Universitatea
Transilvania
din Brașov

TEZĂ DE ABILITARE

Titlu: Cercetări în vederea integrării sistemelor de calcul si comunicații

Domeniul: Inginerie Electronică, Telecomunicații și Tehnologii Informaționale

Autor: Conf. Dr. Ing. Titus Constantin BĂLAN

Universitatea Transilvania - Brașov

BRAŞOV, 2023

CUPRINS

Mulțumiri

Aș dori să mulțumesc domnului profesor Florin Sandu pentru sprijinul constant pe perioada întregului meu parcurs profesional.

Mulțumesc mult colaboratorilor fără de care nu puteam să realizez atâtea lucruri deosebite (majoritatea coautori la articolele publicate și menționate în bibliografie), precum și partenerilor din filialele locale ale companiilor Siemens și Atos, ce m-au sprijinit constant și au sprijinit universitatea într-un parteneriat solid academic-industrie în ultimii 20 de ani.

De asemenea, mulțumesc tuturor colegilor din Universitatea Transilvania care m-au sprijinit în activitatea mea didactică și de cercetare, familiei și tuturor celor dragi care îmi dau energie și motivație.

(A) Summary

The habilitation thesis entitled "*Research on the Integration of Computing and Communication Systems*" presents the scientific achievements of the author after obtaining the scientific title of PhD in the field of electronic engineering and telecommunications (2011) focusing on the research elements implemented during the period when the author worked at the Faculty of Electrical Engineering and Computer Science.

In part (B-i), the habilitation thesis addresses a research topic in the field of Electronic Engineering, Telecommunications and Information Technologies that refers to the integration between computing and communication systems. Since the first GSM telecommunications networks, with the help of the unifying element represented by packet switching ("all-IP"), systems have evolved towards complex, distributed integrated platforms with high mobility needs, capable of serving a wide range of communication services. The evolution of complexity and types of communication services, based on new technologies, has also implied the implementation of new methods for mobility management, for automated orchestration of real/virtualized/emulated infrastructure and testing/instrumentation elements, as well as ways for creating and integrating communication services. The integration at the level of generic hardware-software platforms, the evolution of virtualization technologies and the migration to Cloud and network functions implemented in software have brought new challenges and requirements at the level of cyber security solutions. Another development of computing and communication systems is represented by the introduction of machine learning algorithms, with roles ranging from automation / orchestration, decision support, behavioral analysis methods, to complex artificial intelligence algorithms.

The scientific achievements covered by the habilitation thesis were published in 11 ISI journal articles (of which 8 in Q1 and Q2), 25 ISI indexed articles and 12 articles in other recognized international databases.

Chapter 1, entitled *"Solutions for computing and communication systems integration",* is dedicated to the integrative element with the greatest impact: software orientation of solutions and services. That is why technologies considered disruptive in the area of integration between computing and communication elements are called "*software-defined", (*where the term "defined" includes the meanings *"created, configured, modeled, orchestrated*") and next to them join terms defining the network area where software technologies are applied:

1. For the Radio *Access* area we have the concept of Software Defined *Radio* (SDR)
2. For the *Core* Network area we have the concept of Software Defined *Network* (SDN)

"Software defined" means reconfigurable, easy to integrate and deploy in virtualized systems and in the Cloud, easy to migrate and scale, often using open APIs, thus encouraging innovation and large-scale testing. Thus, two subchapters presenting research in the field are pursued: one dedicated to the core network that includes SDN concepts and one dedicated to the access network that includes SDR concepts.

Chapter 2, entitled "*Cyber Security of Computing and Communication Solutions and Services*" presents cyber security solutions from two perspectives of the author's professional activity: first, the didactic and continuous development perspective presents a series of contributions from the role of founder and coordinator of the master's program "Cybersecurity", which also includes the stages of building a reconfigurable and versatile cybersecurity lab, as well as the coagulation of a local technology hub initiative called "Brasov CyberHub", second, the perspective of implementing innovative solutions for securing computing and communication solutions and services – which represent a series of HW / SW implementations, some of them based on open source solutions. The

chapter presents a series of contributions following the principles of the concept of "Defence in Depth", which aims to apply security methods at different levels, from enduser and terminal to communication elements and peripheral network. The solutions presented also include various methods of assessing/auditing the vulnerabilities of a system, preventing possible cyberattacks, managing and responding to cyber security incidents, as well as forensic investigation of incidents.

Chapter 3, entitled *"Integration of artificial intelligence elements into computing and communication systems*", presents implementations with contribution of artificial intelligence that produce evolution for computing and communications systems with increased complexity, meeting high demands of processing and security. Artificial intelligence can be integrated at various decision-making levels in computing and communication systems, observing over time the migration of processing power from centralized models (Cloud) to elements at the edge (Edge) or to the support of distributed IoT elements.
Thus, the chapter begins with the description of an implementation carried out within the European project H2020 SARMENTI, aiming to integrate IoT communication and intelligence elements for eAgriculture or assisted agriculture, focusing on the implementation area of the analysis and decision support system.
Artificial intelligence ensures process optimization and can make an essential contribution to streamlining critical and emergency services, such as 112 systems. Such an implementation is the one from the ODIN112 project financed through the UEFISCDI Solutions mechanism, whose implementation details are presented.
Another research describes the implementation of a system that identifies modulation of complex radio signals. This is achieved using an artificial intelligence model developed, trained and integrated into the Microsoft Azure Cloud.
The case study on a complex instrumental configuration around a diesel engine test bench shows asmart device dashing based *on state control*, extended to ECUs (Electronic Control Units) equipped with *real-time* diagnostic capabilities and *optimal decision-making. Parameterization* (instantiation) can be *adaptive* (especially through ANN), and all transitions required for state control (at the level of algorithmic state machines, ASM – Algorithmic State Machine) can be decided with *classifiers* and other means of artificial intelligence.

Part (B-ii) presents the evolution and professional achievements of the author (academic, didactic and research and development) and the professional academic development plan, with the definition of research objectives in the field of communications and cyber security and didactic objectives.

(B) Realizări științifice și profesionale și planuri de evoluție și dezvoltare a carierei

(B-i) Realizări științifice și profesionale

Introducere

Domeniul comunicațiilor a suferit transformări deosebite în ultimele două decenii, una dintre direcțiile de dezvoltare fiind reprezentată de creșterea puterii de procesare ce s-a realizat print-o ***integrare a sistemelor de comunicații cu sistemele de calcul***: de la primele rețele de telecomunicații GSM, cu ajutorul elementului unificator reprezentat de comutația de pachete ("all-IP"), sistemele au evoluat spre platforme integrate complexe, distribuite și cu necesități de mobilitate ridicate, capabile să deservească o paletă extinsă de servicii de comunicații.

Evoluția complexității și a tipurilor de servicii de comunicații, construite pe baza noilor tehnologiilor, a presupus și implementarea de noi metode pentru managementul mobilității, pentru orchestrarea automată de infrastructură reală/virtualizată/emulată și elemente de testare/instrumentație, precum și modalități pentru crearea și integrarea de servicii de comunicații.

Integrarea la nivel de platforme hardware-software generice, evoluția tehnologiile de virtualizare și migrarea înspre Cloud și spre funcții de rețea implementate în software au adus noi provocări dar și oportunitatea realizării unor implementări inovative la nivelul platformelor hardware standard ATCA (Advanced Telecom and Computing Architecture) sau utilizând tehnologii noi ce stau la baza rețelelor 5G și al viitoarelor rețele 6G, precum rețelele definite software SDN (Software Defined Networks) și radio definit software (Software Defined Radio).

Vechiul standard TMN (Telecom Management Networks), elaborat încă din anul 1980 dar încă foarte valid, a definit și elemente de monitorizare a rețelelor după modelul cunoscut sub numele FCAPS după tipul parametrilor monitorizați (Fault Configuration Accounting Performance Security). În ultimul deceniu, litera "S" ce definește metodele de management al securității a crescut în importanța acordată metodelor de management al sistemelor de comunicații. Având în vedere că nivelul de implementare în societate al tehnologiilor IT a crescut vertiginos și asistăm la crearea de noi paradigme digitale, ce se bazează pe procesarea unei cantități ridicate de date interschimbabile pe baza modelelor de comunicații „always connected", problema securității cibernetice a devenit una de mare importanță. De aceea un capitol din această teză este dedicat ***metodelor de securitate cibernetică*** și datorită multiplelor colaborări pe care autorul le-a inițiat cu industria pe această temă, precum și a temelor diverse din domeniu abordate în lucrul cu masteranzi.

Metodele de automatizare și orchestrare a rețelelor de comunicații au trecut și ele printr-o fază de evoluție, de la rețelele auto-organizate (self-organising networks) către concepte mai complexe de orchestrare automată pentru resurse eterogene, și mai departe, spre folosirea de ***algoritmi de învățare automată*** (machine learning).

Elementele de inteligentă artificială devin tot mai prezente în cadrul serviciilor de comunicații, de la elemente de suport al deciziei în industrie, pană la analiză comportamentală și la algoritmi complecși de învățare pentru securitate cibernetică. De aceea un capitol al tezei prezintă implementări în acest domeniu.

Lucrarea prezintă o evoluție a comunicațiilor și serviciilor ce corespunde și cu evoluția profesională și chiar personală a autorului. Prin colaborarea cu industria, autorul a avut oportunitatea să lucreze cu tehnologii de telecomunicații 2G și 3G, a lucrat în echipa de dezvoltare pentru primele echipamente de comunicații LTE (4G) în laboratoarele de cercetare din Germania ale

Nokia, pentru ca apoi să coordoneze o linie de produse de comunicații a Siemens și să activeze ca arhitect de rețea pentru soluții de comunicații critice. Pe parte de cercetare și didactică s-a orientat spre rețele definite software și Cloud, cu focus în ultimii ani înspre zona de soluții de securitate, marcată prin înființarea la Brașov în anul 2018 a unuia dintre primele masterate de Securitate Cibernetica din țară.

Implementările prezentate în această teză urmează scenarii de caz din domenii diverse: de la sisteme de comunicații critice, la sisteme multimedia și IoT pentru sisteme de transport în comun, aplicații industriale din verticale diverse (agricultură, industria constructoare de mașini), pană la aplicații și implementări în domeniul academic.

(B-i) Realizări științifice și profesionale

În cadrul acestei lucrări de abilitare sunt prezentate o parte din rezultatele activităților de cercetare ale autorului desfășurate de la începutul activității profesionale, dar cu precădere cele obținute după finalizarea tezei de doctorat.

Conceptul de “Integrare a sistemelor de calcul și comunicații” menționează binomul “comunicații-calcul” ce pare acum indivizibil și se regăsește natural în abrevierea intens utilizată ICT (“Information and Communication Technologies”) ce reprezintă un set divers de metode și resurse tehnologice utilizate pentru a transmite, stoca, crea, partaja sau face schimb de informații.

Însă integrarea “comunicații-calcul” s-a realizat treptat, dacă luăm în considerare separarea inițială între sistemele de telecomunicații ce ofereau ca unic serviciu pe cel de voce („telefonie”) și primele elemente de calcul ce erau orientate spre procesare de algoritmi, de cele mai multe ori foarte specifici.

Preocuparea pentru metodele de “Integrare a sistemelor de calcul și comunicații” s-a concretizat și într-o disciplină de studiu în cadrul programului de studiu de “Tehnologii și Sisteme de Comunicații”, începând cu anul 2013. Integrarea Sistemelor de Calcul cu Telecomunicațiile reprezintă o disciplină ce prezintă evoluția sistemelor de calcul și telecomunicații de la sisteme separate la o integrare a funcțiilor de procesare și comunicații prin folosirea de hardware generic cu putere mare de procesare (cu avantajele deosebite aduse de tehnologiile de virtualizare și cele de software radio), augmentate de noi tehnologii de inteligenta artificială. Majoritatea implementărilor sunt realizate pe baza de mașini virtuale sau sunt disponibile în Cloud, astfel încât studenții să înțeleagă evoluția spre virtualizare, spre idea de hardware generic și software specific, exprimată în tehnologii 5G precum NFV (Network Function Virtualisation), precum și rolul tot mai pregnant al tehnologiilor software în comunicații (SDN, SDR).

Marcând contribuțiile personale ale autorului, teza de abilitare prezintă integrarea și evoluția conceptelor de comunicații înspre servicii, astfel încât puterea de procesare a putut fi plasată în nodurile de comunicație și în deciziile ce se iau la nivel de sistem, uneori bazate pe algoritmi de învățare automată, dar având mereu în vedere și perspectiva securității cibernetice a sistemelor integrate “comunicații-calcul”.

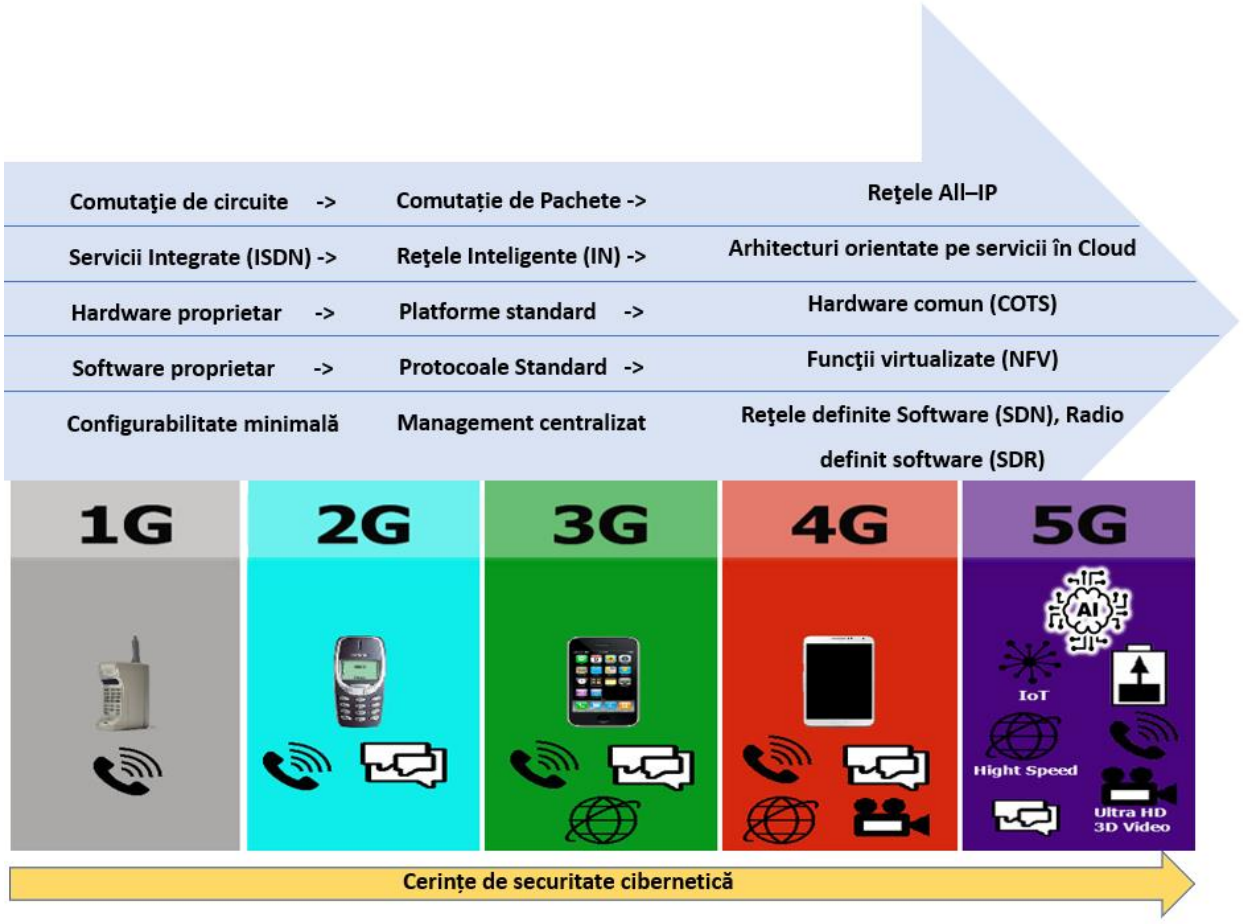


Fig. 1. Integrare a sistemelor de calcul și comunicații:
elementele integrative relativ la evoluția standardelor de telecomunicații

Urmărind evoluția tehnologiilor, dublată de evoluția profesională și a realizărilor autorului, lucrarea de față este organizată în următoarele capitole:

1. Soluții pentru integrarea sistemelor de calculatoare și comunicații
2. Securitatea cibernetică a soluțiilor și serviciilor de calcul și comunicații
3. Integrarea de elemente de inteligenta artificială în cadrul sistemelor de calcul și comunicații

1. Soluții pentru integrarea sistemelor de calcul și comunicații

Integrarea elementelor de calcul și comunicații s-a realizat pe mai multe direcții, așa cum a fost exemplificat în figura 1.

Dintre elementele integrative, cel mai mare impact l-a avut orientarea spre soluții și servicii ***software***. De aceea tehnologiile considerate disruptive în zona de integrare între elemente de calcul și comunicații sunt numite ***„software-defined",*** adică definite software (unde termenul ***"definite"*** include accepțiunile ***„create, configurate, modelate, orchestrate***") și lângă ele se alătură termeni ce definesc zona de rețea unde se aplică tehnologiile software:

- Pentru zona de ***Rețea de Acces (Radio Access)*** avem conceptul de Software Defined ***Radio*** (SDR)
- Pentru zona de ***Rețea de Bază (Core Network)*** avem conceptul de Software Defined ***Network*** (SDN)

„Software defined" însemnă reconfigurabil, ușor de integrat și rulat în sisteme virtualizate și în Cloud, ușor de migrat și scalat, folosind de cele mai multe ori interfețe API deschise, deci încurajând inovația și testarea la scară largă.

De aceea pentru a prezenta implementările și realizările în domeniul integrării sistemelor de calcul și comunicații voi urmări **două subcapitole**: unul dedicat rețelei de bază ce include concepte SDN și unul dedicat rețelei de acces ce include concepte SDR.

1.1. Integrarea sistemelor de calculatoare și comunicații în rețeaua de bază

1.1.1. Soluții de mobilitate în rețele eterogene

Mecanismele de mobilitate sunt elemente cheie ale mediilor inteligente "întotdeauna conectate". De la primele protocoale Mobile IPv4, soluțiile de mobilitate IP au evoluat de la mobilitatea gazdelor la mobilitatea rețelei și migrarea la IPv6, dar există încă scenarii de utilizare specifice care nu sunt acoperite. De asemenea, mobilitatea nu se referă doar la gazde sau persoane fizice, ci și la cod/aplicații și la mașini virtuale.

Continuând tema abordată în cadrul tezei de doctorat intitulată "Soluții de mobilitate în rețele inteligente", sub coordonarea Prof.Dr.Ing. Florin SANDU, susținută în anul 2011, o serie de cercetări s-au axat pe tema metodelor de mobilitate pentru comunicații mobile. O metodă folosită cu succes în propunerea unor soluții de mobilitate se bazează pe protocolul LISP (Locator/Identifier Separation Protocol) ce presupune separarea adreselor IP în două noi spații de numerotare: Endpoint Identifiers (EID-s) și Routing Locators (RLOC-s). Prin introducerea acestei separări, devin disponibile noi capacități de mobilitate, scalabilitate și securitate, precum și noi soluții atât pentru mobilitatea gazdelor ("hosts"), cât și pentru mobilitatea mașinilor virtuale (de exemplu, în interiorul centrelor de date) prin separarea identificatorului și a locației unui terminal al rețelei.

Implementarea din [1] se bazează pe o propunere de arhitectură de rețea conectată în mai multe puncte ("multi-homed") și echilibrată din punct de vedere al încărcării traficului ("load-balanced") LISP pentru mediile urbane, respectiv o arhitectură adaptată în mijloace de transport (cu precădere pentru trenuri) care detaliază implementarea elementelor LISP pentru cazul de utilizare a mobilității. Dacă inițial validarea soluției se face într-un mediu emulat, cazul unei întreprinderi cu locații distribuite, focalizarea e pe scenariile urbane mobile, cum ar fi cazul furnizării de conexiune Internet fiabilă, în mod redundant dar și cu echilibrarea sarcinii ("load-balancing") în sistemele de

transport public. S-a realizat o implementare open-source Open Overlay Router și eficientizare pe bază de concepte Software Defined Networks (SDN), cazul specific al Software Defined – Wide Area Networks (SD-WAN), ce include optimizare WAN (Wide Area Network).

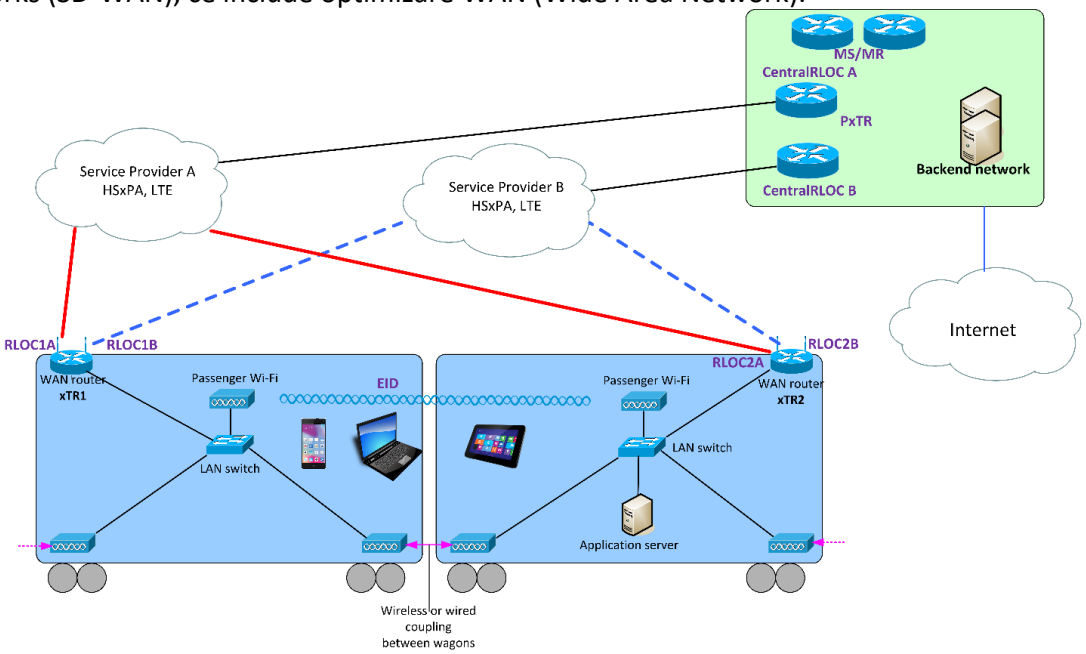


Fig. 2. Arhitectura bazată pe LISP implementată în cadrul sistemului de transport public, conform cu [1]

Desemnarea rolului adreselor IP se face după cum urmează: fiecare router WAN joacă rolul unui Ingress/Egress Tunnel Router (xTR) și are 2 interfețe mobile - de aceea un router 2SIM (cu două SIM-uri) ar fi o soluție bună (exemplu de soluție comercială ar fi modelul Cisco C819 care are și suport LISP). Fiecare dintre aceste interfețe a definit adrese RLOC (routing locators), în timp ce rețeaua "în tren", bazată pe WiFi cu o posibilă rețea de distribuție comutată pentru cuplarea între vagoane, ar utiliza adrese EID (endpoint identifier) într-un anumit interval de adrese. Rețeaua centrală ”back-end” reprezintă nu numai un proxy pentru Internet, ci acționează și cu rol de protecție (firewall) și găzduiește serverele de aplicații. Din perspectiva LISP, rețeaua back-end reprezintă RLOC-urile în locația centrală. Back-end-ul ar trebui să includă, de asemenea, MS/MR (Map Server/Map Resolver) de sine stătător sau co-localizat cu alte elemente.

LISP permite integrarea transparentă a adreselor IPv4 și IPv6, astfel încât ambele tipuri de adrese să poată fi utilizate. În ceea ce privește conectivitatea securizată, cea mai adecvată ar fi utilizarea VPN de date mobile (rețea privată de nivel 2 sau nivel 3 între APN - Access Point Name mobil (și rețeaua back-end). Cu toate acestea, soluția Cisco GET-VPN pe care am implementat-o în demonstrator ar putea aduce mari avantaje, deoarece nu necesită o infrastructură de rutare adiacentă pentru planul de control și se integrează perfect cu infrastructuri multicast care ar putea fi utilizate în caz de urgență pentru aplicații de tip siguranță publică.

Figura 3 descrie arhitectura propusă pe bază de soluții cu sursă deschisă, Open Overlay Router (OOR) – proiect numit inițial LISPmob. OOR este o implementare open-source pentru a crea rețele de suprapunere programabile (overlay), scrise în limbajul de programare C, oferind marele avantaj al flexibilității platformei, deoarece există versiuni dedicate pentru Linux, Android și OpenWRT. Controlerul SDN joacă un rol central în arhitectura SDN. Toate beneficiile rețelelor definite de software sunt disponibile prin intermediul controlerului dedicat OpenDayLight cu suport pentru LISP ca parte a modulului LISPFlowMappings. Această abordare deschide noi perspective, traficul poate fi dirijat din mers prin diferite OORs prin interfațare numai cu OpenDayLight. Încorporarea tehnicilor de optimizare WAN pentru livrarea accelerată a tuturor aplicațiilor din WAN-ul definit software (SD-WAN) prin rețeaua centrală a rețelei LISP este inițial cea mai importantă. SD-WAN este un concept care combină beneficiile tehnicilor de optimizare WAN cu

rețeaua definită software prin virtualizarea WAN. Astfel, politicile pentru optimizarea WAN pot fi descrise și ajustate dinamic la nivel de controler SDN (de exemplu, OpenDaylight) și, de asemenea, sunt activate funcționalități precum controlul căii WAN, conectivitatea independentă de calea de transport, gestionarea încărcării și automatizarea (de exemplu, agregarea mai multor conexiuni la Internet, astfel încât acestea să funcționeze ca o singură suprapunere virtuală cu performanțe și fiabilitate sporite).

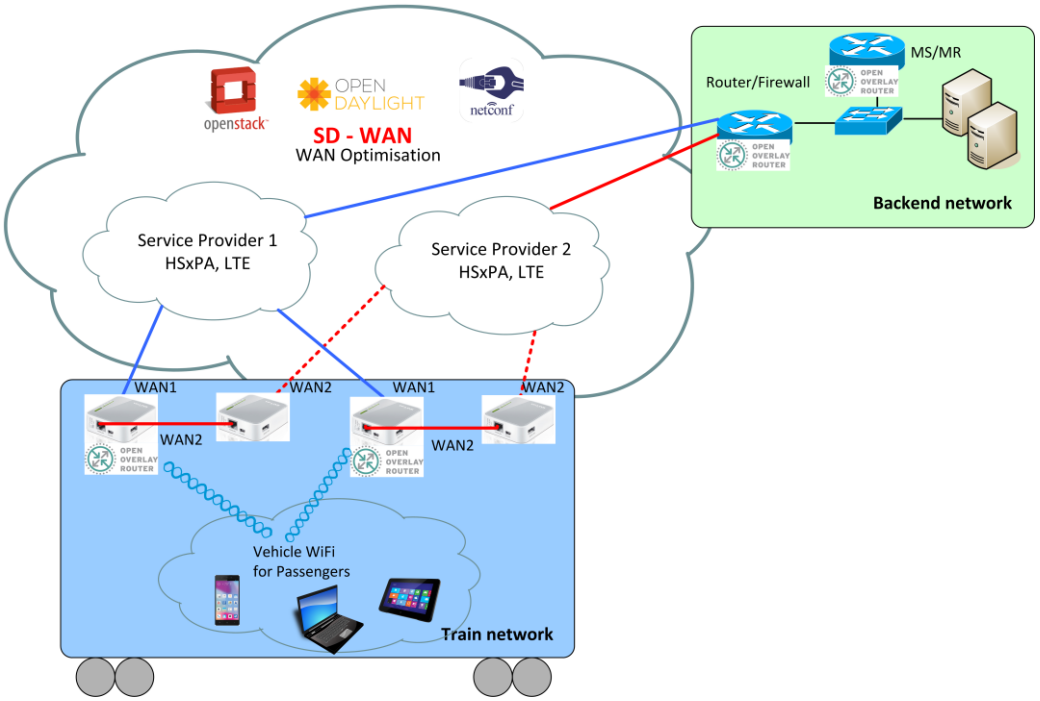


Fig. 3 Prototipare a configurației LISP la bordul vehiculului, bazată pe soluții cu sursă deschisă

OOR poate fi folosit și cu rol de xTR în locația back-end, dar și ca MS/MR de bază unde prefixele EID configurate pot fi înregistrate de xTRs. OOR va răspunde, de asemenea, la MapRequests adresate acestor prefixe.

O altă implementare bazată pe LISP prezentată în [2], extinde conceptul spre un scenariu de mobilitate. Am luat în considerare cazul elementelor IoT din interiorul unei rețele de vehicule sau de transport public.

Există 2 metode care pot fi alese pentru implementarea LISP pentru IoT:

1. pe Gateway-ul IoT, care este, de asemenea, un router multi-RAN, așa cum este detaliat mai jos, în figura 4;
2. direct pe elementul IoT ("thing") folosind versiunea LISP-MN (Mobile Node) a implementării protocolului.

Implementarea IoT Gateway este ilustrativă pentru un ecosistem de rețele suprapuse (overlay), deoarece OOR poate fi integrat cu conceptul de Rețele definite software, LISP având suport și de la OpenDaylight SDN Controller ca parte a modulului LISPFlowMappings, una dintre cele mai dezvoltate soluții deschise de acest tip. OpenDaylight poate juca rolul serverelor de mapare (MS/MR), astfel încât deciziile pentru rutarea inteligentă sunt co-locate cu serverele de mapare LISP. În plus, controlerele SDN joacă un rol crucial în conceptul de ”feliere” a rețelei (network slicing) definit pentru mediile de virtualizare a funcțiilor de rețea în 5G, iar o ”felie de rețea” dedicată operatorului de telefonie mobilă poate fi exact felia IoT.

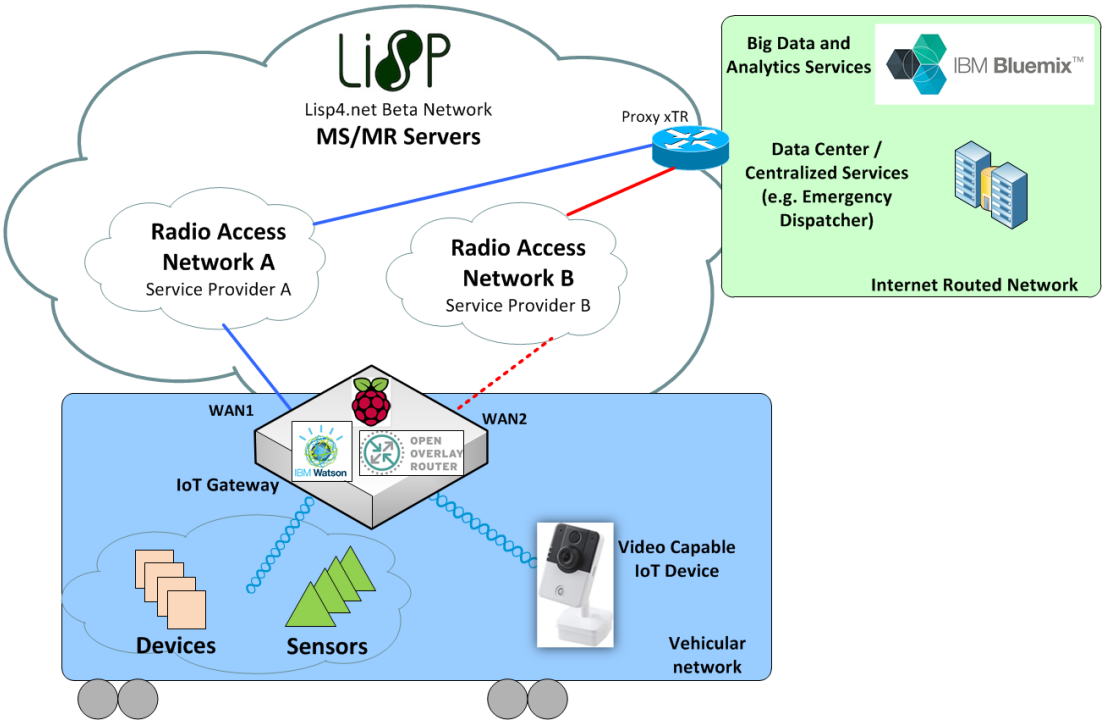


Fig. 4 Configurație LISP la bordul vehiculului pentru IoT, implementată pe sisteme Raspberry Pi – SBC Single Board Computing și cu analiza în Cloud IBM Watson pentru analiza valorilor IoT

Pentru o implementare mobilă și miniaturizată am ales să folosim implementarea Linux OOR, instalată pe un element Raspberry Pi SBC (Single Board Computer) care joacă rolul unui Gateway IoT, deoarece rulează și IBM Watson pentru "RasPi" și poate fi, de asemenea, conectat la IBM Bluemix Cloud pentru analize și procesări suplimentare.

Există mai multe roluri care sunt implementate ca parte a soluției deschise OOR: în prezent, poate funcționa ca xTR, MS / MR, RTR sau LISP-MN. Am activat LISP pe routerul WAN care acționează ca xTR. Un alt scenariu ar fi putut fi utilizarea LISP-MN direct pe telefonul Android, așa cum este descris în [2].

În plus, elementul IoT Gateway are 2 interfețe WAN mobile pentru doi operatori locali de telefonie mobilă, pe care le voi numi în continuare Operator 1 și Operator 2. Pentru a nu oferi detalii comparative cu privire la rețelele publice de telefonie mobilă fără acordul Operatorilor, nu voi menționa denumirea comercială a rețelelor publice utilizate.

Conexiunea a fost posibilă prin modem-uri USB 3G și instrumentul Linux wvdial. Fiecare dintre interfețe are o adresă RLOC publică, așa cum este vizibil în figura 3 privind rețeaua experimentală utilizată. Pentru testele efectuate am ales să utilizez rețeaua pilot publică LISP4 care a fost implementată în întreaga lume, constând din 8 servere de cartografiere și mai multe proxy-xTR care acoperă trei regiuni principale, SUA, Europa și Asia. Rețeaua LISP4 Beta are o rețea crescută de site-uri publice xTR.

Pentru utilizarea rețelei LISP4 Beta a trebuit să furnizez adrese IP publice/rutabile în rețelele Operatorului 1 și Operatorului 2, așa cum se vede în Figura 5.

unitbv-xtr	intouch-ams-mr-ms-1	yes	yes	00:10:00	0	153.16.61.32/28	109.166.171.20 (up) 213.233.72.16 (up)
unitbv-xtr	tdc-mr-ms	yes	yes	00:10:00	0	153.16.61.32/28	109.166.171.20 (up) 213.233.72.16 (up)
unitbv-xtr	upc-mr-ms-1	yes	yes	00:10:00	0	153.16.61.32/28	109.166.171.20 (up) 213.233.72.16 (up)

Fig. 5 LISP4. Implementare beta pentru nodurile xTR "Unitbv"

1.1.1.1. Evaluarea mobilității LISP pentru elemente IoT și multimedia în rețele de comunicații mobile cu echipamente de testare dedicate.

Cerințele privind mobilitatea, redundanța și lățimea de bandă transformă modelele de comunicare utilizate pentru IoT, în principal în cazul comunicațiilor critice și al transferului (streaming) multimedia ("IoMT - Internet of Multimedia Things"), deoarece în prezent, se estimează că traficul video reprezintă 71% din totalul traficului de date mobile, iar această pondere este prognozată să crească la 80% în 2028. Una dintre caracteristicile rețelelor 5G e reprezentată de proliferarea rețelelor radio diferite/eterogene (rețele de acces radio virtualizate, noi radiouri eficiente din punct de vedere energetic, femto-celule, Wifi offloading) și posibilitatea ca obiectele IoT să se conecteze și să echilibreze sarcina între rețele de acces radio RAN duale sau multiple. Pentru a evita ca testele pentru soluții de mobilitate aplicate serviciilor multimedia complexe să fie influențate de problemele de acoperire ale operatorilor de rețele mobile, am efectuat o analiză preliminară a hărților de acoperire 3G și LTE pentru cei doi operatori utilizați în paralel în timpul testelor demonstratorului LISP prezentat în paragraful anterior.

Am folosit următoarea configurație mobilă: un scaner "PCTEL" (produs de RF Solutions), o antenă omnidirecțională și un pachet software "TEMS Investigation" care rulează pe un notebook (cu o configurație hardware specifică pentru Drive-Tests). Scanerul PCTEL (Figura 6) permite evaluarea performanței și oferă soluții optimizate adaptate rețelei wireless testate (de la 130 MHz la 6 GHz). Datele sunt obținute într-o colecție concurentă SeeGull MX - pentru toate benzile RF definite de 3GPP, pentru toate tehnologiile majore simultan (după un modul radio unic, există module de procesare a semnalului de înaltă performanță care rulează în paralel).

Fig. 6 Scanerul RF Solutions "PCTEL"

Datele scanate au fost analizate folosind TEMS Investigation, o soluție activă de testare end-to-end pentru verificare și optimizare RAN eterogenă, permițând operatorilor să testeze și să evalueze calitatea rețelei dintr-o perspectivă a utilizatorului, inclusiv scenarii de mobilitate la bordul vehiculului.

Primul pas pentru setarea configurației rețelelor scanate este selectarea parametrilor purtătorului de canal și frecvență (Figura 7), pentru operatorii de telefonie mobilă evaluați. Am ales frecvența centrală a purtătorului pentru tehnologiile 3G și 4G și lățimea de bandă, specifică fiecărui ISP. Lățimea de bandă pentru 3G este, în general, de 5 MHz, în timp ce lățimea de bandă 4G variază între 5MHz și 20MHz, în funcție de alocarea resurselor pentru frecvențele fiecărui operator, în funcție de licențele radio cărora li se permite funcționarea.

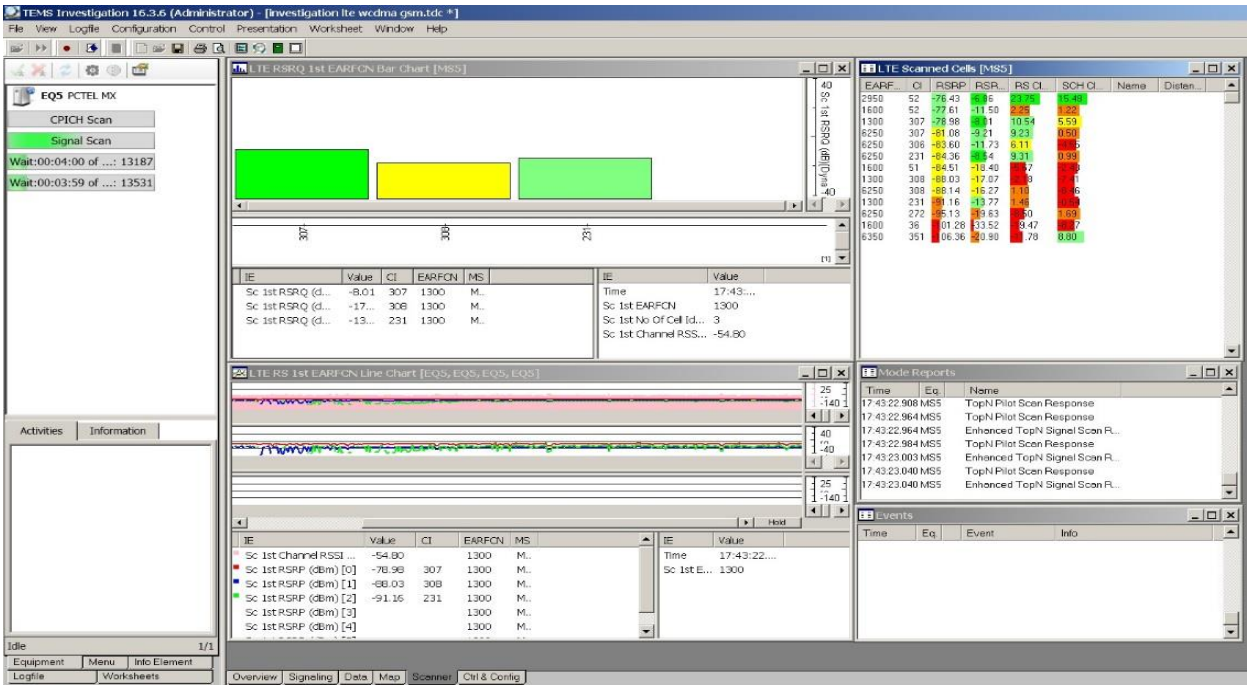


Fig. 7 Setarea frecvențelor centrale LTE în investigația TEMS

În Figura 8 este prezentat, într-un format grafic, secvența de configurare pentru scanerul "PCtell MX SeeGull", folosind software-ul TEMS Investigator. Această configurație este utilizată pentru scanarea capacității serviciului downlink în 3G și 4G pentru cei doi operatori aleși.

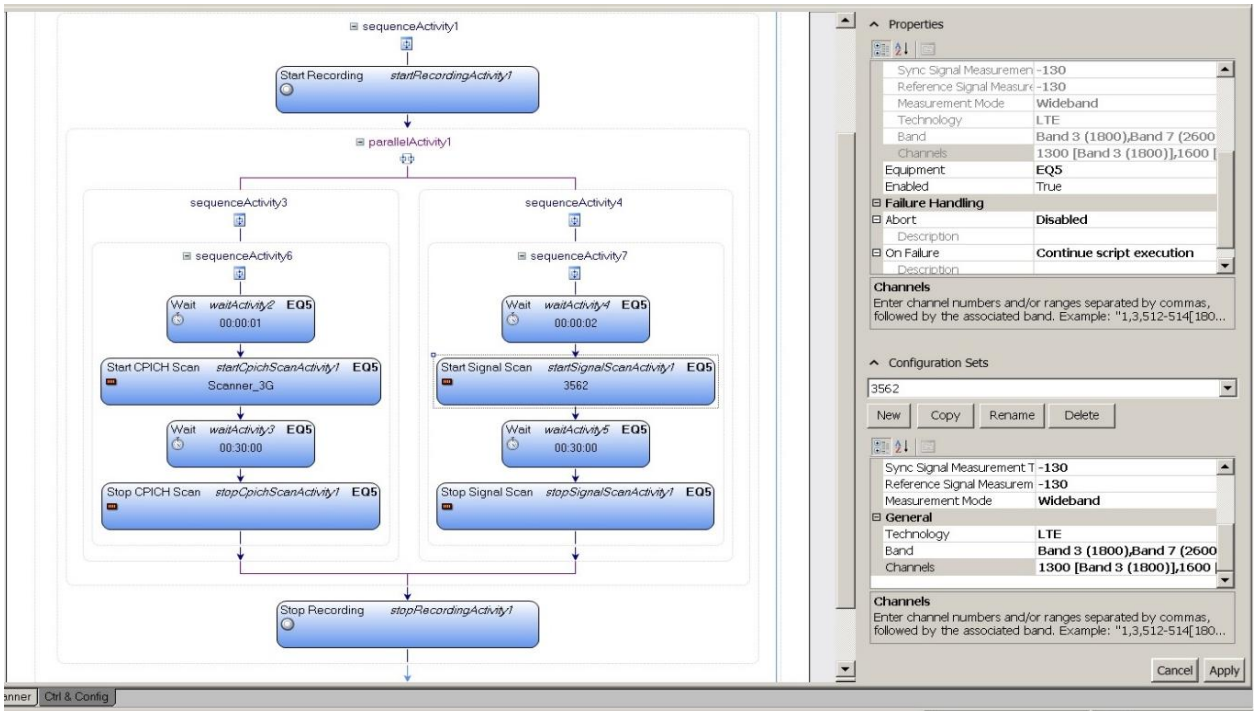


Fig. 8. Testarea configurației folosind programarea vizuală cu "scanerul PCtell MX SeeGull"

Pentru rularea drive-test am folosit o aplicație pentru prelucrarea în timp real a datelor, inclusiv, de asemenea, o reprezentare grafică pentru unii dintre parametri. Astfel, orice eroare sau funcționalitate anormală a sistemului ar putea fi identificată și corectată imediat, astfel încât testul de scanare ar putea continua în mod normal.

Am ales o rută predefinită în orașul Brașov pentru traseul de referință drive-test. Antenele au fost amplasate pe acoperișul automobilului pentru a evita pierderea semnalului; distanța dintre antene și capătul acoperișului mașinii trebuie să fie mai mare decât λ /2.

În timpul rulării testului, se pot identifica condițiile radio de pe ruta respectivă pentru fiecare dintre cei doi operatori și, de asemenea, se poate obține o statistică a celui mai bun canal care urmează să fie utilizat de dispozitivul mobil în timpul efectuării serviciului. Demonstratorul LISP a fost condus urmând circuitul din figura 9 – pentru validarea corectitudinii predării, PCTEL a scanat calitatea legăturii descendente pentru celulele Operator1 și Operator2 cu identitățile celulelor EARFCN (EUTRA Absolute Radio-Frequency Channel Number) 1300 și 6250 (Operator1), 1600 și 2950 (Operatorul 2).

Fig. 9. – Ruta de testare cu evidențierea numerelor de canal diferite: EARFCN (Numărul absolut al canalului de radiofrecvență EUTRA)

Folosind metoda de scanare radio am aflat că nu ambii operatori au o acoperire radio mobilă adecvată în toate părțile traseului de referință drive-test. Există zone în care avem pierderi de semnal pentru unul dintre operatori și acest lucru duce la erori în comportamentul gateway-ului nostru IoT bazat pe LISP, deoarece o interfață mobilă deconectată nu se recuperează de la sine și nu este utilizată din nou în tunelul LISP OOR fără o reinițiere specifică.
Astfel, am decis să introduc, prin scripting, o metodă de "auto-vindecare" a sistemului, făcându-l astfel robust și rezistent la erori.

1.1.1.2. Automatizarea Demonstratorului mobil bazat pe LISP pentru Internetul obiectelor multimedia (IoMT)

Am realizat următorul demonstrator (figura 10) care a fost testat în scenariul de mobilitate.

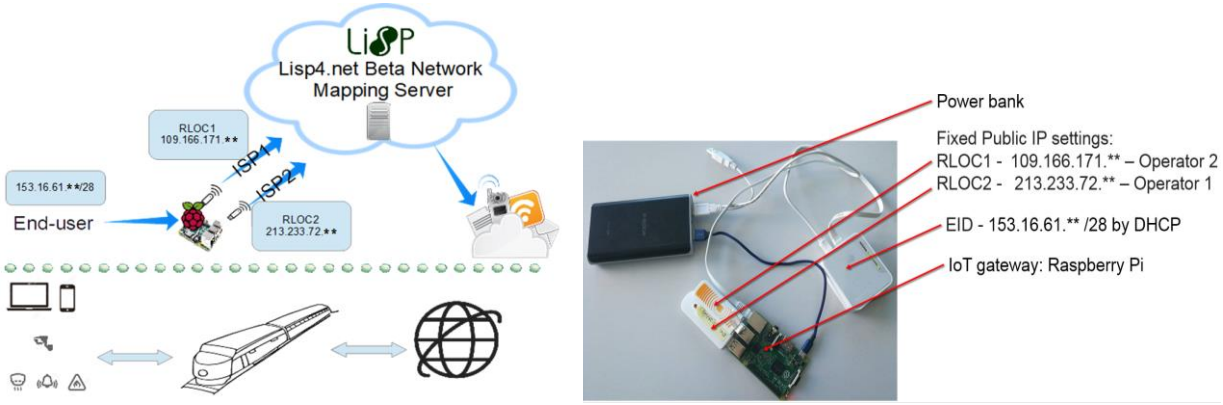


Fig. 10. – Dreapta: Demonstrator PTS (sistem de transport public) pentru IoT mobil cu LISP
Stânga: Mini-sistemul mobil de testare

Au fost considerați consumatori intensivi de lățime de bandă – fluxuri video (pe ecranul utilizatorului final, un "thin client", de exemplu o tabletă conectată la nodul LISP "RasPi", gateway-ul IoT). Demonstratorul IoT, bazat pe LISP, este un sistem autonom, alimentat cu baterii, deci complet mobil. Toți utilizatorii finali sau senzorii și dispozitivele IoT sunt conectați automat la sistem prin WiFi ca conectare la un hot-spot normal.

Automatizarea sistemului pentru tratarea erorilor sau pentru recuperarea pierderii semnalului s-a făcut cu codare bash. LISP aduce și un avantaj suplimentar pentru robustețea sistemului, pe lângă multi-homing și echilibrarea încărcării: ca și în cazul protocolului Mobile IP, cu LISP conexiunile TCP-IP sunt păstrate indiferent de disponibilitatea canalelor fizice / conexiunilor, dar cu avantajul că există mai puține modificări necesare pentru infrastructura de rețea. Cu ajutorul codului implementat, pe lângă menținerea tunelului (și a conexiunii TCP-IP) - acesta este un atribut LISP – am automatizat și o metodă de recuperare a interfeței. În plus LISP aduce avantajul unei implementări end-to-end facile, deoarece nodul mobil nu are nevoie neapărat de o implementare specifică dacă utilizează doar rețele LISP sau proxy-uri LISP.

În scopul testării multimedia, am utilizat tehnologii web. Când vine vorba de comunicații în timp real, WebRTC este un standard relativ nou, permițând browser-elor și aplicațiilor mobile cu capacități de comunicații în timp real (RTC) prin API-uri (Interfețe de programare a aplicațiilor) simple.

Fiind bazat exclusiv pe browser și nesolicitând nicio aplicație sau instalare plug-in, WebRTC reprezintă o opțiune versatilă care ar putea fi ușor integrată și încorporată ca parte a ecosistemului IoT eterogen.

Folosind un driver de cameră web, am simulat o sursă video și am reușit să difuzăm un videoclip cunoscut / de referință, într-un flux WebRTC. Am folosit servere WebRTC disponibile public, cum ar fi OpenTok și AppRTC pentru a produce conferințe video WebRTC.

Chiar dacă nu sunt descrise în cele ce urmează (Figura 11), au fost simulate mai multe fluxuri WebRTC. Astfel, odată difuzat prin intermediul sistemului WebRTC, fluxul video de referință este înregistrat folosind instrumentul RecordRTC și poate fi analizat.

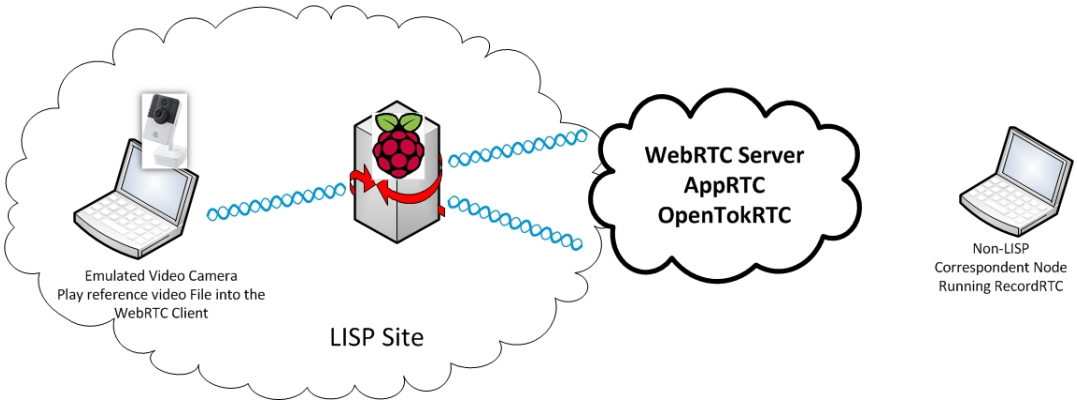


Fig. 11. – Metoda de testare a fluxurilor WebRTC

Alte teste efectuate au fost cele de lățime de bandă pe care le-am realizat cu software-ul Smooth Stream Performance. Am concluzionat că multi-homing-ul LISP nu este eficient în cazul solicitărilor succesive și al semnalizării intensive (a se vedea figura 12), ca în cazul recuperării diferitelor bucăți de streaming pe baza unui manifest. Pentru fiecare tip de streaming (audio/video), se menționează bitrate-ul și răspunsul.

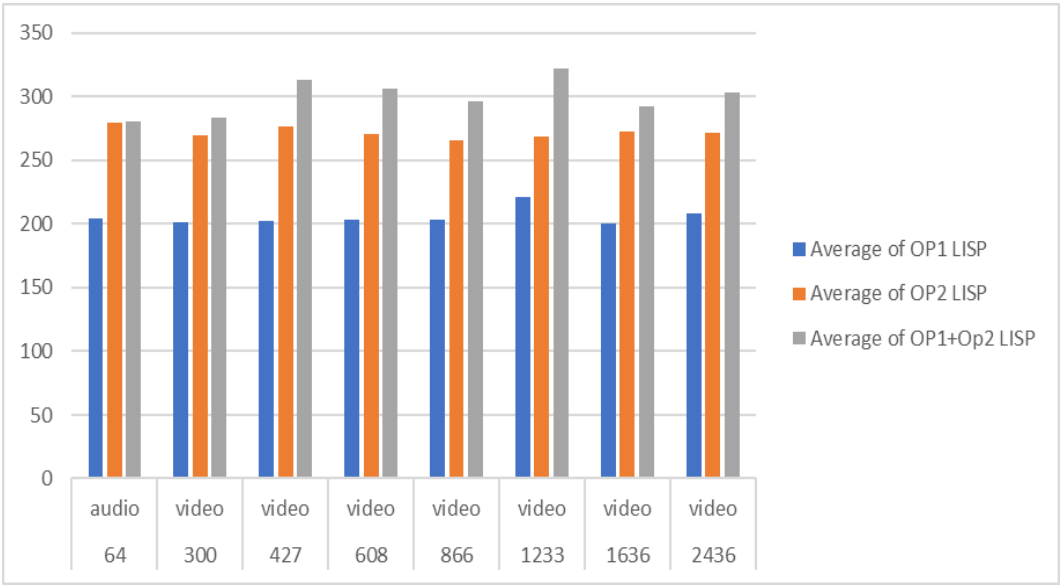


Fig. 12. - Rezultate comparative ale testelor de performanță pentru streaming fără probleme între Operatorul 1, Operatorul 2 și teste multi-homed Operator 1+ Operator 2; Figura indică timpul de răspuns (în ms) pentru a prelua diferite porțiuni de flux de la un server de streaming la distanță.

Rezultatele de mai sus nu indică o îmbunătățire prin utilizarea a două conexiuni WAN paralele, deoarece niciuna dintre conexiunile mobile nu ducea lipsă de lățime de bandă; nu a existat niciun blocaj, chiar dacă semnalizarea excesivă a utilizării a două conexiuni paralele a cauzat propria întârziere.

Calitatea experienței pentru mai multe fluxuri WebRTC prin tuneluri LISP

Am încercat să folosesc mai multe fluxuri multimedia, cum ar fi într-un caz real în care mai multe dispozitive IoMT sunt conectate la același gateway IoT și se concentrează pe calitatea experienței. În scopul testării, am conectat mai multe fluxuri WebRTC la aceeași conferință folosind aceeași implementare OpenTok WebRTC.

Am observat că la fiecare conexiune WebRTC, traficul a fost direcționat fie către Operatorul 1, fie către Operatorul 2. Echilibrarea încărcării observată nu a fost pentru divizarea fluxului video pe două conexiuni mobile WAN, ci pentru distribuția fluxurilor video pe diferite căi de date.

Pentru a explica mai bine situația, s-ar putea face o analogie cu procesoarele multi-core: atunci când se execută doar un fir (în cazul nostru se utilizează o sesiune WebRTC), se utilizează doar un nucleu (în cazul nostru se utilizează în mare parte o rețea de operatori); în cazul în care pornește un al doilea fir, acesta este preluat de al doilea procesor de bază (în cazul nostru Operatorul 2), echilibrând astfel traficul între cei 2 operatori. Acest comportament este vizibil în rezultatele monitorizării lățimii de bandă (a se vedea figura 13). Când este pornit un singur flux webRTC, se utilizează o singură rețea de operatori, apoi este pornit al doilea flux și acest lucru este preluat în cea mai mare parte de Operatorul 2.

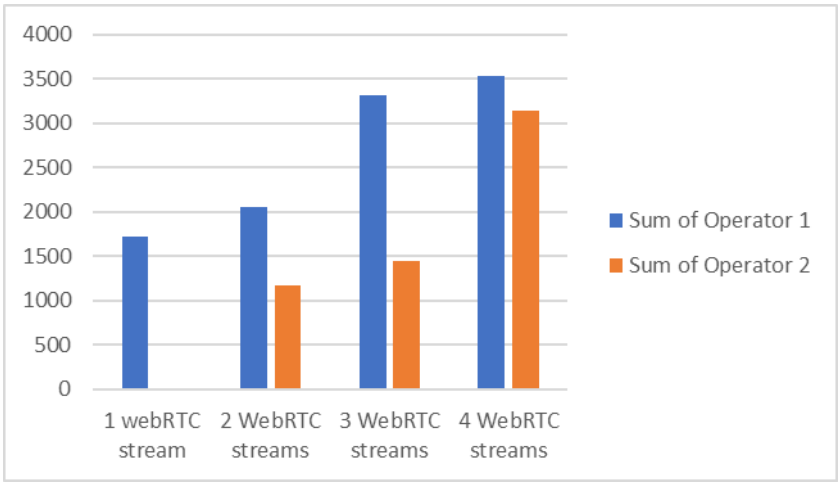


Fig. 13. Testele indică lățimea de bandă furnizată pentru fiecare operator de telefonie mobilă atunci când redați până la 4 fluxuri WebRTC folosind OpenTok

Rezultatele din figurile 12 și 13 indică faptul că beneficiile utilizării a două sau mai multe conexiuni mobile sunt vizibile în cea mai mare parte în cazul informațiilor multimedia atunci când se utilizează mai multe fluxuri video și atunci când congestia afectează rețeaua.

