



УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У
НОВОМ САДУ



Милорад Трифуновић

**Хетерогени систем за детекцију
аномалија у федеративном окружењу
заснован на ПТБ-ФЛА**

МАСТЕР РАД

Нови Сад, 2026.



УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА
21000 НОВИ САД, Трг Доситеја Обрадовића 6

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, РБР :	
Идентификациони број, ИБР :	
Тип документације, ТД :	Монографска документација
Тип записа, ТЗ :	Текстуални штампани материјал
Врста рада, ВР :	Дипломски – мастер рад
Аутор, АУ :	Милорад Трифуновић
Ментор, МН :	проф. др Мирослав Поповић
Наслов рада, НР :	Хетерогени систем за детекцију аномалија у федеративном окружењу заснован на ПТБ-ФЛА
Језик публикације, ЈП :	Српски / латиница
Језик извода, ЈИ :	Српски
Земља публикавања, ЗП :	Република Србија
Уже географско подручје, УГП :	Војводина
Година, ГО :	2026
Издавач, ИЗ :	Ауторски репринт
Место и адреса, МА :	Нови Сад; трг Доситеја Обрадовића 6
Физички опис рада, ФО : (поглавља/страна/ цитата/табела/слика/графика/прилога)	6/40/12/3/3/0/0
Научна област, НО :	Електротехника и рачунарство
Научна дисциплина, НД :	Рачунарска техника
Предметна одредница/Кључне речи, ПО :	Системи на ивици интернета, Федеративно учење, Изолационе Шуме, Детекција Аномалија, Дистрибуирани системи
УДК	
Чува се, ЧУ :	У библиотеци Факултета техничких наука, Нови Сад
Важна напомена, ВН :	
Извод, ИЗ :	У раду је представљен хетерогени федеративни систем за детекцију аномалија пожара који користи сензор температуре и камеру. За сваки тип података обучава се засебна федеративна изолациона шума, а њихови излази се обједињују у коначну оцену аномалије. Евалуација кроз експериментална понављања потврђује функционалност система и показује компромис између квалитета модела обученог над сликама и утрошка ресурса.
Датум прихватања теме, ДП :	
Датум одбране, ДО :	
Чланови комисије, КО :	Председник: проф. др Јелена Радић
	Члан: проф. др Илија Башичевић
	Члан, ментор: проф. др Мирослав Поповић
	Потпис ментора



KEY WORDS DOCUMENTATION

Accession number, ANO :			
Identification number, INO :			
Document type, DT :	Monographic publication		
Type of record, TR :	Textual printed material		
Contents code, CC :	Master Thesis		
Author, AU :	Milorad Trifunović		
Mentor, MN :	Miroslav Popović, PhD		
Title, TI :	Heterogeneous system for anomaly detection in a federated environment based on PTB-FLA		
Language of text, LT :	Serbian		
Language of abstract, LA :	Serbian		
Country of publication, CP :	Republic of Serbia		
Locality of publication, LP :	Vojvodina		
Publication year, PY :	2026		
Publisher, PB :	Author's reprint		
Publication place, PP :	Novi Sad, Dositeja Obradovica sq. 6		
Physical description, PD : (chapters/pages/ref./tables/pictures/graphs/appendixes)	6/40/12/3/3/0/0		
Scientific field, SF :	Electrical Engineering		
Scientific discipline, SD :	Computer Engineering, Engineering of Computer Based Systems		
Subject/Key words, S/KW :	Edge systems, Federated Learning, Isolation Forests, Anomaly Detection, Distributed Systems		
UC			
Holding data, HD :	The Library of Faculty of Technical Sciences, Novi Sad, Serbia		
Note, N :			
Abstract, AB :	This thesis presents a heterogeneous federated system for fire anomaly detection using temperature sensors and cameras. A separate federated isolation forest is trained for each data type, and their outputs are fused into a final anomaly score. Experimental evaluation confirms that the system functions as intended and highlights the trade-off between camera-model performance and resource use.		
Accepted by the Scientific Board on, ASB :			
Defended on, DE :			
Defended Board, DB :	President:	Jelena Radić, PhD	Menthor's sign
	Member:	Ilija Bašičević, PhD	
	Member, Mentor:	Miroslav Popović, PhD	

	УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА 21000 НОВИ САД, Трг Доситеја Обрадовића 6		Број:
	ЗАДАТАК ЗА ЗАВРШНИ РАД		
			Датум:

Студијски програм:	Рачунарство и аутоматика		
Студент:	Милорад Трифуновић	Број индекса:	E2 89/2023
Степен и врста студија:	Мастер академске студије		
Област:	Електротехника и рачунарство		
Ментор:	проф. др Мирослав Поповић		
НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА ИЗДАЈЕ СЕ ЗАДАТАК ЗА ЗАВРШНИ РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА: - проблем – тема рада; - начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна;			

Наслов завршног рада:

Хетерогени систем за детекцију аномалија у федеративном окружењу заснован на ПТВ-ФЛА

Текст задатка

У оквиру овог мастер рада потребно је урадити следеће:

1. Истражити теоријске основе федеративног учења и постојећи алгоритам за детекцију аномалија.
2. Дати основни преглед употребе изолационе шуме за детекцију аномалија са 1-d и N-d типовима података.
3. Дати преглед РТВ-ФЛА окружења за развој алгоритама федеративног учења.
4. Дати преглед рада алгоритма изолационе шуме у федеративном окружењу РТВ-ФЛА.
5. Развити алгоритам изолационих шума над N-d подацима.
6. Прилагодити алгоритам изолационих шума над N-d подацима за рад у федеративном окружењу РТВ-ФЛА.
7. Дефинисати архитектуру хетерогеног система за детекцију аномалија у федеративном окружењу.
8. Направити скуп података за тестирање алгоритма N-d изолационе шуме.
9. Имплементирати и тестирати хетерогени систем за детекцију аномалија у федеративном окружењу.
10. Дискутовати о експерименталним резултатима тестирања.
11. Дати закључке о применљивости решења у реалним системима на ивици интернета.

Руководилац студијског програма:	Ментор рада:

Примерак за: ☐ - Студента; ☐ - Ментора



УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

21000 НОВИ САД, Трг Доситеја Обрадовића 6

ИЗЈАВА О НЕПОСТОЈАЊУ СУКОБА ИНТЕРЕСА

Изјављујем да нисам у сукобу интереса у односу ментор – кандидат и да нисам члан породице (супружник или ванбрачни партнер, родитељ или усвојитељ, дете или усвојеник), повезано лице (крвни сродник ментора/кандидата у правој линији, односно у побочној линији закључно са другим степеном сродства, као ни физичко лице које се према другим основама и околностима може оправдано сматрати интересно повезаним са ментором или кандидатом), односно да нисам зависан/на од ментора/кандидата, да не постоје околности које би могле да утичу на моју непристрасност, нити да стичем било какве користи или погодности за себе или друго лице било позитивним или негативним исходом, као и да немам приватни интерес који утиче, може да утиче или изгледа као да утиче на однос ментор-кандидат.

У Новом Саду, дана _____

Ментор

Кандидат

Захвалност

Нисам очекивао да ће ми мастер студије тећи како су текле. Током својих мастер студија благословен сам био да стасам професионално у зрелијег инжињера и искуснијег човека који мало мање посматра ствари кроз идеалистичне ружичасте наочаре под којима грешка не сме да постоји. Ове студије су ми пружиле прилику да стекнем искуство у и да се остварим као сарадник у настави чиме сам добио прилику да радим са људима и пружим своја искуства и знања другима млађим од себе не би ли им колико толико олакшао пут који је пред њима. Такође, стицајем околности добио сам прилику да стекнем несвакидашња искуства у овом несвакидашњем времену којем и даље живимо. Као што се да примети, изузетно сам захвалан за искуства која сам добио прилику доживети у овом развојном периоду. Захвалан сам такође и свима вама који читате ово. Чим сте се одлучили да прочитате овај рад, шансе су да сте некако допринели мом развоју за шта вам само могу бити захвалан.

САДРЖАЈ

1. Увод.....	7
2. Теоријске основе и сродни радови.....	8
2.1 Федеративно учење	8
2.2 Проблем детекције аномалија	9
2.3 Изолационе шуме	10
2.3.1 Једнодимензионалне изолационе шуме.....	11
2.3.2 Вишедимензионалне изолационе шуме	11
2.4 РТВ-FLA и МРТ-FLA	12
2.5 Једнодимензионалне изолационе шуме у оквиру окружења РТВ-FLA.....	15
2.6 Преглед сродних радова	16
2.6.1 Вишедимензионалне изолационе шуме	17
2.6.2 Хетерогено федеративно учење	18
3. Предлог решења.....	20
3.1 Архитектура хетерогеног система.....	21
3.2 Федеративна изградња модела.....	21
3.2.1 Федеративни модел на основу података температуре	22
3.2.2 Федеративни модел на основу података са камере	23
3.2.3 Агрегација и синхронизација	24
3.3 Одређивање оцена аномалије.....	25
3.4 Обједињавање излаза оба модела	26
3.4.1 Континуалне стратегије фузије	26
3.4.2 Стратегије одлучивања на основу прагова	26
3.5 Ток извршавања и имплементациони детаљи	27

3.6	Ограничења предложеног система	27
4.	Експериментална евалуација	29
4.1	Евалуационе метрике	29
4.2	Поставка експеримента.....	30
4.2.1	Наслеђена једнодимензионална поставка	30
4.2.2	Хетерогени скуп података	30
4.2.3	Протоколи тестирања	31
4.3	Резултати и дискусија	32
4.3.1	Резултати појединачних модела и фузије.....	32
4.3.2	Утицај протокола задржавања и сложености модела	33
4.3.3	Време извршавања и меморија	33
4.3.4	Ограничења експерименталне евалуације	35
4.3.5	Закључак експерименталне евалуације	35
5.	Закључак	36
6.	Литература.....	38

СПИСАК СЛИКА

Слика 1 – Дводимензионални пример аномалије	9
Слика 2 – Средње AUC-ROC и AUC-PR вредности главне конфигурације за $n=40$..	33
Слика 3 – Поређење средњег времена и меморије за конфигурацију 25x6	34

СПИСАК ТАБЕЛА

Табела 1 – Поставка експеримената хетерогеног система.....	31
Табела 2 – Предиктивне метрике главне конфигурације 100x15, n=40.....	32
Табела 3 – Време и вршна меморија федеративне обуке, n=40	34

СКРАЋЕНИЦЕ

PTB-FLA - *Python Testbed for Federated Learning Alghoritms*

MPT-FLA - *MicroPython Testbed for Federated Learning Algorithms*

ФЛ - *федеративно учење*

API - *Application Programing Interface*

TCP - *Transmission Control Protocol*

ФПП - *функција повратног позива*

PCA – *Principal Component Analysis*

1. Увод

Федеративно учење се у корену бави проблемом налажења глобалног модела једног дистрибуираног система на ивици интернета. У оквиру дистрибуираног система неретко се можемо сустрести са системима који баратају са два или више типова сензорских уређаја. Ово значи да за систем са различитим типовима сензорских уређаја, тј. података може се десити да хетерогени систем поседује скуп више глобалних модела уместо само једног који одржава и шаље одговарајућим сензорским уређајима назад након обучавања. У случају скупа више различитих модела, потребно је онда развити и стратегије обједињавања резултата тј. излаза тих модела.

