UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCUREȘTI

ȘCOALA DOCTORALĂ DE AUTOMATICĂ ȘI CALCULATOARE
DEPARTAMENTUL DE CALCULATOARE

Rezumatul tezei doctorale

Securizarea infrastructurilor digitale medicale

Coordonator ştiinţific:
Prof. Dr. Ing. Răzvan Rughiniș

Autor:
Cristian Contasel

BUCUREŞTI

2024

Cuprins

Abstract

Utilizarea sistemelor software e-Sănătate (e-Health) devine din ce în ce mai răspândită în viața noastră de zi cu zi. Sistemele e-Sănătate îmbunătățesc siguranța medicală, minimizează erorile umane și reduc costurile prin automatizarea unei varietăți de fluxuri și proceduri. Pentru a putea face față amenințărilor de securitate, sistemele e-Sănătate necesită o securitate cibernetică robustă, fapt accentuat de adoptarea lor tot mai rapidă în societate. Amenințările cibernetice cu care se confruntă aceste sisteme au potențialul de a compromite îngrijirea pacienților, de a perturba asistența medicală și de a compromite confidențialitatea datelor.

Teza prezentă investighează preponderent soluții software destinate îmbunătățirii rezistenței securității cibernetice a sistemelor de e-Sănătate. Sunt prezentate soluții și metodologii inovatoare pentru contracararea eficientă a amenințărilor de securitate cu care se confruntă serviciile cloud destinate domeniului de e-Sănătate.

Teza este organizată în opt capitole, dintre care un capitol introductiv, un capitol cu privire la stadiul tehnologic actual, cinci capitole de contribuții și un capitol de încheiere și concluzii.

Primul capitol de contribuții se concentrează pe îmbunătățirea arhitecturii sistemelor informatice cu scopul de a atenua amenințările de securitate. Acest lucru se realizează prin dezvoltarea unui nou model arhitectural ce se bazează pe microservicii, cu scopul de a izola și atenua amenințăriile fără a compromite funcționalitatea sistemului de e-Sănătate.

Al doilea capitol de contribuții abordează îmbunătățirea securității sistemelor de e-Sănătate în ceea ce privește mecanismele de autentificare prin valorificarea capacităților telefoanelor inteligente de a prelucra date biometrice și geografice. Astfel, se introduce un mecanism de autentificare îmbunătățit care se bazează pe OAuth 2.0.

Al treilea capitol de contribuții este dedicat îmbunătățirii securității comunicaților dintre dispozitivele medicale portabile și serviciile e-Sănătate. Pentru a putea realiza acest lucru, este propus un nou modul numit Personal Medical Hub. Scopul acestuia de a proteja comunicațiile de atacturi de tip man-in-the-middle.

Al patrulea capitol de contribuții este dedicat îmbunătățirii și analizei comunicațiilor dintre serviciile cloud e-Sănătate și dispozitivele medicale personale/portabile. Obiectivul analizei este de a optimiza consumul de energie și de a garanta schimbul eficient de date între dispozitive, menținând costurile de dezvoltare cât mai reduse.

Ultimul capitol de contribuții introduce un nou model de securizare a sesiunilor care utilizează metode de atestare a dispozitivului client pentru a proteja serviciile cloud, cu scopul de a reduce riscurile asociate diverselor tipuri de amenințări informatice.

Baza tuturor capitolelor de contribuții este reprezentată de soluții software, care au scopul de a valida metodologiile și tehnologiile propuse. Teza reprezintă o bază de studiu pentru cercetările ulterioare, în special în domeniul securizării sistemelor e-Sănătate prin îmbunătățirea serviciilor de tip cloud și utilizarea tehnologiilor puse la dispoziție de către telefoanele inteligente.

Cuvinte cheie: e-Sănătate, securitatea sistemelor e-Sănătate, OAuth 2.0, API-uri de atestare, metodologii de dezvoltare multiplatformă, microservicii e-Sănătate, servicii REST, SafetyNet, Xamarin, monitorizarea pacienților, autentificare, cloud computing.

1. Introducere

1.1 Motivația

Indiferent dacă suntem cetățeni obișnuiți sau profesioniști medicali, sistemele de e-Sănătate au devenit o parte a vieții noastre de zi cu zi. Ținând cont de faptul că ne bazăm pe acestea nu doar pentru monitorizarea stării de sănătate, ci și pentru tratarea și gestionarea bolilor cronice, trebuie să le dăm și capacitatea de a face față problemelor de securitate informatică și de a se asigura că serviciile acestora sunt mereu disponibile.

Având în vedere progresul continuu al tehnologiei, puterea de calcul în creștere, precizia și performanța roboților, precum și dezvoltarea continuă a inteligenței artificiale (AI), este de așteptat ca sistemele de e-Sănătate să se îmbunătățească progresiv, iar serviciile lor să devină accesibile pentru publicul general.

Cu toate acestea, este important să recunoaștem că dezvoltarea sistemelor de e-Sănătate capabile să trateze în mod independent pacienții, fără a fi nevoie de profesioniști medicali, este încă un scenariu inaccesibil. Sistemul medical este în mod inerent conservator, iar tehnologia este încă insuficient de avansată. Deși roboții și dispozitivele profesionale folosite în clinici se îndreaptă spre acest obiectiv, există o creștere alarmantă a vulnerabilităților în securitatea sistemelor software pe care se bazează. Aceste vulnerabilități sunt determinate în primul rând de consumul excesiv de resurse hardware și de costul ridicat al hardware-ului necesar.

Această teză examinează diferite măsuri de securitate pentru sistemele de sănătate electronică, concentrându-se pe principalele servicii și pe componentele lor integrate, cum ar fi dispozitivele portabile (de exemplu, pompele de insulină). Acesta își propune să abordeze provocările de securitate cu care se confruntă profesioniștii din domeniul medical și consumatorii, oferind soluții practice testate în scenarii din lumea reală.

1.2 Obiective

Această teză își propune să investigheze soluții pentru îmbunătățirea securității sistemelor de e-Sănătate. Se concentrează pe abordarea problemelor de securitate identificate la nivelul serviciilor de bază, la nivel de comunicare și la nivelul consumatorului final. Soluțiile propuse pentru îmbunătățirea securității sistemelor de e-Sănătate au fost testate și validate în scenarii reale.

Întrebările principale pe care teza încearcă să le abordeze sunt:

- Cum putem profita de smartphone-urile pentru a spori securitatea cibernetică a sistemelor de e-Sănătate?
- Cum putem îmbunătăți securitatea cibernetică și reziliența sistemelor de e-Sănătate prin adoptarea unei arhitecturi bazate pe microservicii?
- Cum putem integra în siguranță dispozitivele medicale portabile într-un sistem e-Sănătate fără a compromite securitatea cibernetică a sistemului?

1.3 Structura tezei

Prezenta teză este alcătuită din 8 capitole, după cum urmează: un capitol introductiv, un capitol privind stadiul actual tehnologic, 5 capitole de contribuții și un capitol de încheiere care conturează contribuțiile acestei teze și prezintă direcțiile de cercetare viitoare.

Capitolul inițial, cunoscut sub numele de introducere, urmărește să explice și să descrie motivația din spatele acestei teze. În plus, subliniază întrebările de cercetare primare pe care teza încearcă să le abordeze.

Al doilea capitol prezintă stadiul actual al securității sistemelor de e-Sănătate. Soluțiile de securitate pentru sistemul de e-Sănătate sunt împărțite în funcție de componentele care sunt vizate. Prin urmare, capitolul abordează următoarele subiecte: securitatea și disponibilitatea sistemului central e-Health, securitatea dispozitivelor medicale, securitatea aplicațiilor client de tip REST și securitatea globală a ecosistemului e-Sănătate.

Al treilea capitol corespunde garantării unui nivel ridicat de disponibilitate a serviciilor de e-Sănătate pentru a permite elementelor fundamentale ale sistemului să facă față fluctuațiilor de trafic. Modelul arhitectural principal pentru nucleul sistemului e-Sănătate este identificat în primul subcapitol, care prezintă și impactul pandemiei COVID-19 asupra traficului de date al ecosistemului e-Sănătate. Metodologia definită în al doilea subcapitol este pentru prevenirea incidentelor de securitate cibernetică și se bazează pe utilizarea tranziției la microservicii. În plus, este specificat un model de deploy pentru sistemele de e-Sănătate.

Al patrulea capitol se referă la îmbunătățirea securității sistemelor de e-Sănătate (în ceea ce privește mecanismele de autentificare) prin utilizarea caracteristicilor disponibile pe smartphone-uri. Inițial, este oferită o scurtă introducere pentru a introduce amenințările care afectează serviciile cloud pentru e-Sănătate. Aceasta a fost urmată de o clasificare și o discuție a mecanismului de autentificare existent în ceea ce privește nivelul de securitate și ușurința de utilizare. Având în vedere acest lucru, a fost efectuată o evaluare a vulnerabilităților și amenințărilor de securitate asociate cu OAuth 2.0. Obiectivul principal al acestui capitol este de a introduce un nou model de autentificare care este construit pe baza OAuth 2.0. Acest model utilizează datele biometrice și de geolocație ale utilizatorilor pentru a satisface pe deplin cerințele de securitate ale sistemelor de e-Sănătate.

Al cincilea capitol de contribuții se concentrează pe îmbunătățirea securității comunicațiilor între dispozitivele medicale portabile și serviciile ecosistemelor e-Sănătate. Pentru a realiza acest lucru, este efectuată o examinare a problemelor de securitate care afectează dispozitivele medicale mobile și este prezentat un modul nou, cunoscut sub numele de Personal Medical Hub. Personal Medical Hub este conceput pentru a proteja dispozitivele medicale de amenințările de securitate prin utilizarea unei varietăți de modele și fluxuri destinate eliminării și limitării vulnerabilităților..

Capitolul 6 este destinat investigației și îmbunătățirii comunicațiilor dintre dispozitivele medicale personale/portabile și serviciile cloud. Scopul acestei investigații este optimizarea consumului de energie și asigurarea schimbului eficient de date prin analiza tehnologiilor de comunicare între dispozitivele medicale și smartphone-uri. Concomitent, se face o evaluare a influenței metodelor de dezvoltare a aplicațiilor multiplatformă asupra performanței comunicațiilor. Scopul analizei este de a identifica o soluție care să permită ca produsul software să fie executat pe mai multe sisteme de operare mobile cu o singură bază de cod, ceea ce reduce riscurile de securitate menținând simultan performanța componentelor și fluxurilor ecosistemului e-Sănătate.

Capitolul 7 introduce un nou model de securitate care utilizează API-ul de atestare a dispozitivului pentru a proteja serviciile cloud. Inițial, este oferită o imagine de ansamblu concisă a vulnerabilităților din sistemele cloud e-Sănătate, urmată de o explicație a funcționării serviciilor de atestare a dispozitivelor. Îmbunătățirile capitolului se aplică gestionării sesiunilor, cu obiectivul de a reduce diverse amenințări de securitate.

Capitolul 8, care este ultimul capitol, oferă o privire de ansamblu asupra tezei. Prezintă concluziile și constatările principale. Toate contribuțiile originale, precum și direcțiile viitoare de cercetare în ceea ce privește ecosistemele de e-Sănătate, sunt prezentate în acest capitol. Totodată, lista publicațiilor este prezentată în cadrul capitolului.

2. Stadiul tehnologic actual

Importanța asigurării securității și accesibilității serviciilor de e-Sănătate a devenit crucială în societatea noastră actuală. Obținerea unui nivel robust de securitate și asigurarea accesibilității serviciilor de e-Sănătate poate fi o sarcină complexă, condiționată de contextul operațional și de caracteristicile oferite de diverse sisteme. În încercarea de a face funcționalitățile accesibile unui număr mare de utilizatori, nivelul de securitate și performanța sistemului pot fi erodate rapid prin expunerea serviciilor într-un mediu public, nesupravegheat. În plus, existența fluctuațiilor de trafic poate duce la erori în funcționalitate, ceea ce face ca anumite funcții să devină indisponibile și alte funcții să funcționeze incorect. Cercetătorii au propus mai multe metode de-a lungul timpului pentru a aborda provocările și pentru a minimiza apariția erorilor în sistemele de e-Sănătate.

Accentul inițial al acestui studiu va fi pe un set de articole care discută despre securitatea serviciilor software cloud concepute pentru utilizare în medii publice. În continuare, va avea loc o analiză bazată pe o selecție de articole care urmăresc să securizeze dispozitivele integrate în sistemele de e-Sănătate. Această secțiune va acoperi atât securitatea dispozitivului, cât și comunicația dintre dispozitiv și serviciile de bază e-Sănătate. În cele din urmă, se prezintă o analiză a îmbunătățirilor de securitate pentru aplicațiile de tip client. Aceste aplicații, care pot fi aplicații mobile, web sau desktop, au capacitatea de a utiliza servicii cloud.

2.1 Securitatea și disponibilitatea sistemului de bază

Problema asigurării securității și disponibilității aplicațiilor web, indiferent dacă acestea folosesc o arhitectură monolitică sau decuplată, este discutată pe larg în numeroase articole din literatura tehnică de specialitate.