În plus, intenția mea a fost de a limita lățimea de bandă a conexiunilor mobile, astfel încât să se poată evalua mai bine beneficiile multi-homing. Acest lucru a fost efectuat utilizând comanda AT "AT + CGEQREQ", cu intenția de a limita lățimea de bandă a fiecărui operator de rețea la 384 Kbps. Cu toate acestea, comanda menționată nu a avut niciun efect asupra rețelelor operatorilor pe care le-am folosit, astfel încât lățimea de bandă nu a fost limitată pentru a simula congestia. Tendința este de a muta accentul transmisiei de date în rețelele mobile de la calitatea serviciilor la o rată de transfer mai bună. Acest lucru explică lipsa efectului comenzilor QoS utilizate.

Am ajuns la concluzia că, în cazul specific al WebRTC, utilizarea LISP pentru multi-homing aduce beneficii pentru menținerea sesiunilor prin utilizarea tunelului LISP care menține conexiunile TCP deschise cu ajutorul metodei de automatizare implementate pentru recuperarea interfeței în caz de pierdere a semnalului. În plus, echilibrarea încărcării aduce avantaje semnificative atunci când vine vorba de utilizarea mai multor fluxuri WebRTC paralele, un caz de utilizare valid pentru utilizarea mai multor dispozitive capabile video atașate la același gateway IoT bazat pe LISP.

1.1.2. Rețele Definite Software – Software Defined Networks (SDN)

Rețeaua definită software (SDN) reprezintă o arhitectură de rețea dinamică, configurabilă, adaptabilă și eficientă din punct de vedere al costurilor, ceea ce o face ideală pentru nevoile aplicațiilor dinamice și de bandă largă de astăzi. Această arhitectură realizează o *separare a*

funcțiilor de control de funcțiile de transport date, permițând astfel un control al rețelei direct programabil (la nivel de controler SDN) și o metodă de abstractizare a infrastructurii fizice pentru aplicații și servicii (ce se pot implementa prin limbaje de programare generice sau servicii web REST – REpresentational State Transfer).
Mai multe implementări inovative au fost realizate pentru diverse soluții bazate pe rețele definite software, unele doar cu rol de demonstrare a unor concepte noi de orchestrare a traficului [3-6]:

- Prototip de distribuție a traficului în rețele definite software bazată pe principii semantice (Implementare POX și Sesame RDF (Semantic Web)) pentru trafic HTTP
- Implementarea de politici de taxare și control (PCC) în SDN
- Concept de securitate distribuită SDN pe bază de containere Docker
- Tratarea modelului QoS în SDN.

1.1.2.1. Rutare pe principii semantice în rețele definite software (SDN)

Metoda prezentată în [3] se referă la posibilitatea de rutare semantică în rețele definite software prin definirea de reguli de rutare bazate pe alte criterii decât protocoalele standard, ținând cont de relația dintre date și semnificația și utilitatea acestora, creând conștientizarea asupra conținutului (content-awareness) și rutarea ad-hoc a datelor.

Semantic Web este o extensie a World-Wide-Web cu scopul de a extinde conștientizarea calculatoarelor cu privire la semnificațiile datelor și semantică spre interacțiuni mai de încredere în cadrul rețelelor. Scopul demonstratorului implementat a fost acela de a integra în nodurile SDN inteligența (aproape de inteligența artificială exprimată de Web3.0) furnizată de modelele Semantic Web. Demonstratorul SDN efectuează rutarea datelor pe baza unei baze de date de cunoștințe (knowledge database) care conține informații despre *relația socială* dintre gazdele conectate la rețea. Acest lucru se realizează prin implementarea funcțiilor de control ale SDN, care interoghează baza de cunoștințe și acționează dinamic asupra informațiilor învățate, schimbând logica de rutare pe infrastructura de rețea reală, folosind protocolul OpenFlow. În plus, folosind inspecția profundă a pachetelor (DPI) analizăm traficul HTTP Web, folosind tehnici web semantice pure, pentru a identifica interesul utilizatorului de comportament cu accent pe posibile fraude și scenarii teroriste.

Arhitectura SDN pe care am folosit-o ca parte a demonstratorului este vizibilă în Fig. 14. Arhitectura SDN "clasică" are un controler central (controler C0 POX) care este capabil să manipuleze planul ”forwarding” (reprezentat de comutatorul S1) prin protocolul OpenFlow. În afară de componentele obișnuite ale SDN, am construit pe interfața “northbound” aplicația pentru ”rutarea socială", care accesează baza de cunoștințe semantice pentru interogatorii ad-hoc, declanșând regulile de rutare. Implementarea semantică s-a realizat folosind Sesame, este o structură Java pentru prelucrarea și manipularea datelor Resouce Description Framework - RDF (bazată pe interogarea SPARQL) - crearea, analiza, stocarea și interogarea bazelor de cunoștințe.

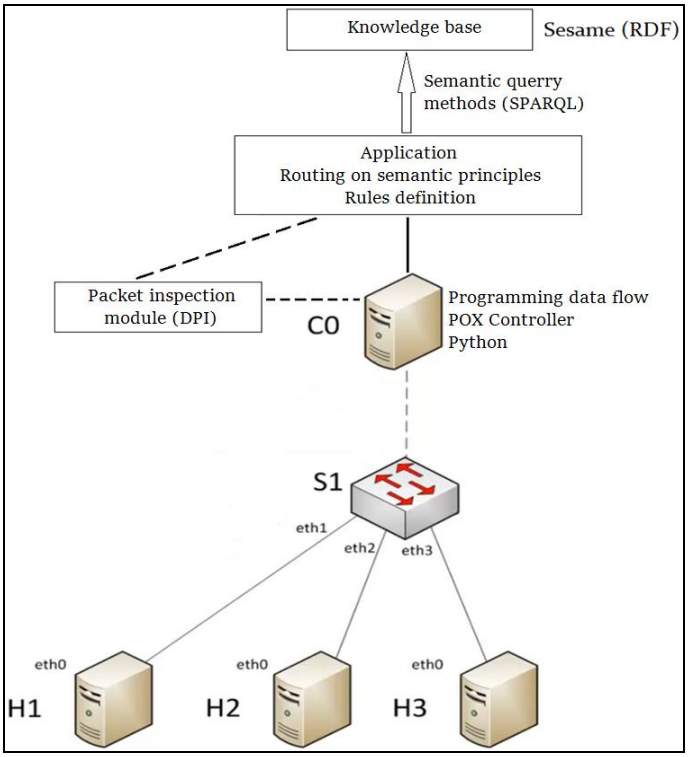


Fig. 14 Arhitectură SDN simplificată pentru rutarea semantică bazată pe conținut. Implementarea efectivă utilizează mai multe pivotări și gazde OpenFlow simulate

În rețelele SDN, logica de comutare este programată la nivel de controler și scrisă în FlowTables [10]. FlowTables includ reguli de „potrivire” („match”) și "acțiuni". O regulă de "potrivire" ar putea fi rezultatul unui interogatoriu de bază de cunoștințe prin SPARQL, în timp ce acțiunea ar putea fi o redirectare - "forward" către o anumită destinație sau o renunțare ("drop") la pachet.
Mai jos este un exemplu de definiție a regulilor de la POX în limbajul de programare python, pe baza adreselor IP și a protocolului de rețea:

```
def addRule(self, address, toAll=False, dl_type=0x800, nw_proto=1):
policyAddRule = of.ofp_flow_mod()
if dl_type == 0x800:
ip_addr = IPAddr(address)
rule_group = (ip_addr, dl_type, nw_proto)
policyAddRule.match.dl_type = dl_type
policyAddRule.match.nw_dst = ip_addr
policyAddRule.match.nw_proto = nw_proto
policyAddRule.priority = 65535
```

Pe lângă abordarea "clasică" a regulilor de potrivire SDN, am introdus interogarea bazei de cunoștințe Sesame din python pentru a extrage perechea de dispozitive (gazde) care au o relație de "cunoștință" ("prietenie"), pe baza principiilor bazelor de cunoștințe KB (Knowledge Base):

```
// Reading from the Sesame repositories
server="http://localhost:8080/openrdf-sesame"
command="/repositories/KBsocial/statements"
import urllib2
request=urllib2.Request(server+command)
request.add_header("Accept","text/plain")
temporar=urllib2.urlopen(request)
result=temporar.read()
(...)
// The SPARQL interrogation
URIpref="http://expl.ro#"
interrogation2='construct {?a x:AcquaintedWith ?b.?b x:AcquaintedWith ?a} where {?a
x:AcquaintedWith ?b}'
```

```
rezconstruct=graf.query(interrogation2,initNs={"x":URIpref})
acquaintance=[(str(x[0]),str(x[2])) for x in rezconstruct]
acquaintance2=[(x.rpartition("#")[2],y.rpartition("#")[2]) for (x,y) in acquaintance]
```

Rezultatul interogatoriului asupra cunoștinței între gazde (care au fost numite H1, H2 ... până la H8) ar indica perechile de gazdă care au "cunoștință una de celalaltă"/ relație

```
>>> acquaintance2
[('H1','H2'), ('H1','H3'),…,('H2','H1'), ('H2','H5'),…, ('H8','H7')]
```

În scop ilustrativ, folosind biblioteca phyton matplolib, se poate construi o reprezentare grafică a relației de cunoștință dintre gazde, ca în figura 15:

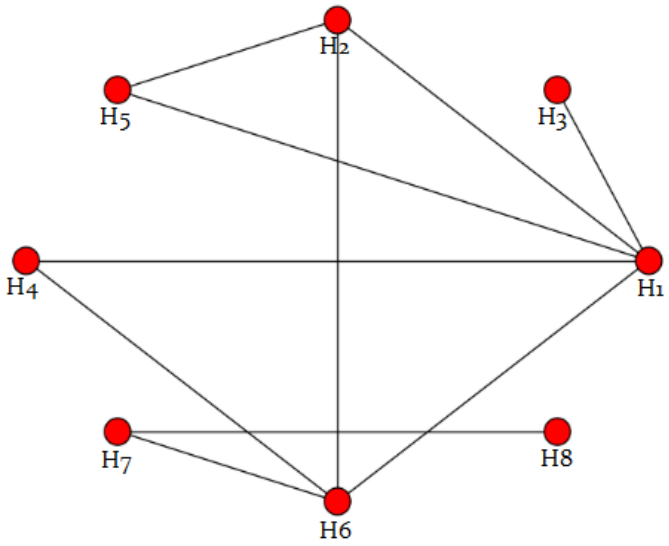


Fig. 15 Relația socială de "cunoaștere" dintre gazde poate fi construită vizual folosind biblioteci dedicate phyton

Folosind relația detaliată de mai sus, am implementat noi reguli de rutare, care redirecționează tot traficul primit de la o gazdă către gazdele "familiare", care au fost descoperite folosind interogațiile bazei de cunoștințe.

Rutarea "bazată pe conținut" pe care o demonstrez este o metodă de identificare a anumitor profilări ale comportamentului utilizatorilor pe baza relațiilor sociale ale utilizatorilor și pe baza conținutului/ resurselor accesate de utilizator. Metodele web semantice pentru a descrie relațiile (de exemplu, OWL- Ontologie Web Language), ar putea fi reutilizate nu numai pentru conținutul paginilor web, ci și pentru orice date legate ca parte a unei baze de date de cunoștințe.

Soluția ar trebui completată cu metode de tip Deep Packet Inspection asupra conținutului paginilor web accesate de utilizatori, cu scopul de a profila anumiți utilizatori. De exemplu, ar putea deveni evident că un utilizator periculos încearcă să construiască arme artizanale și încearcă să adune informații pe Internet despre elementele necesare, pe baza unor baze de date de cunoștințe conectate la acele pagini indexate. Acesta ar fi un exemplu de aplicație legală de interceptare (lawfull interception) care ar putea fi dezvoltată pe baza tehnologiilor SDN.

1.1.2.2. Implementarea de politici de taxare și control în SDN

Implementarea prezentată în [4] își propune extrapolarea funcției de PCC (Policy and Charging Control) - definită de standardul 3GPP (3rd Generation Partnership Project) - către rețelele IP (Internet și Cloud) utilizând conceptul de rețele definite software (SDN) ce permite implementarea de politici și algoritmi la scară largă. Implementarea demonstrează metode pentru definirea de politici de taxare și control pentru echipamente la nivelul controllerului SDN Foodlight, politici adaptate după modelul 3GPP și analiza în detaliu a pachetelor DPI, până la nivelul aplicație din stiva OSI. În viziunea amplă a acestei lucrări, ”taxarea” pornește de la înregistrarea și marcarea amănunțită (”ticketing”), în timp real, a fiecărui eveniment, a fiecărui contor (de durată, de volum,

de bandă – în general de ”calitate a serviciului”), o provocare pentru sistemele avansate de baze de date implicate.

Funcțiile de taxare și control PCC (Policy and Charging Control) sunt implementate la scară largă în rețele de comunicații mobile, fiind standardizate 3GPP. De la primele standardizări 3GPP pentru PCC, în UMTS Release 10, s-a trecut la introducerea de elemente de rețea dedicate PCRF (Policy and Charging Rule Function) în rețele LTE.

Politica de control bazată pe PCC 3GPP și arhitecturile similare sunt acum integrate în rețelele operatorilor, majoritatea dintre ei folosind un server pentru politici.

Platformele pentru politici, care în mod uzual conțin un server pentru politici și dispozitive pentru aplicarea politicilor, fiind deseori conectate și la sistemele de taxare și bazele de date ale abonaților, sunt folosite pentru a ajuta operatorii să controleze dinamic modul în care utilizatorii și aplicațiile folosesc resursele rețelei. Deciziile pot fi bazate pe o varietate de criterii, incluzând consumul de date al clientului, nivelul serviciilor, locația, aplicația, URL, perioada din zi, nivelul congestiei ș.a.

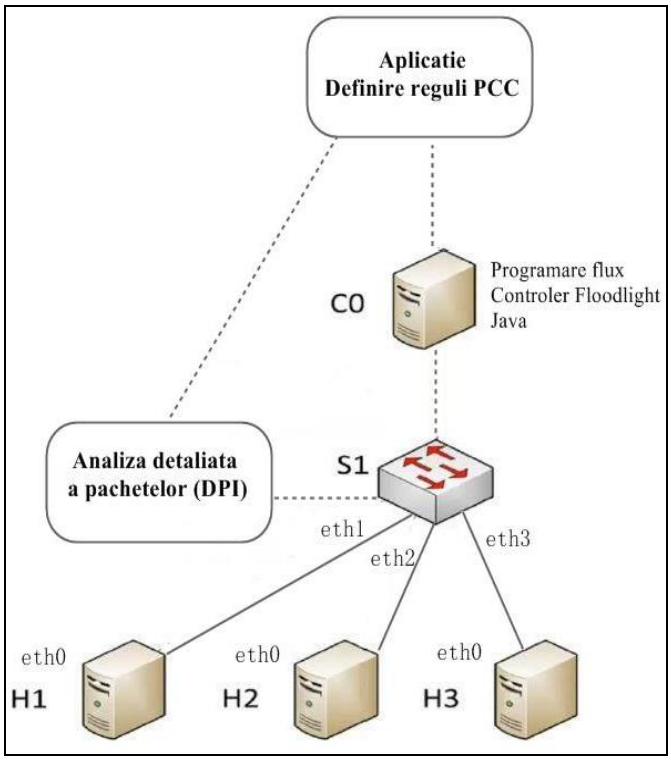


Fig. 16 Arhitectură SDN ce implementează politici de taxare și control bazată pe controller Floodlight Java și nDPI

O configurație a unei reguli PCC include un profil de acțiune care definește calitatea serviciilor (QoS) [5], taxarea, și preluarea controlului pentru a aplica către un flux de date de servicii. Un profil de acțiune PCC poate fi configurat și folosit în una sau mai multe reguli PCC pentru a oferi următoarele funcționalități: controlul calității serviciilor QoS, controlul taxării – PCRF determină când este adecvată taxarea online sau offline pentru o sesiune dată și precizează când pachetele IP asociate cu anumit profil trebuie blocate sau lăsate sa treacă.

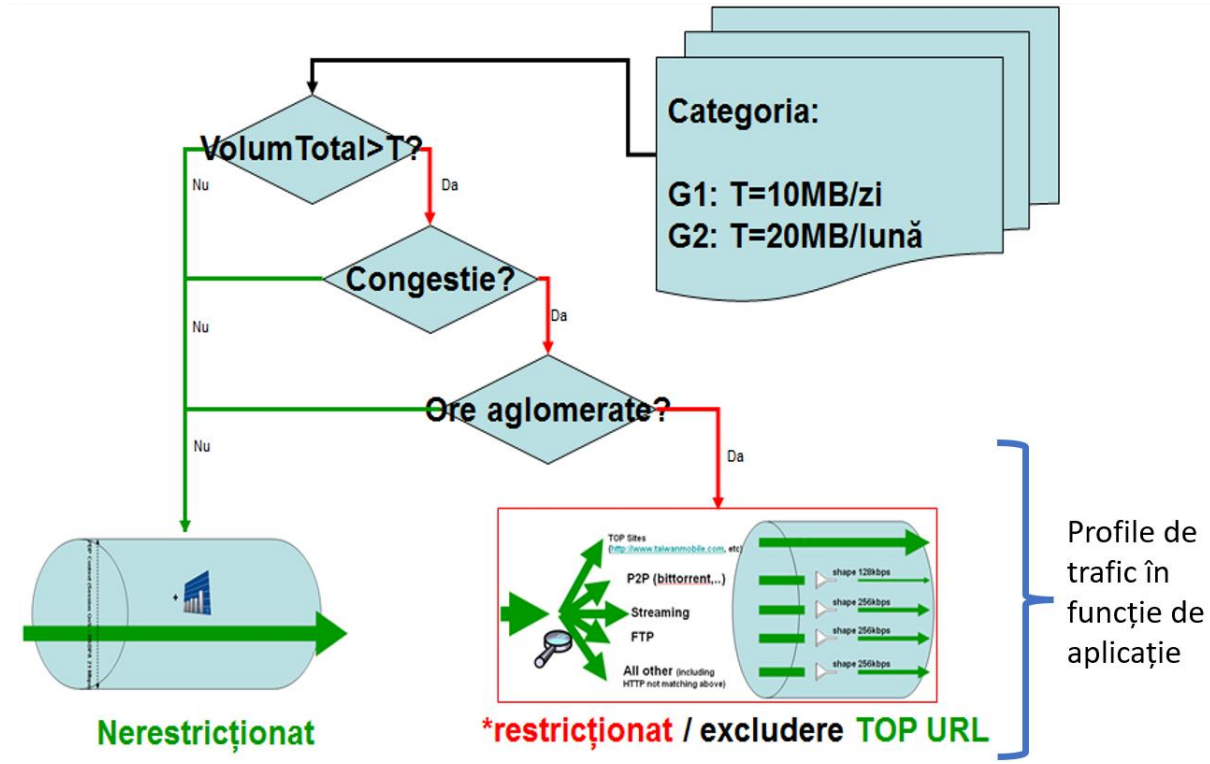


Fig. 17 *Exemplu de profil de Implementarea de politici de taxare și control (PCC) în SDN*

În controlerul Floodlight a fost activat firewall-ul care, neavând definite reguli, blochează tot traficul din rețeaua Mininet.

Blocarea pe baza de aplicatie se face pe baza ntopng care poate extinde regulile tipice de „potrivire” (match) din SDN către nivelele superioare ale stivei OSI.

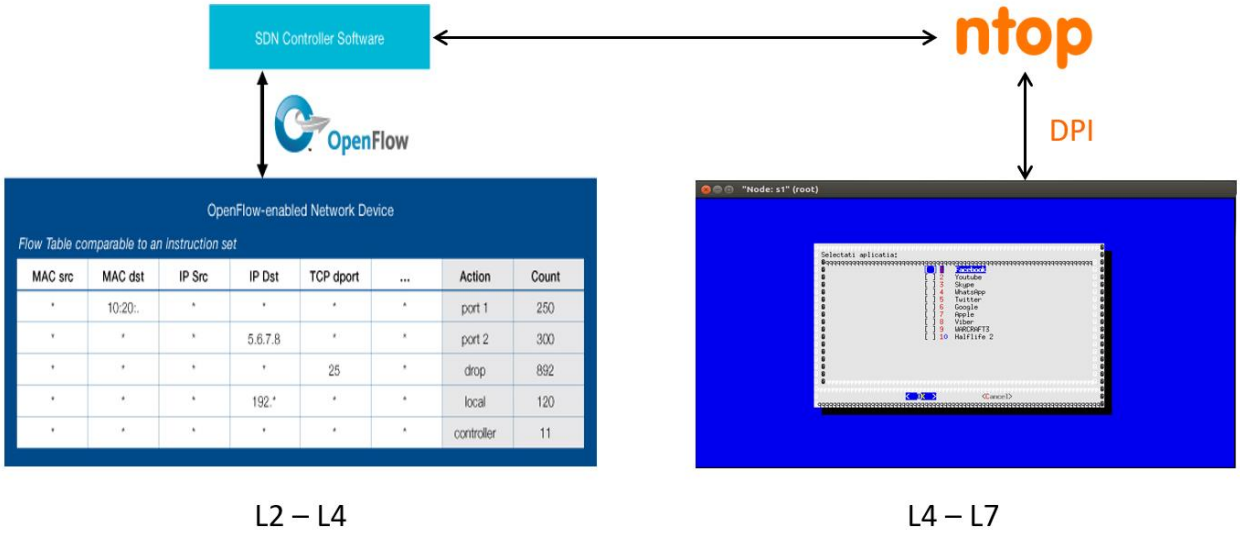


Fig. 18 *Regulile tipice de match ce se scriu în tabele de fluxuri la nivel de comutatoare pot fi complementare de filtrare de pachete pana la nivel 7 în stiva OSI*

1.1.2.3. Concept de securitate distribuită SDN pe bază de containere Docker în rețele industriale

Securitatea rețelelor industriale IP distribuite și conceptul de securitate a rețelei operaționale (OT security) vin sa completeze elementele de securitate ce se aplică în cazul rețelelor IT (IT security), deoarece vulnerabilitățile acestor sisteme ar putea afecta resursele critice, sau întrerupe funcționalități esențiale la nivel național. Firewall-urile de ultimă generație combină ”conștientizarea” asupra aplicațiilor și inspecția profundă a pachetelor pentru a oferi companiilor mai mult control asupra aplicațiilor, detectând și blocând în același timp amenințările de securitate. Exploatând beneficiile rețelelor SDN, am propus o implementare de securitate software, o rețea de elemente de tip „middlebox” distribuite, implementate dinamic ca și containere Linux și gestionate centralizat de un controler, bazat pe rețele definite de software (SDN).

Un middlebox (MB) este definit ca orice dispozitiv intermediar care îndeplinește alte funcții decât funcțiile normale, standard ale unui router IP pe calea datagramei dintre o gazdă sursă și o gazdă de destinație.

În cazul comunicațiilor industriale implementarea unei arhitecturi de securitate bazată pe MBs SDN poate aduce multe avantaje, cum este și implementarea pe care am prezentat-o în [6]. Protocoalele SCADA foarte folosite, cum ar fi Modbus sau IEC 61850, utilizate pentru automatizare, ar putea fi implementate într-o rețea SDN distribuită.

Avantajul implementării securității cu SDN este flexibilitatea sistemului: unele MB ar putea fi implementate la marginea rețelei, unele funcții de securitate trebuie să fie centralizate, așa cum este vizibil în figura 19. Politicile de securitate ar putea fi adaptate la cerere sau pe baza aplicației, iar migrarea și imbricarea ușoară a dispozitivelor de securitate migrate în întreaga rețea sunt îmbunătățite prin utilizarea containerelor Linux.

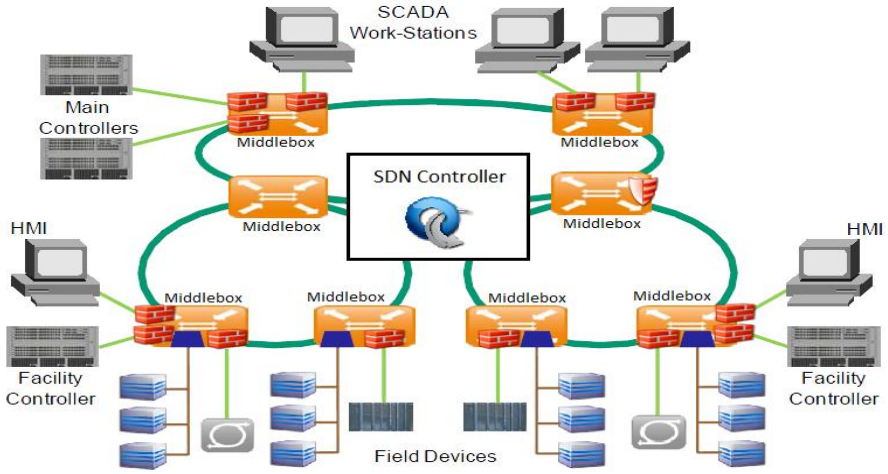


Fig. 19 Arhitectura SDN tipică aplicată pe un sistem SCADA cu middleboxes

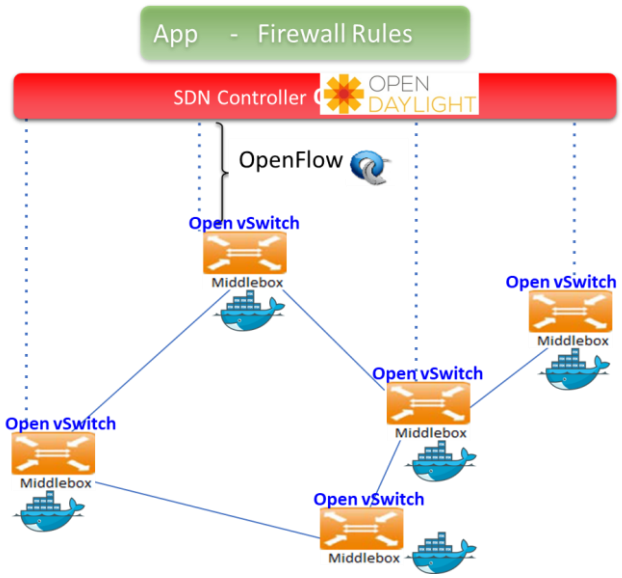


Fig. 20 Arhitectura SDN în implementarea cu controlerul OpenDayligh, cu fiecare switch/middlebox rulând la nivel de containere virtuale

Am implementat o soluție pentru MB virtualizate bazate pe containere Linux (LXC) care pot fi furnizate și configurate la cerere. Containerele Linux Docker oferă mai multe avantaje: rulează pe hardware comun "de la raft" (Commercial Off The Shelf - COTS) cu mai puține cerințe de resurse și nu necesită niciun software specializat pentru *hipervizori.* Tehnologia LXC este inclusă implicit în kernel-ul Linux începând cu versiunea 3.4.

LXC reprezintă o metodă diferită de virtualizare la nivel de sistem de operare. Acesta permite mai multe sisteme Linux izolate (containere) pentru a fi rulate pe un singur sistem de operare gazdă. Kernel-ul gazdă asigură izolarea proceselor și efectuează gestionarea resurselor.

Un container Docker poate porni extrem de rapid, ceea ce îl face cel mai bun candidat pentru scenariile de ”provizionare” (furnizare) la cerere. Containerele Linux oferă performanțe mai bune în comparație cu mașinile virtuale clasice și sunt potrivite pentru cazul unor implementărilor unor elemente decizionale software mai puțin complexe.

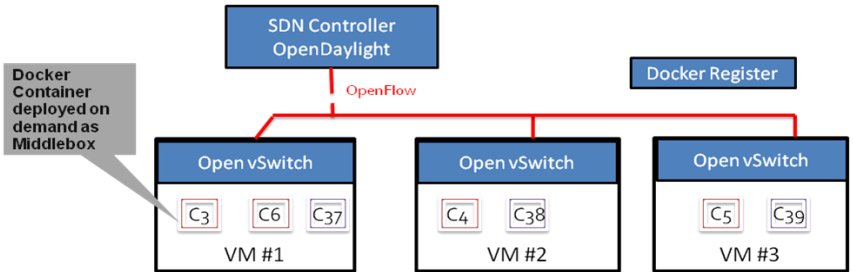


Fig. 21 Arhitectura rețelei SDN de testare

Pentru a simula mai multe noduri de rețea care găzduiesc MBs virtualizate, am construit un mediu de testare compus din 3 mașini virtuale care rulează Linux și fiecare VM care găzduiește mai multe containere (figura 21). Pentru că aveam la dispoziție o singură mașină fizică, am decis să folosesc VMs pentru a simula o topologie de rețea cu 3 noduri. Toate VM rulează peste un sistem de operare Linux folosind modulul de virtualizare Kernel (KVM). Sistemul de operare gazdă este o distribuție Ubuntu pe 64 de biți.

Mașinile virtuale rulează un sistem de operare (”invitat”) bazat pe distribuția Ubuntu 14.04 și fiecare a alocat 1 GB RAM. Pe fiecare VM am instalat un modul de switch virtualizat open source numit "open vSwitch" – după creare, toate containerele de pe un VM vor fi atașate la switch-ul său local. Switch-urile vor fi legate folosind tuneluri GRE (Generic Routing Encapsulation). Pentru a

permite comunicarea între containerele situate pe diferite mașini virtuale, am creat tuneluri GRE între cele 3 instanțe vSwitch deschise. Configurația tunelului este descrisă în figura 20.

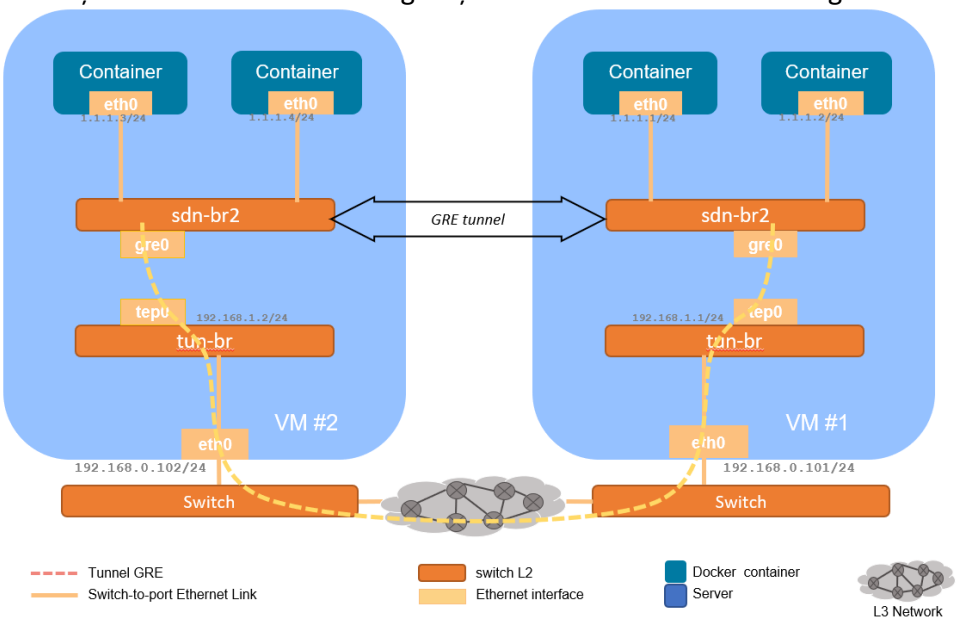


Fig. 22 Legătură virtuală directă între două punți folosind GRE

Fiecare instanță vSwitch deschisă este conectată folosind tuneluri GRE cu partenerii săi din celelalte VM-uri. Funcționalitatea MB este închisă într-un container Docker care poate fi furnizat la cerere. După ce containerul este pornit cu ajutorul controlerului SDN, intrările de flux pot fi introduse în comutatoarele virtuale și traficul direcționat către middlebox.

Când containerul este pornit, Docker va atribui automat adrese MAC și IP, iar containerul va fi atașat la bridge-ul docker0 implicit. Un exemplu cu 2 containere conectate la bridge-ul implicit este prezentat în figura 22.

După ce comutatoarele (switch) sunt înregistrate la controler, toate pachetele primite de switch-uri, care nu se potrivesc cu nicio intrare în tabelul de flux, sunt trimise controlerului care ia deciziile corespunzătoare. Controlerul poate decide să introducă o regulă în tabelul de flux al comutatorului sau să renunțe la pachet. Pe lângă interfața GUI, controlerul expune un set de API care pot fi utilizate pentru a configura automat fluxurile dintre containere. Acest lucru va permite aplicațiilor SDN să furnizeze dinamic containere și să configureze fluxul de date ca răspuns la solicitările utilizatorilor.

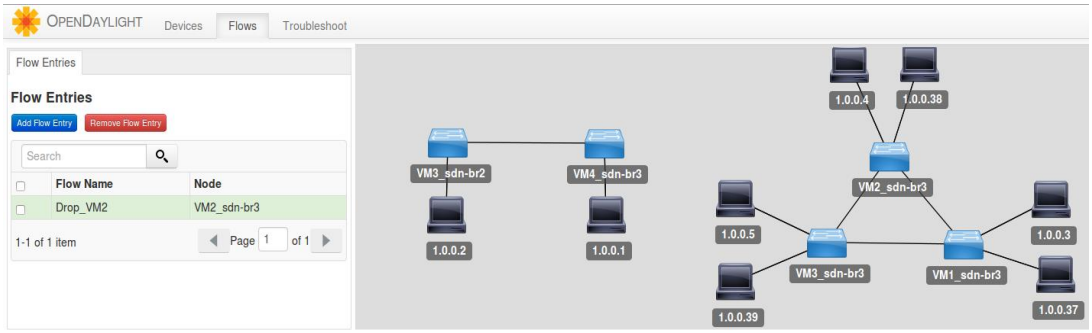


Fig. 23 Utilizarea aceluiași controler OpenDaylight SDN pentru poduri suprapuse

Folosind scripturi, putem instanția containerele Docker în oricare dintre VM-urile disponibile și, în același timp, folosind API furnizate de controlerul SDN, pentru a configura rețeaua de bază pentru a interconecta containerele. Acest lucru creează premisele de ”provizionare” dinamică a MBs. Aplicațiile industriale specifice pot rula la nivel de comutator, prin punerea în aplicare a protocoalelor industriale în containere. Implementările deschise *libmodbus* sau *libiec61850* pot fi

implementate la nivel de container cu avantajul de a exclude problema interoperabilității sistemului de operare, care este rezolvată de Docker.

1.1.3. Soluții pentru orchestrarea și automatizarea echipamentelor de comunicații

Partea de comunicații integrate include și o componentă extrem de importantă de validare din punct de vedere funcțional, dar și din punct de vedere al performanțelor. După cum s-a remarcat și în cazul echipamentelor speciale pentru măsurarea parametrilor rețelelor de comunicații mobile în cazul mobilității LISP, și alte echipamente dedicate au fost folosite pentru teste ale comunicației IP.

Pentru a răspunde acestor preocupări, am propus adoptarea unui cadru (framework) pentru standardizarea *configurării și agregării la distanță* a echipamentelor de telecomunicații, astfel încât acestea să poată fi oferite ulterior ca IaaS (Infrastructure-as-a-Service) de către operatori, similar serviciilor Cloud tradiționale. Ideea din spatele acestui cadru este de a asigura o interfață generică de asigurare a accesului care ”ascunde” complexitatea implementării printr-un set de capabilități standard care sunt independente de furnizor.

Adevărata provocare este de a asigura compatibilitatea între diferite generații de echipamente care aparțin chiar unor clase funcționale specifice, iar propunerea de standardizare a fost legată de adoptarea standardelor NTAF (Network Test Automation Forum) ce vor fi descrise mai jos.

În [7] am prezentat dezvoltarea unui mediu de testare în care platforma IXIA folosită ca element de testare devine parte a infrastructurii și emulator de elemente de rețea. Această implementare a fost realizată în cadrul companiei Siemens și instalată în cadrul laboratorului de testare al Orange Romania.

Pentru a valida soluția a fost configurată o topologie de testare cu ajutorul cadrului. Inițial, în acest scenariu, un Tektronix K1297 (emulator de protocol de rețea de telecomunicații) a fost utilizat pentru emularea a două elemente de rețea HLR (Home Location Register) și un BSC (Base Station Controller) prin rularea a două scenarii predefinite de emulare.

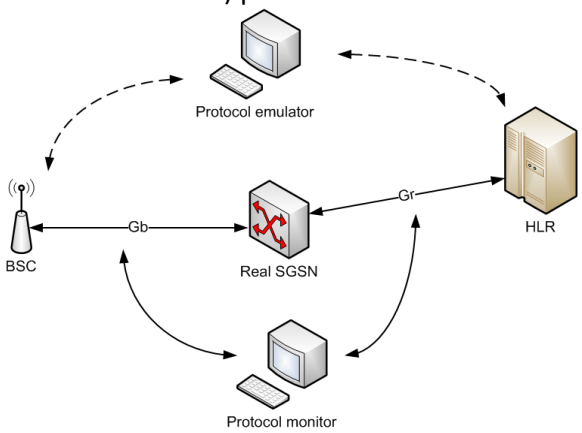


Fig. 24 Mediu de test integrat pentru o rețea 3G

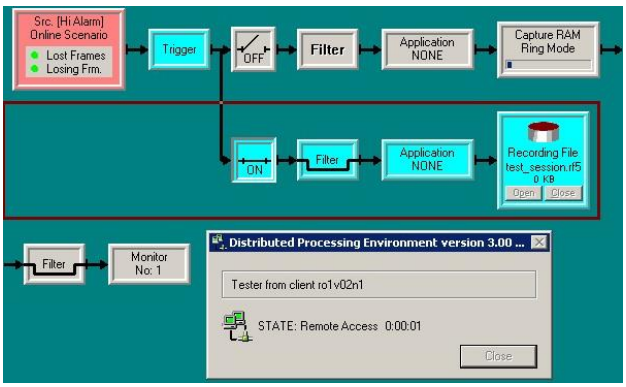


Fig. 25 Control la distanță pentru Tektronix K1297

Sistemul dezvoltat reprezintă un mediu de creare a serviciilor, orchestrația de testare și manager de resurse pentru resurse eterogene și se bazează pe unele concepte enunțate inițial în cadrul tezei de doctorat “Soluții de mobilitate în rețele eterogene”.

Implementarea are următoarele funcționalități:

- Descrierea grafică a topologiei de testare și a configurației elementelor de rețea (arhitectură orientată spre servicii – interfață web) – cuplate într-un mediu de creare de servicii (Service Creation Environment – SCE)
- Orchestrație de testare (definirea de Device-Under-Test DUT, teste care trebuie efectuate)

- Management optim pentru resursele de laborator (resurse moștenite, virtualizate, emulate, infrastructură de testare)
- Programare / Rezervare resurse
- Implementarea automată a configurației pe dispozitivele finale în laborator
- Include testarea de la distanță și controlul de la distanță al echipamentului

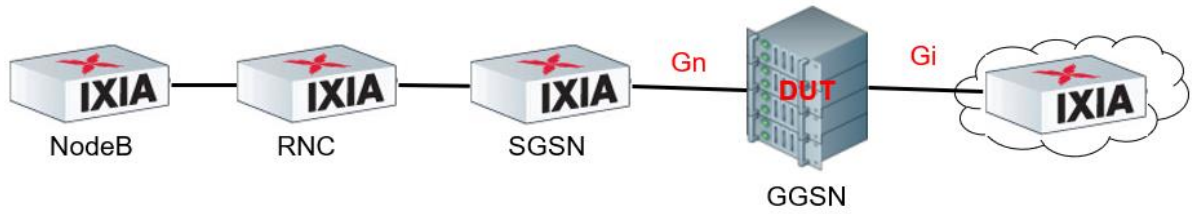


Fig. 26 Configurație de test ce integrează o componentă reală, GGSN ca element testat (Device Under Test) și cu restul rețelei emulate cu ajutorul echipamentelor Ixia

Teste efectuate:

1. Teste de trafic (http, ftp, RTSP) 2G/3G tip abonat
2. Proceduri Pcket Data Protocol PDP multiple – teste de tip Load & Stress
3. Teste directe de tunelare
4. Teste de handover inter SGSN
5. Recuperare GGSN după testele de resetare sistem

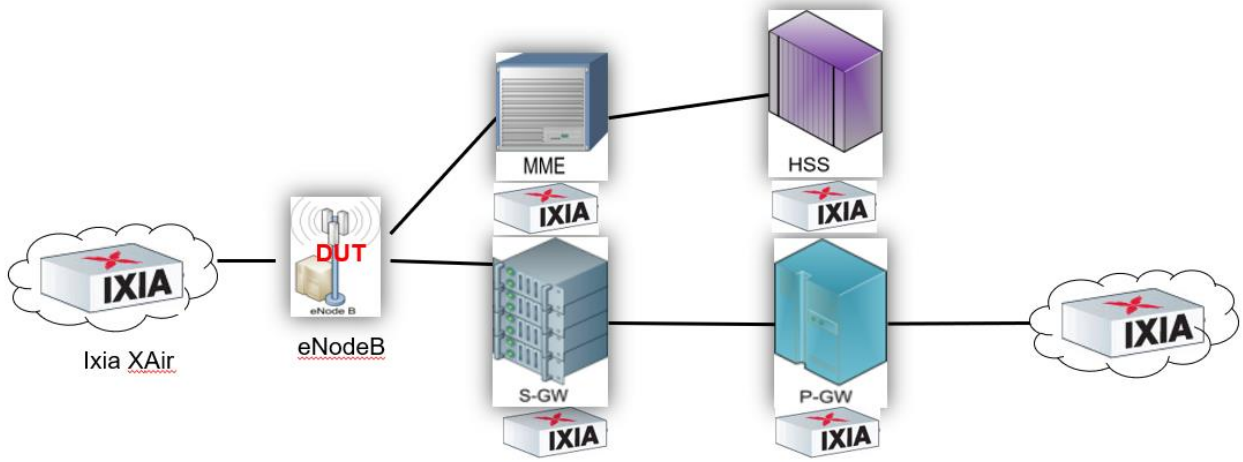


Fig. 27 Configurație de test ce integrează o componentă reală, eNodeB ca element testat (Device Under Test) și cu restul rețelei emulate cu ajutorul diverselor echipamente Ixia

Pentru dezvoltarea sistemului s-a realizat și o interfață grafică și de configurare (Service Creation Environment - SCE) în mediul de dezvoltare Java Spring cu resurse web folosind metode HTML5 pe baza framework-ului Primefaces, implementare descrisă în [8].

Mediul de creare a serviciilor (SCE), diferit de middleware-ul existent în majoritatea platformelor Cloud/IaaS care gestionează doar resursele virtuale, trebuie să fie conceput ca o umbrelă, integrator pentru serviciile de infrastructură bazate pe Cloud și rețelele de telecomunicații reale "clasice".

Deoarece caracteristicile oferite de PrimeFaces pentru a descrie caracteristicile Test Orchestration (definiția testului, selecția, parametrizarea și programarea) au fost ușor de implementat, am decis să implementăm un hibrid: descrierea topologiei și parametrizarea au fost implementate în Java Swing, dar integrate ca Java Applet în pagina SCE (Service Creation Environment). Toate celelalte părți ale sistemului legate de teste și rezultate au fost dezvoltate în PrimeFaces. PrimeFaces este o bibliotecă open source complexă care extinde posibilitățile JSF (Java

Server Faces), o specificație Java pentru construirea interfețelor de utilizator bazate pe componente pentru aplicații web.

În aplicația SCE pe care am dezvoltat-o cu HTML5, integrarea componentelor a fost realizată cu succes: server și bază de date MySQL; server local Apache Tomcat; Biblioteca DWR – Direct Web Remoting, care permite mai multor utilizatori să acceseze interfața web în același timp; Java Server Pages, care permite ca codul Java să fie scris în HTML5. DWR este o bibliotecă care permite Java funcții de apel de la JavaScript și vice-versa, apelul de funcții JavaScript de la Java (de asemenea, numit invers Ajax). Ajax funcționează prin generarea dinamică a JavaScript, pe baza claselor Java. Chiar dacă codul aparent rulează în browser, în realitate, totul rulează în partea de server.

Descrierea infrastructurii pornește de la topologie (figura 28): în cazul nostru solicitarea este de a putea "drag-and-drop" elementele de rețea (numai pictograme, avatare, reprezentând rolul de rețea al unui nod specific) pe o "pânză" (”canvas”), o metodă rapidă și intuitivă. De asemenea, o parte importantă este parametrizarea elementelor de rețea.

Parametrizarea poate avea niveluri diferite: specificând numai unele caracteristici esențiale în SCE și lăsând restul configurației ca o sarcină pentru Managerul de resurse care va procesa solicitarea de serviciu sau va merge în profunzime cu configurarea și specificarea interfețelor, adreselor IP, setarea semnalizărilor și specificarea protocoalelor de utilizat. Faza de parametrizare ar putea include personalizarea paletei de echipamente ce urmează a fi utilizată (echipamente telecom reale, echipamente de testare, servere de aplicații) sau posibilitatea de a alege pentru fiecare funcție de element un furnizor sau un anumit model de echipament, din lista de opțiuni disponibile.

Partea de orchestrație de testare descrie testele și includerea / încărcarea scripturilor de automatizare. Programarea testelor și formularul electronic de selecție a testelor sunt necesare, precum și posibilitatea de navigare a rezultatelor testelor și a statisticilor. O caracteristică specifică este posibilitatea de a defini un dispozitiv în test (DUT) - în acest fel, pe baza interfețelor elementului DUT, sunt disponibile un set de teste.

Un avantaj al rețelelor de telecomunicații este reprezentat de standardizarea clară (ca premisă a managementului complexității): configurațiile sunt standard, rolurile și interfețele elementelor sunt predefinite, precum și fluxurile de mesaje între elemente. Acesta este motivul pentru care și testele ar putea fi definite după câteva modele: de exemplu, în cazul rețelelor 3G, testele de interfață Gn pentru GTP - GPRS Tunneling Protocol între elementele de bază ale pachetelor ar putea fi predefinite sau, de asemenea, în cazul LTE, testele Diameter pentru interfața S6.

Poate cea mai importantă funcție a SCE este generarea informațiilor despre solicitarea serviciului (un rezultat al tuturor acțiunilor de configurare la nivel de SCE). Această solicitare este trimisă de pe platforma web către un manager de resurse care alocă elementele de infrastructură corespunzătoare (reale, emulate sau virtualizate), în continuare face implementarea configurației (configurați interfețe, parametri) și, de asemenea, începe operațiunile de testare programate.

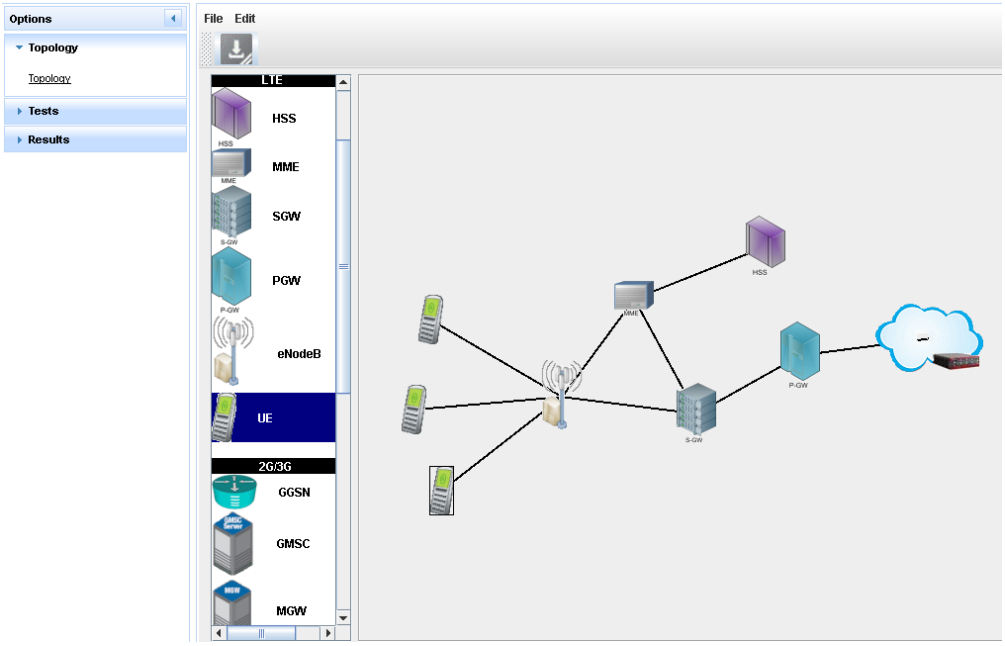


Fig. 28 Descrierea vizuală a topologiei în SCE. Topologia descrie o configurație pentru testarea LTE. Toate elementele reprezintă roluri funcționale, implementarea configurației pe infrastructură va fi efectuată de Resource Manager

Rolurile funcționale descrise includ elemente 3G și LTE și rețele de rutare/ comutare, dar și infrastructura de testare: așa cum este vizibil în Figura 28 , P-GW (Packet Gateway) este conectat la un element Cloud reprezentând un emulator care va genera trafic, așa cum vine de pe Internet, deoarece P-GW este considerat în LTE poarta de acces către alte rețele publice, inclusiv Internet. Toate elementele pot fi parametrizate făcând dublu-clic pe pictograma elementului.

De asemenea, pentru fiecare element avem posibilitatea de a accesa consola de echipamente prin acces shell / SSL (odată ce echipamentul cu rolul de rețea specificat va fi selectat de Managerul de resurse). Meniul SCD este organizat în trei categorii: Topologie, Teste (figura 29) și Rezultate.

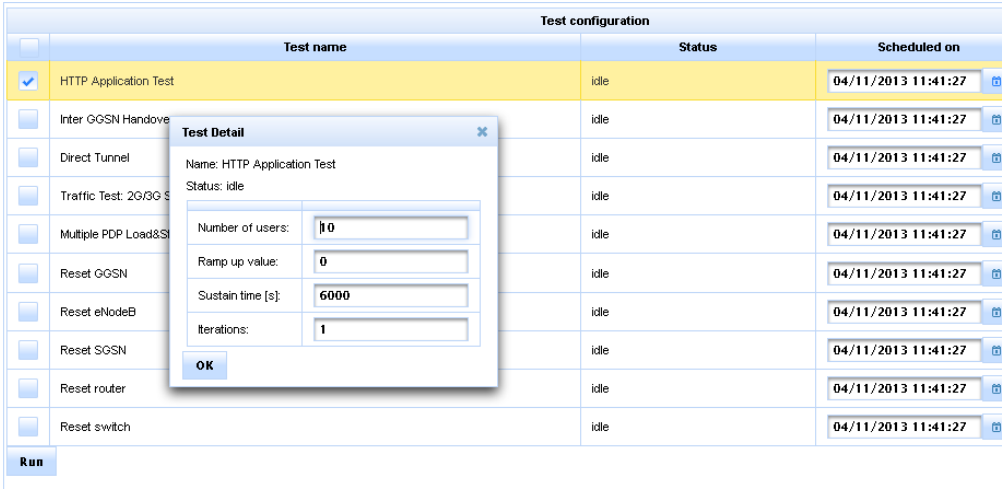


Fig. 29 Orchestrarea testelor include o listă de teste care ar putea fi selectate, ordonate, parametrizate, programate și, de asemenea, starea testului

În implementarea SCE, comunicarea client-server utilizează două tipuri de structuri XML: clientul va genera o solicitare de serviciu de tip "NetworkConfiguration" și serverul va răspunde după procesarea solicitării cu un XML de tip "Rezultat".

