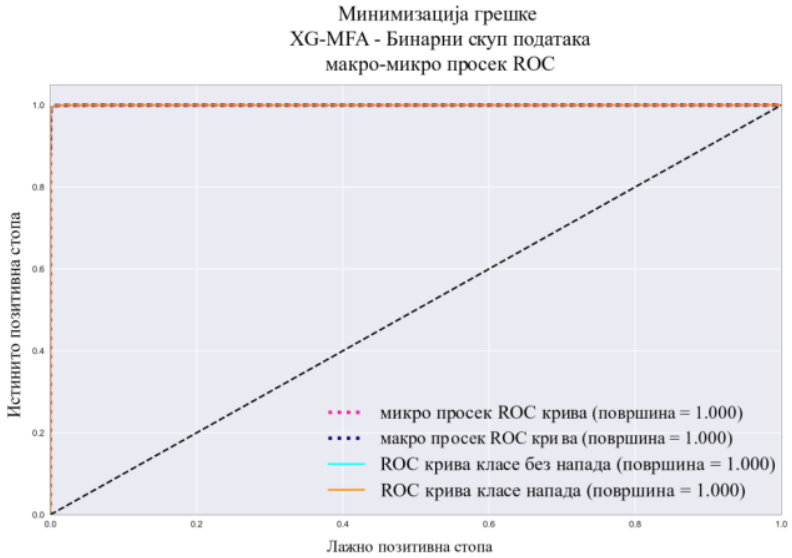
Слика 21 Графикон циља конвергенције за бинарни скуп података [13]

Слика 22 приказује *PR* криву предложеног *XG-MFA* алгоритма за бинарни скуп података. Види се да су просечне вредности прецизности (AP) за класе без напада, са нападом и микро просек једнаке 1.000, што може указује на високу тачност алгоритма приликом поређења између датих класа. Резултат даје основ да алгоритам остварује изузетне перформансе приликом детекције напада у датом контексту.



Слика 22 Графикон криве PR предложеног XG-MFA алгоритма [13]

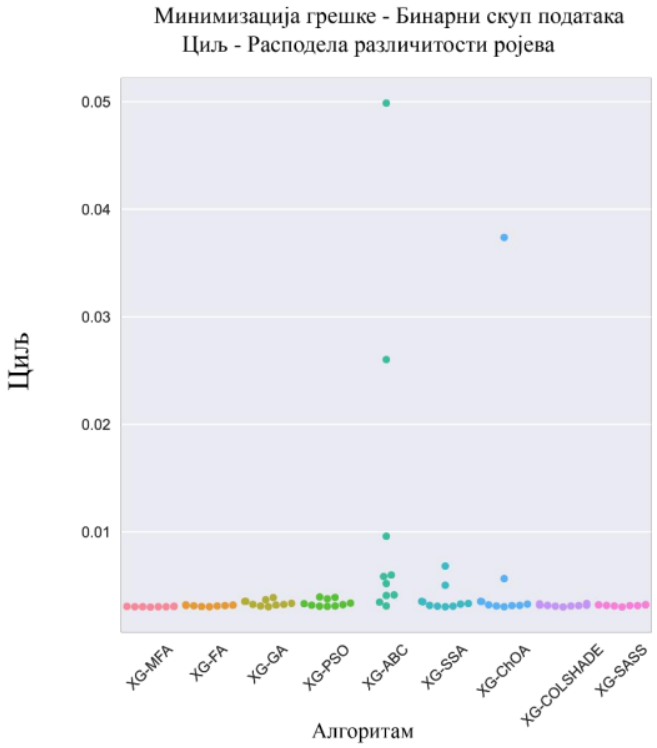
Наредна слика 23 приказује макро и микро просек *ROC* криве за бинарни скуп података. Види се да су све *ROC* криве, укључујући и криве за класе са нападом и без напада, као и микро и макро просеке, савршене са површином од 1.000. Експериментални резултат указује изразито високу тачност предложеног *XG-MFA* алгоритма приликом детекције и класификације напада, показујући његову високу способност тачног разликовања различитих класа.



Слика 23 Графикон макро и микро просека ROC криве за бинарни скуп података [13]

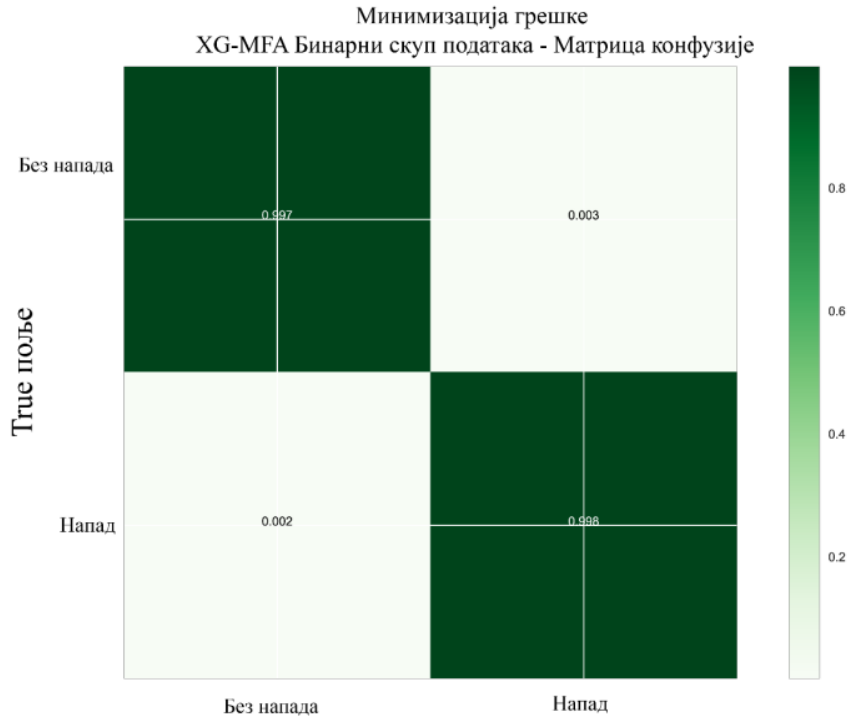
Слика 24 Графикон макро и микро просека ROC криве за бинарни скуп података [13]

Наредна графичка илустрација расподелу различитости ројева у бинарном скупу података. Она, као таква, приказује различите варијације алгоритама оптимизације, укључујући *XG-MFA*, *XG-FA*, *XG-GA* и друге. Различитости у расподели указују на велике разлике у начину на који сваки алгоритам истражује простор решења, постижући различите нивое ефикасности приликом оптимизације.



Слика 24 Графичка илустрација расподеле различитости ројева у бинарном скупу података [13]

Наредна графика приказује матрицу конфузије где се може видети тачност *XG-MFA* алгоритма у датој бинарној класификацији. Боје и бројеви у ћелијама матрице илуструју број тачно класификованих и погрешно класификованих примера за сваку категорију. Вредности у ћелијама означавају висок ниво тачности модела, што представља базу и чврст оквир за поуздану детекцију напада у дистрибуираним системима.



Слика 25 Графичка илустрација бинарног скупа података XG-MFA алгоритма и матрица конфузије [13]

Услед неуравнотежености скупа података приликом експерименталног поступка, неопходно је додатно тестирати проблем бинарне класификације за максимизацију коефицијента Коенове капе. Током процеса експеримента добијени су резултати у виду опште метрике [13]. Алгоритам *XG-MFA* приказује најбољи резултат. Поредбеном анализом постоје одступања у девијацији за класу 0. У овом поступку посматрани (доминантни) алгоритам *XG-MFA* има одговарајуће недостатке у поређењу са *XG-ABC* алгоритмом. За класу 0 посматрају се следећи резултати [13]:

- Најбољих девијација,
- Најгорих девијација,
- Просечних девијација,
- Девијације медијана,
- Стандардне девијације.

У наредној Табели 4 могу се видети остварени резултати дате бинарне класификације [13], где се мерила максимизација коефицијента Коенове капе. У табели се представљају перформансе различитих метода у контексту грешке класификације и Коеновог коефицијента капе. Табела укључује више метрика као што су варијанса, стандардна девијација, медијан, просек, најгори и најбољи резултат за сваку методу, како за грешку

класификације тако и за Коенов коефицијент капе. Циљ и исход приказивања резултата ове табеле јесте да се идентификује која метода остварује најбоље перформансе у смислу минималне грешке класификације и максималног Коеновог коефицијента капе. Резултати су од користи приликом разумевања ефективности сваке методе приликом детекције и класификације у практичним сценаријима.

Табела садржи:

- Методи; наведене су различите методе као што су *SASS-XG*, *COLSHADE-XG*, *ChOA-XG*, *SSA-XG*, *ABC-XG*, *PSO-XG*, *GA-XG*, *FA-XG*, и *MFA-XG*.
- Грешка класификације; подаци укључују варијансу, стандардну девијацију, медијан, просечну вредност, најгори и најбољи резултат за сваку методу.
- Коенов коефицијент капе; слично као и за грешку класификације, укључени су подаци о варијанси, стандардној девијацији, медијану, просеку, најгорем и најбољем резултату за сваку методу.

Табела 4 Резултати експеримента максимизације коефицијента Коенове капе дате бинарне класификације [13]

	Коефицијент Коенове капе (Циљ)						Грешка класификације					
Метод	**Најбољи**	**Најгори**	**Просечни**	**Медијан**	**Стандардни**	**Варијанса**	**Најбољи**	**Најгори**	**Просечни**	**Медијан**	**Стандардни**	**Варијанса**
XG-MFA	**0.993817**	**0.993707**	**0.99378**	**0.99378**	3.64×10−5	1.33×10−9	**0.003021**	**0.003074**	**0.003038**	**0.003038**	1.77×10−5	3.12×10−10
XG-FA	0.993746	0.993345	0.993577	0.993581	1.36×10−4	1.84×10−8	0.003056	0.00325	0.003138	0.003136	6.61×10−5	4.36×10−9
XG-GA	0.993707	0.993454	0.993621	0.993635	7.47×10−5	5.57×10−9	0.003074	0.003197	0.003116	0.003109	3.64×10−5	1.32×10−9
XG-PSO	0.993744	0.993526	0.993644	0.993689	8.44×10−5	7.12×10−9	0.003056	0.003162	0.003105	0.003083	4.12×10−5	1.70×10−9
XG-ABC	0.993707	0.9932	0.993413	0.993381	1.72×10−4	2.97×10−8	0.003074	0.003321	0.003217	0.003233	8.40×10−5	7.06×10−9
XG-SSA	0.993745	0.993562	0.99369	0.993707	5.46×10−5	2.99×10−9	0.003056	0.003144	0.003083	0.003074	2.65×10−5	7.02×10−10
XG-ChOA	0.993744	0.993164	0.993585	0.993617	1.68×10−4	2.86×10−8	0.003056	0.003339	0.003133	0.003118	8.24×10−5	6.78×10−9
XG-COLSHADE	0.99378	0.993164	0.993545	0.993581	1.91×10−4	3.67×10−8	0.003038	0.003339	0.003153	0.003136	9.35×10−5	8.74×10−9
XG-SASS	0.993781	0.993345	0.993604	0.993617	1.30×10−4	1.69×10−8	0.003038	0.00325	0.003125	0.003118	6.33×10−5	4.01×10−9

У наставку се мере перформансе метрикама максимизације коефицијента Коенове капе. Добијени резултати су слични претходно остваренима, који се могу пронаћи у табели где су добијени резултати експеримента минимизације према дефинисаним класама [13]. Предложена метода на које се ослања ово научно истраживање остварује резултате са највишим успехом у односу на друге. Такође, важно је истаћи да резултати за класу 0 и 1, као и макропросечно не остварује највиши могући успех.

Приказују се детаљни резултати према класама, а за њихове најбоље моделе бинарне класификације. Извршен је експеримент максимизације коефицијента Коенове капе. Метрике које су узете у обзир за класе 0 и 1 јесу:

- Прецизност,
- Одзив,
- Ф1-резултат (*F1-score*),
- Макро просечна вредност,
- Пондерисана средња вредност.

Макропросечна вредност представља просечну вредност метрике. У датом случају представља просечну вредност прецизности, одзива и Ф1-резултат свих класа. Метрика, заправо, даје истоветан значај свакој класи. Може се користити онда када су подједнако важне све посматране класе.

Пондерисана просечна вредност представља просечну вредност истих метрика, али превасходно са посебним осврtом на укупан број инстанци у свакој класи. Метрика даје више значаја већим класама. Може се користити онда када класе нису једнако заступљене у датом скупу података.

Такође, у табели је дефинисан број инстанци (узорака) и означен је називом *support*. Инстанце припадају свакој класи у скупу података. У резултатима се може видети да је за класу 0 резултат 32 *571*, док је за класу 1 резултат *124 038* [13]. Укупан број инстанци коришћених приликом прорачуна метрика односи се на макропросечну вредност и пондерисану средњу вредност.

У табели се могу видети различите метрике за различите методе које се деле на две класе, а у контексту класификације. Евалуација је обављена над *56 609* инстанци. Класи 0 припада *32 571* инстанци, док Класи 1 припада *24 038* инстанци. Овим се постиже евалуација приликом постизања идентификације најбољих модела моји могу дати најбољи резултат за дати критеријум. Такође, може се установити и проценити колики ниво успешности остварују модели приликом предвиђања.

Следећа табела приказује резултат бинарне класификације модела [13].

Табела 5 Резултати експеримента максимизације коефицијента Коенове према класама 0 и 1

Метод	Метрика	Класа 0	Класа 1	Макро просечна вредност	Пондерисана средња вредност
XG-MFA	*прецизност*	**0.996811**	0.997208	0.99701	**0.99698**
	одзив	0.997943	**0.995674**	**0.996808**	**0.996979**
	f1-резултат	**0.997376**	**0.99644**	**0.996908**	**0.996979**
XG-FA	*прецизност*	0.99678	0.997167	0.996973	0.996944
	одзив	0.997912	0.995632	0.996772	0.996944
	f1-резултат	0.997346	0.996399	0.996872	0.996944
XG-GA	*прецизност*	0.99608	**0.99808**	**0.99708**	0.996929
	одзив	**0.998588**	0.994675	0.996631	0.996926
	f1-резултат	0.997332	0.996376	0.996853	0.996926
XG-PSO	*прецизност*	0.996475	0.997581	0.997028	0.996945
	одзив	0.998219	0.995216	0.996718	0.996944
	f1-резултат	0.997347	0.996397	0.996872	0.996943
XG-ABC	*прецизност*	0.996262	0.99783	0.997046	0.996928
	одзив	0.998403	0.994925	0.996664	0.996926
	f1-резултат	0.997332	0.996375	0.996854	0.996926
XG-SSA	*прецизност*	0.99678	0.997167	0.996973	0.996944
	одзив	0.997912	0.995632	0.996772	0.996944
	f1-резултат	0.997346	0.996399	0.996872	0.996944
XG-ChOA	*прецизност*	0.996597	0.997415	0.997006	0.996945
	одзив	0.998096	0.995382	0.996739	0.996944
	f1-резултат	0.997346	0.996398	0.996872	0.996944
XG-COLSHADE	*прецизност*	0.996323	0.997831	0.997077	0.996963
	одзив	0.998403	0.995008	0.996706	0.996962
	f1-резултат	0.997362	0.996417	0.99689	0.996961
XG-SASS	*прецизност*	0.996719	0.997291	0.997005	0.996962
	одзив	0.998004	0.995549	0.996777	0.996962
	f1-резултат	0.997361	0.996419	0.99689	0.996961
	Подршка (support)	32571	24038	56609	56609

Дефинисање поставки хиперпараметара за дату бинарну класификацију дефинишу се како би се извршила максимизација коефицијента Коенове капе. Према остваренim резултатима научног истраживања [13] резултати следа претходно поменутих поставки се могу видети у наставку.

Табела приказује најбоље добијене хиперпараметре добијених модела који се могу користити у експерименту. Сваки ред дате табеле односи се на један модел. Колоне приказују различите хиперпараметре и то:

- Стопа учења (енг *Learning Rate*),
- Минимална тежина детета (енгл. *Min Child Weight*),
- Подузорак (енгл. *Subsample*),
- Број колона према стаблу (енгл. *Colsample by Tree*),
- Максимална дубина стабла (енгл. *Max Depth*),
- Гама параметар (енгл. *Gamma*).

Стопа учења (енг *Learning Rate*) представља параметар који може одредити колико модел може учити брзо или споро. Процес се посматра на нивоу обучавања. Уколико дође до изузетно високе стопе учења доводи се потенцијално до брже конвергенције. Такође, истим поступком се може десити и веома брзо прескакање оптималних решења. Самим тим, ово може узроковати дисбаланс, односно, разнолике осцилације перформанси модела. Уколико дође до ниже стопе учења, ово може резултовати веома стабилнијим процесом учења, али га исто тако чини и значајно споријим.

Минимална тежина детета (енгл. *Min Child Weight*) јесте параметар који може контролисати минималну суму тежина датих инстанци. Она омогућава наставак партиционисања чвора у стаблу где се приликом процеса учења врши одлучивање. Неуравнотеженост се може десити услед значајног повећања наведеног параметра, те се може довести поступак до смањења пренаучености модела.

Подузорак (енгл. *Subsample*) представља параметар којим се може одредити ближе део узорака који се могу користити приликом обучавања модела. Може омогућити обучавање модела над подскупом података, уместо на целокупном скупу. Ово представља користан поступак приликом спречавања пренаучености. Такође, може довести и до убрзаног процеса учења над великим скуповима података.

Број колона према стаблу (енгл. *Colsample by Tree)* указује и одређује параметар који дефинише колика је дубина стабла одлучивања приликом процеса учења. Услед постизања веће максималне дубине стабла могу се добити сложенији модели. Они могу превасходно боље научити сложеније и комплексније обрасце у датим подацима. Такође, истим поступком је могуће довести и до пренаучености.

Гама параметар (енгл. *Gamma*) задужен за регулисање регуларизације у оквир алгоритма градијентног појачања стабала - *XGBoost*. Може контролисати колико је неопходно

умањити губитак како би се могла направити нова, додатна, партиција на самом чвору стабла. Приликом повећавања вредности поменутог параметра може се постићи виша регуларизација, што резултује спречавању пренаучености модела.

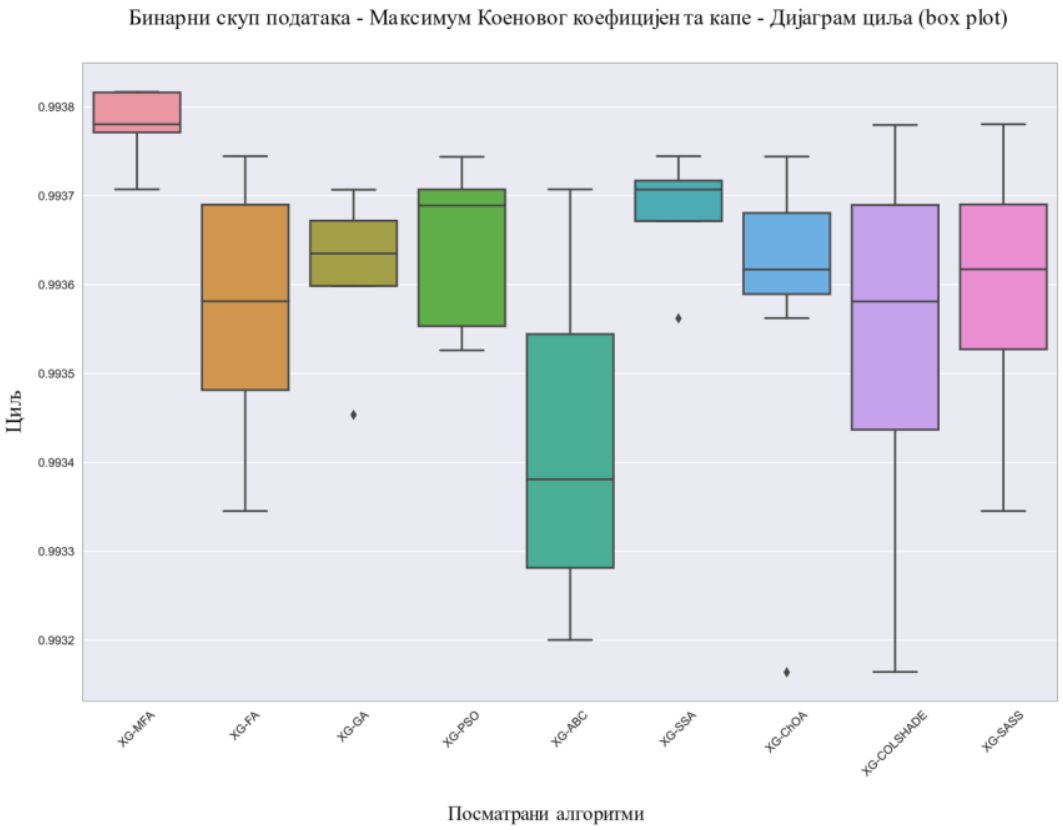
Помоћу наведених хиперпараметара, а на основу њихових вредности, одређују се начини путем којих алгоритми могу учити или се могу прилагодити подацима, а са циљем постизања најбољих исхода и резултата приликом бинарне класификације.