Sistemul de bază al unui ecosistem de tip e-Sănătate se referă la colecția de module software care oferă utilizatorilor și aplicațiilor client endpoint-urile și funcționalitățile sistemului de e-Sănătate.

Pentru a iniția o discuție despre securitatea aplicațiilor web, următoarele ipoteze sunt definite în avans:

- • Aplicația web este inofensivă și este găzduită pe o infrastructură fiabilă și sigură. Infrastructura constă din sistemul de operare și serverul web.
- • Atacatorul are abilitățile de a manipula conținutul sau secvența request-urilor transmise aplicației web, dar nu are capacitatea de a compromite direct infrastructura sau codul aplicației.

Principalele vulnerabilități și metode de a ataca aplicațiile web, așa cum sunt identificate în literatură și prezentate în [1], constau în următoarele:

- Valabilitatea intrării;
- Injectarea SQL;
- Cross-Site Scripting;
- Integritatea stării;
- Corectitudinea logică;

Pentru a atenua aceste atacuri, de-a lungul timpului au fost dezvoltate multe contramăsuri diferite. Următoarea secțiune va prezenta contramăsurile concepute special pentru fiecare dintre aceste categorii.

Pentru a analiza abordările discutate în literatură cu privire la aceste atacuri, vom distinge între două proprietăți care trebuie abordate: proprietatea validității intrării și proprietatea corectitudinii logice.

2.1.1 Valabilitatea intrării

Pentru a analiza măsurile de securitate împotriva vulnerabilităților legate de „validitatea intrării" așa cum este definită în literatura tehnică, se va utiliza aceeași metodologie de clasificare. În consecință, literatura de specialitate oferă următoarele strategii de reducere a vulnerabilităților prin aplicarea conceptului de „securitate prin construcții".

William Robertson și Giovanni Vigna [2] sugerează un model de aplicații web construit pe un sistem robust de tastare. Acest model este conceput pentru a preveni injectarea XSS și SQL prin aplicarea statică a unei separări între structura și conținutul documentelor web și interogările bazei de date generate către aplicația web. Modelul utilizează rutine de tratare specifice care recunosc și tratează cu precizie diferitele tipuri de intrare provenite de la utilizator.

Stephen Thomas și colab. [3] sugerează o abordare nouă care implică aplicarea unui algoritm de înlocuire a instrucțiunilor cu scopul de a reduce vulnerabilitățile cauzate de injectarea SQL. În timpul evaluărilor, soluția propusă a eliminat cu succes 94% dintre vulnerabilitățile studiate. Avantajul principal al acestei abordări este că nu trebuie să fie integrată în mediul de rulare și trebuie executată o singură dată.

În plus, literatura de specialitate prezintă diverse metode de reducere a vulnerabilităților prin aplicarea principiilor „securității prin validare".

Tabelul 1 prezintă o sinteză a soluțiilor analizate în cadrul tezei.

Tabelul 1

Rezumatul soluțiilor pentru validitatea intrării

Soluție	Securitate prin construcție	Securitate prin verificare	Securitate prin protecție
Metoda Robertson	da	nu	nu
Metoda Stephen	da	nu	nu
SQL DOM	da	nu	nu
CANDID	da	nu	nu
WebSSARI	nu	da	da
FlowSpec	nu	da	nu
Metoda Livshits	nu	da	nu
Metoda Nguyen-tuong	nu	da	nu

Saner	nu	da	nu
Noncespaces	nu	nu	da
ScriptGard	nu	nu	da
AMNESIA	nu	nu	da
Metoda Kruegel	nu	nu	da

2.1.2 Corectitudinea logica

Corectitudinea logicii depinde de aplicație datorită faptului că vulnerabilitățile generate de logica aplicației sunt strâns legate de aplicația în sine, având în vedere faptul că fiecare aplicație este distinctă. Pentru a atenua această categorie de vulnerabilități, politicile de securitate pot fi definite în mod explicit în timpul procesului de dezvoltare a aplicației sau implementate ulterior prin utilizarea politicilor de securitate.

Literatura tehnică oferă o varietate de soluții cu impact variabil asupra performanței pentru implementarea conceptului de „securitate prin construcție”, cât și prin conceptul de „securitate prin protecție”.

Tabelul 2 prezintă o sinteză a soluțiilor analizate în cadrul tezei.

Tabelul 2

Rezumatul soluțiilor de validare a intrărilor

Soluție	Securitate prin construcție	Securitate prin verificare	Securitate prin protecție
SIF	da	nu	nu
SELinks	da	nu	nu
UrFlow	da	nu	nu
MiMoSA	nu	da	nu
RoleCast	nu	da	nu
NoTamper	nu	da	nu
BLOCK	nu	nu	da
CLAMP	nu	nu	da

2.2 Securitatea dispozitivelor medicale

Potrivit Organizației Mondiale a Sănătății (OMS), un dispozitiv medical este un dispozitiv, un aparat sau un sistem încorporat care este utilizat pentru monitorizarea, tratarea și diagnosticarea bolilor pacienților [23].

Securitatea dispozitivelor medicale include o serie de instrumente și politici care sunt special concepute pentru a împiedica accesul neautorizat al atacatorilor, cu scopul final de a-i împiedica să obțină controlul asupra dispozitivelor sau să compromită datele pe care acestea le generează.

Caracteristicile de securitate ale dispozitivelor medicale sunt clasificate pe baza funcționalităților și a caracteristicilor pe care le posedă [24]. Caracteristicile de securitate pot fi bazate pe software, hardware și software-hardware.

Accentul principal al secțiunii ulterioare va fi pe vulnerabilitățile și contramăsurile care sunt direcționate către componenta software a dispozitivelor medicale. Formele primare de atacuri care vizează în mod specific dispozitivele medicale, așa cum sunt definite de Maria Papaioannou și colab. [25], sunt:

- Atacurile de interceptare (Eavesdropping attacks);
- Atacurile de falsificare (Spoofing attacks);
- Atacurile bazate pe analiza traficului (Traffic analysis attacks);
- Atacurile de mascaradă (Masquerading attacks);
- Atacurile fizice ;
- Atacurile malware;
- Atacurile man-in-the-middle;
- Atacurile denial-of-service;
- Atacuri de descarcare a bateriei;
- Atacurile de impersonare;
- Atacuri de fabricare/modificare/răspundere a mesajelor;

Pentru a reduce aceste vulnerabilitati, soluțiile propuse în literatura de specialitate vor fi prezentate succint în cele ce urmează.

În studiul lor, Minchul Kim și colab. [34] prezintă o metodă care utilizează criptarea pe dispozitive portabile ca o abordare pentru a proteja împotriva interceptării. Soluția se bazează pe o operațiune XOR care utilizează o cheie generată de ceasul încorporat în microcontrolerul dispozitivului. Criptarea se realizează folosind porți XOR bazate pe hardware. Pentru a preveni o utilizare neautorizată a cheii, ei sugerează implementarea unui mecanism de regenerare legat de un eveniment hardware al dispozitivului.

În studiul lor, Yan și colab. [36] prezintă instrumentul PHY-IDS, care este conceput pentru a identifica atacurile de falsificare care vizează în mod special dispozitivele portabile. PHY-IDS utilizează tehnici de învățare statistică pentru a analiza și identifica comportamentul și datele neobișnuite ale semnalului. Soluția se bazează pe nivelul de putere al unui cadru recepționat, care este măsurat la antena receptorului.

Ibbad Hafeez și colab. [38] sugerează că IoT-KEEPER poate fi utilizat pentru a detecta și a preveni atacurile de trafic. Pentru a realiza acest lucru, IoT-KEEPER efectuează analize de

trafic. Utilizează clustering fuzzy C-means și interpolarea fuzzy pentru a identifica traficul de rețea rău intenționat. Pentru a se proteja împotriva acestei vulnerabilități, IOT-KEEPER implementează restricții de acces la rețea în funcție de tipul traficului rău intenționat. IoT-KEEPER folosește o schemă de clasificare a traficului care nu necesită informații auxiliare, cum ar fi datele despre dispozitiv, pentru a detecta activitățile rău intenționate. În schimb, folosește metadatele de trafic de rețea neetichetate pentru extragerea caracteristicilor.

Mohan Sai și colab. [41] a dezvoltat o tehnică ușoară de detectare a atacurilor de tip denial-of-service, bazată pe învățarea automată. Abordarea lor implică folosirea unei mașini bazată pe vectori de suport pentru a diferenția între traficul rău intenționat și traficul normal. Pentru a identifica anomaliile este folosit un algoritm de clasificare care se bazează pe un model de date simplu. Un algoritm de selecție a caracteristicilor bazat pe corelație este implementat pentru a obține cu ușurința modelul de date. Cu toate acestea, soluția este capabilă doar să detecteze atacuri de tip denial-of-service, dar nu este capabilă să ofere protecție dispozitivelor împotriva acestui tip de atac.

Shanshan Tu și colab. [42] propun un nou algoritm de Q-learning pentru detectarea precisă a atacurilor de impersonare. Algoritmul este viabil atât în medii statice, cât și în medii dinamice. Obiectivul soluției destinată mediului static este de a implementa un joc cu sumă zero între atacator și receptor prin implementarea unui patch pentru securitatea stratului fizic. Soluția pentru un mediu dinamic ia în considerare informațiile despre starea canalelor, inclusiv timpul mediu, rata alarmelor false, rata de detectare a erorilor (MDR) și rata medie de eroare (AER).

Jorge Maestre Vidal și colab. [44] propun o nouă strategie de detectare a atacurilor de mascaradă care este capabilă să detecteze atacurile de mascaradă chiar și atunci când atacatorul imită comportamentul utilizatorilor legitimi. Pentru a realiza acest lucru, strategia introduce trei etape: etapele de analiză, verificare și recunoaștere. În etapa de analiză, algoritmii de aliniere identifică discrepanțele din comportamentul tipic al utilizatorului pentru a identifica un atac de mascaradă. Discrepanțele detectate sunt supuse unei scheme de validare care se bazează pe testul U în timpul etapei de verificare. Strategia implică compararea datelor anterioare cu comportamentul curent al utilizatorului pentru a identifica inconsecvențele care indică un atac de tip mascaradă.

Grant A. Jacoby și colab. [46] au introdus conceptul de utilizare a stării bateriei unui dispozitiv ca un indicator al potențialei modificări fizice pentru a identifica și atenua atacurile de drenare a bateriei. El recomandă ca starea bateriei să fie monitorizată folosind senzori sau circuite dedicate care pot detecta modificări, cum ar fi căderile bruște de tensiune sau curent, atunci când bateria este manipulată, pentru a detecta atacul. Sistemul inițiază procedurile de blocare și declanșează o alarmă atunci când este detectată o anomalie în starea bateriei. Avantajul principal este că nu necesită resurse suplimentare substanțiale sau modificări ale dispozitivului, deoarece se bazează pe baterie și circuitele sale de monitorizare.

Ensieh Modiri Dovom și colab. [47] sugerează o metodă de atenuare a programelor malware care utilizează un arbore de modele fuzzy (FPT). Un FPT este o structură ierarhică care utilizează logica fuzzy pentru a reprezenta modele în date. FPT este folosit pentru a identifica și clasifica programele malware de pe dispozitiv. Procesul de detectare are loc pe dispozitiv. Metoda extrage și grupează anumite caracteristici neclare pe baza comportamentului diferitelor componente și stări software (modele de trafic de rețea, utilizarea resurselor, apeluri de metode). Sistemul este capabil să identifice modele de comportament normal și rău intenționat prin utilizarea FTP, permițând astfel atenuarea timpurie a potențialelor amenințări.

2.3 Securitatea aplicațiilor medicale de tip client REST

Aplicațiile medicale de tip client REST reprezintă întreaga gamă de aplicații medicale web și mobile care utilizează API-uri REST pentru accesarea sau modificarea datelor și resurselor dintr-un sistem medical la distanță.

Pentru a discuta despre securitatea aplicațiilor REST, este necesar să se abordeze separat securitatea aplicațiilor web și a aplicațiilor mobile. Acest lucru se datorează faptului că amenințările și soluțiile de securitate sunt distincte datorită designului și ecosistemului specific mediului de rulare al aplicațiilor.

2.3.1 Securitatea aplicațiilor web medicale de tip client REST

Termenul „ client side" în dezvoltarea web denotă toate aspectele unei aplicații web care sunt afișate sau sunt executate pe dispozitivul client. Aceasta include componentele vizibile ale interfeței cu utilizatorul, cum ar fi textul, imaginile și alte elemente care sunt conținute de UI, precum și orice operație pe care o aplicație o efectuează în interiorul browserului utilizatorului.

Principalele provocări de securitate apar din acțiunile efectuate de anumite aplicații din browser. Aceste acțiuni sunt executate frecvent cu suportul JavaScript, fie direct, fie prin alte modele care se bazează pe această tehnologie.

Principalele măsuri de securitate propuse de literatură se referă la utilizarea conceptului de izolare a execuției codului JavaScript în zone sigure și analiza acestor interacțiuni folosind diverse instrumente pentru a determina o execuție potențial dăunătoare sau incorectă a codului..