Solicitarea prezentată mai jos va include date de autentificare și definiția și planificarea serviciului:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<NetworkConfiguration>
      <AuthenticationData>
            <UserName>Test</UserName>
            <Password>test</Password>
      </AuthenticationData>
      <TestSchedule>
            <TestStart>2012-03-29T23:33:32.264+02:00</TestStart>
      </TestSchedule>
      <Routers>
            <Router DisplayName="DN1" HostName="RT1" ID="1" Vendor="Cisco"
                  Version="7200">
                  <Interfaces>
                        <Interface ID="1" IP="192.168.8.20"
                              Mask="255.255.255.0" />
                  </Interfaces>
            </Router>
      </Routers>
</NetworkConfiguration>
```

1.1.3.1. Abstractizarea / Generalizarea echipamentelor de rețea prin conceptul de "driver"

Un alt aspect important al rețelelor eterogene este posibilitatea de a programa rețeaua, independent de funcțiile specifice furnizorului. Într-una dintre implementările anterioare am folosit standardizarea furnizată de NTAF (Network Test Automation Forum) care utilizează conceptul de dispozitive generice și drivere specifice pentru automatizare. Conceptul de driver NTAF era atât de generic încât avea un exemplu de driver pentru un prăjitor de pâine (a se vedea figura 30) și folosea ca protocol principal XMPP.
Primul set de specificații pe care le-am implementat au fost "Înregistrarea, descoperirea și activarea instrumentelor" și "Modul de automatizare a instrumentelor".

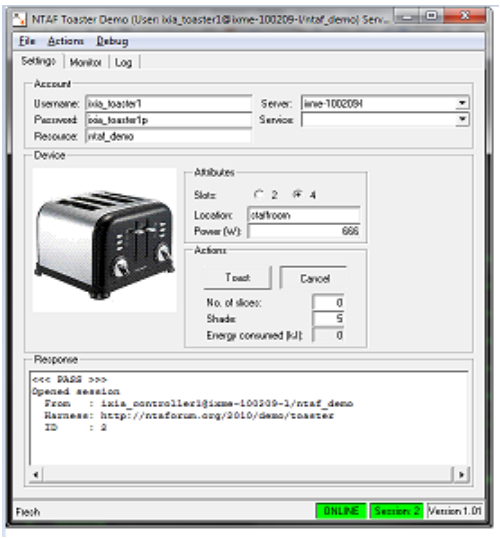


Fig. 30 Concept de driver generic, de exemplu pentru un prăjitor de pâine (sursa: NTAF)

Folosit anterior cu succes pentru camerele de teleconferință, XMPP (Extensible Messaging and Presence Protocol) a fost propus de NTAF pentru automatizarea rețelei, reutilizarea conceptelor de rețele sociale.

În implementarea noastră, am folosit OpenFire ca XMPP Server și Spark ca și client XMPP.

Elementele de rețea au fost astfel agregate într-o "rețea socială", având toate echipamentele integrate enumerate în lista de contacte afișată de Spark (a se vedea figura 31). Elementele de rețea *își publică starea/disponibilitatea și capabilitățile* utilizând XMPP.
În plus, putem trimite comenzi către un echipament dintr-o fereastră de chat bazată pe parser-ul XMPP-to-SNMP pe care l-am implementat.

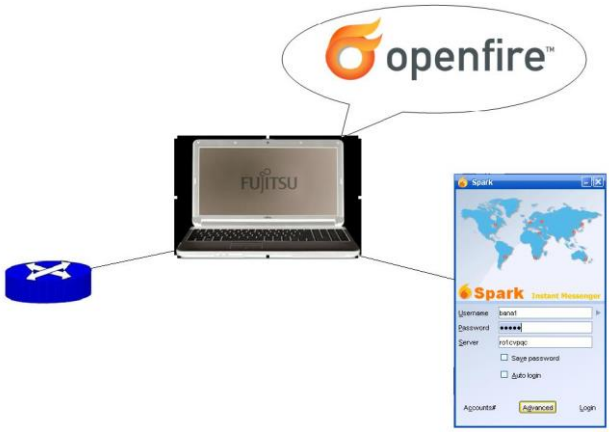


Fig. 31 Implementarea comunicării XMPP cu echipamentele de rețea utilizând Serverul OpenFire XMPP: Elementul de rețea este accesibil prin lista de contacte a clientului Spark

Folosind standardul NTAF prin protocolul XMPP, am automatizat diferite resurse – reale, emulate (imagini Cisco Dynamips) și virtualizate (imagini virtuale Juniper Olive). Cu toate acestea, metoda de comunicare cu fiecare dispozitiv a fost *unitară și independentă de furnizor* (producătorul dispozitivului), deoarece m-am bazat pe drivere (plugin-s).

Pe baza aceluiași concept de driver (conceptul care a fost implementat cu atât de mult succes în cazul instrumentelor virtuale și al standardizării IVI - interfețe virtuale interschimbabile) există, de asemenea, metode programabile pentru abstractizarea rețelei folosind Python.

Pentru a permite extensibilitatea viitoare, soluția implementată utilizează limbaje scriptice dinamice, în special Groovy, care permite definirea în continuare a configurației platformei la fața locului, fără a fi nevoie de a redistribui întreaga soluție. Această abordare modulară permite operatorului să adauge noi echipamente cu ușurință în acest ecosistem și să ofere doar adaptările limbajului de provizionare necesare la fața locului.

După cum se arată în figura 32, soluția introduce două straturi de directare între utilizatorul final și echipamentul real (în cazul prezentat, elementele de rețea telecom formează arhitectura GSM și 3G), cu scopul de a adapta furnizarea independentă a furnizorului la semantica specifică hardware-ului și apoi automatizarea întregii implementări.
O altă abordare de automatizare a echipamentelor de telecomunicații ce au și interfețe grafice este descrisă în [9]

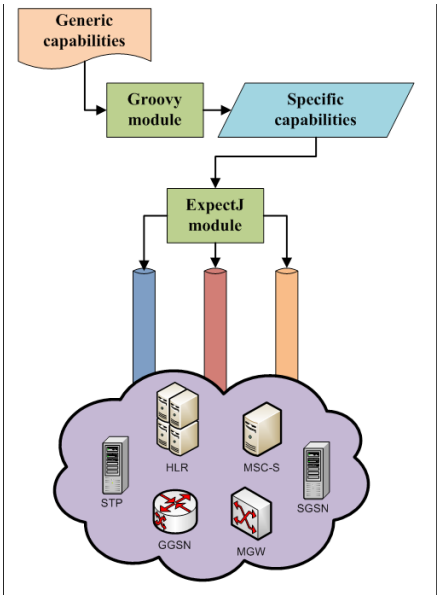


Fig. 32 Abordare modulară de automatizare a echipamentelor telecom prin diverse nivele de scripting

1.1.3.2. Realizarea de apeluri VoIP utilizând un server IMS (IP Multimedia Subsytem) având ca suport o rețea emulată LTE

Implementarea descrisă în [10] este dedicată soluțiilor bazate pe IMS pentru rețelele LTE. Rețeaua ”demo” este formată din 3 componente principale, rețeaua de abonați, rețeaua LTE implementată în OMNeT și comunicarea (folosind mesaje reale) cu mediul exterior, care include și platforma OpenIMS.

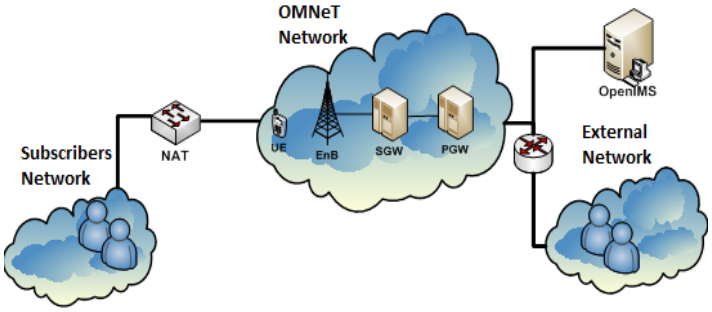


Fig. 32 Componentele demonstratorului pentru VoLTE folosind IMS

Open IMS Core este o implementare open source a elementelor IMS Call session Control Function (CSCFs) și a unui server dedicat abonaților proprii (din rețeaua ”de domiciliu” – HSS, Home Subscriber Server) care formează împreună elementele de bază ale tuturor arhitecturilor IMS/NGN. Este un proiect al Institutului Fraunhofer, ”FOKUS”, care își propune să umple locul IMS în peisajul software Open Source cu o soluție flexibilă și extensibilă.

Pentru a adapta mesajele trimise de la o componentă de rețea, menționată mai sus, la alta, au fost necesare două medieri, un router NAT (Network Address Translation) și un router RIP. NAT, așa cum este vizibil în Fig.33, a fost folosit pentru a direcționa mesajele de la clienții reali de telefoane SIP (Rețeaua abonaților) la subrețeaua OMNeT dedicată utilizatorilor simulați (UE). Acest sub-modul NAT se bazează pe un set de adrese mapate.

Pentru simularea abonaților care utilizează servicii de voce există mai multe opțiuni client SIP: X-Lite, OpenICLite, UCTIMSClient. Am ales să lucrez cu UCTIMCClient, o aplicație special concepută pentru OpenIMS, având o serie de parametri preconfigurați.

Mesajele SIP sunt încapsulate în traficul GTP, în timp ce sunt transportate de rețeaua LTE.

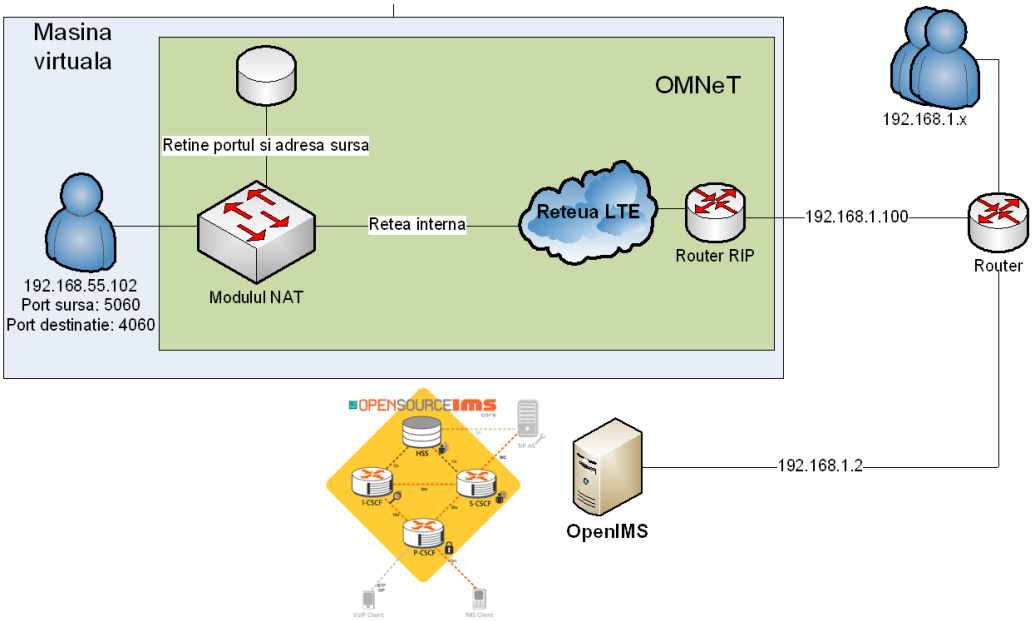


Fig. 33 Arhitectură demonstrator VoLTE folosind OMNeT și OpenIMS

Simulatorul LTE implementat

OMNeT++ este o bibliotecă de simulare C++ extensibilă, modulară, bazată pe componente și un cadru – în primul rând pentru construirea simulatoarelor de rețea. Domeniul LTE EPS este extrem de vast, deci nu am implementat toate funcționalitățile la nivelul OMNeT. Simularea 4Gsim LTE s-a axat pe implementarea semnalizării, dar din motive demonstrative de integrare cu IMS, au fost incluse și o parte din protocoalele privind planul de date.

Am implementat un set de "modele complexe", bazate pe modelul INET existent, inclusiv protocoale și interfețe pentru principalele elemente de rețea ale arhitecturii LTE: acestea sunt User Equipment, eNodeB, MME, HSS, S-GW și P-GW. Așa-numitele "module simple" pe care le-am implementat sunt încorporate în modelele complexe, descriind interfețe de protocol: nivel de interfețe radio, cum ar fi modulul NAS (Non Acess Startum) și modulul LTERadio (utilizat pentru UE pentru comunicația cu eNodeB), S1AP, pentru interconectarea eNB și MME, modulul DiameterS6a, utilizat pentru comunicarea cu HSS. Desigur, modulele importante sunt cele care descriu interfețele GTP-C și GTP-U, deoarece traficul SIP de la utilizatori la IMS-ul de interconectare, a fost transportat la planul utilizatorului LTE prin încapsulare GTP-U.

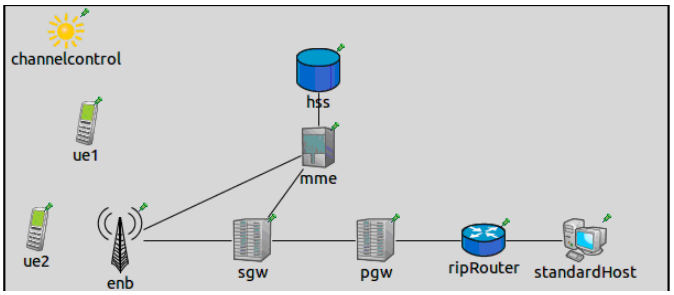


Fig. 34 Arhitectură LTE simplă implementată în 4Gsim OMNeT++

Ca exemplu pentru un modul complex, Fig. 35 arată modelul P-GW pe care l-am implementat în OMNeT, inclusiv interfețele GTP-C și GTP-U, modulul de rutare RIP și aplicația CLI. Majoritatea elementelor reale au un set de comenzi specifice furnizorului, astfel încât acest modul CLI pe care l-am scris permite ca orice element de rețea LTE din rețeaua emulată să fie accesat printr-o interfață "telnet-like". Au fost implementate comenzi CLI specifice, în principal pentru

monitorizarea sau interogarea unora dintre elementele de rețea. De exemplu, o comandă afișează căile utilizate pentru a interoga tunelurile GTP definite la un moment dat la nivelul P-GW. De asemenea, în scopul monitorizării, tcpdump poate fi pornit pe orice interfață simulată pentru captarea pachetelor.

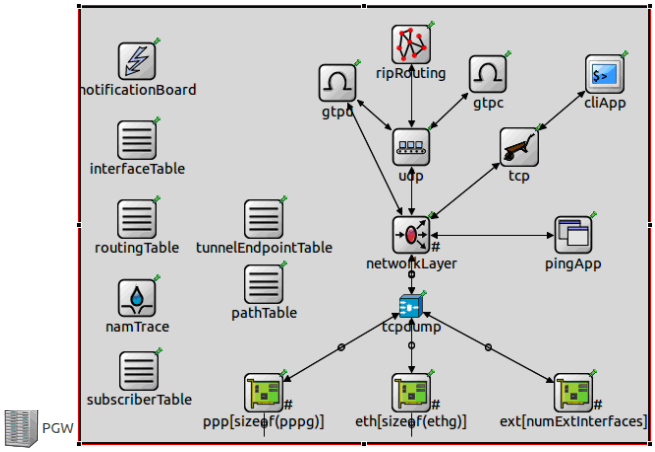


Fig. 35 Modulul P-GW implementat în 4Gsim

Scenariile testate includ atașarea echipamentului mobil la rețeaua LTE, inclusiv alocarea adresei IP și înregistrarea la OpenIMS SIP Server, testarea aplicațiilor ping pe baza modulului PingApp existent în OMNeT, dar scopul demonstratorului a fost scenariul VoIP end-to-end, prin rețeaua LTE și rețeaua IMS.

În scop educațional, toate fluxurile de mesaje au fost monitorizate, la nivel de rețea LTE și la nivel de protocol SIP, iar configurația elementelor de rețea a fost verificată prin aplicația CLI implementată. La nivelul OpenIMS, au fost monitorizate, de asemenea, înregistrarea utilizatorilor SIP și mesajele interne între funcțiile de control al apelurilor/sesiunilor (P-CSCF, I-CSCF și S-CSCF).

1.1.4. Platforme pentru servicii de comunicații multimedia cu scop academic

Unele soluții de comunicații au fost dezvoltate în scop educativ sau din perspectiva creării de servicii pentru comunicații pentru utilizatori academici. În această secțiune voi detalia câteva implementări de acest fel, iar în secțiunea dedicată soluțiilor de securitate voi prezenta și alte soluții dezvoltate cu scop educativ dar acoperind teme de securitate cibernetică.

Soluțiile de comunicații propuse pentru educație capătă o mai mare importanță din perspectiva actuală a unei societăți tot mai orientată spre colaborare prin comunicații moderne, orientare accelerată și de pandemia COVID 19.

O primă implementare o reprezintă o platformă demonstrator bazată pe Unify Circuit WebRTC integrată cu alte aplicații bazate pe web care expun API-uri și dedicate browser-elor simple pe clienți cu putere de calcul scăzută ("thin clients"). WebRTC (Web Real-Time-Communications) permite învățarea mixtă (”blended learning”) în universități și sprijină "universitățile virtuale". În aceste "universități Cloud", furnizorii de echipamente își pot integra și "laboratoarele ca serviciu".

Figura 36 detaliază evoluția modelelor de comunicare (cu un exemplu pentru comunicarea în timp real - mai precis comunicarea vocală) de la comunicațiile clasice la cele mai noi protocoale web.

WebRTC este o colecție de protocoale de comunicații și interfețe de programare a aplicațiilor care permit comunicarea în timp real prin conexiuni peer-to-peer. Informațiile sunt trimise direct în browser și ajung la partenerul de comunicare printr-o interfață HTTPS (Hyper Text Transfer Protocol - Secure). Aplicațiile WebRTC sunt de obicei scrise în JavaScript și HTML5 și sunt procesate de browsere folosind API-urile WebRTC pe care le integrează. Aceste API îndeplinesc funcții de gestionare a conexiunii, codificare și decodare, control media și NAT (Network Address Translation).

Metodele VoIP sunt reduse la minimum, fiind expuse ca aplicații simple și integrate cu interfețe create în JavaScript, HTML sau CSS. Acest serviciu preia funcțiile de control pentru apeluri (de obicei atributul sistemelor dedicate PBX-Private Branch eXchange). Acesta este motivul pentru care costurile sunt reduse semnificativ, de cele mai multe ori tarifarea pentru servicii fiind bazată chiar pe QoS (calitatea serviciilor oferite). Un alt mare avantaj pentru utilizarea WebRTC pentru servicii educaționale este că serviciile de comunicare în timp real pot fi integrate cu alte aplicații și soluții software livrate din Cloud.

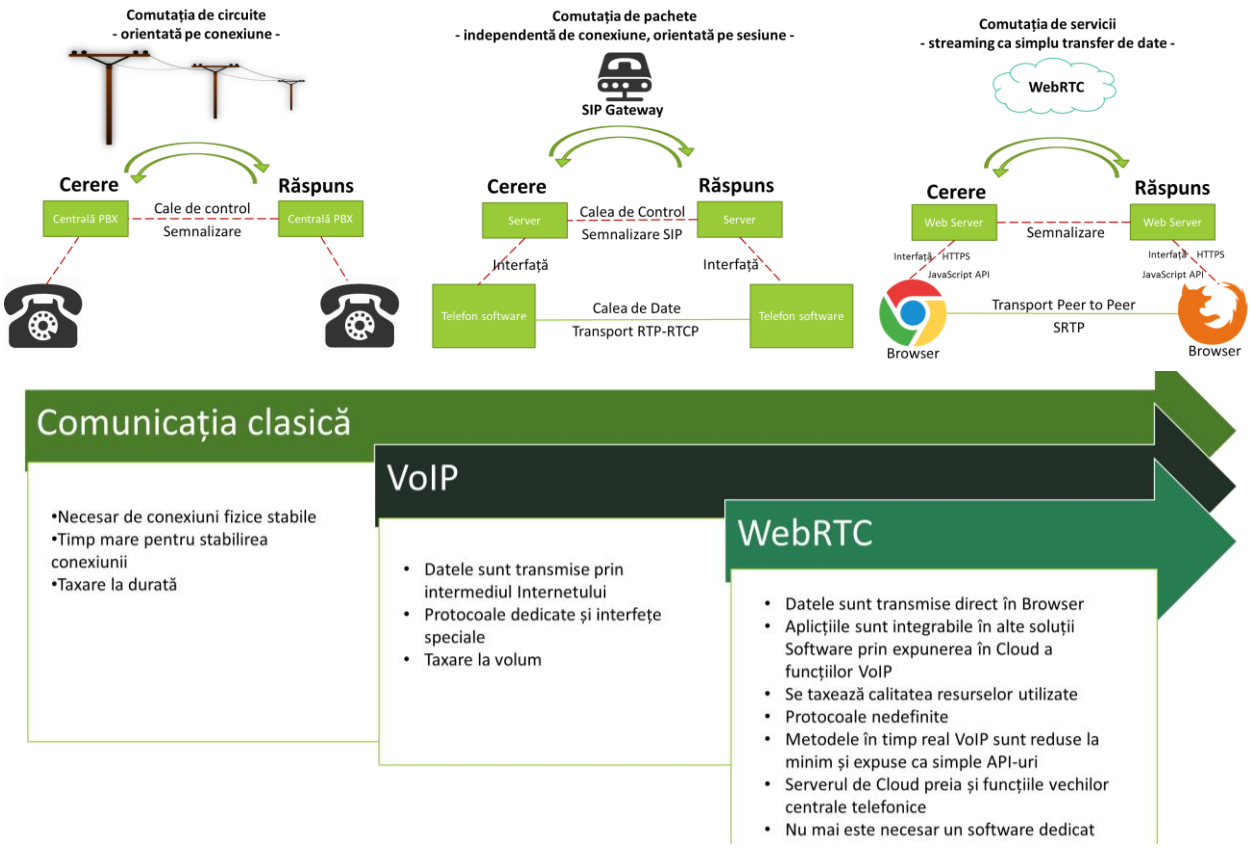


Fig. 36.Evoluția modelelor de comunicație corelate integrării intre sistemele de calcul și comunicații

Scopul demonstratorului descris în [11] a fost de a crea un mediu similar cu o clasă virtuală – ”Circuit” aduce video HD, voce, partajarea ecranului, mesagerie și partajare de fișiere într-un singur panou. Toate acestea sunt foarte utile pentru o platformă educațională [12].

Cu toate acestea, pentru construirea de aplicații personalizate, a fost dezvoltată o interfață grafică de utilizator dedicată, iar aici fiecare dezvoltator are posibilitatea de a face integrări cu alte aplicații, cum ar fi, de exemplu, Moodle. În plus, toate API-urile WebRTC ar trebui să fie invocate și încorporate în aplicația utilizatorului final.

Elementele folosite în implementare sunt detaliate în diagrama de mai jos:

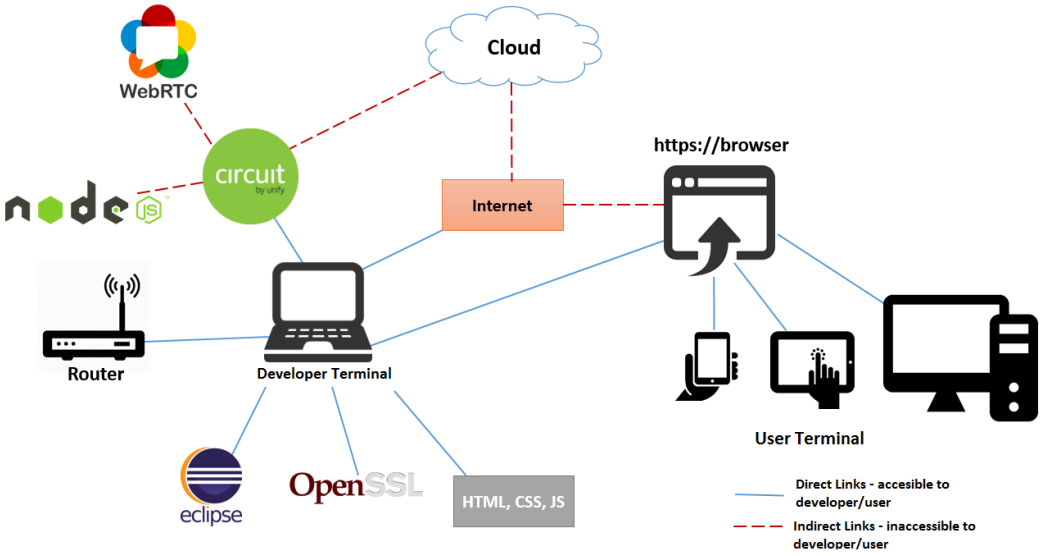


Fig. 37. Implementare pe bază de WebRTC pentru clase virtuale în Internet

Mai jos se regăsește, ca exemplificare, secvența de cod pentru controlul fluxului video:

```
function onVideoChange() {
  var selectedConvId = $convList.options[$convList.selectedIndex].value; //take over the
conversation form the list of convesartions
  var call = _calls[selectedConvId]; //select the conversation
  if (call && call.localMediaType.video !== enableVideo.checked) { //activate video by
bifeaza casuta
    _client.toggleVideo(call.callId).then(function () { //open the video flow
      console.log('Local video was successfully toggled');
    }).catch(function (err) { //exception in case of error
```

O altă implementare prezentată în [13] reprezintă o soluție pentru laboratoarele de calculatoare universitare, pentru a răspunde complexității date de numărul mare de instrumente software complexe, mașini virtuale, diferite sisteme de operare și gama largă de clase de nivel diferit cu lucrări de laborator, în special pentru studenții la ICT. Utilizarea Cloud-ului privat deținut de universități ar putea fi o alternativă, dar nu toate universitățile își pot permite o soluție Thin Client și Zero Client.
Soluția propusă reprezintă un pas intermediar ne-costisitor spre lucrul cu resurse distribuite pentru laboratoarele de calculatoare, un sistem de boot de la distanță, folosind Clonezilla și Diskless Remote Boot în Linux – DRBL.

Scenarii posibile pentru network boot cu Clonezilla și DRBL:

a) Boot de rețea, toate sistemele de fișiere montate de pe server, potrivite pentru funcționarea intensivă a procesorului, aplicații cu stocare intensivă care au nevoie de stocare de rețea dedicată; sistemul de operare instalat nu este afectat;

b) Boot de rețea, sistem de fișiere ”rădăcină” *(root)* montat de pe server, unele partiții locale montate de pe HDD intern pentru date temporare, potrivite pentru funcționarea intensivă a procesorului și utilizarea stocării medii; sistemul de operare instalat nu este afectat, dar este nevoie de o partiție dedicată pentru sistemul de operare încărcat din rețea;

c) Clona de rețea, fiecare stație de lucru este clonată de pe server și apoi este utilizată ca stație de lucru independentă, este nevoie de mai mult timp pentru implementare; sistemul de operare utilizat este suprascris de fiecare dată când se face o implementare.

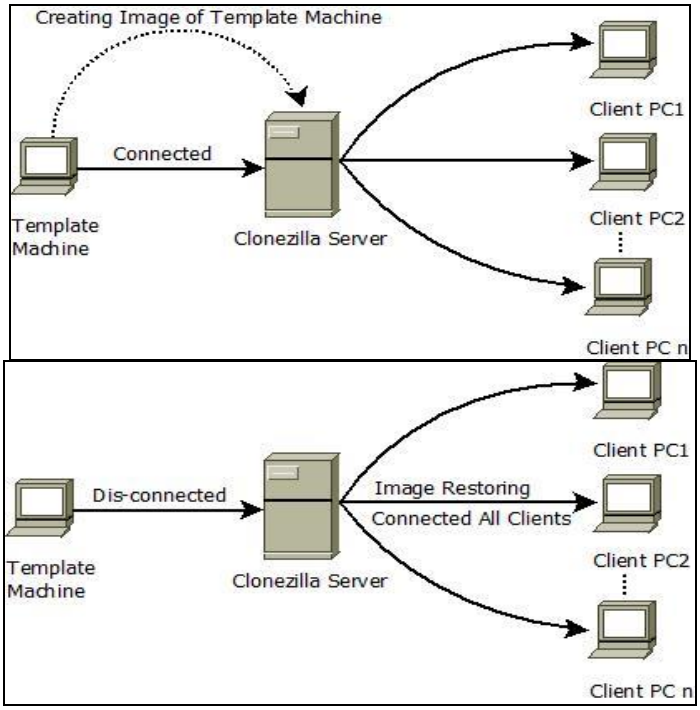


Fig. 38. Dreapta: Imaginea de referință este creată și apoi salvată pe Clonezilla Serverș Stânga: Imaginea de referință este aplicată pe fiecare stație de lucru.
Configurație (de exemplu, adresa IP și numele de gazdă) transmisă fiecărui dispozitiv

Un obiectiv al testului a fost compararea timpului de boot pentru pornirea din rețea și pornirea (restaurarea) imaginii locale Clonezilla. Ambele opțiuni ar putea fi utilizate, dar există limitări clare pentru fiecare opțiune: pornirea din rețea are un blocaj în performanța rețelei, în timp ce restaurarea imaginii Clonezilla utilizează resursele locale de hard disk.

Pentru prima pornire a unei aplicații, bibliotecile partajate sunt încărcate din sistemul de fișiere de rețea, în timp ce la a doua pornire a aplicațiilor; acestea sunt deja încărcate în memorie sau în memoria cache a sistemului de fișiere.

Acesta este motivul pentru care, pentru testare, am inclus ambele opțiuni.

Rezultatele comparative ale testelor sunt prezentate mai jos:

Mode	*Client PC*	*Boot time*	*Start LibreOffice Writer*	*Second Start LibreOffice Writer*	*Start Firefox*	*Firefox Second start*
PXE boot	P4 3,4Ghz 2G	1m 2s	1m 34s	5s	15s	7s
	P4 3,0Ghz 512M	1m 25s	`=- no swap avail.			
	P4 3,0Ghz 512M	2m 5s	5m 54s	3m 15s		
Clonezilla backup	P4 3,0Ghz 512M	8m 30s				
Clonezilla restore	P4 3,4Ghz 2G	6m 51s				
HDD boot	P4 3,0Ghz 512M	59s	1m 13s	16s	52s	24s

Fig. 39. Comparație între metodele de boot-are din rețea

Alte implementări prezentate în [14], [15], [16] abordează interoperabilitatea dispozitivelor IoT, o provocare din cauza protocoalelor de comunicare diferite și a formatelor de reprezentare a datelor. În loc să funcționeze independent, aceste dispozitive individuale ar colabora și ar face schimb de informații structurate în locul datelor brute. În acest context, am introdus un pas intermediar ne-costisitor spre îmbunătățirea interoperabilității rețelelor ”plasă” (”mesh”) de senzori eterogeni într-un laborator de instrumentație universitar, prin utilizarea datelor *adnotate semantic.* Fiind integrată cu soluții moderne de eLearning în inginerie - cum ar fi "instrumentația ca serviciu" și "experimentul ca serviciu" - această abordare *vizează integrarea ontologică* într-un Cloud potențat de capacități avansate de descoperire, interpretare, agregare și gestionare a rețelelor instrumentale eterogene.

Pentru soluția educațională IoT – demonstratorul agregării semantice a datelor produse de sub-”plasele” de senzori eterogene din laboratorul de instrumentație – am folosit protocoalele de bază MQTT (Message Queue Telemetry Transport) și CoAP (Constrained Application Protocol). MQTT este un protocol de comunicare dezvoltat de IBM pentru mesageria între mai multe noduri printr-un broker central, iar CoAP este un protocol dezvoltat de Cisco folosind principiile REST (REpresentational State Transfer) pentru a transfera informații între un singur client și un server; clienții folosiți au fost *mosquitto-cli* (mosquitto_sub și mosquitto_pub) și respectiv *coap-cli*.

Integrarea nodurilor senzorilor eterogeni folosind aceste protocoale de comunicare diferite a fost realizată folosind un gateway multi-protocol implementat în cadrul Eclipse Ponte (cu module JavaScript scrise pentru platforma node.js). Un strat de "persistență" stochează (într-un Mongo DB non-relațional) datele de mesagerie, în conformitate cu specificațiile QoS (Calitatea serviciilor) ale fiecăruia dintre protocoale. Gateway-ul permite transformarea protocolului și medierea semantică a datelor schimbate între nodurile senzorilor demonstratorului. Interfața REST de servicii web implementată poate fi utilizată de un instrument de monitorizare web pentru a oferi vizualizarea în timp real a datelor din rețeaua de senzori – ca date brute, ca diagrame sau hărți de distribuție.

Prin agregarea informațiilor topologice ale rețelei de senzori cu datele senzorilor, pot fi construite hărți precise de vizualizare a datelor, pentru a ilustra, de asemenea, fluxurile de informații și interacțiunile dintre nodurile IoT, oferind un sprijin educațional valoros – de exemplu, în studiul rețelelor inteligente care agregă infrastructura multi-furnizor.

Am realizat o extensie M2M (machine-to-machine) a popularei ontologii IoTDB, cu trimiteri la ontologia generică schema.org. Așa cum am menționat înainte de adnotarea contextului adaugă informații suplimentare (metadate) pentru sarcina utilă. Următorul exemplu ilustrează definiția contextului pentru senzorul de temperatură și umiditate DHT11.

```
{
  "@context": {
    "iot": "https://iotdb.org/pub/iot#",
    "iot-attribute": "https://iotdb.org/pub/iot-attribute#",
    "iot-js": "https://iotdb.org/pub/iot-js#"
```

```
  },
  "@id": "dht11",
  "@type": "sensor",
  "iot:attribute": [
    {
      "@id": "#humidity",
      "@type": "iot:Attribute",
      "iot-js:type": "iot-js:number",
      "iot:name": "humidity",
      "iot:purpose": "iot-attribute:sensor.humidity",
      "iot:role": "https://iotdb.org/pub/iot-attribute#role-reading",
      "iot:unit": "iot-unit:math.fraction.percent"
    },
    {
      "@id": "#temperature",
      "@type": "iot:Attribute",
      "iot-js:type": "iot-js:number",
      "iot:name": "temperature",
      "iot:purpose": "iot-attribute:sensor.temperature",
      "iot:role": "https://iotdb.org/pub/iot-attribute#role-reading",
      "iot:unit": "iot-unit:temperature.si.celsius"
    }
  ],
  "iot:name": "dht11"
}
```


O altă implementare descrisă în [17] prezintă posibilitatea de a emula diferite microcontrolere cunoscute pe aceeași placă de dezvoltare FPGA care va ajuta studenții să învețe diferite sisteme de bază de microprocesoare într-o abordare comparativă. Un dispozitiv FPGA poate fi utilizat pentru a emula diferite sisteme bazate pe diferite arhitecturi de microprocesoare cu scopul de a înțelege profund și de a învăța mai bine principalele discipline de inginerie electronică [18]. Mai mult decât atât, caracteristicile de programabilitate și reconfigurarea parțială încurajează utilizarea dispozitivelor FPGA în laboratoarele de predare.

- Emulația sistemului Arduino pe FPGA: studentul ar putea profita de bibliotecile Arduino pentru a implementa sisteme mai complexe; studenții se pot concentra pe aplicație și nu pe detaliile tehnice
- Emularea plăcii de microprocesor Z80: Z80 este un microprocesor simplu care ar putea fi folosit de studenți pentru a înțelege arhitectura generică a microprocesorului;
- Sistem pe cip (SoC) bazat pe Microblaze: studenții pot dezvolta proiecte complexe SW-HW folosind nuclee ip Xilinx disponibile; acestea ar trebui să pună în aplicare firmware-ul și software-ul de bază.

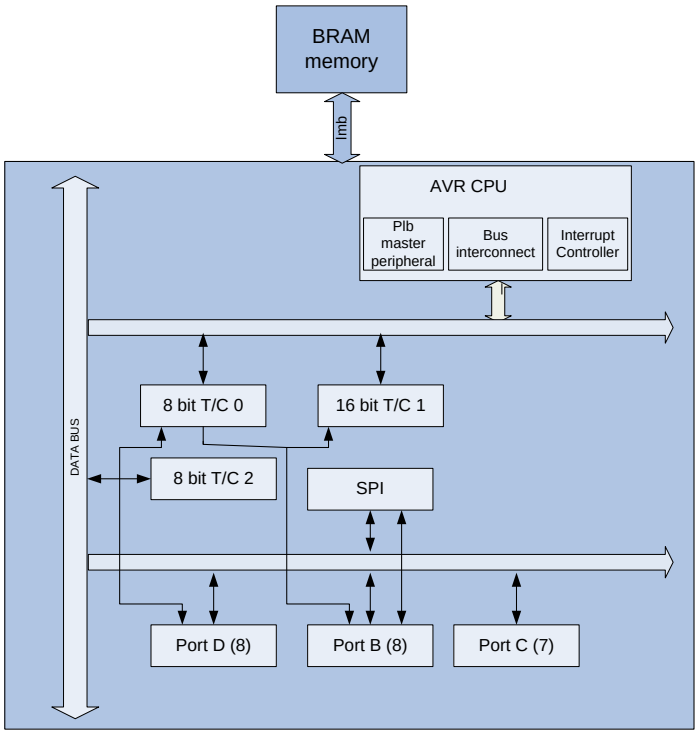


Fig. 40. Implementare RTL a sistemului Arduino

Pentru a emula sistemul Arduino ”Duemilanove” pe FPGA, următoarele nuclee IP au fost implementate în RTL: AVR Instruction Set Architecture, port bidirecțional, controler de întrerupere, cronometru pe 16 biți. Punerea în funcțiune este testată folosind setul de instrumente Arduino.

La rândul său, Xilinx Spartan 3E FPGA împreună cu Xilinx Design Suite 14.1 sunt utilizate în implementarea realizată. Xilinx Design Suite 14.1 (și orice altă versiune a Xilinx Design Suite) conține deja o bibliotecă cu nuclee IP (Nuclee de proprietate intelectuală) care pot fi utilizate pentru a realiza multe exemple practice, cum ar fi: microprocesor Microblaze, nuclee IP de interfață / bus / bridge, nuclee IP de comunicare, nuclee IP periferice sau controlere de memorie IPs.

1.1.5. Servicii de comunicații integrate la nivelul platformelor standard ATCA sau în Cloud

Integrarea sistemelor de calcul și telecomunicații a fost marcată de evoluția platformelor hardware de comunicații de la sisteme proprietare la:

- Elemente hardware standardizate pentru telecomunicații (un exemplu fiind platforma ATCA - Advanced Telecom and Computing Architecture), elemente foarte folosite cu precădere în cadrul sistemelor din rețeaua de bază LTE – asemenea echipamente există printre dotările de cercetare ale Universității Transilvania;
- Elemente generice COTS (Commercial off the Shelf) ce pot forma un Cloud privat (soluție ”on premise”). În acest sens voi prezenta succint o soluție de Cloud ”on-premise” cu 2 implementări, una Eucalyptus, una OpenStack, intrate în dotarea Universității Transilvania prin eforturile autorului și ale firmei Siemens.

În implementările din [4] și [5] se detaliază modul de integrarea hardware și software a procesării pachetelor pe o platformă ATCA (Advanced Telecom and Computing Architecture). Radisysy/Continuous Computing PP50 este folosit ca un sistem avansat cu arhitectură multi-procesor, bazat pe diverse soluții de firmware și management. Accentul se pune pe construirea

mediului de dezvoltare, configurarea software-ului și gestionarea aplicațiilor în mai multe cazuri de utilizare a sistemului de operare (Linux și RMI-OS).

Arhitecturile ATCA standardizate și flexibile sunt folosit pentru o mare diversitate de elemente din rețeaua de bază în telecomunicații, existând chiar și implementări de tip ”LTE-in-a-box” bazate pe ATCA.

Rack-ul ATCA pe care l-am folosit, fabricat de Radisys/Continuous Computing este de tip SH61 40G, având 6 sloturi pentru modulul fata (și 6 în spate, accesibile printr-un RTM - Module de tranziție spate). Există 3 surse de alimentare redundante. Re-configurabilitatea completă este asigurată, deoarece șasiul ce include o placa de management (shelf-manager) rămâne același și doar plăcile pot fi înlocuite și reconfigurate oricând este necesar pentru a îndeplini diverse cerințe aplicative.

Fig. 41 Configurația experimentală – vedere frontală a platformei ATCA 40G instalate

Platforma ATCA 40G are două plăci (blades) PP50 (vezi Figura 42), fiecare cu două procesoare de pachete RMI-Netlogic-Broadcom – tip XLR732 – care au o *arhitectură "super-scalară".*

Streamingul "fluxurilor de date" poate fi comutat fără a fi "despachetat" – un procesor de pachete poate *inspecta* în timp real milioane de fire de streaming simultane (de exemplu în scenarii de securitate). DPI (Deep Packet Inspection) permite identificarea aplicațiilor, *discriminarea* fluxului și *controlul traficului.* De exemplu, fluxurile selectate sunt reproduse pentru o analiză specială și o sinteză imediată a feedback-ului adecvat (de exemplu, intruziune simulată bazată pe teoria jocurilor).

Pentru această performanță remarcabilă, procesoarele de pachete sunt structurate ca *Intelligent Fabric for Automata (IFA)* grupând sute de mii de mici automata echivalente pentru procesarea elementară. Această organizație specială permite calculul predictiv pe baza regulilor sintactice PCRE ale Xpresiunilor Regular E *("regex")* care sunt compatibile cu PERL (Practical Extraction and Reporting Language).

Pentru a detecta *"amprenta digitală"* caracteristică anumitor clase de flux, aceste calcule au loc în mai multe *"mașini virtuale"* care rulează funcțiile generice de fragmentare, direcționare, încapsulare, criptare (și așa mai departe) a limbajului de procesare a pachetelor (PPL). Instrucțiunile PPL sunt grupate în *"reguli"* pentru tratamentul evenimentelor (întreruperea servirii), reguli care sunt grupate în *"politici"* care sunt adaptate dinamic (pentru programarea firelor).

Figura 42 prezintă arhitectura modulelor PP50. Complexitatea lor necesită un procesor de gestionare a lamelor - de tip EZ405 (cu IBM Power PC Architecture), prezentat ca un "IPMC" (IP-Management Controller) împreună cu firmware-ul său (FW) și FPGA auxiliar. Procesorul de management rulează un sistem de operare Linux (Sistem de operare) wind river carrier-grade.

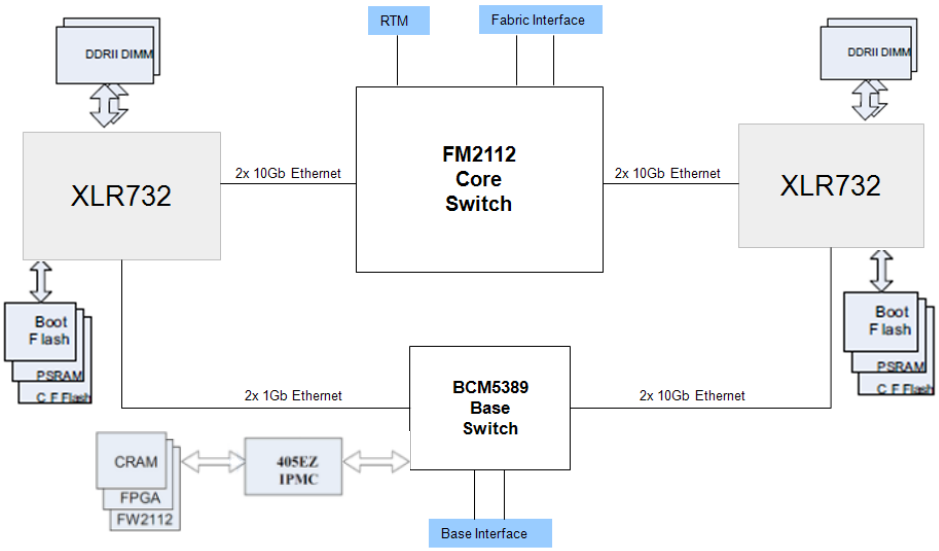


Fig. 42 Arhitectura hardware a modulelor PP50

Un comutator non-bloking de 10GbE ("Core Switch" FM2112) interconectează procesoarele de pachete, I/O și planul de spate (back-plane). Fiecare procesor XLR732 are două porturi de 10 GbE la acest comutator, permițând o capacitate duplex de 10 GbE. I/O extern este atât prin porturi redundante (1GbE standard PICMG 3.1.3 și 10GbE standard PICMG 3.1.9) la back-plane (RTM și Fabric Interface) și cu panoul frontal (prin intermediul direct 1GbE și 10GbE porturi). Aceste porturi sunt conectate la un "Base Switch" (BCM5389) guvernat de protocoalele IPv4/6 & IPsec, cu capacități pentru tunelare și GRE (Generic Routing Encapsulation). PP50 are Compact Flash SSD (fiecare corespunzând unui procesor XLR, așa cum se arată în figura 3). Aceste SSD stochează fișierele (kernel Linux, sistem de fișiere RMI-OS etc.) necesare pentru a porni XLR.

Sistemele de operare (OS) nu sunt recomandate pentru a rula per thread, astfel încât acestea să poată rula pe nuclee (core), de exemplu Linux pe nuclee N (N≥1) și RMI-OS pe nucleele 8-N ale unui XLR "bootloader" (a se vedea figura 43).

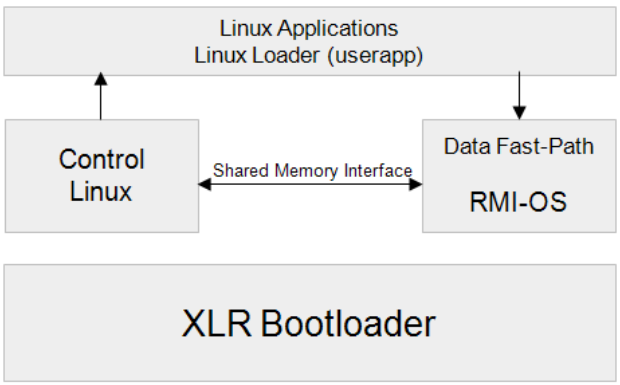


Fig. 43 Configurarea software a modulelor PP

Fiecare dintre procesoarele XLR poate fi pornit independent, prin Compact Flash (pe PP50) sau, în esență, prin rețea. Nucleele Linux pot avea sistemul de fișiere fie în RAM, fie într-un server NFS (Network File System)

În cazurile de utilizare din telecomunicații, Linux ar putea rula software de control (de exemplu, controlul apelurilor, alocarea lățimii de bandă, echilibrarea încărcării), în timp ce RMI-OS ar trebui să gestioneze analiza pachetelor și discriminarea/filtrarea lor (de exemplu, I/O de pachete prin interfețe "fast-path" de 10 Gb).

Nucleele 8-N RMI-OS pot comunica cu N nuclee Linux printr-o interfață de memorie partajată. Comanda Linux *userapp* încarcă, pornește, oprește și descarcă programele RMI-OS din linux (acesta este motivul pentru care cel puțin *core0,* nucleul 1st, ar trebui să ruleze Linux, N≥1).

Fișierele kernel, în formatul executabil și linkable (ELF) sunt încărcate în nucleul XLR (prin comanda *elfload*)

```
PP50-1 $ elfload
```

Se poate lansa apoi orice program specific cu comanda userapp menționată mai sus . De exemplu:

```
userapp xlr_loader xlr_hybrid = RMI_OS_APP_NAME linux_cpu_mask = 000000f kuseg_start_lo = 0x20000000 kuseg_size_lo =
0x20000000
```

De exemplu, pentru CCPU_A RMI_OS_APP_NAME **xlr_hybrid =ccpu_a**

Controlul suplimentar al RMI_OS_APP:

```
cd / rmios_apps
   /usr/local/sbin/userapp load -m 0xfffffff0 -f RMIOS_APP_NAME
   /usr/local/sbin/userapp stop -m 0xfffffff0
   /usr/local/sbin/userapp status
```

Un studiu de caz implementat este CCPU_A, controlul RMI-OS la Linux Network Traffic. În acest fel, se poate gestiona transferul de pachete de rețea de la aplicațiile RMI-OS la stiva de rețea Linux prin apeluri socket standard (trimise de orice aplicație aparținând așa-numitei Linux Userland - care grupează metodele de control ale sistemului de operare ce sunt diferite de cele destinate părții de kernel.

O altă implementare reprezintă schimbul reciproc de mesaje la nivel de cale de control (Control Plane) între RMI-OS și Linux Userland, folosind memoria partajată.

O aplicație RMI-OS poate declanșa o aplicație Linux prin scrierea unui mesaj în această zonă de memorie partajată "Shared Mem". Kernel-ul Linux pune acest mesaj la procesorul de mesaje (message-ring handler FMN) care ar trebui să-l transmite la cererea corespunzătoare Userland.

În acest scop, CCPU_A monitoriză Linux pe *core0 ... core(N-1) și* monitorizează RMI-OS pe *coreN... core7.* Porturile dedicate *GMAC0-3* sunt înregistrate și controlate de Linux (fiind disponibile pentru *nfsroot*). Porturile generice *XGMAC0* și *XMGAC1* sunt înregistrate în Linux, dar controlate de RMI-OS – aplicațiile sale ar trebui să comande **xlr_net_init()** pentru a inițializa cele două XGMAC (în rețeaua generică a XLR), asociindu-le logic cu descriptorii liberi.

Pentru implementarea aplicațiilor de procesare a pachetelor, am construit pe PC-ul auxiliar un mediu de dezvoltare sub CentOS Linux care rulează Netlogic-Broadcom SDK v.1.4 (Software Development Kit) pentru familia XLR și un lanț de instrumente cross-compile. În ceea ce privește funcționalitatea de încărcare a rețelei, serverul principal este instalat pe o placă XE80, dar un server secundar a fost de asemenea testat pe acest PC auxiliar.

Pentru cross-compilarea aplicațiilor de procesare de pachete în Linux pe mașina de dezvoltare, am adăugat următoarea linie în *makefile*:

```
CC =/opt/rmi/1.4/mipscross/crosstool/gcc-3.4.3-glibc-2.3.6/mipsisa32-xlr-linux/
```

bin /mipsisa32-xlr-linux-gcc trimite la compilatorul *gcc*.

Pe lângă platformele de telecomunicații standard precum ATCA, platformele de telecomunicații s-au orientat spre sisteme Cloud ce includ hardware generic.
Mai jos este un exemplu de infrastructură de Cloud din dotarea Departamentul de Electronică și Calculatoare, pe care am realizat-o împreună cu colegii și cu sprijinul firmei Siemens.

Prima topologie reprezintă configurație o de Cloud bazată pe implementarea Eucalyptus, implementare care în prezent nu mai este cu sursă deschisă. Se poate observa structura ierarhică cu controlere la diverse niveluri: Cloud Controller, Cluster Controller și Node controller.

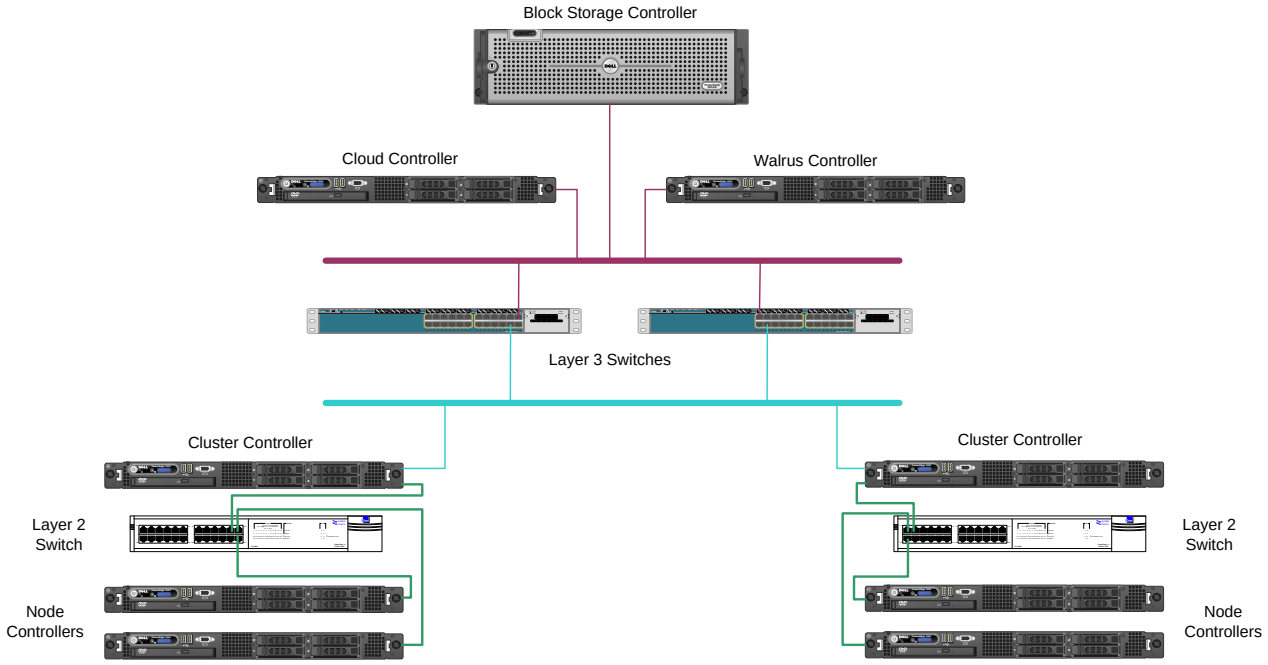


Fig. 44 Configuratie experimentală de laborator în Cloud pe bază de Eucalyptus în dotarea departamentului DEC

Datorită discontinuității proiectului cu sursa deschisă, configurația a fost modificată pe baza proiectului open-sourse openStack, de altfel implementarea de infrastructure-as-a-service cu sursă deschisă cea mai populară.

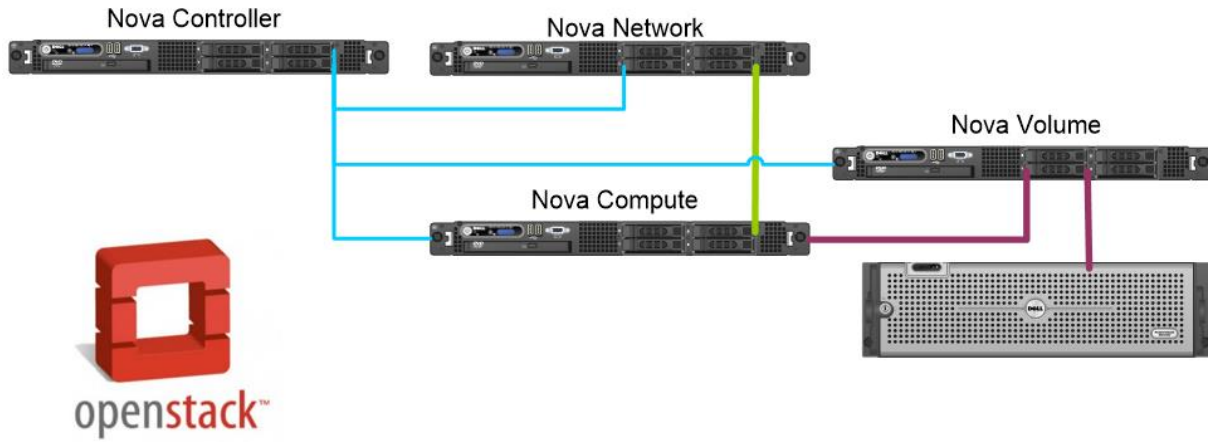


Fig. 45 Configuratie experimentală de laborator în Cloud pe bază de Openstack în dotarea departamentului DEC

Configurația openStack a reutilizat doar o parte dintre echipamentele existente, pentru a implementa componentele principale de procesare (Compute), rețea (Network) și stocare (Volume).
Echipamentele din această configurație s-au refolosit în diverse proiecte, unele realizate cu studenți sau cu rol didactic. De exemplu serverele au fost folosite ca suport de virtualizare pentru de testare virtualizate Ixia.

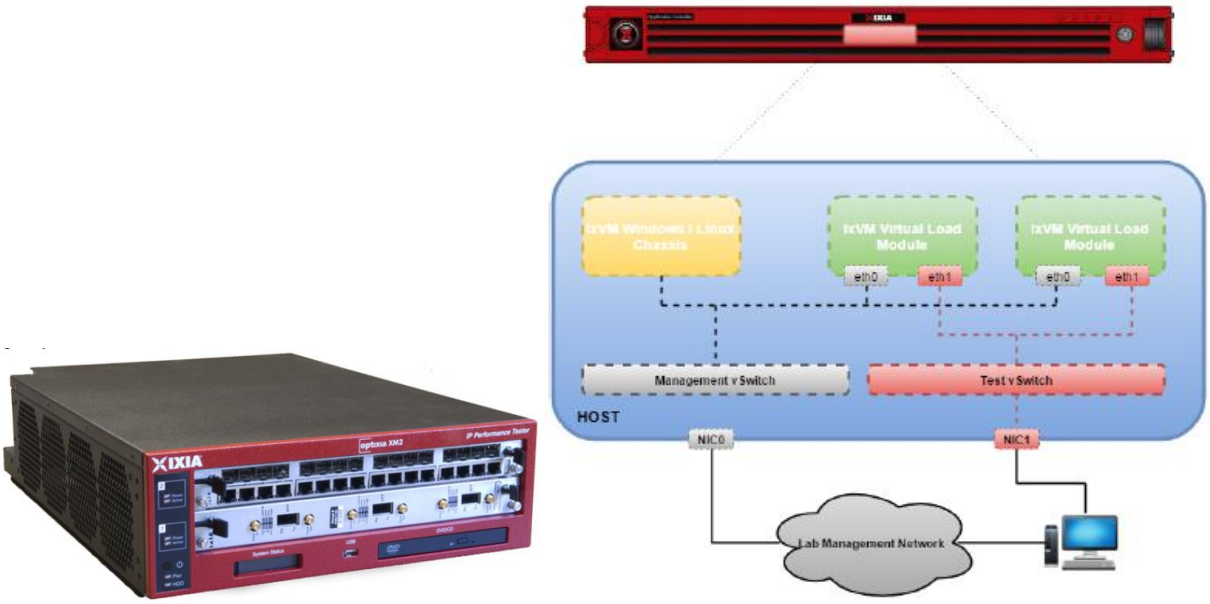


Fig. 46 Configurație experimentală de laborator Ixia

Pe lângă echipamentul Ixia XM2 existent fizic în dotarea departamentului, datorită relației de parteneriat construită cu Ixia am beneficiat și de unele resurse virtualizate.

Astfel, în configurație virtualizată pe serverul Dell au rulat virtualizat elemente Ixia pentru testarea metodelor de inginerie a traficului (traffic engineering) în rețele MPLS și tunelare IPSec, rețeaua de test fiind emulată în GNS3.

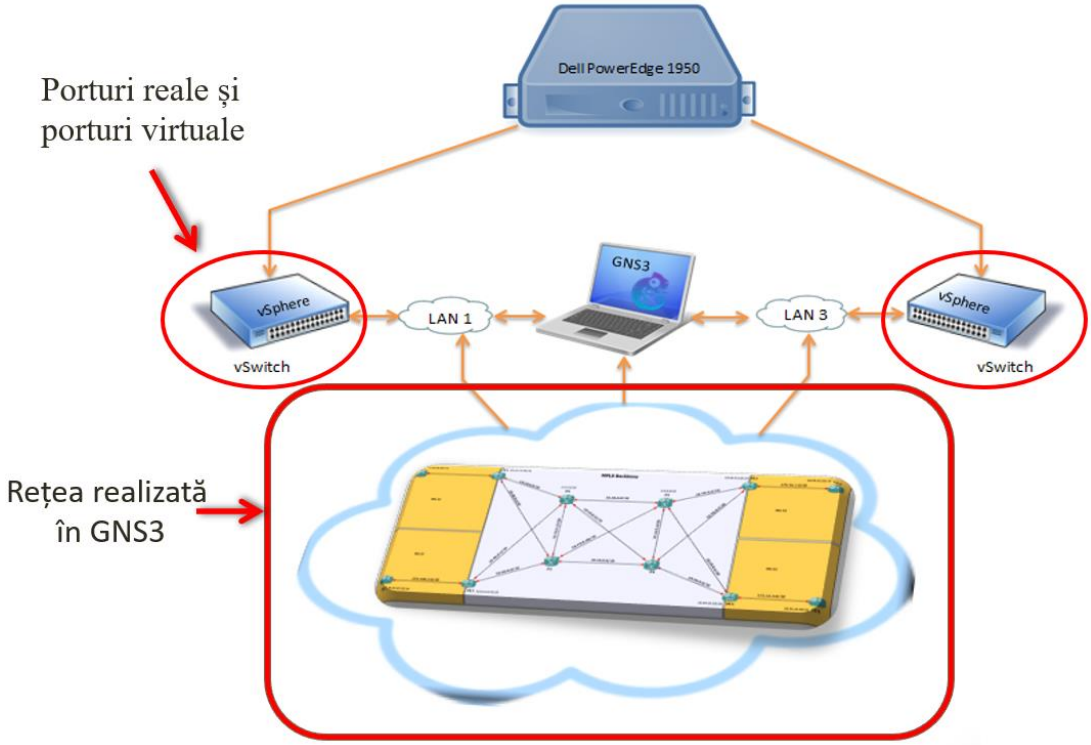


Fig. 47 Implementare virtualizată de rețele MPLS testată cu elemente software Ixia ce rulează virtualizat pe un server Dell

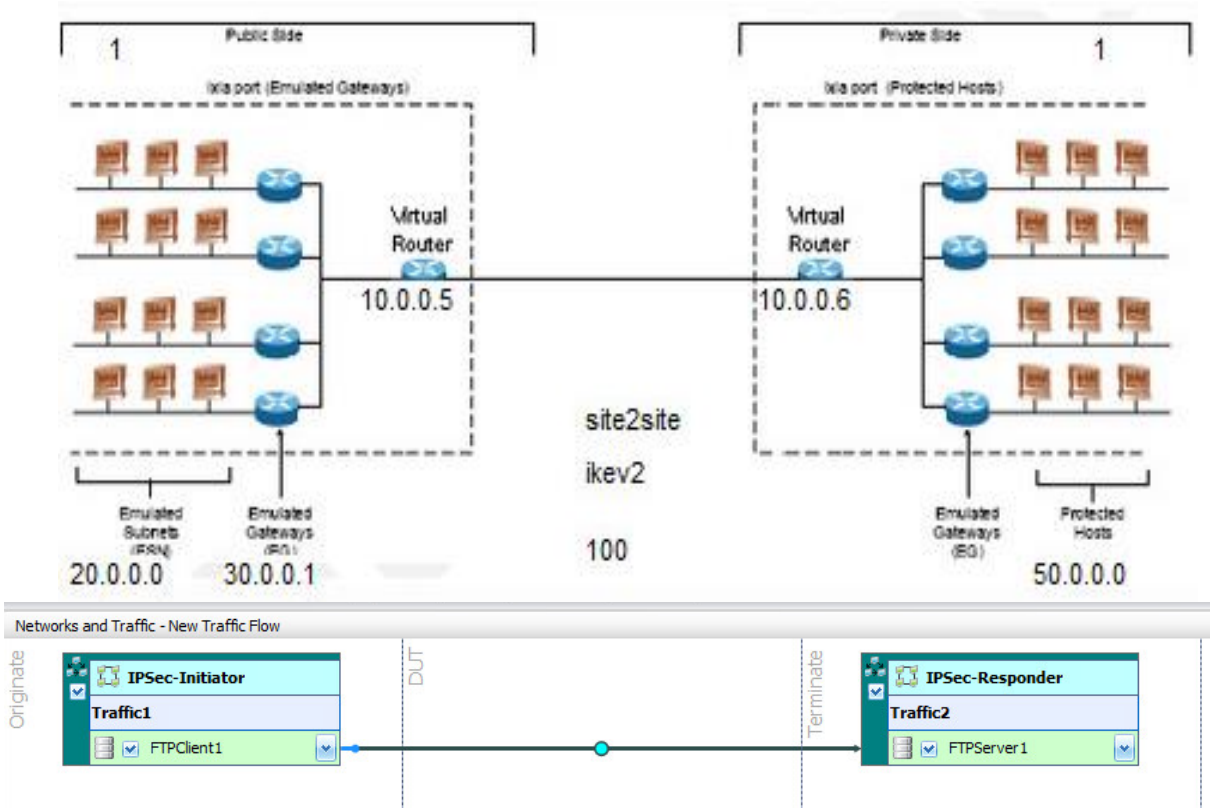


Fig. 48 Testare/emulare IpSec pe bază de software Ixia

1.2. Integrarea sistemelor de calculatoare și comunicații în rețeaua de acces

1.2.1. Radio definit software – Software Defined Radio (SDR)

1.2.1.1. Prototiparea sistemelor SDR pentru comunicații dispozitiv-la-dispozitiv (device-to-device, D2D)

Comunicarea device-to-device (D2D) reprezintă o tehnologie promițătoare pentru a permite dispozitivelor să comunice direct fără interacțiunea punctelor de acces sau a stațiilor de bază. Natura ad-hoc și de proximitate a acestei comunicări introduce unele vulnerabilități de securitate foarte importante. Gestionarea cheilor, controlul accesului, confidențialitatea, rutarea și transmiterea securizată necesită proceduri de semnalizare dedicate și mecanisme de implementare optimizate, adecvate pentru mediul mobil, cu consum redus de energie și cu putere de procesare redusă.

Una dintre implementările realizate și detaliată în [20] propune un mecanism de securitate pentru comunicarea D2D care implică utilizarea funcțiilor fizice neclonabile (PUF) pentru generarea de chei unice, Elliptic-Cryptography (ECC) și Diffie-Hellman Key Exchange (DHKE) - pentru gestionarea cheilor - și Salsa20/20 ca metodă de criptare a cifrului fluxului (stream cypher), potrivită

pentru confidențialitatea transmisiilor fără fir. Toate aceste metode au fost implementate și testate pe o platformă de comunicare Software Defined Radio (SDR) formată dintr-un sistem bazat pe cip (SoC) bazat pe Zync, completat de plăci dedicate anexate (daughter-boards) pentru comunicații pe frecvență radio (RF) de la Analog Devices - o integrare folosind co-design hardware și software.

Mai multe probleme de securitate sunt necesare a fi luate în considerare pentru un mecanism de securitate D2D, cum ar fi confidențialitatea, integritatea și autentificarea. Sistemul de securitate propus oferă soluții pentru următoarele probleme:

- managementul cheilor folosind RO-PUF pentru generarea unica de chei secrete, Elliptic Cryptography pentru generarea cheii publice corespunzătoare cheii secrete, Diffie Hellmann pentru generarea cheii secrete comune și a schimbului de chei;
- criptarea datelor folosind metoda de cifru a fluxului bazată pe algoritmul Salsa20-20, potrivită pentru criptarea comunicațiilor în timp real;

Toate aceste implementări sunt efectuate pe o platformă de comunicare Software Defined Radio (SDR) constând dintr-un sistem bazat pe cip (SoC) bazat pe Zync pe un Digilent "ZedBoard" completat de plăci-fiice de frecvență radio (RF) de la Analog Devices (FMCOMMS3 și FMCOMMS4), o soluție de integrare folosind co-design hardware și software. Platforma SDR reprezintă un sistem excelent de prototipare, permițând posibilitatea de a implementa în hardware algoritmii de securitate complecși. Acesta oferă flexibilitatea de a aplica modulele proiectate (proprietate intelectuală - nuclee IP) în diferite soluții de comunicații radio, de la WiFi la LTE - fie o abordare personalizată, fie una care include sub-sisteme dovedite în industrie bazate pe MATLAB, Xilinx Vivado sau GNU-Radio.

Algoritmii utilizați pentru securitatea D2D sunt prezentați în figura de mai jos:

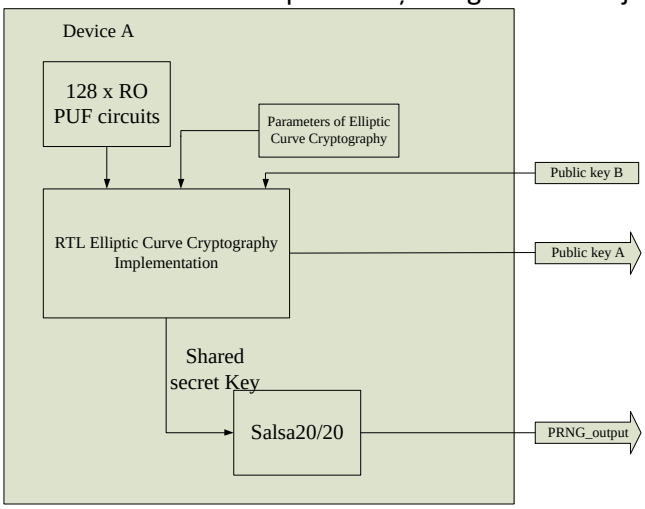


Fig. 49 Testare/Mecanismul de securitate implementat pentru dispozitivele implicate în comunicarea D2D

RO PUF (Ring Oscillator Physical Unclonable Functions) implementat pe Zynq sunt folosite pentru a genera o cheie secretă pentru un dispozitiv implicat în comunicațiile D2D. Fiecare dispozitiv implicat în comunicare primește o cheie secretă generată cu circuitele RO PUF. Operațiunile de criptografie curbă eliptică sunt utilizate pentru generarea unei chei publice corespunzătoare cheii secrete generate cu RO PUF. Următorul pas este de a genera o cheie secretă partajată pentru fiecare dispozitiv folosind:

1. cheia secretă generată cu RO PUF;
2. operațiunile criptografice ale ECC și
3. cheia publică a altor dispozitive implicate în comunicarea D2D.

Folosind algoritmul Diffie-Hellman se stabilește o cheie secretă comună pe un canal nesigur. Cheia secretă comună este folosită ca ”seed” (”sământă”) pentru generatorul de secvențe pseudo-aleatoare Salsa20/20 pentru a obține un flux de chei secrete utilizabile într-o criptare simetrică.

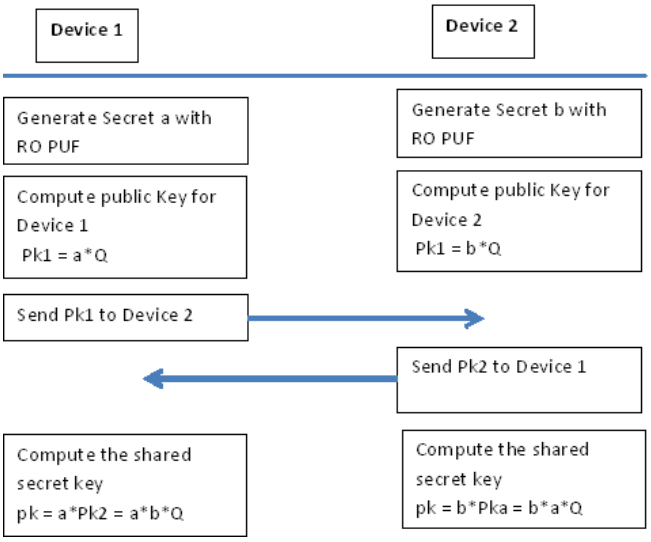


Fig. 50 Protocolul Diffie Hellman bazat pe eliptic curba criptografie

Zynq-7000 SoC (System on Chip) oferă posibilitatea de a combina programabilitatea software a unui procesor bazat pe ARM cu reconfigurabilitatea hardware a unui FPGA, permițând accelerarea hardware-ului în timp ce integrează funcționalitatea CPU, DSP și semnal mixt pe un singur dispozitiv. Caracteristicile enumerate mai sus fac din Zynq7000 o platformă bună pentru implementările SDR ale unei game largi de aplicații transceiver pentru comunicații fără fir. L-am selectat ca fiind foarte potrivit pentru experimentarea comunicării device-to-device și integrarea cu funcțiile complexe de securitate implementate. Pentru demonstrator am folosit o configurație back-to-back (Figura 51) cu interfețe radio cuplate direct, fără limitări și interferențe cu spectrul public.

Fig. 51 Prototip experimental– Back-to-back
"Zedboards" cu plăcile adiționale radio anexate FMCOMMSx AD

Pentru a configura mediul de lucru SDR am folosit co-procesorul Linux ARM și implementarea SoC folosind software-ul Xilinx Vivado la nivelul FPGA, conectat cu placa Analog Devices AD-FMCOMMS3-EBZ ca interfață radio. Sub-sistemul de comunicare a fost implementat folosind AD IP Core pentru comunicații fără fir. Aceeași platformă a fost folosită și pentru alte cercetări, cum ar fi procesarea de imagini transmise prin protocolul WLAN 802.11a descrisă în lucrarea [21].

Dezvoltarea pentru combinarea modulelor de comunicare cu modulele noastre de securitate implementate poate fi realizată în diferite moduri:

- Implementarea software-ului - care rulează pe implementarea ARM core Linux furnizată de dispozitive analogice - care instanțiază, de asemenea, comunicarea cu AD Communication IP Core. Pe lângă acest sistem de operare, pot fi utilizate și alte pachete software de comunicare (de exemplu, cele de la open source GNU Radio).
- Co-proiectare software și hardware folosind MATLAB - în special modulul de comunicare MATLAB și modulele de comunicare LTE Advanced D2D
- Personalizare folosind AD IP Core prin Xilinx Vivado și rulând codul C ”peste” acest IP Core

Generarea de chei secrete de 128 de biți cu circuite RO PUF este prezentată în Figura 10. Rezultatele sunt vizualizate cu Analizorul logic ChipScope furnizat de Xilinx Vivado. În primul rând, sunt generate 64 de biți reprezentând BLS-urile cheii secrete și cealaltă jumătate a acesteia prin schimbarea oscilatoarelor inelare compuse din 5 invertoare conectate într-o buclă.

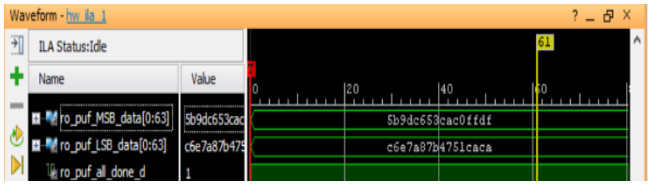


Fig. 52 Rezultatele circuitelor RO PUF implementate pe Zynq

1.2.1.2. Sistem de comunicatii SDN D2D utilizand elemente SDR-RTL ca senzori de spectru

O altă implementare bazată pe tehnologii SDR [22] propune unele modele pentru optimizarea comunicării Device-to-Device (D2D) în contextul mediilor de comunicații aglomerate, prin utilizarea detecției spectrale. Diferite niveluri de descentralizare – în inteligența computațională, procesarea semnalelor, managementul puterii și un procent mai mare de software open-source – au fost abordate într-o perspectivă ”business-oriented” (”orientată comercial”). O rețea de dispozitive SDR de mică putere și ieftine a fost implementată în soluții pentru descoperirii partenerilor și selectarea spectrului ca parte a comunicării D2D în medii urbane congestionate radio. Aceste soluții practice acoperă nu numai receptoarele DST eficiente din punct de vedere al costurilor, ci și inteligența locală, cu un adaos spectaculos: mobilitatea.

În această lucrare am propus o combinație a celor două abordări bazate pe elementele senzorilor de detectare a spectrului distribuit, corelate cu serviciile de localizare și GDB-s (Geo-location Data Base):

- Detectarea spectrului, cunoscută și sub numele de Detecție Energetică (ED) determină starea utilizatorilor primari prin compararea unui prag predefinit cu ieșirea detectorului energetic.
- Baza de date de geo-localizare (GDB) se bazează pe rafinarea și interpretarea informațiilor din așa-numitele hărți de mediu radio (REMs - Radio Environment Maps), pe politicile de spectru și parametrii rețelelor / dispozitivelor de utilizator etc. Abordările GDB existente - și aici putem menționa implementarea bazei de date a spectrului Google - vizează în principal autorizarea dispozitivelor TVWS (TV White Space) să funcționeze cu parametri specificați.

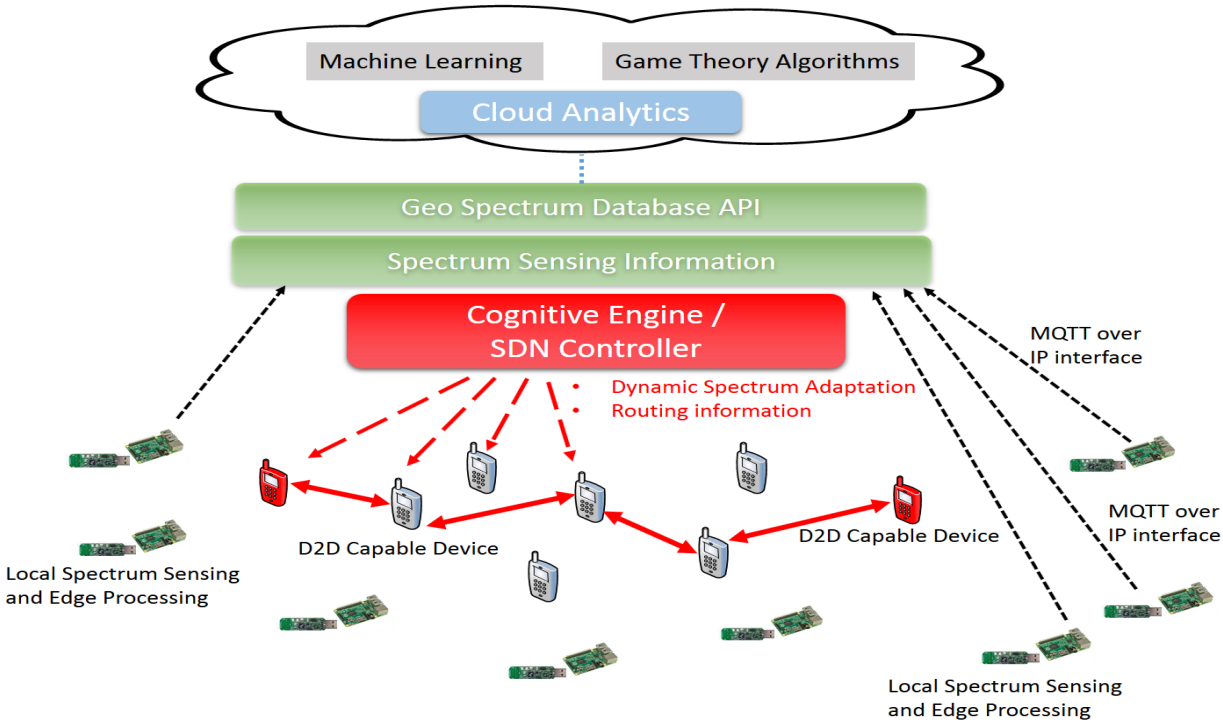
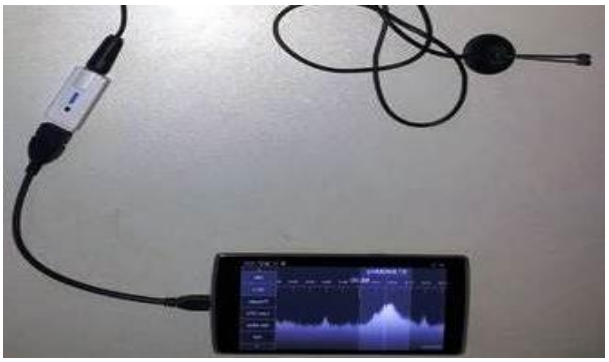


Fig. 53 Arhitectura comunicațiilor SDN D2D utilizând elemente SDR-RTL ca senzori de spectru local

Pentru informațiile privind datele spectrului, există două abordări pe care le voi detalia în continuare:

- Edge (local) SDR "spectrum sensing", cu ajutorul unor entități software precum GNU Radio și apoi utilizând metode IoT (de exemplu, protocolul MQTT) pentru a transmite printr-o interfață IP (un modem 3G, o conexiune WiFi, o conexiune prin cablu), către controlerul SDN, numai rezultatele procesării locale
- Captarea și transmiterea informațiilor spectrului prin TCP către procesarea Cloud - aici se poate face o prelucrare ulterioară, ca în cazul demonstratorului LabVIEW care va fi prezentat în cele ce urmează
- Elementele de detectare sunt noduri SDR ieftine cu calculatoare single board (SBC), dar pot fi și smartphones cu dongle SDR atașate, cum ar fi cel prezentat în figura 54. O a treia opțiune ar fi utilizarea unor elemente dedicate care au performanțe mult mai bune de detectare a spectrului, cum ar fi în cazul unei USRP (de exemplu, ETTUS – National Instruments).



- *Fig. 54 Inteligenta computațională @ Nivel smartphone/Receptor SDR RTL2832U*

- O modalitate simplă de vizualizare a spectrului este aplicația Android SDRTouch ; interfața acestei aplicații e prezentată în fig. 55:

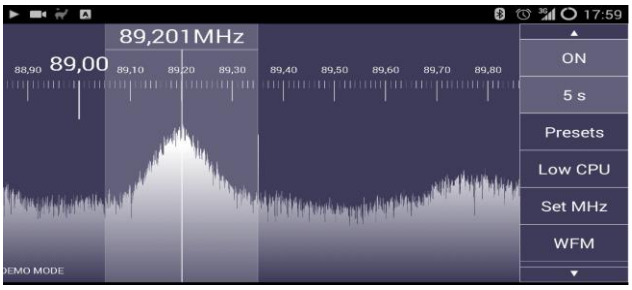


Fig. 55 Exemplu de spectru detectat - cu aplicația SDRtouch

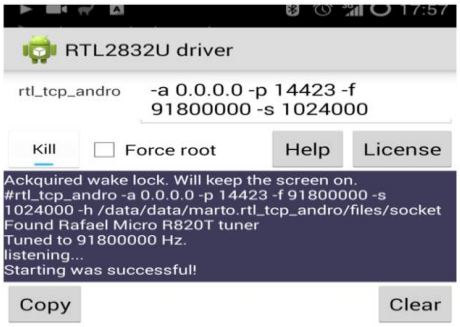


Fig. 56 Utilitar RTL-TCP pentru RTL2832U utilizat pentru transmiterea probelor IQ

Când se dorește să pornim detecția în modul manual, lansăm aplicația RTL-SDR în modul avansat ca în fig. 56

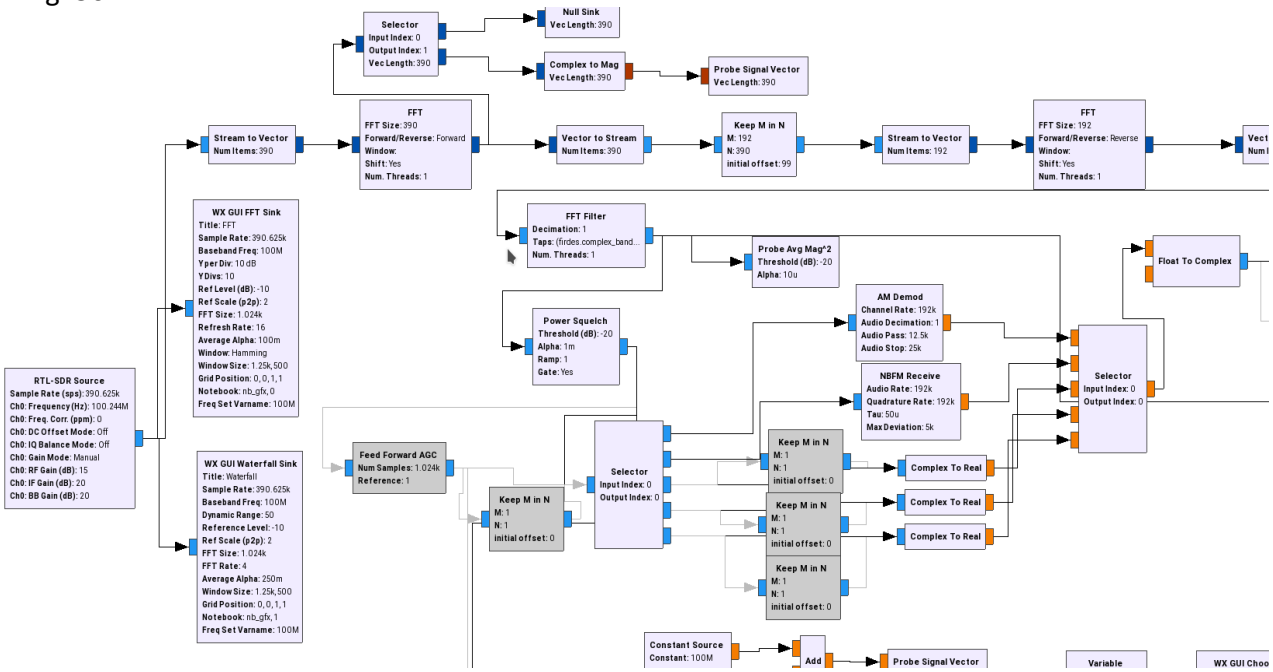


Fig. 57 Implementare modificata pe SCANOO - RADIO GNU pentru a suporta RTL-SDR, cu diferite modulații

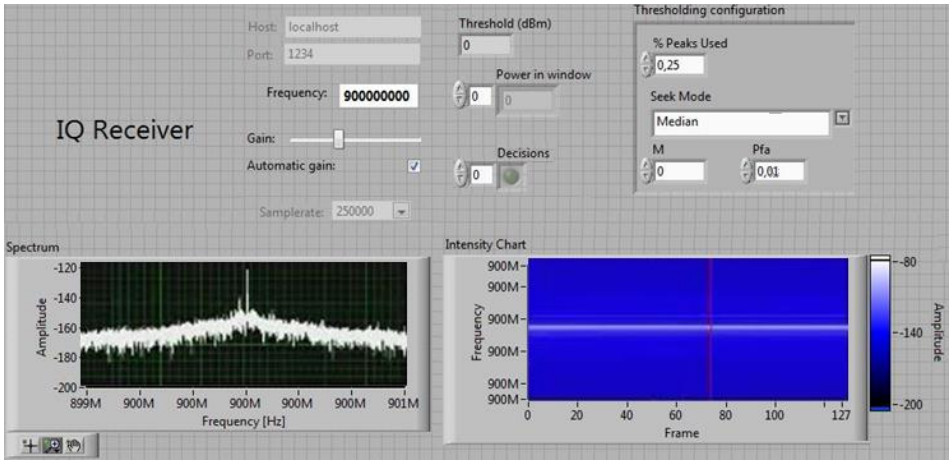
1.2.1.3. Integrarea LabVIEW a receptoarelor radio RTL2832 SDR

Mediul de informatică instrumentală pe care l-am folosit, LabVIEW, a fost modernizat pentru utilizarea viitoare în Cloud – pe cât posibil, conexiunile se fac în același mod, și local și la distanță. Astfel, spre controlabilitatea *unificată* all-IP, interfațarea este controlată ca TCP (chiar dacă este USB la niveluri inferioare, ca în cazul RTL-SDR)! Majoritatea transferurilor de date sunt generice HTTP GET/POST (portul 80 fiind întotdeauna deschis, în comparație cu porturile dedicate pentru soluții speciale).

În diagrama VI din Fig.58, LabVIEW conduce "dongle"-ul RTL-SDR printr-o conexiune TCP. Aceasta se referă la o reducere importantă a costurilor (în comparație cu soluția LabVIEW & USRP), cu avantajul de a menține același nivel de controlabilitate (cu instrumentație virtuală - VI, în acest caz).

Parametrii RTL-SDR sunt preluați de o conexiune de rețea prin serverul încorporat RTL_TCP, prin intermediul gazdei și al portului de interconectare. Acești parametri (câștig, frecvență centrală, rată de eșantionare etc.) sunt destinați pentru a controla recepția semnalului (la intrarea blocului NI-USRP-Rx). Acest control se face în domeniul timpul, dar, deoarece investigarea canalelor disponibile ar trebui să se facă în domeniul frecvență, se efectuează un calcul FFT, furnizând spectrul de semnal.

Media celor mai mici 10 vârfuri spectrale se face pentru a calcula Pragul, apoi, folosind această valoare limită a canalului, EnergyDetect.vi sub-VI este utilizată pentru a măsura puterea în canal. CDB-WDT (tipuri complexe de date cu formă de undă dublă precizie) permit un domeniu de înaltă vizualizare mixtă timp/frecvență în panoul de instrumente virtual.
Recent, National Instruments a răspuns cerințelor "clienților subțiri" (”Thin Clients”) și ale mobilității cu soluții precum "Tabloul de bord al datelor" (”Data Dashboard”).



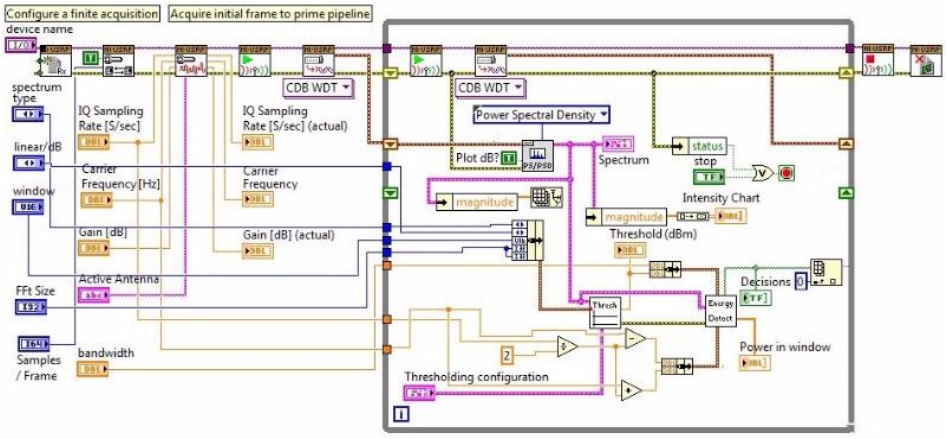


Fig. 58 *Integrarea LabVIEW a receptorului RTL2832U SDR prin TCP*

1.2.2. Evaluarea puterii radiate în câmpul apropiat al unui terminal mobil care funcționează în standardele de comunicare 3G+ și 4G+

În cadrul colaborării cu colegii de la Academia Forțelor Terestre din Sibiu, am propus și evaluat o metodă originală de evaluare a densității de putere radiată a câmpului apropiat în imediat se propune vecinătatea terminalelor mobile care utilizează atât determinarea rezistențelor câmpului electric, cât și a câmpului magnetic [23]. Funcția de distribuție cumulativă complementară (CCDF) este utilizată pentru prima dată pentru a evalua expunerea. O demonstrație a capacităților CCDF pentru a oferi o reprezentare realistă a fost efectuată într-o campanie de măsurare pe un terminal mobil. Evaluarea expunerii a fost efectuată pentru situațiile de operare din viața reală prin selectarea a șapte servicii comune de aplicații utilizate de abonații mobili. Pentru tehnologiile de comunicare 4G+, densitatea de putere în câmp apropiat este cea mai mare în timpul încărcării fișierelor, urmată de VoIP, apel video, descărcare de fișiere, servicii de streaming și navigare. Pentru rețelele 3G+, valorile densității de putere mai mari până la mai mici au fost asociate cu: încărcarea fișierelor, fișierul servicii de descărcare, streaming, VoIP, apeluri video și navigare. În câmpul total apropiat radiat, densitatea de putere s-a dovedit a fi, în medie, de 34 de ori mai mare pentru aplicațiile testate care rulează în 4G+ în comparație cu 3G+, cu valori variind de la 180 de ori - în timpul încărcării fișierelor, până la 1,2 ori - în timpul videoclipului Streaming. Densități de putere radiate semnificativ mai mari au fost emise în timpul utilizării VoIP și apel video pe rețeaua 4G+ în comparație cu rețeaua 3G+. Rezultatele prezente sugerează cu tărie că expunerea mai mare este așteptată pentru aceeași aplicație care rulează sub 4G+ mai degrabă decât sub 3G+. Prin aplicarea unei proceduri originale, s-a subliniat experimental faptul că diferite generații de tehnologii de comunicare vor duce la diferite forme de expunere în amplitudine și în timp, sugerând o nevoie viitoare de introducere a cuantificării ratei dozelor.

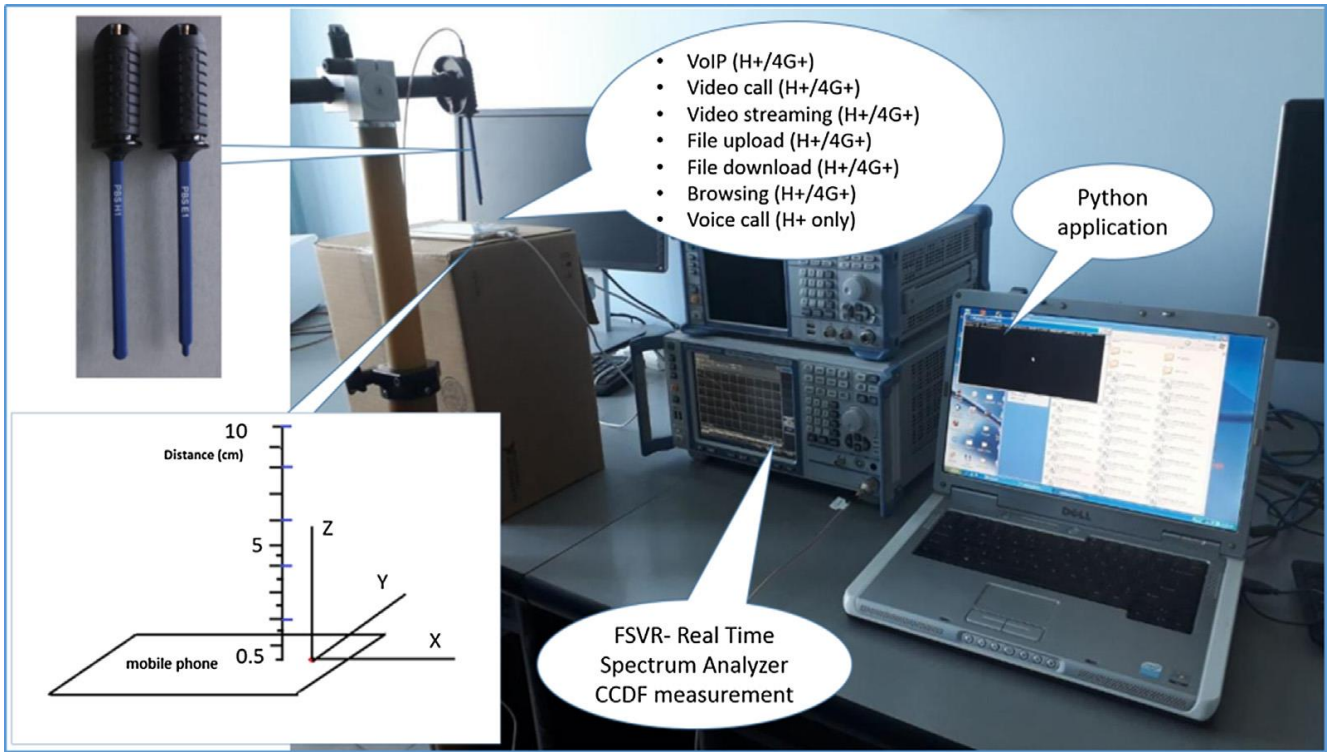


Fig. 59. Stand experimental pentru măsurarea nivelurilor din apropierea câmpului în proximitatea terminalului mobil.

Puterea radiată în câmp apropiat a fost măsurată pentru un model de telefon Huawei P10 Lite WAS-LX1 (care va fi menționat în continuare ca UE) operat în rețeaua comercială Vodafone Ro. Câmpul apropiat a fost măsurat în modurile de rețea 3G+ (H+) și 4G+ (LTE-A) în timp ce rulează următoarele aplicații mobile: VoIP, Apel video, Streaming, Navigare, Descărcare fișiere, Încărcare fișiere și apel vocal (numai în H+). Aplicația WhatsApp a fost utilizată pentru apeluri voIP și apeluri video, în timp ce site-ul de partajare video YouTube a fost folosit pentru streaming (au fost luate în considerare atât calitățile 480p, cât și cele 1080p).

Pentru a nu interfera cu UE în timp ce a avut loc un set de măsurători, am folosit aplicația nPerf Android pentru a testa viteza de descărcare și, respectiv, de încărcare. Aplicația nPerf a fost, de asemenea, utilizată pentru a efectua măsurători de navigare. Toate măsurătorile au fost efectuate în interior, păstrând în același timp bateria complet încărcată. Telefonul mobil împreună cu obiectele din jur au fost plasate într-o poziție fixă. Antena radiantă este situată pe partea inferioară a dispozitivului. Setările rețelei mobile au permis trecerea între modurile de rețea 2G, 3G și 4G. UE funcționează conform standardului HSPA+ atunci când se află în modul de rețea 3G. Frecvențele centrale uplink (UL) au fost de 1967,2 MHz și 1977,2 MHz, corespunzând numărului absolut de radiofrecvență UMTS (UARFCN) 9836 respectiv 9886. În modul de rețea 4G, UE utilizează tehnologia LTE-A cu stația de bază alocată canalului UL centrat pe 1720 MHz, corespunzând la 19.300 EUTRA EARFCN, având o lățime de bandă de 20 MHz. Cu toate acestea, nu a fost observată nicio declanșare CA pentru UL la locul de măsurare pentru tipurile de aplicații testate (estimăm că UE funcționa în condiții radio bune și că a existat o sarcină scăzută a celulei). Cu ajutorul unei aplicații mobile instalate pe terminal, atât indicatorul de rezistență a semnalului primit (_80 dBm), cât și puterea de recepție a semnalului de referință (_82 dBm) au fost măsurate în locația experimentelor.

Graficele din Fig. 60 sunt rezultatul reprezentării puterii medii pe toate cele 1000 de valori înregistrate în fiecare punct și poziție. Raportarea abaterii standard pe câmpurile totale nu este o măsură adecvată, deoarece componentele câmpului E și H au fost măsurate în momente diferite în timp. Cu toate acestea, valorile măsurate pot fi analizate pentru o singură componentă de direcție, așa cum este prezentat în figura de mai jos. Valorile Ey și Hx sunt mai răspândite în jurul mediei la distanțe mai apropiate de UE, în regiunea câmpului reactiv.

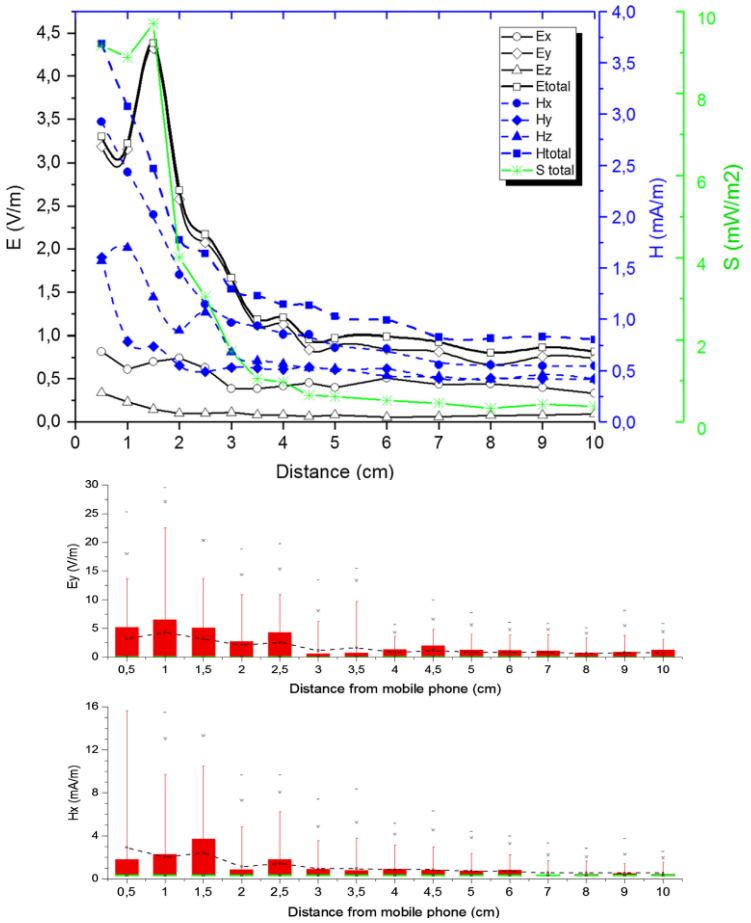


Fig. 60. Variația punctelor forte ale câmpului (E, H) și densitatea puterii cu distanța: aplicația VoIP/4G+. Variația cu distanța și răspândirea în timp a principalelor componente de câmp, Ey și Hx: utilizarea aplicației VoIP/4G+.

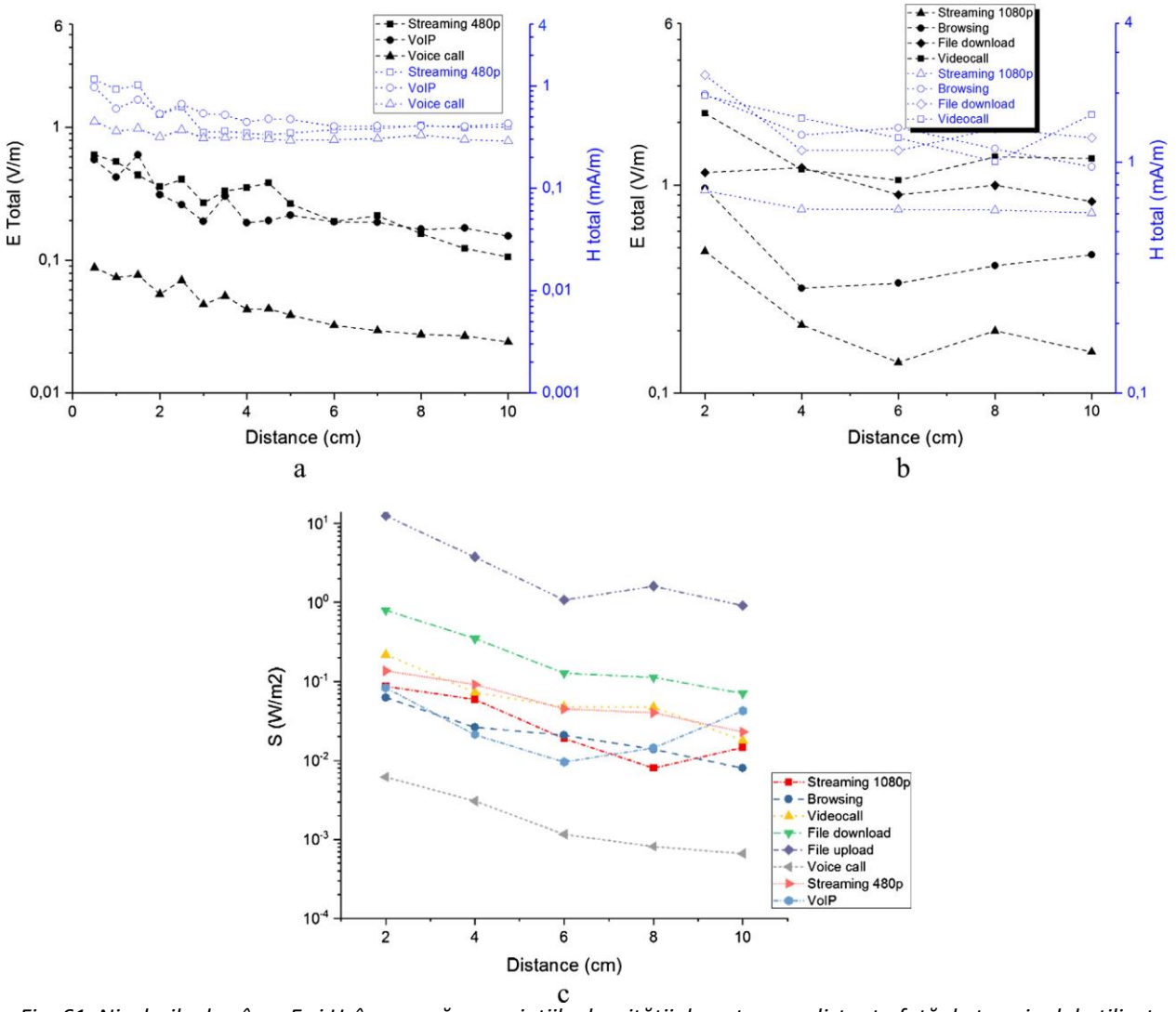


Fig. 61. Nivelurile de câmp E și H, împreună cu variațiile densității de putere cu distanța față de terminalul utilizat pentru diferite servicii de aplicații 3G+.

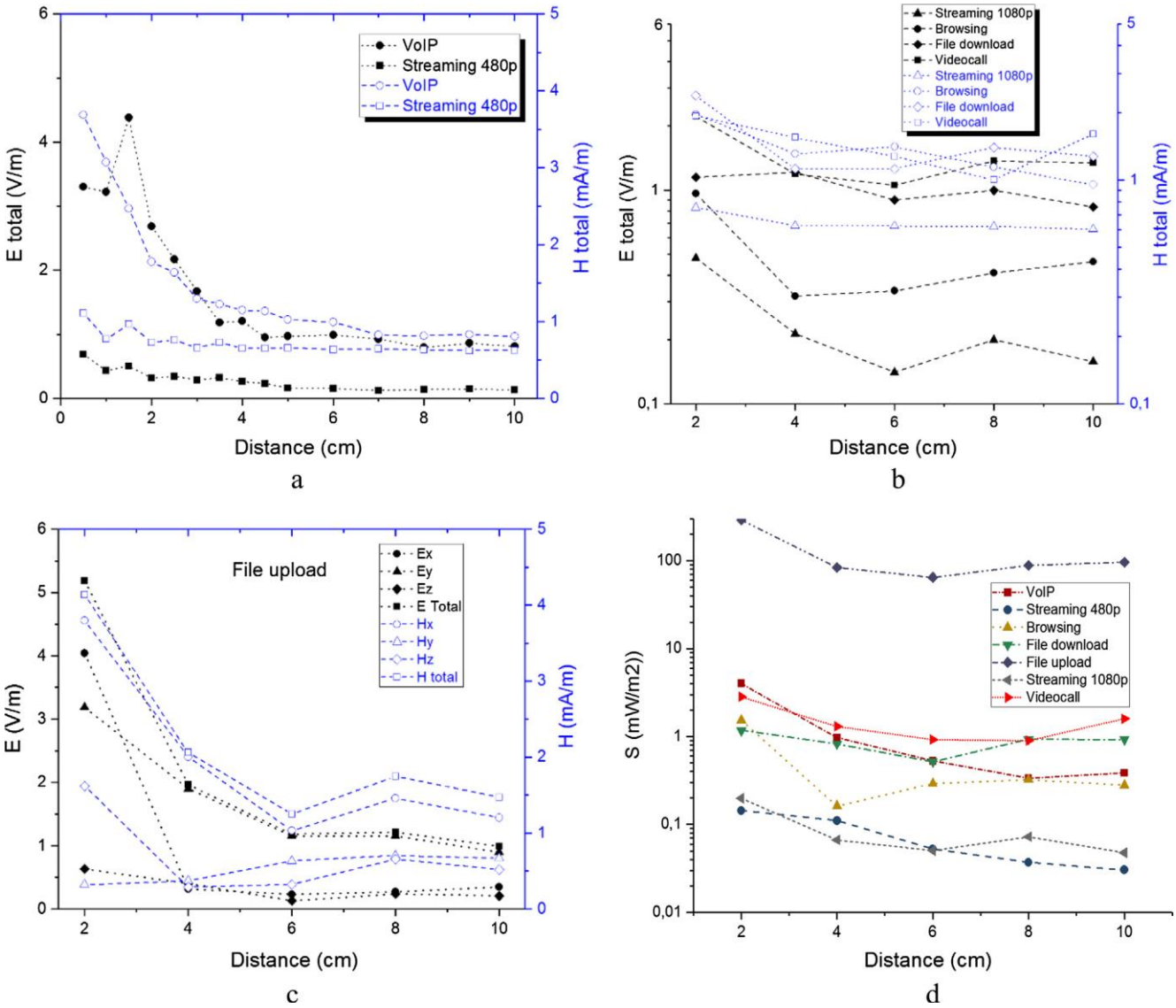


Fig. 62. Variația câmpului E, a câmpului H și a densității de putere cu distanța pentru diferite servicii 4G+.

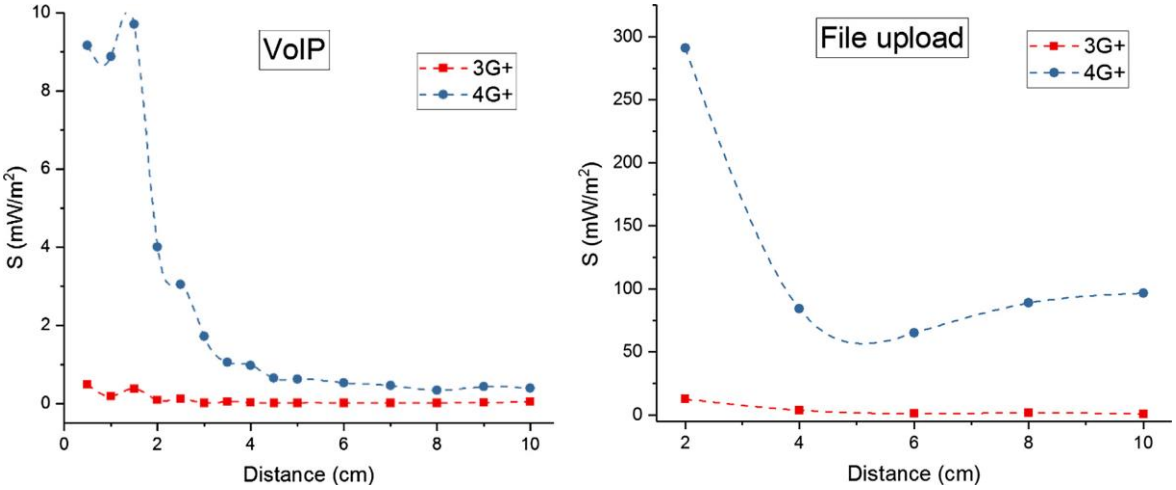


Fig. 63. Comparație între epuizarea densității de putere 3G+ și 4G+ cu distanța din apropierea terminalului: VoIP (a) și încărcarea fișierelor (b).

Scopul acestui studiu a fost de a caracteriza expunerea umană atunci când se utilizează un telefon mobil pentru servicii de voce sau date aparținând diferitelor tehnologii de comunicare. Obiectivul a fost atins prin determinarea densității de putere radiată în câmpul apropiat al dispozitivului, pe baza semnalelor captate secvențial atât de sondele de câmp electric, cât și de cele

magnetice. Statisticile semnalului au fost preluate automat prin măsurători CCDF disponibile. Evaluarea locală, dar realistă a expunerii, a fost efectuată prin măsurarea diferitelor situații care au implicat utilizarea unui număr de servicii de aplicare disponibile pentru abonați mobili moderni.
Pentru scenariile de operare 4G+, densitatea de putere locală a fost cea mai mare în timpul încărcării fișierelor, urmată de VoIP, apel video, descărcare fișiere, servicii de streaming și navigare. Pentru tehnologia 3G+, ordinea descrescătoare a expunerii a fost asociată cu: încărcarea fișierelor, descărcarea fișierelor, streaming, VoIP, apeluri video și servicii de navigare. Este important să se sublinieze că niciuna dintre valorile măsurate ale intensităților câmpului sau ale densității de putere nu a depășit nivelurile de referință specificate în orientările ICNIRP.

Deoarece tehnologia 4G+ este proiectată pentru rate ridicate de date, se preconizează că densitatea de putere în câmp apropiat va fi considerabil mai mare decât în cazul tehnologiei 3G+. Chiar și din punctul de vedere al expunerii utilizatorilor, o rețea 4G+ este mai eficientă pentru rate de date mai mari. În această măsură, s-a observat că aplicații precum VoIP sau video-call, care sunt servicii în timp real care necesită rate de date scăzute, dar constante, au fost asociate cu o expunere semnificativ mai mare în rețeaua 4G+, comparativ cu 3G+. Navigarea duce la valori pentru densitatea de putere care este de 18 ori mai mare pentru 4G+ în comparație cu 3G+. Deoarece descărcarea unui fișier nu necesită o comunicare uplink consecventă cu stația de bază, puterea radiată s-a dovedit a fi în medie de 3 ori mai mare în rețeaua 4G+. Niveluri similare de putere radiată au fost obținute pentru serviciile de streaming în ambele tipuri de rețea (independent de calitatea video selectată). Dintre toate testate aplicații, cele mai mari niveluri de putere radiată au fost măsurate în timpul încărcării fișierelor în ambele tipuri de rețea. Rezultatele arată că, chiar și cu un grad moderat de generalitate, este de așteptat o expunere mai mare pentru o aplicație care rulează sub 4G+ mai degrabă decât sub standardul de comunicare 3G+, având în vedere modelele de telefoane similare (și antenele).

2. Securitatea cibernetica a soluțiilor și serviciilor de calcul și comunicații

Securitatea cibernetică trebuie privită din două perspective în activitatea profesionala a autorului:

- **Perspectiva didactică și de dezvoltare continuă** (platforme de laborator pentru instruire și antrenare ("cyber-range") și inițiative de tip "hub" regional concretizate prin participarea în cadrul Brașov CyberHub) - Din această perspectivă se vor prezenta o serie de contribuții din perspectiva de fondator și coordonator al programului de masterat în limba engleză "Cybersecurity", ce include și etapele de construire a unui laborator de securitate cibernetică reconfigurabil și versatil, precum și coagularea unei inițiative locale de tip hub tehnologic numită "Brașov CyberHub".

- **Perspectiva implementării unor soluții inovative pentru securizarea soluțiilor și serviciilor de calcul și comunicații** – ce reprezintă o serie de implementări HW/SW, în majoritatea lor bazate pe instrumente cu sursa deschisa, realizate și în colaborare cu doctoranzi ai Universității Transilvania, precum și cu masteranzi sau absolvenți internaționali ai programului de master. Unele dintre implementări au fost realizate experimental în cadrul infrastructurii IT a universității, tocmai pentru întărirea metodelor de securitate ale Universității Transilvania.

2.1.Securitatea cibernetică - Perspectiva didactică și de dezvoltare continuă

Înființarea programului de master Cybersecurity în anul 2018 a inclus o etapă importanta de elaborare a curriculei, ținând cont de recomandările Centrului National Cyberint dar urmărind și programa unor universități internaționale precum și curiculla unor certificări de prestigiu din domeniul securității cibernetice (SANS Institute - Global Information Assurance Certification (GIAC), EC-Council, CompTIA). O altă etapă importantă a reprezentat-o construirea unei infrastructuri de laborator de tip *cyberrange,* beneficiind și de o sponsorizare consistenta din partea firmei Atos.
Construirea infrastructurii de laborator a însemnat un proiect în sine, de la infrastructura hardware și infrastructura virtualizată de laborator, până la implementarea laboratoarelor și a unei zone de lucru dedicate fiecărui student, cu acces de la distanță (ceea ce s-a dovedit extrem de utilă în timpul pandemiei de COVID19, dar și pentru unele colaborări internaționale).

O serie de principii au stat la baza conceptului pentru arhitectura laboratorului de securitate cibernetică, descris în [24]:

- Studenții să îl poată utiliza de la distanță prin intermediul VDI (desktop virtualizare) de la resurse din intranetul universității și de la conexiuni externe prin VPN
- Posibilitatea ca fiecare student să aibă propriul mediu de lucru, astfel încât să nu existe conflicte și restricții de funcționare, în condițiile unei cereri mari de resurse (în special procesare, DRAM și HDD).
- Din motive de securitate, sistemele au trebuit izolate de restul infrastructurii universitare, astfel încât orice teste și experimente de securitate să nu afecteze rețeaua operațională
- Componentele sistemului (mașini virtuale) ar trebui să fie instanțiate la cerere pe baza subiectului și a configurației specifice laboratorului, astfel încât o metodă de orchestrare pentru IaaS să fie utilizată

- Posibilitatea ca studenții să editeze configurații, să adauge elemente noi, noi componente software, noi implementări de containere virtuale Docker
- Posibilitate de ”curățare” a sistemului (eliberare a resurselor), după activitatea prestata de fiecare student.

Am analizat software-ul și elementele de rețea virtualizate necesare laboratoarelor noastre care ar trebui să servească mai multor discipline, la momentul construirii laboratorului (cu o re-evaluare constantă a necesităților):

- Pentru discipline ce tratează securitatea rețelei și subiectele de apărare perimetrală am avut nevoie să integrăm diferite elemente de firewall și puncte finale VPN (pfSense, IP Fire, Cisco ASAv, Cisco Firepower Thread Defence, Cisco Firepower Management Center), Sisteme de detectare a intruziunilor / Sisteme de prevenire a intruziunilor (IDS/IPS), routere și switch-uri virtualizate (subiecte legate de atenuarea diferitelor amenințări de securitate L2).
- Pentru teme de *hacking etic* există câteva elemente care ar trebui integrate, cum ar fi: Kali Linux, Metaspoitable, DVWA (Damn Vulnerable Web Applications), diferite instrumente pentru scanarea vulnerabilităților, alte mașini atacabile (Sisteme Windows, Linux, Android, cum ar fi, de exemplu, mașini virtuale preinstalate de diferite distribuții, cum ar fi cele furnizate de OSBoxes)
- Pentru materii ce tratează gestionarea incidentelor de securitate cibernetică, putem recomanda distribuția de Security Onion, inclusiv diferite elemente NIDS (Snort, Suricata, Bro) și HIDS și SUITA ELK Stack Suite (Elastic Search, Logstash, Kibana), dar și alte opțiuni, cum ar fi AlienVault OSSIM (Open Source SIEM) sau soluții comerciale SIEM (Informații de securitate și gestionarea evenimentelor) cu programe academice care oferă abonamente de un an (de exemplu Splunk SIEM).
- Pentru extragerea datelor și subiectele Big Data există imagini dedicate Hadoop/Cloudera și Apache Spark.
- Pentru laboratoarele generice în criptografie și securitatea rețelelor, setul de laboratoare SEED este de mare utilitate.
- De asemenea, este necesară implementarea mașinilor infectate pentru analiza criminalisticii IT și a programelor malware, luând în considerare restricționarea izolării complete de laborator a sandbox-ului de securitate cibernetică din rețeaua operațională universitară; Pentru acest domeniu există, de asemenea, distribuții dedicate care oferă mașini virtuale pre-integrate, cum ar fi Remnux sau SANS DFIR.

Din punct de vedere al costurilor și pentru că trebuia să îndeplinim și condiția de acces de la distantă prin tehnologii de tip desktop virtual VDI, iar Citrix Xen Desktop este o soluție VDI robustă, am decis să folosim hipervizorul Xen Server, licențele de virtualizare fiind gratuite la achiziționarea licențelor XEN Desktop.
Licențele XEN Desktop sunt perpetue, așa că am optat pentru această soluție, deși au fost luate în considerare și alte opțiuni (VmWare vSphere).
Pentru conectare din orice locație printr-o soluție securizată s-a folosit soluția Citrix Netscaler.

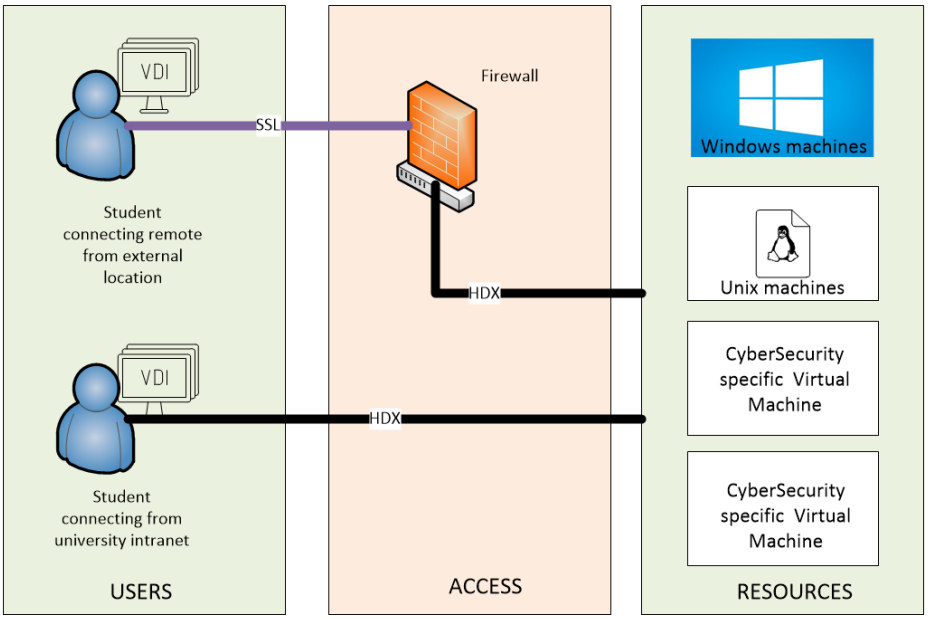


Fig. 64. Desktop-ul virtualizat VDI, implementat prin tehnologia XEN Desktop permite conecta la resurse nu numai utilizatorii intranet universitate, dar, de asemenea, utilizatorii externi

Deoarece majoritatea acestor mașini emulează atacuri și amenințări sau elemente de rețea care pot rula într-un mediu de întreprindere, laboratorul este structurat pe un firewall care separă între zonele de securitate: un mediu LAN (interior), un mediu WAN (exterior) și o zonă demilitarizată (DMZ).

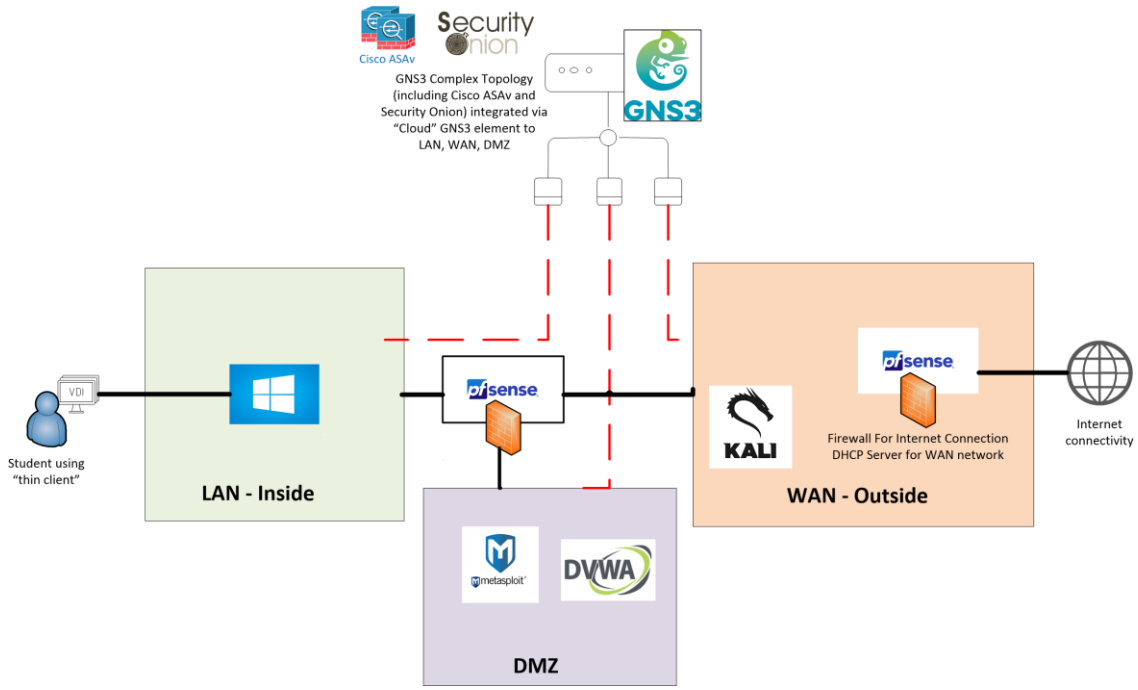


Fig. 65. Mediul de lucru pentru un student al laboratorului de securitate cibernetică. Diferite mașini virtuale pot fi pornite în fiecare zonă sau topologia poate fi extinsă în GNS3, în funcție de scenariul de laborator

Fiecare dintre mașinile virtuale a fost creată în XEN Server ca o imagine de referință ("imagine de aur / golden image"), care este instanțiată pentru fiecare utilizator la cerere. Astfel de imagini includ pe lângă imaginea conexiunii inițiale Windows 10 și alte imagini, cum ar fi: un firewall pfSense, distribuție Kali Linux, un Metasploitable, DVWA etc.

Fiecare student are propriul mediu LAN-WAN-DMZ. Mediul pentru fiecare student este izolat de mediul unui alt student. Acest lucru se face prin utilizarea VLAN-urilor (LAN-uri virtuale), astfel, fiecare profil de student rulează într-o zonă separată VLAN dedicată.
GNS3 a evoluat de la un emulator Cisco IOS, la un orchestrator de rețea complet care poate integra elemente de rețea formează mai mulți furnizori, mașini virtuale (QEMU, VirtualBox, VmWare), containere virtuale Docker. Lista de aparate GNS3 este impresionantă și continuă să se extindă.
Marele avantaj al VM GNS3 este posibilitatea de a conecta topologia GNS3 la elemente externe, astfel, fiecare element poate fi conectat în partea LAN, WAN sau DMZ a topologiei. Figura 66 prezintă o topologie GNS3, inclusiv un element Cisco ASAv care este conectat prin intermediul elementului "Cloud" la rețeaua WAN (unde este activ un server DHCP, așa cum este vizibil în figura 65 și, de asemenea, este furnizată conexiunea la Internet).

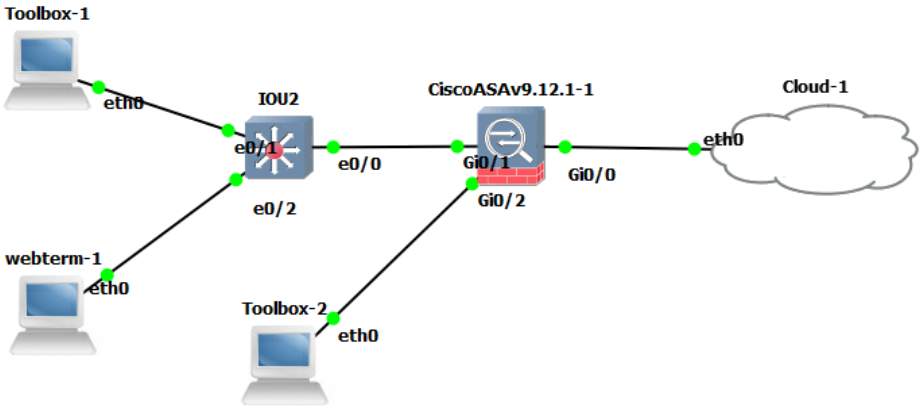


Fig. 66. Topologia GNS3 poate fi integrată cu restul mediului virtualizat. Elementul Cloud-1 face conexiunea Cisco ASAv la rețeaua WAN

Platforma inițială implementată în anul 2019 are unele limitări dintr-o topologie LAN-WAN-DMZ fixă, deci nu toate configurațiile au fost posibile, iar mașinile au fost atribuite în zone specifice (de exemplu, o singură mașină Kali Linux ar putea fi utilizată și conectată numai pe partea WAN, mașina Windows 10 a fost conectată la lan și a fost dificil să se ocupe de integrarea suplimentară a gazdei în topologie, .etc)
În 2022, autorul a candidat la un grant de cercetare în domeniul securității cibernetice, oferit de Fullbright. Grantul obținut a fost folosit pentru a efectua, pe lângă actualizări, o reproiectare a sistemului care a îmbunătățit semnificativ performanța sistemului și, în principal, gradul de utilizare și flexibilitatea acestuia.
După actualizarea platformei de laborator din această fază a doua de dezvoltare, fiecare student are posibilitatea de a-și defini propria topologie în GNS3 (cu drag and drop), poate integra cât mai multe mașini virtuale pe care le dorește (mai multe mașini Windows, Linux și Kali Linux, oricâte firewall-uri dorește, conectate în orice fel, actualizate pe Internet și așa mai departe).

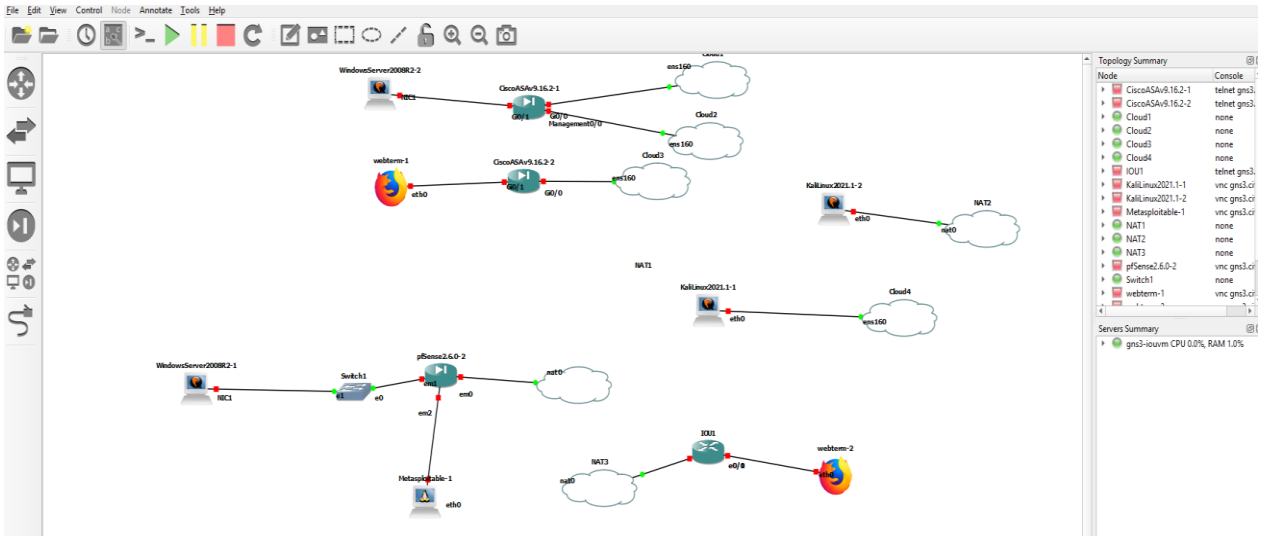


Fig. 67. Topologii GNS3 complexe care pot rula în diferite scenarii (toate împreună sau separate), scenarii flexibile care urmează să fie create de studenți.

Aplicațiile care inițial au fost instalate direct în mașini virtuale care oferă o topologie fixă (Metasploitbale, Kali linux, PfSense, OPNsense, Windows Server), în noua versiune se află instalate în cadrul serverului GNS3, permițând astfel topologii flexibile și rețele virtualizate sunt conținute în interiorul serverului GNS3. O nouă rețea DMZ (în arhitectura de Internet a universității) permite accesul la Internet în cazul în care sunt necesare actualizări și noi instrumente.

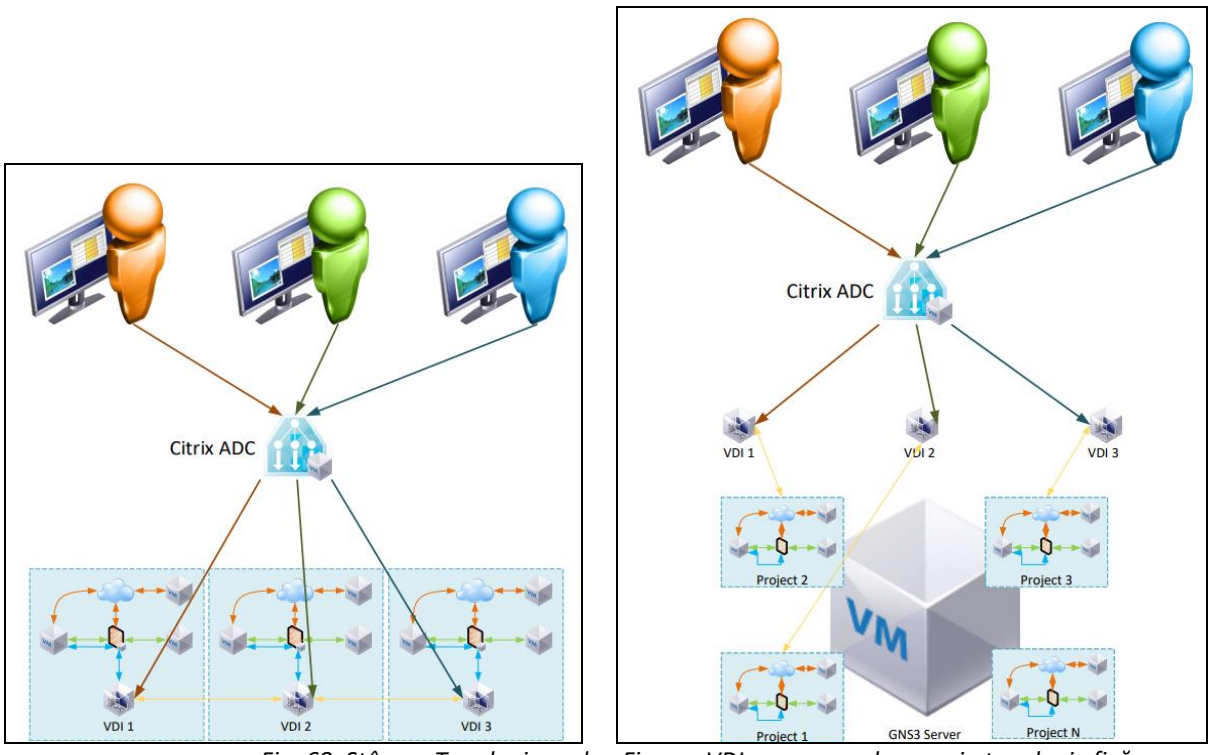


Fig. 68. Stânga: Topologie veche: Fiecare VDI avea acces la propria topologie fixă. Dreapta: Acces topologie nouă de la VDI la GNS3 Server

Pe baza noii infrastructuri de laborator s-a publicat și un nou îndrumar de laborator numit “Network Security and Perimeter Defence – Laboratory Guide”.
Îndrumarul detaliază diferite probleme ale securității rețelei: începe cu metodele de monitorizare a rețelei: syslog, SNMP, Netflow, atât de relevante pentru gestionarea incidentelor, continuă cu detalierea vulnerabilităților de nivel 2 și intră în funcționalitatea Firewall (firewall de generație

următoare), diferite opțiuni de tunelare (L2 și L3) și funcționalitatea IDS / IPS (sistem de detectare a intruziunilor / sistem de prevenire a intruziunilor).
Resursele sunt diferite, incluzând implementări open source, cum ar fi: Pfsense, Kali linux, Metasloptable, Security Onion, Snort, OpenVPN (.etc) și proprietare (cum ar fi Cisco ASA și Cisco IOS, instrumente Solarwinds) și diferite mașini gazde pentru testare (Linux, Windows) și containere virtuale.
Partea de laborator a fost modernizată prin automatizare cu Ansible, astfel încât unele configurații virtualizate să poată fi implementate în mod ad-hoc și automatizat, așa cum s-a prezentat în [25].

Pentru scenariile implementate, toate mașinile virtuale au fost create prin automatizare Ansible, cu excepția VM GNS3 care are propriul fișier OVA. Docker, ca parte a infrastructurii, a fost rulat de pe una din mașinile virtuale, de asemenea, prin intermediul script-uri Ansible.