Овај рад се бави развијањем једног таквог сензорски хетерогеног система за детекцију аномалија пожара. Сензор температуре и камера су употребљени као сензорски уређаји. Федеративна шума прилагођена федеративном окружењу је употребљена за детекцију аномалија и над температурним и камерним подацима. Над уређајима са камером развијена је федеративна шума прилагођена за обраду слике, тј. обраду вишедимензионалних података, док се над уређајима који мере температуру користи једнодимензионална изолациона шума прилагођена за федеративно окружење. На крају, развијене су одређене стратегије обједињавања резултата ова два различита модела како би се добио један униформан резултат на основу ког систем може да одлучи да ли је на основу мерења примећен пожар, тј. аномалија или не.

Рад је организован у шест поглавља. Друго поглавље се бави покривањем теоријских основа које представљају предуслов за целокупно разумевање овог рада. Треће поглавље се бави представљањем решења и уједно представља срж рада. Четврто поглавље се бави експерименталном евалуацијом решења. У петом поглављу се даје резиме и закључај рада. Поголавље шест даје преглед литературе и изворе на које се овај рад ослања.

2. Теоријске основе и сродни радови

2.1 Федеративно учење

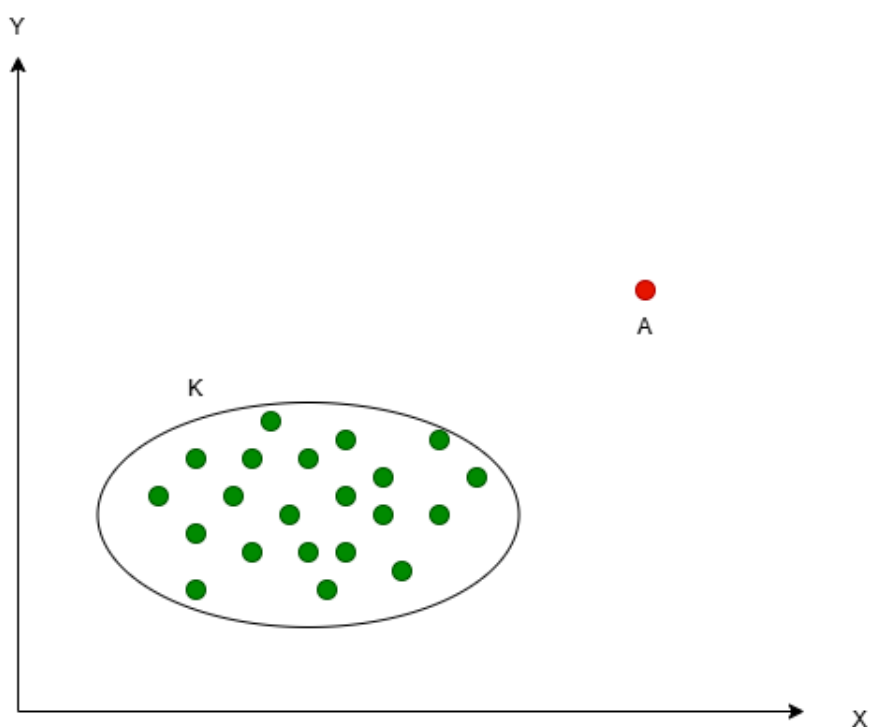
Неретко се данас можемо сустрести са системима где један тип уређаја (*клијент*) бива распоређен у више различитих окружења. Уколико уређаји поседују модел, често ћемо желети да овај модел буде у потпуности, или барем делом дељен између свих осталих уређаја у систему. Један начин долажења до заједничког модела може бити да сви уређаји шаљу своје стечене податке током рада једном централизованом уређају (*серверу*) ради рачунања модела где након рачунице модел бива послат назад свим клијентским уређајима за употребу. Овај начин учења поседује неколико мана. Прва је да уколико су подаци осетљиве природе, рецимо да су у питању мобилни телефони који поседују приватне фотографије корисника, често је неприхватљиво да такви подаци буду слати за централно обучавање. Такође, друга мана која се испољава у оваквом случају је да подаци који се шаљу могу носити велику количину информација и тиме могу оптерећивати и заситити мрежу. Федеративно учење настоји да реши ова два проблема.

Федеративно учење [1] представља технику машинског учења где сваки клијент на основу својих локалних података обучава локални модел и уместо да клијентски уређаји шаљу своје сирове снимљене податке северском уређају, послаће свој локални модел. Серверски уређај, који оркестрира скуп клијентских уређаја, на основу свих пристиглих клијентских модела рачуна заједнички глобални модел. Добијени глобални модел се онда шаље назад сваком клијентском уређају за даљу употребу. Суштинска предност и мотивација за употребу овакве технике машинског учења огледа се у томе што уместо да се шаљу сирови подаци који у себи могу да садрже осетљиве податке и могу по својој

вечичини да оптерете мрежу, шаље се један модел који не представља ништа друго но скуп тежина из којих није тривијално извући конкретне информације на основу којих је модел обучен чиме се постиже већи анонимитет података над којим је трениран модел. Уколико се процес федеративног учења не обавља често, овакав приступ такође постаје прилично погодан за употребу над уређајима са ограниченим ресурсима који раде на ивици интернета. Смањивањем количине података које је потребно послати уједно и умањује количину енергије коју је потребно утрошити за слање података.

2.2 Проблем детекције аномалија

По основној дефиницији [2], проблем детекције аномалија се дефинише као проблем препознавања податка који по својим особинама знатно одступа од скупа који доминантно садржи регуларне податке. Овакав податак који одступа од регуларног скупа се назива *аномалија*. На наредној слици се може видети пример аномалије на дводимензионалним скупом података.



Слика 1 – Дводимензионални пример аномалије

На датој слици скуп K представља скуп тачака класификованих као регуларни и очекивани подаци док тачка A представља аномалију.

Значај детекције аномалија се огледа у томе да аномалије иако ретке, могу представљати битну информацију на коју је потребно реаговати. Аномалија на медицинској слици може указивати на здравствени проблем пацијента. Аномалија у мрежном саобраћају може представљати потенцијални спољашњи напад на систем. Аномалија у мерењу температуре може представљати пожар.

Један од учесталих проблема код класификације аномалија јесте што врло често аномалије бивају неозначене током лабелирања или ако су ипак урачунате у обучавајући скуп, такође често представљају изузетно мали проценат укупног скупа података да би биле ефикасно примећене касније. Због тога се у детекцији аномалија типично користе ненадгледане или полунадгледане методе учења, које покушавају да науче карактеристике нормалног понашања и на основу тога идентификују аномалије који знатно одступају.

Још један проблем детекције аномалија јесте генерализација методе за детекцију аномалије. Неретко да би се аномалија тачно открила, потребно је претходно познавати контекст у коме се аномалија појављује и због променљивости контекста често један метод у једном контексту неће имати исту тачност у другом.

2.3 Изолационе шуме

Један од честих проблема у детекцији аномалија јесте чињеница да су аномалије у великом броју практичних примена ретке и да често нису означене у скупу података који се користи за обучавање модела. Због тога класични надгледани приступи класификацији, који захтевају довољан број примера сваке класе, нису увек погодни за овај тип проблема. *Изолационе шуме* [3] представљају ненадгледани алгоритам за детекцију аномалија који настоји да овај проблем реши без потребе за експлицитно означеним примерима аномалија.

Основна идеја изолационих шума заснива се на претпоставци да се аномалије лакше изолују од уобичајених података. Разлог за то је што су аномалије најчешће ретке и по својим вредностима се разликују од већине узорака у скупу података. Алгоритам зато не покушава директно да моделује расподелу нормалних података, већ насумичним поделама простора покушава да изолује појединачне узорке.

Изолациона шума се састоји од већег броја случајно генерисаних бинарних стабала званим изолационим стаблима. У сваком стаблу се рекурзивно врши насумична подела података све док се појединачни узорак не изолује или док се не достигне задата максимална дубина стабла. Број подела потребних за изоловање узорака представља основу за одређивање његовог степена аномалности. Узорак који се може изоловати након малог броја подела има већу вероватноћу да представља аномалију, док је за узорке који припадају густим областима нормалних података обично потребан већи број подела.

2.3.1 Једнодимензионалне изолационе шуме

Код једнодимензионалних података сваки узорак представљен је једном нумеричком вредношћу x_i . Скуп од n узорака може се представити као: $X = \{x_1, x_2, \dots, x_n\}$. Конструкција изолационог стабла заснива се на насумичном избору вредности поделе p из интервала између минималне и максималне вредности тренутно посматраног скупа: $p \in [\min(X), \max(X)]$. Након избора вредности p , скуп се дели на два подскупа $X_L = \{x_i \mid x_i < p\}$ и $X_R = \{x_i \mid x_i \geq p\}$. Поступак се затим рекурзивно понавља над оба добијена подскупа. Да би се рекурзија зауставила, један од следећих услова мора бити задовољен: (1) у посматраном чвору налази само један узорак, (2) у посматраном чвору налази се скуп истих вредности или, (3) када се достигне максимално дозвољена дубина стабла.

За узорак x , дужина пута $h(x)$ представља број грана које је потребно проћи од корена стабла до завршног чвора који садржи тај узорак. Пошто се изолациона шума састоји од више стабала, за процену аномалности користи се просечна дужина пута $E[h(x)]$. Кратка просечна дужина пута указује на то да је узорак релативно лако одвојити од остатка скупа. Такав узорак има већи степен аномалности. Са друге стране, узорци који се налазе у областима са великим бројем других узорака захтевају већи број подела и имају дужу просечну дужину пута.