2.3.2 Securitatea aplicațiilor mobile medicale de tip client REST

Atacurile asupra dispozitivelor mobile au fost clasificate în patru categorii: atacuri bazate pe aplicații, atacuri bazate pe web, atacuri bazate pe rețea și atacuri bazate pe fizic, după cum este documentat în studii [54]. Integritatea și confidențialitatea datelor și aplicațiilor mobile sunt afectate de aceste atacuri.

O mare parte a literaturii oferă soluții pentru securizarea clientului aplicației mobile REST pe baza politicilor predefinite și încearcă să le pună în aplicare prin diferite soluții. O altă metodă de asigurare a securității este monitorizarea activităților dispozitivului pentru a identifica potențialele anomalii sau aplicații rău intenționate. Acest lucru se face pentru a preveni interacțiunea acestora cu aplicația medicală și pentru a o izola într-un mediu sigur.

2.4 Abordări de securitate pentru ecosistemele de e-Sănătate

Analiza ulterioară a literaturii științifice se concentrează pe diferite tipuri de ecosisteme e-Sănătate și investighează diferite abordări de securizare a acestora. Această secțiune încheie capitolul stadiu actual tehnologic, ilustrând potențialele dorecții de cercetare viitoare și dezvoltări în domeniul securității și disponibilității pentru sistemele de e-Sănătate

În soluțiile propuse de literatură, multe dintre abordările care sunt capabile să securizeze ecosistemele e- Sănătate sunt construite pe o analiză efectuată folosind tehnici NLP sau AI pentru a identifica vulnerabilitățiile, dar acestea nu pot fi atenuate direct. Confidențialitatea și integritatea datelor sunt obiectivele primare ale celorlalte metodologii, care includ sisteme ce

au la bază se blockchain sau criptografie, fără a lua în considerare vulnerabilitățile rămase în cadrul sistemului.

3. Integrarea microserviciilor în sistemele medicale

Un model arhitectural inovator pentru sistemele de sănătate electronică este prezentat în acest capitol, cu obiectivul de a spori reziliența cibernetică și de a asigura o disponibilitate ridicată în fluctuațiilor de trafic. Acesta investighează corelațiile dintre incidentele tipice de securitate cibernetică din domeniul e-Sănătății și defectele arhitecturale, precum și modelele frecvente de proiectare în sistemele operaționale din prezent. Prezintă o metodologie de testare care se bazează pe cercetare, identifică punctele slabe și sugerează soluții viabile. Acest capitol prezintă o strategie de suport cuprinzătoare pentru tranziția de la arhitecturile tradiționale monolitice la microservicii. Această modificare folosește scalabilitatea verticală și orizontală a cloud computingului pentru a optimiza utilizarea resurselor și a garanta fiabilitatea sistemului. În plus, oferă strategii de deploy pentru noile microservicii, cu accent pe securitatea cibernetică și rezistența operațională în mediile e-Sănătate.

3.1 Introducere

Unul dintre impacturile globale ale coronavirusului a fost în industria sănătății. COVID-19 a provocat supraaglomerare în spitale, ceea ce face imposibil ca pacienții și medicii să se întâlnească în persoană pentru o consultație. Sistemele de e-Sănătate, pe lângă rolurile pentru care au fost dezvoltate, și-au asumat un nou rol de mediator pentru a răspunde acestei situații. În plus, noi funcții au fost fie dezvoltate, fie utilizate mai frecvent pentru a satisface această cerere:

- Urmărirea contactelor;
- Telemedicină (consultare online cu un medic);
- Diagnosticare automată;
- Prognoza necesarului de resurse materiale;
- Fișa medicală individuală despre boala COVID-19.

Cele mai frecvente atacuri legate de COVID-19 asupra sistemelor de sănătate electronică sunt ZOOM bombing, atacurile de phishing COVID-19, programele malware și disponibilitatea serviciilor [71].

Acest capitol abordează problemele legate de disponibilitatea a serviciilor în sistemele de sănătate electronică. Pentru a realiza acest lucru, primul pas este extragerea unui model arhitectural comun bazat pe un studiu în unitățile medicale. Acest studiu identifică cele mai frecvent utilizate sisteme software de e-Sănătate, precum și caracteristicile cheie necesare. Studiul a inclus 45 de spitale și clinici medicale din București, din sectorul public și privat.

Pe baza arhitecturii sistemelor software e-Health, 17 din 45 de entități folosesc doar sisteme software locale, în timp ce 28 folosesc aplicații web. Cea mai comună arhitectură a urmat modelul monolit model-view-controller

3.1.1 COVID-19 și traficul în rețea

Pentru a determina variația traficului pentru sistemele e-Sănătate, a fost efectuată o analiză a traficului folosind datele publice CO APCD din aprilie 2018 până în martie 2024. Rezultatele obținute sunt prezentate în Figura 3 și Figura 4.

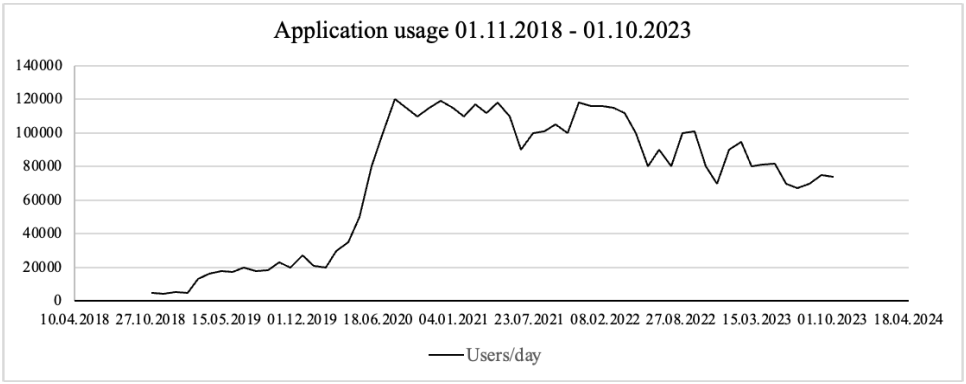

Fig. 3. Utilizarea aplicației între 01.11.2018 și 01.10.2023, în funcție de numărul de utilizatori/zi

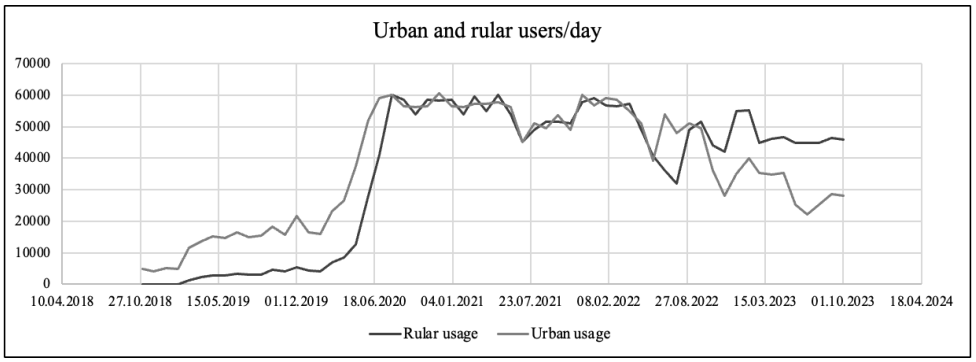

Fig. 4. Utilizarea aplicației între 01.11.2018 și 01.10.2023 în funcție de mediu.

Provocarea actuală a sistemelor software medicale este modul de atenuare a amenințărilor și riscurilor de securitate cibernetică și, de asemenea, modul de gestionare a problemelor de performanță cauzate de volumul de procesare semnificativ crescut ca urmare a adoptării rapide a acestora.

3.1.2 modelul arhitectural e-Sănătate

Pentru a crea o imagine de ansamblu comună a sistemelor software de e-Sănătate analizate, cercetarea a identificat modulele de bază și opționale care pot fi combinate pentru a crea un sistem care include toate caracteristicile descrise anterior.

Sistemul este compus din șapte module interconectate care sunt protejate de mediul extern printr-un firewall. Principalele componente ale arhitecturii sunt:

- aplicația web;
- interpretul de rezultate AI;
- sistemul de laborator;
- server de streaming;
- serverul SQL;
- API-ul sistemelor externe care gestionează hub-ul dispozitivelor portabile și funcția de SMS

3.2 Sistemul propus

Pentru a gestiona eficient diferențele de încărcare și pentru a menține un cost de infrastructură mai mic, caracteristica principală a noii arhitecturi este scalabilitatea sa verticală și orizontală.

Arhitectura de sistem propusă se bazează pe microservicii, care permit ca aplicația monolitică originală să fie împărțită în mai multe servicii independente capabile să efectueze lucrul independent. Această independență permite implementarea sistemului de scalare a sistemului. Ecosistemul e-Sănătate va putea iniția noi instanțe pentru fiecare serviciu, în conformitate cu sarcina sistemului. În plus, ecosistemul e-Health va putea îmbunătăți puterea de calcul a instanțelor actuale.

Divizarea microserviciilor s-a făcut pe baza funcționalității sistemului pentru a putea oferi utilizatorilor caracteristicile independente una de cealaltă, astfel încât, dacă un set de microservicii nu mai funcționează corect, sistemul poate gestiona restul de caracteristici în mod independent.

Pasul de tranziție implică adăugarea serviciilor cloud unul câte unul, iar noul modul gateway API asigură o conectivitate perfectă cu aceste servicii. Pentru a optimiza performanța a fost implementat un sistem de cache.

Arhitectura de microservicii care rezultă este compusă din 16 servicii, care sunt clasificate în Nivelul 1 și Nivelul 2.

Serviciile de nivel 1 sunt mapate la diferite caracteristici ale sistemului pentru a oferi funcționalitatea sistemului. Au un cache și implementează o optimizare a mecanismului de cerere. De asemenea sunt capabilie să stocheze date în modulul SQL.

Serviciile de nivel 2 sunt cele care oferă suport pentru serviciile de nivel 1 și sunt capabile să se integreze cu diverse subsisteme care nu sunt scalabile, cum ar fi furnizorii externi sau aplicațiile învechite (de exemplu, sistemele de laborator).

3.2.1 Depolymentul sistemelor de e-Sănătate pe bază de microservicii

Principalele opțiuni pentru deploymentul microserviciilor în Microsoft Azure sunt Cloud Services și Azure Web Apps. Pentru a determina ce soluție este mai fezabilă, a fost utilizat costul efectiv pentru 24 de ore.

Costul estimat al deploymentului în Azure Cloud Service este de 231,82 USD, în timp ce deploymentul în Azure App Service este estimat la 151,2 USD. În concluzie, Azure Cloud Service este cea mai rentabilă opțiune pentru deployment. Cu toate acestea, decizia de a allege una dintre aceste soluții ar trebui să ia în considerare și puterea de calcul necesară pentru a gestiona același număr de cereri.

3.3 Indicatori pentru evaluarea performanței

Pentru a identifica principalele probleme din sistem, au fost efectuate următoarele tipuri de teste de performanță: teste de stres, teste de anduranță și teste de vârf.

În software-ul e-Sănătate, principalele preocupări legate de numărul de utilizatori provin de la utilizatorii cu rolul de pacient. Din cauza acestei probleme, scenariile concepute ar trebui să se bazeze pe gestionarea acțiunilor principale pe care aceștia le pot efectua

Apache JMeter a fost folosit pentru a efectua teste automate. Pentru a putea efectua un număr mare de teste în paralel, au fost necesare mai multe instanțe JMeter. Instanțele JMeter au fost rulate în Azure utilizând Azure Cloud Service.

Limita superioară pentru JMeter determinată în timpul testului a fost de 1000 utilizatori per instanță. După această limită, performanța lui JMeter s-a degradat considerabil.

3.4 Repere de performanță

Pentru a vedea diferența de performanță dintre arhitectura originală și arhitectura pe bază de microservicii, a fost efectuat același set de teste. Testele au fost efectuate atât utilizând mediul de rulare pus la dispoziție de către Azure Cloud Service, cât și cel pus la dispoziție de către Azure App Service..

3.4.1 Performanța arhitecturii originale

Performanța sistemului a fost grav deteriorată după 170.000 de utilizatori. Pentru a garanta disponibilitatea sistemului e-Sănătate și pentru a preveni defectarea sistemului, o serie de acțiuni pot fi implementate la un cost redus în conformitate cu rezultatele scenariului de testare.

Având în vedere că principalele preocupări legate de numărul de utilizatori sunt generate de rolul pacientului, este posibilă restricționarea accesului pentru acea categorie de utilizatori pe baza unui sistem de așteptare, pentru a limita utilizatorii activi la un număr maxim de 150.000 sau mai mic, în funcție de câți medici ar trebui să fie acomodați de către sistem.

3.4.2 Performanța arhitecturii bazate pe microservicii

Deoarece arhitectura originală a fost capabilă să facă față testelor pentru 170.000 de utilizatori, acum scenariile de testare încep de la 200.000 și sunt rulate în Azure Cloud pentru a oferi o putere de calcul adecvată.

Conform testelor de stres, performanța sistemului a fost îmbunătățită substanțial. Cu toate acestea, adăugarea de noi instanțe la sistem, care este cauzată de scalarea orizontală, are ca rezultat unele solicitări eșuate.

Arhitectura propusă are o rată de îmbunătățire de 98,7%, conform testelor efectuate cu JMeter și prezentate în teză.