Табела 6 Поставке хиперпараметара за моделе бинарне класификације експеримента [13]

Метод	Стопа учења	Минимална тежина детета	Подузорак	Број колона према стаблу	Максимална дубина стабла	Гама параметар
XG-MFA	0.9	1	0.993956	0.790192	10	0.166214
XG-FA	0.9	1	1	1	10	0
XG-GA	0.9	1.929015	1	0.82109	10	0.8
XG-PSO	0.9	1	0.979482	1	10	0.061248
XG-ABC	0.625776	1	0.627028	0.970949	10	0.371569
XG-SSA	0.9	1	1	1	10	0
XG-ChOA	0.876269	1.576144	0.660126	0.766469	10	0.8
XG-COLSHADE	0.874638	1.584114	1	1	10	0
XG-SASS	0.9	1.29875	0.885388	1	10	0.35875

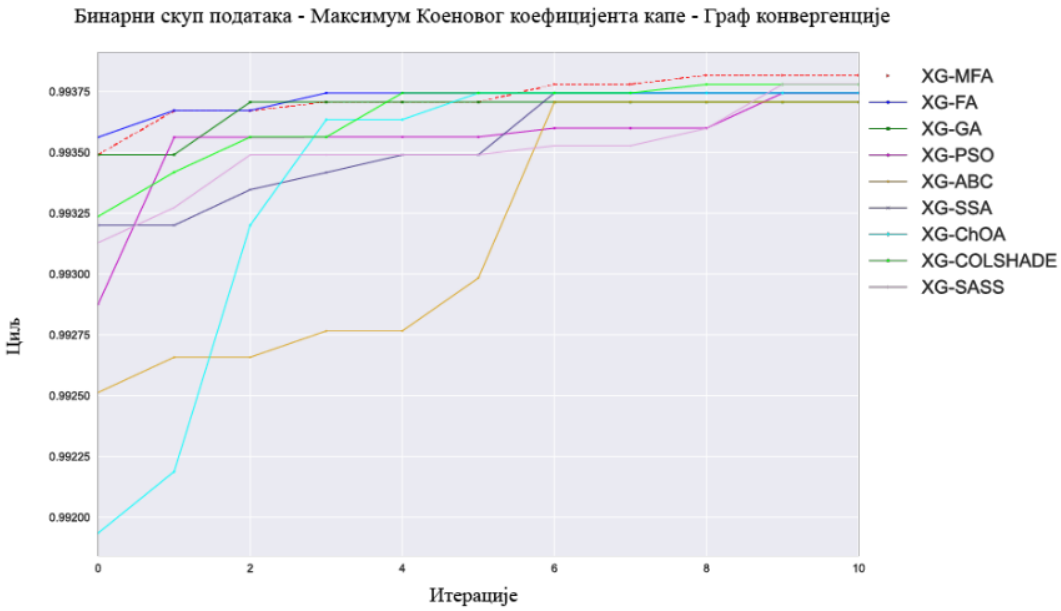
На основу обављених експерименталних анализа [13] у наставку се приказују графикони. Они су одређени на исти начин као и у претходном случају - приликом графичке илустрације резултата експеримента минимизације грешке. За разлику од претходних, у наставку се представљају максималне за дате експерименте.

Слика 26 приказује дијаграме циља за максималне вредности Коеновог коефицијента капе за различите алгоритме. Свака вредност (графички илустрована у виду правоугаоника, односно, кутије) представља распон вредности које је алгоритам постигао током валидације података. Дата илустрација омогућава визуелно поређење стабилности и конзистентности различитих алгоритама у постизању високих вредности Коеновог коефицијента капе, што може представљати мерило поузданости класификације.



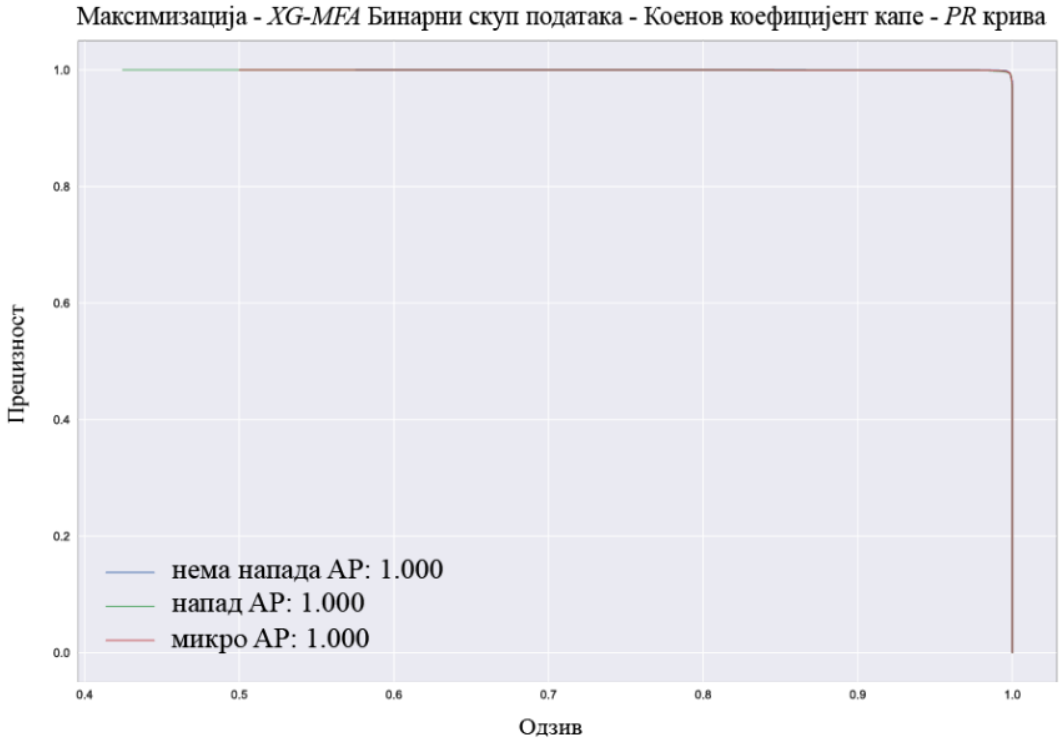
Слика 26 Графичка илустрација дијаграма циља за максималне вредности Коеновог коефицијента капе [13]

Наредна слика илуструје резултате помоћу графикон конвергенције који показује како различити алгоритми могу постизати максималне вредности Коеновог коефицијента капе, током времена. Свака линија представља понашање једног алгоритма, а скокови и падови вредности указују на њихову стабилност и ефикасност приликом процеса оптимизације. Слика једноставније представља поређење брзине конвергенције и коначних постигнутих вредности, што олакшава процену перформанси алгоритама у бинарној класификацији.



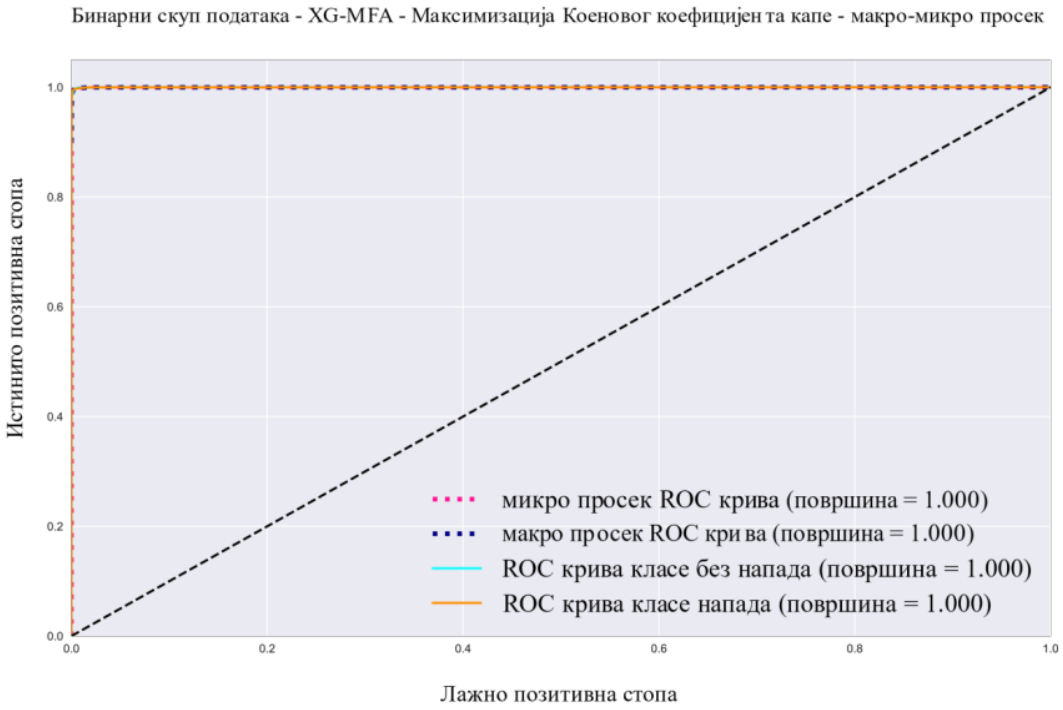
Слика 27 Графикон конвергенције, где се приказују максималне вредности Коеновог коефицијента капе [13]

Слика 28 приказује *PR* криву (Precision-Recall) за бинарни скуп података користећи максималне вредности Коеновог коефицијента капе. На графикону се могу видети да су све вредности *AP* (Average Precision) једнаке 1.000, што, заправо, указује на, готово, савршену прецизност и опозив за класе без напада и са нападом, као и укупно, тј. кумулативно (микро *AP*). Постигнути експериментални резултат за предложени алгоритам *XG-MFA* приказује изванредне перформансе приликом детекције напада у бинарним скуповима података.



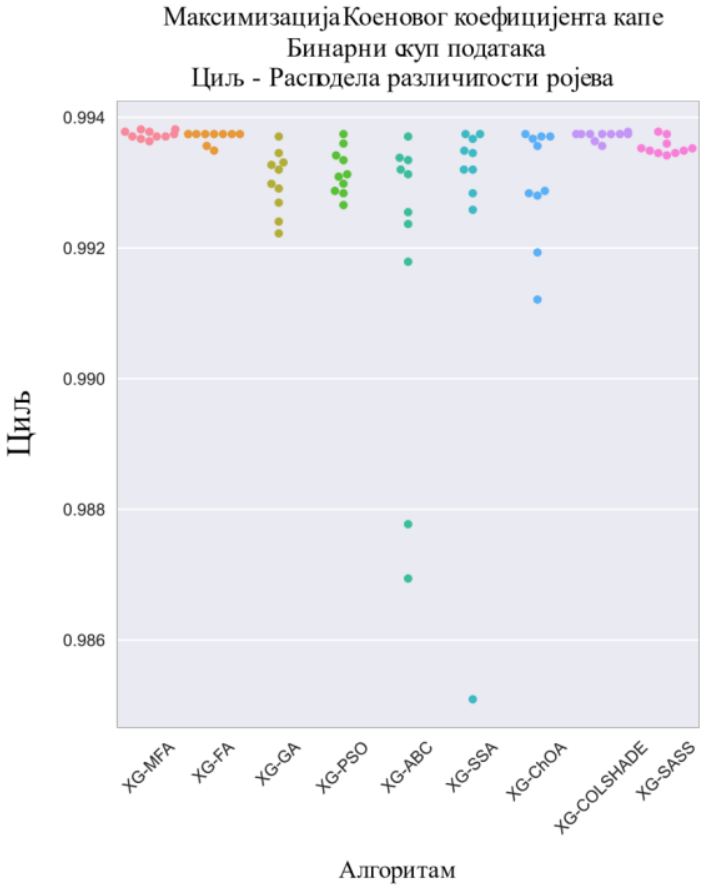
Слика 28 Графичка илустрација PR криве над бинарним скупом података, помоћу максималних вредности Коеновог коефицијента капе [13]

У наставку се приказује слика 29, која илуструје експерименталне резултате за макро и микро просек *ROC* криве, за бинарни скуп података, користећи предложени *XG-MFA* алгоритам. Вредности површине испод криве (AUC) за све класе су 1.000, што указује на савршену дискриминациону способност модела између посматраних позитивних и негативних класа. Постигнути резултат илуструје изванредне перформансе *XG-MFA* алгоритма приликом класификацији бинарних података са максималним вредностима.



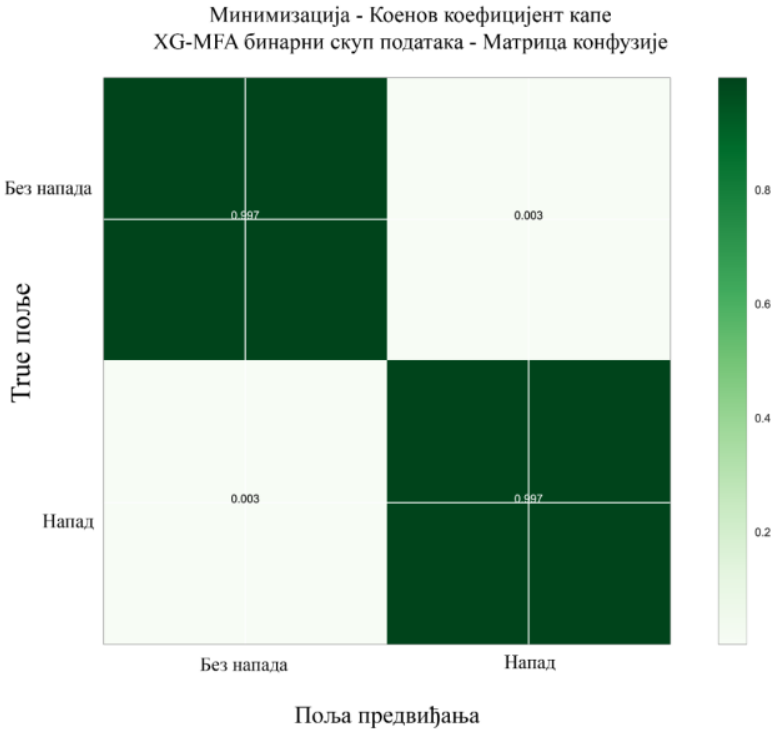
Слика 29 Графичка илустрација макро-микро просека за бинарни скуп података XG-MFA алгоритма [13]

Наредна слика илустрације расподеле различитости појева на основу максималних вредности Коеновог коефицијента капе. На хоризонталној оси приказују се различити разматрани алгоритми, док се на вертикалној оси приказује вредност Коеновог коефицијента капе. У резултатском смислу види се да алгоритми показују различит степен варијације у достизању својих перформансама; неки разматрани алгоритми приказују мање варијације, док други показују већу расподелу резултата.



Слика 30 Графичка илустрација расподеле различитости појева, помоћу максималних вредности Коеновог коефицијента капе [13]

Наредна графика приказује матрицу конфузије за максималне вредности бинарног скупа података коришћењем Коеновог коефицијента капе. Приказује се тачност модела при класификацији узорака, где вредности на дијагонали представљају исправно класификоване узорке. Остварени резултати приказују да модел рефлектује високу тачност у обе класе, са ниским процентом нетачно класификованих узорака



Слика 31 Графичка илустрација матрице конфузије за максималне вредности бинарног скупа података помоћу Коеновог коефицијента капе [13]

Приликом обављања многобројних експерименталних анализа приказује се и вишекласна грешка метахеуристичких метода [13]. Током обављања експерименталног постука алгоритам *XG-MFA* приказује најбоље резултате у погледу перформанси. Приликом датог експерименталног поступка алгоритам слабије показао на два места и то:

1. Стандардна девијација и
2. Варијанса.

У оквиру истог експерименталног постука [13], алгоритам *XG-COLSHADE* током обраде података показује конзистентност; она се огледа у најмањој варијацији својих перформанси. Анализом резултата долази се до јединственог закључка да ово указује на то да поменути фактор остварује најниже вредности за два параметра и то за стандардну девијацију и варијансу. Услед подесних резултата, ово може представљати релевантан фактор приликом одређивања модела, на бази балансираних резултата. Алгоритам *XG-ABC* у истом експерименталном поступку приказује најлошије перформансе.

Табела 7 Приказ општих резултата класификације вишеструких класа [13]

	Класификација грешке (циљ)						Коефицијент Коенове капе					
Метод	**Најбољи**	**Најгори**	**Просечни**	**Медијан**	**Стандардни**	**Варијанса**	**Најбољи**	**Најгори**	**Просечни**	**Медијан**	**Стандардни**	**Варијанса**
XG-MFA	**0.008232**	**0.008462**	**0.008322**	**0.00832**	9.30×10−5	8.66×10−9	**0.986843**	**0.986475**	**0.986699**	0.96704	1.49×10−4	2.22×10−8
XG-FA	0.00832	0.008797	0.008473	0.008409	1.58×10−4	2.53×10−8	0.986704	0.985939	0.986458	0.98656	2.54×10−4	6.46×10−8
XG-GA	0.008356	0.008603	0.008446	0.008435	7.97×10−5	6.35×10−9	0.986645	0.986251	0.986499	0.986516	1.27×10−4	1.62×10−8
XG-PSO	0.008409	0.008727	0.008499	0.008444	9.73×10−5	9.47×10−9	0.986559	0.986052	0.986415	0.986502	1.55×10−4	2.41×10−8
XG-ABC	0.008426	0.008992	0.008687	0.008691	1.71×10−4	2.93×10−8	0.986532	0.985628	0.986114	0.986107	2.74×10−4	7.52×10−8
XG-SSA	0.008356	0.00855	0.008446	0.008426	7.77×10−5	6.04×10−9	0.986643	0.986334	0.9865	0.986532	1.25×10−4	1.56×10−8
XG-ChOA	0.008373	0.008568	0.008464	0.008462	7.20×10−5	5.18×10−9	0.986615	0.986305	0.986471	0.986474	1.15×10−4	1.33×10−8
XG-COLSHADE	0.008303	0.008479	0.008375	0.008364	5.55×10−5	3.08×10−9	0.986729	0.986445	0.986612	0.986629	8.89×10−5	7.91×10−9
XG-SASS	0.008391	0.00885	0.008515	0.008506	1.37×10−4	1.90×10−8	0.986588	0.985855	0.986391	0.986405	2.20×10−4	4.84×10−8

Приликом анализе експерименталних резултата на који се примарно ослања ово научно истраживање [13], резултати се огледају у виду перформанси, а приказују се метрика прецизности, одзива, затим, Ф1-резултат. Прецизније, за три посматране класе, тј. Класа 0, Класа 1 и Класа 2, мери се резултат перформанси. Такође, посматрана табела користи и вредности макропросека и пондерисаног просека. Као и у претходним случајевима, приказује се и број инстанци за сваку посматрану класу дефинисаног скупа података. Евалуацијом је установљено да алгоритам XG-MFA остварује најбоље резултате у оквиру:

- Прецизности,
- Одзива и
- Ф1-резултата / пондерисани просек.

Класа 2 остварује најбоље резултате прецизности и Ф1-резултата. Евалуацијом се установљава да алгоритам *XG-MFA* остварује навећи степен одзива у Класи 0. Такође, истиче се и најбољи резултат у виду прецизности Класе 1.

Алгоритам *XG-PSO* приликом евалуације резултата приказује најбољи резултат у погледу одзива у оквиру посматране Класе 2. Такође, приликом експерименталног поступка указује се на тачност у погледу идентификације свих позитивних инстанци посматране класе. У погледу прецизности датог резултата, може се видети да највиша прецизност припада алгоритму *XG-SSA* у оквиру класе 0. Истим резултатима и истом алгоритму придружују се најбољи резултати у погледу највишег макропросека за прецизност. Суштински, тиме се постиже значајно боље може одредити, тј. предвидети позитивну класу, а на основу вишеструких класа. Такође, уколико постоји било каква неуравнотеженост класа у датом домену, посматрани метод тај сегмент, технички, игнорише. За исти метод резултат одзива класе 1 је највиши, те се тиме постиже ефикасност у домену идентификовања инстанци дате класе.

Како неки методи доминирају у различитим сегментима и њиховим метрикама, уравнотежен и балансиран метод припада *XG-MFA* методи. Тиме се стиче претпоставка да се може узети као модел методе који се може применити у специфичној сфери где се посматрају све метрике и где су све једнако важне. Посматрани експеримент суштински има неуравнотеженост у погледу расподеле класа, а што може утицати на исход перформанси датих модела, где је однос следећи:

- Класа 0: 9 528,
- Класа 1: 23 043,
- Класа 2: 24 038.

Посебна пажња се придаје томе да се резултат може бити више оријентисана према класи 1 и класи 2, с обзиром на то да оне имају веће вредности. Стога, уколико се у обзир узима дата неуравнотеженост, метрика која мери пондерисану просечну вредност може узети наведени сценарио у обзир и самим тим се може приказати свеукупна боља оцена перформанси модела у поређењу са оценом макропросека.

Табела 8 Резултати вишекласне класификације приликом експеримента минимизације грешке [13]

Метод	Метрика	0	1	2	Макро просечна вредност	Пондерисана просечна вредност
XG-MFA	прецизност	0.97615	0.992045	**0.997705**	0.988633	**0.991773**
	одзив	0.975126	0.995747	0.99455	0.988474	**0.991768**
	f1-резултат	**0.975638**	**0.993892**	**0.996125**	**0.988552**	**0.991768**
XG-FA	прецизност	0.974445	**0.992598**	0.997663	0.988235	0.991693
	одзив	**0.97649**	0.99514	0.994384	**0.988671**	0.99168
	f1-резултат	0.975467	0.993867	0.996021	0.988451	0.991686
XG-GA	прецизност	0.975531	0.992129	0.99758	0.988413	0.99165
	одзив	0.974916	0.995617	0.994467	0.988333	0.991644
	f1-резултат	0.975223	0.99387	0.996021	0.988371	0.991645
XG-PSO	прецизност	0.975925	0.99234	0.997082	0.988449	0.991591
	одзив	0.974286	0.99514	**0.99505**	0.988158	0.991591
	f1-резултат	0.975105	0.993738	0.996065	0.988303	0.99159
XG-ABC	прецизност	0.975525	0.991957	0.99758	0.988354	0.991579
	одзив	0.974706	0.995487	0.994509	0.988234	0.991574
	f1-резултат	0.975115	0.993719	0.996042	0.988292	0.991574
XG-SSA	прецизност	**0.976835**	0.991917	0.997247	**0.988666**	0.991642
	одзив	0.973657	**0.995834**	0.994758	0.988083	0.991644
	f1-резултат	0.975243	0.993871	0.996001	0.988372	0.99164
XG-ChOA	прецизност	0.976331	0.992086	0.997248	0.988555	0.991626
	одзив	0.974076	0.995573	0.9948	0.98815	0.991627
	f1-резултат	0.975202	0.993827	0.996022	0.98835	0.991624
XG-COLSHADE	прецизност	0.976441	0.992257	0.997206	0.988635	0.991697
	одзив	0.974391	0.99553	0.994883	0.988268	0.991697
	f1-резултат	0.975415	0.993891	0.996043	0.98845	0.991695
XG-SASS	прецизност	0.976028	0.992257	0.997164	0.988483	0.991609
	одзив	0.974286	0.995443	0.9946	0.988177	0.991609
	f1-резултат	0.975156	0.993847	0.995981	0.988328	0.991607
	Подршка (support)	9528	23,043	24,038	56,609	56,609

У наставку се приказују резултати комбиноване анализе метрике греше, прецизности одзива и *Ф1*-резултата. Указује се на то да је метод *XG-MFA* суштински најбољи међу датим методима. Наредна табела у себи садржи одређене поставке хиперпараметара за вишекласну класификацију, како би се постигла минимизација грешке. Табела приказује поставке за хиперпараметара за различите методе које се користе у експерименталном поступку. Хиперпараметри који се користе су:

- Стопа учења,
- Минимална тежина детета,
- Подузорак,
- Бр. колона према стаблу,
- Максимална дубина стабла,
- Гама параметар.