Једна од важних особина изолационих шума је то што се приликом конструкције стабала најчешће не користи цео скуп података, већ насумично изабран подскуп величине Ψ . На тај начин смањује се рачунска сложеност, али се истовремено олакшава изолација аномалних узорака. Сложеност конструкције једног изолационог стабла над Ψ узорака приближно је $O(\Psi \log(\Psi))$. Ако се шума састоји од t стабала, укупна сложеност обучавања је приближно $O(t \Psi \log(\Psi))$. За одређивање степена аномалности једног новог узорака потребно је проћи кроз сва стабла, па је просечна сложеност $O(t \log(\Psi))$.

2.3.2 Вишедимензионалне изолационе шуме

Код вишедимензионалних података сваки узорак представљен је вектором од d карактеристика $x_i = [x_{i1}, x_{i2}, \dots, x_{id}]$. Скуп података може се записати као $X = [x_1, x_2, \dots, x_i]$. Сваки узорак представља једну тачку у d -димензионалном простору.

Основни принцип изолације остаје исти као у једнодимензионалном случају, али је поред вредности поделе потребно одредити и димензију по којој ће се подела вршити.

Приликом формирања сваког унутрашњег чвора изолационог стабла најпре се насумично бира једна карактеристика $q \in \{1, 2, \dots, d\}$, након чега се за изабрану карактеристику одређује минимална и максимална вредност у тренутно посматраном

подскупу и насумично бира вредност поделе p где $p \in [\min(x_q), \max(x_q)]$. Скуп се затим дели на $X_L = \{x_i \mid x_{iq} < p\}$ и $X_R = \{x_i \mid x_{iq} \geq p\}$.

Поступак се као и раније рекурзивно наставља све док: (1) у посматраном чвору налази само један узорак, (2) у посматраном чвору налази се скуп више узорака истих вредности или, (3) када се достигне максимално дозвољена дубина стабла.

На овај начин свако стабло постепено дели d -димензионални простор на мање области. Пошто се и димензија и граница поделе бирају насумично, различита стабла формирају различите партиције истог простора. И код вишедимензионалних података степен аномалности одређује се на основу просечне дужине $E[h(x_i)]$.

Ако се узорак налази у области простора која је ретко насељена или је по својим карактеристикама значајно издвојена од већине осталих узорака, обично ће бити изолован након релативно малог броја подела. Насупрот томе, узорци који се налазе у густим областима простора захтевају већи број рекурзивних подела.

Суштинска разлика између једnodимензионалног и вишедимензионалног случаја налази се у поступку поделе простора. Код једnodимензионалних података потребно је изабрати само вредност поделе. Код вишедимензионалних података потребно је најпре изабрати једну од расположивих димензија, а затим вредност поделе по тој димензији.

За $d = 1$, поступак се своди на класичну поделу бројевне осе. За $d = 2$, свака подела представља вертикалну или хоризонталну границу (тј. линију) у равни. За произвољан број димензија, поделе представљају хиперравни ортогоналне на једну од координатних оса.

Основна временска сложеност изградње класичне изолационе шуме остаје приближно $O(t \Psi \log(\Psi))$ јер се у сваком чвору за поделу користи само једна насумично изабрана карактеристика.

Ипак, број димензија d утиче на количину меморије потребне за чување улазних података. За N узорака са по d карактеристика, просторна сложеност самог скупа података је $O(N d)$.

2.4 PTB-FLA и MPT-FLA

Развој и испитивање алгоритама федеративног учења подразумева постојање већег броја међусобно повезаних учесника који локално обрађују своје податке и размењују само информације неопходне за формирање заједничког модела. Имплементација целокупне комуникационе инфраструктуре, управљања процесима и синхронизације може значајно да усложни развој новог алгорита. PTB-FLA [4] (*енгл. Python Testbed for Federated Learning*

Algorithms) развијен је са циљем да обезбеди једноставно извршно окружење у којем се алгоритми федеративног учења могу развијати и испитивати без потребе да се за сваки алгоритам посебно имплементира целокупна дистрибуирана инфраструктура. Аутори због тога PTB-FLA описују као алгоритамско тестно окружење, односно као окружење у које се алгоритам федеративног учења може интегрисати и затим тестирати.

PTB-FLA је реализован у програмском језику Python и ослања се на стандардне Python механизме, без додатних спољашњих зависности. Овакав приступ има две важне последице: окружење је релативно једноставно за инсталацију и употребу, а истовремено има мали софтверски отисак. Основна верзија PTB-FLA намењена је извршавању на једном рачунару, при чему се различити учесници федеративног система представљају као независни процеси. На тај начин је на једној машини могуће формирати контролисано окружење које по начину рада одговара систему са више федеративних чворова.

Архитектура PTB-FLA система заснива се на скупу инстанци апликације и одговарајућем скупу инстанци тестног окружења. Посебан покретач креира потребан број независних процеса, при чему сваки процес представља један чвор федеративног система. Апликациони део дефинише конкретан алгоритам, док PTB-FLA преузима одговорност за комуникацију између чворова и правилно извршавање корака федеративног алгоритма. Ова подела омогућава да се логика самог алгоритма посматра одвојено од механизма неопходних за његово дистрибуирано извршавање.

Једна од главних карактеристика PTB-FLA јесте ограничен и једноставан програмски модел. Програмер пише један апликациони програм који се затим покреће у више независних процеса. Конкретно понашање алгоритма задаје се првенствено кроз функције повратног позива (*callback* функције) за клијентску и серверску улогу. Генерички део федеративног алгоритма, укључујући размену порука и редослед извршавања појединих фаза, налази се унутар самог PTB-FLA окружења. Оваква организација је погодна за развој алгоритама јер омогућава истраживачу да се концентрише на начин локалне обраде података и агрегације резултата, уместо на детаље комуникације и управљања процесима.

PTB-FLA обезбеђује генеричку подршку за централизоване и децентрализоване алгоритме федеративног учења. Код централизованог приступа један чвор има улогу сервера, док остали чворови имају улогу клијената. Сервер прослеђује своје локалне податке или модел клијентима, клијенти израчунавају локалне измене, а сервер затим прикупља и агрегира добијене резултате. Комуникациона структура у овом случају има облик звезде. Код децентрализованог приступа не постоји стални централни сервер, већ чворови имају равноправнију улогу и током извршавања наизменично обављају серверске

и клијентске функције. Комуникациона структура тада може имати облик потпуно повезаног графа.

Важан аспект оваквог окружења је раздвајање локалних података модела од приватних података за обучавање. Локални модел може бити размењиван између чворова као део федеративног алгоритма, док приватни подаци остају у оквиру процеса којем припадају и прослеђују се само локалним callback функцијама. На овај начин PTB-FLA прати основни принцип федеративног учења према којем подаци за обучавање не напуштају локални чвор.

Погодност PTB-FLA за развој и тестирање федеративних алгоритама произилази управо из комбинације ових особина. Истраживач може на једном рачунару да покрене више логички независних чворова, да испитује централизоване и децентрализоване начине рада и да мења алгоритамску логику без поновне имплементације комуникационог слоја. Истовремено, једноставан API и употреба callback функција смањују количину инфраструктурног кода који је потребно написати.

Главна ограничење оригиналног PTB-FLA окружења јесте то што се све инстанце извршавају на истом рачунару. Због тога је оно пре свега погодно за развој, функционално тестирање и почетну валидацију алгоритама, док не представља потпуну симулацију стварног дистрибуираног система у којем се чворови налазе на различитим уређајима и комуницирају преко физичке мреже.

Као наставак развоја PTB-FLA настао је MPT-FLA (*енгл. MicroPython Testbed for Federated Learning Algorithms*). Он задржава основни концепт и предности свог претходника, али омогућава да се појединачни чворови извршавају на различитим мрежним уређајима, као што су персонални рачунари и IoT платформе. MPT-FLA је заснован на MicroPython-у и асинхроним Python механизмима (*asyncio*), што омогућава његово извршавање и на уређајима са ограниченим ресурсима. У раду је окружење експериментално проверено на бежичној мрежи која је обухватала персонални рачунар и Raspberry Pi Pico W уређаје.

За потребе овог рада, коришћен је PTB-FLA за развој решења о коме ће се дискутовати у поглављу трећем поглављу. Један смер даљег истраживања може бити прилагођавање и превођење решења у PTB-FLA окружење.

2.5 Једнодимензионалне изолационе шуме у оквиру окружења PTB-FLA

У раду [5] аутора П. Васиљевића, М. Матић и М. Поповића представљена је примена федеративне изолационе шуме за детекцију аномалија на подацима о температури. У конкретном случају сваки посматрани узорак представља једну вредност температуре, па се алгоритам примењује над једнодимензионалним скупом података. Као основа решења коришћен је алгоритам FLiForest [9], који прилагођава принцип изолационих шума федеративном учењу, док је његова специјализација реализована у PTB-FLA окружењу и названа PFLiForest [5].

Основни проблем при преласку са класичне изолационе шуме на федеративно окружење јесте начин изградње заједничких стабала. Код класичног алгоритма целокупан скуп података доступан је процесу који конструише стабло и на основу њега бира вредности по којима се подаци деле. У федеративном систему, са друге стране, подаци морају остати локални код клијената. Због тога није могуће једноставно прикупити све узорке на серверу и над њима изградити класичну изолациону шуму. У раду се овај проблем решава преузимањем основног приступа FLiForest алгоритма, где се стабло гради слој по слој, а између учесника се размењују вредности поделе, а не сами приватни подаци.

PFLiForest је организован као централизовани федеративни алгоритам са једним сервером и више клијената. Клијенти располажу сопственим локалним скуповима података, док сервер оркестрира процес изградње заједничког модела. За комуникацију и оркестрацију користи се генерички централизовани алгоритам који обезбеђује PTB-FLA. На овај начин инфраструктура за размену порука остаје сакривена од саме логике изолационе шуме.

Кључна промена у односу на секвенцијалну изолациону шуму односи се на одређивање вредности поделе чворова стабла. Уместо да један процес одреди поделу на основу свих података, сваки клијент користи сопствене приватне податке да израчуна локални предлог вредности поделе. Ове вредности се шаљу серверу, који их агрегира и формира заједничку вредност поделе. У конкретној реализацији описаној у раду, сервер врши агрегацију усредњавањем вредности добијених од активних клијената. Добијена глобална вредност затим се користи приликом изградње одговарајућег чвора стабла.