3.5 Concluzii

Pentru a atenua riscul care afectează disponibilitatea serviciilor și pentru a garanta disponibilitatea ridicată a sistemelor software e-Sănătate, acest capitol sugerează implementarea cloud computing și a microserviciilor ca soluție. Scopul principal al tranziției de la arhitectura monolitică la arhitectura de microservicii în sistemele software e-Sănătate este de a stabili un nou strat între software-ul învechit și noile așteptări / comportamente ale

utilizatorilor. În plus, se oferă suport și scalare pentru a procesa un volum mare de cereri concurente.

Pentru a face posibilă această decuplare a performanței, acest capitol propune o tranziție la microservicii care permit scalarea verticală și orizontală. Pentru a minimiza costul hardware, propunerea este de a utiliza soluții cloud pentru a găzdui toate componentele sistemului e-Sănătate.

Deoarece microserviciile sunt separate, actualizările și remedierea erorilor pot fi aplicate individual fără a bloca întreg sistemul. Acest lucru permite ca noile funcții și corecțiile de securitate să fie lansate rapid și în siguranță, păstrând întreg sistemul în siguranță. În plus, arhitectura pe bază de microservicii separă serviciile, astfel încât o degradare a securității în unul dintre ele să afecteze si alte microservicii.

Fiecare microserviciu poate avea măsuri de securitate personalizate. Acest lucru permite o securitate mai precisă, adaptată datelor sau tranzacțiilor din cadrul fiecărui serviciu.

3.5.1 Contribuții

- A fost dezvoltat un nou sistem e-Health de microservicii pentru a gestiona eficient fluctuațiile de trafic și pentru a reduce costurile prin încorporarea metodelor de scalare atât pe verticală, cât și pe orizontală.
- A fost configurată o întreagă infrastructură cloud folosind Azure cloud pentru a evalua soluția arhitecturală propusă.
- A fost propusă o metodologie de testare pentru a evalua performanța diferitelor sisteme de e-Sănătate în raport cu disponibilitatea serviciilor și pentru a determina limitările sistemelor.
- Au fost dezvoltate și evaluate o serie de măsuri pentru a garanta disponibilitatea sistemelor software e-Sănătate în cazul în care acestea nu sunt în măsură să facă față variațiilor de trafic.
- A fost creată o strategie de migrare pentru a asigura disponibilitatea sistemelor software e-Health la un cost redus. Această strategie folosește atât mecanisme de scalare verticală, cât și orizontală pentru a aborda în mod specific punctele slabe ale sistemului.
- A fost creat un set de strategii de găzduire pentru sistemele e-Health de microservicii bazate pe soluții Azure cloud, ținând cont de costul serviciilor.
- A fost dezvoltat un model software general prin analizarea produselor disponibile pe piață și pe baza caracteristicilor sistemelor actuale.
- A fost propus și validat un model de clasificare pentru adoptarea sistemelor de e-Sănătate folosind datele reale colectate în timpul pandemiei de COVID-19.

4. Creșterea securității sistemelor prin utilizarea smartphone-urilor

În domeniul medical, sistemele de securitate a aplicațiilor web folosesc adesea strategia de autentificare și credențiale pentru a evalua identitatea utilizatorului. Pe baza credențialelor, sistemul poate valida identitatea utilizatorului. De asemenea, autenticitatea identității este evaluată pe baza strategiei de autentificare. Acest capitol analizează și compară diferite strategii utilizate pentru a implementa sisteme de securitate a aplicațiilor web prin utilizarea locației și a caracteristicilor biometrice ale smartphone-urilor cu scopul de a oferi o autentificare mai sigură.

4.1 Introducere

Autentificarea este o problemă care este adesea revizuită din cauza creșterii continue a puterii de calcul. În consecință, cerințele pentru parole cresc de la an la an, iar complexitatea parolelor implică un efort semnificativ pentru utilizatorul final, dar parolele nesigure încă există.

Acest capitol compară diferite strategii de autentificare utilizate de aplicațiile web pentru procesul de autentificare și urmărește îmbunătățirea acestui proces prin utilizarea funcțiilor smartphone-ului de locație și senzori biometrici.

4.2 Clasificarea mecanismelor de autentificare existente

Această secțiune prezintă o privire de ansamblu asupra celor mai frecvente metode de autentificare pentru aplicațiile web prin utilizarea schemei de clasificare propusă de Renaud și colab. [85] și completată de către Yampolski în [86].

Schema de clasificare arată că există patru categorii de sisteme de autentificare bazate pe locația utilizatorului sau pe baza a ceea ce știe utilizatorul..

4.2.1 Autentificarea bazată pe parolă

Metodele de autentificare prin parolă pot fi clasificate în două categorii principale [88], după cum urmează:

- Parole bazate pe text;
- Parole bazate pe imagini;

Diferențele dintre parolele bazate pe text și parolele bazate pe imagini sunt prezentate în Tabelul 9.

Tabelul 9

Comparația categoriilor de parole

Criterii	Autentificare prin parolă	
	Parole bazate pe text	**Parole bazate pe imagini**
Securitate	Scăzută	Înaltă
Disponibilitate	Mereu	Mereu
Utilizabilitate	Ușoară	Ușoară
Cost	Redus	Crescut

4.2.2 Autentificare pe bază de locație

Sistemele de autentificare bazate pe locație utilizează datele de geolocalizare pentru a valida identitatea utilizatorului. Există două categorii distincte de metode de autentificare: una care necesită specificarea tuturor datelor de geolocalizare în timpul înregistrării, cum ar fi latitudinea, longitudinea și precizia poziției; cealaltă categorie se bazează pe comportamentul utilizatorului și se bazează pe tehnici de inteligență artificială (AI).

Comparația dintre autentificarea pe bază de geolocalizare statică și dinamică este prezentată în Tabelul 10.

Tabelul 10

Comparația sistemelor de autentificare pe bază de locație

Criterii	Autentificare pe bază de locație	
	Locație statică	**Locație dinamică**
Securitate	Înaltă	Scăzută
Disponibilitate	Mereu	Uneori
Utilizabilitate	Ușoară	Ușoară
Cost	Redus	Crescut

4.2.3 Autentificare bazată pe date biometrice

Autentificarea biometrică compară caracteristicile fizice curente cu mostrele stocate pentru a găsi o potrivire între ele. Dacă există o potrivire, utilizatorul este autentificat.

Principalele diferențe ale sistemelor de autentificare pe bază de date biometrice sunt prezentate în Tabelul 11. Comparația se bazează pe cercetările efectuate de către Parvathi Ambalakat [93].

Tabelul 11

Compararea sistemelor de autentificare pe bază de date biometrice

Criterii	Caracteristica biometrică			
	Amprentă	**Facială**	**Iris**	**Retină**
Performanţă	Ridicată	Scăzută	Ridicată	Ridicată
Acceptare	Medie	Ridicată	Scăzută	Scăzută
Ocolire	Ridicată	Ridicată	Scăzută	Scăzută
Colectabilitate	Medium	High	Medie	Scăzută
Distinctivitate	Ridicată	Scăzută	Ridicată	Ridicată

4.3 Vulnerabilitatea OAuth 2.0

OAuth 2.0 is centered around bearer tokens. As a result, the integration of this mechanism is straightforward; however, bearer tokens lack any internal security mechanisms. Nowadays, this is the standard protocol for industry.

OAuth 2.0 este centrat în jurul bearer token-urilor. Ca urmare, integrarea acestui mecanism este simplă; cu toate acestea, bearer token-urile nu au niciun mecanism de securitate internă. În prezent, acesta este protocolul standard pentru industrie

4.3.1 Vulnerabilitățile bearer token-urilor

Un prim set de vulnerabilități este cauzat de faptul că utilizatorii care folosesc acest tip de autorizare nu trebuie să își dovedească identitatea.

Al doilea set de vulnerabilități constă din următoarele amenințări de securitate:

- Redirecționarea token-urilor;
- Reutilizarea token-urilor;
- Falsificarea token-urilor;
- Decriptarea token-urilor;

Al doilea set de vulnerabilități poate fi atenuat sau eliminat prin implementarea unui set minim de măsuri privind generarea și transportul token-ului.

4.4 Propunerea de îmbunătățire a securității OAuth 2.0

Se propune un nou sistem de autentificare îmbunătățit pentru a spori securitatea protocolului OAuth 2.0 pentru aplicațiile cloud. Acest sistem utilizează date biometrice și de locație generate de către dispozitivele mobile cu scopul de a îmbunătăți rezistența cibernetică a aplicațiilor.

Arhitectura propusă se bazează pe o soluție software care folosește sistemul de operare Android, un sistem care este deja protejat cu ajutor serviciilor SafetyNet.

Componenta de autorizare ce va fi folosită diferă în funcție de sursa cererii, după cum urmează:

- Fluxul inițial corespunde cererilor care sunt inițiate din cadrul unei aplicații client Android;
- Al doilea flux corespunde cererilor care sunt inițiate de pe alte dispozitive sau aplicații web.

4.4.1 Utilizarea sistemelor biometrice în Android

În ecosistemul Android, securitatea datelor biometrice este o prioritate. Pentru a preveni scurgerea și compromiterea datelor, smartphone-urile implementează o zonă de securitate numită Trusted Execution Environment (TEE). Pentru a utiliza TEE, trebuie utilizată o colecție de componente software cunoscută sub numele de Trusty, în caz contrar datele nefiind accesibile.

4.4.2 Utilizarea sistemelor de localizare în Android

Android oferă două metode pentru a solicita locația dispozitivului: Utilizarea serviciilor Google Play sau utilizarea LocationListener.

Pentru a stabili o reprezentare mai sigură a locației, latitudinea și longitudinea colectate vor fi criptate cu o funcție bijectivă care ia în considerare inclusiv GUID-ul sesiunii (f(latitudine, longitudine, guid) -> GUID-locație).

Rezultatul acestei funcții va fi decriptat în interiorul aplicației client pentru a prelua locația specifică a utilizatorului (latitudine și longitudine). Rezultatul final va fi comparat cu datele despre locație introduse în cadrul procesului de înregistrare, astfel încât să corespundă cu o toleranță. Toleranța maximă acceptată este definită la nivelul întregului sistem.

4.5 Statisticile de utilizare

Testele au fost efectuate cu următorii parametri: 1000 fire executie, 500 secunde timp de ramp-up, 5 iterații, 50 secunde de activitate maxim și 5000 secunde timp de așteptare.

Rezultatele arată că timpul de răspuns al protocolului de autentificare modificat este aproape dublat. Acest lucru subliniază diferența dintre încărcarea suplimentară de comunicare de pe dispozitivul Android și cea a componentei de autentificare. Pentru solicitarea initiala, timpul este mai mare datorita faptului ca dispozitivul trebuie sa obtina locatia curenta, ceea ce are ca rezultat un timp crescut. În consecință, timpul de răspuns este de aproape patru ori mai lent.

4.6 Concluzii

În acest capitol, au fost examinate caracteristicile primare care pot fi utilizate într-un sistem de autentificare, precum și modul în care aceste caracteristici sunt combinate pentru a crea un protocol mai sigur care se bazează pe OAuth 2.0.

Chiar dacă mecanismul de autentificare este mai sigur acum, sistemul poate fi totuși afectat de atacuri. De exemplu, smartphone-ul poate fi modificat cu Magisk, pentru a patch-ul SELinux.

4.6.1 Contribuții

- A fost dezvoltat un model de autentificare OAuth 2.0 îmbunătățit. Acest model include un mecanism de securitate mai puternic care se bazează pe utilizarea datelor biometrice și a locației smartphone-urilor pentru a verifica identitatea utilizatorului.
- A fost propus un model de clasificare a mecanismelor actuale de autentificare pentru a prezenta și clasifica diferitele modele de autentificare.
- A fost dezvoltat un proces de înregistrare imbunătățit, care a inclus conceptul de zone geografice de încredere.
- A fost dezvoltat și utilizat un model de analiză a performanței și a securității pentru a evalua corect schimbările de performanță și îmbunătățirile de securitate pentru diferite modele de autentificare.

5. Creșterea securității comunicațiilor pentru dispozitivele medicale personale/portabile

Acest capitol prezintă Personal Medical Hub, o soluție de securitate eficientă concepută special pentru dispozitivele medicale compatibile Bluetooth. Obiectivul principal al acestei soluții este de a îmbunătăți confidențialitatea datelor și de a oferi o protecție puternică împotriva diferitelor amenințări de securitate, cum ar fi atacurile de tip man-in-the-middle, breșele de securitate și backdoors.

5.1 Introducere

Dispozitivele medicale mobile pot colecta date despre starea de sănătate a pacientului și pot oferi proceduri de tratament, ceea ce le face utile atât în scopuri de prevenire, cât și de tratament.

Datorită scopului diferit al acestor dispozitive, unele dintre ele pot colecta doar date de la pacienți, date care trebuie descărcate la un cabinet medical sau care trebuie trimise în timp real către sistemele de e-Sănătate.

Bluetooth este tehnologia de comunicare cel mai frecvent utilizată pentru dispozitivele medicale cu comunicații în timp real pentru a face schimb de informații. Bluetooth este adesea folosit pentru transmiterea datelor pacientului către un telefon mobil pentru analiza sau pentru transferul datelor către sisteme e-Sănătate.