Сваки метод дефинише своје вредности датих хиперпараметара.

Табела 9 Најбољи хиперпараметри добијени од стране модела за вишекласну класификацију у експерименталном поступку минимизације грешке [13]

Метод	Стопа учења	Минимална тежина детета	Подузорак	Бр. колона према стаблу	Максимална дубина стабла	Гама параметар
XG-MFA	0.558224	1.390646	1.000000	0.754489	10	0.800000
XG-FA	0.900000	2.356392	1.000000	1.000000	7	0.800000
XG-GA	0.532608	1.671261	1.000000	1.000000	9	0.595526
XG-PSO	0.900000	1.209953	1.000000	0.965372	10	0.162178
XG-ABC	0.516726	1.000000	0.796465	0.842297	10	0.518501
XG-SSA	0.643381	1.000000	1.000000	0.864255	10	0.087284
XG-ChOA	0.650355	1.000000	1.000000	0.800611	10	0.000000
XG-COLSHADE	0.578265	1.981063	1.000000	0.761847	10	0.010795
XG-SASS	0.900000	2.028573	1.000000	1.000000	10	0.800000

Наредна табела приказује остварене резултате коефицијента Коенове капе. Резултати се приказују за различите технике метахеуристика, за разноврсне технике *XGBoost*-а. Током наредног експерименталног поступка користи се коефицијент Коенове капе, како би се извршила процена сагласности између оцењивача. Сваки оцењивач може извршити сопствену класификацију посматраних ставки, те их могу смештати у заједничке ексклузивне категорије. Метода *XG-MFA* остварује најбољи резултат у погледу поузданости методе у односу на друге посматране. Његов резултат се огледа у најбољем резултату у два сегмента и то у просеку и медијану. Током експерименталног поступка остварује највишу вредност за најбољи случај. То може значити да приликом идеалних услова може остваривати највиши степен сагласности између посматраних резултата (оних који се могу предвидети и стварних). Сваки модел је процењен кроз низ метрика како би се утврдила њихова ефикасност и поузданост. Перформансе модела су измерене у различитим аспектима, укључујући прецизност, тачност и конзистентност. Коенов капа коефицијент се користи као главна мера за процену сагласности између предвиђених и стварних ознака.

Сходно томе, метод *XG-SASS* се издваја према најнижој стандардној девијацији и варијанси капа коефицијента. Ови параметри могу указивати на то да свеукупне перформансе ове методе могу бити најконзистентнији међу свим испитиваним датог експеримента. Технички гледано, ово може значити да се посматране перформансе *XG-SASS* методе најмање разликују од просечних перформанси. Конзистентност је аспект од важности приликом процене модела машинског учења, јер може осигурати давање стабилних и предвидивих резултата модела. Док неки методи могу указивати на високу прецизност у разноликим сценаријима, стабилност баланс перформанси кроз различите тестове и скупове података може бити критична за дугорочну примену. Самим тим, иако *XG-MFA* метод може бити најефикаснији у просеку, *XG-SASS* се представља као најпоузданији, у контексту конзистентности. То се може огледати као кључна предност у сценаријима где је стабилност резултата високо критична. Сходно томе, мање варијације у перформансама указују на то да је модел мање осетљив на промене у подацима, што може представљати изузетно важан фактор у многим процедурама апликацијама машинског учења.

Дакле, док метод *XG-MFA* постиже најбоље просечне резултате, с друге стране метод *XG-SASS* остварује највиши ниво конзистентности. У наставку се приказује табела која садржи детаљне податке о перформансама различитих модела машинског учења.

Табела 10 Резултати вишекласне класификације у експерименту максимизације Коеновог капа коефицијента [13]

	Циљ- Коефицијент Коенове капе						Грешка класификације					
Метод	**Најбољи**	**Најгори**	**Средњи**	**Медијан**	**Стандардни**	**Варијанса**	**Најбољи**	**Најгори**	**Средњи**	**Медијан**	**Стандардни**	**Варијанса**
XG-MFA	**0.986785**	0.986417	**0.98667**	**0.98667**	1.25×10−4	1.56×10−8	0.008267	0.008497	0.008339	0.008338	7.80×10−5	6.11×10−9
XG-FA	0.986646	0.986416	0.986585	0.986589	6.76×10−5	4.58×10−9	0.008356	0.008497	0.008393	0.008391	4.18×10−5	1.75×10−9
XG-GA	0.986646	0.98563	0.986348	0.986446	2.93×10−4	8.62×10−8	0.008356	**0.008992**	0.008541	0.008479	1.84×10−4	3.39×10−8
XG-PSO	0.986532	0.986136	0.986369	0.986405	1.55×10−4	2.41×10−8	0.008426	0.008674	0.008528	0.008506	9.71×10−5	9.42×10−9
XG-ABC	0.986502	0.986052	0.986224	0.986207	1.54×10−4	2.38×10−8	**0.008444**	0.008727	**0.008618**	**0.008629**	9.65×10−5	9.32×10−9
XG-SSA	0.986644	0.986078	0.986418	0.98646	1.65×10−4	2.75×10−8	0.008356	0.008709	0.008497	0.00847	1.04×10−4	1.08×10−8
XG-ChOA	0.986589	0.986303	0.986457	0.98646	8.53×10−5	7.27×10−9	0.008391	0.008568	0.008473	0.00847	5.29×10−5	2.80×10−9
XG-COLSHADE	0.986645	0.986277	0.986511	0.986546	1.18×10−4	1.41×10−8	0.008356	0.008585	0.008439	0.008417	7.38×10−5	5.44×10−9
XG-SASS	0.986702	**0.986563**	0.986603	0.986589	3.96×10−5	1.57×10−9	0.00832	0.008409	0.008382	0.008391	2.50×10−5	6.24×10−10

У наставку се приказују графикони који на детаљнији начин пружају визуелизацију постигнутих резултата; омогућавају лакше поређење различитих модела. Подаци са датих илустрација могу боље представити и приближити боље разумевање перформанси модела, кроз различите метрике. У наставку се даје детаљан опис графикона вишеструких скупова података:

- Дијаграм кутија објективности (енгл. *Objective box plot diagram*)
  Графикон приказује *box plot* дијаграме за различите алгоритме коришћене у вишекласном експерименту минимизације грешке. Алгоритми су приказани на хоризонталној оси, док се вредности објективне функције представљају дуж вертикалне осе. Дијаграми *кутије објективности* могу се користити за визуализацију расподеле резултата; могу укључивати медијан, квартиле и екстремне вредности. Такође, могу помагати приликом процене конзистентности и перформанси разноликих алгоритама.

- Графикон конвергенције циља (енгл. *Objective convergence graphs*).
  Ова илустрација приказује графиконе конвергенције објективне функције током итерација разноликих алгоритама. Хоризонтална оса представља број итерација, док вертикална оса представља вредност објективне функције. Графикон показује како се перформансе алгоритама побољшавају током времена, што омогућава процену брзине конвергенције и стабилности сваког алгоритма.

- *XG-MFA* алгоритам - Крива прецизности и одзива (енгл. *PR curve*).
  Графикон приказује криву прецизности и одзива (енгл. *Precision-Recall - PR*) за *XG-MFA* алгоритам у вишекласном експерименту минимизације грешке. Крива прецизности и одзива приказују се дуж вертикалне и хоризонталне осе. Такође, крива показује однос између вредности прецизности и вредности одзива, што је корисно за процену перформанси модела у случајевима када постоји неуравнотеженост класа.

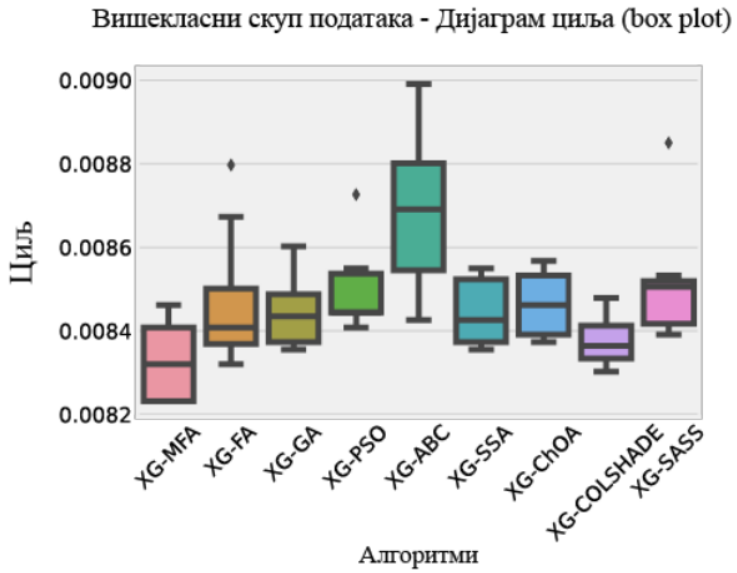
- *XG-MFA* - макро и микро просечна карактеристика пријемника оператора.
  На датом графикону приказује се крива карактеристика пријемника оператора (енгл. *macro/micro average Receiver Operating Characteristic - ROC*), са макро и микро просеком за посматрани *XG-MFA* алгоритам. Хоризонтална оса представља лажно позитивну стопу (енгл. *False Positive Rate*), док вертикална оса представља тачно позитивну стопу (енгл. *True Positive Rate*). Крива карактеристике пријемника оператора омогућава процену перформанси класификатора у различитим опсезима, док макро и микро просеци могу пружити свеобухватније мерење перформанси, за све посматране класе.

- Дијаграм јата различитости циља (енгл. *Objective swarm plot diversity*).
  Овај графикон приказује дијаграме јата који могу приказивати разноликост објективних вредности за различите алгоритме у вишекласном експерименту минимизације грешке. Алгоритми приказују дуж хоризонталне осе, а објективне вредности дуж вертикалне осе. Помоћу дијаграма јата омогућава се визуализација густине података и расподеле објективних вредности, што је може бити од високе користи приликом процене разноликости резултата међу различитим алгоритмима.

- *XG-MFA* алгоритам и матрица конфузије.
  Овај графикон приказује матрицу конфузије (енгл. *Confusion matrix*) за *XG-MFA* алгоритам у вишекласном експерименту минимизације грешке. Матрица конфузије у датој илустрацији приказује број тачно предвиђених и нетачно предвиђених класа. Такође, приказују се стварне ознаке дуж вертикалне осе и предвиђене ознаке дуж хоризонталне осе. Матрица је подесна за процену перформанси посматраног модела, као и за идентификацију класа у којима је модел најчешће правио грешке.

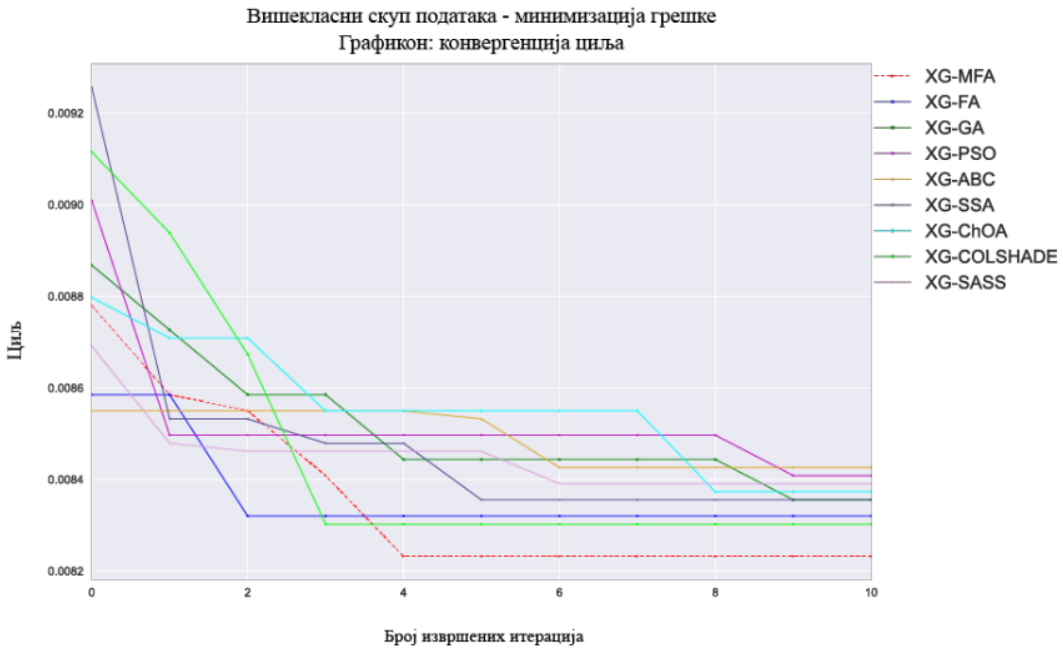
Наредне илустрације приказују графиконе који су идентични оним претходним, али се односе на вишекласни експеримент минимизације грешке. С друге стране, наредне слике експеримената приказују графиконе за експеримент у коме се максимизује вишекласни Коенов капа коефицијент. Поред тога, сваки графикон пружа прецизније увиде у понашање, као и у стабилност алгоритама приликом различитих аспекта класификације. Дати графикони су од суштинског значаја за јаснију анализу, визуелизацију предности и недостатака сваког од посматраних алгоритама. Комбинација свих ових визуализација омогућава збирну процену перформанси и конзистентности модела у вишекласној класификацији.

Наредни графикон приказује дијаграм вишекласног скупа података, где се илуструје дијаграм циља. Представља се распон вредности илустрованих за различите моделе, приказујући мере централне тенденције и распршености података. Различите боје осликавају различите моделе, омогућавајући визуелно поређење њихових перформанси и стабилности истих.



Слика 32 Дијаграм вишекласног скупа података, где се илуструје дијаграм циља [13]

Дијаграм вишекласног скупа података илуструје распон вредности за различите алгоритме. Наредни графикон приказује конвергенцију објективне функције током итерација за различите посматране алгоритме. Приказује се како се перформансе сваког алгоритма мењају током времена, при чему различите боје линија на графикону представљају различите алгоритме. На овај начин омогућено је једноставнија визуелизација у виду праћења и поређења ефикасности и стабилности сваког алгоритма током процеса оптимизације.



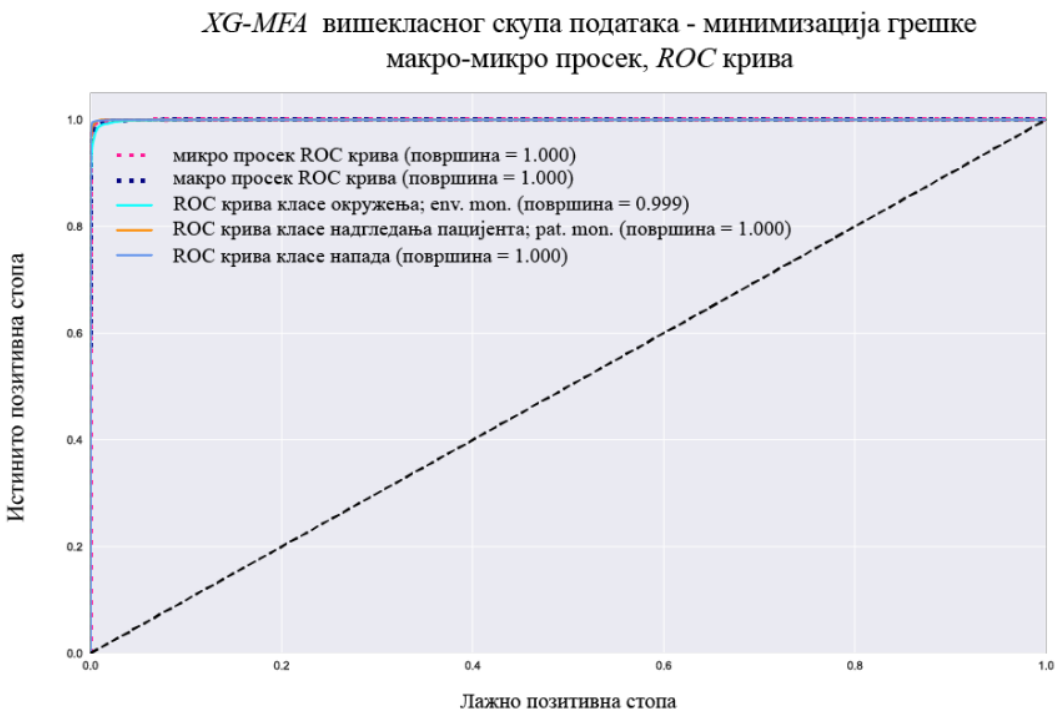
Слика 33 Графикон конвергенције објективне функције током итерација за различите алгоритме, показујући како се перформансе мењају током времена [13]

Графикон конвергенције објективне функције током итерација за различите алгоритме показује како се перформансе могу мењати у функцији времена. У наставку се приказује графикон површине испод криве *PR* (Precision-Recall) за предложени *XG-MFA* алгоритам. Графикон приказује стваран однос између прецизности и одзива у оквиру датих сценарија које имају неуравнотежене класе. На основу просечне прецизности, види се да је *AP* за надгледање окружења (env. mon.) 0.997, док је *AP* за надгледање пацијената (pat. mon.) и у случају напада 1.000, што кумулативно указује на изузетно високу ефикасност алгоритма у различитим контекстима.



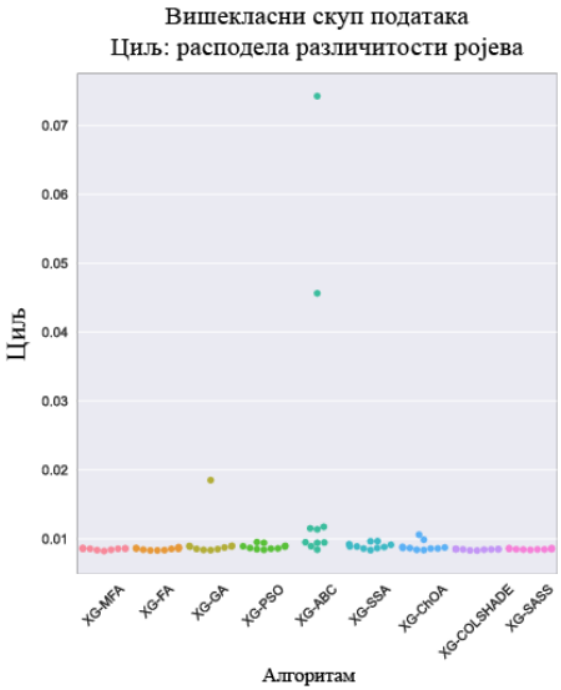
Слика 34 Површина испод криве PR (Precision-Recall) за XG-MFA алгоритам, која илуструје однос између прецизности и одзива у сценаријима са неуравнотеженим класама [13]

Површина испод криве *ROC* (Receiver Operating Characteristic) са макро и микро просецима за предложени *XG-MFA* алгоритам показује перформансе у оквиру разноликих прагова дате класификације. Високе вредности указују на тачност и прецизност алгоритма приликом класификације безбедносних инцидената у дистрибуираном систему.



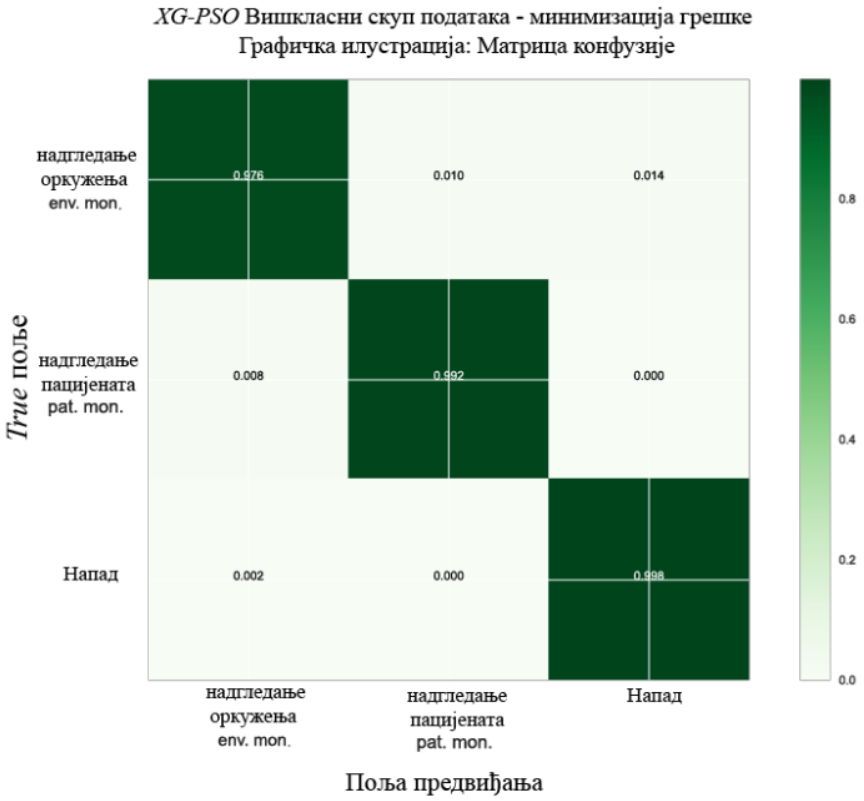
Слика 35 Површина испод криве ROC (енгл. Receiver Operating Characteristic) са макро и микро просецима за XG-MFA алгоритам, омогућавајући процену перформанси у различитим праговима класификације [13]

Наредна графика приказује дијаграм различитости појева. Приказују се густина и расподела објективних вредности за различите алгоритме. Сваки алгоритам је представљен другом бојом, а тачке на дијаграму представљају резултате постигнуте током вишеструког броја итерација. Дијаграм показује како се резултати алгоритама могу разликовати услед варијабилности, при чему неки од алгоритама могу показивати значајнију стабилност у поређењу с другим.



Слика 36 Дијаграм различитости појева за објективне вредности, који визуализује густину и расподелу резултата међу различитим алгоритмима [13]

Наредни графикон, као и претходне матрице конфузије *XG-MFA* алгоритам приказује тачна и нетачна предвиђања за различите класе. Вредности унутар матрице показују колико су предвиђања модела била тачна (дијагонални елементи) у поређењу са предвиђањем (вандијагонални елементи). Дата матрица може помоћи приликом идентификације области у којима модел најчешће може грешити. Тиме се може постећи боље разумевање на који начин је могуће извршити даљу оптимизацију и побољшање тачности модела.