Након што се добије глобална вредност поделе, сваки клијент њоме дели сопствени локални скуп података на одговарајуће партиције и наставља изградњу стабла. Поступак се понавља све док се не достигне задата максимална дубина или док локални подаци у одговарајућој грани више не могу да се раздвајају. Самим тим, клијенти учествују у

формирању заједничке структуре стабла, али њихови оригинални подаци не морају да буду прослеђени серверу.

Друга битна измена односи се на сам начин изградње стабла. Уместо рекурзивног приступа који је природан за конструкцију бинарног стабла, PFLiForest користи ред (*deque*) у коме се чувају чворови и одговарајуће партиције које тек треба обрадити. Чворови се тако обрађују итеративно. Ова измена уведена је ради прилагођавања начина изградње стабла PTB-FLA окружењу и омогућава да се између обраде појединачних чворова извршавају потребне федеративне комуникационе фазе.

Пошто различити клијенти могу имати различите локалне податке, није неопходно да сви заврше изградњу стабла у истом тренутку. Због тога је у PFLiForest уведен додатни механизам синхронизације фаза. Клијент који је завршио изградњу тренутног стабла прелази у стање мировања и више не доставља вредности за даљу агрегацију. Сервер приликом агрегације игнорише такве клијенте, а када сви клијенти заврше стабло, сервер прослеђује сигнал за завршетак тренутне фазе. Ово спречава да поједини клијенти започну изградњу наредног стабла док остали још увек конструишу претходно. Изолациона шума се након тога формира понављањем описаног поступка за задати број стабала. Резултујући модел представљен је као листа изолационих стабала, при чему сваки чвор садржи вредност поделе и референце на леву и десну грану.

Након изградње модела, детекција аномалија задржава основни принцип класичне изолационе шуме. За посматрану вредност пролази се кроз стабла и одређује дужина пута потребна да се та вредност изолује. На основу просечне дужине пута кроз сва стабла формира се оцена аномалије, која се затим пореди са одговарајућим прагом. Федеративни аспект решења се, према томе, првенствено односи на заједничку изградњу модела, док основни принцип коришћења већ обучене изолационе шуме за одређивање оцене аномалије остаје непромењен.

2.6 Преглед сродних радова

Сродни радови од значаја за овај рад могу се посматрати из два правца. Први правац обухвата развој изолационих шума за рад над вишедимензионалним подацима и измене начина на који се простор података дели током изградње изолационих стабала. Други правац обухвата хетерогено федеративно учење, односно приступе који омогућавају заједничко учење у системима у којима клијенти не морају имати исту расподелу података, исти модел или исте хардверске могућности.

2.6.1 Вишедимензионалне изолационе шуме

Оригинални алгоритам изолационе шуме [3] није ограничен на једнодимензионалне податке. Код вишедимензионалног улаза сваки узорак представља тачку у простору више карактеристика, а приликом формирања чвора случајно се бира једна карактеристика и вредност поделе унутар њеног опсега. На тај начин се простор дели хиперравнима које су ортогоналне на једну од координатних оса. Овај приступ задржава једноставност оригиналног алгоритма, али начин поделе може постати ограничење када аномалност узорка не зависи од једне карактеристике појединачно, већ од њихове међусобне зависности.

Једно од раних проширења овог приступа представља SciForest (енгл. *Isolation Forest with Split-selection Criterion*), који су предложили Liu, Ting и Zhou [7]. За разлику од класичне изолационе шуме, код које се у сваком чвору користи само једна случајно изабрана карактеристика, SCiForest омогућава формирање хиперравни на основу више карактеристика истовремено. Од више случајно генерисаних кандидата бира се хиперраван и вредност поделе према посебном критеријуму поделе. Основна мотивација овог приступа јесте детекција груписаних аномалија, које могу бити релативно близу регуларним подацима и због тога теже уочљиве применом класичних случајних подела. Посебно је значајно што овај приступ омогућава да једна подела истовремено зависи од више димензија улазног простора.

Сличан проблем начина поделе вишедимензионалног простора разматра се у раду “*Extended Isolation Forest (EIF)*” [8]. Аутори указују да осно-поравнате поделе класичне изолационе шуме могу увести зависност резултата од оријентације података у простору. Уместо избора једне карактеристике и једне вредности поделе, EIF дозвољава употребу хиперравни произвољне оријентације. Хиперраван се дефинише случајним правцем и случајно изабраном тачком кроз коју пролази, након чега се узорци раздвајају у зависности од стране хиперравни на којој се налазе. На тај начин поступак изолације више није ограничен искључиво на вертикалне, хоризонталне, односно у општем случају осно-поравнате поделе. Ова особина је нарочито значајна код података чија структура зависи од комбинације више карактеристика.

За потребе овог рада употребљени су радови [3] и [5] као основа алгоритма изолационих шума над вишедимензионалним подацима. Остали наведени приступи показују два могућа правца проширења изолационих шума над вишедимензионалним подацима. SCiForest и EIF мењају геометрију самог поступка поделе и омогућавају да се приликом формирања границе узима у обзир више карактеристика истовремено, док RIFI мења критеријум избора подела са циљем очувања структуре података.

2.6.2 Хетерогено федеративно учење

Шири преглед савремених приступа федеративном учењу дат је у раду “*Recent advances on federated learning: A systematic survey*” [6]. Аутори предлажу поделу приступа федеративном учењу на четири веће групе: оптимизацију агрегације, хетерогено федеративно учење, безбедно федеративно учење и правично федеративно учење. За овај рад од највећег значаја је хетерогено федеративно учење. У наведеном прегледу хетерогеност федеративног система посматра се на три различита нивоа: хетерогеност података, хетерогеност модела и системска хетерогеност. Ова подела је значајна јер различити облици хетерогености захтевају различите начине прилагођавања класичног федеративног поступка.

Хетерогеност података настаје када локални скупови података различитих клијената немају исту статистичку расподелу, што представља чест случај у реалним федеративним системима. Различита расподела података може даље довести до тога да локални клијенти конвергирају ка својим локалним оптимумима који се могу знатно разликовати. У моменту усредњавања ових оптимума ради рачунања глобалног модела, локални модели могу се подударити тако да се на крају добије лошији глобални модел који не одговара свим клијентима. Прегледни рад [6] издваја више група приступа овом проблему.

Једна група представља приступе засновани на мета-учењу, као што је Per-FedAvg. Код ових метода циљ није да се формира један глобални модел који је непосредно оптималан за све клијенте, већ модел који представља погодну почетну тачку за локалну персонализацију. Након формирања таквог модела, сваки клијент га са малим бројем локалних корака учења прилагођава сопственој расподели података. На овај начин глобални модел садржи заједничко знање прикупљено од више клијената, док се истовремено омогућава прилагођавање специфичностима појединачних локалних скупова података. Поред тога, користе се трансфер учење и локално дообучавање глобалног модела, као и приступи засновани на груписању клијената [6].

Други облик хетерогености представља хетерогеност модела. Класични алгоритми као што је FedAvg претпостављају да сви клијенти поседују моделе исте архитектуре, тако да се одговарајући параметри могу директно агрегирати. У реалном систему ова претпоставка не мора бити испуњена. Различити уређаји могу располагати различитим ресурсима или користити различите архитектуре прилагођене свом типу података, због чега директно усредњавање параметара више није могуће.

Један од приступа овом проблему представља FedMD [10], који омогућава федеративно учење између клијената са различитим моделима применом трансфера знања и дестилације модела. Уместо захтева да сви учесници имају идентичну структуру мреже и

да се директно агрегирају њени параметри, тежиште се пребацује на размену заједничког знања које различити модели могу да користе. Сличан смер представљају приступи засновани на ансамбл-дестилацији, где се информације више различитих локалних модела користе за формирање заједничког знања.

Посебно решење за хетерогеност модела представља алгоритам HeteroFL [11]. Он је намењен систему у којем клијенти имају различите рачунарске и комуникационе могућности. Клијентима се зато могу доделити модели различитих величина, док се при агрегацији обједињују параметри који представљају заједничке делове тих модела. На овај начин слабији уређаји могу учествовати у федеративном процесу без потребе да обучавају целокупан модел исте величине као ресурсно снажнији клијенти.

Трећу групу представља системска хетерогеност, која се не односи непосредно на структуру података или модела, већ на различите могућности уређаја. Клијенти могу имати различиту процесорску снагу, количину расположиве меморије, брзину комуникације и доступност. Један од проблема који из тога настаје јесу спори клијенти који могу продужити трајање целе федеративне рунде.

За систем који се развија у овом раду посебно је интересантна хетерогеност која настаје због постојања различитих типова сензорских уређаја. Сензор температуре и камере не генеришу податке исте структуре, па самим тим није природно претпоставити да сви клијенти могу користити један идентичан модел. Због тога се проблем може посматрати као комбинација хетерогености података и модела. Уместо формирања једног глобалног модела за све типове уређаја, у овом раду се полази од могућности да различите групе уређаја поседују различите моделе, након чега је потребно објединити њихове излазе у јединствену одлуку система.

Овај приступ се разликује од већине описаних решења за хетерогеност модела. FedMD [10] и сродни приступи из [6] настоје да пренесу знање између различитих архитектура, док HeteroFL [11] настоји да омогући заједничко обучавање варијанти истог модела различите сложености. Са друге стране, код система са различитим типовима сензора различити модели могу имати различите улазе и различиту интерну структуру, тако да непосредно обједињавање њихових параметара није неопходно нити увек могуће. У том случају хетерогеност се може решавати задржавањем више одвојених федеративних модела и накнадним обједињавањем њихових резултата, што представља полазну идеју за решење описано у наредном поглављу.

3. Предлог решења

У овом поглављу представљено је решење хетерогеног федеративног система за детекцију појаве пожара на основу два сензорска типа података: мерења температуре и слика добијених камерама. Полазиште представља федеративна изолациона шума PFLiForest описана у раду [5], која омогућава заједничку изградњу модела без слања изворних података серверу. За разлику од система из рада [5], у коме је сваки клијент обрађивао само једнодимензионалне температурне вредности, сваки клијентски чвор предложеног система обрађује два улаза различите структуре и зато одржава два одвојена модела.

Основна идеја решења јесте да сваки клијентски чвор поседује две федеративне изолационе шуме. Модел заснован на температури обучава се над једнодимензионалним вредностима, док се модел заснован на слици обучава над векторима карактеристика издвојеним из слика. Модели се не обједињавају на нивоу параметара, јер њихови улази и чворови стабала немају исто значење. Уместо тога, њихови нормализовани излази обједињавају се локално на чвору током закључивања. Таква организација задржава специјализован модел за сваки тип сензора, а систему ипак обезбеђује један резултат који означава степен сумње да је у посматраном простору присутан пожар.