```
- vmware_guest:
    hostname: "{{ VMWARE_HOST }}"
    username: "{{ VMWARE_USER }}"
    password: "{{ VMWARE_PASSWORD }}"
    validate_certs: no
    folder: /ha-datacenter/vm/
    name: "{{ item }}"
    state: poweredon
    guest_id: ubuntu64Guest
    esxi_hostname: "{{ esxi_host }}"
    cdrom:
    - iso_path: "[Datastore_2]/ubuntu-18.04.4-desktop-amd64.iso"
      type: "iso"
      controller_number: 0
      unit_number: 0
    disk:
    - size_gb: 15
      type: thin
      datastore: Datastore_2
    hardware:
      memory_mb: '{{ guest_vram }}'
      num_cpus: '{{ guest_vcpu }}'
    networks:
    - name:  '{{vm_network }}'
      ip: '{{ inventory_hostname }}'
      netmask: '{{ guest_netmask }}'
      gateway: '{{ guest_gateway }}'
      dns_servers:
      - '{{ guest_dns_server1 }}'
    wait_for_ip_address: yes
  delegate_to: localhost
  register: deploy_vm
```

Fig. 69. Captură de ecran a scriptului Ansible pentru crearea de mașini virtuale.

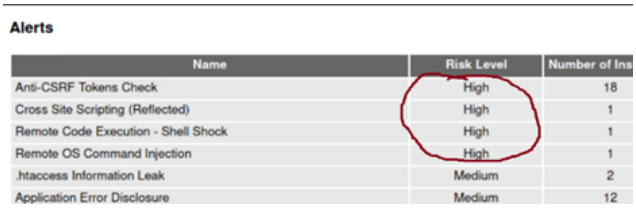
Scopul a fost de a crea diferite medii de laborator care pot fi instanțiate "la cerere / ca serviciu" de către utilizator, prin automatizare. Ca exemplificare, voi descrie unele dintre cele mai interesante scenarii de laborator ce au fost automatizate (implementări modulare ce se pot combina pentru scenarii mai complexe):

Scenariul 1: Scopul acestui scenariu a fost de a realiza scripturi Ansible pentru a permite Owasp ZAP efectua o scanare completă vulnerabilitate pe DVWA (Damn Vulnerable Web Application). Ambele aplicații au fost containere Docker.

```
  - name: running owasp zap full scan container against "{{
    become: yes
    docker_container:
      name: "{{ scan_name }}"
      image: "{{ owasp_zap_image_name }}"
      interactive: yes
      auto_remove: yes
      state: started
      volumes: "{{ reports_location }}:/zap/wrk:rw"
      command: "zap-full-scan.py -t {{ website_url }} -r {{
  - name: getting raw output of the scan
    become: yes
    raw: "docker logs -f {{ scan_name }}"
    register: scan_output
  - debug:
      msg: "{{ scan_output }}"
```

Fig. 70. Captură ecran a unei implementări Ansible folosită pentru scanări OWASP ZAP

Scanarea efectuată împotriva DVWA a generat un raport de securitate detaliat. Scanarea completă OWASP ZAP a verificat pentru o serie de vulnerabilități tipice, care include OWASP TOP 10. În funcție de vulnerabilitățile existente, funcționalitatea aplicației poate fi afectată.



Alerts

Name	Risk Level	Number of Ins
Anti-CSRF Tokens Check	High	18
Cross Site Scripting (Reflected)	High	1
Remote Code Execution - Shell Shock	High	1
Remote OS Command Injection	High	1
.htaccess Information Leak	Medium	2
Application Error Disclosure	Medium	12

Fig. 71. Raport complet scanare Owasp ZAP

Unele dintre vulnerabilitățile cu risc ridicat găsite sunt în figura 71. Atacul CSRF (Cross-Site Request Forgery) forțează țintele să trimită o solicitare HTTP către o destinație vizată fără știrea sau consimțământul lor pentru a executa o acțiune în numele lor. Owasp ZAP are un catalog de soluții pentru remedierea vulnerabilităților găsite.

Scenariul 2: Scopul scenariului a fost de a injecta cod SQL fals și de a falsifica o solicitare între site-uri în WebGoat în timp ce utilitarul de scanarea securității codului Contrast Security a fost folosit pentru a monitoriza livrarea de cod securizat și modificările de securitate în aplicație.

Rezultatele scenariului 2: Contrast Security a efectuat o analiză de securitate în timp real pe Webgoat și a generat un raport detaliat privind postura de securitate a aplicației oferind contramăsuri. Aceste informații ajută dezvoltatorii de aplicații web și echipele de apărare să fie conștienți de securitate și să integreze securitatea în aplicațiile web.

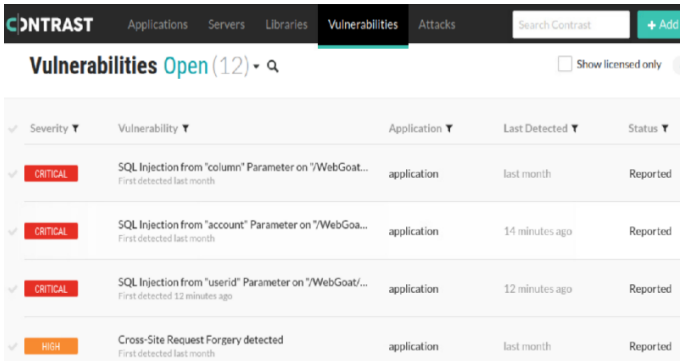


Fig. 72. Captură de ecran a activităților rău intenționate detectate.

Fig. 73. Captură de ecran care oferă detalii despre activitatea de injecție SQL.

Din rezultatele prezentate, Contrast Security monitorizează riscurile de securitate în același mod în care se monitorizează performanța și se utilizează informații despre amenințări pentru a obține un context complet despre un atac în timp ce are loc, apoi pentru a-i preveni imediat efectele. Putem concluziona din scenariul 2, cu ajutorul lui Contrast Security se îmbunătățește MTTD (timp mediu pentru a detecta) și MTTR (timp mediu pentru a răspunde).

Scenariul 3: În acest scenariu, automatizarea prin scripturi Ansible a folosit pentru Nikto pentru a efectua o scanare cuprinzătoare pe serverul Apache pentru a aduna informații.

```
tasks:
  - name: Nikto scanning in action
  # Output available in csv, html, msf+, nbe, txt, xml formats
    command: "/usr/share/nikto/program/nikto.pl -h {{ domain_name }} -o
/tmp/{{ domain_name }}-report.html"
  - name: downloading the report
    fetch:
      src: "/tmp/{{ domain_name }}-report.html"
      dest: "wordpress/lab_03/tmp/{{ report_name }}"
      flat: yes
      ignore_errors: yes
  - debug:
      msg: "Report can be found at {{ report name }}"
```

Fig. 74. Captură de ecran a scripturilor Ansible pentru a efectua scanarea Nikto.

Scenariul 3 Rezultate: Nikto a generat un raport de evaluare cuprinzător pe serverul web Apache. Raportul a indicat lipsa header-ului anti-clickjacking xframe-header, astfel utilizatorii pot face clic pe ceva de fapt diferit de ceea ce au crezut inițial. Acest lucru poate dezvălui apoi informații sensibile utilizatorului rău intenționat și atacatorul poate prelua, de asemenea, controlul asupra computerul utilizatorului.

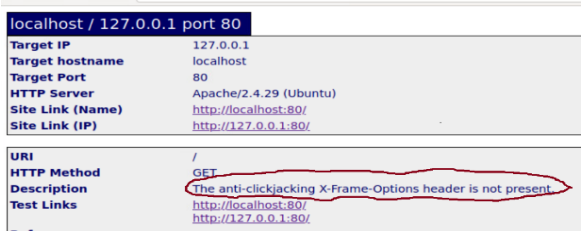


Fig. 75. Captură de ecran a raportului Nikto Scan.

Printre alte vulnerabilități, a dezvăluit, de asemenea, informații precum numărul portului, tipul de server și IP-ul care vor ajuta utilizatorii rău intenționați în timpul recunoașterii.

Scenariul 4: În acest scenariu, s-a automatizat un atac prin "brute force" în rețea. După pornirea serverului Monkey Island și introducerea informațiilor necesare pentru atac, Monkey a început un proces automat de atac.

Scenariul 4 Rezultate: După un atac reușit și raportul generat, s-a identificat că, Monkey a exploatat cu succes țintele și a compromis două mașini. Serverul Monkey Island arată harta procesului de atac.

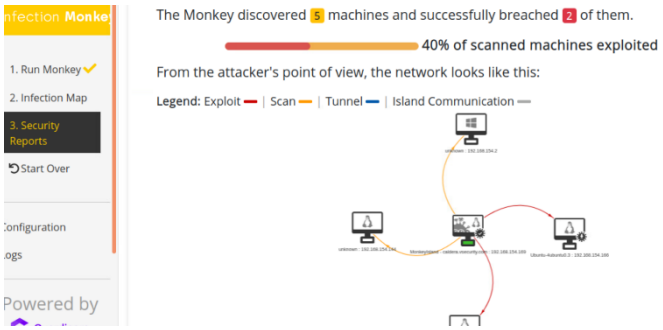


Fig. 76. Captură de ecran a procesului de atac al Infection Monkey

Mașinile cu legături roșii se consideră compromise, iar cele cu legături galbene au fost exploatate. Infection Monkey a furnizat o informație extinsă despre vulnerabilitate și oferă recomandări cu privire la modul de a întări securitatea mașinii gazdă.

Scenariul 5: În acest scenariu s-a utilizat cadrul Metasploitable pentru a scana automat porturi deschise și colecta informații despre serverele și topologia de rețea ESXI ROUTER GNS3, încercându-se și un atac automatizat.

Scenariul 5 Rezultate: S-au scanat porturile deschise de pe ROUTER ESXI și servere. Porturile deschise găsite au fost SSH, HTTP, Telnet și SIP. Acestea sunt informații importante pe care adversarii le pot folosi pentru a căuta bug-urile din servicii și a le exploata.

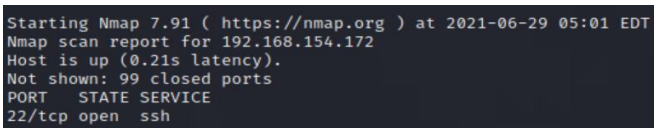


Fig. 77. Scanare Nmap Metasploitable pentru porturi deschise pe router

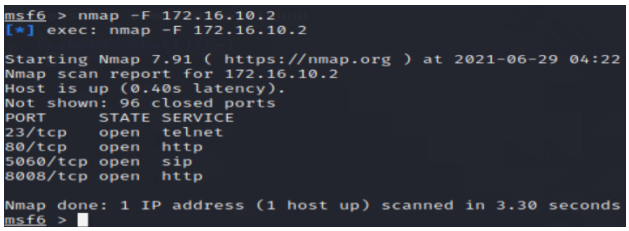


Fig. 78. Scanare Nmap Metasploitable pentru porturi deschise pe serever http.

Fig. 79. Exploatarea routerului ESXI prin ssh.

Scenariul 6: În acest scenariu s-a efectuat o evaluare cuprinzătoare a întregii arhitecturi. Nessus a efectuat scanarea de rețea de bază și avansată în mediul Cloud.

Scenariul 6 Rezultate: Scanarea rețelei a furnizat un raport detaliat despre serverul ESXi. Vulnerabilitățile au fost prezentate în funcție de riscul lor. A fost generat un alt raport de evaluare pentru toate gazdele și serviciile din rețea. Acest exercițiu a oferit informații importante pentru a securizarea serverului ESXi (Cloud) și, de asemenea pentru evaluarea posturii de securitate a sistemului de operare. Cu Nessus, inginerii de securitate pot obține o vizibilitate completă în rețea.

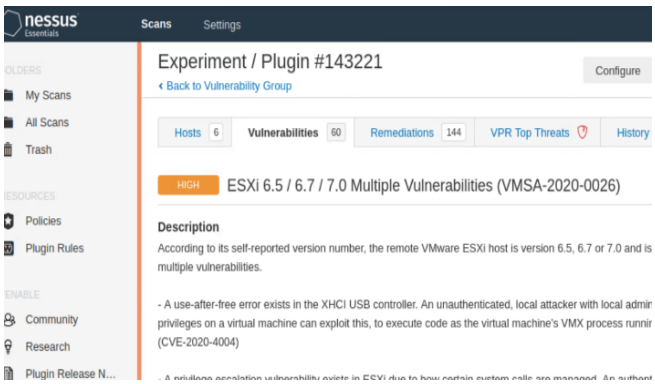


Fig. 80. O descriere detaliată a unei vulnerabilități pe serverul ESXi.

2.2.Soluții pentru securizarea soluțiilor și serviciilor de calcul și comunicații

Integrarea sistemelor de calcul și comunicații trebuie privită și din perspectiva securității datelor și a abordării integrative pe întreg lanțul de procesare și transport al datelor. Sunt prezentate o serie de implementări HW/SW, în majoritatea lor bazate pe instrumente cu sursa deschisă, realizate și în

colaborare cu doctoranzi ai Universității Transilvania, precum și cu masteranzi sau absolvenți internaționali ai programului de master.
Aceasta secțiune prezintă o serie de contribuții urmând principiile conceputului de apărare stratificată "Defence in Depth", ce urmărește aplicarea metodelor de securizare la nivele diferite, de la utilizator și terminal până la elementele de comunicații și rețea periferică. Soluțiile prezentate includ și diverse metode de evaluare/auditare a vulnerabilităților unui sistem, de prevenire a unor posibile atacuri cibernetice, gestionarea și răspunsul la incidente de securitate cibernetică, precum și investigarea criminalistică (termenul consacrat în limba engleza este "forensics") a incidentelor.

2.2.1. Evaluarea vulnerabilităților la nivel de firmware

Unul dintre aspectele legate de testarea (prin evaluări și exerciții specifice) a nivelului de pregătire și răspuns la incidentele de securitate cibernetică a fost detaliat prin propunerea unui unei metodologii de tipul atac-răspuns ce poartă numele de testare purpurie, o combinație a celor două componente de baza ale unui asemenea exercițiu:

- Componenta de atac, ilustrata de echipa roșie
- Componenta de răspuns la incidente, ilustrată de "echipa albastră".

În [26] am propus o metoda de lucru de tip "purple team" (echipa roșie și echipa albastră conlucrează) pentru îmbunătățirea posturii de securitate pentru un dispozitiv încorporat (la nivel de firmware). Pentru îmbunătățirea designului de securitate pentru un dispozitiv încorporat, membrii echipei roșii (Red-Team) vor începe evaluarea firmware-ului urmând pașii următori:

1. Obținerea de informații despre dispozitivul încorporat și versiunea de firmware
2. Extragerea firmware-ul de pe dispozitiv sau descărcați de pe site-ul web al furnizorului
3. Utilizarea instrumentelor de inginerie inversă, cum ar fi: IDA Pro, Ghidra pentru inspectarea binarelor, cum ar fi: httpd, busybox și alte biblioteci de firmware
4. Detectarea erorilor și obținerea de recomandări privind formatarea codului de la un analizor static de cod sursă; verificarea corespondenței codului sursă cu standardului de formatare a codului și standardele de securitate. Instrumentul de analiză a codului sursă se concentrează pe detectarea potențialelor erori (bug-uri) și a problemelor de performanță.
5. Revizuirea codului de securitate pentru fișierele existente este necesară pentru a mapa și a găsi mai multe detalii despre dispozitivul încorporat. Găsirea unei probleme necesită pași suplimentari pentru a urmări codul care necesită remediere. Cele mai multe dintre aceste cazuri necesită, de asemenea, documentația pentru replicarea și înțelegerea erorilor. Aceste remedieri sunt adesea implementate într-o versiune de firmware nouă sau ulterioară.

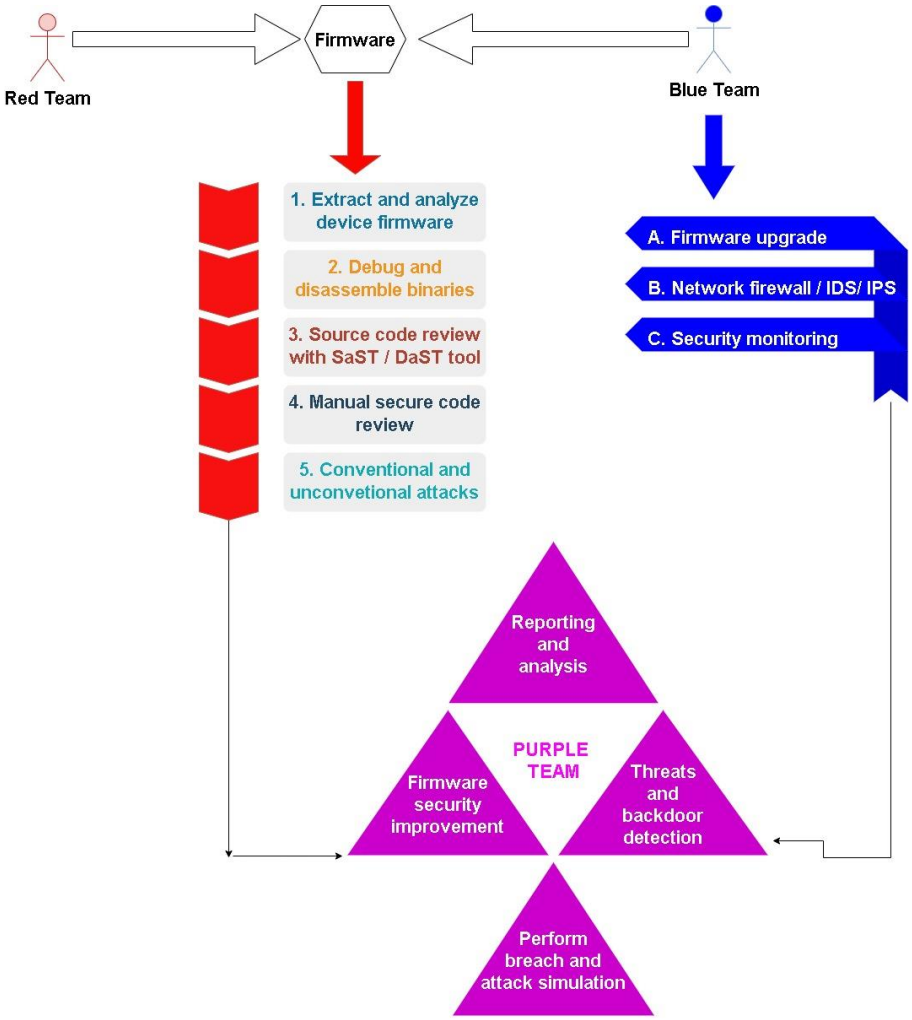


Fig. 81. Metodologia echipei Purple pentru analiza firmware-ului, conform cu [26]

Metodologia urmată se bazează pe utilizarea instrumentului de analiză a firmware-ului (BinWalk) și a instrumentului de inginerie inversă binară (Ghidra), folosind un firmware de punct de acces (access point) în scopuri demonstrative și pe efectuarea analizelor de ”inginerie inversă” pe firmware httpd, binare „busy box” pentru a obține informații despre sistem.
Voi începe prezentarea primului proces din perspectiva echipei roșii (pasul 1 – conform cu figura 81), respectiv extracția și analiza folosind binwalk.

```
┌──(root💀sld)-[~sld/Downloads/test/_rev.zip.extracted]
└─# ls
0.zip  rev.bin

┌──(root💀sld)-[~sld/Downloads/test/_rev.zip.extracted]
└─# binwalk -e rev.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
10328         0x2858          LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 6644380 bytes
1950802       0x1DC452        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2743032 bytes, 611 inodes, blocksize: 13
```

Fig. 82. Comanda binwalk utilizată pentru decomprimarea firmware-ului punctului de acces: binwalk -e firmware.bin

După comanda *binwalk -e* am putut vedea informații despre sistemul de fișiere extras, care este sistemul de fișiere Squashfs. Squashfs este un sistem de fișiere foarte comprimat numai în citire pentru Linux. Squashfs comprimă ambele fișiere, inode și directoare și acceptă dimensiuni de blocuri de până la 1Mbytes pentru o compresie mai mare, utilizează instrumente utilitare Mksquashfs și Unsquashfs pentru comprimarea fișierelor sau încorporarea unui sistem de fișiere în altul sau extragerea acestora dintr-un alt fișier. Unii furnizori pentru sistemul de fișiere comprimat Squashfs LZMA (Lempel–Ziv–Markov chain algorithm) folosesc numărul magic "shsq". Deci, se poate efectua o descărcare HEX pe firmware-ul și filtrul nostru folosind comanda *grep* pentru "shsq", pentru a obține adresa de pornire a firmware-ului. Extragerea binwalk va crea un folder numit _rev.zip (în acest exemplu). Squashfs-root va extrage întregul sistem de fișiere, astfel încât următorul pas ar putea fi analiza binarelor individuale sau utilizarea comenzilor *find*, *grep, awk* pentru căutarea în fișierele de configurare pentru identificarea de noi vulnerabilități.

```
┌──(root💀 sld)-[~sld/Downloads/test/_rev.zip.extracted]
└─# tree -L 1 _rev.bin.extracted/squashfs-root
_rev.bin.extracted/squashfs-root
├── bin
├── debug → /var/debug
├── dev
├── etc → /var/etc
├── etc_ro
├── init → bin/busybox
├── lib
├── mnt
├── proc
├── sbin
├── sys
├── tmp
├── usr
├── var
├── webroot → /var/webroot
└── webroot_ro

12 directories, 4 files
```

Fig. 83. Utilizarea arborelui -L 1 pentru listarea directorului din directorul rădăcină squashfs

```
┌──(root💀 sld)-[~sld/…/_rev.zip.extracted/_rev.bin.extracted/squashfs-root/etc_ro]
└─# cat passwd
root:$1$nalENqL8$jnRFwb1×5S.ygN.3nwTbG1:0:0:root:/:/bin/sh
admin:6HgsSsJIEOc2U:0:0:Administrator:/:/bin/sh
support:Ead09Ca6IhzZY:0:0:Technical Support:/:/bin/sh
user:tGqcT.qjxbEik:0:0:Normal User:/:/bin/sh
nobody:VBcCXSNG7zBAY:0:0:nobody for ftp:/:/bin/sh