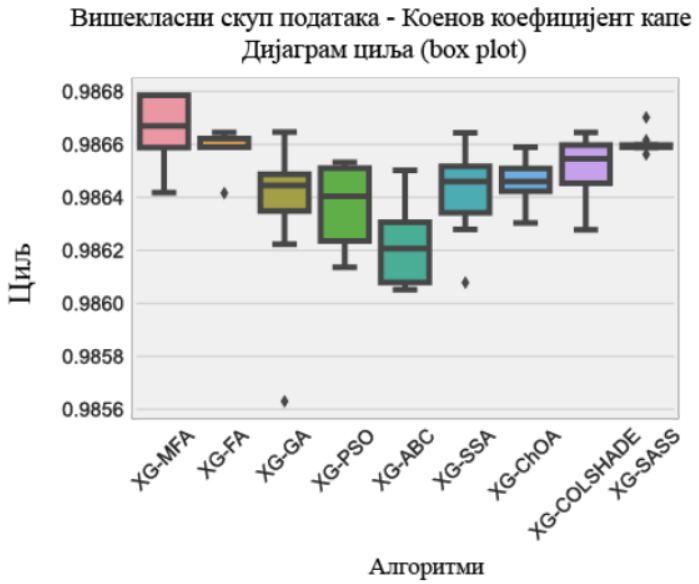


Слика 37 Матрица конфузије за XG-MFA алгоритам, која приказује тачна и нетачна предвиђања за различите класе, помажући тиме идентификације области где модел најчешће греши [13]

Наредни графикони пружају свеобухватан увид у ефикасност и стабилност различитих алгоритама. Свако од датих визуалних приказа помаже приликом идентификације кључних предности и једноставније даје увид у слабости сваког метода. Све графичке илустрације заједно омогућавају сврсисходнију анализу како би се утврдило који алгоритам може пружати најбоље резултате у контексту вишекласне класификације. Поред тога, дати графикони олакшавају поређење различитих приступа и њихову примену у пракси.

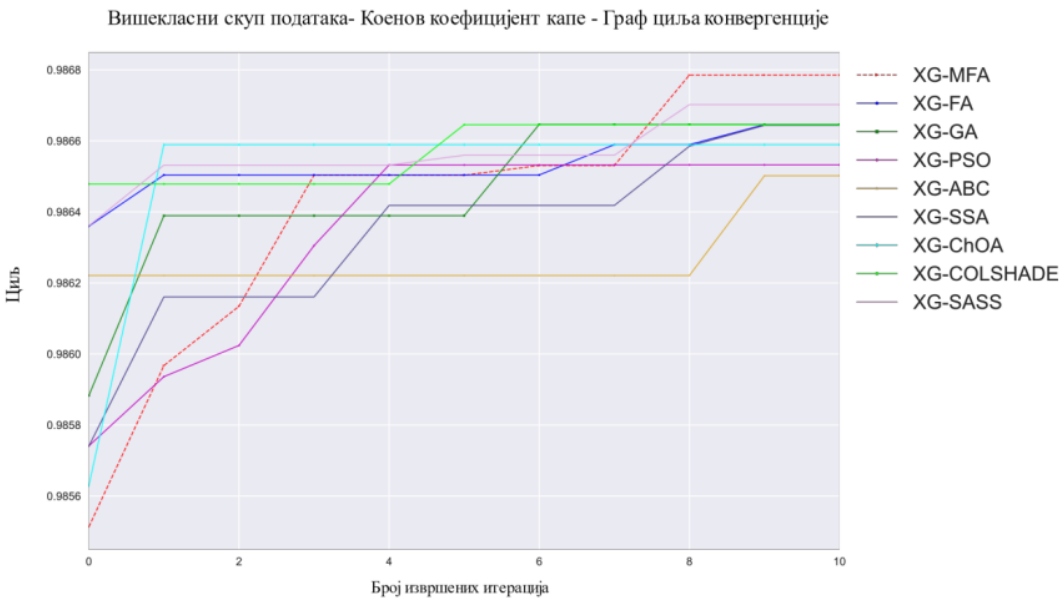
Наредни графикони суштински илуструју максимизацију вредности Коеновог капа коефицијента у вишекласној класификацији.

Дијаграм циља за вредности вишекласног скупа података различитих алгоритама илуструје варијације перформанси међу алгоритмима помоћу Коеновог коефицијента капе. Овај дијаграм указује на то како се алгоритми могу рангирати на основу перформанси, а у поређењу са *XG-MFA* алгоритмом који показује највиши степен стабилности и прецизности.



Слика 38 Дијаграм циља за вредности вишекласног скупа података различитих алгоритама, који помоћу Коеновог коефицијента капе [13]

Слика 39 представља графикон конвергенције за вишекласни скуп података. Приказује се како се резултати различитих алгоритама могу побољшавати током итерација. Свака линија графикона представља посматрани алгоритам, док вертикална оса показује вредности Коеновог коефицијента капе. На основу датог графикона се може закључити да алгоритам *XG-MFA* постиже стабилне и високе резултате током свих итерација, док други алгоритми указују на различите нивое конвергенције и стабилности (или нестабилности).



Слика 39 Графикон конвергенције вишекласног скупа података током итерација, илуструјући како се резултати мењају кроз више итерација [13]

Наредна слика приказује *PR* (Precision-Recall) криву за вишекласни скуп података помоћу Коеновог коефицијента капе, користећи модел *XG-MFA*. Крива PR представља графички приказ односа између прецизности (precision) и одзива (recall) за различите прагове одлучивања.

На *X* оси приказује се одзив (recall), док се на *Y* оси приказује прецизност (precision). Крива је конструисана тако што се мења праг одлучивања модела, при чему се бележе вредности датог тренутка у виду прецизности и одзива.

Легенда датог графикона садржи скраћенице:

- Просечна прецизност за класификацију у оквиру надгледања окружења (env. *mon. AP: Environmental monitoring Average Precision*),
- Просечна прецизност за класификацију у оквиру надгледања пацијената (енгл. *pat. mon. AP: Patient monitoring Average Precision*),
- Просечна прецизност за класификацију напада (енгл. *attack AP: Attack Average Precision*)
- Микро просечна прецизност, која узима у обзир све појединачне примере без претходног осврта на класу (енгл. *micro AP: Micro Average Precision*)

На графикону се могу видети четири линије:

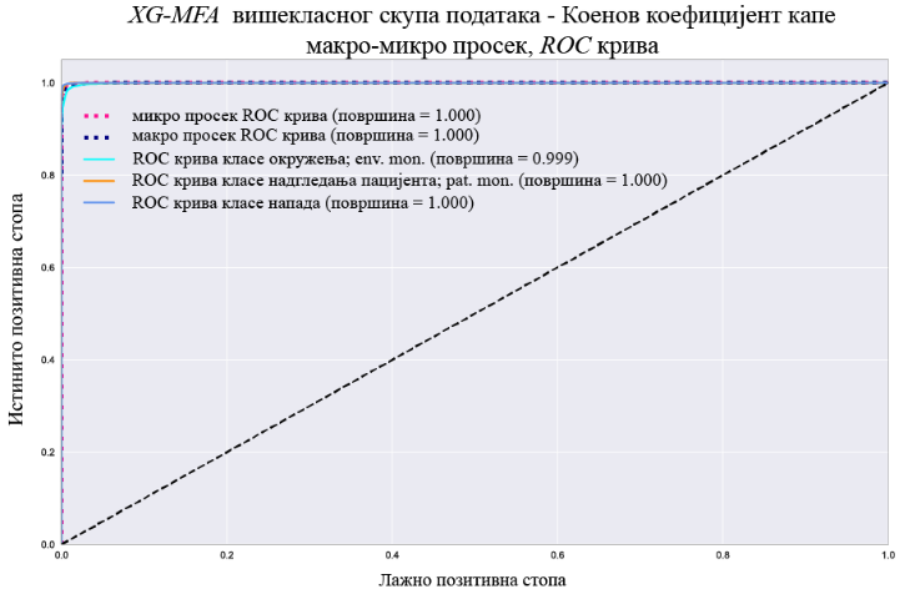
- Плава линија представља криву за просечну прецизност за класификацију, са вредношћу 0.998; указује на високу прецизност у класификацији примера за надгледање окружења.

- Зелена линија представља криву за просечном прецизношћу за класификацију у оквиру надгледања пацијената са вредношћу 1.000; указује на савршену прецизност у класификацији примера за надгледање пацијената.
- Црвена линија представља криву за просечну прецизност за класификацију напада са вредношћу 1.000; указује на савршену прецизност у класификацији примера напада.
- Љубичаста линија представља микро просечну прецизност са вредношћу 1.000; указује на савршену прецизност у укупном просеку свих класификација.



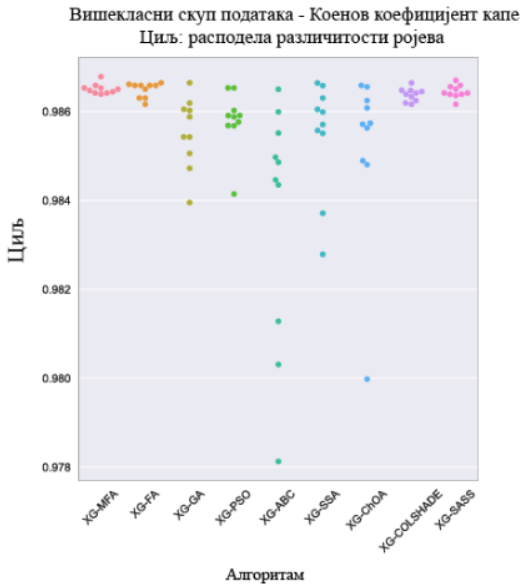
Слика 40 Површина испод криве Precision-Recall, која приказује однос прецизности и одзива за XG-MFA алгоритам, важан за процену модела са неуравнотеженим класама [13]

Слика 41 приказује површину испод криве (ROC). Илуструје се како различити алгоритми могу балансирати између истинито позитивних и лажних позитивних предвиђања. Такође, дати графикон приказује микро и макро просек *ROC* криве. Стога, приказују се појединачне *ROC* криве за класе окружења, надгледања пацијената, као и напада. Висока површина испод криве (вредности близу 1.000) практично указује на високе перформансе алгоритма приликом међусобног разликовања разноликих класа.



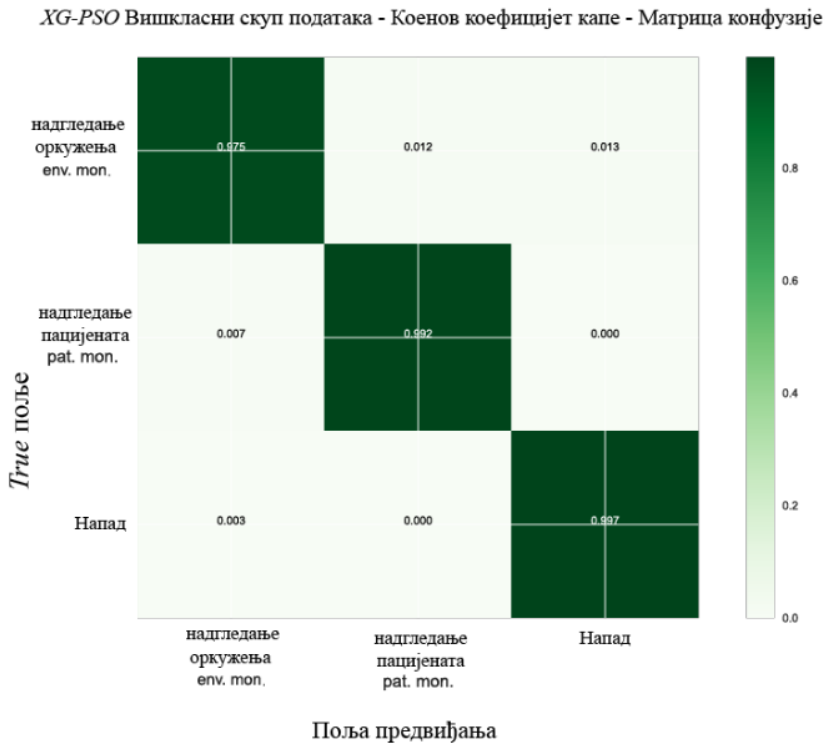
Слика 41 Површина испод криве (енгл. Receiver Operating Characteristic - ROC), приказујући како алгоритам балансира између истинито позитивних и лажних позитивних предвиђања при различитим праговима [13]

Наредна илустрација приказује дијаграм вишекласног скупа података. Приказује се густина резултата, као и распон у погледу перформанси посматраних алгоритама помоћу Коеновог коефицијента капе. Различите боје датог дијаграма представљају различите остварене резултате алгоритама, чиме се, заправо, омогућава сврсисходнија визуелна компарацију перформанси алгоритама. Графикон, даље, приказује како се резултати алгоритама распоређују око одређених вредности, чиме се јасније може идентификовати алгоритам са најстабилнијим и најбољим перформансама.



Слика 42 Дијаграм вишекласног скупа података где се помоћу Коеновог коефицијента капе визуализује густина резултата и распон перформанси различитих алгоритама [13]

У наставку се приказује матрица конфузије која приказује тачну и нетачну класификацију за сваку класу у оквиру вишекласног скупа података. Свакој ћелији матрице одговара број тачних или нетачних предвиђања за одговарајућу комбинацију предвиђаних и стварних класа. Вредности у оквиру матрици показују, заправо, степен прецизности модела која се мери приликом класификације различитих класа. То у будућности може помагати идентификацији области у којима се модел може сусрести са проблемима у погледу тачности.



Слика 43 Матрица конфузије за која приказује детаљне тачне и нетачне класификације за сваку класу [13]

Наредна табела 11 даје на увид детаљан преглед метрика прецизности, одзива и *Ф1*-резултата за различите метахеуристичке методе засноване на *XGBoost* алгоритму за задатке вишеструке класификације. Ове метрике су израчунате за сваку од три класе (0, 1, 2), као и за њихове макро и пондерисане просеке.

Метода *XG-MFA* има највиши макро просек и пондерисани просек у прецизности, одзиву и *Ф1*-резултату, што указује на то да овај метод остварује најбоље укупне перформансе међу свим посматраним методама. Сходно томе, резултат сугерише да је *XG-MFA* способан да одржи високе резултате приликом свих аспекта мерења, што га чини веома поузданим за различите задатке вишеструких класификација.
Поред тога, табела омогућава детаљни увид у перформансе сваког модела по појединачним класама. На пример, метода *XG-GA* остварује најбољи одзив за посматрану класу 0, што значи да је веома ефикасна приликом идентификације позитивних примера у датој класи. Слично томе, *XG-MFA* постиже најбољи одзив за класу 1, што указује на њену супериорност у овој специфичној класи. Са друге стране, *XG-PSO* показује најбоље резултате за класу 2, што указује да је овај метод високо ефикасан приликом идентификовања позитивних примера у овој класи.

Важно је напоменути да оваква анализа може помоћи приликом разумевања моћнијих и слабијих страна сваке методе у оквирима различитих контекста и посматрања. Док *XG-MFA* показује одличне збирне перформансе, друге посматране методе показују да могу бити супериорне у специфичним случајевима, као што је изузетно висока прецизност у одређеним класама. Ово омогућава корисницима да изаберу најприкладнији модел за своје специфичне потребе, што је од суштинске важности за оптимизацију перформанси модела у пракси.

Детаљна анализа података у наредној табели [13] даје резултатски приказ и показује која од посматраних метода јесте најподеснија за специфичне потребе у одговарајућим условима. Поред тога, дата анализа пружа јасан увид у то како различити модели могу обављати послове у различитим сценаријима, што може бити од великог значаја за будућа истраживања и развој нових алгоритама.

На крају, добијени резултати [13] могу бити од суштинске важности за свеукупно унапређење перформанси и поузданости модела, што представља кључ за постизање бољих резултата у различитим технологијама и сферама које су потпомогнуте машинским учењем.

Наредна табела пружа детаљне резултате према различитим класама за моделе вишекласне класификације који остварују најбоље перформансе у симулацији максимизације Коеновог капа коефицијента. Метрика прецизности, одзива и Ф1-резултата су израчунате за сваку од три класе (0, 1, 2), као и за њихове макро и пондерисане просеке.

Метод *XG-MFA* показује најбоље укупне резултате за све класе са највишим вредностима у:

- прецизности,
- одзиву и
- *Ф1*-резултату.

Тиме се указује на то да овај метод може имати тенденцију остваривања најбољих перформанси у различитим сценаријима. Тако, на пример, *XG-MFA* постиже највишу прецизност и *Ф1*-резултат за класу 2, што даље може указивати на његову способност да тачно класификује позитивне примере у датој класи.

Са друге стране, метод *XG-FA* остварује највиши одзив за класу 0 и највишу прецизност за класу 1 [13]. Иако овај метод није имао највише макро просечне и пондерисане просечне вредности, његова специфична ефикасност у овим класама јесте једнако значајна.

Метод *XG-GA* постиже најбољи одзив за класу 0 [13], што може значити да исти може остваривати најбољи исход приликом проналажења свих стварних позитивних примера дате класе. Такође, *XG-PSO* остварује највиши одзив за класу 2, што га представља најефикаснијим приликом прецизне идентификације позитивних примера посматране класе.

Метод *XG-SSA* остварује највиши макро просек за прецизност, што значи да може добро предвиђати позитивне примере у свим класама, без обзира на неуравнотеженост података [13]. Овај метод приказује најбољи одзив за класу 1, што га, заправо, чини веома ефикасним приликом идентификације примера дате класе.

Поред постигнутих резултата у научном истраживању на које се ослања и ова докторска дисертација [13], наредна табела такође пружа јасан увид у контекст који је од изузетно високе важности за разумевање како, заправо, класификација функционише у погледу различитих величина класа.

Сходно томе, дата анализа пружа дубље разумевање перформанси различитих модела и омогућава доношење релевантних одлука о избору најбољег модела за специфичне потребе. Перформансе модела су анализиране кроз различите метрике, чиме се омогућава свеобухватна процена њихове ефикасности [13].

Табела 11 Детаљни резултати по класама за најбоље извођење модела вишекласне класификације - симулација максимизације Коеновог капа коефицијента [13]

Метод	Метрика	0	1	2	Макро просек	Пондерисана просечна вредност
XG-MFA	прецизснот	0.976446	0.991833	0.997704	**0.988661**	**0.991736**
	recall	0.974601	**0.996094**	0.994342	0.988346	**0.991733**
	f1-резултат	**0.975523**	**0.993959**	0.99602	**0.988501**	**0.991731**
XG-FA	прецизснот	0.975333	0.992213	0.99758	0.988375	0.991651
	одзив	0.975231	0.995357	0.994592	0.988393	0.991644
	f1-резултат	0.975282	0.993782	**0.996084**	0.988383	0.991646
XG-GA	прецизснот	0.975142	0.992085	**0.997788**	0.988338	0.991655
	одзив	**0.975756**	0.9954	0.994342	**0.988499**	0.991644
	f1-резултат	0.975449	0.99374	0.996062	0.988417	0.991647
XG-PSO	прецизснот	0.975223	**0.992467**	0.997206	0.9883	0.991578
	одзив	0.974916	0.995226	0.994675	0.988272	0.991574
	f1-резултат	0.97507	0.993846	0.995939	0.988285	0.991574
XG-ABC	прецизснот	**0.976521**	0.99183	0.997247	0.988533	0.991554
	одзив	0.973447	0.995704	0.994758	0.98797	0.991556
	f1-резултат	0.974981	0.993763	0.996001	0.988247	0.991552
XG-SSA	прецизснот	0.976333	0.992086	0.997289	0.98857	0.991644
	одзив	0.974181	0.995617	0.994758	0.988186	0.991644
	f1-резултат	0.975256	0.993849	0.996022	0.988376	0.991642
XG-ChOA	прецизснот	0.975126	0.992086	0.997704	0.988305	0.991617
	одзив	0.975126	0.995573	0.994342	0.988347	0.991609
	f1-резултат	0.975126	0.993827	0.99602	0.988324	0.991611
XG-COLSHADE	прецизснот	0.975535	0.992086	0.997621	0.988414	0.991651
	одзив	0.975126	0.995573	0.994425	0.988375	0.991644
	f1-резултат	0.975331	0.993827	0.996021	0.988393	0.991645
XG-SASS	прецизснот	0.975436	0.992173	0.997663	0.988424	0.991687
	одзив	0.975231	0.995704	0.994342	0.988426	0.99168
	f1-резултат	0.975333	0.993935	0.996	0.988423	0.991681
	Подршка (support)	9528	23,043	24,038	56,609	56,609

Табела 12 представља сажетак хиперпараметара који се користе приликом евалуације вишекласне класификације према коефицијенту Коенове капе. Сваки ред у табели представља један метод и његове одговарајуће вредности хиперпараметара. Такође, хиперпараметри представљају кључ за подешавање перформанси модела, а њихова оптимизација може значајно побољшати свеукупну тачност и ефикасност класификације. У наставку се могу видети постигнути резултати експеримента [13]:

- Метод *XG-MFA* има стопу учења од 0.780152, минималну тежину детета од 1.000000, подузорак од 1.000000, број колона према стаблу од 1.000000, максималну дубину стабла од 9 и гама параметар од 0.517589. Дати метод је представља одличне резултате у разноликим тестовима.
- Метод *XG-FA* има стопу учења од 0.900000, минималну тежину детета од 1.265482, подузорак од 1.000000, број колона према стаблу од 0.983060, максималну дубину стабла од 9 и гама параметар од 0.222017. Посматрани метод се издваја у односу на друге својим прилагођеним вредностима хиперпараметара.
- Метод *XG-GA* има стопу учења од 0.506328, минималну тежину детета од 1.000000, подузорак од 0.816145, број колона према стаблу од 0.945690, максималну дубину стабла од 10 и гама параметар од 0.800000. Метод се резултује тако да има способност да добро функционише са мањим стопама учења.
- Метод *XG-PSO* има стопу учења од 0.837106, минималну тежину детета од 1.000000, подузорак од 1.000000, број колона према стаблу од 1.000000, максималну дубину стабла од 10 и гама параметар од 0.559077. Посматрани метод је показује изразито добру стабилност у разним тестовима.
- Метод *XG-ABC* има стопу учења од 0.566515, минималну тежину детета од 2.084170, подузорак од 0.989990, број колона према стаблу од 1.000000, максималну дубину стабла од 10 и гама параметар од 0.569104. На основу резултата, посматрани метод има високе вредности за неке хиперпараметре, што значајно може утицати на његове перформансе.
- Метод *XG-SSA* има стопу учења од 0.897294, минималну тежину детета од 1.103403, подузорак од 1.000000, број колона према стаблу од 1.000000, максималну дубину стабла од 10 и гама параметар од 0.612487. Резултат методе огледа се у изразитој ефикасности у разноликим сценаријима.
- Метод *XG-ChOA* има стопу учења од 0.900000, минималну тежину детета од 1.000000, подузорак од 1.000000, број колона према стаблу од 1.000000, максималну дубину стабла од 9 и гама параметар од 0.800000. Доказује се да метод има конзистентне вредности хиперпараметара.
- Метод *XG-COLSHADE* има стопу учења од 0.465601, минималну тежину детета од 3.091252, подузорак од 1.000000, број колона према стаблу од 1.000000, максималну дубину стабла од 9 и гама параметар од 0.800000. Метод има специфичне вредности које га издвајају од осталих, у виду ефикасности, тачности, као и класификација података.