Решење прати програмски модел окружења PTB-FLA и MPT-FLA: апликациони део дефинише локалну обраду и серверску агрегацију кроз функције повратног позива, док окружење обезбеђује комуникацију и редослед извршавања федеративних фаза. Прототип и експериментална евалуација изведени су у PTB-FLA окружењу, а исте улоге клијента и сервера могу се пренети на MPT-FLA ради извршавања на физички раздвојеним уређајима на ивици интернета. У наставку су описани архитектура система, поступак изградње оба модела, одређивање оцена аномалије и стратегије обједињавања резултата.

3.1 Архитектура хетерогеног система

Предложени систем је организован као централизовани федеративни систем са једним оркестрационим сервером и скупом клијентских чворова. Сваки клијентски чвор садржи сензор температуре и камеру, локално чува оба скупа података и поседује две изолационе шуме. Оркестрациони сервер не поседује сирове сензорске податке, већ оркестрира федеративне рунде, прикупља локалне предлоге подела и формира глобалне параметре чворова стабала. Комуникациона топологија наслеђена је из рада [5] и има облик звезде: клијенти комуницирају са сервером, али међусобно не размењују приватне податке.

Са становишта обуке, систем садржи две узастопне федеративне фазе над истим скупом клијентских чворова. У првој фази локалне температурне вредности учествују у формирању глобалне једнодимензионалне изолационе шуме. У другој фази локалне карактеристике слика учествују у формирању глобалне вишедимензионалне изолационе шуме. Оркестрациони сервер за сваку фазу одржава одвојено стање: ред чворова који се обрађују, текућу фазу, број формираних стабала и одговарајући глобални модел. Такво раздвајање спречава мешање параметара различитих модалитета.

Фаза обучавања извршава се секвенцијално, најпре за температурну, а затим за камерну шуму. Овакав редослед поједностављује синхронизацију и омогућава употребу исте инстанце федеративног окружења, а не утиче на логичку независност модела. По завршетку обе федеративне фазе сваки клијентски чвор располаже шумом обученом мерењима температуре и шумом обученом на сликама. У фази закључивања чвор истом догађају придружује две оцене аномалије и локално их обједињава у јединствену одлуку.

При обради новог догађаја претпоставља се да мерење температуре и узимање слика на истом чвору описују исто посматрано место у приближно истом временском интервалу. Упаривање се врши локално на основу временске ознаке, па ради фузије није потребно слати сирову слику или низ вредности температуре серверу. Чвор најпре израчунава две скаларне оцене, а затим над њима примењује изабрану стратегију фузије.

3.2 Федеративна изградња модела

Оба модела граде се по истом општем поступку преузетом из PFLiForest алгоритма [5]. Изолациона шума формира се као уређена листа од T бинарних стабала, што за сваки од два модела можемо записати као:

$$F = (\tau_1, \tau_2, \dots, \tau_T)$$

Свако стабло гради се итеративно, обиласком по нивоима. На клијенту i ред у почетку садржи корен r , његов цео локални скуп D_i и дубину нула; касније сваки елемент реда садржи текући чвор v , локалну партицију која му припада и дубину тог чвора:

$$Q_i^0 = [(r, D_i, 0)]; (v, D_{i,v}, \ell_v) \in Q_i$$

Пре прикупљања предлога сервер задаје исти индекс карактеристике q_v свим активним клијентима. Код модела на основу података температуре он је увек нула, а код моделе на основу података слике се равномерно насумично бира међу d расположивих карактеристика:

$$q_v = 0 \text{ (температура),}$$

$$q_v \in [0, \dots, d - 1] \text{ (камера)}$$

Сваки чвор чува глобалну вредност поделе p_v , заједнички индекс карактеристике q_v и референце на левог и десног потомка. Његов запис је:

$$v = (p_v, q_v, v_L, v_R)$$

За сваки чвор активни клијенти израчунавају локални предлог поделе. Сервер агрегира важеће предлоге тежинском средином описаном у одељку 3.2.3 и свима враћа исту глобалну поделу p_v за изабрано q_v . Клијент i тада своју партицију дели на леву и десну:

$$D_{i,v}^L = \{x \in D_{i,v} | x_{q_v} < p_v\}$$

$$D_{i,v}^R = \{x \in D_{i,v} | x_{q_v} \geq p_v\}$$

Пошто се размењују параметри поделе, величине локалних партиција и контролне поруке, ниједан корак изградње не захтева слање оригиналних узорака серверу.

Изградња гране на клијенту i престаје када је достигнута максимална дубина, када његова локална партиција има највише један узорак или када вредности изабране карактеристике у тој партицији више нису различите.

Када су све гране завршене, добијено стабло додаје се шуми и започиње изградња наредног стабла.

3.2.1 Федеративни модел на основу података температуре

За модел трениран на подацима температуре локална партиција клијента i представљена је скупом скаларних вредности D_i . Активни клијент насумично бира локалну вредност поделе p_i између минималне и максималне вредности текуће партиције. Поред вредности p_i , клијент одређује број узорака који би се нашли у левој и десној партицији. Серверу се, према томе, шаље предлог (p_i, n_i^L, n_i^R) , а не појединачна мерења температуре.

Ако локална партиција не садржи довољно различитих вредности, клијент шаље ознаку да за посматрани чвор нема важећи предлог.

Након пријема глобалне вредности поделе p , сваки клијент дели своју партицију на $D_i^L = \{x \in D_i | x < p\}$ и $D_i^R = \{x \in D_i | x \geq p\}$. Тако сви клијенти користе исту структуру модела, иако су њихове локалне расподеле различите. Поступак одговара једнодимензионалном решењу из рада [5], уз употребу величине партиције приликом агрегације како би допринос клијента био сразмеран количини података на основу које је формиран његов предлог.

3.2.2 Федеративни модел на основу података са камере

Модел обучен на подацима слике проширује описани федеративни поступак на слике. За разлику од једнодимензионалне температуре, слика садржи велики број вредности које би директну изградњу изолационе шуме учиниле споријом и захтевнијом у погледу меморије. Зато се пре изградње изолационе шуме слика претвара у краћи вектор карактеристика. Током федеративне изградње размењују се предлози подела, а не сирове слике.

У прототипу полазна слика има 210×140 пиксела. Из ње се издваја црвени канал, а вредности пиксела деле се са 255 како би биле у интервалу $[0,1]$. Потом се слика претвара у низ од 29.400 бројева, где сваки број одговара једном пикселу црвеног канала. Анализа главних компоненти (енгл. Principal Component Analysis, PCA) сажима тај низ пре уласка у изолациону шуму.

Интуитивно, PCA учи из нормалних слика из скупа за обучавање како се оне међусобно разликују од просечне слике. На основу тих разлика издваја обрасце које називамо главним компонентама. Једна компонента може, на пример, описивати промену осветљености већег дела слике, али не мора одговарати једном конкретном предмету или делу слике. Њена вредност показује колико је одређени образац изражен у посматраној слици.

За сваку слику PCA враћа 100 вредности главних компоненти уместо 29.400 интензитета пиксела. Компоненте не представљају 100 изабраних пиксела, већ сажету информацију из целе слике. Тако добијени вектор чини улаз изолационе шуме обученој на подацима слике, која у овој поставци има 100 улазних карактеристика.

PCA се обучава искључиво са 200 нормалних слика које су додељене обуци два клијента, по 100 слика сваком. Преосталих 151 слика без пожара и 41 слика пожара не утичу на избор главних компоненти. На њих се само примењује већ обучена PCA трансформација, чиме се спречава да тестни подаци утичу на предобраду модела.

Оваква предобрада приближно 294 пута смањује број улазних вредности и олакшава изградњу и примену шуме обученој са подацима слике. Ипак, РСА задржава обрасце који најбоље описују разлике међу нормалним сликама које припадају обучавајућем скупу, а не нужно оне који су најважнији за уочавање пожара. Ситни детаљи пламена или дима зато могу бити ослабљени. Избор 100 компоненти представља практичан компромис чији је учинак проверен експериментално у четвртом поглављу.

За федеративну изградњу шуме обучене са подацима слике сви клијенти морају користити исту РСА трансформацију. Само тада, на пример, пета компонента има исто значење на сваком клијенту и сервер може смислено да обједини њихове предлоге поделе. У прототипу процеси локално учитавају исти обједињени обучавајући скуп и зато формирају једнаку РСА базу. У стварно дистрибуираној примени заједничка база могла би да се добије из јавног калибрационог скупа, унапред обученог модела или федеративним РСА поступком, без обједињавања сирових слика.

При формирању чвора камерног стабла потребно је одредити и карактеристику q и вредност поделе p . Да би глобална подела имала исто значење на свим клијентима, индекс q бира се заједнички за текућу федеративну рунду, на серверу. Сваки активни клијент затим одређује локални интервал вредности изабране карактеристике и из њега генерише предлог p_i . Сервер агрегира само међусобно упоредиве предлоге за исту карактеристику и клијентима враћа пар (q, p) .

По пријему пара (q, p) , клијент дели локалну партицију на узорке за које важи $x_q < p$ и узорке за које важи $x_q \geq p$. У свакој наредној федеративној рунди може бити изабрана друга карактеристика, па стабло постепено дели d -димензионални простор хиперравнима ортогоналним на координатне осе. Сваки чвор модела зато, поред вредности поделе, мора да чува и индекс карактеристике. Током предвиђања исти индекс се користи за избор компоненте улазног вектора на основу које се одређује следећа грана.

3.2.3 Агрегација и синхронизација

Агрегација локалних предлога изводи се на основу пристиглих предлога од активних клијената. Нека је m_i број локалних узорака који су учествовали у формирању предлога p_i , и нека i представља индекс конкретног клијента. Глобална вредност поделе израчунава се као тежинска средина важећих предлога по принципу FedAvg алгоритма [12] и може да се израчуна следећом формулом:

$$p = \frac{\sum_i m_i p_i}{\sum_i m_i}$$

Процес изградње користи три стања: INITIAL, CLIENT_RESTING и END_TREE. Клијент је у почетном стању док има чворове које треба обрадити. Када испразни локални ред, прелази у стање CLIENT_RESTING, након чега сервер игнорише његове поруке при агрегацији, али га задржава у комуникационим рундама ради синхронизације. Када више не постоји ниједан активан клијент, сервер поставља стање END_TREE и шаље га свим учесницима. Тек након пријема овог стања учесници завршавају текуће стабло и прелазе на наредно. За сваки чвор извршавају се две комуникационе размене. У првој клијенти шаљу локалне предлоге поделе, сервер их агрегира и враћа глобалне параметре модела. У другој се размењује стање фазе, чиме се спречава да клијент који је раније завршио локални део започне следеће стабло док остали клијенти још обрађују претходно. Цена овакве синхронизације је већи број порука, али се добија детерминистички редослед федеративних корака и заједничка структура модела.