În acest capitol este introdusă o arhitectură de comunicație modificată bazată pe un Hub personal medical pentru a îmbunătăți securitatea dispozitivelor medicale Bluetooth.

Personal Medical Hub este o soluție de securitate puternică care îmbunătățește confidențialitatea datelor și oferă protecție împotriva amenințărilor de securitate, cum ar fi atacurile de tip man-in-the-middle, breșele de securitate și backdoors.

5.2 Arhitectura generală a sistemului

Sistemul prezentat este alcătuit din patru subsisteme: dispozitivul medical, smartphone-ul pacientului, sistemul cloud și sistemul e-Sănătate.

Conform clasificării nivelelor de securitate pentru dispozitivele medicale elaborată de către Johannes Sametinger și colab. [104], dispozitivele medicale portabile sunt clasificate ca având un risc mediu spre foarte mare.

Una dintre cele mai frecvente preocupări de securitate este asociată cu atacurile de tip man-in-the-middle. Atacurile de acest tip constituie aproximativ 35% dintre atacuri [105].

5.3 Arhitectura propusă pentru îmbunătățirea securității

Personal Device Hub reprezintă un hub Bluetooth interpus între toate canalele de comunicare ale dispozitivului medical. Hub-ul este echipat cu interfețe Bluetooth și Wi-Fi

pentru comunicare. Scopul principal al Personal Device Hub este de a gestiona și reduce atacurile de tip denial of service și man-in-the-middle.

Pentru a atinge acest obiectiv, Personal Device Hub utilizează trei abordări distincte:

- Reduce vulnerabilitatea prin actualizarea dispozitivului la cel mai recent firmware furnizat de producătorul dispozitivului.
- Analizează traficul de rețea pentru a detecta comportamentul neobișnuit și aplică filtre sau blochează sursele care nu sunt incluse pe lista de încredere.
- Criptează traficul dintre dispozitiv și cloud pentru a preveni falsificarea certificatelor.

5.3.1 Gestionarea vulnerabilităţilir şi a atacurilor

Componentele cheie ale Personal Device Hub sunt analizatorul de trafic și managerul de securitate al dispozitivului, care sunt derivate din cele două funcții principale ale dispozitivului (controlul traficului de rețea și criptarea comunicațiilor pentru infrastructura cloud; actualizarea dispozitivelor vulnerabile care au încă suport de la producător) .

În funcție de starea unei vulnerabilități, sistemul poate alege dintre trei scenarii:

- Filtrarea atacurilor;
- Preluarea, notificarea și instalarea actualizărilor;
- Getionarea unui dispozitiv nesigur.

5.4 Evaluarea de securitate

Pentru a evalua eficiența Personalului Medical Hub, a fost folosită o pompă de insulină veche cu conexiune Bluetooth.

Cele mai problematice vulnerabilități sunt cele care necesită respingerea pe baza filtrului, iar rata de fixare depinde de calitatea filtrelor dobândite. În cazul atacurilor de tip denial of service, analizatorul de trafic oferă cea mai eficientă protecție.

În dezvoltările viitoare, este necesar să se consolideze capacitatea Personal Medical Hub de a aborda problemele de autentificare și vulnerabilitățile legate de XSRF (Cross-Site Request Forgery).

5.5 Contribuţii

- O soluție nouă a fost concepută pentru a îmbunătăți comunicația dintre dispozitivele medicale portabile și serviciile cloud e-Sănătate. Soluția, numită Personal Medical Hub, îmbunătățește securitatea comunicației dintre dispozitivele medicale portabile și serviciile cloud e- Sănătate și reduce riscurile atacurilor de tip man-in-the-middle.
- A fost dezvoltată o strategie de securitate pentru a aborda diferite atacuri care se bazează pe vulnerabilități. Strategia are capacitatea de a determina între trei scenarii: filtrarea atacurilor, gestionarea unui dispozitiv nesecurizat și determinarea căii de rezolvare a vulnerabilității dispozitivului.

- A fost dezvoltat un model de evaluare de securitate pentru comunicația dispozitivelor medicale și a fost utilizat pentru a evalua cât de eficient a funcționat Personal Medical Hubs cu diferite dispozitive medicale.

6. Creșterea performanței de comunicație între dispozitivele medicale personale/portabile și serviciile cloud

Acest capitol va examina impactul performanței asupra unei varietăți de tehnici de comunicare destinate distanțelor scurte care sunt susținute modelele de dezvoltare software multiplatformă, precum și impactul global al performanței generate de soluții de dezvoltare multiplatformă, folosind metoda de testare comparativă.

6.1 Introducere

Tehnologiile primare de comunicație care permit dispozitivelor mobile să facă schimb de date pot fi împărțite în două categorii: tehnologii cu rază lungă de acțiune și tehnologii cu rază scurtă de acțiune.

Principalii exponenți ai tehnologiilor cu rază scurtă de acțiune sunt Bluetooth, Wi-Fi, NFC și tehnologia infraroșu.

Tehnologiile cu rază lungă de acțiune sunt reprezentate de sistemele GSM și tehnologiile prin satelit precum GPS-ul.

Acest capitol va examina modul în care tehnologiile de comunicații ale dispozitivelor mobile funcționează pe distanțe scurte și modul în care soluții de dezvoltare multiplatformă afectează această performanță.

6.2 Performanța tehnologiilor de comunicații pentru distanțe scurte între dispozitive mobile

Principalele tehnologii de comunicație destinate distanțelor scurte, conform lui Toshiya Tamura și colab. [111], sunt: Wi-Fi, Bluetooth și NFC.

6.2.1 Bluetooth

Bluetooth funcționează pe banda licențiată ISM (Industrial, Științific, Medical) de 2,4 GHz. Există 79 de canale de comunicație, iar fiecare pachet va fi transmis o singură dată. Fiecare canal are o lățime de bandă de 1 MHz.

Protocolul de comunicație are o structură master-slave și este bazat pe pachete [113]. Fiecare master poate comunica cu până la șapte dispozitive slave. Toate dispozitivele din rețea folosesc un singur ceas principal. Rolul de master este determinat de comun acord (un master poate deveni slave la un moment dat). La un moment dat, doar masterul și un slave pot comunica, masterul determinând ce dispozitiv poate să se adreseze.

6.2.2 Wi-Fi Direct

Wi-Fi Direct (numit anterior Peer to Peer Wi-Fi) este un standard care permite dispozitivelor să se conecteze fără a fi nevoie de un punct de acces (AP). Permite comunicarea la viteza unei rețele Wi-Fi.

Dispozitivul care funcționează ca AP este decis prin negocieri; în consecință, ambele dispozitive trebuie să execute rolurile client și AP (care sunt roluri logice). În același mod ca Wi-Fi Protected, punctul de acces este protejat de un PIN.

6.2.3 NFC

Tehnologia de comunicare NFC permite comunicarea între două dispozitive care sunt situate la o distanță de maxim 10 cm. Fiecare dispozitiv are capacitatea de a funcționa în trei moduri distincte: emulare card, citire/scriere și P2P (peer-to-peer) [116].

Standardul permite rate de transfer cuprinse între 106 Kbps și 424 Kbps și operează la 13,56 MHz (frecvență care nu necesită o licență) [117]. Se bazează pe principiul inducției magnetice. Există două moduri de funcționare: activ și pasiv.

6.2.4 Compararea tehnologiilor

Toate caracteristicile tehnologiilor de comunicație pe distanță scurtă sunt prezentate în Tabelul 15.

Tabelul 15

Comparația tehnologiilor de comunicație pe distanță scurtă

Caracteristică	Bluetooth	Wi-Fi Direct	NFC
Aria de acoperire maxima	50 m	45 m	20 cm
Frecvență	2.4 GHz	2.4 GHz	13.56 MHz
Rata de transfer	1 Mbps	54 Mbps	424 Kbps
Tip de rețea	WPAN	WPAN	P2P
Configurare	Necesita ajustari	Necesita ajustari	Prin apropiere
Timp de conectare	6s	6s	0.1s
Standardul	IEEE 802.15.1	-	ISO 13157

6.2.5 Validarea tehnologică a tehnologiilor

Pentru a verifica din punct de vedere tehnic tehnologiile furnizate mai sus, a fost efectuat un test de schimb de informații în format text simplu și binar.

Validarea funcțională a fost realizată folosind o aplicație care a fost special concepută pentru acest scop și este compatibilă cu ecosistemul Android. Testele au fost efectuate independent în activități separate. Toate tehnologiile au necesitat existența unei rutine asincrone pentru recepție și a unui rutine distincte pentru transmisie. Toate tehnologiile menționate mai sus au fost supuse unei validări funcționale cu succes.

6.3 Performanța comunicării pentru aplicațiile multiplatformă

Performanța aplicațiilor hibride multiplatformă și compilate multiplatformă reprezintă punctul principal al analizei, deoarece aplicațiile web mobile sunt limitate la actualizarea dinamică și interacțiunea lor cu serviciile sistemului de operare [120] este insuficientă pentru a satisface cerințele aplicațiilor medicale [121].

6.3.1 Dezvoltarea folosind tehnicile de compilare multiplatformă

Exponentul principal al soluțiilor de dezvoltare multiplatformă bazate pe compilarea codului este Microsoft MAUI (Xamarin), care corespunde cu .NET-Android /.NET-iOS. Utilizând C# ca limbaj de programare principal, soluția facilitează utilizarea interferențelor native și oferă acces direct la API-ul nativ. Fiecare platformă (în afară de.NET MAUI, care oferă o posibilitate comună de UI) trebuie să aibă propriul proiect creat special pentru interfața cu utilizatorul, iar bibliotecile portabile (PCL) sunt folosite pentru a partaja codul între ele.

6.3.2 Dezvoltarea folosind tehnici hibride web

Scripturile sunt fundamentul aplicațiilor dezvoltate prin tehnici hibride web. Scripturile pot fi executate prin diversele rutine ale browserelor web [124]. O colecție de API-uri pentru manipularea componentelor de nivel inferior (funcții hardware, managementul resurselor etc.) care sunt vizibile din JavaScript este, de asemenea, pusă la dispoziția dezvoltatorului [125].

Aplicațiile hibride prezintă un decalaj semnificativ de performanță în comparație cu aplicațiile native, în primul rând ca urmare a naturii distincte a resurselor.

6.3.3 Analiza comparativă a consumului de energie

Tabelul 16 ilustrează rezultatele evaluării pentru transmisia Bluetooth.

Tabelul 16

Consumul de energie pentru comunicarea prin Bluetooth

Tip aplicație	Consum pe distanta scurta (mW)	Consum pe distanță lungă (mW)
Nativă	524,8	536,8
Compilată multiplatformă	527,1	539,1
Hibrid multiplatformă	648,3	685,7

Tabelul 17 ilustrează rezultatele evaluării pentru transmisia NFC.

Tabelul 17

Consumul de energie pentru comunicații bazate pe NFC

Tip aplicație	Consum (mW)
Nativă	42
Compilată multiplatformă	51,2
Hibrid multiplatformă	67,9

6.3.4 Analiză comparativă din punct de vedere al performanței de calcul

Aplicația nativă a atins cea mai mare viteză de transmisie a datelor, urmată de aplicația compilată multiplatformă . Acest lucru sugerează că ACW și MCW au o supraîncărcare mai mică decât apelurile JavaScript.

6.4 Performanță din perspectiva utilizatorului asupra aplicațiilor multiplatformă

Pentru a evalua impactul metodelor de dezvoltare multiplatformă asupra performanței aplicațiilor medicale mobile, a fost efectuată o analiză în timp real. Această analiză a fost efectuată utilizând următoarele patru criterii primare:

- Timpul de execuție;
- Timpul de pornire;
- Utilizarea procesorului;
- Utilizarea memoriei.

Se observă că Flutter este mai eficient decât .Net în ceea ce privește randarea și timpul de navigare. Această discrepanță este produsă de motorul de randare Flutter Skia, care este utilizat pentru redarea grafică.

În ceea ce privește timpul de pornire, testele indică faptul că ambele soluții prezintă variabilitate în performanță, cu fluctuații mai vizibile raportate pentru Flutter.

Legat de utilizarea procesorului Flutter consumă resurse CPU mai mari în comparație cu .NET, ceea ce duce la un consum crescut al bateriei și la încălzirea dispozitivului. Aplicațiile .NET arată o utilizare redusă a CPU și demonstrează o eficiență superioară în gestionarea resurselor sistemului.

În ceea ce privește utilizarea memoriei, .NET consumă mai puțină memorie și generează o utilizare mai stabilă a memoriei în comparație cu Flutter.

Dacă aplicațiile native nu sunt o alternativă viabilă din cauza costurilor financiare crescute și a timpului de dezvoltare, aplicațiile compilate multiplatformă sunt soluția preferată în ecosistemele e-Sănătate pentru eficientizarea consumului de resurse. Acest lucru este susținut de analiza performanței prezentată, care se bazează pe timpul de execuție, timpul de pornire, utilizarea CPU și utilizarea memoriei.