- Метод *XG-SASS* има стопу учења од 0.900000, минималну тежину детета од 1.107956, подузорак од 1.000000, број колона према стаблу од 1.000000, максималну дубину стабла од 9 и гама параметар од 0.800000. Метод остварује високу ефикасност и стабилност током предефинисаних тестова.

Табела 12 Најбоље добијени модели хиперпараметара за вишекласну класификацију у оквиру експеримента за максимизацију Коеновог капа коефицијента [13]

Метод	Стопа учења	Минимална тежина детета	Подузорак	Број колона по стаблу	Максимална дубина	Гама
XG-MFA	0.780152	1.000000	1.000000	1.000000	9	0.517589
XG-FA	0.900000	1.265482	1.000000	0.983060	9	0.222017
XG-GA	0.506328	1.000000	0.816145	0.945690	10	0.800000
XG-PSO	0.837106	1.000000	1.000000	1.000000	10	0.559077
XG-ABC	0.568515	2.084170	0.989990	1.000000	10	0.569104
XG-SSA	0.897294	1.103403	1.000000	1.000000	10	0.612487
XG-ChOA	0.900000	1.000000	1.000000	1.000000	9	0.800000
XG-COLSHADE	0.465601	3.091252	1.000000	1.000000	9	0.800000
XG-SASS	0.900000	1.107956	1.000000	1.000000	9	0.800000

11.2 Статистички модел као механизам потврде достигнутих резултата

Како би се додатно проценили експериментални резултати и успоставила њихова статистичка важност, прикупљени су и анализирани најбољи резултати добијени из тридесет независних експеримената, односно, поновног покретања сваког алгоритма који се узима у обзир и који се може представити као серија података. Први корак у овом поступку укључује одређивање одговарајућег типа статистичког теста, односно, разматра се да ли би требало користити параметарске или непараметарске тестове.

Сходно томе, прикладност параметарских тестова може се проценити испитивањем:

- независности,
- нормалности и
- хомоскедастичности варијансе (хомогености варијансе) у подацима [53].

Критеријум независности је задовољен јер свако појединачно покретање метахеуристике може почети са генерисањем насумичним, односно, случајним скупом решења.
У датом поступку, анализа варијансе (енгл. *ANOVA*) може бити примењена уколико су подаци нормално распоређени и хомоскедастични. Уколико дати услови нису испуњени, тј. у случају да претпоставка нормалности не може бити или није испуњена, користе се непараметарски тестови као што је Крускал-Валисов тест. Како би се проверила нормалност података, могу се користити тестови као што су Шапиро-Вилк тест или Колмогоров-Смирнов тест. Такође, хомоскедастичност варијансе се испитује Лејновим тестом или Бартлетовим тестом.

Поред тога, како би се пар алгоритма могао упоређивати, може се размотрити примена пост-хок анализе. Поменута анализа омогућава детаљније увид у то који алгоритми имају значајно боље или лошије перформансе у поређењу са другим алгоритмима. На пример, Тукијев тест или Дунканов тест могу бити коришћени за поменути тип анализе.

У случају да су подаци хетероскедастични или не прате нормалну дистрибуцију, могу се применити одговарајући непараметарски тестови. Такав приступ може осигурати тачнију и прецизнију процену резултата, са посебним освртом на значајност истих.
Такође, значајан поступак приликом анализе података јесте израчунавање коефицијента варијације, помоћу кога се омогућава поређење степена варијабилности између различитих сетова података. Ово је нарочито корисно приликом поступака поређења резултата алгоритама који могу показивати различите нивое перформанси.

Сходно свему претходно наведеном, статистичка валидација, не само да обезбеђује позитивно мишљење у поузданост остварених резултата, већ може пружити основу за одређивање који алгоритми могу пружати најбоље резултате под различитим околностима, тј. условима. Дата свеобухватна анализа омогућава комплексније

разумевање перформанси алгоритама и идентификацију потенцијалних области за побољшање истог.

Процена претпоставке нормалности је извршена коришћењем Шапиро–Вилковог теста, са индивидуалном анализом проблема [54] за сва четири експеримента која су спроведена у оквиру истраживања, а на које се ослања докторска дисертација [13]. Спроведени тестови су:

- бинарна класификација (са грешком и Коеновим коефицијентом капе као циљевима) и
- вишекласна класификација (са грешком и Коеновим капа коефицијентом као циљевима).

Шапиро–Вилков тест је примењен независно на сваки од алгоритама у овом експерименталном поступку [13], а на основу ког се заснива ово научно истраживање. Укупно су разматрана четири сценарија. За сваки од њих су генерисане *p*-вредности. У свим случајевима, резултујуће *p*-вредности биле су мање од 0.05. Такав резултат указује да нулта хипотеза (H0) може бити одбачена. На основу резултата експеримента, може се извести закључак да посматрани подаци не прате нормалну дистрибуцију у сва четири сценарија. Добијени резултати су кључни, јер могу указивати на предност употребе непараметарских метода за даљу анализу. Такође, тестови су показали да алгоритми раде конзистентно у сваком од сценарија, али је примена Шапиро–Вилковог теста неопходна да би се обезбедила тачност закључака. Додатно, резултати ових тестова помажу у бољем разумевању природе података и неопходности коришћења одговарајућих статистичких метода.

Поред тога, циљ примене датог теста јесте процена да ли су посматрани подаци у релевантном складу са нормалном расподелом, што је корак од важности приликом одабира одговарајућих статистичких тестова за даљу и будућу анализу. Уколико подаци не прате нормалну дистрибуцију, потребно је размотрити алтернативне тестове који не претпостављају нормалност, као што су непараметарски тестови.

Уколико се нулта хипотеза одбаци, што је случај у овом научном истраживању [13], на које се примарно ослања докторска дисертација, тиме се указује на изузетно високу потребу за коришћењем специфичних методологија које могу бити отпорне на одступања од нормалности. Тиме се може укључивати употребу робусних статистика или примена разноликих трансформација података, а са циљем свеукупног побољшања нормалности дистрибуције истих.

Такође, од важности је напоменути да остварени резултати Шапиро–Вилковог теста могу пружити јасан увид у природу дистрибуције података. То даље имплицира да се може утицати на интерпретацију и валидност закључака добијених на основу датих експеримената [13].

Стога, утврђивање нормалности података јесте кључни корак у датој статистичкој анализи који пружа могућности одабира најприкладнијих метода за анализу посматраних података, уз доношење веродостојних закључака.

Табела 13 пружа детаљне резултате Шапиро-Вилкових тестова нормалности за различите проблеме и методе [13]. Дати тестови користе се за процену да ли подаци могу пратити нормалну дистрибуцију за различите алгоритме засноване на *XGBoost*-у, укључујући *XG-MFA, XG-FA, XG-GA, XG-PSO, XG-ABC, XG-SSA, XG-ChOA, XG-COLSHADE* и *XG-SASS*. Шапиро-Вилков тест је извршен за сваки алгоритам у четири различита сценарија:

1. бинарна грешка,
2. бинарни капа коефицијент,
3. вишекласна (мултикласна) грешка и
4. вишекласни (мултикласни) капа коефицијент.

Вредности у табели представљају *p*-вредности добијене из датих тестова. Све *p*-вредности имају вредности мање од 0.05, што даље може указивати да нулта хипотеза нормалности може бити одбачена у свим случајевима. У пракси то значи да подаци не прате нормалну дистрибуцију ни у једном од разматраних сценарија.

Дата анализа нормалности података је кључна за одређивање релевантних статистичких метода које би требало применити у будућој анализи. Уколико се подаци не распоређују нормално, неопходно је користити непараметарске тестове или друге методе које не захтевају нормалност. Тиме се може обезбедити да резултати анализе буду поуздани и валидни.

Такође, дата табела приказује важност теста нормалности података пре него што се настави са другим релевантним статистичким тестовима. Осим што табеларни приказ помаже у избору правих метода за анализу, иста може пружати јасан увид у структуру и природу података. То може бити од користи приликом бољег разумевања проблема и интерпретације резултата.

Табела 13 Резултати Шапиро-Вилкових тестова нормалности за различите XGBoost алгоритме у различитим сценаријима [13]

Проблем	XG-MFA	XG-FA	XG-GA	XG-PSO	XG-ABC	XG-SSA	XG-ChOA	XG-COLSHADE	XG-SASS
Бинарна грешка	0.048	0.041	0.045	0.038	0.036	0.032	0.043	0.026	0.019
Бинарна Капа	0.042	0.042	0.040	0.036	0.039	0.033	0.045	0.035	0.026
Вишекласна грешка	0.021	0.030	0.042	0.031	0.043	0.025	0.019	0.020	0.023
Вишекласна Капа	0.035	0.038	0.021	0.040	0.035	0.029	0.042	0.027	0.030

Услед тога што услов нормалности није испуњен, самим тим се може истаћи да није безбедно примењивати параметарске тестове. Стога, настављена је примена непараметарског Вилкоксоновог теста [13] са рангирањем [55], помоћу идентичне серије података која обухвата најбоље добијене вредности приликом сваког покретању алгоритма. На основу научног истраживања на коме се заснива докторска [13] предложена *MFA* метода представља се као контролна метода. Сходно томе, Вилкоксонов тест са рангирањем је спроводи се над посматраном серијом података. У свим видовима датих поступака, израчунате *p*-вредности остварују резултате мање од 0.05, за сва четири посматрана сценарија. Резултати као такви могу недвосмислено указивати на то да је увођење *MFA* методе статистички вишеструко побољшало перформансе у односу на све конкурентне методе, тако и за праг (ниво) значајности $\alpha=0.1$ и $\alpha=0.05$ [13].

Поред тога, добијени резултати потенцирају супериорност *MFA* методе у свим анализираним сценаријима [13]. Вилкоксонов тест са рангирањем омогућава извођење закључака о статистичкој значајности перформанси, без обзира на евентуална одступања од нормалности података. Ово је од изузетне важности приликом потврде да свеукупна побољшања нису случајна, већ да она представљају збирни резултат ефективности уведене методе.

Резултати датог теста су релевантни, не само приликом процене перформанси у контексту овог истраживања [13], а на које се ослања докторска дисертација, већ исти могу имати значајно ширу примену у другим областима где је потребно исправно проценити и упоредити методе. С тим у вези, добијени резултати могу бити основа за будућа истраживања и унапређење метода анализе података. Тиме се може додатно потврдити важност коришћења статистички значајних метода приликом валидације резултата у научним оквирима и новим научним достигнућима.

Остварени резултати [13] могу пружити позитивно запажање да *MFA* метода није само боља у просеку, већ и да може остваривати стабилније перформансе остварујући их кроз разнолике услове и сценарије. Ово може бити од кључне важности приликом примене у стварним ситуацијама где је потребна конзистентност и поузданост релевантне методе.

Табела 14 Резултати Вилкоксоновог теста са рангирањем за процену статистичке значајности перформанси XG-MFA методе у односу на конкурентске методе у различитим сценаријима [13]

Проблем/ꝑвредности	XG-FA	XG-GA	XG-PSO	XG-ABC	XG-SSA	XG-ChOA	XG-COLSHADE	XG-SASS
Бинарна грешка	0.016	0.037	0.028	0.008	0.025	0.031	0.034	0.031
Бинарна Капа	0.025	0.036	0.026	0.027	0.031	0.029	0.040	0.039
Вишекласна грешка	0.034	0.035	0.030	0.019	0.035	0.035	0.041	0.027
Вишекласна Капа	0.040	0.026	0.028	0.024	0.042	0.036	0.038	0.033

Формулација и поимање резултата најуспешнијих модела *SHAP* анализа је препозната као механизам за свеобухватно унапређење транспарентности перформанси модела. Такође, омогућавају се различите две анализе помоћу *SHAP*-а за извршене експерименте [13]. Утврђује се важност карактеристика *XGBoost* модела. Сходно томе, важност се може одређивати на основу тежине процењених чворова, при чему се већа важност приписује чворовима од којих посматрања више зависе. Важност се може израчунати на једном одлучујућем стаблу и затим се просечно вреднује преко свих преосталих стабала.

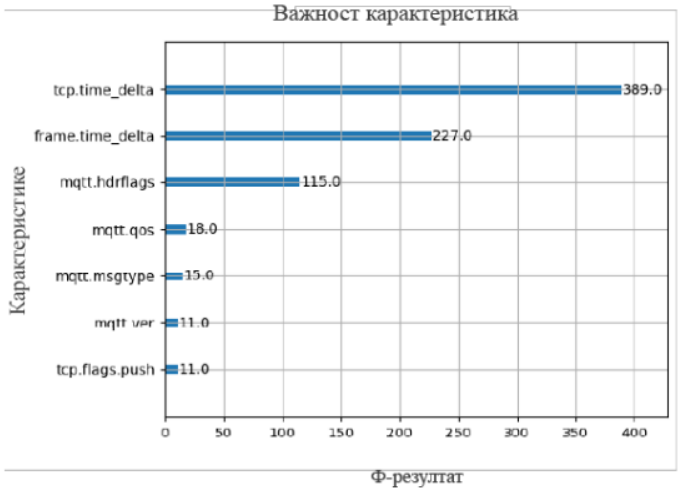
Резултати приказани на Слици 7a сугеришу да на основу важности коју одређује *XGBoost*, *tcp.time_delta* има високу улогу у одређивању исхода у бинарној класификацији, а затим следе карактеристике *frame.time_delta, mqtt.hdrflags* и *mqtt.msgtype*. Иако су разматране и додатне карактеристике, оне су показале мању важност. Слични резултати су приказани и за вишекласну класификацију на Слици 7b, где *tcp.time_delta* приказује изузетно високу важност приликом одређивању исхода. Међутим, у односу на важност у бинарној класификацији, утицај јесте нешто нижи. Ову карактеристику такође прате *frame.time_delta* и *mqtt.hdrflags*, који у датој илустрацији показују већи утицај у односу на бинарну класификацију.

Поред ових карактеристика, од користи је видети и утицај других мање значајних карактеристика. Вредно је помена да је процена важности варијабли такође битна за разумевање доприноса сваке промењиве у моделовању. Додатно, ови резултати могу помагати у фином подешавању модела и побољшању његових перформанси у будућности. Анализа важности карактеристика може открити и потенцијалне прилике за уклањање нерелевантних или мање битних променљивих (варијабли), што би могло поједноставити модел и значајно допринети убрзавању времена израчунавања.

Наредна слика приказује важност различитих карактеристика у моделима бинарне и вишекласне класификације заснованим на *XGBoost*-у [13]. Дати графикони омогућавају једноставније разумевање које карактеристике највише могу допринети одлукама модела.

На графикону се може видети важност карактеристика у моделу бинарне класификације. Најзначајнија карактеристика је *tcp.time_delta* са оценом важности од 519.0, што указује на то да ова карактеристика има највећи утицај на посматрани модел. Следе

frame.time_delta са оценом 311.0 *mqtt.hdrflags* са оценом 81.0, и *mqtt.msgtype* са оценом 31.0. Преостале карактеристике, као што су *mqtt.qos*, *tcp.flags.push*, *mqtt.ver, mqtt.retain,* и *tcp.flags.ack*, имају мању важност, али се и даље узимају у обзир у датом моделу [13].

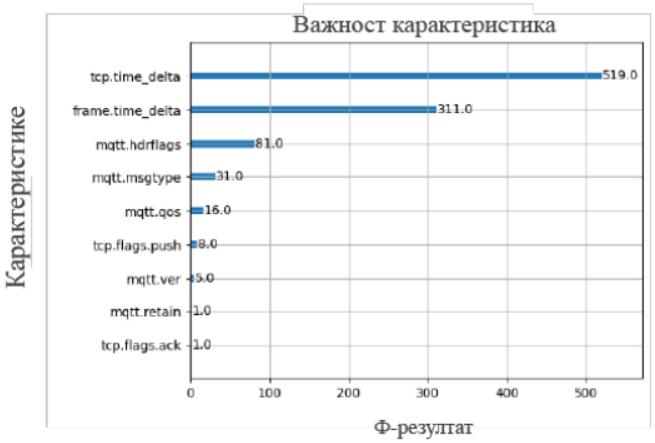


Слика 44 Интерпретација важности карактеристика у бинарној и вишекласној класификацији помоћу XGBoost-а [13]

На наредном графикону може се видети важност карактеристика у моделу вишекласне класификације. Као и у претходном случају, на датом графикону је *tcp.time_delta* најзначајнија карактеристика са оценом 389.0, али је њена важност мања у поређењу са бинарном класификацијом. *frame.time_delta* је друга по важности са оценом 227.0. *mqtt.hdrflags* је следећа са оценом 115.0, док остале карактеристике, као што су *mqtt.qos*, *mqtt.msgtype, mqtt.ver*, и *tcp.flags.push*, имају релативно мању важност, али су и даље од значаја за дати модел [13].

Сврха ове анализе важности карактеристика јесте пружање бољег и јаснијег увида у то како модели *XGBoost* могу доносити одлуке и које карактеристике највише могу утицати на њихова предвиђања. Стога, ово може бити од користи за будућу оптимизацију модела, као и за идентификацију кључних променљивих које могу бити од значаја за детаљнију интерпретацију података. На основу ових резултата, могу се предузети кораци за даље унапређење модела и боље разумевање података.

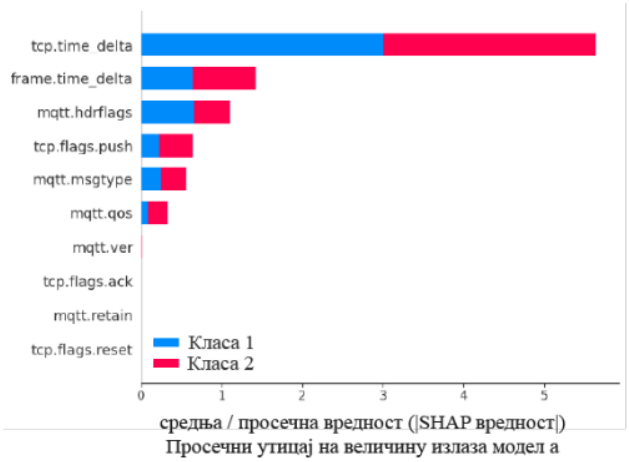
Одређена карактеристика [13] за најуспешније реализоване моделе у оба обављена експеримента могу се видети на наредној илустрацији.



Слика 45 Интерпретација важности карактеристика у бинарној и вишекласној класификацији помоћу XGBoost-а [13]

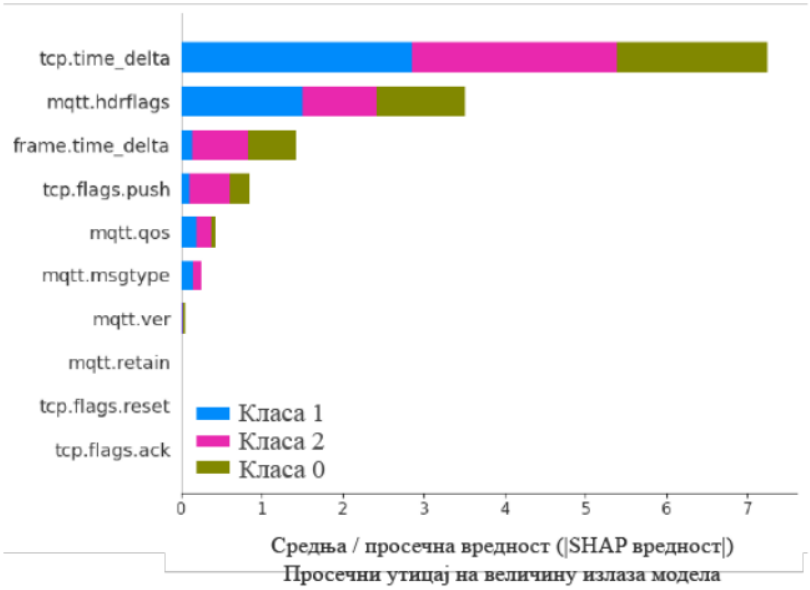
У наставку, наредне слике приказују утицај различитих карактеристика на излаз модела користећи *SHAP* (енгл. *SHapley Additive exPlanations*) анализу [13]. Оваква анализа омогућава сврсисходнији увид у то како различите карактеристике могу утицати на предикције (предвиђања) модела, како у бинарној, тако и у вишекласној класификацији. Целокупна анализа јесте интуитиван и снажан механизам за боље и једноставније превиђање модела машинског учења.

Графикон илуструје *SHAP* вредности за бинарну класификацију. На истом се може видети да карактеристика *tcp.time_delta* има највећи просечни утицај на излаз модела, са значајним доприносом обе класе (Класа 1 и Класа 0). У датом графикону може се видети да карактеристика *frame.time_delta* јесте, заправо, друга најважнија карактеристика и да као таква има веома значајан утицај на обе посматране класе. Даље, карактеристика *mqtt.hdrflags* потврђује да има већи утицај на класу 1, док остале карактеристике, тј. *tcp.flags.push, mqtt.msgtype*, и *mqtt.qos* имају већи утицај на класу 0. Овакав резултат указује да су одлуке модела за класе 1 и 0 подједнако зависне од одређених карактеристика, али са диференцијалним степеном потенцијала, односно, утицаја на различите класе [13]. Такође, може се извести тврдња да је модел осетљив на специфичне карактеристике које различито утичу на класификационе одлуке за класе 0 и 1.



Слика 46 SHAP анализа утицаја карактеристика у бинарној и вишекласна класификацији помоћу XGBoost-а [13]

Наредни графикон приказује *SHAP* вредности за вишекласну класификацију. Карактеристика *tcp.time_delta* поново преовладава као најзначајнија карактеристика са највећим утицајем, али се на основу датог приказа може видети и њен већи допринос класи 2 и класи 0. С друге стране, карактеристика *mqtt.hdrflags* јесте друга најважнија карактеристика и показује значајан утицај на све три класе, али највише на класу 1. Преостале карактеристике *frame.time_delta* и *tcp.flags.push* такође показују велики утицај на све три класе, са разноликим степеном утицаја. Оваква анализа помаже приликом бољег разумевања како различите карактеристике могу утицати на одлуке модела за сваку класу засебно [13].