По завршетку обуке сервер је учествовао само у оркестрацији и агрегацији, док су приватни скупови остали код клијената. Резултат су две одвојене глобалне шуме: шума F_T обучена са подацима температуре и шума F_C обучена на подацима слике. Федеративни део поступка односи се на формирање ових модела; њихова каснија употреба за одређивање оцене аномалије може се извршавати локално, без комуникације са сервером.

3.3 Одређивање оцена аномалије

За нови узорак пролази се кроз свако стабло од корена до завршног чвора. Број пређених грана представља дужину пута $h(x)$. Код шуме обученесна подацима температуре одлука о грани доноси се непосредним поређењем температуре са вредношћу p . Код шуме обучене са подацима слике у сваком чвору најпре се из вектора карактеристика чита компонента q , а затим се она пореди са p . Кратак просечан пут указује на узорак који се лако издваја из простора нормалних података, док дужи пут указује на узорак у густој, очекиваној области.

За оба сензорска типа користи се нормализована оцена изолационе шуме. Нека је $E[h_M(x)]$ просечна дужина пута кроз шуму сензорског типа M , где M може бити T за температуру или C за камеру, а n_M број узорака употребљених за обуку. Оцена аномалије израчунава се на следећи начин:

$$s_M(x) = 2^{\frac{E[h_M(x)]}{c(n_M)}}$$

$$c(n) = 2(\ln(n-1) + 0,577) - \frac{2(n-1)}{n}$$

Оцене s_T и s_C налазе се у интервалу $[0,1]$, где код обе оцене већа вредност означава израженију аномалију. За сваки модел одређује се праг τ_T , односно τ_C . Узорак се на нивоу једног сензора сматра аномалијом када је његова оцена већа или једнака одговарајућем прагу. Праг није универзалан, јер зависи од расподеле података, броја стабала, максималне дубине и услова у којима је сензор постављен.

3.4 Обједињавање излаза оба модела

Оцене два модела описују различито виђење истог догађаја. Повишена температура може бити последица пожара, али и извора топлоте који није видљив камери; визуелни образац пламена или дима може бити уочен пре значајног раста температуре, али камера може реаговати и на осветљење или објекат сличне боје. Због тога се коначна одлука не заснива искључиво на једном сензору. За сваки упарени догађај формирају се оцена s_T температурног модела и оцена s_C камерног модела, након чега се примењује једна од стратегија фузије.

3.4.1 Континуалне стратегије фузије

Континуалне стратегије задржавају информацију о сигурности да ли је посматрани узорак аномалија за оба модела и као резултат дају нову оцену у интервалу $[0,1]$. У систему су разматрани производ, аритметичка средина и тежинска средина:

$$s_{\text{prod}} = s_T \cdot s_C$$

$$s_{\text{avg}} = \frac{s_T + s_C}{2}$$

$$s_w = w_T s_T + w_C s_C, w_T + w_C = 1$$

Производ је конзервативнија стратегија, јер висока коначна оцена захтева да оба модела истовремено дају високу оцену. Аритметичка средина даје једнак значај сензорима и погодна је када не постоји унапред позната разлика у њиховој поузданости. Тежинска средина омогућава прилагођавање конкретном окружењу: већи коефицијент може се доделити сензору који је у датим условима стабилнији или раније реагује. За сваку континуалну стратегију коначна оцена пореди се са посебно калибрисаним прагом τ_F .

3.4.2 Стратегије одлучивања на основу прагова

Поред континуалних оцена, примењују се логичке стратегије AND и OR над бинарним одлукама појединачних сензора. Нека је $y_T = 1$ за $[s_T \geq \tau_T]$ тј. $y_T = 0$ за $[s_T < \tau_T]$, а Нека је $y_C = 1$ за $[s_C \geq \tau_C]$ тј. $y_C = 0$ за $[s_C < \tau_C]$. Тада су коначне одлуке дефинисане са:

$$y_{\text{AND}} = y_T \wedge y_C$$

$$y_{OR} = y_T \vee y_C$$

AND стратегија проглашава пожар само ако су оба модела детектовала аномалију. Она је погодна када је цена лажног аларма висока, али може пропустити рану фазу пожара у којој је само један сензор реаговао. OR стратегија активира аларм ако је најмање један модел детектовао аномалију. Она даје већу осетљивост и погоднија је за рано упозорење, али може повећати број лажних аларма.

Све стратегије се оцењују истим метрикама описаним у четвртном поглављу као и појединачни модели. На основу резултата може се изабрати једна подразумевана стратегија за конкретно постављање система. Чување и појединачних оцена уз коначну одлуку остаје корисно, јер омогућава оператору да разликује сагласност оба сензора од случаја у коме је аларм изазвао само један сензор.

3.5 Ток извршавања и имплементациони детаљи

Комплетан ток рада подељен је у три фазе. У првој сваки клијент користи свој локални скуп нормалних узорака температуре и федеративно се обучава шума F_T . У другој исти клијенти користе локално предобрађене карактеристике слика и обучава се шума F_C . У трећој сваки упарени догађај на клијентском чвору пролази кроз обе шуме, добијају се s_T и s_C , а затим се примењује изабрана стратегија фузије. Сервер током прве две фазе агрегира параметре, док се цела трећа фаза извршава локално на клијентском чвору.

Прототип [14] је реализован у програмском језику Python. NumPy се користи за рад са нумеричким низовима и матричке операције, Pillow за учитавање слика, а функционалности библиотеке scikit-learn за анализу главних компоненти и израчунавање евалуационих метрика. PTB-FLA обезбеђује генерички централизовани федеративни алгоритам и комуникацију између процеса.

Подаци за обуку изолационих шума садрже само узорке нормалне класе. За случај података са камере, слике се претварају у векторе једнаке дужине и пројектују у простор мањег броја компоненти. За случај података о температури сваки узорак остаје једна скаларна карактеристика. Иако се исти поступак изградње стабала користи за оба сензорска типа, модели се чувају одвојено како би индекс карактеристике, вредности поделе и нормализациони параметри задржали значење које имају у свом домену.

3.6 Ограничења предложеног система

Прво ограничење односи се на комуникациону сложеност. За сваки унутрашњи чвор стабла потребна је најмање једна рунда размене параметара и једна рунда синхронизације. У најнеповољнијем случају број обрађених чворова расте експоненцијално са максималном

дубином, а поступак се понавља за свако стабло и за оба сензорска типа. Ограничење је израженије код модела обученог над сликама, јер локална обрада вишедимензионалних партиција захтева више меморије. Практично решење подразумева ограничење дубине, броја стабала и броја карактеристика после предобrade.

Друго ограничење јесте претпоставка да су учесници доступни током целе обуке. Стања CLIENT_RESTING и END_TREE решавају различито време локалног завршетка, али прототип не обухвата динамичко прикључивање нових клијената, трајни прекид везе нити наставак делимично изграђеног стабла после отказа.

Коначна одлука зависи и од исправног упаривања два сензорска типа. Ако мерење температуре и слика не описују исти простор и време, њихово обједињавање може произвести погрешан резултат. Предложено решење не покрива такође случај када један од сензора постане недоступан.

На крају, употреба осно-поравнатих подела и редукованих вектора карактеристика не користи у потпуности просторну структуру слике. Такав приступ је изабран због једноставности, малог модела и могућности извршавања на ивици интернета. Његова оправданост, као и избор броја стабала, дубине, броја компоненти, прагова и стратегије фузије, испитују се у наредном поглављу кроз експерименталну евалуацију.

4. Експериментална евалуација

У овом поглављу представљена је експериментална евалуација предложеног хетерогеног система. Полазиште представља једнодимензионална федеративна изолациона шума PFLiForest из рада [5], док се допринос овог рада огледа у проширењу на вишедимензионалне камерне податке и у обједињавању излаза две независно обучене федеративне шуме. Модел на основу података о температури и модел на основу слика са камере и стратегије фузије испитани су у 40 поновљених извршавања за сваку од две конфигурације, чиме је број понављања по конфигурацији усклађен са полазним радом.

Поред метрика мере квалитета излаза система анализирани су време обуке, вршно заузеће Python меморије и варијабилност резултата између псеудослучајних семена. Приказане су средња вредност и стандардна девијација. Резултати су тумачени у односу на циљ претходног рада, високу тачност уз меморијски буџет од приближно 160 kB, али два система не користе исти скуп података нити исту рачунарску платформу. Поређење зато показује трендове и цену проширења, а не апсолутну надмоћ једног решења.

4.1 Евалуационе метрике

Као и у полазној евалуацији, основне предиктивне мере изводе се из матрице конфузије. Ознаке TP и TN представљају исправно препознате пожарне и нормалне узорке, док FP означава лажни аларм, а FN пропуштени пожар. Прецизност описује удео стварних пожара међу активираним алармима, осетљивост удео откривених пожара, а F1 мера њихове хармонијску средину.

$$\text{Precision} = \frac{TP}{TP + FP}, \text{Recall} = \frac{TP}{TP + FN}$$

$$F_1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

AUC-ROC мери способност рангирања позитивне класе кроз однос осетљивости и стопе лажно позитивних одлука за све прагове. Пошто је број пожарних узорака знатно мањи од броја нормалних, приказана је и AUC-PR метрика. Она је у овом случају информативнија, јер директно одражава компромис између прецизности и осетљивости. Вредност AUC-PR случајног рангирања приближно је једнака уделу позитивне класе у посматраном скупу.

За континуалне стратегије фузије најпре је израчуната јединствена оцена аномалије, а затим је праг биран у тачки максималне F1 мере. Код AND и OR стратегија прагови су претходно примењени на појединачне сензорске оцене, па је њихов излаз бинарна одлука. За свако семе најпре је израчунат просек два клијентска резултата. Средња вредност и стандардна девијација су затим израчунате преко 40 семена.