┌──(root💀 sld)-[~sld/…/_rev.zip.extracted/_rev.bin.extracted/squashfs-root/etc_ro]
└─# cat shadow
root:$1$OVhtCyFa$7tISyKW1KGssHAQj1vI3i1:14319:::::
```

Fig. 84. Informații implicite din /etc_ro/shadow, /etc_ro/passwd care conține o listă a conturilor sistemului, oferind pentru fiecare cont câteva informații utile cum ar fi
ID-ul de utilizator, ID-ul grupului, directorul de domiciliu, shell.

Următoarea acțiune va fi pasul (2), depanarea și dezasamblarea unui binar. Pentru acest exemplu, voi dezasambla httpd binar situat în: _rev.bin. extracted/squashfs-root/bin.

Prin operația de dezasamblare aplicată pe binare, se restabilește codul aplicației software într-un format lizibil și ușor de înțeles. Fișierul codului de asamblare poate fi utilizat în procesele de inginerie inversă pentru a stabili fluxurile logice ale programului de calculator sau vulnerabilitățile acestuia într-un mediu de lucru.

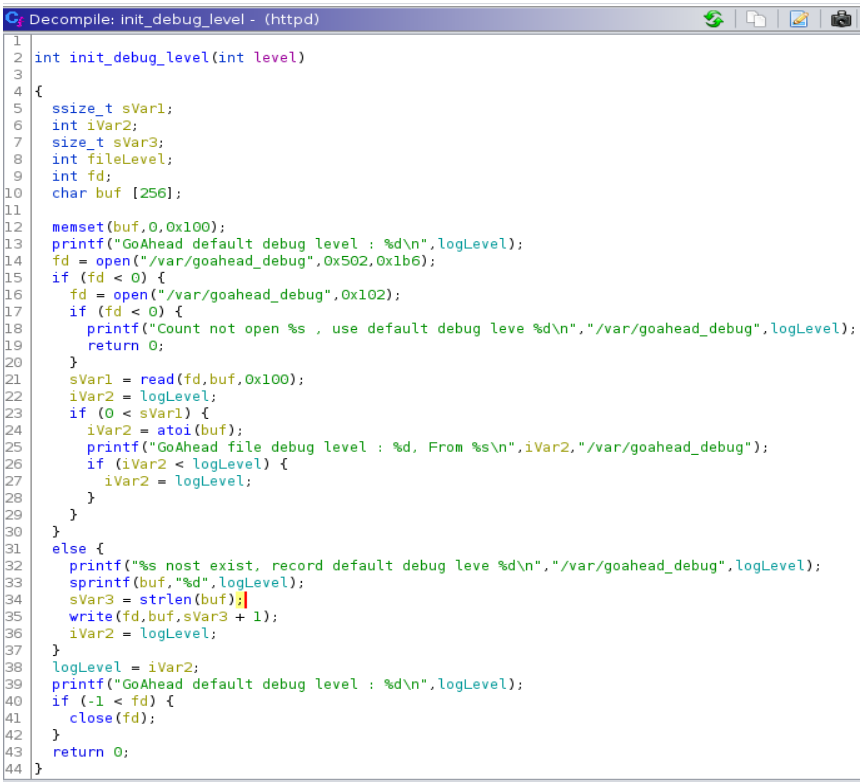


Fig. 85. În imaginea de mai sus putem vedea funcțiile de afișare potențial periculoasă pe liniile 13, 18, 25, 32, 33, 39 care ar putea duce la overflow întreg. Depășirile de numere întregi sunt consecința creșterilor/înmulțirilor "sălbatice", în general din cauza lipsei de validare a variabilelor implicate.

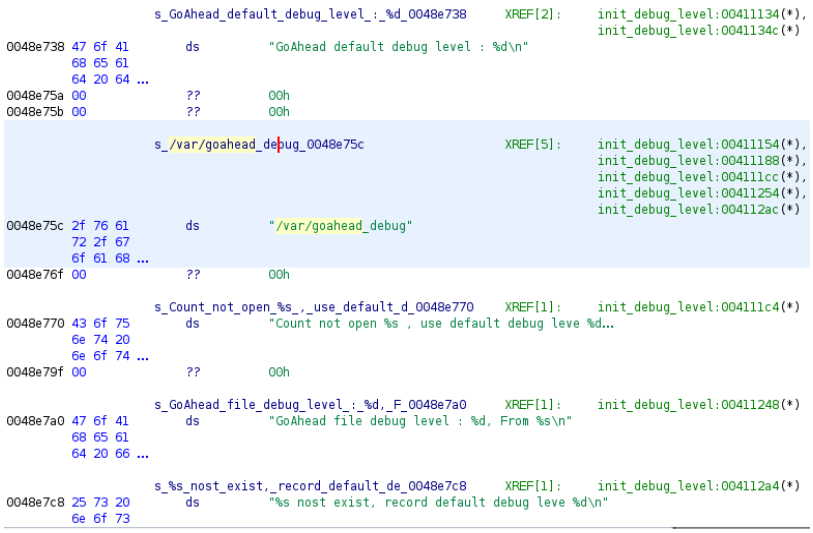


Fig. 86. –Vizualizarea de asamblare a binarului http poate fi utilizată pentru a evalua diferite apeluri de sistem sau probleme de cod vulnerabile

Partea de analiză a sistemului de fișiere squashfs cu instrumente de inginerie inversă precum Ghidra sau IDA-Pro reprezintă următorul pas. Prima recomandare este identificarea porturilor de comunicare serială (UART - Universal Asynchronous Receiver Transmitter) care sunt prezente în majoritatea punctelor de acces și dispozitivelor încorporate și utilizarea acestora pentru a obține acces shell la dispozitiv.

Echipa albastră oferă protecție în timp real împotriva atacurilor folosind acțiuni și reguli predefinite pentru firewall-uri, sisteme de prevenire a intruziunilor. Metoda eficientă este de a deconecta punctul de acces sau punctele de acces vulnerabile și de a utiliza distribuția wireless alternativă până când un nou upgrade de firmware va fi disponibil de la furnizor.

Echipa albastră din cadrul echipei violet (purple) acoperă managementul vulnerabilităților și actualizarea firmware-ului (A), detectarea conexiunilor suspecte interne sau noi folosind alerte de jurnal și reguli I.D.S / I.P.S / Firewall (B) și verifică instrumentele de monitorizare (C) pentru a identifica noi amenințări potențiale (a se vedea Figura 81). Tema unificatoare este aceea de a convinge echipa roș-albastră să cadă de acord asupra obiectivului lor comun de îmbunătățire organizațională și să nu introducă încă o entitate în mix. Membrii SOC (Security Operations Center) responsabili de fluxul de date sau membrii echipei albastre trebuie să utilizeze metode de automatizare și SOAR (Security Orchestration, Automation and Response) pentru declanșarea alertelor către o platformă de gestionare a incidentelor pentru întreaga rețea.

Echipa violet scrie un raport complet care va include o hartă detaliată a amenințărilor cu starea de execuție a fiecărei tehnici și o analiză atât din partea echipei roșii, cât și a celei albastre, precum și un ghid detaliat pentru implementarea oricărui risc asociat recomandat care nu a fost abordat pe deplin în timpul exercițiului. Folosind tehnici ofensive, echipa albastră împreună cu echipa roșie monitorizează simultan jurnalele și sistemele. Dacă o tehnică are succes, capacitățile actuale ale echipei violet sunt crearea și utilizarea unui nou mecanism de prevenire / detectare pentru fiecare tehnică utilizată cu succes în exercițiu. Prin utilizarea fiecărei categorii a cadrului MITRE ATT&CK , echipa violet trebuie să cartografieze un set personalizat de tactici și tehnici bazate pe riscuri, standarde industriale, pentru a crea o imagine de ansamblu clară pentru organizație.

2.2.2. Metodologie de securitate ofensivă aplicată pentru sisteme software de comunicații Windows Communication Foundation (WCF)

Windows Communication Foundation (WCF) este un cadru de comunicare pentru construirea de aplicații conectate, orientate spre servicii, lansate inițial de Microsoft ca parte a .NET Framework, dar acum fiind cu sursă deschisă. Comunicarea bazată pe mesaje WCF este o soluție foarte populară utilizată pentru trimiterea de mesaje asincrone de la un punct final de serviciu la altul. Deoarece WCF oferă multe funcționalități, are un model de dezvoltare de mare consum și, adesea, măsurile de securitate implementate în aplicații nu sunt adecvate. În acest studiu [27] am propus o metodologie pentru analiza securității ofensive a unui punct final sau serviciu WCF, din perspectiva echipei roșii. Sunt prezentate o abordare pas cu pas, informații empirice și un raport detaliat de analiză a vulnerabilităților WCF, propunând recomandări pentru atenuarea atacurilor și securizarea punctelor finale.

În [27] am propus următoarea metodologie pentru evaluarea Windows Communication Foundation Red-Team ce oferă diferite etape, instrumente și tehnici pentru a analiza un serviciu WCF pentru a descoperi noi vulnerabilități potențiale:

Pasul 1 - Identificați informațiile publice Scurse WSDL
Primul pas este găsirea de fișiere WSDL Web Services Description Language (WSDL) care ar putea conține informații sensibile și scurgeri de informații prin fișiere WSDL.

Pasul 2. Puncte finale WCF nesigure

O posibilitate comună pentru a descoperi vulnerabilități este de a găsi puncte finale WCF nesigure. Contractele de servicii sunt identificabile prin atributul ServiceContractAttribute și contractele de operare prin atributul OperationContractAttribute. Contractul de operare se aplică metodelor de expunere a acestora ca parte a funcționalității furnizate de serviciul WCF. În această parte a contractului există posibile vulnerabilități expuse. Serviciile expuse prin contracte fără nicio protecție sunt periculoase și ar putea fi o problemă reală de securitate.

Analiza oricărui serviciu WCF începând cu decompilarea aplicației:

1. Folosim interogări WMIC (Windows Management Instrumentation command-line) pentru a găsi executabile cu informații WCF
2. Verificarea fiecare executabil și DLL găsit folosind interogare WMIC cu dnSpy. După pornirea dnSpy și încărcarea unui executabil sau a unui fișier bibliotecă, pe partea de referință, căutăm System.ServiceModel. Sistemul. Opțiunea ServiceModel este necesară pentru a crea serviciul WCF.
3. Folosind căutarea dnSpy, se caută [ServiceContract] și [OperationContract]. Aceste atribute vor expune interfața ca serviciu WCF.
4. Pentru comunicare și posibila exploatare, trebuie să creăm un client pentru a comunica cu serviciul WCF.

Pasul 3. Vulnerabilități Xml / WS / REST - instrumente pentru evaluarea vulnerabilității

Următoarele instrumente sunt utilizate pentru testarea diferitelor tipuri de vulnerabilități legate de servicii WCF XML/WS/REST:

A. SoapUI - SOAP UI este un instrument open source de testare API și, de asemenea, independent de platformă. SoapUI permite utilizatorilor să execute teste automate funcționale, de regresie, de conformitate și de încărcare pe diferite API-uri Web.

B. WCFTestClient - Clientul de testare Windows Communication Foundation (WCF) (WcfTestClient.exe) este un instrument GUI care permite utilizatorilor să introducă parametrii de testare, să trimită acea intrare la serviciu și să vizualizeze răspunsul pe care serviciul îl trimite înapoi. Acesta oferă o experiență perfectă de testare a serviciilor atunci când este combinat cu gazda de servicii WCF.

C. WSSAT - WSSAT este un instrument utilizat pentru scanarea serviciilor web care oferă opțiunea prin editarea fișierelor de configurare pentru a adăuga, actualiza sau șterge vulnerabilități. Acest instrument acceptă adresele WSDL ca intrare și efectuează teste statice și dinamice împotriva vulnerabilităților de securitate. Cu acest instrument, toate serviciile web ar putea fi analizate simultan, iar evaluarea generală a securității ar putea fi văzută de organizație.

D. WS-Attacker - WS-Attacker este un cadru modular pentru testarea penetrării în domeniul serviciilor web. WS-Attacker oferă o funcționalitate pentru a încărca fișiere WSDL și trimite mesaje SOAP la punctele finale ale serviciului Web (care este executat utilizând cadrul SoapUI de bază). Această funcționalitate poate fi extinsă utilizând diverse plugin-uri și biblioteci pentru a construi atacuri specifice de servicii Web.

Fig. 87. Informații colectate de la un serviciu public WCF folosind testarea serviciului WCF cu WcfTestClient

Pasul 4. Lipsa autentificării sau criptarea transportului

Protecția insuficientă a nivelului de transport este o deficiență de securitate cauzată de faptul că aplicațiile nu iau nicio măsură pentru a proteja traficul de rețea. În timpul autentificării, aplicațiile pot utiliza SSL/TLS, dar adesea nu reușesc să o utilizeze în altă parte a aplicației, lăsând astfel datele

și ID-urile de sesiune expuse. Datele expuse și ID-urile de sesiune pot fi interceptate, ceea ce înseamnă că aplicația este vulnerabilă la exploatare.

Fig. 88. Utilizarea WcfScan pentru testarea configurației legăturilor de securitate pe un serviciu WCF expus publice

WcfScan - Un instrument pentru scanarea .NET de puncte finale TCP WCF, testându-se securitatea configurațiilor. Acest instrument creează un contract de servicii foarte simplu, generic și încearcă să se conecteze la URL-ul punctului final al serviciului furnizat, parcurgând toate opțiunile posibile de setare de securitate. În cele din urmă, contractul generic nu va face un apel end-to-end reușit la serviciu; cu toate acestea, va funcționa bine pentru enumerarea setărilor de securitate interpretând excepțiile pe care le returnează .NET framework. Acest lucru permite testerului să se concentreze asupra rezultatelor, mai degrabă decât să scrie codul repetitiv (boilerplate) care este necesar doar pentru câteva minute. Pentru testerul care nu este familiarizat cu dezvoltarea în .NET, WcfScan vă poate ajuta să evaluați rapid setările de configurare de securitate de bază pentru un NET. Legarea serviciului TCP. În acest exemplu, am folosit WcfScan împotriva unui serviciu WCF deschis pentru a verifica nivelul de securitate. Pentru această demonstrație, am folosit un serviciu WCF deschis, găsit cu Google Dork în scopuri de testare (Figura 88).

Acești pași și exemple detaliate pot fi urmate în timpul evaluărilor de securitate ofensive de către membrii echipei roșii. Ca dezvoltări viitoare, intenționăm să studiem și să documentăm evaluarea și implementările echipei albastre pentru a atenua încălcările expuse ale WCF.

2.2.3. Email Gateway metode de evaluare a vulnerabilităților de securitate cibernetică

Conform raportului Check Point Research (CPR) 2020, 63% din programele malware din 2019 au fost livrate prin atașamente de e-mail. Statisticile de securitate cibernetică la nivelul anului 2021 arată că 92% din atacurile cibernetice livrate prin e-mailuri, în timp ce 66% din programele malware au fost instalate prin atașamente de e-mail rău intenționate.

Majoritatea acestor fișiere rău intenționate sunt în formă de PDF-uri, documente Microsoft Office, fișiere electronice, arhive ZIP sau RAR etc. Aceste fișiere sunt atașate de atacatori pe e-mail cu intenția de a instala programe malware care pot corupe date sau pot obține informații. Unele dintre acestea oferă hackerilor acces la mașina victimelor, permițându-le să monitorizeze ecranul, să obțină acces la multe alte sisteme de rețea și să înregistreze apăsări de taste.

Scopul acestei cercetării descrisă în [28] fost acela de a detecta și preveni atașamentele de e-mail rău intenționate la nivelul serverului de email al Universității Transilvania din Brașov, implementat cu SurgeMail, prin integrarea Proxmox Mail Gateway (PMG) și Cuckoo Sandbox. Obiectivele au inclus: integrarea gateway-ului de e-mail opensource cu serverul de e-mail, detectarea e-mailurilor rău intenționate prin integrarea Cuckoo Sandbox și implementarea metodologiilor de blocare și alarmare.

Configurația experimentală (figura 89) a fost virtualizată, am configurat SurgeMail ca server de e-mail intern, Proxmox Email Gateway 6.4 (PMG) pentru a scana toate e-mailurile primite și trimise iar Cuckoo Sandbox 2.0.7 a fost configurat pentru analiza atașamentelor de e-mail rău intenționate.

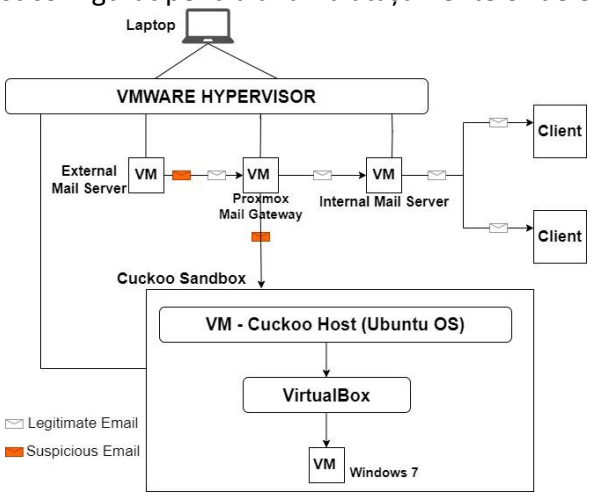


Fig. 89. Configurarea arhitecturii experimentale de protectie email

Fluxul de execuție

Așa cum este ilustrat în Fig. 90, toate e-mailurile primite sau trimise către serverul de poștă electronică internă trec mai întâi prin gateway-ul de e-mail Proxmox pentru scanarea fiecărui e-mail înainte de a ajunge la serverul de e-mail intern. Dacă sunt detectate atașamente suspecte, vor fi puse sub directorul de carantină la nivel PMG și gateway-ul de poștă electronică informează administratorul serverului de e-mail despre fișierul suspect. Apoi, fișierul suspect va fi trimis automat la Sandboxing Cuckoo folosind API-ul Cuckoo pentru analize suplimentare. Această analiză ajută la determinarea dacă fișierul suspect care a fost detectat la nivel de Proxmox nu a fost cumva un caz fals pozitiv, dar, de asemenea, ajută administratorul de sistem să știe ce malware a fost destinat să facă în cazul în care fișierul rău intenționat este confirmat de Cuckoo Sandbox. Prin urmare, dacă nu se găsește nicio activitate rău intenționată prin sandboxing, atunci poșta va fi pusă sub fluxul normal pentru a ajunge la destinația dorită.

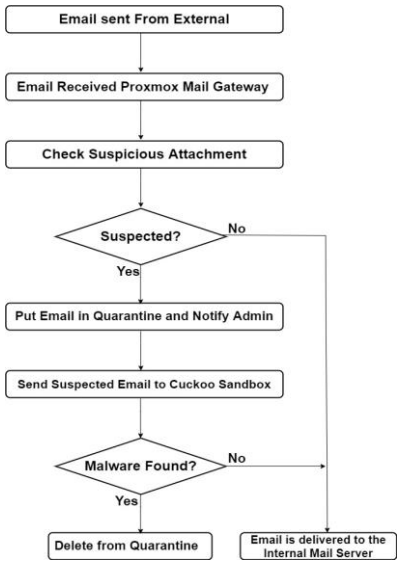


Fig. 90. Flux de lucru pentru executarea gateway-ului de e-mail, reprezentarea diagramei bloc

PMG include motorul opensource antivirus ClamAV încorporat pentru detectarea malware-ului, troienilor și software-ului rău intenționat. Include un agent de scanare multi-threaded cu

performanțe excelente și capacitatea de a actualiza automat modificările semnăturii. Cu toate acestea, deoarece PMG poate detecta rezultate fals pozitive în timp ce e-mailul a fost important pentru expeditor, Cuckoo Sandbox a fost integrat cu PMG pentru analizarea e-mailurilor suspecte. Obiectivul de a notifica administratorul de sistem de e-mail despre malware a fost atins doar parțial datorită tehnicii de clasificare a severității Cuckoo sandbox. Cuckoo poate genera un raport al unui astfel de comportament, clasificând severitatea activităților și a performanței pe o scară de la 1 la 10, prin care 10 este considerat ca fiind cel mai sever. Din păcate, datorită logicii de bază a tehnicii de clasificare a severității, această clasificare a scorului poate fi într-adevăr înșelătoare. În plus, unele dintre probele care au fost prezentate au fost clasate chiar peste 10, cum ar fi 11/10, 15/10. Acest lucru poate face ca scorurile din Cuckoo sandbox sa fie incerte. Deoarece Proxmox Mail Gateway a detectat deja fișierul rău intenționat, PMG trimite e-mailul de notificare administratorului de sistem despre starea unei acțiuni rău intenționate.

2.3.Securitatea dispozitivelor IoT

Una dintre zonele de aplicare a soluțiilor de securitate pentru care am realizat mai multe implementări o reprezintă domeniul IoT. Metodele implementate pentru securitatea IoT sunt:

- Analiza securității protocoalelor de securitate cibernetică
- Implementarea de metode de securitate cibernetică la nivelul gateway-ului IoT prin implementare hardware
- Metodă de criptografica de securizare a sistemelor pe chip (SoC - System on Chip) folosite pentru dispozitive IoT

[29] detaliază 3 direcții principale de analiză a protocoalelor IoT standard: securitate firmware, securitatea software pe toată perioada de dezvoltare (un subiect ce a evoluat înspre tehnologii de tip DevSecops) și detecția în timp real a intruziunilor.

Ca bază pentru analiza am pornit de la considerațiile de securitate din standardul CoAP, explorând modul în care acestea sunt, de asemenea, exprimate în MQTT:

1. Fără securitate (No Security)
2. Cheie pre-partajată (Pre-Shared Key)
3. Cheie publică brută (Raw Public Keys)
4. Certificate (Certificates)

- Modul "Fără securitate" este cel mai simplu de realizat, deoarece nu necesită dependențe de alte protocoale, dar este complet specific aplicației. Acest lucru implică o metodă prin care fie se utilizează un strat de rețea securizat (IPSec sau VPN), fie aplicația în sine criptează sarcinile utile și gestionează toate operațiunile de criptare / decriptare.
- Modul PSK (Cheie pre-partajată) necesită configurația inițială a secretul partajat la punctele terminale și își asumă capacitatea fiecărui dispozitiv de a menține o listă de chei. În timp ce acest lucru permite o procesare mai rapidă și o implementare relativ ușoară, lipsa secretului pre-partajat poate fi considerată critică în colectarea datelor, aplicații în care un hacker ar putea înregistra conversații criptate și apoi le-ar putea decripta mai târziu. De asemenea, este sigur să presupunem că secretul pre-partajat poate fi, de asemenea, introdus manual de către un om, mai degrabă decât generat automat, ceea ce plantează o responsabilitate uriașă asupra utilizatorului final real (dacă PSK este slab, poate fi susceptibil la atacuri de forță brută).
- Ca alternativă la PSK, RPK (RawPublicKey) poate oferi un secret perfect înainte și, de asemenea, elimină factorul uman din cheie ecuația generației. Cu toate acestea, autentificarea cheilor publice trebuie să se realizeze și printr-o metodă out-of-band (în afara benzii). Astfel, punctele finale trebuie să mențină o listă de chei publice din lista albă sau

trebuie să interogheze o entitate centru de încredere de nume de domeniu pentru a valida cheia. Acest lucru este necesar pentru a evita atacurile man-in-the-middle. Raw Public Keys reprezintă o alternativă mixtă de securitate la certificate mai grele și chei pre-partajate ușoare și încep să devină din ce în ce mai populare în rândul implementărilor TLS.

- Autentificarea și criptarea tradițională bazată pe certificate oferă cel mai înalt nivel de securitate, deoarece garantează identitatea colegilor pe baza unor furnizori de certificate bine stabiliți. În plus, posibilitatea de a revoca certificatele având în vedere utilizarea ilicită îl face mai capabil să reacționeze la diferite atacuri, așa cum s-a dovedit deja cu HTTP. Cu toate acestea, dacă ignorăm cerințele de capacitate și cheltuielile generale suplimentare din mesajele schimbate, apare o problemă de etică din cauza caracterului omniprezent al IoT: în ce măsură suntem pregătiți să predăm toate aspectele de securitate ale mașinilor, trenurilor și chiar locuințelor noastre, unui grup mic de companii de securitate, sau pentru infrastructuri critice voi folosi alternativa unor sisteme de certificate locale, dublate de existența unor sisteme de securitate hardware de tip HSM (hardware security module).

Securitatea suplimentară poate fi impusă prin transmiterea de date anonimizate (de exemplu, în loc trimiterii sintaxei notației obiectului JavaScript cu chei în text simplu - acestea pot fi pur și simplu mapate la id-urile specifice aplicației) sau folosirea unor metode de tipul criptării homomorfice. În acest fel, adevăratul sens al datelor schimbate prin ecosistemul IoT este cunoscut numai de dezvoltatorul de servicii, dar acest lucru vine cu costul performanței.
Anonimizarea singură nu poate asigura confidențialitatea datelor și trebuie utilizată în combinație cu alte tehnici de securitate, iar o securitate completa se obține acoperind toate aspectele triadei CIA.
Datorita caracterului eterogen al componentelor IoT și al multiplelor soluții de la producători diferiți ce triluiesc integrate, o soluție pentru această situație nu este banală, deoarece trebuie să se ocupe de negocierea nivelului de securitate între toate dispozitivele și ar putea acționa chiar ca un sistem de detectare a intruziunilor care filtrează traficul suspect. În acest fel, putem regândi de exemplu conceptul de casă inteligentă pentru a acționa mai degrabă ca un sistem complet autonom decât ca o colecție de senzori și actuatori capabili să reacționeze la diferite amenințări de securitate. Aceste funcții ar putea fi, desigur, distribuite de-a lungul diferitelor terminale, de aici și interesul tot mai ridicat spre utilizarea tehnologiei blockchain. Autentificarea distribuită, ca alternativă la controlul centralizat, și un consens comun între diferite resurse IoT ar putea fi cheia adevăratei securități în lumea computerelor omniprezente.
Concluzia studiului, după ce a oferit niște exemple concrete de implementare în cazul protocoalelor standard IoT, a fost ca cel mai probabil va fi necesară o combinație de algoritmi de învățare automată (behaviour analytics) și tehnici de inspecție profundă a pachetelor (dublate de accesul la sisteme de inteligenta – threat intelligence) pentru a identifica astfel de scenarii.

2.3.1. Securitate hardware pentru IoT

In [30] este detaliată o metodă de securizare a unui gateway IoT printr-o implementare hardware.
Securitatea IoT joacă un rol important în funcționalitatea corectă și eficientă a dispozitivelor interconectate. Din considerente de eficiență, o parte din prelucrarea datelor IoT este optimă pentru a fi implementată într-un mod distribuit, la marginile rețelei, la nivelul fiecărui IoT Gateway, mai degrabă decât centralizat, la nivel de Cloud. În consecință, implementările hardware ale funcțiilor de securitate, cum ar fi discriminarea și filtrarea pachetelor, devin un element esențial în arhitecturile IoT. Implementarea din [] se concentrează pe punerea în aplicare practică și teoretică a algoritmului Wu Manber de inspecție profundă a pachetelor în FPGA. Inspecția profundă a pachetelor face parte din gateway-ul IoT securizat care filtrează mesajele primite facilitând fluxul de date în siguranță între dispozitivele Edge și Cloud.

Un Gateway de securitate IoT poate acționa ca un firewall între datele colectate de la dispozitivele interconectate (senzori, sisteme pe chip SoC) și sistemele care vor stoca și procesa datele achiziționate. Un Gateway IoT îndeplinește mai multe funcții critice, de la traducerea protocoalelor la criptarea, procesarea, gestionarea și filtrarea datelor și este plasat între dispozitivele interconectate și sistemele finale. Funcția principală a Gateway-ului IoT este traducerea protocolului de la rețelele de senzori de alimentare la internet sau LAN. Acesta poate decripta, autentifica sau filtra datele primite de la dispozitivele IoT, facilitând fluxul de date în siguranță între dispozitivele Edge și Cloud. Datorită cantității mari de date transferate și prelucrate în timp real (în funcție de ecosistemul IoT), discriminarea pachetelor și operațiunile de securitate sunt optime pentru a fi implementate în hardware. Astfel, criptarea, autentificarea sau filtrarea sunt suficient de rapide pentru un transfer de date în timp real și cantitatea de informații care este redirecționată către Cloud este redusă.
În continuare se prezinta o propunere de implementare hardware, ca parte a Gateway-ului IoT, ce implementează algoritmul de căutare multi-model MPSearch (Multi-Path Search). Acesta componenta ajută Gateway-ul IoT să filtreze mesajele primite în rețeaua IoT. Filtrul Internet se bazează pe identificarea unor modele în câmpul de sarcină utilă al unui mesaj IoT. Împreună cu criptarea și autentificarea, acesta este un pas important în securizarea dispozitivelor interconectate și a comunicării dintre ele. Arhitectura propusă este prezentată în figura de mai jos:

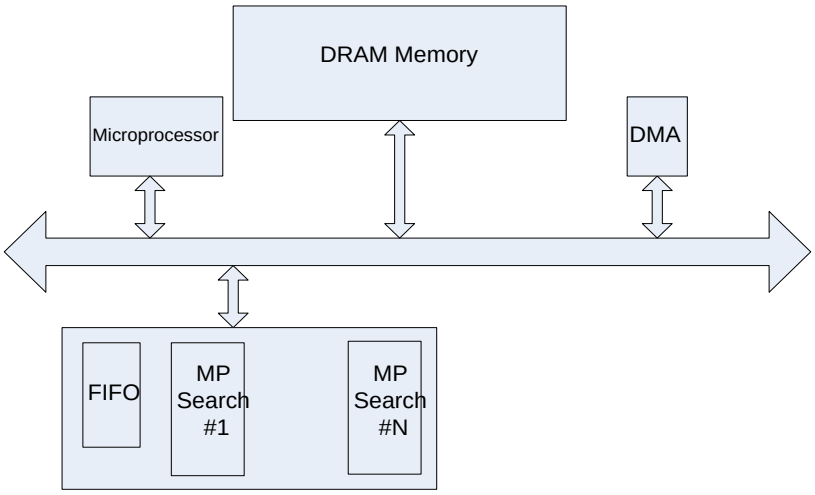


Fig. 91. Arhitectura hardware a SoC utilizată pentru implementarea algoritmului Wu Manber

Textul și modelele primite de pe Internet sau LAN sunt stocate în memoria DRAM și cu ajutorul unui DMA, o parte dintre ele sunt transmise periodic către buffer-ele nucleului IP (Intellectual Property core) hardware care implementează căutarea multi-model, MPSearch. IP core multiPatternSearch primește datele din FIFO și le prelucrează pentru a obține valorile pre-calculate necesare pentru a implementa căutarea. Având valorile pre-calculate, nucleul IP-ului numit MPSearch Slice, care implementează partea de căutare începe să ruleze. MPSearch Slice execută partea de căutare pe un text mic și numai pentru unele modele. În funcție de resursele disponibile, mai mult de o felie MPSearch pot fi utilizate pentru a realiza un flux (pipeline) de căutare multi model. Puține modele sunt căutarea în părți mici ale textului într-un mod de pipeline: primul text este procesat de felie MPSearch 1, apoi este trecut la al doilea MPSearch Slice 2; între timp, MPSearch Slice 1 primește un alt text și începe căutarea prin ele și așa mai departe (a se vedea fig. 2.2). Viteza de căutare este destul de rapid datorită implementării hardware a căutării cu mai multe modele și datorită numărului tot mai mare de felii MPSearch care pot fi utilizate. Folosind această implementare modulară ca o matrice de felii MPSearch, acesta poate fi găsit un compromis între viteza de căutare multi-model și resursele hardware disponibile. În cazul unui FPGA, reconfigurarea parțială poate fi utilizată pentru a modifica conținutul tabelelor pre-calculate în cazul unui ASIC, celulele de memorie

ar putea fi utilizate pentru a stoca aceste tabele. În ambele cazuri, zona feliilor MPSearch scade. Având în vedere că un nucleu MPSearch IP execută căutarea multi-model într-un timp maxim egal cu t_N , apoi după N * t_N toate instanțele MPSearch procesează o secvență din text. Se poate spune că lungimea totală a textului prelucrat este lungimea unei secvențe, l_{seq} înmulțită cu N. Sincronizarea dintre instanțe se realizează cu ușurință asigurându-se că toate instanțele au terminat căutarea cu mai multe modele. Timpii de execuție diferiți sunt obținuți datorită lungimilor inegale ale modelelor sau datorită numărului de potriviri ale unui model dintr-un text. Cele două protocoale de mesaje IoT, MQTT și CoAP utilizează protocoalele TCP sau UDP pentru a trimite mesajele lor. Chiar dacă limita pachetului TCP este teoretic de 64KB, unitatea maximă de transmisie este mult mai mică datorită limitei platformelor hardware ale dispozitivelor. Unitatea maximă de transmisie poate fi în jur de 1400-1500 octeți.
De aceea, o instanță MPSearch poate lua în considerare secvențe de text de dimensiune 1400-1500 octeți.

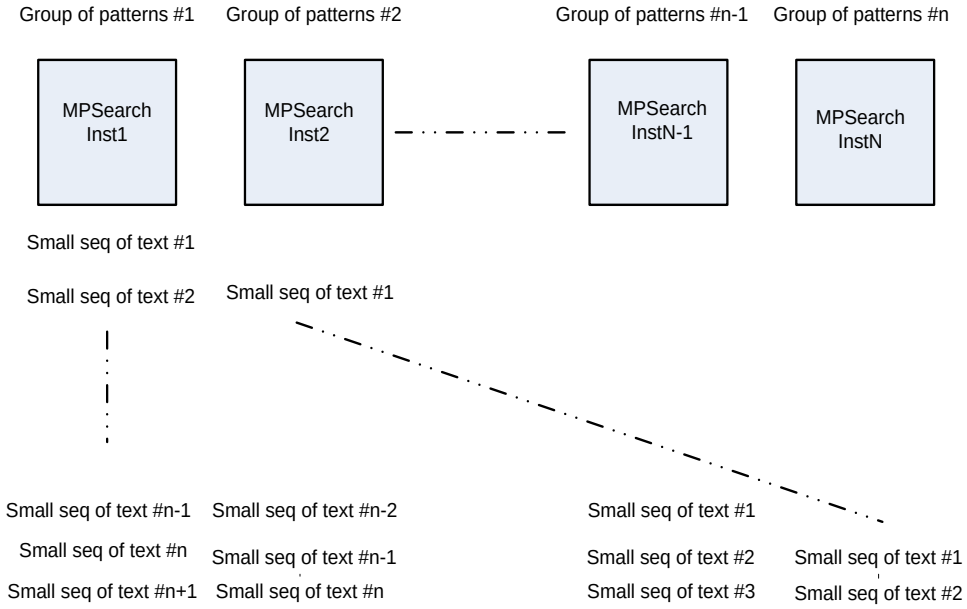


Fig. 92. Arhitectura pipeline a algoritmului Wu Manber

Implementarea mai multor algoritmi de căutare în hardware, cum ar fi Wu-Manber, crește semnificativ viteza de procesare. Un nivel MPSearch scanează un text de 1024 de caractere pentru a găsi potriviri cu un model în doar 2ms. Sunt folosite aproximativ 10 000 de bistabile pentru implementarea Wu-Manber, cele mai multe dintre ele folosite pentru a stoca subșirul de text de 1024 de caractere. Având în vedere mai mult de un model, tabelul SHIFT și timpul de parcurgere sunt în creștere, ceea ce determină o mică creștere a timpului total de căutare. Un alt avantaj al implementării hardware este că nucleul IP de căutare multi-model poate rula la o frecvență mai mare în comparație cu frecvența sistemului, ceea ce înseamnă că pachetele de procesare ajung mai lent decât sunt procesate. În cazul căutărilor cu mai multe modele, timpul de execuție nu crește considerabil.
Implementarea prezentată pentru un gateway de securitate IoT, împreună cu protocolul de criptare și autentificare, se poate utiliza pentru analiza datelor de trafic ale rețelelor și aplicațiilor, fie pentru investigații pre-atac de tip “forensics”, fie pentru analiza incidentelor în curs de desfășurare, și poate reduce volumele totale de trafic de rețea care pot duce la atacuri DdoS (Distributed denial of Service).

2.3.2. Soluție de securitate criptografică bazată pe PUF pentru sistemele IoT cu sistem pe cip SoC

Integrarea procesoarelor multicore și a perifericelor de la mai mulți furnizori de nuclee de proprietate intelectuală (IP core) ca și componente hardware ale sistemelor multiprocesoare IoT pe cip (SoC) reprezintă o sursă de vulnerabilități de securitate pentru comunicarea la nivel de cip (in-chip). Una dintre implementările de securitate SoC realizate și prezentată în [31] este ilustrativă pentru aplicațiile IoT. Mecanismul utilizat în această abordare utilizează PUF (Physical Unclonable Functions) și criptografia simetrică pentru a cripta mesajele transferate în cadrul SoC între microprocesor și perifericele sale. Mecanismul este validat experimental la nivelul FPGA, un scenariu de implementare vizat fiind pentru un dispozitiv bazat pe IoT ARM.

Diversitatea și numărul crescut de elemente IoT și furnizorii care implementează nuclee SoC și IP combinate la nivelul stațiilor de lucru IoT (de exemplu ARM, Altair Semiconductors, Qualcomm) introduc unele breșe și vulnerabilități specifice de securitate. Contramăsurile de securitate implementate la nivel de software nu sunt suficiente; un mecanism de securitate ar trebui, de asemenea, să fie luat în considerare la nivelul hardware al SoC, care mai târziu va fi utilizat în dispozitivul IoT. Unele dintre soc-uri includ nuclee IP criptografice implementate la nivel hardware care pot fi responsabile pentru generarea unei chei criptografice publice, decriptarea/criptarea unui mesaj primit/trimis prin rețea de pe un alt dispozitiv sau poarta rețelei.

Mecanismul criptografic propus introduce două operațiuni, criptarea și autentificarea, care sunt traduse la nivelul SoC între nucleele microprocesoarelor și periferice. Cele două operațiuni criptografice utilizează circuite PUF (funcții fizice neclonabile). Inspirate de biometrie, PUF-urile oferă o modalitate unică de a identifica circuitele integrate și pot fi folosite ca metodă de protecție împotriva unor atacuri de securitate, cum ar fi: troieni hardware, bus snooping sau inserții malware.

Comparabile într-un mod simplist cu o "amprentă unică" a unui IC care diferențiază un IC de altul (deși aparent identic), PUF-urile exploatează variabilitatea inerentă în fabricarea circuitelor integrate pentru a implementa funcții de răspuns la provocare a căror ieșire depinde de intrare și de micro-structura fizică a dispozitivului. Unele operațiuni, critice din punct de vedere al securității, în care PUF ar putea servi drept identificator unic ca parte a implementării IoT sunt: autentificarea, integritatea datelor, controlul accesului și confidențialitatea. Circuitul PUF utilizat pentru prototipul experimental FPGA, validând mecanismul propus, este oscilatorul inelar PUF (RO PUF).

Un dispozitiv conectat la Internet este susceptibil la atacuri la diferite niveluri:

1) comunicații (man in the middle, weak random number generator, code vulnerabilities);
2) servicii de securitate (code downgrade, change of ownership or environment, factory oversupply);
3) atacuri fizice (non-invasive attacks: clock or power glitch, side channel attacks; invasive attacks: package removal—microprobe station);
4) software (buffer overflows; interrupts; malware).

Clasificarea atacurilor este prezentată în figura de mai jos:

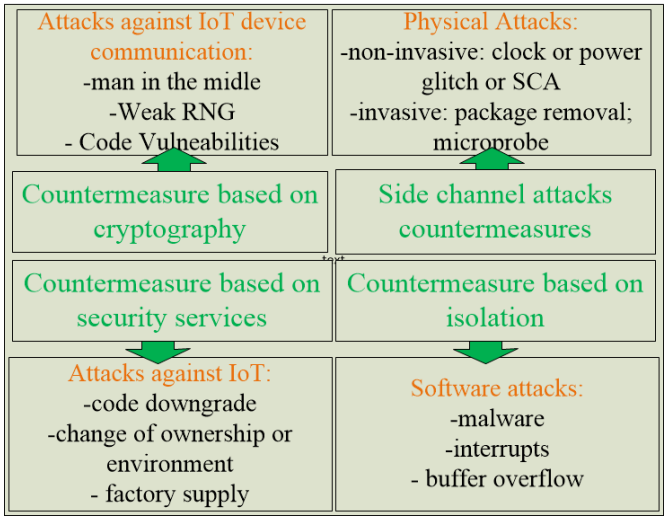


Fig. 93. Clasificarea atacurilor de securitate

Având în vedere clasificarea prezentată mai sus, atacurile fizice (categoria a 3-a) și cele software (categoria a 4-a) pot fi oprite prin metoda introdusă, bazată pe PUF.

Mecanismul de securitate este validat printr-un prototip FPGA (Field-Programmable Gate Array) care arată: i) implementarea și validarea a două operațiuni de securitate (criptare și autentificare) la nivelul SoC între microprocesoare și periferice; ii) utilizarea cheilor secrete PUF cu algoritmi criptografici simetrici care elimină cerința unui canal securizat pentru a transfera cheia secretă în diferite nuclee IP; iii) analiza mecanismului propus din punct de vedere al performantei și al resurselor hardware.

Toate implementările au fost realizate pe Xilinx Virtex 4 FPGA - dispozitivele XC4VSX35.

Metoda introdusă își propune să analizeze și să valideze experimental utilizarea operațiunilor bazate pe criptografic (criptare/decriptare, autentificare) în interiorul SoC-urilor IoT cu costuri minime în ceea ce privește resursele hardware necesare pentru performanță.

Criptarea utilizată pentru securizarea datelor transferate prin magistrala internă sau stocate în registre periferice sau în memorie se bazează pe criptarea unică a pad-ului. Pad-ul unic (cheia criptografică) utilizat pentru criptare este generat folosind circuite PUF și cifru de flux Salsa. Adresa de memorie este implicată în calculul pad-ului unic atunci când vine vorba de securizarea datelor stocate.

Mecanismul se bazează pe metodologia descrisă mai jos:

- Determinarea perifericelor SoC critice

- Nucleele IP care procesează informații sensibile vor deține mecanismul criptografic. Datele citite sau scrise din nucleele IP critice sunt criptate.

- Generarea cheilor secrete PUF

- Cheia secretă este generată folosind circuite PUF și algoritmul Salsa 20/20. Salsa 20/20 este o funcție pseudo-random bazată pe operațiuni add-rotate-xor. Algoritmul mapează o cheie de 256 de biți, un nonce pe 64 de biți și un contor de 64 de biți la un bloc de 512 biți al fluxului de chei. Algoritmul generează un flux de secvențe binare pseudo-random (blocuri de 512 biți) care pot fi utilizate ca chei criptate pentru criptarea pad-ului unic.

- Criptare și decriptare

Figura de mai jos prezintă mecanismul general de criptare care implică microprocesorul și un periferic din interiorul unui domeniu critic. Cheia secretă este o cheie pseudo-random generată cu ajutorul răspunsurilor PUF și a cifrului fluxului pseudo-random Salsa 20/20. Atât microprocesorul, cât și perifericul au acces ușor (conexiuni directe) la răspunsurile PUF și au, de asemenea, un înveliș care conține cifrul fluxului pseudo-random Salsa20/20. Nucleul IP din figura 94 este un periferic critic care procesează informații critice, astfel încât operațiunile de citire și scriere dintre

microprocesor și registrele periferice să fie criptate. Deoarece ambele periferice au conexiuni directe la ieșirea circuitelor PUF, nu este nevoie de un canal sigur pentru a transmite o cheie secretă, eliminând dezavantajul criptografiei simetrice. Celelalte periferice care nu au voie să utilizeze informațiile critice nu au acces la circuitele PUF și nici la cifrul fluxului Salsa 20/20. În același mod, datele scrise în memoria sistemului sau citite din memorie pot fi criptate utilizând criptarea unică a pad-ului. Adresa de memorie va fi utilizată de funcția Salsa 20/20 (ca valoare contor de 64 de biți) pentru a genera aceeași cheie pentru operațiunile de criptare/decriptare (Figura 95).

Dacă SoC este complex, pot fi luate în considerare domenii mai critice: fiecare domeniu conține perifericele care comunică între ele și fiecare domeniu va avea o cheie unică generată cu circuite PUF.

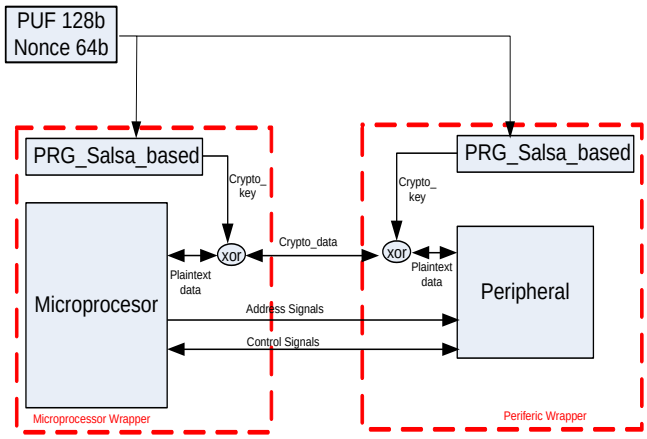


Fig. 94. Schema de criptare între microprocesor și periferice.

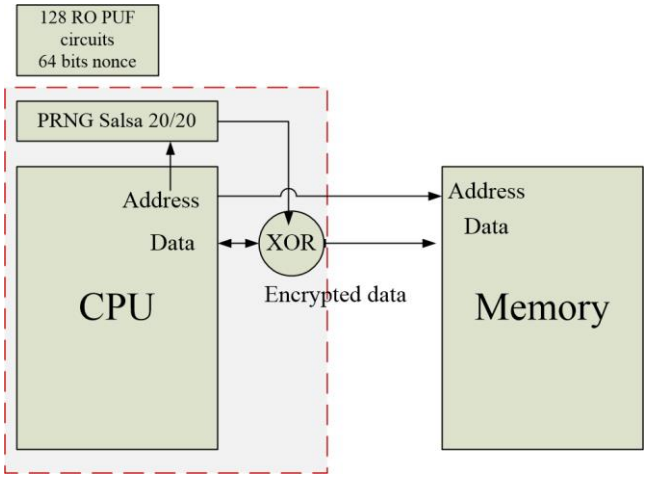


Fig. 95. Schema de criptare între microprocesor și memoria sistemului

- Autentificarea nucleelor IP

- Acest pas presupune completarea învelișului de lângă periferice și microprocesor cu registrele binare necesare pentru autentificarea unui miez IP (marcat cu linie punctată în Figura 94). Autentificarea se bazează pe cunoașterea aceleiași chei pseudo-random. Dacă două nuclee IP au voie să facă schimb de date, învelișurile lor vor genera aceleași secvențe de pseudo-random. Microprocesorul dintr-un domeniu poate citi o valoare de biți mixtă a unei chei pseudo-random și o poate compara cu valoarea sa de un bit mixt. Confirmarea identității sursei de date contribuie, de-a lungul operațiunilor de criptare/decriptare, la contracararea amenințărilor la adresa securității.

Mecanismul propus se poate alătura cu ușurință SoC ARM. Circuitele PUF sunt implementate pe o parte a matriței de siliciu, în timp ce învelișul de criptare poate fi adăugat la nucleele IP, conectate pe interfața de date.

Am analizat posibilitatea de a integra elementele de criptare de securitate compus din circuite PUF și Salsa PRG pe sistemul de evaluare a pornirii designului ARM 3 Cortex furnizat de ARM. Cortex-M3 DesignStart Eval oferă dezvoltatorilor o modalitate ușoară de a dezvolta și simula modele SoC bazate pe procesorul ARM Cortex-M3. Designul ARM 3 Cortex este prezentat în figura de mai jos:

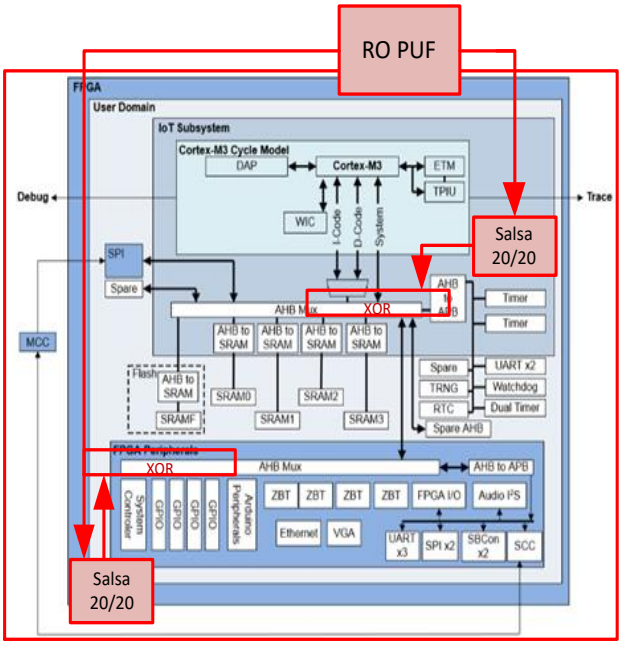


Fig. 96 ARM 3 Cortex DesignStart Eval

În timp ce majoritatea conceptelor de securitate IoT abordează comunicarea dintre elementele IoT, mecanismul propus vizează securitatea comunicării dintre nucleele IP din interiorul unui SoC IoT. Implementarea hardware propusă în lucrare poate fi extinsă cu ușurință pentru a găzdui soc-uri mai complexe, cu un număr crescut de periferice și interfețe, inclusiv nuclee IP radio specifice IoT.

2.4.Soluții pro-active pentru criminalistică digitală

Criminalistica digitală (IT Forensics) este descrisă ca parte a științei criminalistice care se concentrează pe investigarea și examinarea artefactelor colectate de pe dispozitivele electronice. Pe de altă parte, Institutul Național de Tehnologie a Standardelor (NIST) o explică ca fiind "aplicarea științei la identificarea, colectarea, examinarea și analiza datelor, păstrând în același timp integritatea informațiilor și menținând un lanț strict de custodie a datelor". Criminalistica pro-activă poate fi descrisă ca proiectarea și configurarea sistemelor pentru a face organizația receptivă la investigațiile digitale în viitor.

Implementarea realizată în [32] a avut drept scop analiza investigațiilor criminalistice digitale pro-active prin valorificarea simulării/emulării adversarului într-un mediu virtualizat. Emularea adversarului este o implicare a echipei care simulează amenințările cunoscute pentru a determina acțiunile și comportamentele atacatorilor. De acum înainte, obiectivele cercetării constau în a permite monitorizarea criminalistică a terminalelor (endpoints), emularea adversarului,

automatizarea identificării și colectării artefactelor criminalistice digitale și, în cele din urmă, examinarea încrucișată a probelor obținute de la dispozitivele de rețea și terminale endpoint.

Infrastructura digitală de criminalistică și de răspuns la incidență (hardware și software) este instalată în avans, anticipând incidente viitoare care ar putea necesita acces rapid la artefacte de probe electronice pentru investigații. Figura de mai jos ilustrează conceptul pro-activ de criminalistică digitală folosind o diagramă a fluxului de proces.

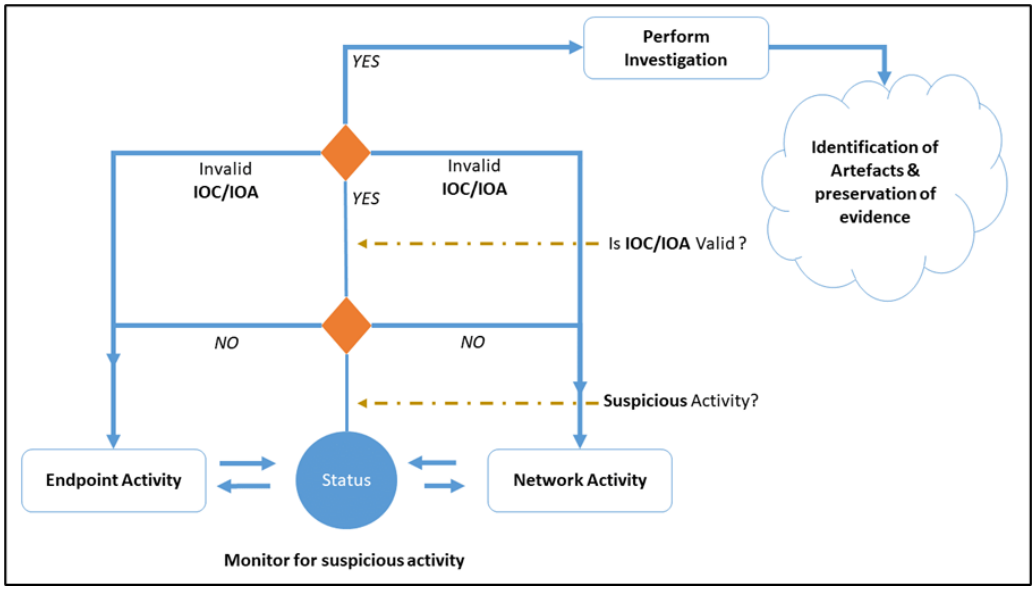


Fig. 97 Un model conceptual pentru criminalistica digitală pro-activă

Investigația criminalistică digitală pro-activă începe cu monitorizarea rețelelor și a stațiilor de lucru în cazul în care un server de monitorizare asistat printr-un agent (în cazul terminalelor HIDS – Host Intrusion Detecyion System) sau un punct de detecție („network tap") de rețea (în cazul NIDS - Network Intrusion Detection System) comunică în mod constant printr-o rețea în căutarea unui comportament suspect. Starea corespunde unei alerte sau unei notificări primite, iar anchetatorul medico-legal verifică dacă este pozitiv, fals pozitiv, negativ sau fals negativ. Investigatorul verifică dacă există sau nu un indicator de compromis (IOC), dacă da, atunci începe o anchetă fie în rețea și/sau pe terminal. Identificarea artefactelor este automată în atacurile cunoscute, ceea ce face mai ușor pentru investigatorul criminalist să extragă și să păstreze probele. Investigația este efectuată pe lângă monitorizarea securității, unde vizibilitatea este crescută atât pe rețea, cât și pe dispozitivele terminale.

Topologia experimentala are 3 părți: atacatorul, Internetul și rețeaua internă. Implementarea utilizează mașina virtuală Kali Linux ca instrument de testare a penetrării. Rețeaua și gazda pentru regiunea de atac sunt notate cu un fundal roșu, urmat de regiunea albastră care reprezintă Internetul. Ultima regiune este o rețea internă simulată și gazdele respective. Pe marginile regiunii de atac și a rețelei interne sunt două routere. Routerele virtualizate Vyos sunt folosite pentru a crea o rețea WAN. În rețeaua internă, există un comutator care conectează serverul web Linux, Windows Server și stația de lucru Analist.

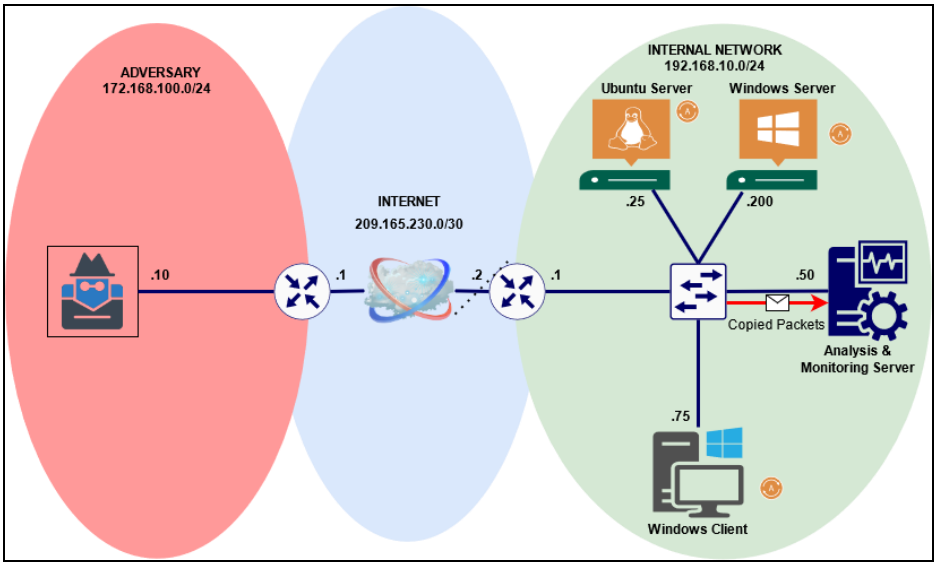


Fig. 98 Topologie experimentală pentru criminalistica digitală pro-activă

Au fost implementate instrumente de emulare a adversarului, cum ar fi cadrul Metasploit, Covenant C2, Imperiul PowerShell, Nmap, hydra și scripturile personalizate. Ca răspuns la atacurile lansate, au fost configurate și efectuate software-uri de criminalistică digitală și răspuns la incidență (DFIR -Digital Forensics Incident Response), cum ar fi Suricata (NIDS), Wazuh (HIDS), WireShark și CapME (susținute de Stenographer), stiva ELK și Velociraptor Digital Forensics/EDR (Endpoint Detection and Response).

Cercetarea a avut patru obiective dintre care trei au fost îndeplinite, iar ultimul a fost parțial îndeplinit:

- Primul obiectiv a fost acela de a permite monitorizarea criminalistică a punctelor finale, iar acest lucru a fost realizat prin crearea unui mediu de rețea virtualizat care a simulat rețelele din lumea reală. Această configurație de virtualizare a fost compusă din software de emulare adversar, precum și de monitorizare a securității și instrumente criminalistice digitale. Analistul a configurat NIDS și HIDS și a implementat agenți în sistemele care urmau să fie monitorizate. Software-ul de criminalistică digitală velociraptor/Endpoint Detection and Response a fost instalat pe serverul de monitorizare, iar agenții au fost implementați pe mașini virtuale client/server. Prin acțiunile menționate mai sus, a fost stabilit primul pas al modelului pro-activ de criminalistică digitală, care este pregătirea pentru infrastructură și capacitățile sporite de detectare a incidentelor. În mod substanțial, monitorizarea criminalistică a stațiilor de lucru a făcut posibilă îndeplinirea fără efort a funcțiilor criminalistice digitale, cum ar fi reducerea, examinarea, colaționarea și reconstituirea probelor de la dispozitivele de rețea și de la dispozitivele endpoint, permițând astfel analistului să își îndeplinească sarcinile în mod eficient, obținând în același timp dovezi digitale cuprinzătoare.
- Al doilea obiectiv a fost de a emula adversarul care imită tacticile, tehnicile și procedurile utilizate de adversari în compromiterea rețelelor și sistemelor. S-a reușit reproducerea a șapte (7) tehnici de emulare a adversarului împreună cu cadrul matricilor Mitre ATT&CK. Din motive ilustrative, un singur scenariu de atac a fost documentat și demonstrat. Printre fazele implementate, se poate menționa faza de recunoaștere, accesul inițial, executarea și persistența codului, escaladarea privilegiilor, accesul la credențiale, descoperirea și mișcarea laterală, C2 și ex-filtrarea datelor [27]. Această tehnică a permis explorarea diverselor tehnici de atac, ca rezultat nu numai evaluarea modului în care acestea sunt investigate, dar efectuarea investigației în sine. Au fost discutate mai multe concepte criminalistice digitale, de la sisteme de fișiere, criminalistică de memorie și criminalistică de rețea, oferind astfel o evaluare detaliată a criminalisticii digitale pro-active.

- Al treilea obiectiv a fost automatizarea identificării și colectării artefactelor digitale. Automatizarea identificării și colectării artefactelor digitale s-a făcut de către NIDS fiind asistat de Stenographer un software complet de captare a pachetelor. În timpul experimentelor de laborator, s-a observat că automatizarea componentei de identificare a îmbunătățit capacitățile de investigație ale analistului, făcând mai eficientă extragerea artefactelor digitale. În plus, criminalistica digitală Velociraptor/EDR a fost foarte inventivă în efectuarea investigațiilor medico-legale asupra punctului final, în special în obținerea de probe în direct printr-o rețea. Cu toate acestea, extracția artefactului a avut nevoie de un analist pentru a examina și colecta artefactele digitale. Prin urmare, s-a ajuns la concluzia că colectarea automată a artefactelor digitale se poate face într-o anumită măsură, adică prin capacități de detecție îmbunătățite. Ca urmare, eforturile de automatizare ar trebui să se concentreze pe detectarea și conservarea, în timp ce investigația criminalistică digitală în sine este efectuată de un investigator criminalist folosind cunoștințele și abilitățile lor, precum și software specializat.