Слика 47 SHAP анализа утицаја карактеристика у бинарној и вишекласној класификацији помоћу XGBoost-а [13]

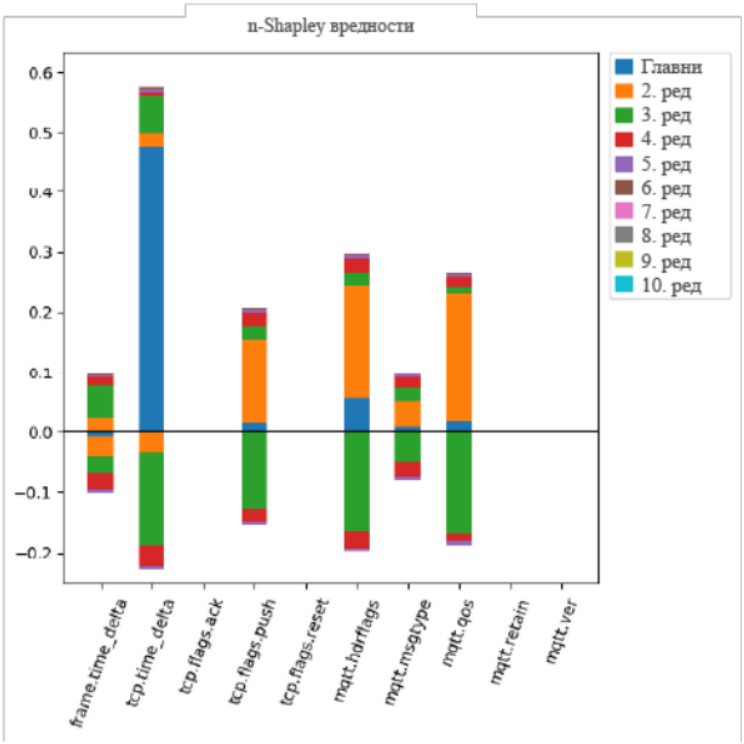
Сврха *SHAP* анализе јесте пружање транспарентности приликом функционисања модела омогућавајући прецизније разумевање на који начин карактеристике утичу могу утицати предвиђања. Таква анализа може бити посебно корисна за даљу оптимизацију модела, као и за идентификацију кључних карактеристика које могу бити од значаја за будућа научна истраживања.

Наредна илустрација Слика 48 приказује *nSHAP* анализу 10. реда за бинарну и вишекласну класификацију. Дата анализа на коју се ослања и истраживање у овој докторској дисертацији [13] омогућава да се ближе схвати до ког степена различите особине утичу на одређени резултат, укључујући интеракције до 10. реда. Процес анализе обухвата одвојено испитивање утицаја сваке карактеристике, како би се детаљније разумеле њихове међусобно остварене интеракције и резултати као узроци позитивних индикатора. Такав приступ пружа јасније разумевање како појединачне карактеристике могу допринети моделу и тиме омогућавајући да се уочи скривени обрасци који можда не би били очигледни на први поглед. Сходно датој анализи, може се идентификовати које карактеристике остварују, тј. имају највећи утицај и како њихова интеракција може позитивно утицати на свеукупни исход модела. Поред свега наведеног, дата анализа помаже квалитетнијој и сврсисходнијој оптимизацији модела тако што се превасходно идентификују и уклањају карактеристике које потенцијално могу унети шум или могу имати минималан утицај на исти. Тиме се постиже већа прецизност и ефикасност модела у реалним сценаријима, односно, у пракси. У контексту бинарне класификације, *nSHAP* анализа може бити од изузетне користи приликом асистенције приликом обављања процеса разликовања који атрибути највише могу

допринети одвајању класа, док у вишекласној класификацији може омогућавати боље разумевање како различити фактори утичу на класификацију над више класа. Из претходно наведеног, дата анализа јесте кључна за унапређење транспарентности и поузданости модела, што може бити од суштинског значаја у критичним применама као што су и здравство и безбедност од детекције упада у дистрибуирани систем.

Дакле, наредне илустрацију приказују да обављена анализа *nSHAP* може пружити јасан и детаљан поглед тако да се може ближе разумети начин на који различите карактеристике интерагују и могу утицати на предвиђања модела. Дата анализа не само да омогућава да се разумеју појединачни исходи карактеристика, већ тиме омогућавају бољу идентификацију како се оне међусобно односе и утичу на коначне исходе. Корелације и интерреаговање вишег реда може откривати непосредности и сложености које нису видљиве кроз основну анализу. Поред свега тога, овакав приступ омогућава целокупно побољшање тачности и поузданости модела, јер се тако може боље разумети како различите карактеристике могу доприносити укупним перформансама.

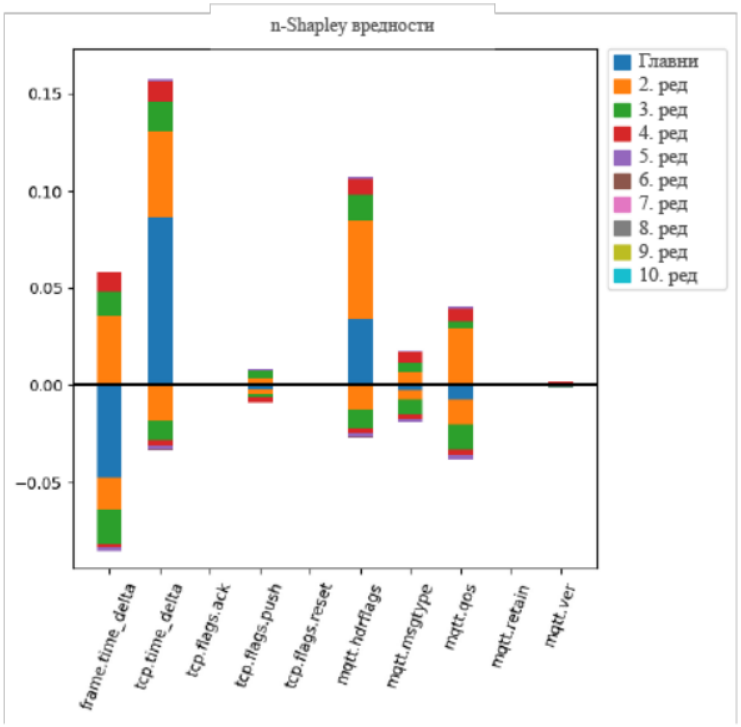
У наставку се приказује графикон [13] који илуструје како карактеристике могу утицати на бинарну класификацију кроз 10 нивоа интеракција, тј. 10 редова. У датом графикону може се видети да *frame.time_delta* и *tcp.time_delta* остварују значајне базне доприносе приликом одређивања исхода, али такође постоје и доприноси вишег нивоа, као што су други, трећи ред итд. Истиче се да је од важности видети да различите особине могу имати различите степене утицаја, кроз различите редове интеракција. Тако, на пример, карактеристике попут mqtt.hdrflags и tcp.flags.push могу имати значајне утицаје на више нивоа, показујући како комплексне синтезе, остварујући бројне интеракције, између карактеристика могу збирно утицати на коначни исход класификације. Дати детаљан увид омогућава свеукупно боље разумевање како појединачне особине и њихове међусобне синтезе могу утицати на модел. Дубља анализа открива да неке карактеристике могу имати изненађујуће велике доприносе у комбинацијама са другим атрибутима, што може истицати важност узимања у обзир виших редова интеракција приликом оптимизацији модела. Информација као таква може бити кључна за фино и напредније подешавање модела, као и за његово побољшање прецизности и робусности.



Слика 48 nSHAP анализа 10. реда за бинарну и вишекласну класификацију са приказом интеракција карактеристика [13]

Наредна слика 49 приказује доприносе карактеристика за вишекласну класификацију до десетог реда. Уочава се сличан образац, где *frame.time_delta* и *tcp.time_delta* остварују ауторитативне улоге, али такође, постоје бројни доприноси вишег реда; карактеристике као што су *mqtt.hdrflags* и *tcp.flags.push* својом синтезом показују значајан утицај кроз више нивоа интеракција. Идентификована анализа омогућава боље разумевање процеса обављања изузетно сложених и комплексних интеракција између карактеристика, а које збирно могу позитивно утицати на предвиђања модела.

Анализа *nSHAP* је извршена за редове од другог до десетог, укључујући *Shapley–Taylor* анализу. Дата анализа омогућава ближе одређивање до које мере различите карактеристике могу допринети одређеном исходу, независно од одређене класификације која спроводи. У датој анализи укупно су спроведене три анализе које су користиле *nSHAP* методологију. Вредности *n-Shapley* до десетог реда су приказују се на слици 49, која, заправо, илуструје како интеракције вишег реда могу приликом коначног исхода утицати на свеобухватне резултате.



Слика 49 nSHAP анализа 10. реда за бинарну и вишекласну класификацију са приказом интеракција карактеристика [13]

У наставку експерименталног поступка, у Табели 15 [13] приказују се перформансе предложеног модела у поређењу са најчешће коришћеним техникама машинског учења за сличне проблеме класификације. Перформансе се процењују помоћу проблема минимизације грешке. На основу тога, резултати потврђују ефикасност новог решења. Предложени *XG-MFA* модел [13] суштински постиже највише оцене за све метрике осим одзива, где је најбољи резултат постиже стабло одлучивања (*DT*). Дата табела омогућава детаљнији приказ у контексту погледа на то како се различити модели машинског учења могу извршавати у реалним сценаријима.
Разматрани су следећи модели машинског учења:

- Алгоритам Наивни Бајес (енгл. *Naive Bayes – NB*),
- Алгоритам К-најближих суседа (енгл. *K-Nearest Neighbors - KNN*),
- Алгоритам насумичне шуме (енгл. *Random Forest - RF*),
- Адаптивно појачавање (енгл. *AdaBoost - AB*),
- Логистичка регресија (енгл. *Logistic Regression - LogR*),
- Стабло одлучивања (енгл. *Decision Tree - DT*) и
- предложени *XG-MFA*.

Сваки од ових модела је оцењен на основу прецизности, одзива, тачности и Ф1-резултата, пружајући свеобухватну слику њихове ефикасности.

Резултати у табели показују да алгоритам Наивни Бајес досеже највећи одзив, али знатно нижи Ф1-резултат и тачност у поређењу са другим моделима. Алгоритам к-најближих суседа (KNN) и алгоритам насумичне (RF) шуме досежу изузетно високу стопу оцене, готово у свим метрика, са Ф1-резултатом преко 99.5%. Алгоритам адаптивног појачавања (AB) такође постиже одличне перформансе, али у поређењу са алгоритмом насумичне шуме (RF) и алгоритмом к-најближих суседа (KNN) ипак су нешто слабије [13].

Логистичка регресија (LogR) показује високе, тј. добре перформансе са тачношћу од 99.5036%, али са нешто нижим Ф1-резултатом приликом поређења са другим моделима [13]. Стабло одлучивања (DT) у датом експерименту постиже најбољи одзив, што даље може указивати на његову изузетну ефикасност у идентификовању позитивних случајева [13] Предложени *XG-MFA* модел има највише оцене у свим категоријама, што потврђује његову супериорност у односу на друге моделе.

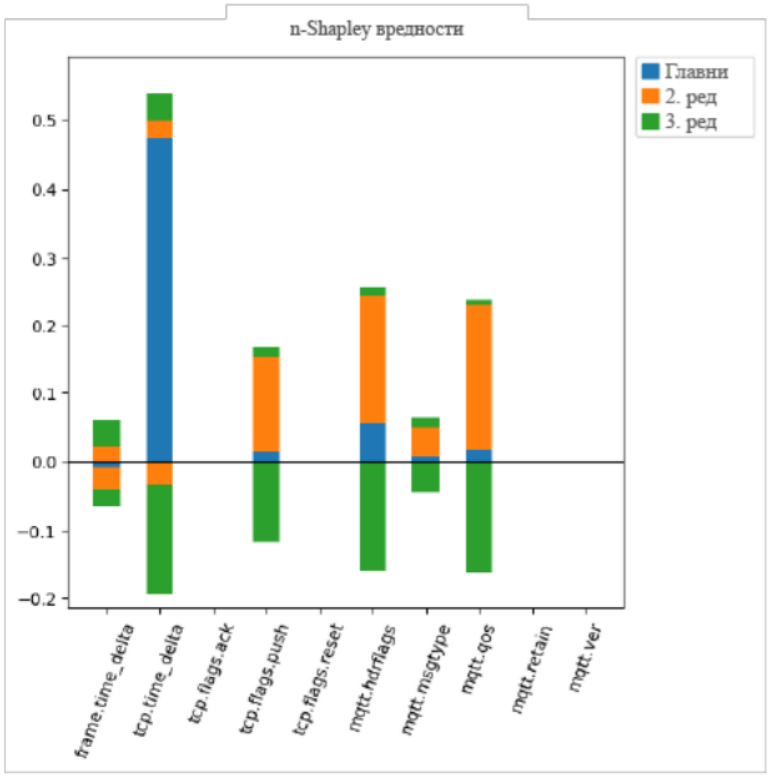
Табела 15 Поређење перформанси различитих модела машинског учења на IoT-Flock здравственом скупу података за предвиђање малициозног и нормалног саобраћаја [13]

Класификатор машинског учења (ML)	Прецизност	Одзив	Тачност	F1-Резултат
NB	79.6712	99.7052	52.1821	68.5093
KNN	99.6501	99.6865	99.4872	99.5868
RF	99.7069	99.7954	99.5121	99.6534
AB	99.5547	99.4457	99.5037	99.4748
LogR	95.2879	90.3515	99.5036	94.7071
DT	99.6945	**99.7992**	99.4788	99.6389
XG-MFA	**99.6998**	99.6997	**99.6997**	**99.6996**

Наредна илустрација приказује резултате *Shapley–Taylor* анализе, која се може користити коришћена за процену утицаја различитих карактеристика на исходе модела у бинарним и вишекласним класификацијама [13]. На слици се приказују главни доприноси карактеристика (означени плавом бојом), као и доприноси другог и трећег реда интеракција између карактеристика (означено наранџастом и зеленом бојом) [13]. Дата анализа значајно доприноси приликом разумевању како различите карактеристике и њихово међусобно интерреаговање утичу на предвиђања модела.

Резултати *Shapley–Taylor* анализе могу се видети на наредној илустрацији, на Слици 10. Дата анализа омогућава јаснији увид у то како различите карактеристике, као и њихове међусобне интеракције, могу утицати на перформансе модела.

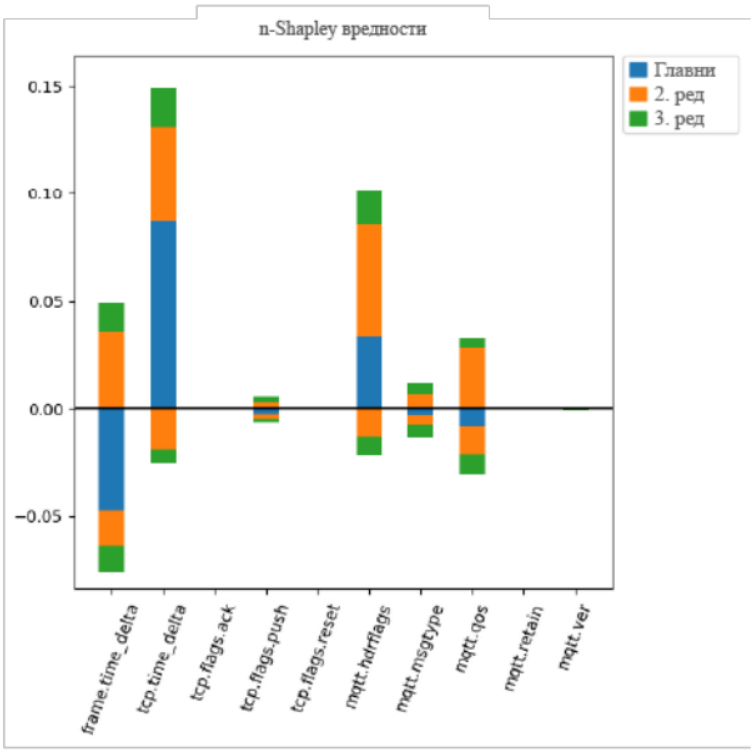
Слика 50 приказује резултате анализе бинарне класификацију, док Слика 51 приказује исте резултате за вишекласну класификацију [13].
У бинарној класификацији (Слика 50), можемо видети да је карактеристика *tcp.time_delta* најзначајнија са највећим главним доприносом (означено плавом бојом). Интеракције другог и трећег реда (означено бојама наранџастом и зеленом) такође значајно доприносе предвиђањима, што даље може указивати на сложене међусобне односе између карактеристика. Карактеристике као што су *frame.time_delta* и *mqtt.hdrflags* такође указују на изузетно значајне доприносе, што даље имплицира да су ове карактеристике од високе важности за постизање тачности модела.



Слика 50 Шапли–Тејлор анализа карактеристика бинарна класификација [13]

За вишекласну класификацију (Слика 51), резултати су слични, али проналазе се поједине разлике у значају карактеристика. Поново *tcp.time_delta* постиже највећи допринос, док се види да интеракције другог и трећег реда постижу значајнији утицај на коначне одлуке модела у односу на посматрану бинарну класификацију. Карактеристика *mqtt.hdrflags* приказује повећану важност у вишекласној класификацији, што имплицира на њену изузетну релевантну корисност приликом одређивања различитих класа.

Постигнути резултати [13] јесу изузетно корисни за даљу оптимизацију модела, јер пружају чвршћи увид у то како различите карактеристике и њихове интеракције утичу на тачност предвиђања.



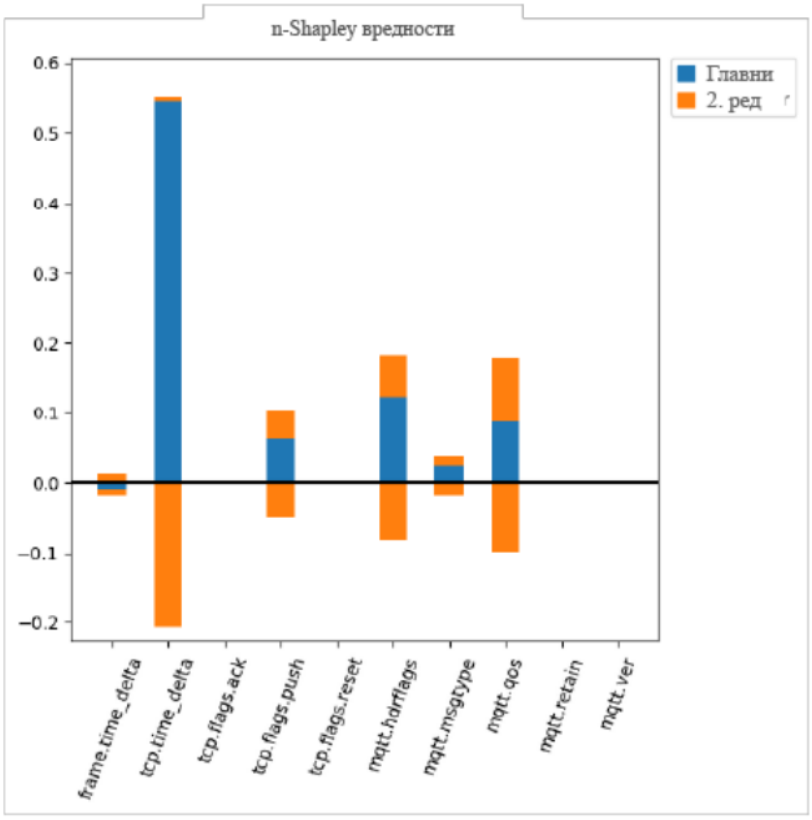
Слика 51 Шапли–Тејлор анализа карактеристика вишекласна класификација [13]

У наставку експерименталног поступка наредна слика [13] приказује *nSHAP* анализу другог реда за различите карактеристике модела, као и њихове интеракције у бинарним и вишекласним класификацијама. На слици се приказују важни доприноси карактеристика (означени плавом бојом) и доприноси другог реда интеракција (означени наранџастом бојом) [13]. Дата анализа је корисна за разумевање различитих карактеристика и њихових међусобних интеракција које својом синтезом директно утичу на излаз модела.

На крају се приказује верни Шаплијев индекс интеракције (енгл. *Faithful Shapley interaction index*). Дата анализа омогућава снажно разумевање како главне карактеристике, као и њихове интеракције другог реда, заиста могу утицати на предвиђања модела. Слика 52 приказује резултате *nSHAP* анализе другог реда за бинарну класификацију, док Слика 53 приказује исте резултате за вишекласну класификацију.

У бинарној класификацији (Слика 52), карактеристика *tcp.time_delta* потврђује највећи главни допринос, али такође остварује значајне интеракције другог реда са другим

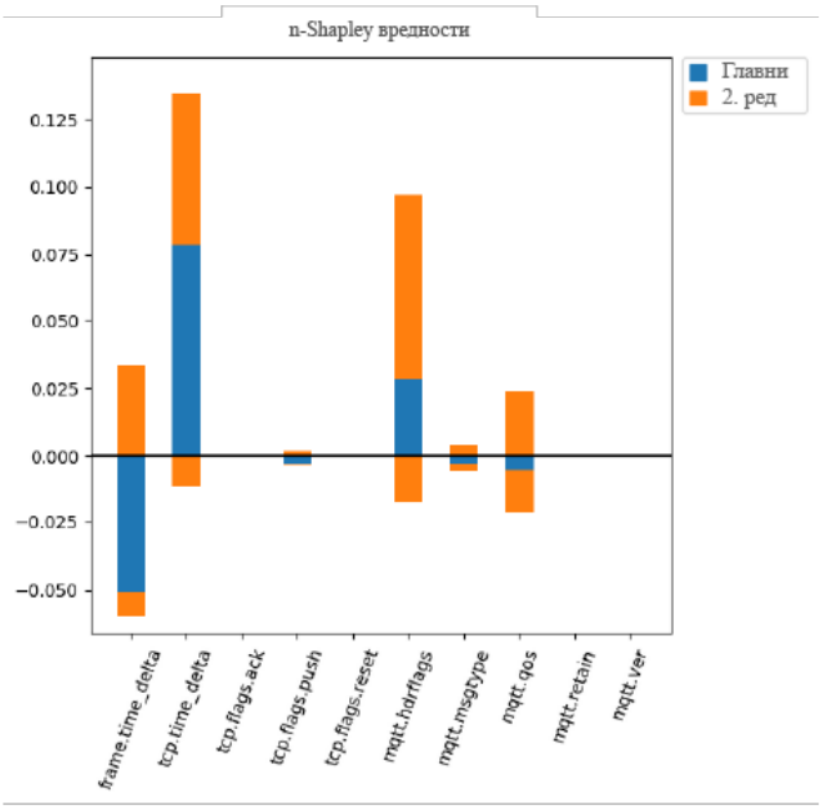
карактеристикама. Карактеристика *frame.time_delta* такође демонстрира значајан допринос са интеракцијама које су од важности за тачност предвиђања модела. Остале карактеристике као што су *tcp.flags.push* и *mqtt.hdrflags* потврђује различите степене утицаја у зависности од њихових интеракција са другим карактеристикама.