4.2 Поставка експеримента

4.2.1 Наслеђена једнодимензионална поставка

У раду [5] PFLiForest је испитан са два клијента и не-IID (*енгл. non-IID, non Independent and Identically Distributed*) температурним подацима. Варијације су максимална дубина стабла, број стабала и број обучавајућих узорака по клијенту. Дубина је узимала вредности 4, 6, 8, 10 и 12, број стабала 10, 25, 50, 75 и 100, а локални скуп за обучавање 50, 100, 150 и 200 узорака. Свака од 100 комбинација извршена је 40 пута. Синтетички тест скуп садржао је 10.000 одбирака и 10% аномалија добијених заменом изабраних вредности тачкама изван нормалног температурног опсега.

Као оптимална, под ограничењем од приближно 160 kB, изабрана је тачка E(6, 25, 200), односно дубина шест, 25 стабала и 200 узорака по клијенту. У овом раду та поставка служи као референтна тачка за процену додатне цене вишедимензионалног модела. За непосредније поређење употребљена је и тачка B(6, 25, 100), јер staticFireNet располаже са 351 нормалним узорком и не омогућава два непреклапајућа локална скупа од по 200 узорака.

4.2.2 Хетерогени скуп података

Нова поставка заснована је на скупу staticFireNet [13] који садржи 351 слику класе NoFire и 41 слику класе Fire. Укупан број узорака је 392, а удео пожарне класе 10,46%. Сваки догађај представљен је паром који чине слика и температура са заједничком ознаком за тај пар. За обуку изолационих шума користе се искључиво нормални узорци, док тестирање обухвата обе класе.

Из слике димензија 210x140 издваја се црвени канал, нормализује на интервал $[0,1]$ и развија у вектор од 29.400 вредности. PCA га своди на 100 карактеристика. За свако семе PCA модел се обучава искључиво над 200 NoFire слика додељених федеративној обуци, по 100 на сваком клијенту. Преосталих 151 NoFire и свих 41 Fire слика не утичу на средњу вредност ни PCA базу, већ се само пресликавају обученом трансформацијом. Температуре су синтетички генерисане из $N(27, 0.5^2)$ и ограничене на $[20, 34]$ °C за NoFire, односно из $N(50, 8^2)$ и ограничене на $[35, 110]$ °C за Fire.

Параметар	Главна поставка	Упоредива поставка В
Број клијената	2	2
Узорака по клијенту	100	100
Број стабала по шуми	100	25
Максимална дубина	15	6
Број PCA компоненти	100	100
Обучавајући скуп	NoFire	NoFire
Сензорски модели	температура + камера	температура + камера

Табела 1 – Поставка експеримената хетерогеног система

4.2.3 Протоколи тестирања

Коначна евалуација користи строги протокол задржавања, тј. тестни и евалуациони подаци су строго раздвојени. Два клијента обучавају моделе над по 100 различитих NoFire узорака, док тест садржи преостали 151 NoFire и свих 41 Fire узорака, укупно 192 узорка са 21,35% аномалија. И главна конфигурација 100x15 и упоредива конфигурација 25x6 извршене су 40 пута, са семенима од 42 до 81. Семе истовремено одређује поделу података, синтетичке температуре, PCA базу и насумичне изборе током изградње шуме.

Првих 100 PCA компоненти задржава у просеку $99,2695\% \pm 0,0650\%$ варијансе нормалног обучавајућег скупа.

Експерименти су извршени под оперативним системом Windows 10, на процесору Intel Core i7-1165G7 са осам логичких процесора и 15,7 GiB радне меморије. Коришћени су Python 3.12.10, NumPy 2.2.4 и scikit-learn 1.6.1. Сва три процеса, један сервер и два клијента, једног семена покретана су истовремено, док су различита семена извршавана секвенцијално како не би делила исте локалне комуникационе крајње тачке.

У сваком експерименту прво је у обучена шума обучена на подацима температурне, а затим шума обучена на подацима слике. За сваки чвор сервер бира заједнички индекс карактеристике q ; код температуре је q увек 0, док код камере припада скупу $[0, 99]$.

Клијенти шаљу локалне предлоге поделе и величине локалних партиција, сервер рачуна глобалну поделу и враћа исти пар (p,q) свим клијентима. Фузија се након обуке извршава локално и не захтева нову комуникацију са сервером.

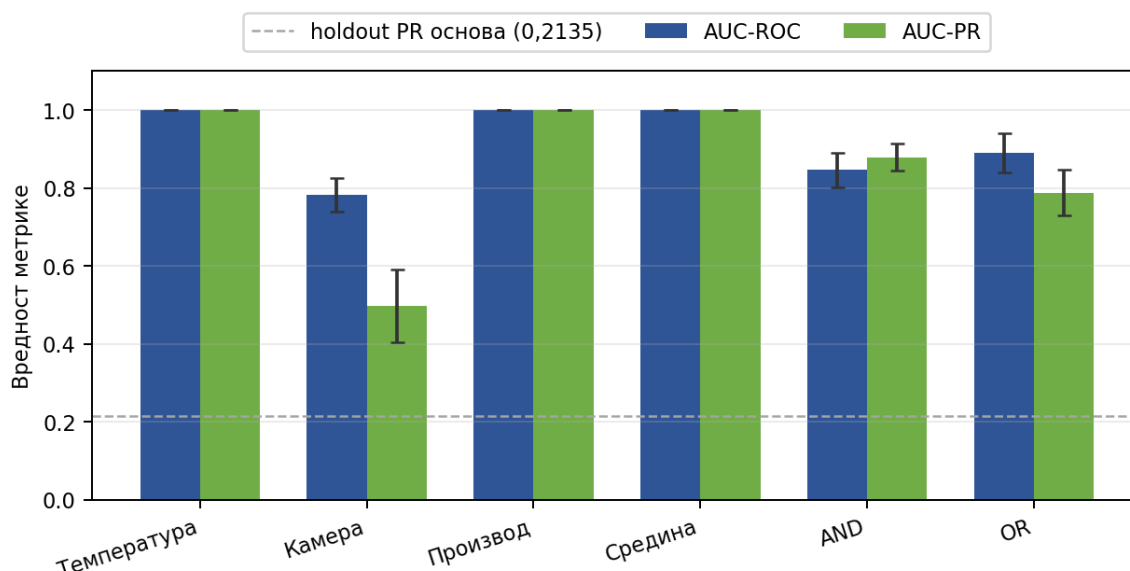
4.3 Резултати и дискусија

4.3.1 Резултати појединачних модела и фузије

Табела 2 приказује резултате 40 извршавања главне конфигурације. Модел обучен мерењима температуре у сваком извршавању потпуно раздваја класе. Модел обучен на подацима слике постиже AUC-ROC $0,7827 \pm 0,0424$, и AUC-PR $0,4978 \pm 0,0938$. У скупу протокола задржавања Fire узорци чине 21,35% података (41 од 192), па би модел који узорке рангира насумично имао очекивани AUC-PR од око 0,2135. Камерни модел постиже AUC-PR од 0,4978, што је 2,33 пута више од насумичне основе и показује да успешно даје више оцене Fire узорцима него NoFire узорцима.

Модел/фузија	AUC-ROC	AUC-PR	F1
Температура	$1,0000 \pm 0,0000$	$1,0000 \pm 0,0000$	$1,0000 \pm 0,0000$
Камера	$0,7827 \pm 0,0424$	$0,4978 \pm 0,0938$	—
Производ	$1,0000 \pm 0,0001$	$1,0000 \pm 0,0003$	$0,9997 \pm 0,0019$
Аритметичка средина	$1,0000 \pm 0,0000$	$1,0000 \pm 0,0000$	$1,0000 \pm 0,0000$
Тежинска средина 0,5/0,5	$1,0000 \pm 0,0000$	$1,0000 \pm 0,0000$	$1,0000 \pm 0,0000$
AND	$0,8460 \pm 0,0440$	$0,8789 \pm 0,0346$	$0,8140 \pm 0,0636$
OR	$0,8894 \pm 0,0500$	$0,7881 \pm 0,0580$	$0,7237 \pm 0,0927$

Табела 2 – Предиктивне метрике главне конфигурације 100x15, n=40



Слика 2 – Средње AUC-ROC и AUC-PR вредности главне конфигурације за $n=40$

Аритметичка и тежинска средина у свих 40 извршавања достижу AUC-ROC, AUC-PR и F1 једнаке 1,0000. Тежинска стратегија са тежинама 0,5 и 0,5 еквивалентна је аритметичкој средини. Производ је готово савршен: средњи F1 износи $0,9997 \pm 0,0019$, а минимум по семенима 0,9881. AND стратегија даје F1 $0,8140 \pm 0,0636$, док OR даје $0,7237 \pm 0,0927$. Пошто AND и OR имају бинарни излаз, њихове AUC вредности описују једну оперативну тачку и нису непосредно упоредиве са пуном кривом континуалних оцена.

У свих 40 извршавања аритметичка и тежинска средина имају $TN=151$, $FP=0$, $FN=0$ и $TP=41$. Ова стабилност не доказује да камера побољшава детекцију, јер синтетичка температура сама потпуно раздваја класе: нормална температура не прелази $34\text{ }^{\circ}\text{C}$, а пожарна није мања од $35\text{ }^{\circ}\text{C}$.

4.3.2 Утицај протокола задржавања и сложености модела

Коригована главна конфигурација 100×15 постиже камерни AUC-ROC $0,7827 \pm 0,0424$ и AUC-PR $0,4978 \pm 0,0938$. Конфигурација 25×6 постиже AUC-ROC $0,6720 \pm 0,0544$, и AUC-PR $0,3418 \pm 0,0680$. Камерни AUC-PR мање конфигурације је за 1,60 пута изнад PR основе.

Пошто су обе конфигурације испитане над истих 40 семена, њихова разлика је анализирана упарено. Главна конфигурација повећава камерни AUC-ROC у просеку за 0,1107. AUC-PR је већи за 0,1559, са интервалом $[0,1227, 0,1892]$. Већи број стабала и дубље партиционисање зато дају статистички јасно боље рангирање узорака са камере.