- Ultimul obiectiv a fost de a examina încrucișat dovezile digitale găsite din surse de rețea cu cele provenite de la dispozitivele endpoint, în vederea coroborării dovezilor din ambele perspective. S-a observat că abordarea a oferit o perspectivă solidă și coerență între artefactele digitale găsite în rețea și dispozitivele endpoint, eliminând astfel orice îndoială că s-a întâmplat într-adevăr un incident. În unele experimente s-a observat că mai multe artefacte au fost găsite pe punctul final, spre deosebire de rețea și invers. Prin urmare, dovezi atât de la rețea, cât și de la dispozitivele endpoint vor permite unui analist să observe ceea ce s-a întâmplat cu adevărat.

2.5.Soluții de prevenire a atacurilor bazate pe inginerie software

91% din toate atacurile cibernetice încep cu un e-mail de *phishing* către o victimă neașteptată, conform unei raport Delloite. Scopul acestei cercetări, descrise în [33], este de a demonstra metoda de implementare a unei arhitecturi phishing as a service (PhaaS) și a unui atac omograf (homograph attack) cu un nume de domeniu internaționalizat (IDN - Internationalized Domain Name), adică folosind un domeniu similar de nivel superior, într-o campanie reală de phishing. Campania oficială a vizat studenții de la Universitatea "Transilvania" din Brașov – într-o campanie oficială de phishing aprobată de departamentul IT al universității, în cadrul unei campanii informative privind securitatea cibernetică. În cele ce urmează voi descrie succint implementarea (platforma, instrumentele și metodologiile implementate utilizate pentru verificarea nivelului de conștientizare pentru acest tip de atac), campania fiind evaluată în funcție de numărul de utilizatori care își transmit datele confidențiale care ar putea compromite unul sau mai multe sisteme.
Campania de phishing se bazează pe o arhitectură dedicată care utilizează diferite instrumente specifice, prezentate mai jos:
A – Domeniul a fost selectat folosind DNStwist.
DNS fuzzing este un flux de lucru automat pentru descoperirea domeniilor potențial rău intenționate care vizează o organizație. Acest instrument funcționează generând o listă mare de permutări bazate pe un nume de domeniu pe care îl furnizați și apoi verificând dacă oricare dintre aceste permutări sunt în uz. În plus, poate genera hash-uri neclare ale paginilor web pentru a vedea dacă acestea fac parte dintr-un atac de phishing în curs de desfășurare sau uzurparea identității mărcii și multe altele.

Fig. 99 Domeniile generate de instrumentul dnstwist arată cea mai mare rată de succes a unui domeniu care utilizează în viitoarele atacuri de phishing. Pagina de control cPanel este utilizată în campania de phishing.

Folosind DNStwist, am selectat domeniul unit-bv.ro ca domeniu principal utilizat pentru campania de phishing.

B – PhaaS (Phishing as a Service platform)

Gophish a fost selectat pentru a fi platforma de phishing. Gophish este un cadru de phishing puternic, open-source, care facilitează testarea expunerii organizației la phishing.

C - Servicii de găzduire și panou de control

Pentru testele de phishing am folosit un serviciu de găzduire, oferind un cPanel și un IP dedicat pentru teste modificarea înregistrărilor DNS pentru autentificarea prin e-mail sau, pentru gestionarea subdomeniilor care ar putea fi utilizate o campanie de phishing, verificarea și implementarea fiecărui detaliu legat de campania de phishing, inclusiv diferite teste pentru creșterea scorului de livrare a corespondenței.

D. Reputation service checker

Se utilizează un *serviciu de reputație* care măsoară reputația domeniului și oferă sugestii de îmbunătățire a capacității de distribuție (”livrabilității”) în cadrul campaniei de phishing [10].

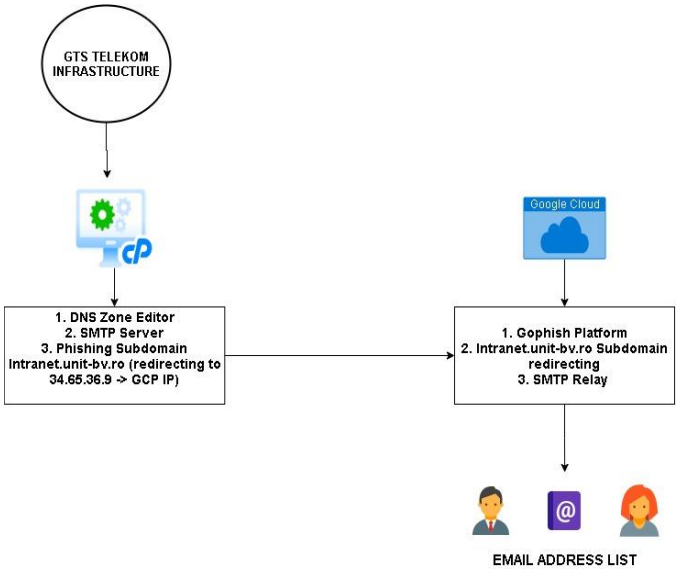


Fig. 100 Prezentare generală a arhitecturii campaniei de phishing, domeniul a fost găzduit în infrastructura GTS Telekom

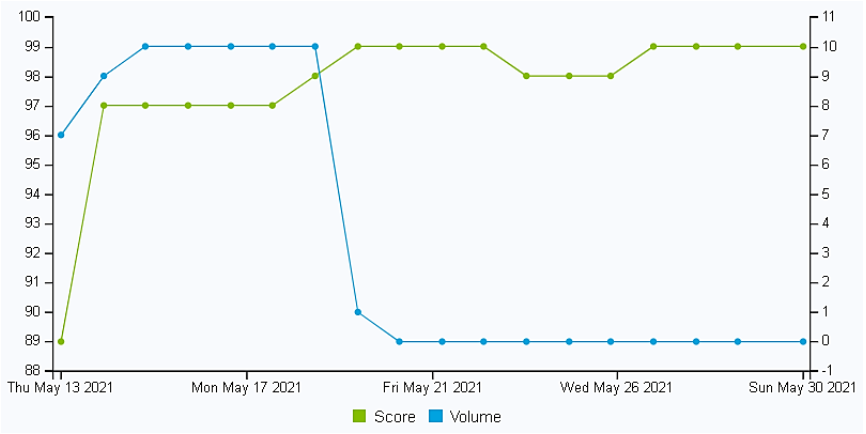


Fig. 101 În imaginea de mai sus putem vedea o livrare a corespondenței în creștere de la data începerii campaniei până la data de 30/05/2021. Campania a inclus crearea de e-mailuri de phishing și emularea site-ului web clonă (s-a clonat site-ul de intranet al universității) unde studenții erau rugați să își introducă credentialale.

Am obținut următoarele rezultate, în cadrul campaniei oficiale de phishing (faza 1) de la Universitatea "Transilvania":

1. Data: 14 mai 2021 - 17 mai 2021
2. Trimite mail-uri: 16185
3. Mail-uri deschise: 456
4. Click pe link-ul: 314
5. Date cu caracter personal transmise: 272
6. Rata de succes = datele trimise la sută din e-mailurile deschise = > 59.65

Rezultatele indică faptul că mulți studenți au accesat link-urile și mai mult de jumătate dintre cei care accesează link-ul și-au introdus, de asemenea, credențialele. Trebuie luat în considerare faptul că aceasta este evaluarea pre-formare și că profilurile studenților sunt limitate, astfel încât expunerea la servicii dată de acreditările studenților este, de asemenea, limitată. Cu toate acestea, în cazul în care credențialele pentru utilizatorii cu profiluri îmbunătățite sunt furate, acesta poate fi sursa altor atacuri rău intenționate.

Cadrul oferă posibilitatea de a vedea acreditările utilizatorilor care au fost victime. Aceste victime vor fi notificate cu privire la încălcare și li se va cere să își schimbe datele de acreditare.

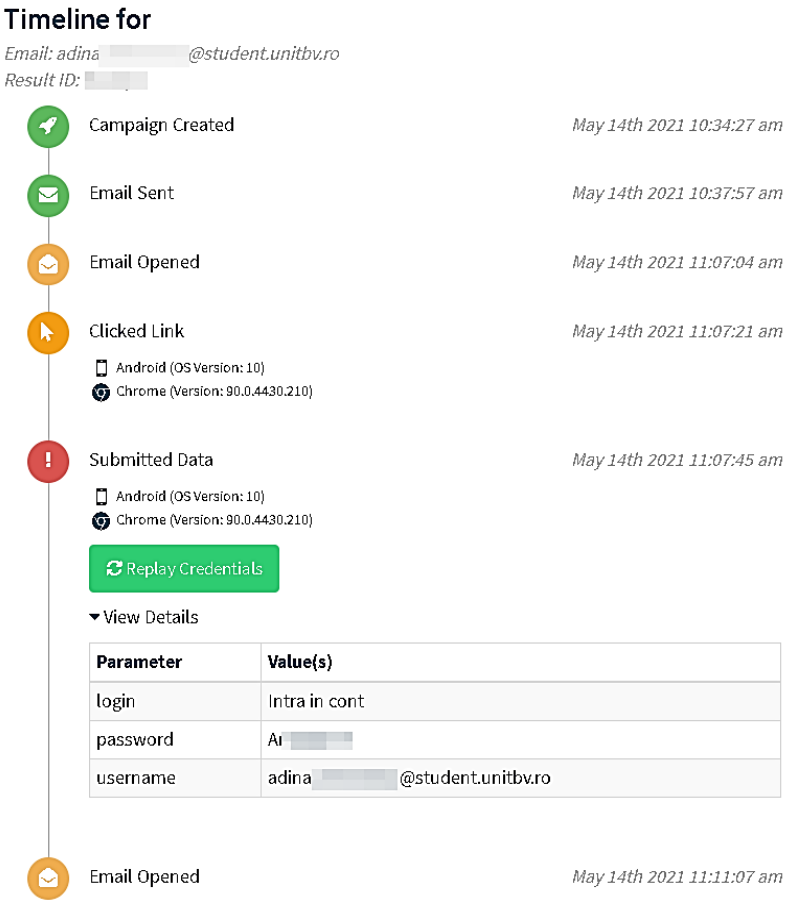


Fig. 102 Dovada detaliilor inserate, a numelui de utilizator și a parolei pentru o anumită victimă

3. Integrarea de elemente de inteligență artificială în sisteme de calcul și comunicații

Sistemele de calcul și comunicații au crescut în complexitate pana la un nivel la care, pentru a putea face fata cererilor de servicii ad-hoc, mai ales sub paradigma „as-a-service” și cerințelor crescute de procesare și de securitate au avut nevoie de aportul adițional al inteligenței artificiale. Inteligența artificială poate fi integrată la diverse nivele decizionale în sistemele de calcul și comunicații, observându-se în timp migrarea puterii de procesare din modele centralizate (Cloud) spre elemente de la periferie (Edge) sau spre suportul unor elemente IoT distribuite.

3.1.Analiză și asistență decizională pentru aplicații IoT în agricultură inteligentă

Una dintre implementările realizate în cadrul proiectului european H2020 SARMENTI reprezintă integrarea unor elemente de comunicații și inteligență pentru eAgricultură sau agricultură asistată, realizări prezentate și în [34], [35].

Agricultura inteligentă, bazată pe noi tipuri de senzori, analiză de date și automatizare, este un factor important pentru optimizarea randamentelor și maximizarea eficienței pentru a alimenta populația în creștere a lumii, limitând în același timp poluarea mediului. Scopul cercetării a fost de a implementa un sistem multi-senzor Internet of Things (IoT) pentru agricultură constând dintr-o sondă de sol, o sondă de aer și un înregistrator inteligent de date. Detaliile de implementare se concentrează pe elementul de integrare și pe senzorul inovator de identificare a gazelor bazat pe inteligența artificială. Contribuția autorului tezei se concentrează în zona de implementare a sistemului de analiză și sprijin decizional, care oferă recomandări agricole și este îmbunătățit cu o buclă de feedback din partea fermierilor și un indice de încredere socială care va crește fiabilitatea sistemului.

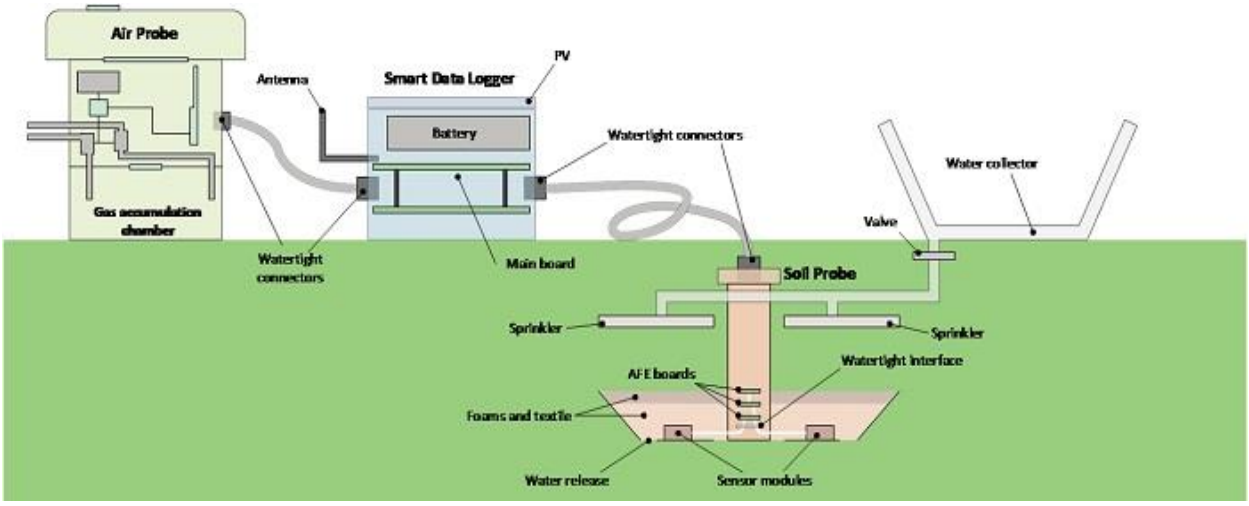


Fig. 103 Privire de ansamblu sistem inteligent SARMENTI, conform [34]

3.1.1. Analiză și asistență decizională

În proiectul SARMENTI, partea de analiză propune inspectarea datelor produse și transmise de senzori (sol și aer) și alte dispozitive conectate (stații meteorologice, drone aeriene), împreună cu seturi de date disponibile anterior și know-how-ul fermierilor. Scopul este de a descoperi și înțelege

conexiunile dintre seturile de date și apoi de a sprijini utilizatorii (fermierii) cu sprijin decizional prin predicții și prescripții.
Analiza și sprijinul decizional se bazează pe un model conceptual care ia în considerare diverse date de intrare, cum ar fi un model de evoluție a plantelor și factori de mediu, seturi de date istorice etc.
Evoluția plantelor este un subiect holistic care implică factori din mai multe domenii. Unele studii afirmă că disponibilitatea azotului (N) și/sau a fosforului (P) poate influența creșterea plantelor în majoritatea ecosistemelor, prin urmare modelul conceptual inițial al plantelor se concentrează pe una dintre componentele dominante, N. Utilizarea eficientă a îngrășămintelor ar putea avea un impact important atât asupra mediului natural, cât și asupra câștigurilor comerciale. Scăderea cu 1% a utilizării îngrășămintelor N singur este estimat să conducă la economii anuale de 1,1 miliarde dolari.

Modelul de predicție este o problemă multidisciplinară care trebuie să ia în considerare factorii majori de impact asupra creșterii plantelor. Pentru efectuarea analizei predictive, modelul de proces numit Cross Industry Standard Process for Data Mining (CRISP-DM) este utilizat în lucrarea de față.

În timpul dezvoltării modelelor inițiale de plante, au fost identificați mai mulți factori care influențează direct creșterea plantelor. Modelele inițiale ale fabricii vor lua în considerare acești factori de influență iterativ, în faza de dezvoltare a prototipului:

- Vremea: probabil, unul dintre cei mai importanți factori de mediu care influențează ciclul de viață al culturilor este vremea. Este de preferat să aveți acces la datele meteorologice cât mai aproape de locația fermei, prin urmare este analizată opțiunea de utilizare a stațiilor meteorologice locale;
- Date privind senzorii de sol: disponibilitatea nutrienților în sol va avea un impact uriaș asupra modelului de creștere a plantelor. Modelul de predicție va lua în considerare aceste valori ale nutrienților, împreună cu propriile interconexiuni, de exemplu, influențarea substanțială a pH-ului nutrienților disponibili pentru plante.
  - Nodul SARMENTI va oferi două seturi redundante de senzori de sol. Prin urmare, după faza de calibrare și validare, modelele pot lua în considerare fie utilizarea ambelor puncte de date, fie utilizarea celui mai stabil senzor pentru intervale specifice;
- Date privind sonda de aer: sonda de aer poate oferi indicații cu privire la pierderea nutrienților specifici prin emisiile gazoase, care reprezintă o pierdere de nutrienți pentru plante și poate fi un factor foarte important de poluare a aerului;
- Teledetecția spectrală: cele mai recente progrese în dezvoltarea agriculturii implică utilizarea de vehicule aeriene fără pilot (UAV- uri) capabile de măsurători multi-spectrale sau chiar hiper-spectrale de teledetecție pentru agricultură. Este important să se ia în considerare acest tip de intrare în modelul de decizie / predicție. Dacă fermierii posedă o astfel de tehnologie, ei pot oferi rezultatele ca input în modelul de evoluție a plantelor. Aceste tipuri de măsurători ar putea fi utilizate pentru a măsura variabile precum starea solului, sănătatea plantelor și îngrășămintele;
- Feedback-ul fermierului: fermierul va fi în măsură să furnizeze contribuții legate de:
  1. Plante care ating reperele;
  2. Îngrășăminte: dacă s-au aplicat îngrășăminte, dacă da, ce fel (natural, artificial), compoziție, cantitate. În funcție de aceste aspecte, trebuie utilizat modelul de descompunere a îngrășămintelor.
  - Această intrare va permite sistemului să calibreze modelul cu adevărul real al solului și, de asemenea, în timp pentru a calibra modelul teoretic al instalației pentru condițiile specifice ale fermei, obținând astfel o precizie mai bună;
- Feedback social de la ferme similare: Analiza între ferme va fi inclusă în algoritmul de învățare automată, în special pentru fermele similare: dimensiune, locație, tip de sol, culturi. Această caracteristică va fi detaliată în secțiunea următoare.

3.1.2. Platforma de analiză a datelor

Platforma back-end server se bazează pe Atos Codex Datalake Engine, care este o soluție Cloudera complet integrată. Sistemul oferă mijloacele de colectare a datelor de pe dispozitivele conectate la Internet. Acesta acționează ca un hub de date inteligent, gestionând analizele și direcționând fluxurile de date către aplicațiile specificate pentru utilizarea eficientă a serviciilor.

După cum este descris în figura 104, componentele software cheie sunt: platforma de virtualizare Open Stack, sistemul de operare redHat pentru întreprinderi, Cloudera Manager pentru hadoop File System, StreamSets pentru ingestia și curățarea flexibilă a datelor, stocarea datelor brute în sistemul de fișiere Hadoop cu replicare SW, curățarea datelor, transformarea prin Jupyter în timpul buclei de știință a datelor, prelucrarea distribuită a datelor și analiza prin Apache Spark2, Servirea și prezentarea datelor cu ElasticSearch și Kibana.

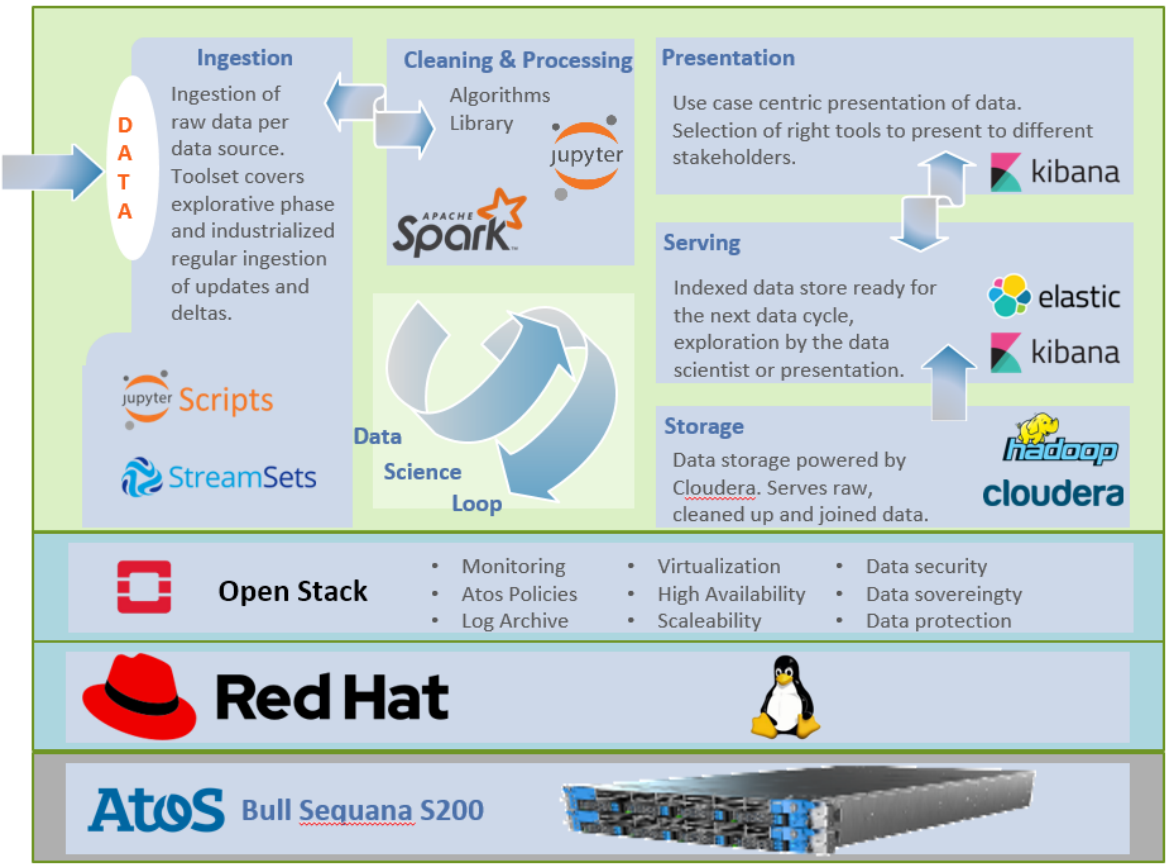


Fig. 104 Stiva software de analiză a datelor și bucla de știință a datelor.

Bucla de prelucrare/analiză date se bazează pe un proces ETL tipic: extragere, transformare, încărcare. Acest lucru permite ingestia de date brute, curățarea și pre-procesarea datelor înainte de a fi disponibile pentru vizualizare, precum și pentru prelucrarea de către algoritmii de predicție și prescripție. Această buclă prelucrare/analiză datelor permite iterarea rezultatelor analizei împreună cu utilizatorii experți (parteneri de proiect agricol).

Figura 105 detaliază proiectarea platformei de analiză în arhitectura SARMENTI. De asemenea, descrie căile de comunicare și protocoalele dintre dispozitivele IoT și platforma de analiză.

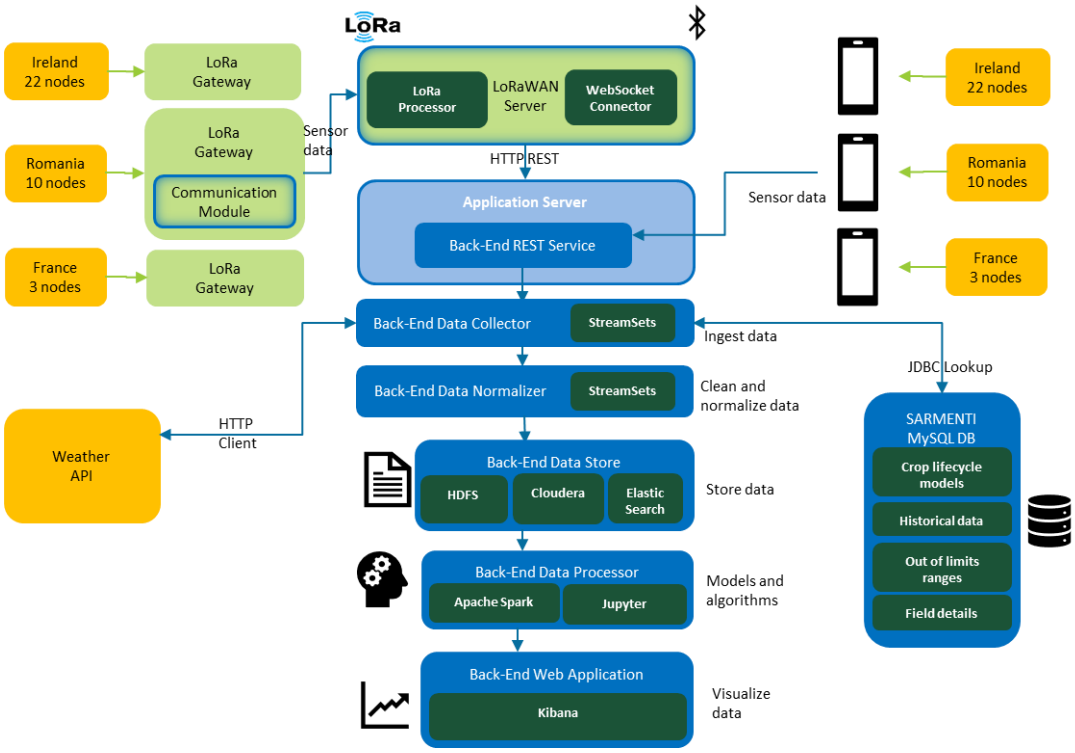


Fig. 105 Platforma de analiză și căile de comunicare de pe dispozitivele IoT.

3.1.3. Bucla de feedback social și indicele de încredere pentru modelul de decizie și predicție

Într-o abordare simplă de analiză a datelor, toate punctele de date sunt egale, ceea ce ar putea fi aplicat și pentru SARMENTI. Fiecare nod este practic identic: același număr de senzori, aceeași calitate a ieșirii dacă calibrarea și corecțiile de derivă au succes, aceleași protocoale de comunicare. Dar, de fapt apar diferențe ce pot fi cauzate de exemplu de nodurile cu senzori defecți, adâncimea diferită a senzorului de sol, tipul sau panta diferită a câmpului, influențate de evenimente externe etc., ar putea duce la corelații false sau pot influența în mod greșit suportul decizional. Împreună cu diversitatea plantelor cultivate și cu nevoile și caracteristicile lor specifice, complexitatea analizelor crește exponențial.

Acest lucru ar putea fi rezolvat prin simpla accesare a mai multor date pentru a acoperi fiecare scenariu posibil cu suficiente puncte de date. Din păcate, SARMENTI poate oferi doar câteva puncte de date zilnice pentru fiecare tip de plantă abordată, dar are acces la cunoștințele unor parteneri agricoli excelenți care pot oferi informații valoroase.

Prin urmare, Indicele de încredere a fost creat pentru seria de date, care, în versiunea sa inițială actuală include relevanța punctului de date, fiabilitatea senzorilor care l-au produs și un feedback social.

Indicele de încredere – aflat în prezent în stadiul său inițial – include trei componente principale, așa cum este ilustrat în figura 106 într-o formă simplificată:

1. Relevanța punctului de date
2. Fiabilitatea senzorului
3. Feedback-ul social

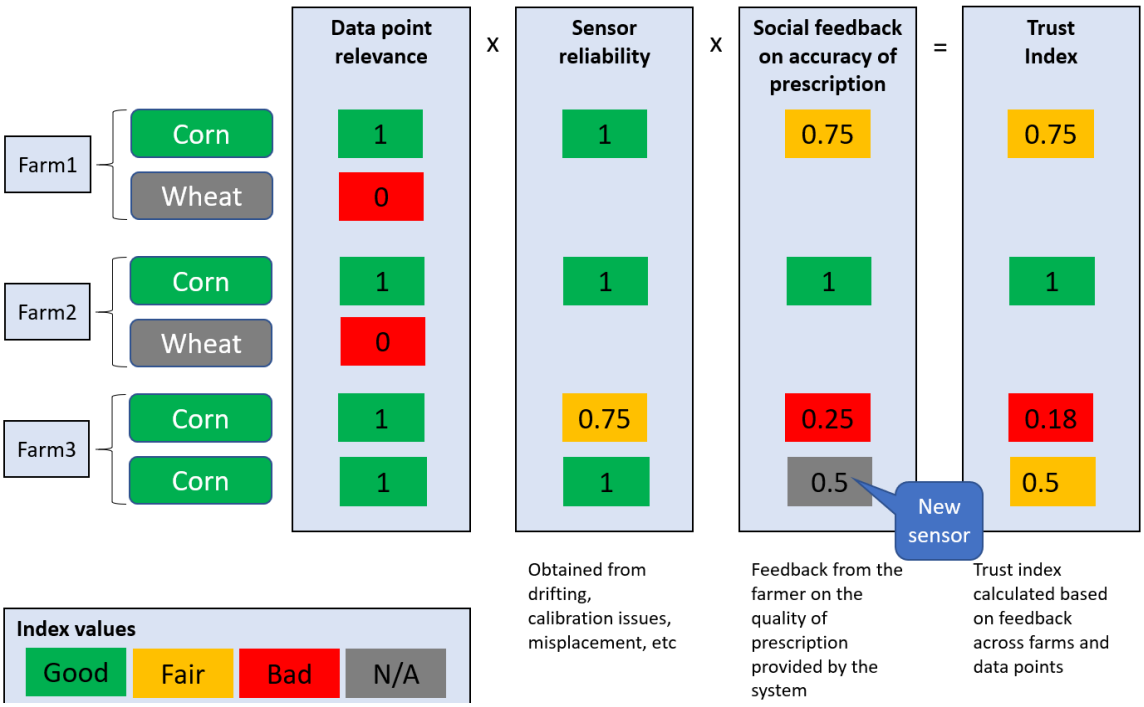


Fig. 106 Social Trust Index – calculul eșantioanelor pentru același tip de cultură (Porumb).

De exemplu, pentru calcularea unei predicții, algoritmul consideră relevantă o valoare a senzorului care deservește același tip de cultură, este plasată în același tip de sol sau asemănări bazate pe locație (ferme învecinate). În plus, unele valori sunt identificate ca fiind îndoielnice din cauza derapajelor, a problemelor de calibrare sau a poziției greșite pe teren. Aceste valori primesc un scor mai mic al factor failibilitate (reliability). Senzorii aplasați în locuri noi sunt în mod implicit luați în considerare în faza de încercare, deci cu o fiabilitate mai mică a senzorului.

Platforma este planificată să utilizeze o abordare ioT socială în care fermele similare pot lua în considerare rezultatele ciclului anterior al culturilor, în care prescripțiile de succes au o pondere mai mare decât cele invalidate de fermieri. Fermierii pot accesa platforma de analiză prin intermediul aplicației web numită "SARMENTI Farm Advisor" care se concentrează pe furnizarea de predicții în timp real fermierului. Aplicația este optimizata/ajustata pentru dispozitivele mobile cu ecran mic (telefoane, tablete) și oferă utilizatorului posibilitatea de:

- conectare cu unul dintre rolurile definite (fermier, producător de senzori, administrator);
- vizualizare a recomandărilor și a altor date din modelul de predicție;
- să primească notificări cu privire la cantitatea sugerată de îngrășământ care urmează să fie aplicată pe teren;
- să ofere feedback pentru modelul de predicție pentru a-l optimiza.

Platforma de analiză face predicții și oferă sfaturi (prescripții) fermierului cu privire la diverse aspecte, cum ar fi consumul de îngrășăminte, rata de creștere a culturilor, randamentul culturilor [33]. Decizia finală de a urma sfaturile este cu privire la agricultorul care poate oferi feedback cu privire la calitatea prescripțiilor și măsurile luate (de exemplu, cantitatea de îngrășăminte aplicate, etapele de evoluție a plantelor etc.).
Feedback-ul social al fermierului cu privire la acuratețea prescripției permite platformei de analiză să învețe de la fermierii experți în agricultură disponibili în SARMENTI, precum și să învețe de la o multitudine de dispozitive odată ce produsul este implementat în număr mare. Această relație dintre dispozitive, seturile lor de date produse și interacțiunea cu fermierii face tranziția către un *IoT social.*

Acest indice de încredere poate fi vizualizat în platforma de analiză, împreună cu componentele sale, așa cum este descris în Figura 107.

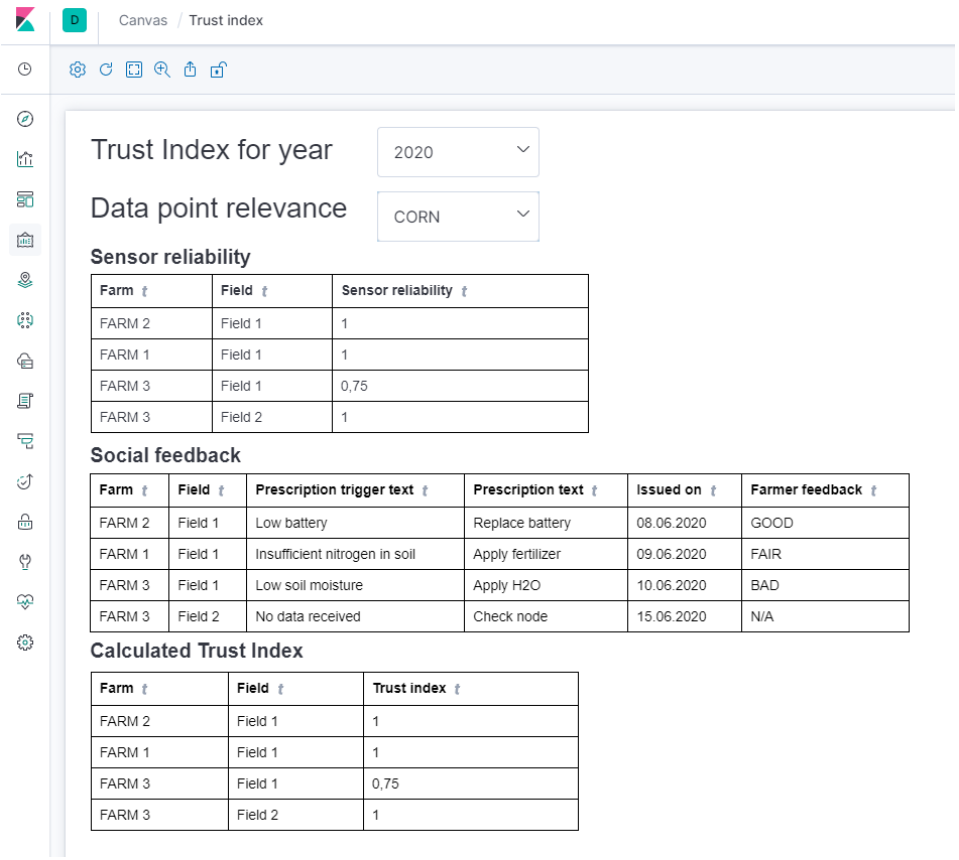


Fig. 107 Social Trust Index inițial, afișat în platforma analitică.

În plus, Social Trust Index se află la confluența dintre cele două bucle de feedback ale sistemului: bucla de feedback a utilizatorilor (user feedback loop) în care fermierul oferă feedback și bucla de interpretare (data science loop) date în care analistul de date și fermierul analizează algoritmii de învățare și fac ajustări și îmbunătățiri. Componentele și valorile Indicelui de încredere sunt descrise într-un fișier JSON simplu, făcând ajustările ușor de făcut, la fel de simple ca editarea unui fișier text, așa cum se vede în cu excepția de mai jos:

“SocialFeedback”: [
{ “Name” : “Good”, “Weight” : 1 },
{ “Name” : “Fair”, “Weight” : 0.75 },
{ “Name” : “N/A”, “Weight” : 0.5 },
{ “Name” : “Bad”, “Weight” : 0.25 }],

Indicele de încredere permite crearea unui algoritm îmbunătățit în care fiecare rețetă bună este întărită (consolidată), așa cum este descris în figura 108.

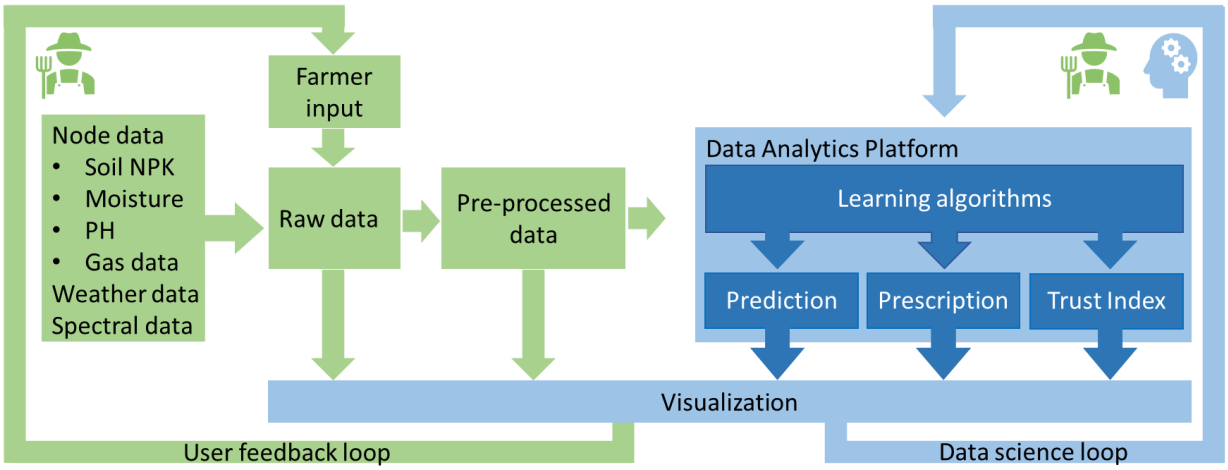


Fig. 108 Platforma de analiză: fluxul de date, procesele principale și buclele de feedback.

Pe partea de analiză a datelor Back-End-Server, algoritmii de extragere a datelor au fost produși pentru modelul fabricii care a generat consolidarea unui model de predicție pentru principalii nutrienți, cum ar fi azotul.

Pe baza datelor agricole disponibile, au fost create mai multe modele de plante conceptuale inițiale. Una dintre ele reflectă nevoile plantelor în ceea ce privește azotul. O vizualizare a unui astfel de model pentru porumb poate fi văzută în figura 109. Modele similare descriu alte caracteristici ale plantelor, de exemplu suprafața frunzelor, numărul de frunze etc.

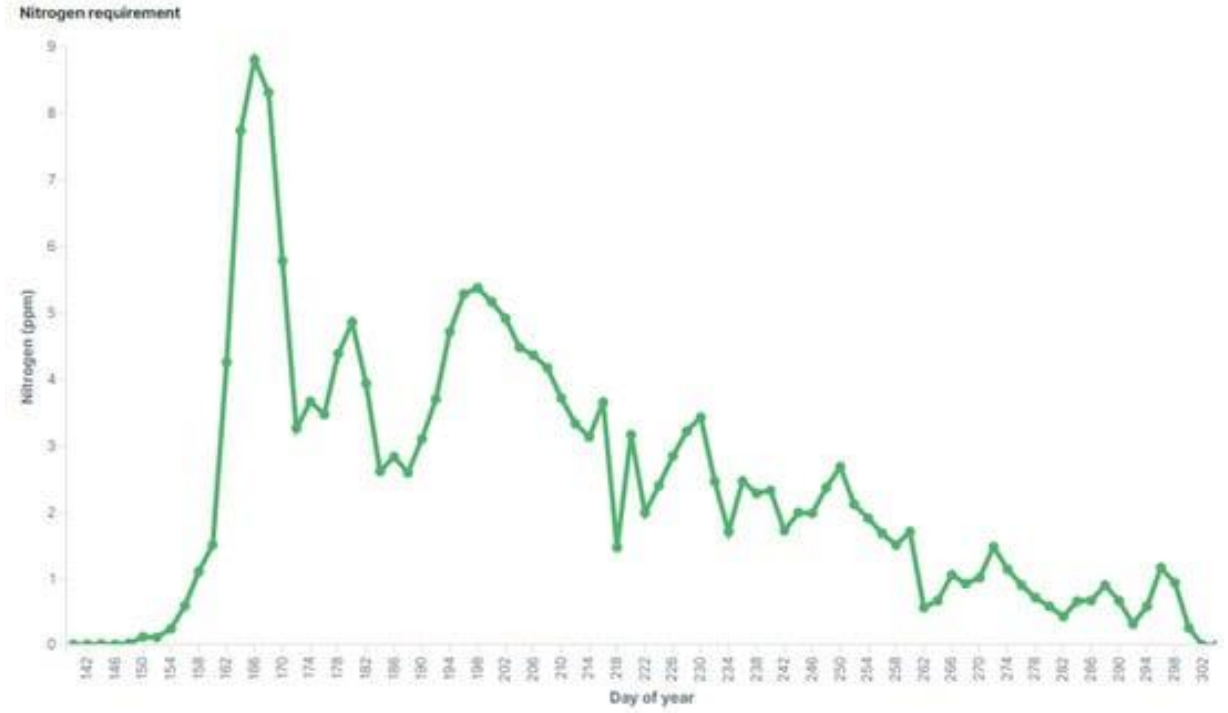


Fig. 109 Model conceptual - nevoia zilnică de azot a plantelor.

În plus, furnizorii de semințe oferă informații cu privire la modelele de creștere a plantelor, inclusiv modalități de a identifica vizual unele "repere". De exemplu, figura 110 prezintă aceste repere și calendarul lor pentru porumb.

	Vegetative growth								Reproductive growth			
Milestone	VE	V2	V5	V8	V10	V12	V14	VT	R1	R2-R3	R6	
Days	0	7	21	32	38	44	49	56	63	70-84	120	160
Stage	Germination and emergence		Plant established	Cob development		Active growth. Leaves and cob development		Pollination		Kernel development	End of mass gain	Ready for harvest

Fig. 110 Etapele de creștere a porumbului.

Prin utilizarea algoritmilor tipici de clasificare, cum ar fi regresia liniară sau modelele de mașini vectoriale de sprijin, apar deja în ceea ce privește nevoile de nutrienți ai plantelor. De exemplu, creșterea timpurie a plantelor necesită niveluri ridicate de azot din sol. Modele similare au fost observate în raport cu zona frunzelor de plante în stadiile inițiale de creștere a plantelor.

Modelul plantelor, împreună cu caracteristicile speciale de creștere a plantelor (repere de creștere, pH-ul solului, feedback-ul fermierilor, vreme etc.) sunt analizate în modulul de analiză a datelor și se generează o predicție pentru evoluția plantelor și consumul de nutrienți proiectat, care poate fi observat în figura 111 pentru azot.

Fig. 111 Simularea predicției pentru reperele de porumb și consumul de azot.

Pe baza previziunilor privind etapele și consumul de nutrienți, se generează prescripții pentru ca fermierul să efectueze acțiunile corespunzătoare în teren. Aceste prescripții sunt transmise printr-un mecanism de notificare. Algoritmul de învățare este re-pus în aplicare prin feedback-ul de la fermier, care poate valida / invalida prescripția pe baza celor mai bune practici agricole și a experienței sale. Acest lucru se realizează prin intermediul aplicației web numită "SARMENTI Farm Advisor".

3.2. Inteligenta Artificiala pentru creșterea eficientei sistemelor de calcul și comunicații integrate în cadrul infrastructurilor critice (sisteme de apel de urgență 112).

Inteligența artificială asigură optimizarea proceselor și pot aduce un aport esențial în cadrul eficientizării serviciilor critice și de urgență, precum sisteme 112.

Proiectul ODIN112 s-a desfășurat între anii 2021 și 2023, a fost un proiect de cercetare finanțat prin mecanismul UEFISCDI Soluții, iar partenerul coordonator a fost Academia Tehnică Militară, iar parte din rezultatele proiectului au fost diseminate în articolele de jurnal [36], [37].

Arhitectura sistemului ODIN112 (a se vedea Figura 112) este construită în jurul diferitelor module de procesare a vorbirii pentru a îmbunătăți serviciile de urgență din România. Include un modul de recunoaștere a vorbirii pentru a transcrie automat apelurile și pentru a îmbunătăți scrierile operatorului, precum și un modul de clasificare a emoțiilor apelantului. Sistemul ODIN112 este menit să sprijine operatorul în evaluarea situației cu scopul final de a reduce timpul de răspuns al serviciilor de urgență (de exemplu, ambulanțe, pompieri și poliție).

Arhitectura generală a sistemului informațional este compusă dintr-un proxy de tip centrală telefonică, modulul IVR (pentru asistarea automată a telefoanelor având un sistem de tip chatbot), interfața utilizator și un set de micro-servicii care asigură funcțiile de clasificare și detecție evenimente acustice, analiza emoțiilor, transcrierea vorbirii, arhivarea apelurilor. Componenta Manager folosește micro-servicii pentru a gestiona procesarea în timp real a fluxurilor audio asociate cu apelurile de intrare. Toate modulele sunt încapsulate în containere standard (de tip Docker), iar comunicarea dintre ele se face prin interfețe simple, standard, folosind mesaje și invocări de metode. Sistemul are un modul de luare a deciziilor, iar aceste decizii facilitează integrarea în Sistemul Național Unic pentru Apeluri de Urgență (SNUAU).

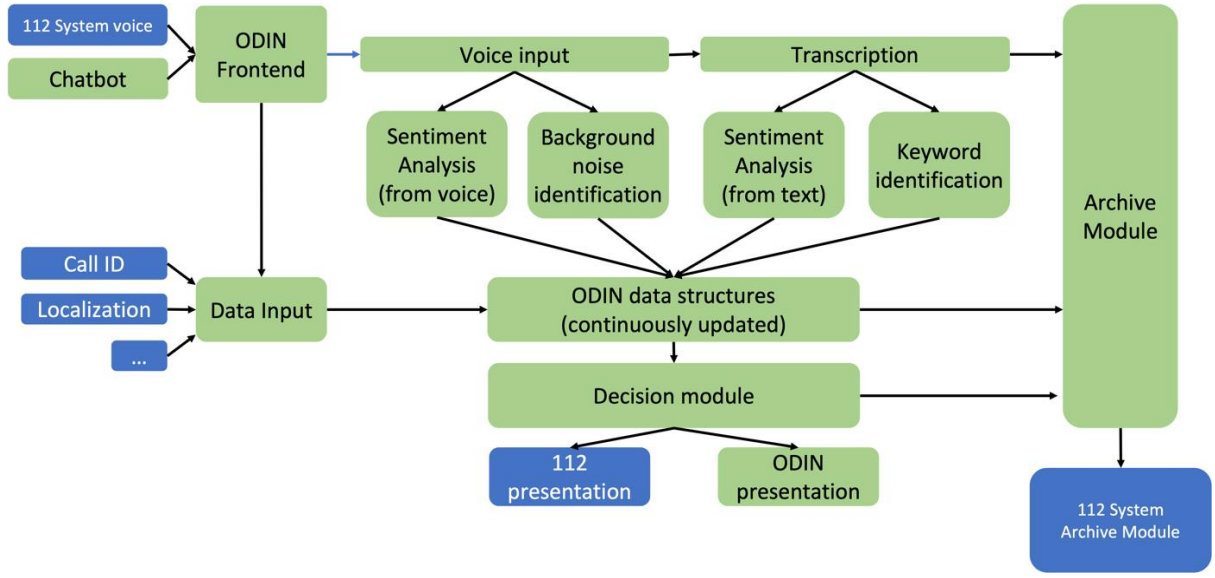


Fig. 112 Arhitectura ODIN112: Componente funcționale
(componentele sistemului de urgență 112 existente sunt reprezentate cu albastru).

Integrarea dintre componentele din interiorul sistemului ODIN112 este prezentată în Figura 113. Când sosește un nou apel, componenta Manager notifică backend-ul modulului de interfață cu utilizatorul să înregistreze apelul. Managerul începe, de asemenea, să multiplice fluxul audio la serviciile de transcriere, identificare zgomote de fundal și analiză a sentimentelor vocale. Comunicarea dintre Manager și serviciile/modulele de procesare se face folosind fluxuri TCP bidirecționale, permițând livrarea de noi fragmente audio pentru procesare în orice moment (realizarea procesării în timp real) și fiecare modul de serviciu să ofere rezultate noi de îndată ce acestea sunt disponibil.

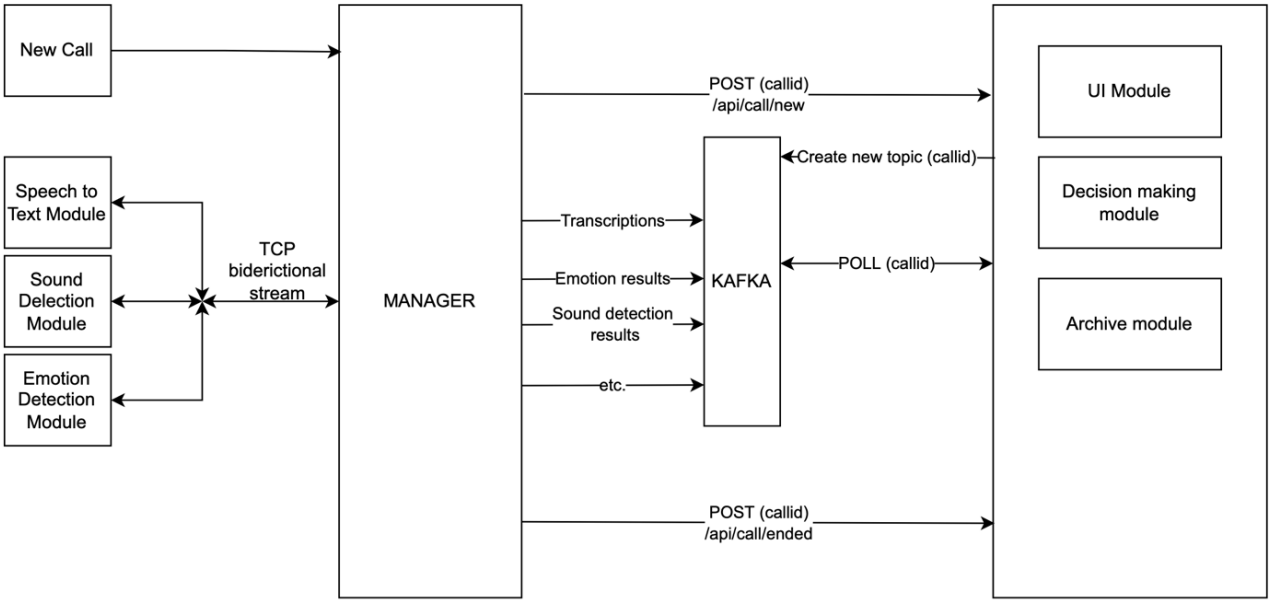


Fig. 113 Arhitectura ODIN112: Componente de comunicare și integrare.

Comunicarea din punct de vedere al datelor (constând din rezultate de detectare a transcrierilor, emoțiilor și sunetului) între manager și aplicația backend se realizează prin cozile Kafka, asigurând procesarea fluxului scalabilă și tolerantă la erori. Utilizarea unei astfel de implementări ajută la decuplarea producătorilor și consumatorilor sistemului, oferind o procesare fiabilă pentru fiecare mesaj furnizat.

Fiecare apel este tratat pe un subiect Kafka definit ca ID unic al apelului. Când managerul observă sfârșitul unui apel, notifică toate celelalte componente (inclusiv modulul backend), așteaptă ultimele rezultate de la fiecare dintre serviciile de procesare și apoi dezactivează fluxurile pentru apelul care tocmai s-a încheiat.

Principalele componente software ale solutiei sunt:

- Modul de transcriere a convorbirii în text
  - Asigură transcrierea în timp real a convorbirilor de urgență
  - Folosește un model de recunoaștere a vorbirii dezvoltat prin intermediul toolkit-ului Kaldi
  - Pentru antrenarea și testarea modelului s-au utilizat atât seturi de date disponibile public cât și date colectate prin intermediul aplicației ECHO dezvoltată în cadrul proiectului (echo.readerbench.com)
  - Asigură o rată scăzută a erorilor (WER) de 8.94%
- Modulul de recunoaștere și clasificare sunete de fundal
  - Capabil să identifice 58 clase de sunete de fundal care pot să apară pe parcursul unei convorbiri de urgență
  - Folosește ca și clasificator o rețea neuronală TALNet
  - Pentru antrenare și testare a fost folosit setul de date ESC-50 la care au fost adăugate sunete extrase din videoclipuri de pe platforma YouTube
  - Acuratețea obținută este de 80% pentru o serie de clase de sunete.
- Modul de înregistrare și arhivare a convorbirilor
  - Asigură arhivarea datelor colectate pe timpul apelului de urgență
  - Sistemul de fișiere folosit este Hadoop, datele fiind salvate în format JSON
  - Oferă posibilitatea de căutare a informațiilor pe baza identificatorului de caz (CALL ID)
- Modul de asistare a deciziei

  - Reprezintă interfața cu operatorul folosită pentru afișarea transcrierii convorbirii, a stărilor emoționale și a zgomotelor de fundal identificate
  - Permite asistare deciziei operatorului oferind suport prin sugerarea unui nod de index (categoria incidentului)
  - Permite integrarea ușoară cu alte sisteme folosind serviciul REST pus la dispoziție
- Modul de tip chatbot
  - Asigură preluarea și prioritizarea apelurilor în situații speciale, în care toți operatorii centrului sau dispeceratului de urgentă sunt ocupați (de exemplu, în cazul fenomenelor naturale)
  - Dezvoltat folosind platforma FreeSwitch
  - Folosește un arbore de decizie care clasifică apelurile în patru categorii: urgențe medicale, poliție, pompieri și non-urgente
- Modul de recunoaștere și clasificare a stărilor emoționale ale interlocutorilor în convorbiri telefonice
  - Identifică în timp real stările emoționale prin procesarea vocii apelantului (stare neutră, teamă, tristețe, dezgust, furie, plictiseală, bucurie, nervozitate)
  - Folosește ca și clasificator o rețea neuronală pre-antrenată VGG16
  - Seturile de date utilizate pentru antrenare și testare au fost EMO-IIT, EMO-DB precum și înregistrări realizate în cadrul proiectului cu actori profesioniști
  - Acuratețea obținută este de 93,56%

Fig. 114 Interfața cu operatorul folosită pentru afișarea transcrierii convorbirii, a stărilor emoționale și a zgomotelor de fundal identificate, precum și o posibilă clasificare a cazului

3.3.Sistem de detecție a semnalelor (SIGINT) bazat pe învățare automată cu SDR

În [38] se prezintă implementarea unui sistem care identifică modularea semnalelor radio complexe. Acest lucru este realizat folosind un model de inteligență artificială dezvoltat, instruit și integrat în Cloud-ul Microsoft Azure. Considerăm că platformele bazate pe Cloud oferă suficientă flexibilitate și putere de procesare pentru a le utiliza în locul computerelor convenționale pentru procesarea semnalelor bazate pe inteligența artificială. Am testat implementarea folosind o platformă radio definită de software dezvoltată în GNU Radio care generează și primește semnale modulate reale. Acest proces asigură că soluția propusă este viabilă pentru a fi utilizată în sisteme

reale de procesare a semnalului. Rezultatele obtinute arata ca pentru anumite tipuri de modulații, identificarea se face cu un grad ridicat de succes. Utilizarea unei platforme bazate pe Cloud permite accesul rapid la sistem. Utilizatorul este capabil să identifice modularea semnalului folosind doar un laptop care are acces la internet.

Implementarea evaluează fezabilitatea efectuării recunoașterii modulației bazate pe Cloud folosind rețele neuronale artificiale și DST. Abordarea propusă utilizează Cloud computing în locul hardware-ului tradițional (CPU (Central Processing Unit) sau GPU (Graphical Processing Unit)) pentru a obține modelul instruit al rețelei de inteligență artificială. Utilizarea Cloud computing-ului elimină limitele impuse de echipamentele hardware dedicate prin furnizarea unei puteri de procesare suficiente cerute de rețeaua neuronală.

Sistemul implementat are o arhitectură bazată pe simbioza dintre cele două componente: hardware și software. Ele se întrepătrund pentru a crea un sistem omogen și eficient. Figura 115 arată modul în care componentele sistemului sunt interconectate.**Error! Reference source not found.**

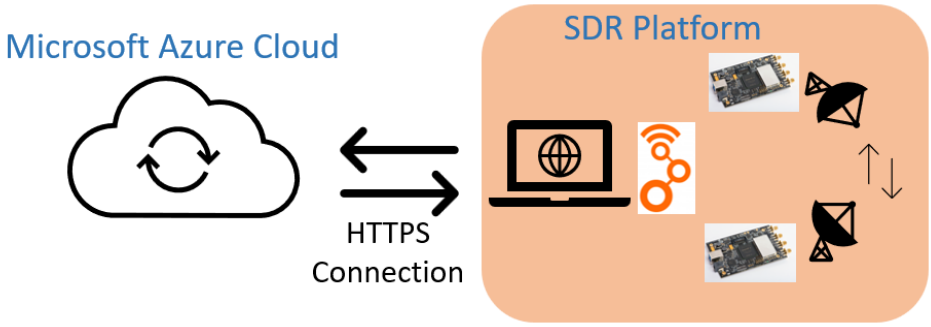


Fig. 115 Interconectarea componentelor în configurația SDR experimentală

Modul în care componentele sistemului funcționează și comunică pot fi văzute în figura 116. În partea superioară a figurii 116 sunt prezentate componentele care sunt utilizate la antrenarea și validarea rețelei neuronale. Baza de date, după ce este pregătită, este încărcată în serviciul Microsoft Azure Auto ML unde este configurată de inteligența artificială. În urma părții de antrenare și validare, se realizează *modelul instruit.* În partea inferioară a imaginii sunt prezentate componentele utilizate pentru a testa modelul instruit. Platforma DST este utilizată pentru a trimite și a primi semnale modulate. Eșantioanele modulate primite sunt inserate în modelul instruit integrat (integrat în Cloud Microsoft Azure) care generează răspunsul cu tipul de modulație identificat.**Error! Reference source not found.Error! Reference source not found.**

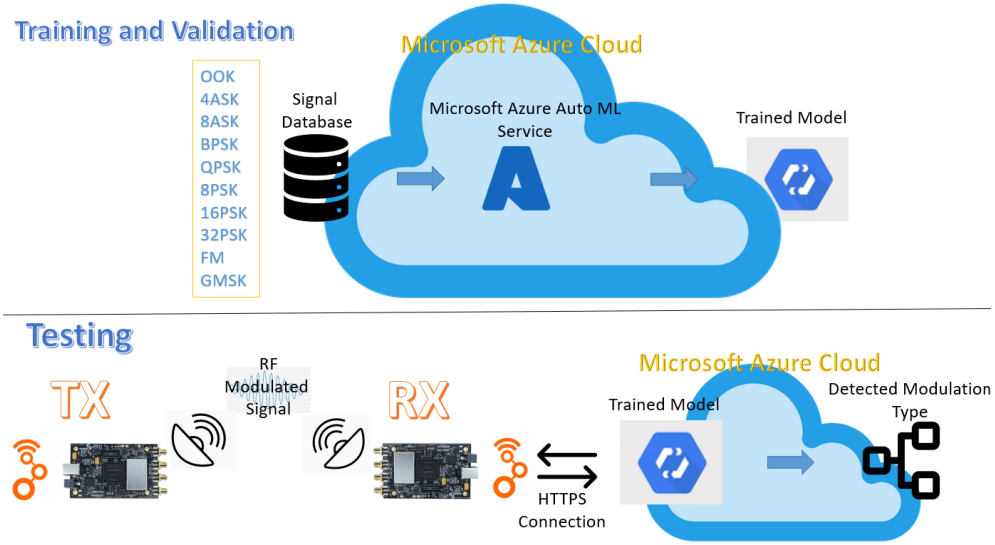


Fig. 116 Componente funcționale ale sistemului.

Principalul pas pentru obținerea unui model de inteligență artificială este de a avea o bază de date suficient de mare și completă pentru a permite instruirea, validarea și testarea unui model cât mai eficient posibil. Pentru a obține cele mai concludente rezultate, baza de date a semnalelor RF numită "RADIOML 2018.01A", care a fost creată și utilizată pentru prima dată pe hârtie, a fost aleasă ca punct de plecare.**Error! Reference source not found.Error! Reference source not found.**

În această bază de date găsim semnale care sunt modulate folosind următoarele 24 de scheme de modulare: OOK, 4ASK, 8ASK, BPSK, QPSK, 8PSK, 16PSK, 32PSK, 16APSK, 32APSK, 64APSK, 128APSK, 16QAM, 32QAM, 64QAM, 128QAM, 256QAM, AM-SSB-WC, AM-SSB-SC, AM-DSB-WC, AM-DSB-SC, FM, GMSK și OQPSK.

Pentru a obține setul de date dorit pentru instruirea rețelei neuronale, numai înregistrările pentru următoarele zece clase de modulare au fost extrase din baza de date: OOK, 4ASK, 8ASK, BPSK, QPSK, 8PSK, 16PSK, 32PSK, FM și GMSK. De asemenea, acestea sunt investigațiile și scenariile de cercetare utilizate. Doar aceste zece modulații au fost selectate pentru că sunt suficiente pentru a valida această abordare și multe dintre ele sunt utilizate în comunicațiile mobile.

Pentru fiecare dintre aceste zece clase, au fost extrase 1024 de fișe de formare și 256 de înregistrări de testare pentru fiecare dintre nivelurile SNR între [2 dB, 30 dB]. 153600 de înregistrări sunt disponibile pentru instruire și 38400 pentru testare, fiecare dintre ele având 1024 de elemente complexe.

Funcționalitatea ML automată din serviciul "Microsoft Azure AutoML" a fost utilizată pentru a defini, instrui, testa și valida rețeaua neuronală. După ce a fost începută definirea noului model, se alege baza de date utilizată pentru instruire și validare. Următorul pas este de a analiza datele pentru a identifica problemele potențiale. După cum pot fi menționate posibile probleme: lipsesc date în anumite coloane, nu toate datele de intrare au același format sau pentru unele date de intrare nu avem date de ieșire.

După finalizarea procesului de instruire, au rezultat un număr de 46 de modele, fiecare dintre acestea având o anumită valoare de precizie. **Error! Not a valid bookmark self-reference.** enumeră primele 16 modele care au obținut cea mai bună precizie dintre cele 46 generate.

Tabel 1. Acuratețea modelelor

Algorithm name	Accuracy	Sampling
SparseNormalizer, GBoostClassifier	0.64831	100.00%
MaxAbsScaler, LightGBM	0.60833	100.00%
SparseNormalizer, GBoostClassifier	0.60117	100.00%
SparseNormalizer, GBoostClassifier	0.58980	100.00%
SparseNormalizer, GBoostClassifier	0.58559	100.00%
SparseNormalizer, GBoostClassifier	0.57396	100.00%
RobustScaler, LightGBM	0.56163	100.00%
SparseNormalizer, GBoostClassifier	0.55794	100.00%
SparseNormalizer, GBoostClassifier	0.55551	100.00%
StandardScalerWrapper,XGBoostClassifier	0.54870	100.00%
SparseNormalizer, LightGBM	0.54132	100.00%
SparseNormalizer, GBoostClassifier	0.53568	100.00%
MaxAbsScaler, GradientBoosting	0.53229	100.00%
MaxAbsScaler, XGBoostClassifier	0.52804	100.00%
RobustScaler, LightGBM	0.52682	100.00%
RobustScaler, LightGBM	0.52248	100.00%

Pentru integrare, se alege modelul cu cea mai mare precizie. Pentru acest model sunt generate și rezultatele obținute în urma validării modelului după instruirea acestuia.

Timpul necesar pentru a obține acest model este de 9 ore, 21 de minute și 19 secunde. În acest timp, s-a efectuat atât instruirea propriu-zisă, cât și validarea rezultatelor.

Toate valorile obținute în urma validării acestui model sunt:

1. Precizie = 0,64831
2. Precizie macro medie = 0,68130
3. Precizie medie micro = 0,79536

Cea mai importantă caracteristică a modelului instruit este *matricea de confuzie.* Acesta poate fi văzut în **Error! Not a valid bookmark self-reference.**. După cum se poate observa în matricea de confuzie, cele mai bune rezultate sunt înregistrate pentru modulațiile: FM, BPSK, GMSK, OOK și 4ASK. Cele mai slabe rezultate sunt înregistrate pentru modulațiile: 8PSK, 16APSK, 32APSK, QPSK și 8ASK.

Tabel 2. Matricea de confuzie

	16PSK	32PSK	4ASK	BASK	8PSK	BPSK	FM	GMSK	OOK	QPSK
16PSK	634	599	0	0	611	1	1	10	0	448
32PSK	618	639	0	0	579	0	2	12	1	453
4ASK	0	0	1715	424	0	0	0	0	165	0
BASK	0	0	664	1616	0	0	0	0	24	0
8PSK	607	664	0	0	613	1	0	6	0	413
BPSK	7	4	0	0	5	2281	0	2	0	5
FM	0	1	0	0	0	0	2303	0	0	0
GMSK	58	58	0	0	68		1	2084	0	35
OOK	0	0	58	0	0	0	0	0	2246	0
QPSK	440	399	0	0	442	1	1	215	0	806

Precizia rezultată diferă pentru fiecare modulație. Unele modulații au o precizie mai bună decât celelalte. În**Error! Not a valid bookmark self-reference.** este listată acuratețea pentru fiecare modulare.

Tabel 3. Precizia pentru fiecare modulație.

Modulație	16PSK	32PSK	4ASK	8ASK	8PSK	BPSK	FM	GMSK	OOK	QPSK
Precizie	0.26%	0.27%	0.72%	0.68%	0.25%	0.96%	0.97%	0.88%	0.95%	0.34%

Am arătat că procesarea semnalului se poate face folosind Cloud computing. Acesta poate fi utilizat pentru definirea, instruirea și implementarea rețelei neuronale. Această metodă îmbunătățește metoda tradițională de dezvoltare a IA pentru procesarearcu semnalelor. În plus, la modul tradițional de utilizare a hardware-ului dedicat, această metodă asigură rezultate similare, dar într-un mod mai rapid și mai ieftin.

Am arătat că având o bază de date bună cu probe de instruire și cunoștințe minime de procesare a semnalului și rețele neuronale, modelele de rețele neuronale pot fi instruite și implementate.

În comparație cu abordarea standard a utilizării rețelelor neuronale pe un computer local, rețelele neuronale bazate pe Cloud au atât avantaje, cât și dezavantaje. Acestea sunt prezentate în **Error! Not a valid bookmark self-reference.**și au fost extrase prin compararea rezultatelor obținute în această lucrare cu cele obținute teoretic. **Error! Reference source not found.**

Tabel 4. Rețele neuronale bazate pe Cloud vs rețele neuronale locale

Rețele neuronale bazate pe Cloud	Rețele neuronale locale
Mai puțin costisitoare	Mai multă flexibilitate în formare și integrare
Hardware-ul utilizat poate fi selectat în funcție de nevoile utilizatorului	Când este nevoie de hardware nou, acesta trebuie cumpărat
Mai puține cunoștințe necesare	Precizia medie a tuturor modulațiilor este mai bună
Ușor de configurat și de antrenat	Mai multe caracteristici de formare pot fi extrase pentru a verifica performanța generală
Modelul instruit poate fi integrat cu ușurință în Cloud și accesat de oriunde	
Precizie comparabilă pentru modulații precum BPSK, FM și OOK	

În tabelul 5 este prezentată o comparație între rezultatele obținute în această lucrare cu rezultatele obținute în literatura de specialitate [38] utilizarea rețelelor neuronale convenționale. Acest tabel arată că pentru BPSK, FM, OOK și GMSK rata de detecție este similară. Pentru restul modulațiilor diferența este mai mare în favoarea rețelei neuronale convenționale dezvoltate pe un computer local.**Error! Reference source not found.**

Tabel 5. Compararea rezultatelor rețelelor neuronale bazate pe Cloud și a rețelelor neuronale locale

Modulate / Model NN	16PSK	32PSK	4ASK	8ASK	8PSK	BPSK	FM	GMSK	OOK	QPSK
Model implementat cu SNR = 2 - 30dB	26%	27%	72%	68%	25%	96%	97%	88%	95%	34%
Model din literatura de specialitate SNR = 2 - 30dB	~75%	~78%	~88%	~90%	~92%	~95%	~95%	~95%	~95%	~95%

Principalele direcții de cercetare ulterioare constau în îmbunătățirea modelului rețelei neuronale prin utilizarea unei baze de date cu mai multe tipuri de modulație care au o gamă mai largă de zgomot și interferențe. O altă direcție de cercetare viitoare constă în integrarea modelului instruit într-un sistem care va detecta tipul de modulare în timp real și îl va putea demodula direct fără intervenția umană.u

3.4. Implementare Cloud-/Edge- de algoritmi de Inteligență Artificiala pentru aplicații în industrie

Cercetările prezentate în [39] au vizat implementarea IA în prelucrarea datelor de la senzori privind, în special, *alocarea calculelor* (locală și/sau centralizată) în mediul distribuit.

Modelul Cloud-/Edge- computing (procesare-stocare-teletransmisie) a fost extins în paradigma *Cloud AI /Edge AI*.

Abordarea dispozitivelor inteligente bazată pe *controlul prin stare* a fost extinsă la ECU (unități de control electronic – Electronic Control Units) dotate cu capabilități de diagnosticare în *timp real* și *decizie optimală.*

Parametrizarea (instanțierea) poate fi *adaptivă* (mai ales prin ANN), iar toate tranzițiile necesare pentru controlul prin stare (la nivelul mașinilor algoritmice de stare, ASM – Algorithmic State Machine) pot fi decise cu *clasificatori* și alte mijloace IA. O astfel de ASM poate distribui, de asemenea, *sarcinile* localizate / centralizate, în conformitate cu extensia paradigma *Cloud AI /Edge AI* a paradigmei Cloud-/Edge- computing.

S-au studiat *senzorii virtuali cu IA* – care emulează senzorii reali, pe baza experienței acumulate din utilizarea anterioară a acestora în sisteme complexe (împreună, cu *alți* senzori reali care *se vor păstra* în configurația cu *noul* senzor virtual).

Studiul de caz asupra unei configurații instrumentale complexe, în jurul unui stand de testare a motoarelor Diesel, a vizat predicția efectului nedorit ale contra-presiunii din instalația de evacuare asupra performanței. Echipa de cercetare a fost una multi-disciplinară iar rezultatele științifice au necesitat un efort de sinteză - *informatică / inginerie (mecanică și electronică),* fiind publicate într-un jurnal prestigios.

Corelația dintre presiunea gazelor de la ieșirea din eșapament (p [kPa]) și performanța motorului, în principal puterea efectivă (P_e [kW]), a fost extrasă dintr-un set amplu de date culese de la un motor diesel turbo, pe un banc de încercare dinamometric, în moduri de funcționare stabilă, caracterizate de sarcină (exprimată în procente din valoarea maximă de cuplu motor admisă în regim regulat) și viteză de rotație (Turația [rpm]).

A fost colectat un set complet de măsurători, atât pentru analize statistice cât și pentru configurarea și testarea tuturor soluțiilor IA dezvoltate pentru a putea prezice puterea efectivă.

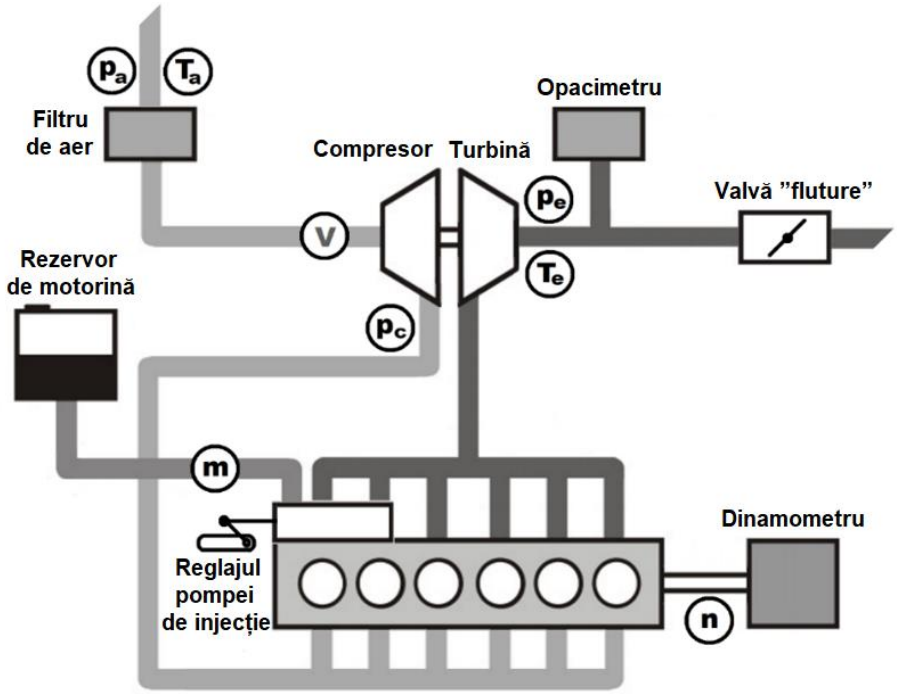


Fig. 117 Motor Diesel

Algoritmii implementați au cuprins ANN (Artificial Neural Networks), apoi clasificatorii și regresorii.

O atenție deosebită a fost acordată IA în Cloud bazată pe algoritmi avansați, intensiv-computaționali, care pot să conteze pe resurse cu putere de procesare și/sau capacitate de stocare practic *"infinită"*.

Într-o primă abordare, învățarea automată (Machine Learning) a fost implementată cu Cloud-MATLAB, începând cu procedurile de antrenare/instruire și până la alegerea

”adversarială”/”competițonală” a modelului "MaaS" (Model as a Service) dintr-o gamă foarte largă, pe principiul GAN – Generative Adversarial (neural) Network. Pe setul unic de date de instruire și testare utilizat în toate studiile de caz, MATLAB a ales GPR (Gaussian Process Regressor) optimizat ca fiind cel mai bun MaaS ce poate fi invocat prin API (Application Programming Interface).

S-a încărcat în Cloud (MathWorks "MATLAB online") lista cu seturile de date de antrenare, Pe (Sarcină, Turație, p). S-a configurat MATLAB pentru a genera un model IA de predicție a puterii efective pe baza celor trei intrări (sarcină, turație și presiune la eșapament). S-a lansat competiția GAN care a determinat ca fiind cel mai performant modelul GPR (Gaussian Process Regressor) al *Regresorului Liniar Gaussian* cu *optimizare Bayesiană* – care folosește aproximări succesive cu variabile aleatoare distribuite gaussian, având hyper-parametri (precum rata de învățare sau criteriul de eroare pentru evaluarea ponderilor) a căror interdependență statistică respectă teorema lui Bayes a probabilităților condiționate.

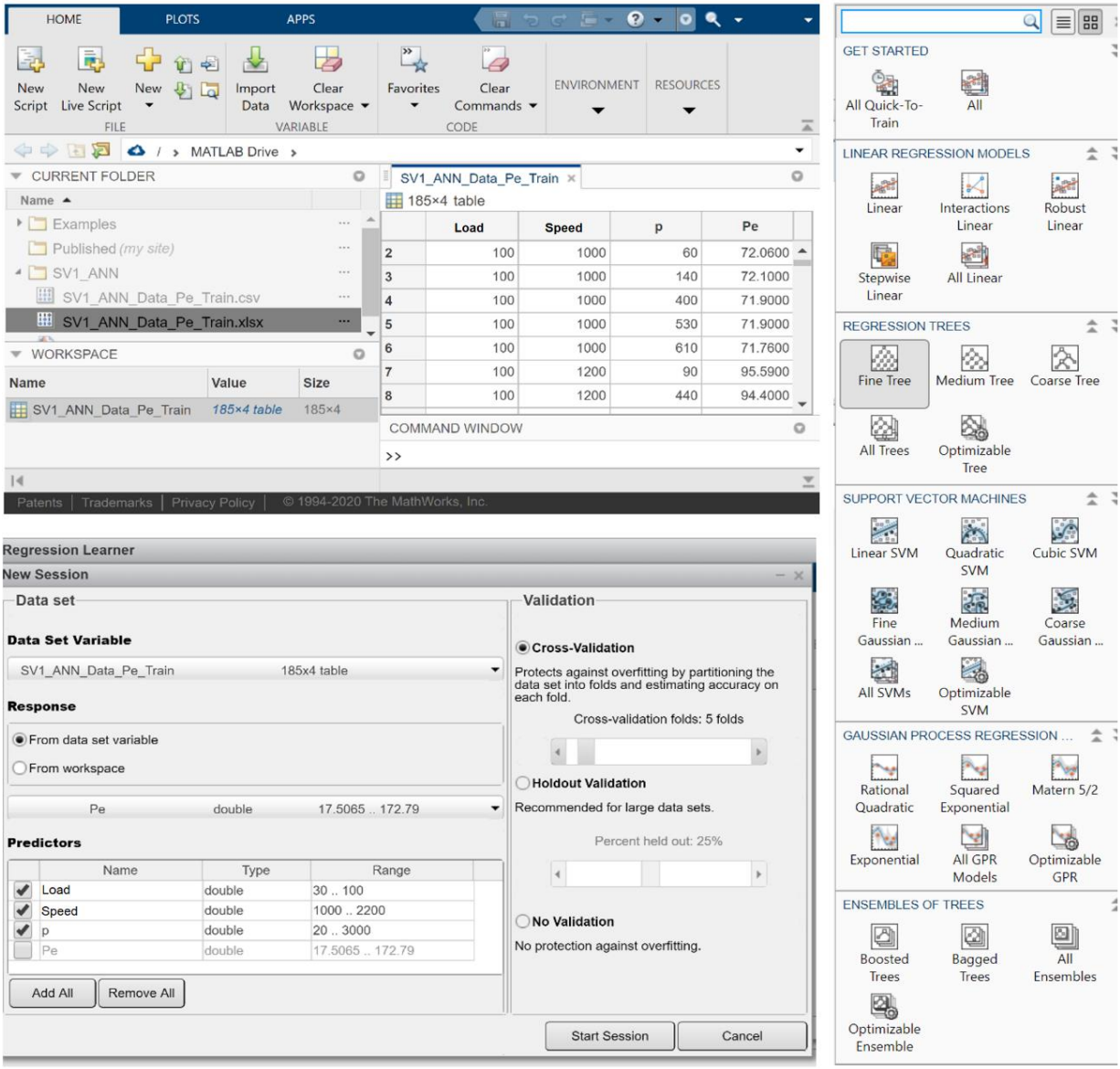
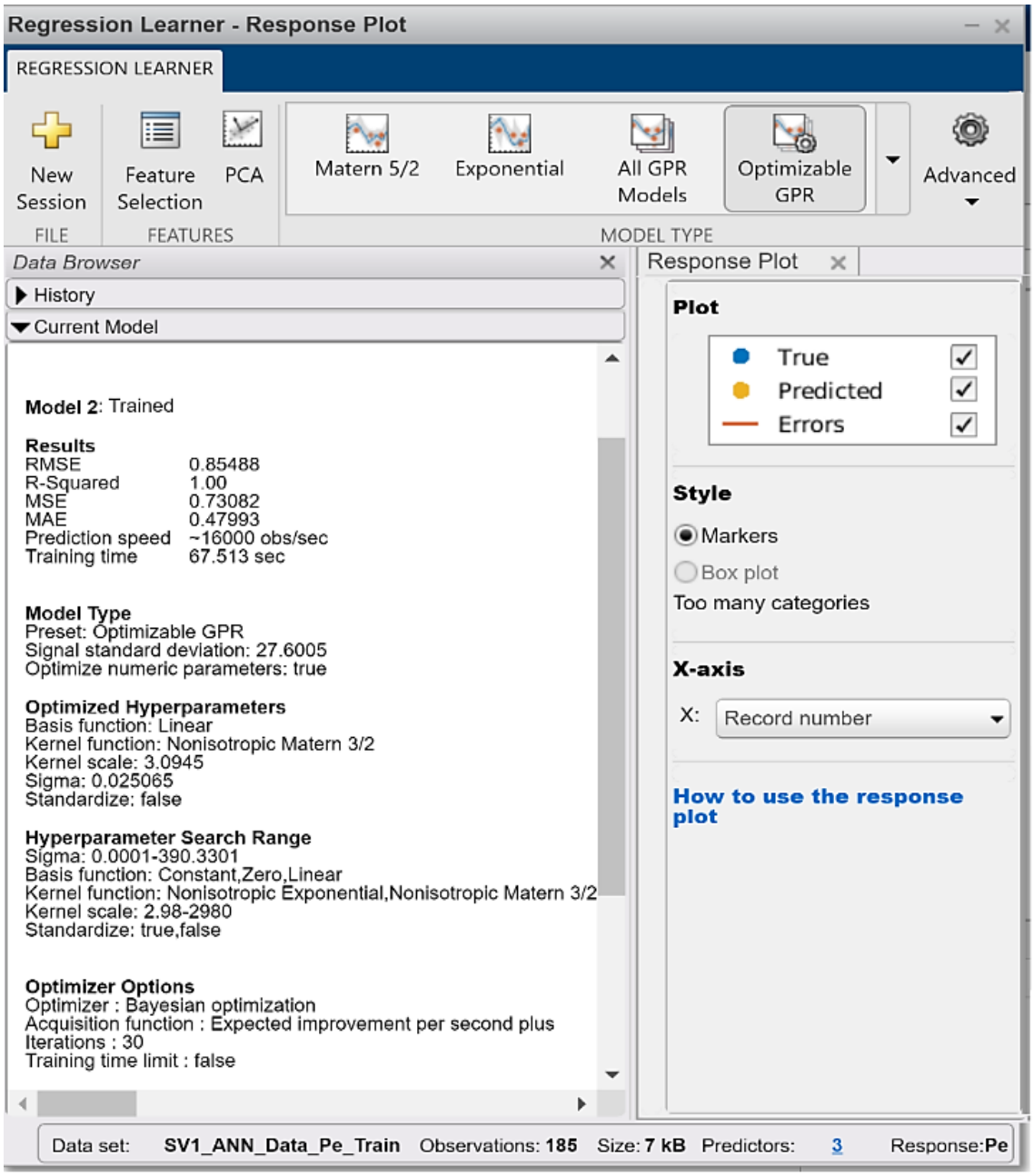


Fig. 118 Modul cum se poate configura MathWorks pentru a genera un model AI

S-au afișat caracteristicile și parametrii modelului generat:



S-a afișat graficul predicțiilor:

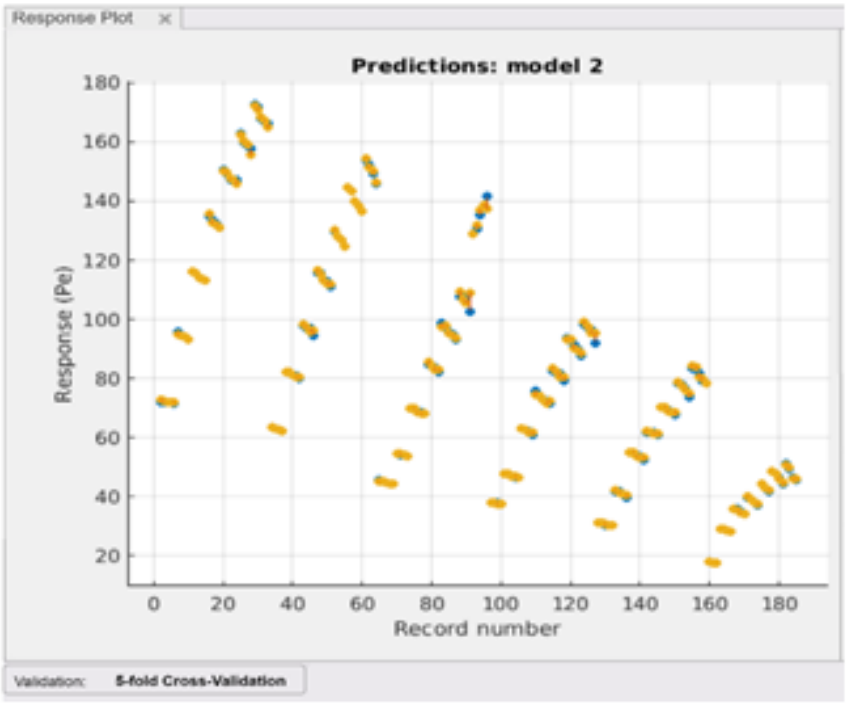


Fig. 119 Implementarea Levenberg-Marquardt cu ANNHUB

Următoarea soluție de IA în Cloud a fost un API Keras pentru ANN. Calculul de bază (”de fundal” – *backend)* s-a bazat pe biblioteci Tensorflow (care manevrează principalele matrice de date multidimensionale ca pe "tensori"). A fost obținut un ANN competitiv relativ "dens" (cu mulți neuroni pe strat) – un pas spre WNN (Wide NN), către DNN (Deep NN – "rețele neuronale profunde") cu multe straturi.

Bibliotecile specifice au fost NumPy, Pandas și Seaborn pentru crearea de tensori (principalele matrice de date multidimensionale), citirea datelor și, respectiv, analiza datelor înainte de definirea modelului. Pentru crearea și prezentarea diferitelor documente necesare și produse în implementarea Keras, am utilizat Jupyter Notebook.

Fiecare dintre cele două straturi "dense" ale ANN a avut 64 de neuroni, astfel încât, pentru cele trei intrări, au rezultat (3 +1 pentru termenul liber) x 64 = 256 de ponderi pentru primul strat; pentru al doilea strat, au rezultat (64 + 1) × 64 = 4160 ponderi; pentru neuronul de ieșire 64 + 1 = 65 de ponderi, astfel încât totalul a fost de 256 + 4160 + 65 = 4481 coeficienți.

Funcția de activare pentru primul strat ascuns a fost ReLU (Rectified Linear Unit – funcția de ”redresare” simplă ”monoalternanță)”, iar pentru al doilea strat ascuns, a fost sigmoida (tangenta hiperbolică deplasată deasupra lui 0 și normalizată).

Ca și criteriu pentru calculele de optimizare (prin metoda "back-propagation" a aproximărilor succesive) am ales minimizarea RMS (Root Mean Square – eroarea medie pătratică de aproximare) *"optimizer = rms"* cu criteriul "pierdere = MSE" (Mean Squared Error). Celelalte metode de optimizare disponibile sunt SGD (Stochastic Gradient Descent), și versiunea ei îmbunătățită (sub aspectul timpului de rulare și al utilizării memoriei), metoda ADAM.

```
# define the function to build the Keras NN model

def build_model():
    model = keras.Sequential([
        keras.layers.Dense(64, activation=tf.nn.relu, input_shape=[3]),
        keras.layers.Dense(64, activation=tf.nn.sigmoid),
        keras.layers.Dense(1)
    ])

    rms = keras.optimizers.RMSprop(0.001)
    sgd = keras.optimizers.SGD(lr=0.01, decay=1e-6, momentum=0.9, nesterov=True)
    adam = keras.optimizers.Adam(lr=0.001, beta_1=0.9, beta_2=0.999, epsilon=None, decay=0.0, amsgrad=False)

    model.compile(loss='mean_squared_error', optimizer=rms, metrics=['mae', 'mse', 'accuracy'])
    return model
```

```
# build the model

model = build_model()
model.summary()

early_stop = keras.callbacks.EarlyStopping(monitor='val_loss', patience=0.05)
```

```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
dense_7 (Dense)              (None, 64)                256
_________________________________________________________________
dense_8 (Dense)              (None, 64)                4160
_________________________________________________________________
dense_9 (Dense)              (None, 1)                 65
=================================================================
Total params: 4,481
Trainable params: 4,481
Non-trainable params: 0
_________________________________________________________________
```

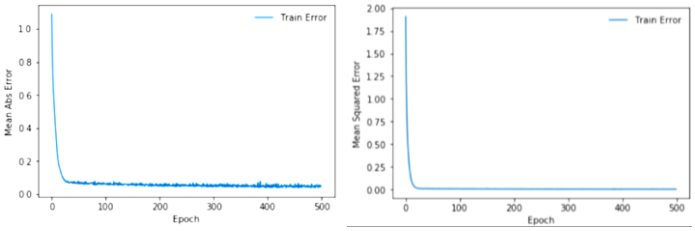
Fig. 120 ANN cu 2 straturi ”dense” (cu câte 64 neuroni) astfel că, pentru cele trei intrări, sunt (3+1) x 64 = 256 ponderi (incluzând termenii liberi, ”bias”), iar pentru stratul 2 sunt (64+1) x 64 = 4160, iar pentru ultimul neuron, de ieșire, 64+1 = 65 ponderi – în total 256 + 4160 + 65 = 4481 coeficienți.

Ultima etapă a calculelor Keras a cuprins antrenarea rețelei. În acest scop, metoda de acordare *(fit)* a fost invocată și parametrizată pentru modelul configurat mai sus. Au fost comandate cinci sute de iterații (”epoci”) (folosind pentru testare 20% din propriile date de antrenare, *normed_train_data ,* adică *validation_split* = 0,2).

```
# train the model

history = model.fit(
    normed_train_data, normed_train_labels,
    epochs=500, validation_split=0.2, verbose=0,
    callbacks=[])

plot_history(history)
```



Pentru a evalua precizia modelului, s-a calculat MSE pentru setul de testare:

```
# evaluate the model

loss, mae, mse, acc = model.evaluate(normed_test_data, normed_test_labels, verbose=0)
print("Testing set Mean Squared Error: {:5.2f}".format(mse))
```

```
Testing set Mean Squared Error:  0.01
```

Fig. 121 Reprezentare grafică a procesului de training; se va verifica eroare pătratică a algoritmului care pentru antrenarea actuală este de 0.01

Următoarea soluție Cloud AI (accesată prin API) a avut la bază accesul prin portalul ANNHUB la o ANN eficientă Levenberg–Marquardt (L-M). Metoda L-M particularizată pentru ANN ia în considerare, iterativ, optimizarea (în cadrul procedurii de *antrenare)* a *coeficienților* rețelei neurale prin folosirea acestora într-o estimare a *ieșirilor* din rețea ca funcție de *intrările* în rețea, dar și de o serie de *variabile de stare.* Aceste variabile de stare sunt alese de obicei pentru a exprima cât mai compact ecuațiile sistemului, dar în cazul de față sunt *chiar coeficienții* neuronilor (ponderile).

Ajustările iterative ale coeficienților reprezintă adăugiri ale acestora proporționale cu *derivata* funcției de estimare (în raport cu aceștia), derivată care este înmulțită cu *pasul* (incrementul) de optimizare al coeficienților. Același principiu ”derivativ” îl are și metoda SGD sus-menționată. Calculele L-M se fac, în cazul general multi-dimensional, cu matricele Jacobiene ale derivatelor parțiale ale variabilelor în raport cu toate celelalte. Specifică algoritmului L-M este și adăugarea unei componente a corecției care este proporțională cu eroarea iterativă de estimare (factorul său de proporționalitate se zice *factor de amortizare,* ajustat la fiecare iterație și tot mai mic – în sensul amortizării acestei componente pe măsură ce erorile de estimare scad).
Modul de lucru: S-au încărcat datele de antrenare (184 de seturi Sarcină-Turație-p-Pe) și testare (62 de seturi).

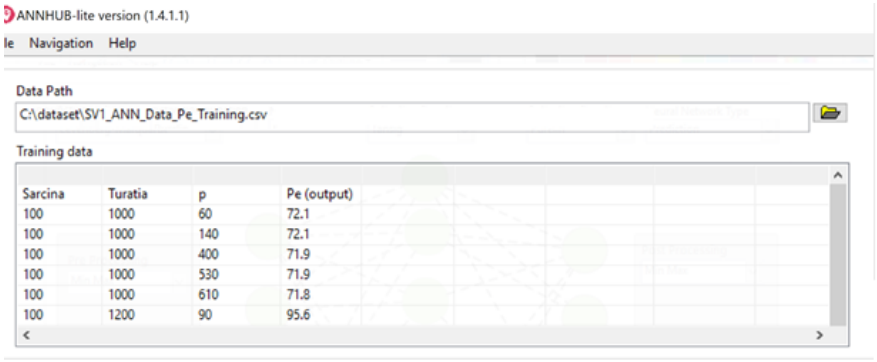


Fig. 122 Modul în care se face încărcarea datelor de training și testing

S-a configurat algoritmul L-M și procesul de antrenare:

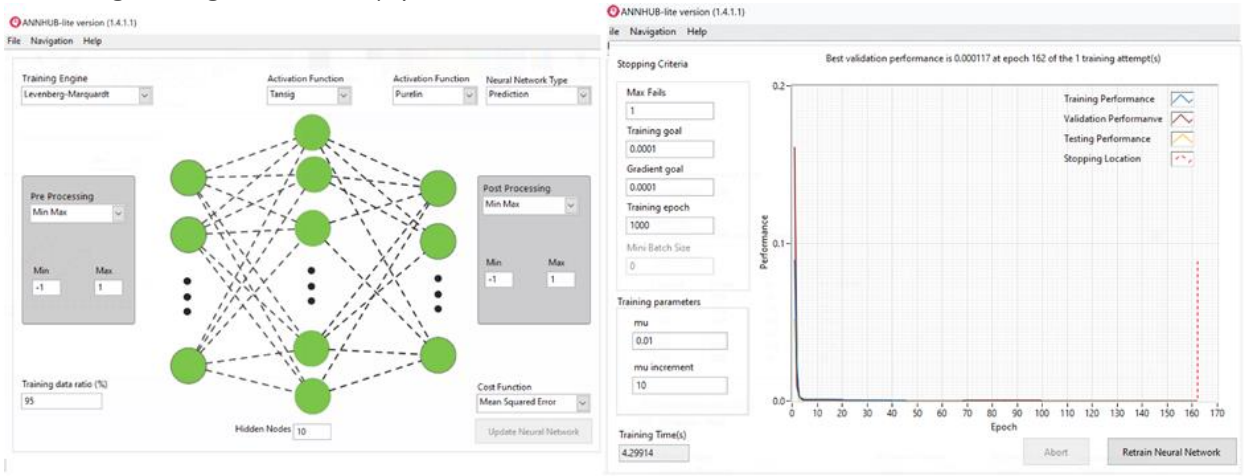


Fig. 123 modul de configurare a algoritmului Lenvenberg-Marquardt și procesul de antrenare al algoritmului

Testarea (efectuată pe cele 62 de seturi – ”samples” – evidențiază diferențele minimale dintre ”Target” – albastru și ”Predicted output” – roșu:

Fig. 124 Diferențele minimale dintre "Target" – albastru și "Predicted output" – roșu în cazul ANNHUB

Ultima soluție Cloud AI a constituit o implementare a metodei "XGBoost" – XGB "eXtended Gradient Boosting" (cu optimizarea iterativă a clasificatorilor, prin combinarea "forțată"–"boosted", fără invalidare, a unor clasificatori aparent ne-performanți care, dacă ar fi luați în considerare individual, ar fi eliminați de calculele uzuale de convergență încă de la primele aproximări succesive).

Un prim model XGBoost *(xgbooxt-test-raw)* a fost implementat fără pre-normalizarea seturilor de date de instruire și testare (cele trei intrări - Sarcină, Turație și presiunea *p* a gazelor de eșapament precum și ieșirea *Pe,* puterea efectivă). S-a obținut un regresor (combinație de modele liniare) destul de performant: coeficientul de determinare "R squared", adică raportul varianța "explicită" (a valorilor prezise) / varianța valorilor observate (de testare) a fost 0,949760939140567, apropiat de 1 (s-a considerat varianța uzuală, σ^2 , pătratul deviației standard σ). Tipul de model a fost setat "manual" ca parametru "booster" pentru XGBRegressor (*gblinear* – alternativa fiind *gbtree)* și, după faza de antrenare, a fost exportat (ca *xgb_model.dat)* de către modulul *pickle,* spre a fi preluat de Python (așa cum se vede mai jos, implementarea XGBoost în Python a fost similară cu manipularea Keras a modelelor Tensorflow):

```
import pandas as pd
import xgboost as xgboost
import numpy as np
import pickle
from sklearn.metrics import explained_variance_score
train_dataset = pd.read_csv("./dataset/SV1_ANN_Data_Pe_Train.csv")
test_dataset = pd.read_csv("./dataset/SV1_ANN_Data_Pe_Test.csv")
train_stats = train_dataset.describe()
train_stats = train_stats.transpose()
train_y = train_dataset.pop("Pe")
xgb_model = xgboost.XGBRegressor(
  booster="gblinear", colsample_bytree=0.4, gamma=0,
  learning_rate=0.07, max_depth=3, min_child_weight=1.5,
  n_estimators=10000, reg_alpha=0.75,
  reg_lambda=0.45, subsample=0.6, seed=42)
test_y = test_dataset.pop("Pe")
predictions = xgb_model.predict(test_dataset)
print(explained_variance_score(predictions,test_y))
0.949760939140567
pickle.dump(xgb_model, open("xgb_model.dat", "wb"))
```

Fig. 125 Antrenarea eXtended Gradient Boosting Regressor (XGBRegressor) a modelului gblinear.

Modelul a fost rulat (în faza de testare), așa cum se vede mai jos, prin "citirea" modelului "boost" ("rb" – reading the boost) model care a fost "scris" ("wb" – "writing the boost") în faza de antrenare. În extrasul următor, XGBRegressor a prezis puterea efectivă (Pe) = 122.855095 kW pentru Sarcina = 90%, Turația = 1800 rpm, și presiunea (p) = 250 mmWC (Water Column – coloană de apă):

```
import pickle
import pandas as pd
import xgboost as xgboost
model = pickle.load(open("xgb_model.dat", "rb"))
L = 90
S = 1800
p = 250
df = pd.DataFrame([[L, S, p]], columns=["Load", "Speed", "p"])
prediction = model.predict(df)
print(prediction)

[122.855095]
```

Fig. 126 Predicția XGBRegressor a puterii efective (Pe) = 122,855095 kW pentru sarcină = 90%, turație = 1800 rpm și contrapresiune evacuare (EBP) (p) = 250 mmWC.

Expunerea *xgb_model.dat* printr-o API se poate face cu un micro-server web generat cu "Flask" mini-framework, programat în Python. O metodă HTTP (Hyper-Text Transfer Protocol) "GET" (Hyper-Text Transfer Protocol) poate recepționa direct parametrii ("Sarcină", "Turație" și "p") în URL-ul (Uniform Resource Locator) scris direct în bara de adrese a browserului, de exemplu, http://localhost:5000/api/predict? L=90&S=1800&p=250. *"xgb_model.dat"* (importat prin modulul *pickle* în micro- *server.py* minusculă) returnează valoarea "prediction".

Soluția XGB are opțiunea GridSearch (oferită de biblioteca dedicată Sklearn) pentru căutare și selecție optimală dintr-o multitudine de modele instruite cu mai multe combinații de parametri.

Analiza comparativă a metodelor Cloud AI s-a făcut pentru cele 62 de seturi de testare menționate anterior. Așa cum am menționat, pentru XGB, coeficientul de determinare ”R squared” a rezultat 0,949760939140567. Pentru GPR, așa cum se vede din ”Response Plot”, ”R squared” = 1 iar precizia relativă (calculată ca raportul dintre eroarea medie absolută, MAE, Mean Absolute Error și P e medie) a rezultat *MAE / mean_Pe* = 0,47993 / 82,76 = 0,5799%. Pentru L-M, așa cum se poate vedea din ultima listă rezultată în urma procesului de testare (stânga jos), ”R squared” = 0,999615. În fine, pentru metoda Keras, așa cum s-a arătat, pentru setul de testare, MSE = 0,01 deci RMSE = 0,1 astfel că precizia relativă se poate calcula, de data aceasta, *RMSE/ mean_Pe* = 0,1 / 82,76 = 0,1208%.

Metodele Cloud AI au avantajul specifc al MaaS care e intensiv computațional. MaaS e o capabilitate de mare viitor în direcția *"optimizării continue"* (susținută de IA) a algoritmilor în exploatare, o extensie a "implementării/desfășurării continue" (“continuous deployment”) a micro-serviciilor în Cloud.

(B-ii) Planuri de evoluție și dezvoltare a carierei

Premisele dezvoltării carierei universitare – realizări anterioare

Activitatea mea profesională s-a desfășurat în cadrul Departamentului de Electronică și Calculatoare al Universității Transilvania din Braşov, Facultatea de Inginerie Electrică și Știința Calculatoarelor, un colectiv dinamic, în care îmi regăsesc foarte multe valori. Am participat la activități diverse, de natură didactică, științifică, de cercetare sau de colaborare cu alte instituții sau firme din domeniul tehnologiei informațiilor și comunicațiilor.
În cadrul acestui colectiv îmi propun să îmi organizez cariera viitoare, iar obiectivul principal pentru care realizez acest plan al dezvoltării universitare este obținerea abilitării în vederea conducerii de lucrări de doctorat, un deziderat ce va sprijini dezvoltarea echipei de cercetare din care fac parte, un alt obiectiv fiind obținerea titlului științific de profesor în cadrul de Departamentului Electronică și Calculatoare.
Voi continua să îmi îndrept atenția către discipline ale programului de studii Securitate Cibernetică, de a cărui coordonare mă ocup, dar și ale programelor de licență ale departamentului, în special la nivelul programului de studiu "Tehnologii și Sisteme de Telecomunicații".
Voi rămâne implicat în activitățile de până acum, dar îmi propun să dezvolt şi să extind aceste activități. În această propunere de dezvoltare a carierei universitare voi arăta pașii pe care doresc să îi urmez în viitor, având la bază tot ce am obținut în carieră până acum, motiv pentru care descrierea de față cuprinde:

I Elementele de succes în cariera mea profesională anterioară

II Dezvoltarea carierei mele viitoare

I. Elementele de succes în cariera mea profesională anterioară

I. 1. Studii

Studii doctorale:

2007 - 2011 – Universitatea Transilvania din Braşov - Facultatea de Inginerie Electrică și Știința Calculatoarelor – am obținut Diploma de doctor în domeniul Inginerie Electronică și Telecomunicații cu teza intitulată „Soluții de mobilitate în rețele eterogene" sub coordonarea D-lui Prof. Dr. Ing. Florin SANDU.

Studii de master

2007 – 2009 – Universitatea Transilvania din Braşov – Facultatea de Inginerie Electrică și Știința Calculatoarelor, Masterat Rețele de Comunicații Digitale

Studii de licență

2002-2007 – Universitatea Transilvania din Braşov, Facultatea de Inginerie Electrică și Știința Calculatoarelor, Electronică Aplicată –Diplomă de inginer.

Pe lângă studiile universitare, datorită colaborărilor cu industria unde se cer unele certificări specifice, am efectuat stagii de:
- specializare tehnică, dintre aș menționa certificări Cisco CCNP, Cisco CyberOps, SND, Collaboration, bursa Fulbright în Statele Unite pentru Cybersecurity în universități, certificări Linux Professional Institute sau cursuri de audit de securitate
- specializare în management de proiecte și în coordonarea de echipe tehnice: certificările PRINCE 2 (Projects IN Controlled Environments) Foundation și Practitioner, Central Computer and Telecommunications Agency (CCTA); Harvard Business Publishing - Leading in the Digital Age (LIDA); în desfășurare este programul numit Gold for Technology Leaders, organizat de University of

Cambridge, Institute for Manufacturing (IfM) în colaborare cu Paderborn University – SICP, Software Innovation Campus Paderborn.

I. 2. Sumar de activitate

Realizările profesionale anterioare au îmbinat cariera academică și colaborarea cu industria. Experiența dobândită în proiecte internaționale din industrie, cu mare răspundere, s-a reflectat în cadrul parcursului academic, atât la nivel didactic, cât și din punct de vedere al cercetării.

Din punct de vedere didactic printre cele mai importante realizări aș menționa activitatea de fondator și coordonator al programului de master "Securitate cibernetică" la Universitatea "Transilvania" din Brașov, Facultatea de Inginerie Electrică și Știința Calculatoarelor, începând cu luna octombrie 2018, program de studii ce a trecut cu succes printr-un proces de acreditare ARACIS in anul 2020 (ca parte a DSUM – Domeniul de Studii Universitare de Master – ETTI, Electronică, Telecomunicații și Tehnologii Informaționale) și reprezintă unul dintre programele de studii atractive pentru absolvenți dar si pentru candidații din industria IT.

Înființarea programului de master “Cybersecurity” în limba engleza, într-un domeniu de actualitate si de mare atractivitate a presupus și un efort din punct de vedere al infrastructurii. Astfel s-a construit un mediu de laborator de securitate cibernetică virtualizată, bazat pe o sponsorizare inițială de aproximativ 100.000 EUR, urmată de alte investiții ale universității, un mediul de tip “cyberrange” –descris parțial in capitolul 3. Infrastructura a fost modernizată printr-un grant de cercetare pe care l-am obținut în urma unei alte competiții de proiecte în domeniul Cybersecurity organizată de Comisia Fulbright Polonia in anul 2022.

La momentul actual putem spune ca Universitatea Transilvania are una dintre cele mai dezvoltate platforme de laborator de securitate cibernetică din țară.

Din punct de vedere didactic înființarea programului de masterat a inclus o etapă importanta de elaborare a curriculei, ținând cont de recomandările Centrului National Cyberint care a devenit și partener al programului de master, susținând cu specialiști o parte dintre disciplinele de specialitate foarte tehnice. Pentru a dispune de experți în domeniu și a putea prezenta studenților ultimele tehnologii într-un domeniu foarte dinamic cum este cel al securității cibernetice, am inițiat mai multe colaborări cu industria IT locală ce sprijină programul de master și din punct de vedere didactic, ce au culminat cu lansare in anul 2021 a Brasov Cyber Hub, o inițiativă pe care doresc să o subliniez. Brasov Cyber Hub are printre membrii fondatori Universitatea Transilvania, Centrul National Cyberint, Agentia Metropolitană Brașov și compania Atos. Brasov CyberHub este organizat pe 3 direcții unde autorul a avut o implicare directă în implementări în sprijinul studenților dar și pentru prestigiul Universității Transilvania:

- Educațional: cursuri și workshop-uri dedicate (Cisco, Palo Alto), burse ISACA substanțiale valoric precum și acces gratuit la cursuri de specialitate pentru studenți interesați de securitate ciberentica, sustinere programului Vinere Cyber in licee sub coordonarea Cyberint
- Evenimente, „Hackatons”: aș sublinia un eveniment de tip CTF (Capture the Flag) care are loc anual în luna ianuarie și se numește CTF Eminescu.
- Antreprenoriat: acceleratorul de afaceri RoBoost inițiat de compania Atos.

Unul dintre evenimentele organizate de hub îl reprezintă “Brașov Cybersecurity Conference” care aduce la Brașov specialiști și companii de renume din domeniul IT (cu reprezentare la nivel de Country Managers), miniștrii și secretari de stat, directori ai Cyberint și ai Directoratului Național de Securitate Cibernetică, Brașovul devenind din acest punct de vedere un exemplu de bune practici la nivel de țară.

Tot din punct de vedere educațional am considerat extrem de important ca absolvenții noștri să poată obține certificări profesionale în domeniu, foarte importante pe piața muncii, considerându-le complementare pregătirii universitare, ci nu înlocuitoare ale acesteia. Astfel, începând cu anul 2015 am devenit instructor la Academia Cisco a Universității Transilvania (după o perioadă de câțiva ani în care

academia nu mai avea activitate), m-am certificat și am introdus la academie și cursuri în zona de Securitate Cibernetică și am stabilit noi parteneriate cu Comptia și EC-Council, precum și cu Hack-the-Box. În anul 2023 am pornit și o Academie Palo Alto, unul dintre producătorii importanți de soluții de Securitate cibernetică și suntem în discuții pentru inițierea unei Academii Microsoft (în special pe temele Cloud, Securitate și inteligență Artificială).
Partea de organizare și funcționare a unui program de masterat a fost aprofundată printr-o vizită de lucru in Statele Unite. În urma unui proces de selecție internațional, am participat la un stagiu Fulbright in Statele Unite ale Americii numit "Cybersecurity in Universities" desfășurat in lunile martie și aprilie 2022, ce a inclus întâlniri cu reprezentanți ai industriei și autorităților locale dar și vizite la universități americane de prestigiu și întâlniri cu coordonatorii programelor de Securitate cibernetică locale dintre care aș menționa: Columbia University, New York University, George Washington University, Maryland University, Marymount University, Mongomery College, precum și socializarea cu un grup de lucru format din cadre didactice ale unor universități europene.
Din punct de vedere al proiectelor de cercetare și colaborare cu alte universități am depus o propunere de proiect numita "Challenges Solving in Cybersecurity Study Program" pentru apelul de proiect Erasmus+ KA2 2023. Proiectul își propune îmbunătățirea programelor de studiu de securitatea cibernetică existente cu soluții educaționale inovatoare, ceea ce va duce și la o nouă etapă în dezvoltarea infrastructurii de laborator existente, iar partenerii din consorțiu sunt: Kaunas University of Technology (Lituania), University of Tartu (Estonia), University of Aveiro (Portugalia).
Tot la nivel de parteneriate universitare, prin intermediul consorțiului universitar UNITA la care se va alătura și Universitatea Transilvania, am pus bazele unor colaborări ce se pot dezvolta într-un posibil program de studii de masterat în parteneriat cu universități din Franta și Italia, precum și cu alte universități din Romania pe tema tehnologiilor centrate pe date (DataCentric tehnologies).

Rezultatele obținute pe parcursul activității de cercetare pot fi sumarizate astfel:
- 2 cărți/capitole de cărți în edituri internaționale;
- 3 cărți/capitole de cărți în edituri naționale;
- 4 materiale didactice în edituri naționale;
- 48 de articole științifice publicate în reviste și conferințe internaționale indexate ISI sau BDI, dintre care:
  - 11 în reviste indexate ISI; dintre care 8 în lista Q1 și Q2 după factorul de impact
  - 25 în proceedings indexate ISI;
  - 12 articole indexate BDI;
- in jur de 300 de citări în articole dintre care peste 80 în articole indexate ISI (reviste și proceedings);

- Responsabil partener / director în un proiect național și patru internaționale:
  - Responsabil partener și coordonator de proiect în ODIN 112 UEFISCDI PNIII Soluții - Contract 37SOL/2021, acronim ODIN112
  - Responsabil partener și coordonator de proiect în proiectul Orizont 2020 SARMENTI- "Smart multisensor embedded and secure system for soil nutrient and gaseous emission monitoring", ID acord de grant: 825325
  - Partener responsabil pentru proiectul "Implementation of a Voice Over IP Capability for NATO Wide Secure Voice Services: VOSIP", NATO Communication and Information Agency – NCIA, număr contract RFQ-C0-14137-VOSIP,
  - Partener responsabil pentru proiectul "EGSE for Small Sat - A Baseline Verification and Validation", 2018-2019; Grant acordat de: ESA - Agenția Spațială Europeană, Apel: Romanian Incentive Scheme – Activity Type b) – Activități de cercetare-dezvoltare
  - Responsabil partener și coordonator: Proiect Comisia Fulbright CS07 - Ofertă minigrant pentru dezvoltarea programelor orientate spre securitate cibernetică perioada:2022-2023
- Membru în echipele de cercetare în 6 proiecte internaționale

- Management Committee member (substitute) in COST Action CA15104 – "Inclusive Radio Communication Networks for 5G and beyond (IRACON), 2016 – 2020, EU H2020
- Management Committee member (substitute) in COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living – GOOD BROTHER, 2020-2024
- Member in COST Action CA20120 - Intelligence-Enabling Radio Communications for Seamless Inclusive Interactions (INTERACT) 2021-2025
- EU FP7 Project 4WARD - Architecture and Design for the Future Internet (2008-2010), contract number: 216041
- Leonardo da Vinci project: "Valorisation of an Experiment-based Training System through a Transnational Network Development – VET-TREND", RO/06 / B /F /NT175014 – under the supervision of „Transilvania" University of Brasov (2006-2008)
- European Union Program – eSTART "Program multi-regional de studii masterale in domeniul e-Activitati eSTART" POSDRU /86/1.2/S/54956
- Reprezentant al Universității Transilvania cu rol de observator/consultant pentru proiectul QTSTRAT - Elaborarea strategiei pentru dezvoltarea capabilităților naționale în domeniul comunicațiilor cuantice, Contract: 2 PS / 11.11.2021, Universitatea Babeș-Bolyai din Cluj-Napoca (UBB)

- Alte proiecte depuse sau în evaluare:
  - Erasmus + KA2 "Challenges Solving in Cybersecurity Study Program", în evaluare, depus în martie 2023
  - Proiect depus in competiția UEFISCDI PN-III-CERC-CO-PED-3-2021, Kit de securitate împotriva amenințărilor cibernetice pentru administrația publică, proiect in parteneriat cu Directoratul National de Securitate Cibernetica (DNSC) și Agenția Metropolitană Brașov (AMB), cu o propunere de soluție de Securitate pentru administrația publica, declarat necâștigător
- Membru în asociații științifice:
  - IEEE (Institute of Electrical and Electronics Engineers)
  - IEEE Broadcasting Society
  - Membru Task Force Cybersecurity în cadrul ANIS (Asociația Națională pentru Industria de Software)
  - Membru al DC Cybersecurity TaskForce, grup pe lucru coordonat de Camera de Comerț a României în Statele Unite, la Washington DC
- Premii și distincții:
  - Câștigător regional - ESNC (European Satellite Navigation Competition 2016) – competiție de inovare organizată de Agenția Spațială Europeană, calificat în finala competiției de la Madrid, octombrie 2016
  - Premiul ANIS – "Premiul Asociației Patronale a Industriei de Software și Servicii" pentru propunerea unui curriculum în domeniul securității cibernetice pentru disciplina "Securitatea rețelelor și apărarea perimetrală"
  - Cisco Instructor Excellence Award - Advanced Level Instructor since 2019
- Recenzor pentru diferite reviste precum: IEEE Access, Measurement, IEEE Transactions On Broadcasting, Wireless Networks, Sensors, Applied Sciences

Activitatea de cercetare și dezvoltare a autorului a început în industrie, prin parcursul profesional anterior anului 2013 al angajării în cadrul Universității Transilvania din Brașov dar și prin proiectele și colaborările susținute până în prezent alături de firme relevante din domeniu (Siemens, Nokia Siemens Networks, Atos, Eviden). Consider că modul de lucru în proiecte internaționale, cu mare răspundere, în contact cu cele mai noi tehnologii, precum și componenta antreprenorială pe care trebuie să o transmitem și către absolvenți, se conturează foarte bine prin colaborarea cu industria. Experiența din industrie și rolurile ocupate în diverse stadii de timp de pot rezuma astfel:

- Head of Cybersecurity (Big Data and Security) – arhitect soluții tehnice (CyberSecurity, Mission Critical Systems), coordonare strategie și ofertă pentru piața locală
- Presales Manager (Big Data and Security) – definire/arhitect soluții tehnice (CyberSecurity, Mission Critical Systems), contact cu clienții și identificare oportunități de piață, coordonare oferte pentru elaborarea ofertelor, estimări ale efortului tehnic, lucrul cu echipe din departamentele Juridic, Comercial, Achiziții și productive pentru elaborarea ofertelor/contractelor
- Product Lifecycle Manager – Suorite din 2012 până în 2013, responsabil pentru definirea soluțiilor și liniei de produse Suorite (un set de instrumente software pentru monitorizarea rețelei și migrarea datelor), responsabil pentru controlul investițiilor, procesul de dezvoltare, poziționarea pe piață, strategia de marketing și vânzări
- Manager de proiect: Coordonarea soluției inovatoare pentru managementul resurselor în Cloud - echipa IaaS FARM (Infrastructure as a Service Framework for Automatic Resource Management)
- Arhitect pentru soluții de comunicații și securitate – arhitectură de soluții personalizate pentru diferiți clienți (NATO, ESA, Siemens), soluții de comunicare, securitate cibernetică și cloud
- Inginer Telecomunicații – 10.2005-05.2008: Planificarea, optimizarea și configurarea rețelelor de comunicații, integrare și testare a software-ului de comunicații și a platformelor telecom dedicate rețelelor mobile - teste de interoperabilitate (IOT);

În cadrul centrului R&D Center Düsseldorf al Nokia Siemens Networks, între anii 2008 și 2010 am activat ca și Inginer integrare și testare software de telecomunicații, în echipa de dezvoltare a primelor echipamente 4G LTE - LTE eNodeB Transport Module pentru NTT Docomo Japonia și Nokia Siemens Networks.

II Dezvoltarea carierei mele viitoare

Cadrul prin care îmi propun construirea carierei se bazează pe un set de valori: feedback, transparență, deschidere la nou, comunicare, lucru în echipă, colaborări cu mediul socio-economic pe baza atragerii unor contracte în cadrul universității. Mă bazez pe susținerea acestor valori din partea colectivului Departamentului de Electronică și Calculatoare și pe promovarea lor în rândul colaboratorilor.

În cazul acceptării tezei de abilitare voi avea ca obiectiv descoperirea și implicarea atât a studenților cât și a altor persoane dornice și capabile sa-și lărgească și îmbunătățească cunoștințele științifice prin studii de doctorat.

Îmi doresc să construiesc o carieră academică în cadrul unui colectiv cu un înalt nivel profesional ce va contribui la creșterea valorică a programelor de studii din facultate și a rezultatelor de cercetare ce vor conduce spre creșterea reputației, succesul și o vizibilitate crescută a Facultății de Inginerie Electrică și Știința Calculatoarelor din cadrul Universității Transilvania Brașov. Instrumentele utilizate în îndeplinirea planului de dezvoltare vor fi atât menținerea și creșterea standardelor de excelență academică și profesională, cât și colaborarea nemijlocită cu colegii – cadre didactice și de cercetare – și cu studenții.

Ca obiectiv imediat îmi propun menținerea și creșterea valorică a programului de masterat de CyberSecurity pe care îl coordonez, dar și creșterea unui ecosistem școlar și a unei echipe de colegi și colaboratori în scopul obținerii de granturi de cercetare și a implementării de proiecte noi și metode noi de lucru cu studenții, masteranzii și doctoranzii.

Un rezultat imediat al obținerii abilitării va fi posibilitatea de coordonare de doctoranzi, un pas necesar pentru a putea strânge colaborarea cu absolvenți de mare valoare sau colaboratori din industrie (unii dintre ei deja implicați în activități ale universității) ce și-au exprimat deja de câțiva ani dorința de a colabora în cadrul unui doctorat. Până la momentul de față, datorită lipsei

abilitării, am reușit să colaborez pe teme interdisciplinare cu alți colegi abilitați față de care îmi exprim gratitudinea pentru modul de lucru deschis și eficient pe care îl avem. Astfel, în prezent fac (sau am făcut) parte din comisiile de îndrumare ale unor doctoranzi (unul dintre ei devenit doctor), dintre care aș dori să remarc primii patru doctoranzi din lista de mai jos, ale căror teme sunt în zona de securitate cibernetică:

- Drd. Lucian Ilca, coordonator Prof. Dr. Petre Ogrutan, tema: Detecția și răspunsul automat la amenințări de securitate cibernetică
- Drd. Alexandre Rekeraho, coordonator Prof. Dr. Daniel Cotfas, tema: Cyber security challenges for IoT-based smart renewable energy networks
- Drd. Rebecca Acheampong, coordonator Prof. Dr. Dorin Popovici, tema: Addressing Cybersecurity Concerns in Virtual and Augmented Reality
- Drd. Tuyishime Emmanuel, coordonator Prof. Dr. Petru Cotfas, tema: Addressing Cybersecurity Challenges in Remote Control Engineering Applications
- Drd. Mihai Oproiu, coordonator Prof. Dr. Petru Cotfas, tema: Contribuții la utilizarea sistemelor de instrumentație virtuală în domeniul energiilor regenerabile
- Drd. Florin Radu, coordonator Prof. Dr. Petru Cotfas, tema: Instrumentația virtuală și controlul la distanță – aplicații în educație, cercetare și industrie
- Drd. Horia Modran, coordonator Prof. Dr. Doru Ursuțiu, tema: Sisteme bazate pe Inteligență Artificială în procesarea avansată a semnalelor
- Dr. Tinasche Chamunorwa, coordonator Prof. Dr. Doru Ursuțiu, tema: New Methods and Systems for Computer-based Learning in Digital Electronics Education

Aceste colaborări prin teme de doctorat interdisciplinare ce îmbină securitatea cibernetică cu alte domenii au început să aibă primele rezultate de cercetare, publicații la conferințe și jurnale indexate ISI (unele dintre ele se regăsesc în lista de lucrări prezentată în zona de bibliografie).

Activitățile de cercetare viitoare se vor baza pe experiența acumulată până în prezent ce se regăsește în cele trei capitole ale prezentei teze: domeniul comunicațiilor, al sistemelor Cloud și IoT, domeniul securității cibernetice și domeniul inteligenței artificiale ce își exercită influența asupra domeniului ICT în general. Experiențele acumulate vor fi în permanență actualizate și vor include noile tendințe impuse de tehnologie, piață și industrie.
Securitatea cibernetică reprezintă un domeniu orizontal, componentă constituentă a aproape fiecărui sistem electronic, din faza de proiectare, în etapele de dezvoltare, testare și până la integrarea și rularea de servicii pentru beneficiarul final. Fiind un domeniu orizontal, se poate aplica cu succes în mai multe domenii verticale, dintre care aș numi pe cele: medical, militar/apărare, transport și telecomunicații, financiar, energetic, etc.
Securitatea cibernetică a devenit parte din strategia de securitate a statelor și alianțelor.

Astfel, direcțiile de cercetare, care vor reprezenta baza temelor de doctorat propuse, vor aborda domenii verticale ce corespund/țintesc viitoare apeluri de finanțare și valorificare a rezultatelor, precum și cerințele unor posibili parteneri industriali sau academici.
Exemple de direcții de cercetare posibile:

1. Metode de detecție și răspuns la incidente aplicate:
   1.a) – sistemelor critice și aplicațiilor militare (pentru a beneficia de deschiderea finanțărilor din proiectele European Defence Fund, fondurile de inovare NATO Diana și de relația bună în proiectul ODIN112 descris în teză, realizat anterior cu Academia Tehnica Militară)
   1.b) – sistemelor medicale (pentru a beneficia de parteneriatele formate în cadrul proiectului COST Action Good Brother cu UMF ”Carol Davila” din București și cu alți parteneri)

2. Sisteme de securizare în Cloud și securizare Edge-to-Cloud (pentru a putea beneficia de parteneriatul cu firma Atos/Eviden care are un centru de competențe la nivel global pentru securitate Cloud în Romania, precum și de alte parteneriate cu Microsoft și alți producători)
3. Automatizarea și securizarea metodelor de colaborare în societatea digitală pentru administrația publică (sinergii cu activitățile Brașov CyberHub unde Agenția Metropolitană Brașov este partener și necesitatea implementării de soluții bazate pe inteligență artificială în administrație)
4. Rețele de calculatoare cuantice sau teme legate de post-quantum cryptography (datorită existenței grupului QTSTRAT și a mai multor inițiative de finanțare în această zonă).

Temele de mai sus sunt doar unele exemple, de subliniat este dorința de orientare a temelor spre proiecte, posibile finanțări și parteneriate, mergând până la viitoare valențe comerciale (pe modelul de incubare/spin-off pe care unele universități în promovează).

Obiectivele de cercetare în domeniul comunicațiilor și al securității cibernetice:

- sporirea valoarii colectivului de cercetare al departamentului și în special a direcției de cercetare deja definită în zona de "Tehnologii de comunicații și securitate cibernetica" cu două subdomenii: Soluții de telecomunicații și Soluții de Securitate cibernetică.
- atragerea de fonduri prin participarea la proiecte naționale, internaționale și cu terți prin inițierea sau participarea la propuneri de proiecte cu colaboratori din țară și din străinătate;
- pregătirea de viitoare cadre didactice cu expertiză ridicată (programul de masterat "Securitate Cibernetica" este foarte căutat, atrăgând parte dintre absolvenții cei mai buni, deci avem avantajul lucrului cu o resursă umană de înaltă calitate)
- creșterea impactului și a vizibilității autorului și echipei din care face parte, a facultății și a universității - prin valorificarea rezultatelor cercetărilor, prin publicarea de articole în reviste și cărți în edituri recunoscute (reviste cu factor de impact mare cotate Q1 și Q2 – cel puțin un articol pe an), participarea la conferințe internaționale de prestigiu cotate ISI sau indexate în baze de date (publicarea a cel puțin două articole pe an) și implicarea în organizarea de evenimente științifice dintre care aș vreau să subliniez inițiativa Brașov CyberHub;
- lărgirea bazei materiale existente în prezent în laboratorul de cercetare, prin dotare cu noi echipamente de ultimă generație sau dezvoltarea de noi elemente de laborator virtualizat ce pot deveni baza unor viitoare colaborări
- consolidarea colaborărilor existente și dezvoltarea altora la nivel național și internațional - prin inițierea de parteneriate de tip Erasmus+, participarea la propuneri comune de proiecte sau organizarea de evenimente științifice; strângerea relațiilor cu mediul economic și cu producătorii de tehnologie; doresc continuarea și întărirea parteneriatelor deja construite cu instituții cu atribuții in domeniul securității cibernetice dintre care voi menționa: Centrul Național Cyberint, Directoratul Național pentru securitate Cibernetică, Serviciul de Telecomunicații Speciale, Academia Tehnica Militară, Agenția de Cercetare pentru Tehnică și Tehnologii Militare (ACTTM), Departamentul Regional de Studii pentru Managementul Resurselor de Apărare (DRESMARA).

Activitatea de cercetare e direct legată de cea didactică. Obiectivele activității didactice avute în vedere pentru dezvoltarea carierei didactice a autorului sunt:

- creșterea valorii didactice la nivel de curs și laboratoare ale programului de master Cybersecurity pe care autorul îl coordonează, ale departamentului (DEC) și facultății (IESC) în vederea pregătirii altor vizite de acreditare (realizarea unui fond consistent de publicații în domeniu, inclusiv materiale didactice);

- Utilizarea metodelor moderne de educație bazate pe interactivitate, problematizare și aplicare practică;
- Implementarea de simulări software, laboratoare virtuale și în Cloud, de demonstrații practice bazate pe sisteme electronice portabile sau pe accesarea laboratoarelor la distanță în cadrul activităților de predare, în vederea creșterii atractivității cursurilor teoretice;
- Dezvoltarea sau actualizarea materialelor didactice bazate pe rezultatele cercetărilor efectuate sau a studiilor bibliografice din domeniu și prezentarea lor în format digital.
- Modernizarea continuă a lucrărilor de laborator;
- Încurajarea și coordonarea studenților în efectuarea de mobilități Erasmus+ pentru dezvoltarea lor personală, prin realizarea schimbului științific și cultural din cadrul universităților partenere;
- Implicarea studenților în activitățile de cercetare în vederea participării lor la manifestări și evenimente științifice și precum și la competiții studențești - în acest sens se dorește, în parteneriat cu Brașov CyberHub organizarea de ”hackatons” și competitii de tip Capture the Flag cu teme definite de posibili beneficiari. Rezultatele competițiilor de tip hackaton pot deveni primele idei ce pot fi promovate în programe de mentorat și inovare de tip Innovation Labs și mai târziu se pot transforma în entități de tip startup. De aceea un obiectiv important este încercarea de formare a unei gândiri antreprenoriale în rândul studenților;
- Identificarea și atragerea studenților de la master către studiile doctorale în vederea formării lor ca specialiști de top în domeniul de activitate;
- Lucrul în echipe de lucru mixte, ce implică studenți din ani de studii diferite, pentru a exista continuitate a unor proiecte. Implicarea în echipa mixte și a unor elevi: dezvoltarea colaborării cu mediul preuniversitar la nivel de liceu în vederea atragerii elevilor către domeniile de inginerie.
- O mai bună mediatizare a rezultatelor și realizărilor studenților și cadrelor didactice.

Adițional, cu sprijinul conducerii, sunt realizabile următoarele obiective:

- Doresc realizarea unui puternic centru de certificare pentru academii relevante în cadrul facultății IESC: pe langa Academia Cisco deja existentă, Academia Palo Alto / Fortinet și Academia Microsoft (o academie cu multiple beneficii pentru studenți, de la teme de programare și inteligență artificială, la cele ce se referă la elemente de Cloud;
- Implicarea industriei și a unor beneficiari în alegerea unor teme de proiect și de practică relevante pe care studenții să le rezolve în echipă (metodă pe care am observat-o în timpul vizitei de lucru Fulbright în Statele Unite ale Americii);
- Dezvoltarea colaborărilor deja începute în cadrul consorțiului universitar UNITA și posibilitatea unor sisteme de diplomă dublă;
- Posibilitatea de oferire de micro-credite și cursuri dedicate pentru terți;
- Continuarea și sporirea numărului de evenimente ale Brașov CyberHub, respectiv organizarea de noi ediții ale conferinței hub-ului.

(B-iii) Bibliografie

Capitolul 1

[1] **Balan, T.**, Robu, D. and Sandu, F., 2017. Multihoming for mobile internet of multimedia things. *Mobile Information Systems*, *2017*.

[2] **Balan, T.**, Robu, D. and Sandu, F., 2016. LISP Optimisation of Mobile Data Streaming in Connected Societies. *Mobile Information Systems*, *2016*.

[3] **Balan, T.**, Zamfir, S., Robu, D. and Sandu, F., 2016, June. Contributions to content-based software defined networks. In *2016 International Conference on Communications (COMM)* (pp. 159-162). IEEE.

[4] Zamfir, S., **Balan, T.**, Sandu, F. and Costache, C., 2016, June. Solutions for deep packet inspection in industrial communications. In *2016 International Conference on Communications (COMM)* (pp. 153-158). IEEE.

[5] **Balan, T.C.**, 2014. Network policy function virtualization via SDN and packet processing. *Review of the Air Force Academy*, (3), p.73.

[6] Costache C., **Balan T.**, Sandu F., Robu D., 2014, Software-Defined Networks for Secure Distributed Industrial Communications, *6th Győr Symposium and 3rd Hungarian-Polish and 1st Hungarian-Romanian Joint Conference on Computational Intelligence, 2014*

[7] Zamfir, S., **Balan, T.** and Sandu, F., 2015. Automating Telecom Equipment for Cloud Integration. *Review of the Air Force Academy*, (3), p.113.

[8] **Balan T**., Hadade A, Machidon O, Curpen R, 2013, Service Creation Environment for Distributed Telecom Infrastructure – IaaS, *The 4th International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics, (MACRo2013)*

[9] Nica, A., Balan, A., Zaharia, C. and **Balan, T.**, 2022. Automated Testing of GUI Based Communication Elements. In *Online Engineering and Society 4.0: Proceedings of the 18th International Conference on Remote Engineering and Virtual Instrumentation* (pp. 380-390). Springer International Publishing.

[10] Curpen, R., **Balan, T.**, Sandu, F., Costache, C. and Cerchez, C., 2014, May. Demonstrator for voice communication over LTE. In *2014 10th International Conference on Communications (COMM)* (pp. 1-4). IEEE.

[11] **Balan, T.**, Stanciu, A., Sandu, F. and Surariu, S., 2017. WEBRTC BASED ELEARNING PLATFORM. *eLearning & Software for Education*, *2*.

[12] Robu, D., Curpen, R., Ilie, D., **Balan, T.** (2021). Open Source Online Conference System for Industry Experts Participation in Education. In: Auer, M.E., Tsiatsos, T. (eds) Internet of Things, Infrastructures and Mobile Applications. IMCL 2019. Advances in Intelligent Systems and Computing, vol 1192. Springer

[13] **Balan, T.C.**, Robu, D.N. and Sandu, F., 2015, October. Ad-hoc lab computer network configuration using remote resources. In *2015 IEEE 21st International Symposium for Design and Technology in Electronic Packaging (SIITME)* (pp. 393-396). IEEE.

[14] Sandu, F., Costache, C. and **Balan, T.**, 2015, October. Semantic data aggregation in heterogeneous learning environments. In 2015 IEEE 21st International Symposium for Design and Technology in Electronic Packaging (SIITME) (pp. 409-412). IEEE.

[15] Zamfir, S., **Balan, T.**, Sandu, F., Costache, C. (2016). Mobile Communication Solutions for the Services in the Internet of Things. In: Exploring Services Science. IESS 2016. Lecture Notes in Business Information Processing, vol 247. Springer

[16] **Balan T.**, Bîrlă P, Marcu C, Onceru I, IoT Web-Shared Variables–Publish, Collect And Analysis In The Cloud, Review of the Air Force Academy, pg. 65-70, 2017, issn:20694733 isbn:1842-9238

[17] Stanciu A, **Balan T.**, Sandu F. and Gerigan C., "Reconfigurable platform for embedded systems teaching," 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), Constanta, Romania, 2017

[18] Machidon O., **Balan T.**, Curpen R., „Cloud Perspective on Reconfigurable Hardware", Review of the Air Force Academy – Brasov, Romania Vol XII, No 2/2013, pag.23-28

[19] Costache C., Sandu F., **Balan T.**, Nedelcu A., Covei A."Business Integration of Industrial Communications with Cloud Computing", 10th International Conference on Communications, Bucharest, May 29-31, 2014

[20] **Balan, T.**, Balan, A. and Sandu, F., 2019. SDR implementation of a D2D security cryptographic mechanism. *IEEE Access*, *7*, pp.38847-38855.

[21] Timofte, A.G., Florin, R.A.D.U., Balan, A. and **Balan, T.C.**, 2020, June. SDR-Based Platform for Processing the Images Transmitted Through the WLAN 802.11 a Protocol. In *2020 13th International Conference on Communications (COMM)* (pp. 387-392). IEEE.

[22] Robu D., **Balan T.**, Stanciu A. and Sandu F., "SDR-assisted device-to-device communication in radio-congested environments," *2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Cagliari, Italy, 2017, pp. 1-7

[23] Sârbu, A., Bechet, A., **Balan, T.**, Robu, D., Bechet, P. and Miclăuș, S., 2019. Using CCDF statistics for characterizing the radiated power dynamics in the near field of a mobile phone operating in 3G+ and 4G+ communication standards. *Measurement*, *134*, pp.874-887.

Capitolul 2

[24] **Balan, T.**, Robu, D., Sandu, F., Balan, A. (2021). Building a Virtualized Cybersecurity Lab. In: Auer, M.E., Tsiatsos, T. (eds) Internet of Things, Infrastructures and Mobile Applications. IMCL 2019. Advances in Intelligent Systems and Computing, vol 1192. Springer

[25] Acheampong, R., **Balan, T.C.**, Popovici, D.M. and Rekeraho, A., 2022, June. Security scenarios automation and deployment in virtual environment using ansible. In 2022 14th International Conference on Communications (COMM) (pp. 1-7). IEEE

[26] Ilca, L.F., **Balan, T.** (2022). Purple Team Security Assessment of Firmware Vulnerabilities. In: Auer, M.E., Bhimavaram, K.R., Yue, XG. (eds) Online Engineering and Society 4.0. REV 2021. Lecture Notes in Networks and Systems, vol 298. Springer

[27] Ilca L. and **Balan T.**, "Windows Communication Foundation Penetration Testing Methodology," 2021 16th International Conference on Engineering of Modern Electric Systems (EMES), Oradea, Romania, 2021

[28] Rekeraho A., **Balan T.**, Cotfas D., Cotfas P, R. Acheampong and C. Musuroi, "Sandbox Integrated Gateway for the Discovery of Cybersecurity Vulnerabilities," 2022 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 2022

[29] Zamfir S., **Balan T.**, Iliescu I. and Sandu F., "A security analysis on standard IoT protocols," 2016 International Conference on Applied and Theoretical Electricity (ICATE), Craiova, Romania, 2016

[30] Stanciu A, **Balan T.**, Gerigan C. and Zamfir S., "Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm," 2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP), Brasov, Romania, 2017

[31] Balan, A., **Balan, T.**, Cirstea, M. and Sandu, F., 2020. A PUF-based cryptographic security solution for IoT systems on chip. EURASIP Journal on Wireless Communications and Networking, 2020(1), pp.1-22.

[32] Machaka, V. and **Balan, T.**, 2022. Investigating Proactive Digital Forensics Leveraging Adversary Emulation. Applied Sciences, 12(18), p.9077.

[33] Ilca F. and **Balan T.**, "Phishing as a Service Campaign using IDN Homograph Attack," 2021 International Aegean Conference on Electrical Machines and Power Electronics (ACEMP) & 2021 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM), Brasov, Romania, 2021

Capitolul 3

[34] **Balan, T.**, Dumitru, C., Dudnik, G., Alessi, E., Lesecq, S., Correvon, M., Passaniti, F. and Licciardello, A., 2020. Smart multi-sensor platform for analytics and social decision support in agriculture. Sensors, 20(15), p.4127.

[35] Lesecq, S., Gougis, M., Gouze, E., Di Matteo, A., Alessi, E., Di Palma, V., Di Salvo, S., O'Riordan, A., Shao, H., Mouzakitis, G., **Balan T.** and Ponsardin, G., 2020, November. SARMENTI: in-situ real-time soil nutrients and gaseous emission measurement. In 2020 7th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE) (pp. 1-4). IEEE.

[36] Mocanu, B.C., Filip, I.D., Ungureanu, R.D., Negru, C., Dascalu, M., Toma, S.A**., Balan, T.C.**, Bica, I. and Pop, F., 2022. ODIN IVR-interactive solution for emergency calls handling. Applied Sciences, 12(21), p.10844.

[37] Ungureanu, D., Toma, S.A., Filip, I.D., Mocanu, B.C., Aciobăniței, I., Marghescu, B., **Balan, T.**, Dascalu, M., Bica, I. and Pop, F., 2023. ODIN112–AI-Assisted Emergency Services in Romania. Applied Sciences, 13(1), p.639.

[38] Radu, F., Cotfas, P.A., Alexandru, M., **Balan, T.C.**, Popescu, V. and Cotfas, D.T., 2023. Signals Intelligence System with Software-Defined Radio. Applied Sciences, 13(8), p.5199.

[39] Fernoaga, V., Sandu, V. and **Balan, T.**, 2020. Artificial intelligence for the prediction of exhaust back pressure effect on the performance of diesel engines. Applied Sciences, 10(20), p.7370.