Слика 52 nSHAP анализа другог реда за бинарну и вишекласну класификацију - Бинарна nSHAP анализа [13]

За вишекласну класификацију (Слика 53), *tcp.time_delta* и даље показује изузетно висок утицај, док се види и значајан допринос других карактеристика као што су *frame.time_delta* и *mqtt.hdrflags*. Интеракције другог реда овде такође играју важну улогу, што указује на сложеност односа између карактеристика приликом постављених различитих класификационим задацима.

Постигнути резултати веома су корисни за даље побољшање модела, јер омогућавају боље разумевање међусобних односа и утицаја различитих карактеристика приликом идентификовања критичних тачака у моделу које би требало оптимизовати за боље перформансе.



Слика 53 nSHAP анализа другог реда за вишекласну класификацију - вишекласна nSHAP анализа [13]

12. Анализа обављених експеримената

Анализирани су постигнути резултати експеримената који су спроведени у оквиру истраживања са циљем процене ефикасности и робусности предложених алгоритама машинског учења у детекцији и превенцији упада у дистрибуиране системе. Експерименти су обухватили разноврсне скупове података, укључујући бинарне и вишекласне, како би се обезбедила свеобухватна процена перформанси алгоритама у различитим сценаријима.

Анализом обављених експеримената потврђени су следећи резултати:

- Побољшање алгоритама за детекцију упада; хибридном оптимизацијом алгоритама машинског учења унапређен је постојећи алгоритам за детекцију упада у дистрибуиране системе, побољшавајући њихову тачност и ефикасност.
- Имплементација *XG-MFA* алгоритма; анализиран је и тестиран оптимизовани алгоритам *XG-MFA* који остварује и постиже најбоље перформансе приликом класификације података.

- Оптимизација алгоритама машинског учења; проучени су и оптимизовани алгоритми машинског учења, повећавајући тачност предвиђања.
- Унапређење безбедности података; истраживање доприноси унапређењу безбедности осетљивих посматраних скупова података кроз ефикасније технике детекције и превенције упада у дистрибуирани систем у оквиру ког се користе исти.
- Примена метахеуристичких метода; коришћење напредних метахеуристичких метода за оптимизацију алгоритама машинског учења може омогућити бољу обраду и класификацију података.
- Дубинско учење за детекцију упада; имплементација дубоких неуронских мрежа за детекцију упада показује значајна побољшања у постизању тачности и брзини детекције.
- Евалуација и компаративна анализа; обављена је детаљна евалуација и компаративна анализа перформанси различитих алгоритама, пружајући детаљнији увид у њихове предности и мане.
- Анализа експерименталних скупова података; анализиран је скуп података за различите експерименте, омогућавајући тестирање и валидацију резултата оптимизованог алгоритма.
- Побољшање заштите дистрибуираних система; истраживање показује како оптимизоване методе могу ефикасно побољшати заштиту дистрибуираних система од савремених безбедносних претњи и изазова.

12.1. Закључна разматрања докторске дисертације

У овој докторској дисертацији анализирани су и евалуирани различити алгоритми за класификацију података, посебно фокусирајући се на детекцију и превенцију упада у дистрибуиране системе. Увођење напредних метода дубоког учења и метахеуристике показује значајан потенцијал у овом домену. Стога, изводе се закључци је да је од важности континуирано праћење и ажурирање безбедносних мера због све бржег развоја савремених претњи и рањивости по дистрибуиран систем. Такође, препоручено је истраживање нових техника и алгоритама који би могли додатно повећати сигурност и отпорност система на савремене нападе. Сходно наведеном, докторска дисертација садржи тринаест поглавља где је свако поглавље било усмерено на теоријско поткрепљење чињеница и експерименталне евалуације.

Прво поглавље представља уводна разматрања, где се пружа преглед циљева и значаја истраживања, истичући важност унапређења безбедности дистрибуираних система путем напредних алгоритама машинског учења. У овом поглављу наглашава се потреба за ефикасним методама детекције и превенције упада у контексту дистрибуираних система. Такође, у уводном делу разматрани су безбедносни изазови у заштити осетљивих података од савремених претњи.

У другом поглављу обрађују се основни концепти и теорије где се постављају претпоставке за разумевање метода и техника коришћених приликом научног истраживања. Обухваћени су појмови дистрибуираних система, машинског учења и дубоког учења. Такође, разматрани су принципи оптимизације алгоритама и метахеуристике који представљају кључни фактор за оптимизацију метода детекције упада.

Треће поглавље даје преглед у области науке и литературе. Обрађују се резултати научни радова из области који се односе на анализу и примену алгоритама машинског учења у дистрибуираним системима. Приказују се најновија достигнућа и трендови у области заштите дистрибуираних система. Такође, истичу се кључни резултати и исходи који су поставили темеље за даље истраживање у области ове докторске дисертације.

Четврто поглавље уводи у област дистрибуираних система и машинског учења. Описује се како се дистрибуирани системи могу интегрисати са алгоритмима машинског учења, а са циљем побољшања детекције упада и заштите података. Анализира се улога дистрибуираних система у савременим безбедносним оквирима. Такође, у поглављу се анализирају предности коришћења машинског учења приликом детекције и превенције упада у дистрибуиран систем.

Пето поглавље уводи у машинско учење и алгоритми неуронских мрежа. Поглавље се фокусира на различите алгоритме машинског учења и неуронских мрежа који се користе у истраживању, са акцентом на њихове предности и ограничења. Разматрају се спецификације и перформансе различитих модела. Посебна пажња посвећена је алгоритму *XG-MFA*, његовој структури и примени.

Шесто поглавље указује на проблеме оптимизације алгоритама машинског учења. Анализирају се проблеми и изазови приликом оптимизације алгоритама машинског учења, укључујући указивање за потребом за побољшањем тачности. Анализирају се различите технике оптимизације и њиховим ефектима на перформансе алгоритама.

Седмо поглавље уводи у област дубоког учења, где се објашњавају концепти, укључујући структуру и примену дубоких неуронских мрежа приликом детекцији упада у дистрибуиране системе.

Осмо поглавље представља метахеуристичке поступке високог нивоа. Даје се преглед различитих метахеуристичких метода, као и њихова сврсисходна примена приликом оптимизације алгоритама за детекцију упада. У докторској дисертацији истражују се и анализирају најефикасније метахеуристике, као и њихова примена у области истраживања. Посебан осврт и фокус су на методима, као што су оптимизација ројеви честица и еволутивни алгоритми.

Девето поглавље представља предложени оптимизовани алгоритам. Представља се детаљан опис оптимизованог алгоритма XG-MFA, укључујући методе, технике и кораке

коришћене у његовој имплементацији. Описују се специфичне карактеристике које чине овај алгоритам ефикасним. Такође , разматрају се резултати експерименталних тестова који потврђују његову супериорност у поређењу са другим алгоритмима у релевантним опсезима.

Десето поглавље укључује експериментални скуп података. Дефинише се опис скупа података коришћених током извођења експеримената, укључујући изворе, врсте података и методе за њихово прикупљање и обраду. У поглављу се разматрају карактеристике и структура анализираних података. Такође, приказују се методе препроцесирања и припреме података за даљу анализу.

Једанаесто поглавље приказује резултате евалуације експеримента, као и компаративну анализу резултата. У датом поглављу приказују се и презентују се анализа резултата експеримената, укључујући поређење перформанси различитих алгоритама. Врши се опсервација импликација добијених резултата за свеукупно унапређење безбедности дистрибуираних система.

У дванаестом поглављу ове докторске дисертације дају се закључци обављених експеримената. Приказује се сажетак кључних налаза истраживања, где се даје оквир за будуће научно истраживање. Такође, разматрају се практичне импликације резултата истраживања.

Тринаесто поглавље представља литературу која приказује списак свих коришћених извора и референци које су биле од користи приликом овог научног истраживања, обезбеђујући потпуну документацију и веродостојност рада.

Резултати су показали да предложени оптимизовани алгоритам *XG-MFA* остварује боље резултате у односу на друге алгоритме у већини случајева, показујући инфериорност у контексту тачности и робусности. Поред тога, оптимизовани алгоритам остварује највише вредности на *PR* и *ROC* кривама, што додатно указује на његов потенцијал за побољшање класификације и детекције упада у дистрибуиран систем.

Такође, анализа показује да предложени алгоритам обезбеђује висок ниво заштите од упада, нарочито у контексту савремених напада као што су *DoS*, *DDoS*, и *ransomware*. Ово се постиже захваљујући напредним технолошким решењима и оптимизацијама које су интегрисане у алгоритам, омогућавајући брзу и тачну детекцију на савремене безбедносне претње.

На основу анализе обављених експеримената, могу се извући значајни закључци који доприносе бољем разумевању и побољшању безбедносних система у дистрибуираним окружењима. Пре свега, резултати указују да напредни алгоритми машинског учења, као што је *XG-MFA*, може значајно унапредити детекцију и превенцију упада, обезбеђујући висок ниво сигурности и поузданости. Ово научно истраживање је такође потврдило важност континуираног развоја и унапређења свих безбедносних технологија, како би

се могло одговорити на све сложеније и софистицираније претње у савременом дигиталном свету.
Додатно, анализа истиче високу потребу за интеграцијом различитих приступа приликом развоју безбедносних решења дистрибуираних система, укључујући хибридне методе које комбинују примену машинског учења и вештачке интелигенције, заједно са сложеним алгоритмима. Такође, наглашава се важност заштите уређаја интернет ствари и других критичних компоненти дистрибуираних система, који су често мета напада због своје рањивости и неусаглашености стандарда.

Закључна разматрања указују да резултати овог научног истраживања пружају допринос унапређењу безбедности дистрибуираних система и постављају темељ за будућа истраживања са фокусом на развој напреднијих и софистицираних решења за детекцију и превенцију упада, где је од посебне важности заштита интегритета података.

Испитивање алгоритама машинског учења оптимизовани модификованим алгоритмом свитаца (енгл. *Frefly algorithm*), нуди сложене и високо комплексне могућности приликом превазилажења потенцијалних безбедносних изазова. Исти се могу повезивати са интеграцијом *IoT*-а у концепту *Healthcare 4.0*. Модели развијени за потребе научно-истраживачког рада [13] и докторске тезе показују изузетно снажне и високе перформансе приликом откривања безбедносних проблема у *IoT* уређајима, а који се могу користити у концепту *Healthcare 4.0*. Тиме се истиче ефикасност и потенцијал машинског учења у комбинацији са метахеуристикама модификованих алгоритама светлуцавих мушица.

Предложени модел научно-истраживачког рада [13], а на који се ослања ова докторска дисертација, комбинује *XGBoost* са модификованим алгоритмом свитаца (XG-MFA), показује инфериорне резултате приликом обављања задатака вишекласне и бинарне класификације. Остварени резултати сугеришу да је овакав приступ високо ефикасан приликом откривања сложених безбедносних претњи за дистрибуиране системе у поређењу са постојећим методама. Примена *SHAP* анализе омогућава јасније разумевање доприноса различитих карактеристика на одлуке модела, што је додатно унапредило ефикасност и поузданост модела.

Разматрани и предложен модел заснован на оптимизацији хибридних алгоритама и неуронских мрежа представља значајан корак напред у области детекције упада и заштите дистрибуираних система. Неуронске мреже, посебно дубоке неуронске мреже (DNN), показују својеврстан и изузетан потенцијал приликом откривања сложених шаблона и аномалија [80] [99] које могу указивати на безбедносне претње и рањивости. Таквим приступом, у комбинацији са метахеуристичким алгоритмима као што је модификовани алгоритам свитаца (MFA), може омогућити моделовање кохерентних процеса интеракције између различитих карактеристика и њиховог утицаја на безбедност дистрибуираног система.

Дистрибуирани системи посебно могу бити рањиви на малициозне нападе због њихове комплексне природе и велике количине података који се морају обрађивати искључиво у реалном времену. Проблеми који се могу јавити у концепту *Healthcare 4.0* додатно наглашавају потребу за робусним и поузданим моделима за детекцију упада.
Healthcare 4.0 подразумева интеграцију IoT уређаја у медицинске системе, што омогућава побољшану дијагностику, праћење и лечење пацијената. Међутим, ови системи су такође мета напада који могу угрозити приватност пацијената и интегритет података.

Предложени оптимизовани модел, који комбинује неуронске мреже и метахеуристичке алгоритме, показује изузетну способност приликом детекције различитих типова упада. Резултати експеримената показују да овај приступ не само да повећава тачност детекције, већ и смањује број лажних позитивних и лажних негативних детекција, што, заправо, представља кључ за остваривање ефикасности унутар безбедносних система. Стога је посебно од важности напоменути да предложени модел успева да одржи високе перформансе и у условима високог интензитета мрежног саобраћаја и оптерећења, у виду и масивних и великих количина података, што га чини идеалним за примену у реалним условима.

Наредне анализе доказују да примена *SHAP* методе доприноси бољем разумевању утицаја појединачних карактеристика на одлуке модела. Ово посебно може бити од значаја у контексту концепта *Healthcare 4.0*, где је од критичног значаја разумети који фактори највише могу утицати на свеукупну безбедност и како их ефикасно контролисати. *SHAP* анализа показује да карактеристике као што су *tcp.time_delta* и *frame.time_delta* [13] имају кључну улогу приликом детекције малициозних активности, чиме се, заправо, активирају мере заштите и превенције дистрибуираног система. SHAP анализа је такође показала да *mqtt.hdrflags* има значајан утицај на класификацију, посебно у вишекласном сценарију. Ова карактеристика, заједно са *frame.time_delta* и *tcp.flags.push* игра кључну улогу у одлукама модела и указује на комплексне интеракције између различитих карактеристика које могу утицати на коначни исход.

Резултати [13] такође показују да предложени модел има изузетно ефикасан механизам приликом детекције напада, а који су специфични за здравствене системе, као што су напади на *IoT* уређаје који могу пратити кључне и виталне знаке пацијената. Ово је од изузетне важности за одржавање сигурности и поузданости здравствених услуга у савременој дигиталној ери. Применом оптимизације хиперпараметара и коришћењем метахеуристичких алгоритама, постижу се синтеза, те се таква корелација огледа у значајном побољшању приликом детекције упада и заштите дистрибуираних система.

Истраживање ове докторске тезе пружа основ за будућа истраживања и развој нових модела који могу комбиновати напредне технике машинског учења и метахеуристике. Предложени модел [13] показује да је могуће постићи висок ниво безбедности и поузданости, чак и у сложеним и динамичним окружењима као што су поменути здравствени и други дистрибуирани системи. Даљим истраживањем и развојем очекује

се да ови модели могу постати још ефикаснији и прилагодљивији, омогућавајући пракси безбедну и поуздану интеграцију *IoT* уређаја у различите секторе.

На основу свега наведеног, може се закључити да оптимизација хибридних алгоритама и употреба неуронских мрежа могу бити кључни фактор за побољшање безбедности дистрибуираних система. Тиме се омогућава прецизнија и бржу детекцију упада, чиме се може смањити ризик од безбедносних инцидената и осигуравајући интегритет података. Предложени модел *XG-MFA* [13]показује инфериорне резултате и тиме представља значајан корак напред у области високо-технолошке безбедности и заштите дистрибуираних система, са посебним акцентом у контексту *Healthcare 4.0*.

Експериментални део рада укључује анализу *IoT-Flock* генерисаног скупа података из здравствених *IoT* уређаја. Резултати показују да предложени модел *XG-MFA* има највиши ниво прецизности приликом класификације, надмашујући друге иновативне метахеуристичке методе. Предложени модел је посебно успешан током детекције рањивог саобраћаја, чиме се значајно могу побољшати мере безбедности у здравственим системима који користе уређаје интернет ствари.

Оптимизација хиперпараметара и употреба метахеуристика показују се као изразито ефикасни алати приликом унапређења перформанси модела машинског учења. Омогућавају прецизније и брже детекције безбедносних претњи, чиме се значајно смањује ризик од цурења података и других безбедносних инцидената. Употреба хибридних алгоритама, као што је предложени модел *XG-MFA* [13], доказује да је могуће постићи значајна побољшања у односу на традиционалне методе. Ово научно истраживање показује да интеграција напредних алгоритама машинског учења и метахеуристика може бити кључна за свеукупно побољшање безбедности дистрибуираних система. Унапређење техника детекције упада и превенције од активности које могу постићи високе рањивости јесу од кључног значаја за стварање безбедности и интегритета података у савременим мрежним инфраструктурама.

Експериментални резултати потврђују да је предложени модел *XG-MFA* [13] надмашио друге методе, као што су генетски алгоритам (XG-GA), алгоритам роја честица (XG-PSO) и друге. Резултати показују да је *XG-MFA* [13] остварује највиши ниво прецизности, најмању стопу грешке и најбоље укупне перформансе приликом постављених различитих задатака класификације. Поред тога, важност примене оптимизације хиперпараметара показује се кључном за постизање високих перформанси модела. Употреба метода као што су минимизација грешке и максимизација коефицијента Коенове капе додатно побољшавају тачност и поузданост модела. Овакви резултати доказује важност оптимизације приликом развоја софистицираних алгоритама детекције упада у дистрибуирани систем или једну мрежну инфраструктуру.

Резултати експеримената указују на то да је предложени модел не само ефикасан већ и робустан у различитим сценаријима. То може бити посебно важно за примену у реалним условима где модели морају бити прилагодљиви и поуздани у различитим околностима.

Предложени приступ [13] такође наглашава значај коришћења напредних метахеуристика за побољшање перформанси модела машинског учења.

Напослетку, ово научно истраживање пружа значајан допринос у области анализе модела за унапређење безбедности дистрибуираних система и указује на нове смерове за будућа истраживања. Помоћу оптимизације хибридних алгоритама и примену напредних техника машинског учења, могуће је значајно побољшати безбедносне механизме и осигурати интегритет података у различитим доменима, што је експериментални поступцима то и потврђено [13].

Докторска теза наглашава и указује на изузетно високу потребу за континуираном анализом, оптимизацијом и унапређењем свих безбедносних механизама, како би се правилно и правовремено одговорило на све веће свакодневне изазове, а који се заснивају на интеграцији *IoT* уређаја и других напредних технологија у сваки сегмент савремене дигиталне ере.

12.2 Будући рад и будућа истраживања

Будући оквир истраживања у области заштите, превенције и детекције упада у дистрибуиране системе суштински обухвата више аспеката савремене безбедносне инфраструктуре и нових претњи које се континуирано појављују. Стога, будуће истраживање огледа се у развоју нових напредних хибридних алгоритама машинског учења и вештачке интелигенције који могу ефикасно детектовати и спречавати упаде у дистрибуиран систем у реалном времену. Такви алгоритми требало би да буду довољно робусни и могу идентификовати и одговоре на широк спектар савремених напада као што су: *DoS* (Denial of Service), *DDoS* (Distributed Denial of Service), *Ransomware*, *Phishing* и *APT* (Advanced Persistent Threats).

Нове рањивости у дистрибуираним системима често се појављују услед сложености и хетерогености уређаја и мрежа које заједно чине један интегрисан или сегментиран систем. Суштина будућих решења се огледа у томе да су уређаји интернет ствари посебно осетљиви услед њихове изузетно ограничене рачунарске моћи, као и недостатка напредних безбедносних механизама. Како је овакав проблем реалан у пракси, наведена мана их чини примарним циљевима за нападаче који могу искористити управо поменуту рањивост за покретање ботнет мреже или ширење малвера кроз уређаје. Будуће истраживање суштински се може фокусирати на развоју специјализованих решења за *IoT* уређаје који могу обезбедити сврсисходнију интеграцију безбедносних механизама без значајног утицаја на перформансе физичких уређаја.

Како би се спречили најновији напади, од важности је развијање и имплементирање свеобухватних безбедносних оквира који укључују хибридне методе детекције. Такве методе требало би да комбинују предности статичке и динамичке анализе, као и технике машинског учења како би се обезбедила боља тачност, као и мањи број лажно

позитивних резултата. Поред тога, неопходно је унапређивање постојећих система за превенцију упада (IPS) и система за детекцију упада (IDS), како би били у стању да идентификују и одговоре на нове типове претњи у раној фази.

Такође, важан аспект будућих истраживања требало би да буде развој система за аутоматско ажурирање и *крпљење* рањивости у дистрибуираним системима. Дати системи требало би да користе, поред нових прилагођених решења, тако и напредне алгоритме за анализу саобраћаја и препознавање свих аномалија како би могли проактивно откривати потенцијалне нападе. Тиме би се аутоматски могле применити све неопходне безбедносне мере превенције и евентуалне *закрпе* датог дистрибуираног система.

Узимајући у обзир брзину развоја и интеграције *IoT* уређаја у различите сфере живота и рада, од важности је да се будућа истраживања заснивају и на питањима приватности и интегритету података, као и усаглашености са регулативама. Разматрање приватности података у контексту нових безбедносних решења може обезбедити, не само сигурност, већ и заштиту осетљивих информација од евентуалне злоупотребе.

Сходно предложеним разматрањима, будући оквир истраживања огледа се у свеобухватном приступу развоја нових решења и примени иновативних технологија за детекцију, превенцију и заштиту дистрибуираних система од савремених претњи. Фокус будућег истраживања на адаптивним и самоучећим системима, који се могу брзо прилагодити новим нападима и рањивостима, представља кључни корак напред према постизању робусније и сигурније мрежне инфраструктуре у ери дигиталне трансформације.

13. Литература

[1] National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing. Извор: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (приступљено 11. јуна, 2023. године).

[2] National Institute of Standards and Technology. (n.d.). Internet of Things (IoT). Извор from https://csrc.nist.gov/glossary/term/internet_of_things (accessed June 13, 2023).

[3] National Institute of Standards and Technology. (n.d.). Artificial Intelligence. Извор: https://www.nist.gov/artificial-intelligence (приступљено 14. јуна, 2023).