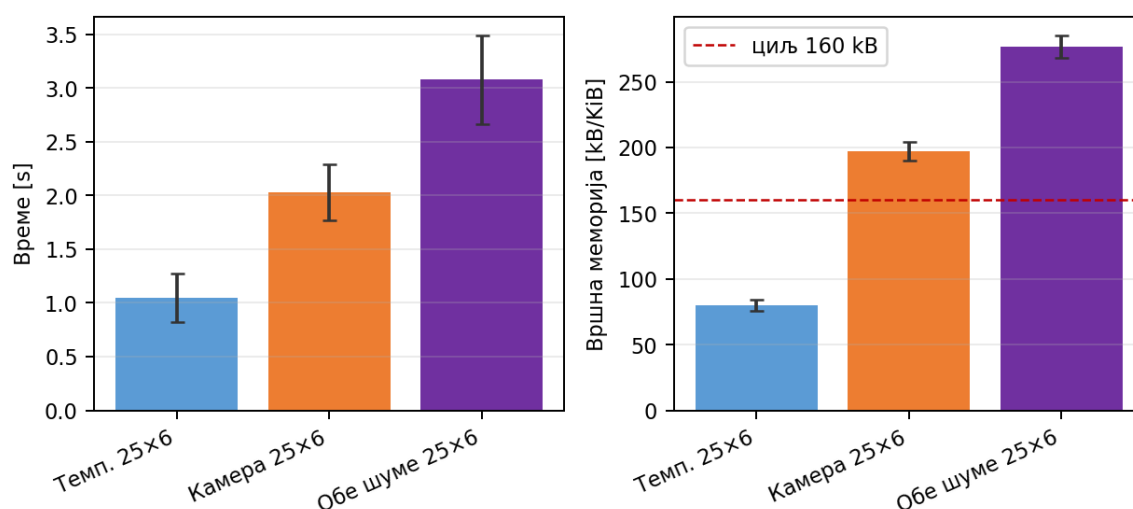
4.3.3 Време извршавања и меморија

Мерење је обављено одвојено током изградње сваке шуме. У главној конфигурацији температурна грана захтева $21,237 \pm 3,505\text{ s}$ и $1054,7 \pm 56,3\text{ KiB}$, а камерна $42,619 \pm 6,612\text{ s}$

и $2157,5 \pm 61,9$ KiB. У конфигурацији 25x6 температурна грана захтева $1,047 \pm 0,222$ s и $80,0 \pm 4,3$ KiB, а камерна $2,030 \pm 0,259$ s и $197,1 \pm 7,1$ KiB. Време обухвата само федеративну изградњу шуме. Учитавање слика, обучавање и примена PCA трансформације нису укључени. tracemalloc бележи Python доделе.

Конфигурација	Модел	Време [s]	Вршна меморија
100x15	Температура	$21,237 \pm 3,505$	$1054,7 \pm 56,3$ KiB
100x15	Камера	$42,619 \pm 6,612$	$2157,5 \pm 61,9$ KiB
25x6	Температура	$1,047 \pm 0,222$	$80,0 \pm 4,3$ KiB
25x6	Камера	$2,030 \pm 0,259$	$197,1 \pm 7,1$ KiB
25x6	Обе шуме, апроксимација	$3,078 \pm 0,413^{**}$	$277,0 \pm 8,5$ KiB**

Табела 3 – Време и вршна меморија федеративне обуке, n=40



Слика 3 – Поређење средњег времена и меморије за конфигурацију 25x6

У конфигурацији 25x6 секвенцијална обука обе шуме траје $3,078 \pm 0,413$ s. Апроксимирани збир одвојено измерених додела износи $277,0 \pm 8,5$ KiB. Овај збир показује да хетерогени систем прелази циљ од 160 KiB из рада [5]. Главна конфигурација захтева приближно 20,75 пута више времена и 11,60 пута већи апроксимативни простор од 25x6, па је њено боље рангирање плаћено знатно већом потрошњом ресурса.

4.3.4 Ограничења експерименталне евалуације

Најважније ограничење остаје начин генерисања температуре. Нормална класа има максимум 34 °C, а пожарна минимум 35 °C, па се расподеле не преклапају. Због тога савршени резултати аритметичке и тежинске фузије потврђују исправан ток с-краја-на-крај, али не доказују комплементарност два сензора. За такву тврдњу потребни су реални упарени одбирци или барем синтетичке температурне расподеле које се преклапају.

Коначно, 40 псеудослучајних понављања отклања ограничење малог броја извршавања. Ипак, понављања поново деле исти коначни скуп од 392 слике, па нису независни узорци из популације различитих пожарних сцена. Приказани интервали описују варијабилност поделе, РСА базе и шуме на staticFireNet скупу, а не спољну генерализацију. Будућа евалуација могла би да укључи независан спољни скуп, различите тежине фузије и сценарије отказа где један од два сензора прекину мерити спољашњу средину.

4.3.5 Закључак експерименталне евалуације

Четрдесет поновљених извршавања потврђује да имплементација стабилно гради једнодимензионалну и вишедимензионалну федеративну шуму, враћа заједничке параметре поделе клијентима и локално обједињује излазе. Камерна конфигурација 100x15 постиже AUC-ROC $0,7827 \pm 0,0424$ и AUC-PR $0,4978 \pm 0,0938$, статистички јасно више од 25x6, али уз око 20,75 пута веће време и 11,60 пута већи апроксимативни простор. Обе камерне конфигурације остају изнад случајне PR основе.

Континуалне средње фузије остају савршене у свих 40 извршавања, али тај резултат потиче од синтетички потпуно раздвојиве температуре. Зато најважнији резултат овог рада није доказ предиктивне користи хетерогености, већ функционална потврда архитектуре, квантификација варијабилности камерног модела и квантификација компромисне потрошње ресурса. Строга тврдња о користи фузије захтева независан скуп са реалним преклапањем расподела вероватноћа података са сензора.

5. Закључак

Овај рад отвара један пут постизања сензорске хетерогености комбиновањем различитих модела употребом различитих стратегијама фузије излаза тих модела. Такође, дат је начин обучавања изолационе шуме у федеративном окружењу која барата са вишедимензионалним улазом где је потребно размишљати и о синхронизацији случајног одабара карактеристике над којом се даље прави случајан пресек по чвору над свим укљученим клијентима.

Експериментална евалуација је показала да и даље постоји простор за побољшање резултата изолационе шуме обучене над сликама са камере. Тренутно у предложеном хетерогеном систему шума измерених температура већински доприноси високој крајњој тачности.

Из перспективе меморијске ефикасности, очигледно је да је потребно размишљати о решењу које би дало боље меморијске резултате. Један пут ка оваквом решењу могао би бити комбиновање свих сензорских мерења у један вектор који би даље представљао улаз у вишедимензионалну изолациону шуму. Свођење слике на статистичке податке уређене у један вектор заједно са температуром као још једна димензија тог вектора би могло представљати једно такво решење у случају овог рада.

Рад [6] јасно показује да постоји више различитих начина постизања хетерогености у контексту федеративног учења који се сви разликују од предложеног решења у овом раду. Посматрајући поделу из рада [6] не би било погрешно рећи да се ова мастер тема бави развијањем сензорски хетерогеног система, док само федеративно учење различитих изолационих шума у систему и даље спада у хомогено федеративно учење по питању обуке јер се шуме обучавају изоловано једна од друге. Ова чињеница може представљати добар мотив да један пут даљег истраживања буде усмерен ка хетерогености током обучавања у окружењу федеративног учења.

6. Литература

- [1] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. 2023. Communication-Efficient Learning of Deep Networks from Decentralized Data. arXiv:1602.05629 [cs.LG]. <https://arxiv.org/abs/1602.05629>
- [2] Varun Chandola, Arindam Banerjee, and Vipin Kumar. 2009. Anomaly detection: A survey. *ACM Comput. Surv.* 41, 3, Article 15 (July 2009), 58 pages. <https://doi.org/10.1145/1541880.1541882>
- [3] Liu, F.T., Ting, K.M. and Zhou, Z. (2008) Isolation Forest. 2008 *8th IEEE International Conference on Data Mining*, Pisa, 15-19 December 2008, 413-422. <https://doi.org/10.1109/icdm.2008.17>
- [4] M. Popovic, M. Popovic, I. Kastelan, M. Djukic and S. Ghilezan, "A Simple Python Testbed for Federated Learning Algorithms," 2023 *Zooming Innovation in Consumer Technologies Conference (ZINC)*, Novi Sad, Serbia, 2023, pp. 148-153, doi: 10.1109/ZINC58345.2023.10173859.
- [5] P. Vasiljevic, M. Matic and M. Popovic, "Federated Isolation Forest for Efficient Anomaly Detection on Edge IoT Systems," *2025 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC)*, Novi Sad, Serbia, 2025, pp. 30-35, doi: 10.1109/ZINC65316.2025.11103552.
- [6] B. Liu, N. Lv, Y. Guo, and Y. Li, "Recent advances on federated learning: A systematic survey," *Neurocomputing*, vol. 597, Art. no. 128019, 2024, doi: 10.1016/j.neucom.2024.128019.
- [7] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "On detecting clustered anomalies using SCiForest," in *Proc. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)*, 2010, pp. 274–290, doi: 10.1007/978-3-642-15883-4_18.
- [8] S. Hariri, M. Carrasco Kind, and R. J. Brunner, "Extended Isolation Forest," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 4, pp. 1479–1489, 2021, doi: 10.1109/TKDE.2019.2947676.
- [9] Xiang, H., Zhang, X., Xu, X., Beheshti, A., Qi, L., Hong, Y., & Dou, W. (2024). Federated learning-based anomaly detection with isolation forest in the IoT-edge continuum. *ACM Transactions on Multimedia Computing, Communications, and Applications*, Just Accepted. <https://doi.org/10.1145/3702995>

-
- [10] Daliang Li, Junpu Wang, Fedmd: Heterogenous federated learning via model distillation, 2019, arXiv preprint arXiv:1910.03581.
 - [11] Enmao Diao, Jie Ding, Vahid Tarokh, HeteroFL: Computation and communication efficient federated learning for heterogeneous clients, ICLR (2021)
 - [12] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, vol. 54, pp. 1273–1282, 2017.
 - [13] M. Trifunović, “staticFireNet: Dataset of RGB images of rooms with and without a fire from POV of a statically positioned camera,” GitHub repository. [Online]. Available: <https://github.com/brzotrciloradmi/staticFireNet> [Accessed: Sep. 23, 2026].
 - [14] LinguineP, “TemperatureFLAnomalyDetection,” GitHub repository, branch: `local_node_staticFireNet_temperature_fusion`. [Online]. Available: https://github.com/LinguineP/TemperatureFLAnomalyDetection/tree/local_node_static_FireNet_temperature_fusion [Accessed: Sep. 23, 2026].