6.5 Concluzii

Testele comparative au arătat că soluțiile de compilare multiplatformă au obținut cea mai mare performanță, cu o scădere a performanței cu 10,6% comparativ cu aplicațiile native. În sens invers, tehnicile bazate pe web au ca rezultat o depreciere a performanței cu 34,4%.

În ceea ce privește tehnologiile de comunicație pe distanță scurtă care pot fi utilizate pentru schimbul de date între dispozitive și dispozitivele medicale portabile, Bluetooth este o soluție viabilă, în special datorită seturilor mici de date care trebuie partajate și a acoperirii sale suficiente.

6.5.1 Contribuții

- A fost efectuată comparația și evaluarea diferitelor tehnologii pentru comunicația pe distanțe scurte cu scopul de a determina limitările lor tehnologice și performanța de comunicare.

- A fost efectuată comparația și evaluarea diferitelor tehnologii de dezvoltare multiplatformă (Flutter și .Net) pentru a evalua performanța generală din perspectiva utilizatorului.
- A fost propusă o metodologie de analiză comparativă pentru a compara performanța de calcul, consumul de energie și ușurința de dezvoltare a aplicațiilor native, compilate multiplatformă și hibride multiplatformă.
- A fost propusă o metodologie de analiză comparativă pentru a determina diferențele unei soluții multi-platformă în contextul performanței tehnologiilor de comunicare pe distanțe scurte.

7. Îmbunătățirea securității aplicațiilor mobile medicale bazate pe cloud folosind API-uri de atestare a dispozitivelor

7.1 Introducere

Acest capitol examinează problemele de securitate primare și soluționarea acestora prin utilizarea serviciilor de atestare de la nivelul dispozitivelor mobile. Aceste servicii confirmă autenticitatea aplicației client, precum și a dispozitivului care rulează aplicația.

7.2 Vulnerabilitatea serviciilor REST în contextul aplicațiilor mobile

Caracteristicile de securitate încorporate oferite de sistemul de operare reduc frecvența problemelor de securitate prezente în aplicații. Din păcate, aceste caracteristici sunt incapabile să protejeze sistemul de atacurile care provin la niveluri inferioare ale stivei de aplicații.

Pentru a reduce acest tip de probleme de securitate, Android oferă funcționalitatea de atestare a dispozitivului numită SafetyNet [141]. SafetyNet este capabil să verifice integritatea smartphone-ului, poate oferi informații despre starea root a dispozitivului, deblocarea bootloaderului și integritatea aplicației. Implementarea acestor tipuri de validări reduce posibilitatea unui atac și împiedică atacatorii să folosească unelte de analiză dinamică

7.3 API-ul de atestare pentru Android

Android SafetyNet [141] reprezintă o soluție de securitate furnizată prin serviciile Google Play care este capabilă să protejeze aplicația pentru unele probleme de securitate, cum ar fi: utilizatori falși, modificarea dispozitivului pe care rulează, aplicații malware, modificarea URL-urilor.

Soluția SafetyNet este compusă din patru componente: Attestation API, Safe Browsing API, reCAPTCHA API și Verify Apps API [141].

7.4 Utilizarea API-ului de atestare pentru a securiza serviciile cloud

Componenta de gestionare a sesiunii este o parte integrantă a majorității serviciilor web. Principalele proprietăți care trebuie luate în considerare pentru componenta de gestionare a sesiunii sunt criptarea, disponibilitatea ridicată și securitatea. Componenta de criptare este necesară pentru a preveni atacurile „man-in-the-middle”. Pentru a evita modificarea sau furtul cookie-urilor de sesiune, trebuie utilizat SSL/TLS.

Chiar dacă pe partea de server verificările de integritate și securitate sunt în controlul nostru, din păcate, aplicația client rulează într-un mediu necontrolat. Pornind de la această premisă, scopul este de a asigura integritatea și controlul securității aplicației client. SafetyNet permite conexiuni mai sigure și de încredere între server și client.

Principala îmbunătățire pe care o poate aduce API-ul de atestare este eliminarea accesului clientului la componentele de gestionare a sesiunii dacă comunicarea a fost deja invalidată de

mecanismul de atestare. Validarea continuă este esențială, nu numai când începe sesiunea, ci și în timpul fiecărei sesiuni de reîmprospătare sau expirare.

7.5 Evaluarea securității

Prin analiza calitativă a mecanismului de protecție, după 1 an de funcționare, mecanismul a reușit să protejeze sistemul de un număr de 3871 de atacuri, la un număr activ de utilizatori ai aplicației de 52,3 K.

Analizând modelele de amenințare pentru cloud computing folosind modelul STRIDE (spoofing, tampering, repudiation information disclosure, denial of service, elevation of privilege) [145], atestarea intergității dispozitivului oferă un mediu cloud mai sigur.

Din păcate, ca toate mecanismele de securitate, există câteva metode de a ocoli API-ul de atestare SafetyNet. Un exemplu este Magisk, care reprezintă o modalitate modernă de a debloca

7.6 Contribuții

- A fost dezvoltat un system nou și inovator de management al sesiunilor. Acest sistem încorporează informații detaliate cu privire la integritatea clientului, incluzând atât aplicația client, cât și dispozitivul client..
- A fost dezvoltată o metodologie de analiză a securității pentru a identifica vulnerabilitățile de securitate în serviciile REST pentru aplicațiile cloud, cum ar Flooding Attacks, Action Tampering, Injection and Payload attacks, și JSON hijacking.
- A fost propusă o metodologie de analiză a securității pentru a evalua eficiența diferitelor instrumente în abordarea diferitelor probleme de integritate a dispozitivului.
- A fost dezvoltat un model de clasificare pentru problemele de securitate care afectează aplicațiile mobile. Obiectivul fiind prezentarea principalelor probleme de securitate.

8. Concluzii

8.1 Contribuții

Această teză oferă soluții validate și prototipate pentru a asigura o disponibilitate ridicată a serviciilor de e-Sănătate și pentru a oferi o modalitate sigură de integrare pentru software-ul vechi, dar și pentru diversele dispozitivele medicale, cu scopul de a genera o experiență completă și sigură pentru toți utilizatorii care folosesc sistemul, indiferent de rolul lor. Prin implementarea acestor soluții în aplicații puse în producție, această teză contribuie la securitatea software-ului e-Sănătate în diferite contexte.

8.2 Lista detaliata

- **Migrarea sistemelor e-Sănătate de la modelul de arhitectură monolitic la o arhitectură pe bază de microservicii**
  - A fost dezvoltat un nou sistem e-Health de microservicii pentru a gestiona eficient fluctuațiile de trafic și pentru a reduce costurile prin încorporarea metodelor de scalare atât pe verticală, cât și pe orizontală.
  - A fost configurată o întreagă infrastructură cloud folosind Azure cloud pentru a evalua soluția arhitecturală propusă.
  - A fost propusă o metodologie de testare pentru a evalua performanța diferitelor sisteme de e-Sănătate în raport cu disponibilitatea serviciilor și pentru a determina limitările sistemelor.
  - Au fost dezvoltate și evaluate o serie de măsuri pentru a garanta disponibilitatea sistemelor software e-Sănătate în cazul în care acestea nu sunt în măsură să facă față variațiilor de trafic.
  - A fost creată o strategie de migrare pentru a asigura disponibilitatea sistemelor software e-Health la un cost redus. Această strategie folosește atât mecanisme de scalare verticală, cât și orizontală pentru a aborda în mod specific punctele slabe ale sistemului.
  - A fost creat un set de strategii de găzduire pentru sistemele e-Health de microservicii bazate pe soluții Azure cloud, ținând cont de costul serviciilor.
  - A fost dezvoltat un model software general prin analizarea produselor disponibile pe piață și pe baza caracteristicilor sistemelor actuale.
  - A fost propus și validat un model de clasificare pentru adoptarea sistemelor de e-Sănătate folosind datele reale colectate în timpul pandemiei de COVID-19.
- **Îmbunătățirea securității aplicațiilor mobile bazate pe servicii cloud e-Sănătate folosind API-ul de atestare a dispozitivului**
  - A fost dezvoltat un system nou și inovator de management al sesiunilor. Acest sistem încorporează informații detaliate cu privire la integritatea clientului, incluzând atât aplicația client, cât și dispozitivul client..

- A fost dezvoltată o metodologie de analiză a securității pentru a identifica vulnerabilitățile de securitate în serviciile REST pentru aplicațiile cloud, cum ar Flooding Attacks, Action Tampering, Injection and Payload attacks, și JSON hijacking.
- A fost propusă o metodologie de analiză a securității pentru a evalua eficiența diferitelor instrumente în abordarea diferitelor probleme de integritate a dispozitivului.
- A fost dezvoltat un model de clasificare pentru problemele de securitate care afectează aplicațiile mobile. Obiectivul fiind prezentarea principalelor probleme de securitate.

- **Creșterea securității aplicațiilor e-Sănătate prin utilizarea serviciilor de localizare a smartphone-urilor și a datelor biometrice**
  - A fost dezvoltat un model de autentificare OAuth 2.0 îmbunătățit. Acest model include un mecanism de securitate mai puternic care se bazează pe utilizarea datelor biometrice și a locației smartphone-urilor pentru a verifica identitatea utilizatorului.
  - A fost propus un model de clasificare a mecanismelor actuale de autentificare pentru a prezenta și clasifica diferitele modele de autentificare.
  - A fost dezvoltat un proces de înregistrare imbunătățit, care a inclus conceptul de zone geografice de încredere.
  - A fost dezvoltat și utilizat un model de analiză a performanței și a securității pentru a evalua corect schimbările de performanță și îmbunătățirile de securitate pentru diferite modele de autentificare.
- **Creșterea securității comunicațiilor pentru dispozitivele medicale Bluetooth în sistemele e-Sănătate**
  - O soluție nouă a fost concepută pentru a îmbunătăți comunicația dintre dispozitivele medicale portabile și serviciile cloud e-Sănătate. Soluția, numită Personal Medical Hub, îmbunătățește securitatea comunicației dintre dispozitivele medicale portabile și serviciile cloud e- Sănătate și reduce riscurile atacurilor de tip man-in-the-middle.
  - A fost dezvoltată o strategie de securitate pentru a aborda diferite atacuri care se bazează pe vulnerabilități. Strategia are capacitatea de a determina între trei scenarii: filtrarea atacurilor, gestionarea unui dispozitiv nesecurizat și determinarea căii de rezolvare a vulnerabilității dispozitivului.
  - A fost dezvoltat un model de evaluare de securitate pentru comunicația dispozitivelor medicale și a fost utilizat pentru a evalua cât de eficient a funcționat Personal Medical Hubs cu diferite dispozitive medicale.
- **Creșterea performanței de comunicație între dispozitivele medicale personale și serviciile cloud e-Sănătate pe baza sistemelor de dezvoltare multiplatformă**
  - A fost efectuată comparația și evaluarea diferitelor tehnologii pentru comunicația pe distanțe scurte cu scopul de a determina limitările lor tehnologice și performanța de comunicare.
  - A fost efectuată comparația și evaluarea diferitelor tehnologii de dezvoltare multiplatformă (Flutter și .Net) pentru a evalua performanța generală din perspectiva utilizatorului.
  - A fost propusă o metodologie de analiză comparativă pentru a compara performanța de calcul, consumul de energie și ușurința de dezvoltare a aplicațiilor native, compilate multiplatformă și hibride multiplatformă.

- A fost propusă o metodologie de analiză comparativă pentru a determina diferențele unei soluții multi-platformă în contextul performanței tehnologiilor de comunicare pe distanțe scurte.

8.3 Domenii de cercetare viitoare

Din perspectiva soluțiilor dezvoltate în prezenta teză, domeniile primare de cercetare în securitatea ecosistemelor e-Sănătate sunt următoarele:

- Integrarea ceasurilor inteligente pentru a spori securitatea sistemelor prin îmbunătățirea percepției asupra activităților și preocupărilor utilizatorilor.
- Încorporarea inteligenței artificiale și a roboticii pentru a proteja procesele medicale de erorile umane.
- Identificarea vulnerabilităților și protecția algoritmilor de inteligență artificială care sunt disponibili pentru medicina de laborator.
- Securizarea și protecția sistemlor de analiză destinate seturilor mari de date pentru e-Sănătate.

8.4 Lista publicațiilor originale

Jurnale (acceptat la publicare)**:**

- **Cristian Contaşel**, Razvan Rughinis, Dumitru-Cristian Tranca și Dinu Țurcanu, “Enhancing e-Health cybersecurity and resilience: shifting from monolithic to microservices architecture”, National University Of Science And Technology "POLITEHNICA" Bucharest Scientific Bulletin. Series C: Electrical Engineering and Computer Science. 2024.

Conferințe:

- Robert-Mihai Ciurea și **Cristian Contaşel** "Impact of cross platform mobile frameworks on end user performance. Flutter vs .NET 6. " XGEN International Conference on Science Communications, Journal OPACJ, No. 3, 2024
- **Cristian Contaşel**, Dumitru-Cristian Tranca și Alexandru-Viorel Palacean, "Increasing the security of web applications by using smartphones." 2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2022
- **Cristian Contaşel**, Dumitru-Cristian Tranca, Alexandru-Viorel Palacean și Daniel Rosner, "Increasing communication security for Bluetooth Medical Devices in eHealth systems." *2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2022.*
- **Cristian Contaşel**, Dumitru Cristian Tranca și Alexandru-Viorel Palacean, "Cloud based mobile application security enforcement using device attestation API." *2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2021.*

- Alexandru-Viorel Palacean, Dumitru-Cristian Trancă, **Cristian Contaşel**, Răzvan Tătăroiu și Cristian Duțescu, "IoT Enabled Optimized Architectures for GPS Anti-Theft Tracking Devices." 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2021.
- Alina Irina Pîrvan, George Cristian Pătru, Dumitru Cristian Trancă, **Cristian Contaşel** și Daniel Rosner, "Infrastructure independent rail quality diagnosis and monitoring system." 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2019.
- **Cristian Contaşel**, Razvan Rughinis, Daniel Rosner, și Dumitru-Cristian Tranca, "Impact of Cross-Platform Development Frameworks on the Performance of Mobile Communications for Short Distances." The International Scientific Conference eLearning and Software for Education. Vol. 3. " Carol I" National Defence University, 2018.

Bibliografie

[1] Hoffman, Andrew. " Web application security. ". " O'Reilly Media, Inc.", 2024.

[2] Robertson, William K., and Giovanni Vigna. "Static Enforcement of Web Application Integrity Through Strong Typing." USENIX Security Symposium. Vol. 9. 2009.

[3] Thomas, Stephen, Laurie Williams, and Tao Xie. "On automated prepared statement generation to remove SQL injection vulnerabilities." Information and Software technology 51.3 (2009): 589-598.

[4] McClure, Russell A., and Ingolf H. Krüger. "SQL DOM: compile time checking of dynamic SQL statements." Proceedings of the 27th international conference on Software engineering. 2005.

[5] Bisht, Prithvi, Parthasarathy Madhusudan, and V. N. Venkatakrishnan. "CANDID: Dynamic candidate evaluations for automatic prevention of SQL injection attacks." ACM Transactions on Information and System Security (TISSEC) 13.2 (2010): 1-39.

[6] Huang, Yao-Wen, et al. "Securing web application code by static analysis and runtime protection." Proceedings of the 13th international conference on World Wide Web. 2004.

[7] Smits, Jeff, Guido Wachsmuth, and Eelco Visser. "Flowspec: A declarative specification language for intra-procedural flow-sensitive data-flow analysis." Journal of Computer Languages 57 (2020): 100924.

[8] Livshits, V. Benjamin, and Monica S. Lam. "Finding Security Vulnerabilities in Java Applications with Static Analysis." USENIX security symposium. Vol. 14. 2005.

[9] Nguyen-Tuong, Anh, et al. "Automatically hardening web applications using precise tainting." IFIP International Information Security Conference. Boston, MA: Springer US, 2005.

[10] Balzarotti, Davide, et al. "Saner: Composing static and dynamic analysis to validate sanitization in web applications." 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008.

[11] Van Gundy, Matthew, and Hao Chen. "Noncespaces: Using Randomization to Enforce Information Flow Tracking and Thwart Cross-Site Scripting Attacks." NDSS. 2009.

[12] Saxena, Prateek, David Molnar, and Benjamin Livshits. "SCRIPTGARD: automatic context-sensitive sanitization for large-scale legacy web applications." Proceedings of the 18th ACM conference on Computer and communications security. 2011.

[13] Halfond, William GJ, and Alessandro Orso. "AMNESIA: analysis and monitoring for neutralizing SQL-injection attacks." Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering. 2005.

[14] Kruegel, Christopher, Giovanni Vigna, and William Robertson. "A multi-model approach to the detection of web-based attacks." Computer Networks 48.5 (2005): 717-738.

[15] Chong, Stephen, Krishnaprasad Vikram, and Andrew C. Myers. "SIF: Enforcing Confidentiality and Integrity in Web Applications." USENIX Security Symposium. 2007.

[16] Corcoran, Brian J., Nikhil Swamy, and Michael Hicks. "Cross-tier, label-based security enforcement for web applications." Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. 2009.

[17] Chlipala, Adam. "Static Checking of {Dynamically-Varying} Security Policies in {Database-Backed} Applications." 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI 10). 2010.

[18] Li, Xiaowei, and Yuan Xue. "Block: a black-box approach for detection of state violation attacks towards web applications." Proceedings of the 27th Annual Computer Security Applications Conference. 2011.

[19] Parno, Bryan, et al. "CLAMP: Practical prevention of large-scale data leaks." 2009 30th IEEE Symposium on Security and Privacy. IEEE, 2009.
[20] Son, Sooel, Kathryn S. McKinley, and Vitaly Shmatikov. "Rolecast: finding missing security checks when you do not know what checks are." Proceedings of the 2011 ACM international conference on Object oriented programming systems languages and applications. 2011.
[21] Balzarotti, Davide, et al. "Multi-module vulnerability analysis of web-based applications." Proceedings of the 14th ACM conference on Computer and communications security. 2007.
[22] Bisht, Prithvi, et al. "Notamper: automatic blackbox detection of parameter tampering opportunities in web applications." Proceedings of the 17th ACM conference on Computer and communications security. 2010.
[23] World Health Organization. "Health technology assessment of medical devices." (2011).
[24] Almohri, Hussain, et al. "On threat modeling and mitigation of medical cyber-physical systems." 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2017.
[25] Papaioannou, Maria, et al. "A survey on security threats and countermeasures in internet of medical things (IoMT)." Transactions on Emerging Telecommunications Technologies 33.6 (2022): e4049.
[26] Nguyen, Tri-Hai, and Myungsik Yoo. "A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers." International Journal of Distributed Sensor Networks 13.11 (2017): 1550147717739157.
[27] Van Der Merwe, J. Rossouw, et al. "Classification of spoofing attack types." 2018 European Navigation Conference (ENC). IEEE, 2018.
[28] Basyoni, Lamiaa, et al. "Traffic analysis attacks on Tor: A survey." 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.
[29] Abbas, Sohail, et al. "Masquerading attacks detection in mobile ad hoc networks." IEEE Access 6 (2018): 55013-55025.
[30] Pandey, Abhishek Kumar, et al. "Trends in malware attacks: Identification and mitigation strategies." Critical Concepts, Standards, and Techniques in Cyber Forensics. IGI Global, 2020. 47-60.
[31] Mahjabin, Tasnuva, et al. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques." International Journal of Distributed Sensor Networks 13.12 (2017): 1550147717741463.
[32] Franklin, Joshua M., et al. Security analysis of first responder mobile and wearable devices. US Department of Commerce, National Institute of Standards and Technology, 2020.
[33] Grassi, Paul A., Michael E. Garcia, and James L. Fenton. "Digital Identity Guidelines." NIST special publication 800 (2017): 63-3.
[34] Kim, Minchul, and Taeweon Suh. "Eavesdropping vulnerability and countermeasure in infrared communication for IoT devices." Sensors 21.24 (2021): 8207.
[35] Lei, Hongjiang, et al. "Safeguarding UAV IoT communication systems against randomly located eavesdroppers." IEEE Internet of Things Journal 7.2 (2019): 1230-1244.
[36] Yan, Wenqing, et al. "PHY-IDS: A physical-layer spoofing attack detection system for wearable devices." Proceedings of the 6th ACM Workshop on Wearable Systems and Applications. 2020.
[37] Shoukry, Yasser, et al. "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015.

[38] Hafeez, Ibbad, et al. "IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge." IEEE Transactions on Network and Service Management 17.1 (2020): 45-59.
[39] Ahmed, M. Meraj, et al. "Defense against on-chip trojans enabling traffic analysis attacks." 2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). IEEE, 2020.
[40] Paudel, Ramesh, Timothy Muncy, and William Eberle. "Detecting dos attack in smart home iot devices using a graph-based approach." 2019 IEEE international conference on big data (big data). IEEE, 2019.
[41] Sai, Kuthada Mohan, et al. "Lightweight Intrusion Detection System In IoT Networks Using Raspberry pi 3b+." SysCom. 2021.
[42] Tu, Shanshan, et al. "Security in fog computing: A novel technique to tackle an impersonation attack." IEEE Access 6 (2018): 74993-75001.
[43] Lee, Seo Jin, et al. "IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction." IEEE Access 8 (2020): 65520-65529.
[44] Vidal, Jorge Maestre, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. "Online masquerade detection resistant to mimicry." Expert Systems with Applications 61 (2016): 162-180.
[45] Jo, Hyo Jin, et al. "Mauth-can: Masquerade-attack-proof authentication for in-vehicle networks." IEEE transactions on vehicular technology 69.2 (2019): 2204-2218.
[46] Jacoby, Grant A., Randy Marchany, and NathanielJ Davis. "Battery-based intrusion detection a first line of defense." Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.. IEEE, 2004.
[47] Dovom, Ensieh Modiri, et al. "Fuzzy pattern tree for edge malware detection and categorization in IoT." Journal of Systems Architecture 97 (2019): 1-7.
[48] HaddadPajouh, Hamed, et al. "A deep recurrent neural network based approach for internet of things malware threat hunting." Future Generation Computer Systems 85 (2018): 88-96.
[49] Fielding, Roy Thomas. Architectural styles and the design of network-based software architectures. University of California, Irvine, 2000.
[50] Goltzsche, David, et al. "Trustjs: Trusted client-side execution of javascript." Proceedings of the 10th European Workshop on Systems Security. 2017.
[51] Van Acker, Steven, and Andrei Sabelfeld. "Javascript sandboxing: Isolating and restricting client-side javascript." Foundations of Security Analysis and Design VIII: FOSAD 2014/2015/2016 Tutorial Lectures 15 (2016): 32-86.
[52] De Groef, Willem. "Client-and Server-Side Security Technologies for JavaScript Web Applications." eng. PhD thesis. University of Leuven (2016).
[53] Stats, StatCounter Global. "Mobile operating system market share worldwide." Dostopno prek https://gs. statcounter. com/os-market-share/mobile/worldwide (2024).
[54] Nachenberg, Carey. "A window into mobile device security–Examining the security approaches employed in Apple's iOS and Google's Android." Symantec Security Response (2011).
[55] Bwalya, Michael, and Christopher Chembe. "A Security Framework for Mobile Application Systems: Case of Android Applications." Zambia ICT Journal 3.2 (2019): 31-43.
[56] Popa, Daniela, et al. "A security framework for mobile cloud applications." 2013 11th RoEduNet International Conference. IEEE, 2013.
[57] Lima, António, et al. "A security monitoring framework for mobile devices." Electronics 9.8 (2020): 1197.

[58] Nyambo, Devotha, Zaipuna Yonah, and Charles Tarimo. "Framework for developing secure converged web and mobile applications." International Journal of Computing and Digital Systems 9.2 (2020): 167-177.
[59] Hussain, Muzammil, et al. "A security framework for mHealth apps on Android platform." Computers & Security 75 (2018): 191-217.
[60] Phung, Phu H., et al. "Hybridguard: A principal-based permission and fine-grained policy enforcement framework for web-based mobile applications." 2017 IEEE Security and Privacy Workshops (SPW). IEEE, 2017.
[61] Krupp, Brian, Nigamanth Sridhar, and Wenbing Zhao. "SPE: security and privacy enhancement framework for mobile devices." IEEE Transactions on Dependable and Secure Computing 14.4 (2015): 433-446.
[62] Savola, Reijo M., and Markus Sihvonen. "Metrics driven security management framework for e-health digital ecosystem focusing on chronic diseases." Proceedings of the International Conference on Management of Emergent Digital EcoSystems. 2012.
[63] Kubendiran, Mohan, Satyapal Singh, and Arun Kumar Sangaiah. "Enhanced security framework for e-health systems using blockchain." Journal of Information Processing Systems 15.2 (2019): 239-250.
[64] Sfar, Arbia Riahi, et al. "Privacy preservation using game theory in e-health application." Journal of information security and applications 66 (2022): 103158.
[65] Ksibi, Sondes, Faouzi Jaidi, and Adel Bouhoula. "A Comprehensive Quantified Approach for Security Risk Management in e-Health Systems." ICETE (2). 2020.
[66] Modi, Kirit J., and Nirali Kapadia. "Securing healthcare information over cloud using hybrid approach." Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2017, Volume 2. Springer Singapore, 2019.
[67] Zhou, Jun, et al. "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system." IEEE transactions on parallel and distributed systems 26.6 (2014): 1693-1703.
[68] Silvestri, Stefano, et al. "Cyber threat assessment and management for securing healthcare ecosystems using natural language processing." International Journal of Information Security 23.1 (2024): 31-50.
[69] Kalis, Brian, Matt Collier, and Richard Fu. "10 promising AI applications in health care." Harvard business review (2018): 2-5.
[70] Business Research Company, “Patient Access /Front-end RCM Solutions Global Market Report 2024,” 2024.
[71] Weil, Tim, and San Murugesan. "IT risk and resilience—Cybersecurity response to COVID-19." IT professional 22.3 (2020): 4-10.
[72] Zaragoza, Pascal, et al. "Leveraging the layered architecture for microservice recovery." 2022 IEEE 19th International Conference on Software Architecture (ICSA). IEEE, 2022.
[73] Blinowski, Grzegorz, Anna Ojdowska, and Adam Przybyłek. "Monolithic vs. microservice architecture: A performance and scalability evaluation." IEEE Access 10 (2022): 20357-20374.
[74] Chouhan, Utkarsh, Vaibhav Tiwari, and Hradesh Kumar. "Comparing Microservices and Monolithic Applications in a DevOps Context." 2023 3rd Asian Conference on Innovation in Technology (ASIANCON). IEEE, 2023.
[75] Dickstein, Michael J., Kate Ho, and Nathaniel Mark. "Market segmentation and competition in health insurance." Journal of Political Economy 132.1 (2024): 96-148.
[76] Mulvaney-Day, Norah, et al. "Trends in use of telehealth for behavioral health care during the COVID-19 pandemic: considerations for payers and employers." American Journal of Health Promotion 36.7 (2022): 1237-1241.

[77] Millnert, Victor, and Johan Eker. "HoloScale: Horizontal and vertical scaling of cloud resources." 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC). IEEE, 2020.
[78] Gupta, Bulbul, Pooja Mittal, and Tabish Mufti. "A review on amazon web service (aws), microsoft azure & google cloud platform (gcp) services." Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India. 2021.
[79] Breneman, James E., Chittaranjan Sahay, and Elmer E. Lewis. “Introduction to reliability engineering. “ John Wiley & Sons, 2022..
[80] Pargaonkar, Shravan. "A comprehensive review of performance testing methodologies and best practices: software quality engineering." International Journal of Science and Research (IJSR) 12.8 (2023): 2008-2014.
[81] Czuper, Michal. “Applying automated performance testing with Apache Jmeter”. MS thesis. 2022.
[82] “Internet Security Threat Report” , United Stated of America, Volume 24, February 2019
[83] Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." 2012 IEEE symposium on security and privacy. IEEE, 2012.
[84] Mayer, Peter, et al. "Supporting Decision Makers in Choosing Suitable Authentication Schemes." HAISA. 2016.
[85] Renaud, Karen. "Quantifying the quality of web authentication mechanisms a usability perspective." Journal of Web Engineering (2004): 095-123.
[86] Yampolskiy, Roman V. "User authentication via behavior based passwords." 2007 IEEE Long Island Systems, Applications and Technology Conference. IEEE, 2007.
[87] Aravindhan, K., and R. R. Karthiga. "One time password: A survey." International Journal of Emerging Trends in Engineering and Development 1.3 (2013): 613-623..
[88] Joshi, Abhilash M., and Balachandra Muniyal. "Authentication Using Text and Graphical Password." 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2018.
[89] Bhand, Amol, et al. "Enhancement of password authentication system using graphical images." 2015 International Conference on Information Processing (ICIP). IEEE, 2015.
[90] Chen, Chien-Ming, Xiaojie Zhang, and Tsu-Yang Wu. "A secure condition-based location authentication protocol for mobile devices." 2016 Third International Conference on Computing Measurement Control and Sensor Network (CMCSN). IEEE, 2016.
[91] Zhang, Feng, Aron Kondoro, and Sead Muftic. "Location-based authentication and authorization using smart phones." 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2012.
[92] Bhattacharyya, Debnath, et al. "Biometric authentication: A review." International Journal of u-and e-Service, Science and Technology 2.3 (2009): 13-28.
[93] Ambalakat, Parvathi. "Security of biometric authentication systems." 21st Computer Science Seminar. Vol. 1. 2005.
[94] Singh, Jaimandeep, and Naveen Kumar Chaudhary. "OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities." Journal of Information Security and Applications 65 (2022): 103091.
[95] Sievierinov, Oleksii, and Oleh Kholosha. "Securing Bearer token in OAuth2. 0." COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES (2021).
[96] Contașel, Cristian, Dumitru-Cristian Trancă, and Alexandru-Viorel Pălăcean. "Cloud based mobile application security enforcement using device attestation API." 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2021.

[97] Paquette, Allie, Frank Painter, and Jennifer Leigh Jackson. "Management and risk assessment of wireless medical devices in the hospital." Biomedical Instrumentation & Technology 45.3 (2011): 243-248.
[98] Omboni, Stefano, Luca Campolo, and Edoardo Panzeri. "Telehealth in chronic disease management and the role of the Internet-of-Medical-Things: the Tholomeus® experience." Expert Review of Medical Devices 17.7 (2020): 659-670.
[99] Meisner, Marta. "Financial consequences of cyber attacks leading to data breaches in healthcare sector." Copernican Journal of Finance & Accounting 6.3 (2017): 63-73.
[100] Williams, Patricia AH, and Andrew J. Woodward. "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem." Medical Devices: Evidence and Research (2015): 305-316.
[101] Tervoort, Tom, et al. "Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: a scoping review." IEEE access 8 (2020): 84352-84361.
[102] Hassija, Vikas, et al. "Security issues in implantable medical devices: Fact or fiction?." Sustainable Cities and Society 66 (2021): 102552.
[103] Liu, Long, et al. "Use-related risk analysis for medical devices based on improved FMEA." Work 41.Supplement 1 (2012): 5860-5865.
[104] Sametinger, Johannes, et al. "Security challenges for medical devices." Communications of the ACM 58.4 (2015): 74-82.
[105] "X-Force Threat Intelligence Index 2022 ", IBM Security, 2022
[106] European Parliament and Council of the European Union, "Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices," Official Journal of the European Union, vol. 60, no. April 2014, pp. 1–175, 2017
[107] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3.4 (2013): 1922-1926.
[108] Joh, HyunChul, and Yashwant K. Malaiya. "Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics." The 2011 international conference on security and management (sam). 2011.
[109] Dikkers, Frederik G., et al. "Live surgery broadcast: who is benefiting?." European Archives of Oto-Rhino-Laryngology 273 (2016): 1331-1333.
[110] Crescente, Mary Louise, and Doris Lee. "Critical issues of m-learning: design models, adoption processes, and future trends." Journal of the Chinese institute of industrial engineers 28.2 (2011): 111-123.
[111] Dalmasso, Isabelle, et al. "Survey, comparison and evaluation of cross platform mobile application development tools." 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2013.
[112] Tamura, Toshiya, and Isao Masuda. "Device connectivity technologies using short-distance wireless communications." Fujitsu Sci. Tech. J 49.2 (2013): 213-219.
[113] Bisdikian, Chatschik. "An overview of the Bluetooth wireless technology." IEEE Communications magazine 39.12 (2001): 86-94.
[114] Sobya, D. "Embedded multiple source real time monitoring and control by bluetooth support with master slave architecture and algorithms." (2018).
[115] Lee, Jae Hyeck, Myong-Soon Park, and Sayed Chhattan Shah. "Wi-Fi direct based mobile ad hoc network." 2017 2nd International Conference on Computer and Communication Systems (ICCCS). IEEE, 2017.
[116] Belghazi, Zakariae, et al. "Secure WiFi-direct using key exchange for IoT device-to-device communications in a smart environment." Future Internet 11.12 (2019): 251.
[117] Roland, Michael, Josef Langer, and Josef Scharinger. "Relay attacks on secure element-enabled mobile devices: virtual pickpocketing revisited." Information Security and

Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27. Springer Berlin Heidelberg, 2012.
[118] Lathiya, Poonam, and Jing Wang. "Near-field communications (NFC) for wireless power transfer (WPT): An overview." Wireless Power Transfer–Recent Development, Applications and New Perspectives (2021): 95-122.
[119] Preethi, K., Anjali Sinha, and April Nandini. "Contactless communication through near field communication." International Journal of Advanced Research in Computer Science and Software Engineering 2.4 (2012): 158-163.
[120] Kostakos, Vassilis, and Eamonn O'Neill. "NFC on mobile phones: issues, lessons and future research." Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07). IEEE, 2007.
[121] Jobe, William. "Native Apps vs. Mobile Web Apps." International Journal of Interactive Mobile Technologies 7.4 (2013).
[122] Kulkarni, Prajakta, and Yusuf Öztürk. "Requirements and design spaces of mobile medical care." ACM SIGMOBILE Mobile Computing and Communications Review 11.3 (2007): 12-30.
[123] Mark Reynolds, "Xamarin Mobile Application Development for Android", Pakt Publishing, UK, 2014
[124] Dickson, Jared. "Xamarin mobile development." (2013).
[125] Andrew Lunny, "PhoneGap Beginner's Guide", Pakt Publishing, UK, 2011
[126] Shrivasi, Avinash, and Anandkumar Pardeshi. "Implementation of cross-platform mobile application using phone-gap framework." International Journal of Computer Science and Engineering (IJCSE) 3 (2014): 23-30.
[127] Wargo, John M. PhoneGap essentials: Building cross-platform mobile apps. Addison-Wesley, 2012.
[128] Gomez, Carles, Joaquim Oller, and Josep Paradells. "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology." sensors 12.9 (2012): 11734-11753.
[129] Moron, María José, et al. "Overhead and Segmentation Mismatch Effect on Bluetooth WPAN Performance." Wireless personal communications 50 (2009): 161-180.
[130] Andonoska, Anita, and Kire Jakimoski. "Performance Evaluation of Mobile Applications." Proceedings of the Third International Conference on Autonomic and Autonomous Systems (ICAS'07), Struga, Macedonia. 2018.
[131] Datta, Diya, and Kajanan Sangaralingam. "Do app launch times impact their subsequent commercial success?." International Journal of Big Data Intelligence 3.4 (2016): 279-287.
[132] Dorfer, Thomas, Lukas Demetz, and Stefan Huber. "Impact of mobile cross-platform development on CPU, memory and battery of mobile devices when using common mobile app features." Procedia Computer Science 175 (2020): 189-196.
[133] Gil, Celio, et al. "A conceptual exploration for the safe development of mobile devices software based on OWASP." Int. J. Appl. Eng. Res 13.18 (2018): 13603-13609.
[134] Mulligan, Gavin, and Denis Gračanin. "A comparison of SOAP and REST implementations of a service based interaction independence middleware framework." Proceedings of the 2009 Winter Simulation Conference (WSC). IEEE, 2009.
[135] Neumann, Andy, Nuno Laranjeiro, and Jorge Bernardino. "An analysis of public REST web service APIs." IEEE Transactions on Services Computing 14.4 (2018): 957-970.

[136] Díaz-Rojas, Josué Alejandro, et al. "Web api security vulnerabilities and mitigation mechanisms: A systematic mapping study." 2021 9th International Conference in Software Engineering Research and Innovation (CONISOFT). IEEE, 2021.
[137] Zhao, Fengyu, Xin Peng, and Wenyun Zhao. "Multi-tier security feature modeling for service-oriented application integration." 2009 Eighth IEEE/ACIS International Conference on Computer and Information Science. IEEE, 2009.
[138] Masood, Adnan, and Jim Java. "Static analysis for web service security-Tools & techniques for a secure development life cycle." 2015 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, 2015.
[139] Zhang, Yi. "User Identity Hiding Method of Android." Research Anthology on Securing Mobile Technologies and Applications. IGI Global, 2021. 413-425.
[140] Garg, Shivi, and Niyati Baliyan. "Android security assessment: A review, taxonomy and research gap study." Computers & Security 100 (2021): 102087.
[141] Mulliner, Collin. "Inside Android's SafetyNet Attestation: Attack and Defense." 34th Chaos Communication Congress, 2017
[142] Kim, Taehun, et al. "Breaking ad-hoc runtime integrity protection mechanisms in android financial apps." Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017.
[143] Nguyen-Vu, Long, et al. "Android rooting: An arms race between evasion and detection." Security and Communication Networks 2017.1 (2017): 4121765.
[144] Furfaro, Angelo, et al. "Modelling and simulation of a defense strategy to face indirect DDoS flooding attacks." Internet and Distributed Computing Systems: 7th International Conference, IDCS 2014, Calabria, Italy, September 22-24, 2014. Proceedings 7. Springer International Publishing, 2014.
[145] Xin, Tong, and Ban Xiaofang. "Online banking security analysis based on STRIDE threat model." International Journal of Security and Its Applications 8.2 (2014): 271-282.
[146] Florea, Iulia Maria, Gabriel Ghinita, and Razvan Rughinis. "Sharing of network flow data across organizations using searchable encryption." 2021 23rd International Conference on Control Systems and Computer Science (CSCS). IEEE, 2021.
[147] Vochescu, Alexandru, Ioana Culic, and Alexandru Radovici. "Multi-layer security framework for IoT devices." 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2020.
[148] Pepito, Joseph Andrew, et al. "Intelligent humanoid robots expressing artificial humanlike empathy in nursing situations." Nursing Philosophy 21.4 (2020): e12318.
[149] Liu, Tangyou, et al. "A Review on the Form and Complexity of Human–Robot Interaction in the Evolution of Autonomous Surgery." Advanced Intelligent Systems (2024): 2400197.
[150] Reed, J. Craig, and Nicolas Dunaway. "Cyberbiosecurity Implications for the Laboratory of the Future." Frontiers in bioengineering and biotechnology 7 (2019): 182.
[151] Adeghe, Ehizogie Paul, Chioma Anthonia Okolo, and Olumuyiwa Tolulope Ojeyinka. "The role of big data in healthcare: A review of implications for patient outcomes and treatment personalization." World Journal of Biology Pharmacy and Health Sciences 17.3 (2024): 198-204.