[4] IBM. (n.d.). Machine Learning. Извор: https://www.ibm.com/topics/machine-learning (приступљено 14. јуна, 2023).

[5] IEEE. (2020). Authors of "Deep Learning-Based Intrusion Detection for Cyber-Physical Systems." Извор: https://ieeexplore.ieee.org/document/9107771/authors#authors (приступљено 16., 2023).

[6] Association for Computing Machinery. (2017). Machine Learning Security: Threats, Risks, and Countermeasures. Извор: https://dl.acm.org/doi/abs/10.1145/3052973.3053009 (приступљено 17. јуна, 2023).

[7] National Institute of Standards and Technology. (2023). Deep Learning-Based Intrusion Detection in Adversarial Environments. Извор: https://www.nist.gov/publications/deep-learning-based-intrusion-detection-adversaries (приступљено 23. јуна, 2023).

[8] OWASP Foundation. (n.d.). Intrusion Detection. Извор: https://owasp.org/www-community/controls/Intrusion_Detection (приступљено 26. јуна, 2023).

[9] Baeldung. (n.d.). Distributed System vs. Distributed Computing. Извор: https://www.baeldung.com/cs/distributed-system-vs-distributed-computing (приступљено 24. јуна, 2023).

[10] Apache Hadoop. (n.d.). Hadoop. Извор: from https://hadoop.apache.org/ (приступљено 26. јуна, 2023).

[11] Krazytech. (n.d.). Cloud Computing vs. Distributed Computing. Извор: https://krazytech.com/technical-papers/cloud-computing-vs-distributed-computing (приступљено 27. јуна, 2023).

[12] Google Developers. (n.d.). Generative Adversarial Networks (GANs). Извор https://developers.google.com/machine-learning/gan/generator (приступљено 1. јула, 2023).

[13] Savanović, N., Toskovic, A., Petrovic, A., Zivkovic, M., Damaševičius, R., Jovanovic, L., Bacanin, N., & Nikolic, B. (2023). Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning. Sustainability, 15(12), 12563. https://doi.org/10.3390/su151612563

[14] Sahani, N., Zhu, R., Cho, J.-H., & Liu, C.-C. (2023). Machine Learning-Based Intrusion Detection for Smart Grid Computing: A Survey. ACM Transactions on Cyber-Physical Systems, 7(2), Article 11. https://doi.org/10.1145/3578366

[15] National Science Foundation. (n.d.). Cyber-Physical Systems (CPS) Program. Извор: https://new.nsf.gov/funding/opportunities/cyber-physical-systems-cps (приступљено 24. јуна, 2023).

[16] Mari, A.-G., Zinca, D., & Dobrota, V. (2023). Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network. Sensors, 23(3), 1315. https://doi.org/10.3390/s23031315

[17] TechTarget. (n.d.). Generative Adversarial Network (GAN). Извор: https://www.techtarget.com/searchenterpriseai/definition/generative-adversarial-network-GAN (приступљено 27. јуна, 2023).

[18] Hosseini, S., & Zade, B. M. H. (2020). New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN. Computer Networks, 173, 107168. https://doi.org/10.1016/j.comnet.2020.107168

[19] Habiba, M., Islam, M. R., Muyeen, S., & Ali, A. S. (2023). Edge intelligence for network intrusion prevention in IoT ecosystem. Computers and Electrical Engineering, 108, 108727. https://doi.org/10.1016/j.compeleceng.2023.108727

[20] Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2021). A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks. Procedia Computer Science, 210, 94-103. https://doi.org/10.1016/j.procs.2022.10.124

[21] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[22] Z. Wang and F. A. Ghaleb, "An Attention-Based Convolutional Neural Network for Intrusion Detection Model," in IEEE Access, vol. 11, pp. 43116-43127, 2023, doi: 10.1109/ACCESS.2023.3271408.

[23] V. Hnamte, H. Nhung-Nguyen, J. Hussain and Y. Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," in IEEE Access, vol. 11, pp. 37131-37148, 2023, doi: 10.1109/ACCESS.2023.3266979.

[24] Taherdoost, H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics 2023, 12, 1901. https://doi.org/10.3390/electronics12081901

[25] Spiceworks. (n.d.). What is Linear Regression? Извор: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-linear-regression/ (приступљено 13. јула, 2023).

[26] Vikani, B. (2015). Linear Regression. Извор: https://bhagyeshvikani.blogspot.com/2015/10/linear-regression.html (приступљено 15. јула, 2023).

[27] Dataquest. (n.d.). Top 10 Machine Learning Algorithms for Beginners. Извор: https://www.dataquest.io/blog/top-10-machine-learning-algorithms-for-beginners/ (приступљено 21 јула, 2023).

[28] Simplilearn. (n.d.). 10 Algorithms Machine Learning Engineers Need to Know. Извор: https://www.simplilearn.com/10-algorithms-machine-learning-engineers-need-to-know-article (приступљено 22. јула, 2023).

[29] The Mathmo. (2016). Rusty Machine: Machine Learning in Rust. Извор: https://athemathmo.github.io/2016/03/07/rusty-machine.html (приступљено 24. јула, 2023).

[30] Hypertextbookshop. (n.d.). Data Mining: Concepts and Techniques. Извор: https://www.hypertextbookshop.com/dataminingbook/public_version/contents/chapters/chapter001/section002/green/page001.html (приступљено 25. јула, 2023).

[31] Deep Learning (Adaptive Computation and Machine Learning series) by Ian Goodfellow (Author), Yoshua Bengio (Author), Aaron Courville (Author)

[32] Harifi, S., Mohammadzadeh, J., Khalilian, M. et al. Giza Pyramids Construction: an ancient-inspired metaheuristic algorithm for optimization. Evol. Intel. 14, 1743–1761 (2021). https://doi.org/10.1007/s12065-020-00451-3

[33] Wolfram MathWorld. (n.d.). Polynomial Time. Извор: https://mathworld.wolfram.com/PolynomialTime.html (приступљено 10. августа, 2023).

[34] Wolfram MathWorld. (n.d.). NP-Hard Problem. Извор: https://mathworld.wolfram.com/NP-HardProblem.html (приступљено 13. августа, 2023).

[35] D. H. Wolpert and W. G. Macready, "No free lunch theorems for optimization," in IEEE Transactions on Evolutionary Computation, vol. 1, no. 1, pp. 67-82, April 1997, doi: 10.1109/4235.585893.

[36] Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. Sensors 2021, 21, 3025. https://doi.org/10.3390/s21093025

[37] IoT Healthcare Security Dataset. Извор: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset (приступљено 14. августа, 2023.)

[38] Vaccari I, Chiola G, Aiello M, Mongelli M, Cambiaso E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT. Sensors (Basel). 2020 Nov 18;20(22):6578. doi: 10.3390/s20226578. PMID: 33217936; PMCID: PMC7698741.

[39] Scikit-learn: Machine Learning in Python. Извро: https://scikit-learn.org/stable/ (приступљено 21. августа, 2023.)

[40] Yang, Xin-She. (2010). Firefly Algorithms for Multimodal Optimization. 5792. 10.1007/978-3-642-04944-6_14.

[41] Grefenstette, J.J. (Ed.). (1987). Genetic Algorithms and their Applications: Proceedings of the Second International Conference on Genetic Algorithms (1st ed.). Psychology Press. https://doi.org/10.4324/9780203761595

[42] Alam, T., Qamar, S., Dixit, A., & Benaida, M. (2020). Genetic Algorithm: Reviews, Implementations, and Applications. International Journal of Engineering Pedagogy (iJEP), 10(6), pp. 57–77. https://doi.org/10.3991/ijep.v10i6.14567

[43] Kennedy, J. and Eberhart, R. (1995) Particle Swarm Optimization. Proceedings of the IEEE International Conference on Neural Networks, 4, 1942-1948. http://dx.doi.org/10.1109/ICNN.1995.488968

[44] Karaboga, D., & Basturk, B. (2007). On the performance of artificial bee colony (ABC) algorithm. Applied Soft Computing, 8(1), 687-697. https://doi.org/10.1016/j.asoc.2007.05.007

[45] Khishe, M., & Mosavi, M. (2020). Chimp optimization algorithm. Expert Systems With Applications, 149, 113338. https://doi.org/10.1016/j.eswa.2020.113338

[46] Gurrola-Ramos, J.; Hernàndez-Aguirre, A.; Dalmau-Cedeño, O. COLSHADE for real-world single-objective constrained optimization problems. In Proceedings of the 2020 IEEE Congress on Evolutionary Computation (CEC), Glasgow, UK, 19–24 July 2020; IEEE: New York, NY, USA, 2020; pp. 1–8.

[47] Zhao, J., Zhang, B., Guo, X., Qi, L., & Li, Z. (2021). Self-Adapting Spherical Search Algorithm with Differential Evolution for Global Optimization. Mathematics, 10(23), 4519. https://doi.org/10.3390/math10234519

[48] Hossin, M and Sulaiman, M.N. (2015) A Review on Evaluation Metrics for Data Classification Evaluations. International Journal of Data Mining & Knowledge Management Process, 5, 11 p. https://doi.org/10.5121/ijdkp.2015.5201

[49] Arabameri, A.; Chen, W.; Lombardo, L.; Blaschke, T.; Tien Bui, D. Hybrid Computational Intelligence Models for Improvement Gully Erosion Assessment. Remote Sens. 2020, 12, 140. https://doi.org/10.3390/rs12010140

[50] Pepe MS, Janes H, Longton G, Leisenring W, Newcomb P. Limitations of the odds ratio in gauging the performance of a diagnostic, prognostic, or screening marker. American Journal of Epidemiology. 2004 May;159(9):882-890. DOI: 10.1093/aje/kwh101. PMID: 15105181.

[51] Van Den Eeckhaut, M., Vanwalleghem, T., Poesen, J., Govers, G., Verstraeten, G. and Vandekerckhove, L. (2006) Prediction of Landslide Susceptibility Using Rare Events Logistic Regression: A Case-Study in the Flemish Ardennes (Belgium). Geomorphology, 76, 392-410.

[52] Warrens, M.J. Kappa coefficients for dichotomous-nominal classifications. Adv Data Anal Classif 15, 193–208 (2021). https://doi.org/10.1007/s11634-020-00394-8

[53] LaTorre, A., Molina, D., Osaba, E., Poyatos, J., Del Ser, J., & Herrera, F. (2021). A prescription of methodological guidelines for comparing bio-inspired optimization algorithms. Swarm and Evolutionary Computation, 67, 100973. https://doi.org/10.1016/j.swevo.2021.100973

[54] Shapiro, S.S. and Francia, R.S. (1972) An Approximate Analysis of Variance Test for Normality. Journal of the American Statistical Association, 67, 215-216.

[55] Wilcoxon, F. Individual comparisons by ranking methods. In Breakthroughs in Statistics; Springer: Berlin/Heidelberg, Germany, 1992; pp. 196–202

[56] Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

[57] Barr, R., & Massoulié, L. (2004). Proceedings of the ACM SIGCOMM 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication.

[58] Bishop, M. (2003). Computer Security: Art and Science. Addison-Wesley.

[59] Verbraeken, J., Wolting, M., Katzy, J., Kloppenburg, J., Verbelen, T., & Rellermeyer, J. S. (2019). A Survey on Distributed Machine Learning. ArXiv. https://doi.org/10.1145/3377454.

[60] Chollet, F. (2018). Deep Learning with Python. Manning Publications.

[61] Dean, J., & Ghemawat, S. (2004). MapReduce: Simplified data processing on large clusters. OSDI.

[62] Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222-232.

[63] Duda, R. O., Hart, P. E., & Stork, D. G. (2001). Pattern Classification (2nd ed.). Wiley.

[64] Freund, Y., & Schapire, R. E. (1997). A decision-theoretic generalization of on-line learning and an application to boosting. Journal of Computer and System Sciences, 55(1), 119-139.

[65] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[66] Gurney, K. (1997). An Introduction to Neural Networks. CRC Press.

[67] Han, J., Pei, J., & Kamber, M. (2011). Data Mining: Concepts and Techniques. Morgan Kaufmann.

[68] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 770-778.

[69] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780.

[70] Hossain, M. S., Muhammad, G., & Rahman, S. M. (2020). Cyber-physical cloud-oriented multi-modal medical framework for health monitoring. Future Generation Computer Systems, 90, 362-373.

[71] Huang, G., Liu, Z., Van Der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 4700-4708.

[72] Jain, S., Pawar, P. M., & Muthalagu, R. (2022). Hybrid intelligent intrusion detection system for internet of things. Telematics and Informatics Reports, 8, 100030. https://doi.org/10.1016/j.teler.2022.100030.

[73] Jia, Y., Shelhamer, E., Donahue, J., Karayev, S., Long, J., Girshick, R., ... & Darrell, T. (2014). Caffe: Convolutional architecture for fast feature embedding. Proceedings of the 22nd ACM International Conference on Multimedia, 675-678.

[74] Bae, G., Jang, S., Kim, M., Joe, I. (2019). Autoencoder-Based on Anomaly Detection with Intrusion Scoring for Smart Factory Environments. In: Park, J., Shen, H., Sung, Y., Tian, H. (eds) Parallel and Distributed Computing, Applications and Technologies. PDCAT 2018. Communications in Computer and Information Science, vol 931. Springer, Singapore. https://doi.org/10.1007/978-981-13-5907-1_44.

[75] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25, 1097-1105.

[76] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[77] Lee, J. H., & Choi, J. (2016). Application of machine learning algorithms in intrusion detection system: A survey. Journal of Electrical Engineering & Technology, 11(6), 1835-1842.

[78] Kwon, D., Kim, H., Kim, J. et al. A survey of deep learning-based network anomaly detection. Cluster Comput 22 (Suppl 1), 949–961 (2019). https://doi.org/10.1007/s10586-017-1117-8.

[79] Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., & Alsaadi, F. E. (2017). A survey of deep neural network architectures and their applications. Neurocomputing, 234, 11-26.

[80] Malaiya, R.K., Kwon, D., Suh, S.C., Kim, H., Kim, I., & Kim, J. (2019). An Empirical Evaluation of Deep Learning for Network Anomaly Detection. IEEE Access, 7, 140806-140817.

[81] McAfee. (2019). McAfee Labs 2019 Threats Predictions Report. (извор: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/, приступљено 1.7.2024.).

[82] Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., Petersen, S., Beattie, C., Sadik, A., Antonoglou, I., King, H., Kumaran, D., Wierstra, D., Legg, S., & Hassabis, D. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533. https://doi.org/10.1038/nature14236.

[83] I. Aljamal, A. Tekeoğlu, K. Bekiroglu and S. Sengupta, "Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, HI, USA, 2019, pp. 84-89, doi: 10.1109/SERA.2019.8886794.

[84] Eryılmaz, E. E., Akleylek, S., Ertek, Y., Kılıç, E. (2024). A Systematic Survey of Machine Learning and Deep Learning Models Used in Industrial Internet of Things Security. MANAS Journal of Engineering, 12(1), 1-28. https://doi.org/10.51354/mjen.1197753.

[85] Mohri, M., Rostamizadeh, A., & Talwalkar, A. (2018). Foundations of Machine Learning (2nd ed.). MIT Press.

[86] Ng, A. Y., & Jordan, M. I. (2002). On discriminative vs. generative classifiers: A comparison of logistic regression and naive Bayes. Advances in Neural Information Processing Systems, 14, 841-848.

[87] R. Khurana and H. Gupta, "A hybrid model on cloud security," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2016, pp. 347-352, doi: 10.1109/ICRITO.2016.7784979.

[88] Papernot, N., McDaniel, P., & Goodfellow, I. (2016). Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. arXiv preprint arXiv:1605.07277.

[89] Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, Jake Vanderplas, Alexandre Passos, David Cournapeau, Matthieu Brucher,

Matthieu Perrot, and Édouard Duchesnay. 2011. Scikit-learn: Machine Learning in Python. J. Mach. Learn. Res. 12, null (2/1/2011), 2825–2830.

[90] X. Zhang, J. Ran and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2019, pp. 456-460, doi: 10.1109/ICCSNT47585.2019.8962490.

[91] M. Azizjon, A. Jumabek and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 2020, pp. 218-224, doi: 10.1109/ICAIIC48513.2020.9064976.

[92] J. F. Cañola Garcia and G. E. T. Blandon, "A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks," in IEEE Access, vol. 10, pp. 83043-83060, 2022, doi: 10.1109/ACCESS.2022.3196642.

[93] Mohammadpour, L.; Ling, T.C.; Liew, C.S.; Aryanfar, A. A Survey of CNN-Based Network Intrusion Detection. Appl. Sci. 2022, 12, 8162. https://doi.org/10.3390/app12168162.

[94] Saxe, J., & Berlin, K. (2017). Deep neural network based malware detection using two-dimensional binary program features. Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, 1-8.

[95] Schmidhuber, J. (2014). Deep learning in neural networks: An overview. Neural Networks, 61, 85-117. https://doi.org/10.1016/j.neunet.2014.09.003.

[96] Shaikh, S. H., & Memon, N. N. (2018). An efficient anomaly-based approach to intrusion detection system using machine learning algorithms. Journal of Ambient Intelligence and Humanized Computing, 9(2), 333-344.

[97] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310-1321.

[98] Silver D, Huang A, Maddison CJ, Guez A, Sifre L, van den Driessche G, Schrittwieser J, Antonoglou I, Panneershelvam V, Lanctot M, Dieleman S, Grewe D, Nham J, Kalchbrenner N, Sutskever I, Lillicrap T, Leach M, Kavukcuoglu K, Graepel T, Hassabis D. Mastering the game of Go with deep neural networks and tree search. Nature. 2016 Jan 28;529(7587):484-9. doi: 10.1038/nature16961. PMID: 26819042.

[99] B. Subba, S. Biswas and S. Karmakar, "A Neural Network based system for Intrusion Detection and attack classification," 2016 Twenty Second National Conference on Communication (NCC), Guwahati, India, 2016, pp. 1-6, doi: 10.1109/NCC.2016.7561088.

[100] Sutskever, I., Vinyals, O., & Le, Q. V. (2014). Sequence to sequence learning with neural networks. Advances in Neural Information Processing Systems, 27, 3104-3112.

[101] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, Andrew Rabinovich; Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 1-9.

[102] Chanchaichujit, J., Tan, A., Meng, F., Eaimkhong, S. (2019). Internet of Things (IoT) and Big Data Analytics in Healthcare. In: Healthcare 4.0. Palgrave Pivot, Singapore. https://doi.org/10.1007/978-981-13-8114-0_2.

[103] Mohamed, A.B., Idris, N.B., Shanmugum, B. (2012). A Brief Introduction to Intrusion Detection System. In: Ponnambalam, S.G., Parkkinen, J., Ramanathan, K.C. (eds) Trends in Intelligent Robotics, Automation, and Manufacturing. IRAM 2012. Communications in Computer and Information Science, vol 330. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35197-6_29.

[104] K. Woods and K. W. Bowyer, "Generating ROC curves for artificial neural networks," in IEEE Transactions on Medical Imaging, vol. 16, no. 3, pp. 329-337, June 1997, doi: 10.1109/42.585767.

[105] S. M. Vieira, U. Kaymak and J. M. C. Sousa, "Cohen's kappa coefficient as a performance measure for feature selection," International Conference on Fuzzy Systems, Barcelona, Spain, 2010, pp. 1-8, doi: 10.1109/FUZZY.2010.5584447.

[106] Shamshirband, S., Fathi, M., Dehzangi, A., Chronopoulos, A. T., & Alinejad-Rokny, H. (2020). A review on deep learning approaches in healthcare systems: Taxonomies, challenges, and open issues. Journal of Biomedical Informatics, 113, 103627. https://doi.org/10.1016/j.jbi.2020.103627.

[107] Haleem, A., Javaid, M., Pratap Singh, R., & Suman, R. (2021). Medical 4.0 technologies for healthcare: Features, capabilities, and applications. Internet of Things and Cyber-Physical Systems, 2, 12-30. https://doi.org/10.1016/j.iotcps.2022.04.001.

[108] L. R. Darwish, M. M. Farag and M. T. El-Wakad, "Towards Reinforcing Healthcare 4.0: A Green Real-Time IIoT Scheduling and Nesting Architecture for COVID-19 Large-Scale 3D Printing Tasks," in IEEE Access, vol. 8, pp. 213916-213927, 2020, doi: 10.1109/ACCESS.2020.3040544.

Анализа безбедносних модела детекције упада у дистрибуиране системе, оптимизацијом хибридних алгоритама неуронских мрежа

ORIGINALITY REPORT

1 %
SIMILARITY INDEX

PRIMARY SOURCES

1	portalcris.vdu.lt Internet	101 words — < 1%
2	vbs.rs Internet	26 words — < 1%
3	nardus.mpn.gov.rs Internet	24 words — < 1%
4	sr.wikipedia.org Internet	24 words — < 1%
5	eteze.bg.ac.rs Internet	19 words — < 1%
6	www.incibe.es Internet	18 words — < 1%
7	fedorabg.bg.ac.rs Internet	16 words — < 1%
8	community.deeplearning.ai Internet	11 words — < 1%
9	www.coursehero.com Internet	11 words — < 1%

10	www2.mdpi.com Internet	11 words — < 1%
11	Zorana Rončević, Ida Zahović, Ivana Pajčin, Mila Grahovac, Siniša Dodić, Jovana Grahovac, Jelena Dodić. "Effect of carbon sources on xanthan production by Xanthomonas spp. isolated from pepper leaves", Food and Feed Research, 2019 Crossref	10 words — < 1%
12	assets.researchsquare.com Internet	10 words — < 1%
13	jakov.kpu.edu.rs Internet	10 words — < 1%
14	Asmaa Halbouni, Teddy Surya Gunawan, Mohamed Hadi Habaebi, Murad Halbouni, Mira Kartiwi, Robiah Ahmad. "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System", IEEE Access, 2022 Crossref	9 words — < 1%
15	rfasper.fasper.bg.ac.rs Internet	9 words — < 1%
16	www.cs.uoi.gr Internet	9 words — < 1%
17	www.manualzz.com Internet	9 words — < 1%
18	www.plusbog.dk Internet	9 words — < 1%
19	csrc.nist.gov Internet	

8 words — < 1%

20 grafar.grf.bg.ac.rs
Internet
8 words — < 1%

21 "Fog Computing for Healthcare 4.0 Environments", Springer Science and Business Media LLC, 2021
Crossref
7 words — < 1%

22 Nikola Savanović, Ana Toskovic, Aleksandar Petrovic, Miodrag Zivkovic et al. "Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning", Sustainability, 2023
Crossref
6 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF