IOSUD – UNIVERSITATEA „DUNĂREA DE JOS” DIN GALAȚI
Școala Doctorală de Științe Fundamentale și Inginerești

TEZĂ DE DOCTORAT
Rezumat
Contribuții privind securitatea informației prin implementarea mecanismelor hibride de autentificare

Doctorand,

Georgiana CRIHAN-AFOCȘOAIE

Conducător științific,

Prof. univ. dr. ing. Luminița DUMITRIU

Seria I 2: Calculatoare și tehnologia informației Nr. 9
GALAȚI
2024

IOSUD – UNIVERSITATEA „DUNĂREA DE JOS” DIN GALAȚI
Școala Doctorală de Științe Fundamentale și Inginerești

TEZĂ DE DOCTORAT

Rezumat

Contribuții privind securitatea informației prin implementarea mecanismelor hibride de autentificare

Doctorand,

Georgiana CRIHAN-AFOCȘOAIE

Președinte:	**Prof. dr. ing. habil. Marian BARBU** *Universitatea „Dunărea de Jos” din Galați*
Conducător științific:	**Prof. dr. ing. Luminița DUMITRIU** *Universitatea „Dunărea de Jos” din Galați*
Referenți științifici:	**Prof. dr. ing. Nicolae ȚĂPUȘ** *Universitatea Națională de Știință și Tehnologie Politehnica București*
	Prof. dr. ing. Horia CIOCÂRLIE *Universitatea Politehnică Timișoara*
	Conf. dr. ing. Emilia PECHEANU *Universitatea „Dunărea de Jos” din Galați*

Seria I 2: Calculatoare și tehnologia informației Nr. 9
GALAȚI
2024

Seriile tezelor de doctorat susținute public în UDJG începând cu 1 octombrie 2013 sunt:

Domeniul fundamental ȘTIINȚE INGINEREȘTI

Seria I 1**:** **Biotehnologii**
Seria I 2**:** **Calculatoare și tehnologia informației**
Seria I 3: **Inginerie electrică**
Seria I 4**:** **Inginerie industrială**
Seria I 5: **Ingineria materialelor**
Seria I 6**:** **Inginerie mecanică**
Seria I 7**:** **Ingineria produselor alimentare**
Seria I 8: **Ingineria sistemelor**
Seria I 9**:** **Inginerie și management în agicultură și dezvoltare rurală**

Domeniul fundamental ȘTIINȚE SOCIALE

Seria E 1: **Economie**
Seria E 2: **Management**
Seria E 3: **Marketing**
Seria SSEF: **Știința sportului și educației fizice**
Seria SJ: **Drept**

Domeniul fundamental ȘTIINȚE UMANISTE

Seria U 1: **Filologie- Engleză**
Seria U 2: **Filologie- Română**
Seria U 3**:** **Istorie**
Seria U 4: **Filologie - Franceză**

Domeniul fundamental MATEMATICĂ ȘI ȘTIINȚE ALE NATURII

Seria C: **Chimie**

Domeniul fundamental ȘTIINȚE BIOMEDICALE

Seria M: **Medicină**
Seria F: **Farmacie**

CUPRINS

Cuvinte cheie:

Autentificare biometrică; criptare complet homomorfă; algoritm BFV; algoritm BGV; algoritm CKKS; autentificare facială; recunoașterea amprentei; Raspberry Pi; module Arduino; autentificare RFID;

INTRODUCERE

În mediul actual de securitate aflat într-o dinamică permanentă, caracterizat prin diversificarea continuă a vectorilor de atac datorită digitalizării din majoritatea domeniilor de activitate, mecanismele de identificare și autentificare au devenit o condiție esențială pentru asigurarea securității informațiilor. Urmare la incidentele de securitate recente, se poate afirma faptul că autentificarea utilizatorilor constituie prima linie de apărare împotriva atacurilor emergente și poate fi considerată un element definitoriu al oricărei infrastructuri de securitate. Autentificarea cu un singur factor s-a dovedit a fi vulnerabilă la vectorii de atac și pentru a preveni aceste atacuri, este necesară o schemă de autentificare matură, de înaltă securitate, pentru a susține profilul dinamic al utilizatorilor în diverse aplicații. Mai exact, nivelul de protecție pentru mecanismul de control al accesului crește exponențial, atunci când doi sau mai mulți factori sunt aplicați ca parte a procesului de verificare a identității și este adoptată o metodă de autentificare hibridă fundamentată pe asocierea și implementarea complementară factorilor de autentificare, bazați pe „ceva ce ești”, „ceva ce ai” sau „ceva ce știi” [3].

Motivați de această nevoie emergentă, în această cercetare am proiectat două mecanisme de autentificare inovatoare și hibride, obținute prin interconectarea componentei biometrice („ceva ce ești”) și a componentei criptografice („ceva ce ai”), doi factori promițători care joacă un rol esențial în securizarea informațiilor în sistemele actuale de control al accesului. Aceste instrumente pot fi utilizate pentru a proteja credențialele de acces ale utilizatorului împotriva persoanelor neautorizate, dar și pentru a facilita accesul securizat la sistemele și rețelele informatice

Obiectivele tezei

Contribuțiile principale ale prezentei teze de doctorat se concentrează pe următoarele obiective operaționale principale, după cum urmează:

1. Analizarea stadiului actual al metodelor și mecanismelor de autentificare în contextul mediului de securitate aflat într-o dinamică permanentă, în vederea identificării factorilor care au cel mai bun potențial de dezvoltare pentru securizarea datelor de acces ale utilizatorilor.
2. Proiectarea, dezvoltarea și implementarea unui mecanism hibrid de autentificare, cu trei straturi structurale bazate pe amprentă, componenta RFID și componenta criptografică, realizate prin interconectarea mai multor module Arduino, destinat pentru securizarea sistemelor informaționale independente, dar și pentru dispozitivele de rețea.
3. Proiectarea, dezvoltarea și implementarea unui mecanism de autentificare versatil și non-invaziv cu două straturi structurale de autentificare, care combină caracteristicile biometrice faciale și componenta criptografică, un sistem relativ complex și compact care cuprinde module Raspberry Pi și Arduino, având ca destinație integrarea în cadrul sistemelor care vehiculează informații extrem de

sensibile din infrastructuri critice (în special în domeniul militar), unde numărul utilizatorilor autorizați este limitat și restricționat.

4. Îmbunătățirea securității stocării informațiilor biometrice ale utilizatorului prin criptarea datelor utilizând diferiți algoritmi de criptare homomorfă.
5. Realizarea unei analize comparative între algoritmii criptografici selectați pentru experimentare, și anume algoritmul de criptare ***parțial*** homomorf Paillier, respectiv algoritmii de criptare ***complet*** homomorfă Brakerski-Fan-Vercauteren (BFV), Brakerski-Gentry-Vaikuntanathan (BGV) și Cheon-Kim-Kim-Son (CKKS) aplicați asupra bazelor de date biometrice, utilizând o serie de parametri statistici, specifici domeniului de prelucrare a imaginilor, cu scopul de a identifica și evalua cel mai eficient și convenabil algoritm care poate oferi o securitate puternică, cu o bună performanță de recunoaștere.
6. Evaluarea vulnerabilităților, identificarea potențialelor atacuri asupra elementelor componente din cadrul mecanismelor de autentificare propuse și prezentarea unor direcții inovatoare de contracarare a acestora în contextul abstractizării instrumentelor de atac.

Conținutul capitolelor

Primul capitol al cercetării științifice aduce în prim plan fundamentarea teoretică și crearea cadrului conceptual al metodelor și mecanismelor de autentificare actuale, fiind descrise principalele vulnerabilități, potențialele atacuri și metodele de contracarare ale acestora în actualul mediu de securitate. Se pune accentul pe factorii biometrici și algoritmii criptografici homomorfi selectați pentru implementare, utilizați pentru a securiza datele stocate ale unui sistem de autentificare biometric.

Capitolul 2 al lucrării constă în descrierea arhitecturii soluțiilor tehnice propuse, atât din punct de vedere al construcției hardware în ceea ce privește modul de interconectare și funcționare a modulelor utilizate, dar și din punct de vedere software, fiind prezentate configurările elementelor componente, modalitatea de a realiza managementul bazei de date a utilizatorilor autorizați, dar și etapizarea procesului de autentificare. De asemenea, analiza comparativă cu metodele și mecanismele prezentate în literatura de specialitate are rolul de a evidenția principalele avantaje ale mecanismelor propuse și aportul acestora în îmbunătățirea capabilităților sistemelor informaționale și optimizarea nivelului de acces.

Structurarea capitolului 3 în două părți are drept obiectiv descrierea matematică, în prima parte, a algoritmilor criptografici homomorfi, respectiv criptosistemul Paillier și algoritmii complet homomorfi BFV, BGV și CKKS, urmând ca în cea de-a doua parte atenția să se concentreze pe evaluarea algoritmilor criptografici utilizând o serie de parametri statistici, precum analiza histogramei, entropiei, eroarea pătratică medie (MSE - Mean Squared Error), raportul maxim semnal/ zgomot (PSNR - Peak Signal-to-Noise Ratio), măsura indicelui de similaritate structurală (SSIM - Structural Similarity Index), rata de modificare a numărului de pixeli (NPCR - Number of Pixel Change Rate), intensitatea medie unificată de schimbare (UACI - Unified Average Changing Intensity), precum și timpul mediu de criptare.

Capitolul 4 este focalizat pe analiza principalelor vulnerabilități ale factorilor din structura mecanismelor de autentificare propuse, din punct de vedere al implicațiilor

privind asigurarea confidențialității, integrității și autenticității informațiilor disponibile într-un sistem informatic, fizic sau virtualizat, dar și pe prezentarea atacurilor emergente la adresa acestora și a diverselor contramăsuri, prin care se poate realiza suplimentarea măsurilor de securitate. Elementul de noutate constă în descrierea direcțiilor viitoare de acțiune ce pot fi asociate mecanismelor create, care sunt în stadiu incipient de testare și validare în comunitatea științifică, dar prezintă un potențial deosebit de dezvoltare.

Capitolul 5 este rezervat descrierii unor scenarii de implementare a mecanismelor de autentificare proiectate, prin integrarea acestor instrumente de protecție a accesului în diverse ipoteze de lucru prin care se ilustrează versatilitatea acestora, dar și potențialul lor ridicat de a fi valorificate în domenii sensibile, caracterizate prin cerințe stricte privind necesitatea asigurării unui nivel înalt de protecție a informațiilor vehiculate în format electronic.

Teza de doctorat se încheie cu prezentarea concluziilor finale, care sintetizează principalele beneficii ale implementării acestor dispozitive în infrastructura de rețea, identificarea direcțiilor de cercetare viitoare şi diseminarea rezultatelor specifice de cercetare, diagrama de mai jos prezentată în figura 1 concentrând structura și punctele esențiale abordate în cadrul lucrării. Tematica tezei de doctorat este de actualitate și se află într-o continuă dinamică și dezvoltare, fiind determinată de interacțiunea permanentă a utilizatorilor cu sistemele de comunicații și informatică și serviciile oferite de acestea, care constituie obiectul digitalizării cu mediul înconjurător, dar și de nevoia stringentă de securizare a datelor de acces în timp real.

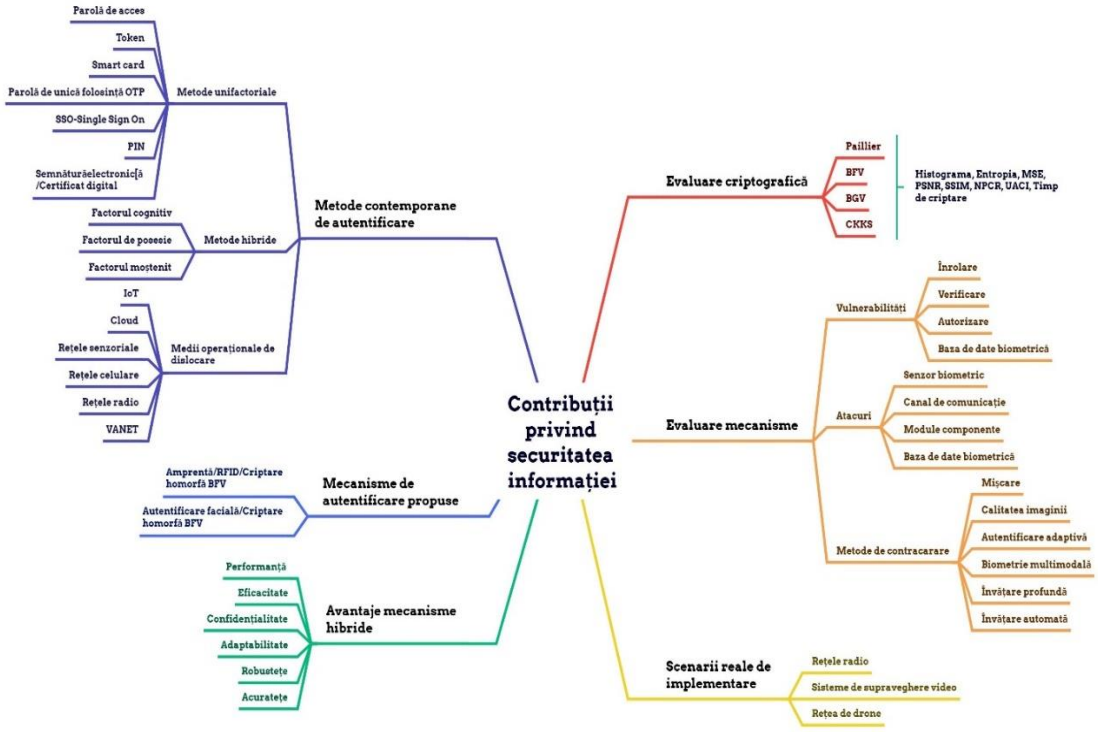


Fig. 1.1 Structura și punctele cheie ale tezei de doctorat

CAPITOLUL I STADIUL ACTUAL AL PROTECȚIEI INFORMAȚIILOR BIOMETRICE PRIN UTILIZAREA ALGORITMILOR DE CRIPTARE HOMOMORFĂ

1.1 Metode de autentificare actuale utilizate în sistemele și rețelele informaționale

În contextul actual în care autentificarea devine prima linie de apărare împotriva vectorilor de atac, necesitatea securizării sistemelor informatice reprezintă principala preocupare în ceea ce privește asigurarea unui flux informațional protejat într-un posibil mediu agresiv. Implementarea acestui deziderat se poate realiza prin interconectarea celor trei piloni ai triadei CIA - confidențialitate, integritate și disponibilitate într-un sistem unitar prin care să se asigure fundamentul unei infrastructuri informatice protejate în cadrul unei organizații [8]. Analizând principiile de securizare a informațiilor menționate anterior, se poate evidenția faptul că, mecanismele de autentificare reprezintă un element imperativ în asigurarea securității informațiilor, rolul acestora fiind de a spori gradul de securizare al datelor sensibile vehiculate în mediul electronic, care necesită o protecție suplimentară, dar și de a realiza controlul accesului la sistemele și resursele unei entități organizaționale.

Autentificarea, offline sau online, are drept obiectiv stabilirea identității unui utilizator care încearcă să acceseze un sistem, prin introducerea și verificarea unei informații unice cunoscute numai de către utilizatorul care încearcă să se autentifice și sistemul de autentificare [9]. Autentificarea are loc de obicei la începutul unei sesiuni de comunicații, rolul acesteia fiind de a confirma identitatea părților active în sesiune. Implementarea unui proces de autentificare cuprinde, în principiu, unul din cei trei factori principali, și anume factorul bazat pe cunoștințe „ceva ce știi”, factorul bazat pe posesie „ceva ce ai” și factorul bazat pe caracteristici moștenite „ceva ce ești” [10]. Primul factor de autentificare „Ceva ce știi”, se bazează pe introducerea în sistem de către utilizator a unui element memorat pentru a-și dovedi identitatea, un bun exemplu în aceest sens fiind o parolă, o frază de acces, un cod PIN sau răspunsul la o întrebare secretă, utilizate pentru a dovedi dreptul de proprietate asupra identității. Al doilea factor de autentificare „Ceva ce ai”, presupune ca solicitantul să dețină un obiect fizic, precum un smart card sau un token de autentificare. Al treilea factor „Ceva ce ești” este reprezentat de autentificarea biometrică care funcționează prin compararea caracteristicilor reale ale utilizatorului cu datele stocate într-o bază de date pentru a determina veridicitatea trăsăturilor solicitantului.

Cei trei factori de autentificare sunt considerați cei mai uzitați factori în validarea identității utilizatorului, iar în cele ce urmează va fi realizată o descriere a metodelor și mecanismelor de autentificare recente integrate în sistemele de comunicații și informatică. Cu cât necesitatea utilizatorului de a accesa cât mai multe aplicații crește, cu atât standardele și mecanismele se diversifică, astfel încât selectarea mecanismului de autentificare potrivit este esențială pentru asigurarea operațiunilor securizate și compatibilitatea utilizării.

Una din metodele consacrate este autentificarea biometrică care constă în procesul de verificare și confirmare a identității unei persoane pe baza datelor biometrice ale acesteia. Principalele metode de autentificare biometrică utilizate în prezent, se bazează pe cele două categorii principale precizate în referința [3], respectiv biometria fiziologică și biometria comportamentală.

Metodele de autentificare se dezvoltă la diverse nivele funcționale, precum nivel de rețea, aplicații, endpoint/device și la nivel virtualizat. Prin urmare, fiecare metodă de autentificare are propriile avantaje și dezavantaje, iar selectarea unei anumite metode pentru implementare în infrastructura informațională este strâns corelată cu cerințele de securizare și nivelul funcțional la care se urmărește dezvoltarea acesteia.

Având în vedere acest deziderat, prezenta teză de doctorat are ca obiectiv principal proiectarea, implementarea și evaluarea unor mecanisme de autentificare hibride, neinvazive și scalabile, prin combinarea unor metode biometrice bazate pe caracteristici fiziologice cu algoritmi de criptare asimetrici homomorfi, cu scopul de a minimiza riscul accesului neautorizat, de a asigura confidențialitatea, integritatea și disponibilitatea informațiilor, dar și de a diminua riscurile de securitate generate de diferiți vectori de atac.

1.2 Vulnerabilități, atacuri și metode de contracarare specifice mecanismelor de autentificare

În ciuda avantajelor semnificative și a viitorului promițător pe care le dețin, protocoalele, mecanismele și metodele de autentificare sunt predispuse la vulnerabilități și amenințări multiple care le pot afecta performanța în termeni de conectivitate, productivitate, operațiuni și precizie și pot periclita securitatea datelor utilizatorului în procesul de autentificare. Exploatarea vulnerabilităților din procesul de autentificare se poate manifesta la nivelul următoarelor paliere: vulnerabilitățile rețelei, vulnerabilitățile platformei, vulnerabilitățile existente la nivelul aplicațiilor datorate erorilor de software, dar și vulnerabilitățile generate de un management defectuos.

Pe lângă factorii interni și externi care pot vulnerabiliza procesul de autentificare, există trei puncte critice care pot fi exploatate în detrimentul utilizatorului. În momentul în care utilizatorul introduce credențialele de acees, acestea ar putea fi atacate de un script sau un potențial atacator. În mod similar, atunci când credențialele de acces sunt transmise pe un canal de comunicații: fir, radio, wireless, acestea ar putea fi interceptate de un posibil atacator. În cele din urmă, atunci când credențialele de acces sunt comparate cu intrările din baza de date, acestea ar putea fi modificate pentru a obține o penetrare reușită.

Având la bază cele 3 puncte critice menționate anterior, am realizat o clasificare a principalelor tipuri de atacuri care pot periclita siguranța mecanismelor de autentificare, și am propus o serie de măsuri care pot contracara efectele negative ale acestora conform datelor prezentate în tabelul 1.1. Scopul acestor atacuri este de a distruge confidențialitatea, integritatea și autenticitatea informațiilor disponibile într-o rețea și de a exploata punctele vulnerabile din securitatea sistemelor, aplicațiilor, protocoalelor pentru a prelua controlul.

Tabel 1.1 *Măsuri de contracarare a vectorilor de atac [17]*

Potențiale amenințări la adresa autentificării	**Obiectivele securității afectate**	**Contramăsuri**
Parole implicite	Confidențialitate	Utilizarea unor parole de autentificare unice Constrângerea utilizatorilor să își schimbe parolele implicite prin intermediul setărilor din politicile de securitate Utilizarea metodelor de autentificare hibride
Atacuri de tip dicționar precalculat	Integritatea	Utilizarea unor tehnici de apărare de tip salting
Atac de reluare	Integritatea	Utilizarea parolelor unice (Exemplu: Schema Lamport – schema de generat parole one-time) Aplicarea unui mecanism de provocare și răspuns
Căutări exhaustive	Integritatea	Utilizarea parolelor cu un nivel ridicat de entropie Implementarea de politici de securitate în rețea Limitarea numărului de încercări în cazul autentificării utilizatorilor
Man-in-the-Middle	Confidențialitatea Integritatea	Utilizarea mecanismelor de criptare asimetrică sau simetrică Utilizarea unei rețele private virtuale (VPN)
Impersonarea/ mascaradarea/ clonarea	Confidențialitatea	Aplicarea autentificării bazată pe mai mulți factori de autentificare (2FA/MFA) Elaborarea și implementarea politicilor de securitate
Injecții SQL	Integritatea	Aplicarea autentificării bazată pe mai mulți factori de autentificare (2FA/MFA) Utilizarea funcțiilor criptografice hash pentru parole Utilizarea instrumentelor de protecție precum web firewall

Ghicirea parolei	Confidențialitate	Crearea unor parole cu entropie ridicată Evitarea utilizării unor parole anterioare
Furtul credențialelor de acces	Confidențialitate	Utilizarea unor parole diferite pentru diversele conturi ale unui utilizator Aplicarea autentificării bazată pe mai mulți factori de autentificare (2FA/MFA) Utilizarea unor mecanisme de tip CAPTCHA
Inginerie socială	Disponibilitate	Creșterea gradului de conștientizare a utilizatorilor Implementarea politicilor de securitate în rețelele informatice Adoptarea conceptului de apărare în adâncime prin implementarea unor tehnici procedurale pe nivele de securitate
Interzicerea utilizării serviciilor (Denial of Services)	Disponibilitate Non - repudierea	Crearea unor liste de control acces Accesul pe bază de semnătură digitală
Atac de tip forță brută	Confidențialitate	Utilizarea unor parole de autentificare unice și complexe Blocarea conturilor după un număr limitat de încercări nereușite de autentificare Aplicarea autentificării bazată pe mai mulți factori de autentificare (2FA/MFA) Utilizarea mecanismelor de criptare
Atac de tip phishing	Disponibilitate	Utilizarea unor parole de autentificare unice și complexe Utilizarea de certificate SSL pentru site-uri web Utilizarea unei rețele private virtuale (VPN)
Malware	Disponibilitate	Implementarea unui mecanism de tip “Application Whitelisting” Monitorizarea jurnalelor utilizând soluția de gestionare a incidentelor și evenimentelor de securitate (SIEM)
Amenințare persistentă avansată (APT)	Disponibilitate	Elaborarea și implementarea politicilor de securitate Utilizarea instrumentelor de protecție precum IDS/IPS/IDPS, Next Generation Firewall (NGFW) Utilizarea unei rețele private virtuale (VPN)

Implementarea unor contramăsuri de securitate eficiente la nivel hardware, software sau firmware este esențială pentru a securiza mecanismele de autentificare și a ajuta la depășirea oricărei vulnerabilități exploatabile și a lacunelor de securitate în diferite domenii care se bazează pe infrastructuri critice. Drept urmare procesul de autentificare ar trebui conceput și structurat astfel încât să asigure cel mai înalt nivel de securitate posibil pentru a preîntâmpina orice acces rău intenționat dezvoltat la nivel fizic și/sau logic. Acest lucru se poate realiza prin folosirea unei scheme de autentificare puternice, bazată pe mai mulți factori de autentificare, care poate ajuta la reducerea accesului neautorizat la resursele informaționale. Pe de altă parte, adoptarea unor soluții bazate pe algoritmi și protocoale criptografice în cadrul rețelei și/sau de la nivelul fizic sunt obligatorii pentru beneficia de o comunicație securizată cu supraîncărcare minimă. De asemenea, soluțiile tehnice non-criptografice, precum sistemele de detectare sau de prevenire a intruziunilor IDS/IPS/IDPS ar trebui proiectate pentru a monitoriza traficul de date și a preîntâmpina amenințările iminente la adresa utilizatorilor și a resurselor informaționale.

1.3 Abordarea hibridă

Creșterea dependenței de rețelele de telecomunicații și date a dovedit că autentificarea cu un singur factor este vulnerabilă în fața potențialilor vectori de atac, iar pentru a preveni aceste atacuri este necesară o schemă de autentificare matură, cu securitate sporită, care să susțină profilul dinamic al utilizatorilor în diferite sisteme și aplicații. Mecanismul de autentificare hibridă cu mai mulți factori poate fi văzut ca o extensie a autentificării cu doi factori și poate crește nivelul de securitate pentru mecanismele de control al accesului datorită numărului mai mare de factori necesari în procesul de verificare și validare a identității unei persoane. Acum este considerat un standard de facto pentru orice sistem care necesită securitate puternică.

Analizând diversitatea factorilor de autentificare și a mediilor operaționale de implementare a acestora, prezentate în literatura de specialitate, se poate evidenția că există o nevoie stringentă de securizare a accesului utilizatorilor în toate domeniile de activitate, fiind valorificați atât factorii tradiționali de autentificare, cât și factori inovatori care să adauge un nivel suplimentar de protecție sistemelor împotriva accesului neautorizat și a celorlalte tipologii de atacuri. Cu toate acestea, putem constata că factorii dominanți, valorificați în majoritatea scenariilor de autentificare, sunt reprezentați de componenta biometrică, fie cea fiziologică, fie cea comportamentală și algoritmii criptografici simetrici sau asimetrici în funcție de situație. Un alt aspect demn de remarcat, este că majoritatea metodelor propuse sunt dezvoltate la nivel software, ceea ce implică costuri mult mai reduse și un nivel mai scăzut de securizare comparativ cu nivelul hardware, care este considerat a fi superior, dar mult mai dificil de realizat din punct de vedere al asigurării logistice. O alternativă viabilă în suplimentarea măsurilor de securitate în cadrul mecanismelor de autentificare îl constituie și adoptarea următorilor factori reprezentativi specificați în cadrul referinței [28], respectiv factorul de timp, factorul de locație sau factorul de sunet ambiental.

1.4 Autentificarea biometrică

Procesul de autentificarea biometrică are la bază un algoritm de comparare, prin care se realizează potrivirea datelor biometrice preluate de un senzor interconectat la un sistem informatic cu șabloanele stocate, confirmate, autentice dintr-o bază de date cu informații biometrice. Printre cele mai bune abordări propuse pentru consolidarea procesului de autentificare a utilizatorilor se numără metodele biometrice bazate pe modele unice, cum ar fi trăsăturile fiziologice și comportamentale, care au demonstrat un efect pozitiv tangibil asupra asigurării securității contului în diverse domenii de activitate. Recunoașterea care se fundamentează pe trăsături fiziologice precum amprenta [29-30], fața [31-33], irisul [34-35], urechea [36-37], venele degetelor [38-39], bătăile inimii [40], electroencefalograma (EEG) [41], geometria palmei [42], mirosul [43] este studiată și implementată pe scară largă în diferite tipuri de scheme de păstrare a confidențialității informațiilor utilizate în aplicații din lumea reală pentru rețele radio, cloud computing, IoT, rețele informatice, rețele vehiculare. Principalul avantaj al biometriei bazate pe caracteristicile fiziologice ale utilizatorului constă în colectarea și verificarea datelor de autentificare, care se bazează pe un proces neinvaziv, dar și pe faptul că multe părți ale corpului, precum amprenta, retina și irisul, prezintă cel mai mare grad de stabilitate de-a lungul vieții unui individ.

1.4.1 Autentificarea bazată pe amprentă

Chiar dacă automatizarea recunoșterii amprentei digitale este studiată de mai bine de un secol în diferite domenii de activitate, îmbunătățiri semnificative au fost aduse acestei tehnici de-a lungul timpului pentru consolidarea procesului de autentificare a utilizatorilor prin integrarea cu alte tehnici computaționale moderne. Popularitatea amprentelor biometrice este generată de facilitatea inerentă de colectare și, de asemenea, de diversitatea surselor (zece degete) disponibile pentru identificarea unui individ, având în vedere unicitatea, invariabilitatea și consistența fiecărei amprente în parte. Recunoașterea amprentei, probabil cea mai des utilizată tehnologie biometrică în prezent, poate oferi o precizie de până la 99% în unele cazuri și funcționează prin încercarea de a identifica elementele de detaliu din structura amprentelor, precum crestele degetelor și punctele de detaliu.

1.4.2 Autentificarea bazată pe caracteristicile faciale

Arhitectura feței umane este una complexă și într-o continuă dinamică datorită trăsăturilor fizice care pot suferi modificări de-a lungul timpului. Recunoașterea facială este un mijloc natural de verificare a identității unei persoane, și se bazează pe trăsături faciale specifice, cum ar fi poziția ochilor, a nasului și a gurii împreună cu distanța dintre ele, dar și pe metode adiționale de verificare a particularităților fizice, precum pistruii de pe față, alunițele, semnele particulare pentru a valida identitatea unui utilizator. Probabil una dintre cele mai mari provocări ale sistemelor de autentificare facială îl reprezintă diferențierea unei perechi de gemeni identici, care au caracteristici faciale greu de distins, test care a fost realizat cu succes în cazul cercetării de față, deoarece mecanismul nostru a dat dovadă de promptitudine și eficacitate în identificarea fiecăruia în parte. Dezvoltarea continuă a potențialului recunoașterii faciale este determinată în mare parte de trendul ascendent de digitalizare din majoritatea domeniilor de activitate și dependenţa tot mai mare de sistemele informatice și necesitatea securizării acestora.

1.5 Concluzii

Acest capitol a oferit o imagine de ansamblu asupra diferitelor probleme și provocări deschise în domeniul de cercetare al metodelor și mecanismelor de autentificare actuale, constituind cadrul introductiv și punctul de pornire pentru următoarele două capitole, care alcătuiesc nucleul central al prezentei teze de doctorat structurată pe contribuții originale referitoare la proiectarea, testarea și evaluarea unor mecanisme hibride de autentificare la nivel hardware și software, capabile să fie aplicate diferitelor sisteme de comunicații și informatică în diverse scenarii de implementare. Propunerea actuală aduce în prim plan o serie de tehnologii conexe precum microcontrolere, microprocesoare, dar și diferiți algoritmi de criptare homomorfă, utilizați atât la nivel practic, cât și teoretic, prin combinarea cărora se urmărește implementarea unei noi abordări privind procesarea și protejarea datelor biometrice confidențiale împotriva accesului neautorizat, arhitectura metodelor de autentificare abordate putând fi reprezentată grafic conform datelor din figura 1.2.

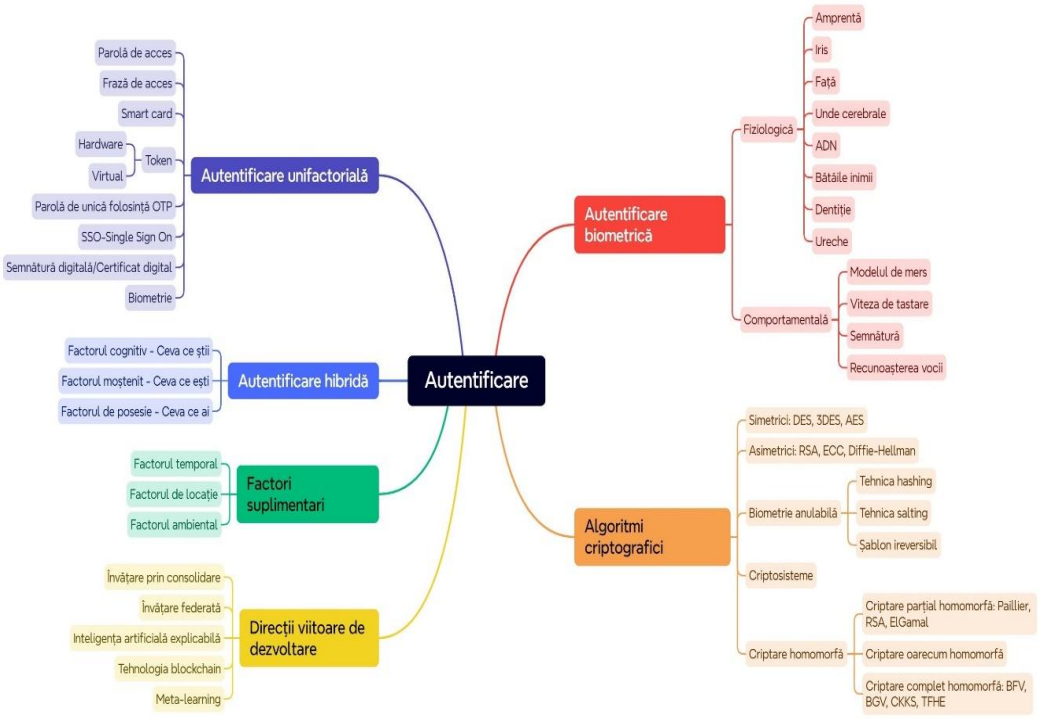


Fig. 1.2 Stadiul actual al metodelor de autentificare

CAPITOLUL II PROPUNERI DE ARHITECTURĂ A MECANISMELOR HIBRIDE DE AUTENTIFICARE

2.1 Mecanismul de autentificare bazat pe amprentă și componenta RFID

2.1.1 Structura hardware

Configurația primei soluții tehnice propuse pentru securizarea procesului de autentificare, constă în utilizarea unei plăci de dezvoltare Arduino Pro Micro 5V/16MHz care se interconectează cu un cititor de identificare prin radiofrecvență (RFID) și un scanner de amprente de înaltă performanță programate cu software-ul open-source Arduino Integrated Development Environment (IDE) și bibliotecile sale suplimentare, așa cum este prezentat în figura 2.1.

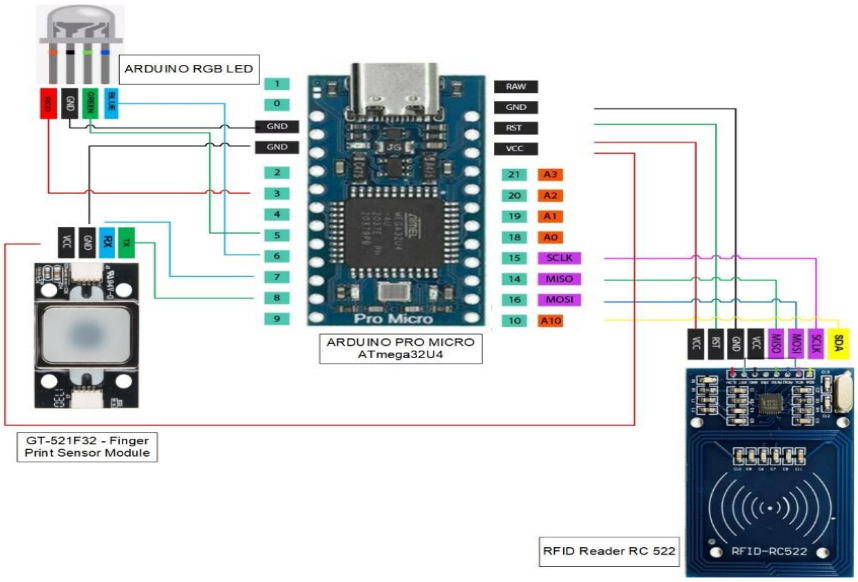


Fig. 2.1 Arhitectura mecanismului de autentificare bazat pe module Arduino [60]

2.1.2 Structura software

Din punct de vedere software, configurarea componentelor mecanismului de autentificare s-a realizat etapizat utilizând software-ul Arduino IDE, versiunea 1.8.19 și o serie de librării suplimentare, precum FPS_GT511C3.h (librăria senzorului de amprentă), SoftwareSerial.h (librăria anexă senzorului prin care se asigură conexiunea serială), Keyboard.h (librăria necesară comunicării via USB), EEPROM.h (librăria anexă pentru stocarea parolelor), SPI.h (librăria pentru conexiunea cu dispozitivele care utilizează magistrala SPI), MFRC522.h (librăria de configurare a modulului RFID).

Interfața grafică creată facilitează efectuarea unei serii de sarcini pentru managementul centralizat al bazei de date a amprentelor utilizatorilor, așa cum este redat în figura 2.2. Toate aceste operațiuni au rolul de a asigura o gestionare eficientă a înregistrărilor din sistem și o monitorizare a accesului, bazându-se pe execuția algoritmilor de scanare și deblocare PC, de înregistrare carduri, precum și de înregistrare amprentă prin alocarea unui anumit ID.

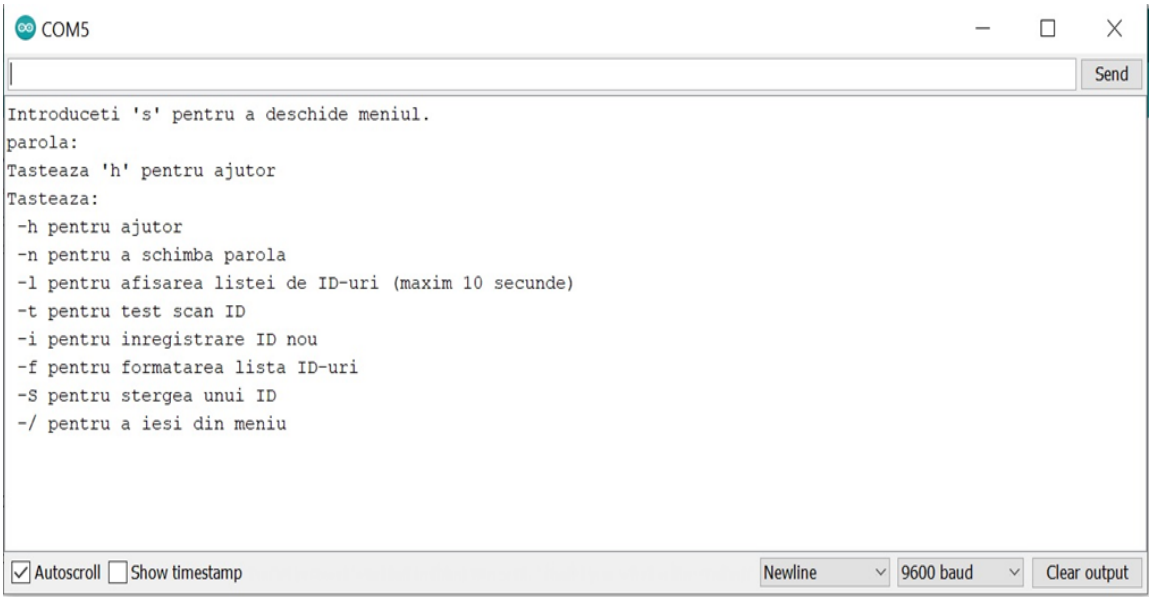


Fig. 2.2 Interfață configurare amprente de acces

2.1.3 Funcționarea mecanismului de autentificare

Procesul de autentificare biometrică al amprentei cuprinde trei faze principale, înregistrarea, verificarea și identificarea conform specificațiilor din referința [61]. În faza de înregistrare, se efectuează operația de preluare a informațiilor de la senzorul biometric, extragerea caracteristicilor biometrice autentice și stocarea șablonului în baza de date. În faza de verificare se realizează o comparație între noile capturi de date cu datele de referință ale persoanei care se autentifică. În cele din urmă în cadrul procesului de identificare, sistemul compară caracteristicile extrase din proba biometrică capturată cu șabloanele tuturor utilizatorilor din datele stocate în baza de date a sistemului, rezultatul fiind o listă de utilizatori, care poate fi goală sau poate conține una sau mai multe înregistrări care se potrivesc.

Prezentul mecanism de autentificare funcționează prin parcurgerea a două etape de verificare pentru accesarea sistemelor și resurselor rețelei de către utilizatorul autorizat, astfel: validarea ID card-ului și verificarea amprentei. În primul rând, datele seriale ale cardului de acces sunt verificate în sistem, urmând ca modulul de amprentă prin care se realizează tehnica de extracție a detaliilor să genereze șablonul utilizatorului și să îl transmită spre identificare și verificare către microcontroler.

Comparativ cu metodele structurate pe fuziunea dintre componentele biometrice și criptografice propuse în literatura de specialitate [30], [62], [63], [64], [65], [65], [66], originalitatea acestei metode derivă din nivelul de dezvoltare al metodei, în cazul nostru fiind cel hardware și baza de date utilizată pentru experimentare, care este

cea proprie generată de interacțiunea în timp real a utilizatorilor cu sistemul informatic pe care se autentifică, în timp ce majoritatea metodelor propuse folosesc baze de date predefinite existente la nivel internațional. Considerăm că interacțiunea directă, oferă rezultate mult mai relevante în contextul autentificării deoarece pot fi analizate situații neprevăzute influențate de diverși factori de natură intrinsecă sau extrinsecă, precum transpirația, zgârieturi, murdărie, cicatrici care pot afecta în mod pozitiv sau negativ verificarea identității utilizatorului și implicit acordarea drepturilor de acces.

2.2 Mecanismul de autentificare bazat pe autentificarea facială

2.2.1 Structura hardware

Din punct de vedere tehnic, cel de-al doilea mecanism de autentificare utilizat pentru experimentare, cuprinde două componente fizice principale: un modul Raspberry Pi 4 Model B cu un sistem de 8 GB LPDDR4 SDRAM și procesor quad-core 1.5 GHz, interconectat cu un microcontroler Arduino ESP32, așa cum este prezentat în figura 2.3. Modulul Raspberry Pi 4, acționează ca un hotspot activ ce poate fi accesat de celelalte dispozitive și stabilește conexiunea cu placa de dezvoltare Arduino ESP 32 și PC-ul prin capabilitățile Wi-Fi, care sunt considerați a fi clienți Wi-Fi. În timpul procesului de autentificare, modulul Raspberry Pi 4 scanează fețele utilizatorilor identificate în cadru, le compară cu cele din baza de date biometrică și dacă este identificată fața utilizatorului autorizat, furnizează informațiile de conectare către modulul ESP32, așa cum este prezentat în figura 2.3.

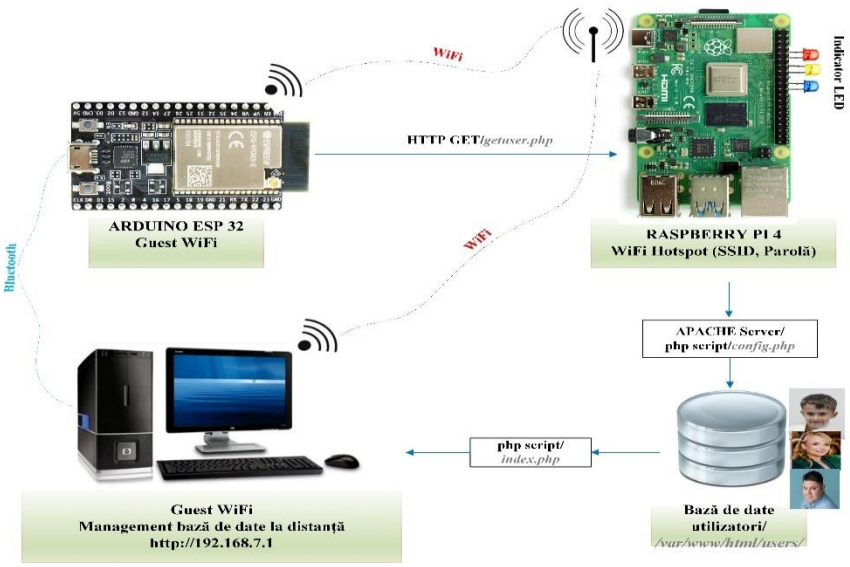


Fig. 2.3 Arhitectura mecanismui de autentificare bazat pe module Raspberry și Arduino [67]

2.2.2 Structura software

Mecanismul de autentificare propus este un sistem complex care presupune mai multe configurări software, astfel:

- instalarea și configurarea Raspberry Pi cu software-ul Python și bibliotecile sale standard folosite pentru identificare și autentificare,
- configurarea portului COM utilizând software-ul C++ în vederea realizării conexiunii dintre aplicația care rulează pe Raspberry Pi și portul serial specific al PC-ului pentru a citi și raporta datele colectate,
- configurarea plăcii de dezvoltare Arduino ESP 32 cu software-ul open-source Arduino Integrated Development Environment (IDE) și bibliotecile sale suplimentare.

Mai mult decât atât, este necesară configurarea avansată a regiștrilor Windows și gestionarea politicii de grup pentru a avea drepturi suficiente în vederea executării recunoașterii faciale și identificării persoanelor în funcție de caracteristicile lor fizice. Pe lângă acestea, a fost dezvoltată o interfață grafică web securizată în PHP și Apache, pentru gestionarea bazei de date a utilizatorilor, care poate fi accesată online folosind un link asociat unei adrese IP statice, doar pe bază de user și parolă stabilite de către administratorul aplicației. Interfața web oferă o serie de facilități referitoare la introducerea parametrilor de funcționare a aplicației, de înregistrare a utilizatorilor în sistem, dar și de gestionare a acestora, lista utilizatorilor autorizați fiind direct corelată cu baza de date a sistemului de operare și implicit cu drepturile de acces alocate acestora.

2.2.3 Funcționarea mecanismului de autentificare

Funcționarea acestui mecanism are la bază două etape principale. Prima etapă constă în crearea bazei de date cu conturile utilizatorilor și pozele acestora care sunt centralizate pe dispozitivul extern, în timp ce a doua etapă include procesele de identificare, autentificare și autorizare a utilizatorilor în sistemul informatic. A doua etapă implică scanarea facială a utilizatorilor folosind un senzor adecvat inclus în placa de dezvoltare Arduino ESP 32, extragerea caracteristicilor distinctive, producerea de vectori de caracteristici ca șabloane biometrice și stocarea lor într-o bază de date. Decizia de acceptare sau respingere depinde de o comparație între imaginile utilizatorilor stocate în baza de date și vectorul de caracteristici rezultat în urma proceselor de identificare, autentificare și autorizare.

Unul dintre principalele avantaje ale acestui mecanism este reprezentat de faptul că baza de date facială a utilizatorilor este centralizată, stocată și criptată extern pe dispozitivul Raspberry Pi prin care se asigură astfel posibilitatea gestionării bazei de date de la distanță prin consolă bazată pe o interfață web de către un administrator sau de către persoane autorizate. Pentru a spori nivelul de securitate al bazei de date, accesul la consola web este protejat cu o parolă stabilită de personalul autorizat pentru a executa gestionarea bazei de date. Diferența majoră între schema de autentificare propusă în cadrul acestei teze de doctorat și celelalte lucrări de specialitate [33], [68], [69], [70], [71], [72], [73], [74] constă în nivelul de implementare și acuratețea recunoașterei utilizatorilor autorizați.

Mecanismul nostru de autentificare este dezvoltat la nivel hardware, care este considerat superior implementării software în termeni de securitate și testat pe fețe reale ale utilizatorilor, în comparație cu celelalte metode dezvoltate și testate pe seturi predefinite de date faciale disponibile online. Analizând timpul de criptare rezultat în urma aplicării diferiților algoritmi de criptare homomorfă, se poate constata că acest mecanism asigură printre cei mai buni timpi de criptare dintre schemele de recunoaștere facială dezvoltate, realizând obiectivele operaționale stabilite în faza inițială. Ținând cont că acest mecanism de autentificare este conceput pentru sisteme închise și rețele care necesită un nivel ridicat de protecție a informațiilor, poate fi o alegere potrivită atât pentru distribuția client, cât și pentru server, dar și pentru celelalte tipologii de rețele, precum rețelele radio și de supraveghere.

2.3 Concluzii

Punctul comun al mecanismelor create îl constituie securizarea informațiilor biometrice prin utilizarea algoritmilor criptografici homomorfi, pentru a păstra confidențialitatea, integritatea și disponibilitatea datelor. Chiar dacă principiul de funcționare al celor două mecanisme de autentificare este asemănător, o diferență majoră poate fi constatată la nivelul bazei de date biometrice, în sensul că dacă în primul caz baza de date cu amprente biometrice se generează automat de către senzorul biometric în memoria acestuia, în cel de-al doilea caz, baza de date cu imagini faciale ale utilizatorilor este constituită de către administratorul de securitate al sistemului pe dispozitivul extern. De remarcat însă că în ambele cazuri, managementul bazei de date se realizează prin intermediul unei interfețe grafice cu acces restricționat prin user și parolă, la care poate avea acces doar personalul cu atribuții pe linie de administrare a sistemelor informatice.

CAPITOLUL III CONTRIBUȚII PRIVIND EVALUAREA ALGORITMILOR CRIPTOGRAFICI HOMOMORFI

3.1 Criptarea homomorfă

O serie de tehnici specifice, care includ sisteme biometrice anulabile, criptosisteme și criptare homomorfă au fost dezvoltate pentru protecția informațiilor biometrice stocate în baza de date împotriva diferitelor tipuri de atacuri conform specificațiilor din referința [76]. Algoritmii de criptare homomorfă reprezintă o opțiune promițătoare pentru protejarea informațiilor biometrice prin criptare, deoarece permit efectuarea diverselor operațiuni direct asupra datelor criptate, fără a decripta și fără a degrada acuratețea recunoașterii imaginilor și asigură, de asemenea, confidențialitatea în timp ce informațiile sunt transferate și prelucrate de către o platformă nesigură.

În cadrul prezentei teze de doctorat, am optat pentru implementarea algoritmilor de criptare homomorfă, deoarece această modalitate de criptare contribuie semnificativ la protejarea datelor biometrice, utilizate pentru identificarea și autentificarea unui utilizator, asigurând confidențialitatea informațiilor referitoare la utilizator în conformitate cu prevederile legislației privind protecția datelor, cum ar fi Regulamentul General de Protecție a Datelor al Uniunii Europene, care oferă linii directoare stricte pentru manipularea și diseminarea datelor cu caracter personal [77].

3.1.1 Taxonomia metodelor de criptare homomorfă

Criptarea homomorfă este o construcție criptografică specială, o structură de nișă a criptografiei moderne care se fundamentează pe conceptul de homorfism și permite efectuarea de către o terță parte (de exemplu, cloud, furnizor de servicii, IoT) a anumitor operațiuni, menținând în același timp caracteristicile funcției și formatul datelor criptate. În funcție de tipul și numărul de operațiuni care se pot executa asupra lor, schemele de criptare homomorfă se clasifică în următoarele tipuri: criptare parțial homomorfă (PHE), criptare oarecum homomorfă (SHE) sau criptare complet homomorfă (FHE).

Spre deosebire de algoritmul criptografic Paillier, care este fundamentat pe o schemă parțial homomorfă, bazată pe operația de adunare, algoritmii de criptare complet homomorfă BFV, BGV și CKKS sunt structurați pe teoria învățării cu erori - Ring Learning with Errors (RLWE) compusă din inele polinomiale, care permit executarea mai multor operații aditive și multiplicative asupra datelor criptate fără a modifica conținutul textului cifrat rezultat, în care nivelul de zgomot se extinde simultan cu numărul de operații efectuate, așa cum este specificat în referința [81]. Pentru managementul zgomotului și optimizarea schemelor de criptare pot fi implementate câteva proceduri specifice precum bootstrapping, reliniarizare și comutare de modul pentru a minimiza nivelul de zgomot și a-l menține sub o anumită limită favorabilă executării unei decriptări eficiente și în timp util. O schemă de criptare complet homomorfă este caracterizată de următoarele patru operațiuni: Generarea cheilor, Criptare, Decriptare și Evaluare. Ceea ce particularizează aceste tehnici homomorfe

față de tehnicile clasice de criptare este operațiunea de Evaluare, care are ca input texte cifrate și generează un text cifrat evaluat corespunzător unui text simplu funcțional.

Deși diferențele și asemănările semnificative dintre algoritmii Paillier, BFV, BGV și CKKS au fost evidențiate la nivel teoretic în literatura de specialitate, în special la nivelul textelor cifrate, în cadrul cercetării de față ne-am propus să prezentăm o abordare alternativă în ceea ce privește testarea schemelor de criptare homomorfă la nivelul implementării asupra imaginilor biometrice, cu scopul de a obține un mecanism robust, eficient și rapid de autentificare.

3.2 Definirea parametrilor statistici utilizați în evaluarea cantitativă și calitativă a algoritmilor de criptare homomorfă

În cadrul acestui subcapitol sunt prezentate rezultatele experimentelor și analiza comparativă a algoritmilor criptografici homomorfi Paillier, BFV, BGV și CKKS asupra imaginilor biometrice. Testarea și implementarea au fost realizate în limbajul de programare Python, versiunea 3.10, pe 64 de biți, iar pentru mediul de experimentare a fost utilizat un sistem informatic Intel core i5, 2,4 GHz, 8 GB RAM și 500 GB SSD cu sistemul de operare Windows 11 Pro. Mai multe biblioteci open source pentru procesarea imaginilor au fost utilizate în Python, cum ar fi Numpy, OpenCV, Matplotlib, Scipy și Pillow, pentru a rula algoritmii de criptare și operațiunile specifice asupra datelor biometrice extrase.

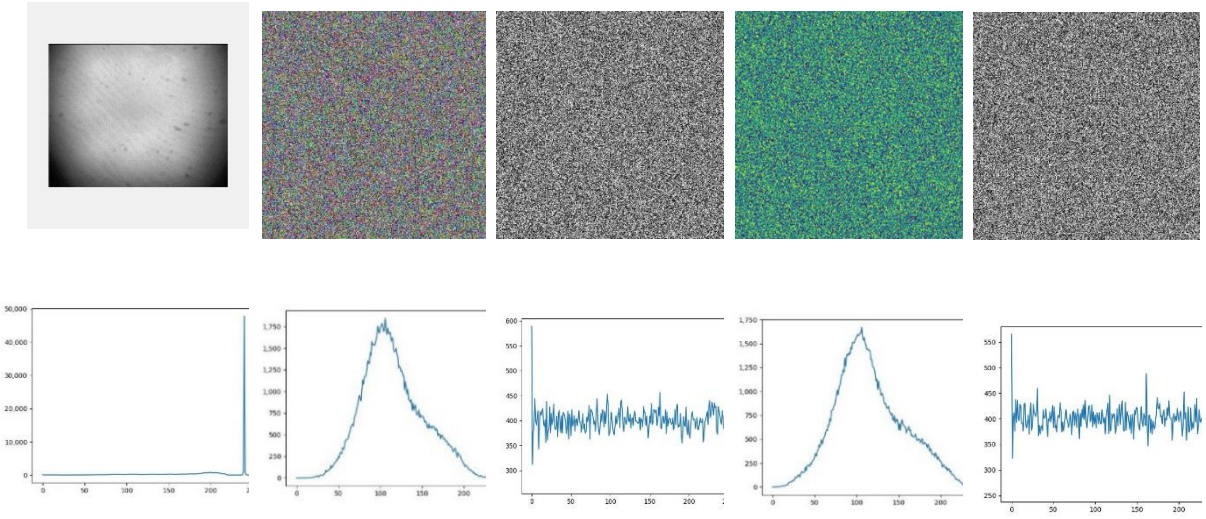
Dacă în cazul primului mecanism de autentificare, s-au utilizat pentru testare amprente extrase de la senzorul biometric cu dimensiunea fixă de 258x202 pixeli și rezoluția de 450 dpi, în cazul celui de-al doilea mecanism, respectiv cel bazat pe autentificarea facială s-a pus accent pe maleabilitate și având în vedere că structura imaginilor este mai complexă s-au utilizat diferite dimensiuni de imagine (256x256, 512x512, 1024x1024, 2048x2048 pixeli) pentru a identifica varianta optimă, în ceea ce privește performanța, dar și eficiența algoritmilor de criptare.

Parametrii statistici utilizați pentru identificarea celui mai potrivit algoritm pentru mecanismele de autentificare sunt aplicați pe imagini biometrice, aparținând diferiților utilizatori autorizați în sistem și cuprind analiza histogramei, analiza entropiei, eroarea pătratică medie (MSE), raportul maxim de semnal-zgomot (PSNR), măsura indicelui de similaritate structurală (SSIM), rata de modificare a numărului de pixeli (NPCR), intensitatea medie unificată de schimbare (UACI) și timpul mediu de criptare.

3.3 Evaluarea algoritmilor de criptare homomorfă asupra amprentelor biometrice

Luând în considerare primul parametru, prin realizarea unei analize comparative între histograma imaginii biometrice originale și imaginile biometrice aferente criptate prezentate în graficele din figura 3.1, se poate observa o diferență semnificativă între acestea, necesară și oportună pentru a evita orice suspiciune și pentru a putea rezista la gama diversificată de atacuri cibernetice.

Histogramele imaginilor criptate sunt complet diferite de histograma imaginii originale, astfel încât vectorii de atac nu vor putea obține imaginea originală prin intermediul histogramei imaginii criptate. Un algoritm perfect sigur trebuie să producă o imagine criptată cu histograme uniforme și complet diferite în comparație cu imaginea originală.



(a) (b) (c) (d) (e)

Fig. 3.1 Reprezentarea grafică a histogramelor (a) Imaginea biometrică originală (b) Imaginea criptată cu algoritmul Paillier (c) Imaginea criptată cu algoritmul BFV (d) Imaginea criptată cu algoritmul BGV (e) Imaginea criptată cu algoritmul CKKS

Dacă în cazul histogramelor obținute prin utilizarea algoritmilor de criptare Paillier și BGV se poate vedea că histogramele sunt caracterizate în integralitate prin forme unimodale, declinate central comparativ cu histograma imaginii originale, care prezintă o declinare la dreapta, ceea ce indică o distribuție diferită a intensității pixelilor din structura imaginilor, în cazul algoritmilor BFV și CKKS situația este complet diferită. Histogramele aferente acestor algoritmi sunt multimodale, caracterizate printr-o distribuție relativ egală și centralizată a pixelilor luminoși atât în zonele întunecate, în tonurile medii, cât și în zonele luminoase.

Plecând de la premisa că valoarea optimă a entropiei este 8, ceea ce indică gradul de dezordine cel mai mare ce poate fi obținut la nivel de pixel, rezultatele obținute reliefează că algoritmii criptografici BFV și CKKS au valorile cele mai apropiate de ținta maximă și reprezintă opțiunea cea mai benefică de implementare în analiza acestui parametru, asigurând un nivel de securitate îmbunătățit comparativ cu ceilalți algoritmi supuși evaluării. Drept urmare, din experimentele numerice, prezentate în figura 3.2, putem observa că valoarea șablonului criptat este mult mai mare și se apropie de valoarea ideală comparativ cu valoarea șablonului biometric brut. De asemenea, valorile obținute pentru algoritmii criptografici homomorfi BFV și CKKS dovedesc că aceștia pot fi considerați siguri pentru implementare împotriva diferitelor metode de distrugere a criptării, asigurând robustețe și adaptabilitate, caracteristici esențiale și necesare pentru protejarea informațiilor biometrice furnizate de mecanismele de autentificare hibride propuse în cadrul cercetării de față.

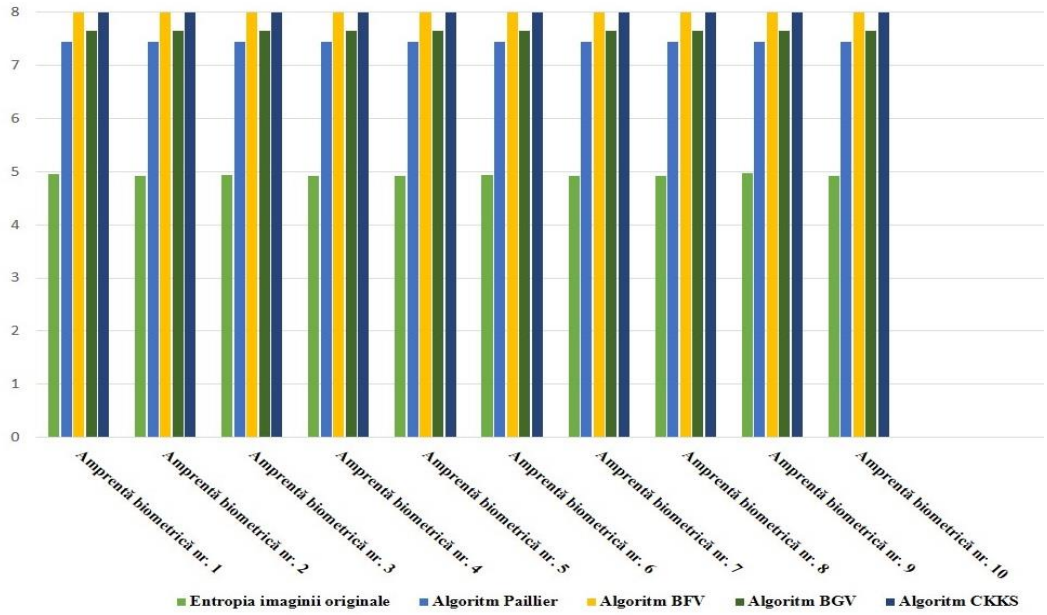


Fig. 3.2 Reprezentarea grafică a rezultatelor entropiei amprentelor biometrice

Din rezultatele experimentale obținute pentru următorii parametri evaluați, valorile mai ridicate ale parametrului MSE rezultate pentru imaginile biometrice criptate folosind algoritmii BFV și CKKS ce ating o medie de 0.158, indică cât de bine se păstrează calitatea imaginii și se minimizează distorsiunile, păstrând în același timp o eficiență ridicată de criptare comparativ cu celelalte scheme de criptare analizate. Pe de altă parte, la interpretarea valorilor PSNR, se poate observa că algoritmii criptografici homomorfi selectați pentru evaluare au scoruri similare cu diferențe relativ mici care converg în jurul valorii 27.9. Valorile mici obținute indică un nivel de zgomot ridicat și, în consecință, o diferență semnificativă identificată între imaginea biometrică originală și versiunea sa criptată și sugerează eficiența și acuratețea implementării algoritmilor selectați în securizarea șabloanelor biometrice. Mai mult decât atât, majoritatea valorilor SSIM calculate sunt apropiate de valoarea +1. Cu toate acestea, deși diferențele par a fi relativ mici, se poate remarca superioritatea algoritmului de criptare homomorfă BFV și faptul că prin intermediul acestui algoritm se poate obține o imagine cu un nivel de similaritate echivalent cu originalul prin procesul de decriptare.

Diferența mică dintre valorile parametrilor calculați denotă precizia ridicată, acuratețea și stabilitatea senzorului biometric utilizat pentru proiectarea mecanismului de autentificare, fapt prezentat în descrierea tehnică a dispozitivului și demonstrat din punct de vedere practic în prezenta cercetare.

Un alt parametru care scoate în evidență diferențe substanțiale în legătură cu nivelul de difuzie și confuzie la nivelul imaginilor biometrice criptate analizate este UACI. Luând în considerare valorile obținute pentru parametrul UACI, rezultatele cele mai bune sunt obținute pentru algoritmii de criptare BFV și CKKS, care au valori statistice relativ apropiate, caracterizate prin uniformitate deoarece sunt concentrate în jurul valorii 33.3, deși imaginile analizate provin de la utilizatori diferiți și implicit au caracteristici diferite. La polul opus se află parametrul NPCR care este definit prin valori cu un grad ridicat de similitudine, întrucât toți algoritmii de criptare se apropie de procentul maximal de 100%.

Cu toate acestea, se diferențiază și de această dată rezultatele mai ridicate ale algoritmilor BFV și CKKS, prin care se evidențiază o sensibilitate mai ridicată a acestora la micile modificări ale șablonului inițial. Superioritatea algoritmilor BFV și CKKS în procesul de criptare față de imaginile biometrice, sugerează faptul că sunt o alegere mai potrivită pentru integrarea în structura mecanismului de autentificare hibrid propus deoarece dovedesc sustenabilitate, adaptabilitate și robustețe în ceea ce privește asigurarea unui grad mai ridicat de eficiență în procesul de criptare a datelor utilizatorilor.

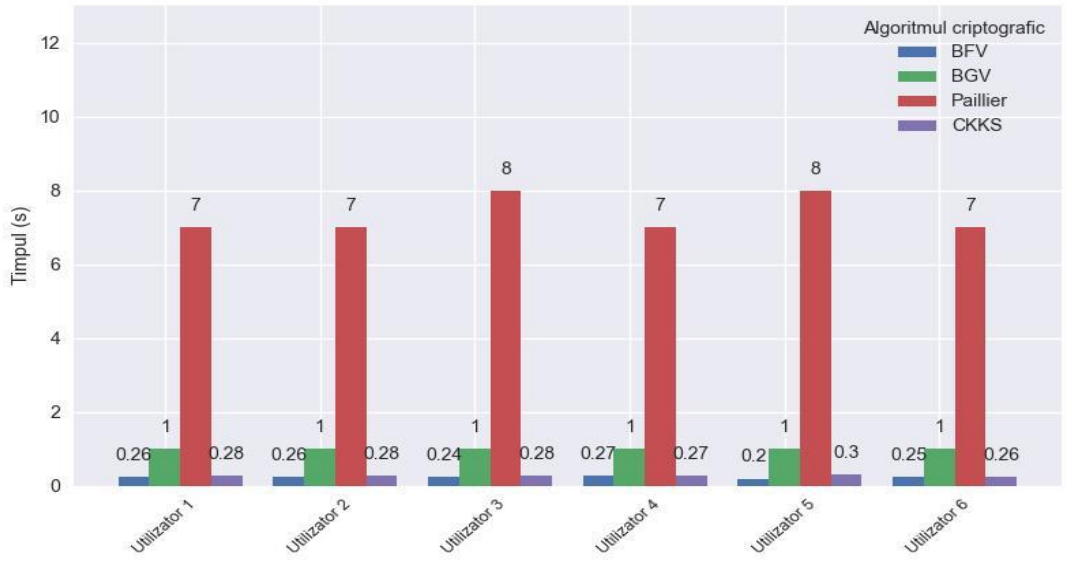


Fig. 3.3 Analiza factorului de timp în contextul criptării amprentelor cu algoritmii criptografici homomorfi Paillier, BFV, BGV și CKKS

În final, ultimul parametru analizat, probabil unul dintre cele mai relevante elemente în analiza performanței algoritmilor criptografici, este reprezentat de timpul de execuție, care ar trebui să genereze valori minime pentru efectuarea unei autentificări și criptări biometrice eficiente în vederea obținerii celor mai bune rezultate și dezvoltarea unui mecanism de autentificare de încredere. Dacă în cazul mecanismului de autentificare facial evaluarea factorului de timp s-a realizat asupra imaginilor biometrice având setate dimensiuni diferite, în cazul prezentului mecanism am utilizat exclusiv imaginile originale cu dimensiunea fixă generate de senzorul biometric, ținând cont și de complexitatea mai redusă a structurii imaginilor, dar și de faptul că acestea sunt monocrone. Analizând graficul prezentat în figura 3.3, pe axa factorului de timp, se poate observa o distincție majoră între algoritmii de criptare homomorfă, algoritmul BFV fiind superior algoritmilor Paillier, BGV și CKKS în ceea ce privește timpul de criptare aferent imaginilor biometrice analizate, provenite de la diferiți utilizatori autorizați în sistem.

Un lucru este cert, că cele mai mici valori pentru timpul de criptare sunt obținute prin intermediul algoritmului BFV care consumă în medie 0.2s pentru criptarea imaginii biometrice cu dimensiunea de 258x202 pixeli și rezoluția de 450 dpi pe care o folosim pentru experimentare. Nu este de neglijat valoarea obținută prin aplicarea algoritmului CKKS, care are o medie de 0.28s, ceea ce face din acest algoritm o variantă secundă de implementare. Spre deosebire de algoritmii precedenți, valorile rezultate prin aplicarea algoritmului BGV au o medie de criptare de 1s, ceea ce reprezintă o variantă acceptabilă, dar ținând cont de ecuația eficacitate – promptitudine

pentru a îmbunătăți performanțele de calcul ale sistemului și nivelul de securitate, această variantă nu se încadrează în cerințele operaționale și poate fi luată în considerare doar ca variantă de rezervă.

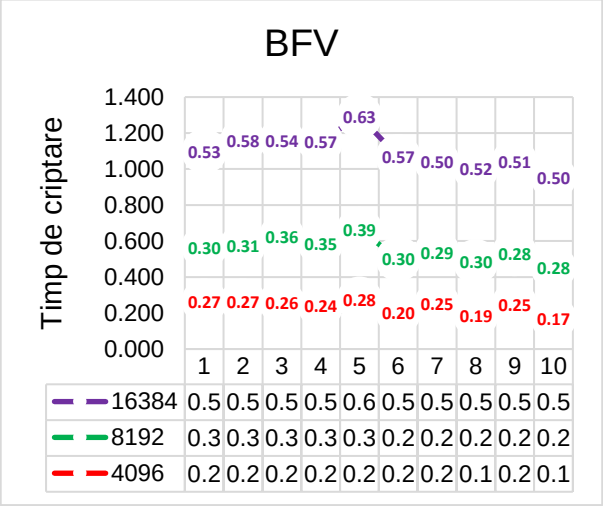


Fig. 3.4 Analiza relației dintre gradul modulului polinomial și timpul de criptare în cazul algoritmului BFV

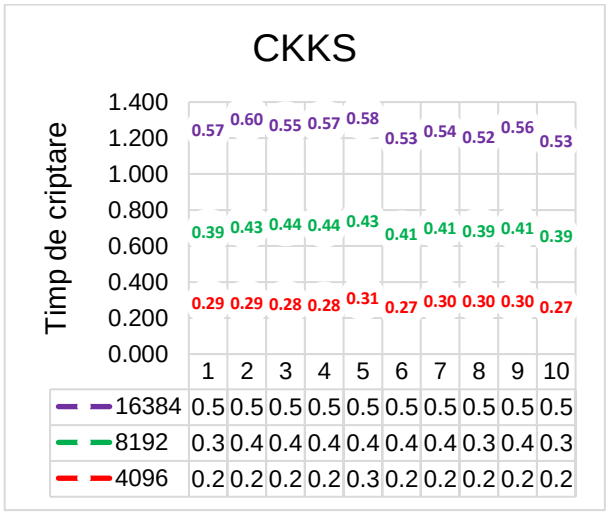


Fig. 3.5 Analiza relației dintre gradul modulului polinomial și timpul de criptare în cazul algoritmului CKKS

Având în vedere că evaluarea parametrilor anteriori a demonstrat superioritatea și eficacitatea algoritmilor criptografici BFV și CKKS în ceea ce privește criptarea imaginilor biometrice, în continuare pentru a realiza o departajare clară, am efectuat o analiză a influenței gradului modulului polinomial asupra timpului de criptare. Conform datelor din figurile 3.4 și 3.5, se poate observa clar relația de directă proporționalitate între valoarea gradului modulului polinomial și timpul de criptare și se poate constata că rezultatele algoritmului BFV sunt mult mai bune comparativ cu algoritmul CKKS. Dacă în cazul BFV timpul cel mai bun de criptare aferent gradului modulului polinomial 4096 atinge valoarea aproximativă de 0.2s, în cazul algoritmului CKKS acesta se încadrează în 0.28s, o diferență mică, dar care validează încă o dată superioritatea algoritmului BFV.

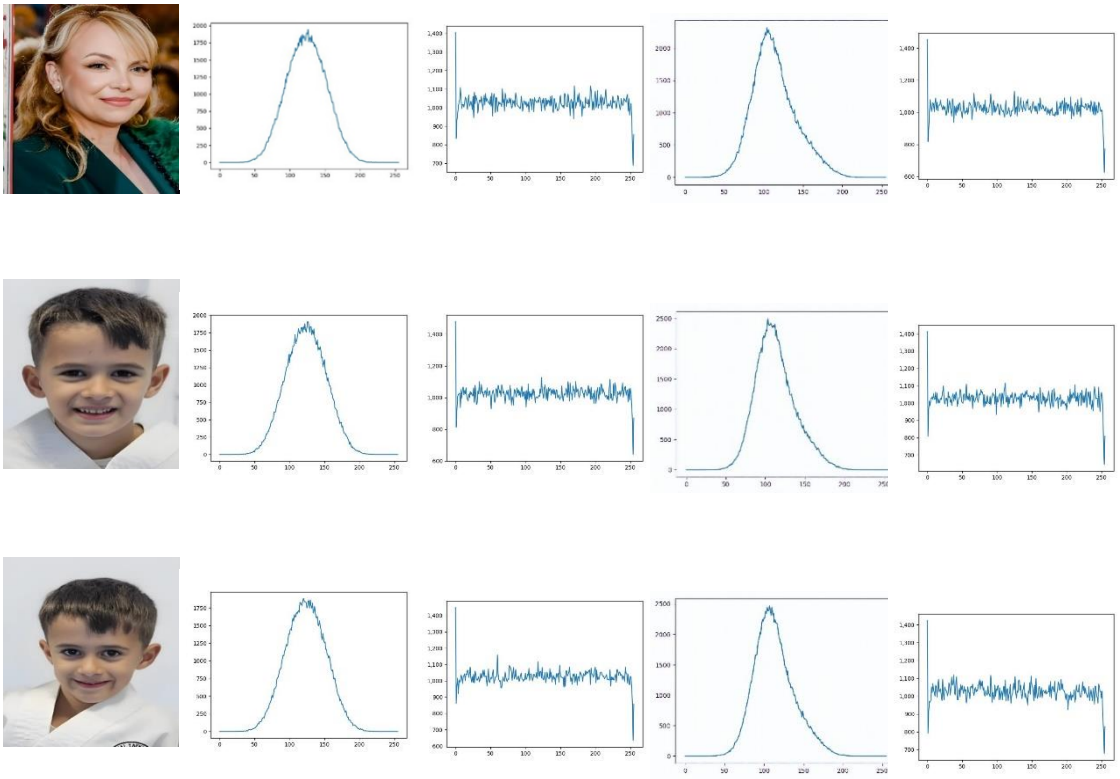
Sintetizând rezultatele obținute pentru parametrii analizați, se poate evidenția faptul că algoritmul BFV este preponderent majoritar în cazurile prezentate, necesită mai puțin timp de calcul comparativ cu ceilalți algoritmi criptografici homomorfi, de unde reiese că această schemă de criptare este mai eficientă, mai convenabilă și oferă fiabilitate atunci când este valorificată în procesul de criptare.

3.4 Evaluarea algoritmilor de criptare homomorfă asupra imaginilor faciale ale utilizatorilor

Comparativ cu mecanismul de autentificare precedent, în care baza de date este preluată automat de la senzorul biometric, în acest caz este atributul persoanei responsabile de implementarea și managementul măsurilor de securitate în sistemul informatic, să creeze baza de date cu utilizatorii autorizați și să asigneze drepturile de

acces în sistem, diferențiat conform prevederilor principiului „necesitatea de a cunoaște”.

Analizând histogramele afișate în figura 3.6, generate pentru imaginile biometrice criptate cu algoritmii de criptare Paillier, BFV, BGV și CKKS, în ceea ce privește efectele vizuale, se pot observa diferențe semnificative privind diseminarea intensității pixelilor între acestea. În timp ce imaginile biometrice criptate cu algoritmii Paillier și BGV sunt caracterizate prin distribuție unimodală, având valorile, precum și forma imaginii, situate central în jurul unor valori de referință, histogramele imaginilor criptate cu algoritmii BFV și CKKS sunt distincte și se diferențiază printr-o distribuție multimodală a pixelilor, centralizată de-a lungul întregului interval, care cuprinde atât zonele întunecate, cât și în zonele luminoase. Similar cu situația precedentă, histogramele rezultate prin aplicarea algoritmilor BFV și CKKS sunt echilibrate, complet diferite de histogramele imaginilor originale, ceea ce reprezintă un avantaj semnificativ comparativ cu ceilalți algoritmi.



a) b) c) d)

Fig. 3.6 Utilizator 1, 2, 3 – Reprezentarea grafică a histogramelor (a) Imaginea criptată cu algoritmul Paillier (b) Imaginea criptată cu algoritmul BFV, (c) Imaginea criptată cu algoritmul BGV, (d) Imaginea criptată cu algoritmul CKKS

Pentru a rezolva o sarcină dificilă și pentru a face acest studiu mai complet, am recrutat o pereche de gemeni masculi identici pentru rezultatele experimentale cu scopul de a verifica capabilitatea dispozitivului proiectat de a distinge caracteristici fizice aproape identice și de a verifica acuratețea procesului de autentificare. Această ipoteză de recunoaștere și autentificare efectivă pe gemeni este necesară pentru a verifica rata

de eroare de acceptare în sistem, deoarece posibilitatea apariției erorilor este maximă din cauza inexactităților generate de extragerea, potrivirea sau verificarea caracteristicilor. Figura 3.6 prezintă histogramele de la o pereche de gemeni masculi identici. În timp ce histogramele imaginilor criptate cu algoritmul Paillier și BGV prezintă forme și valori aproape identice, histogramele generate pe imaginile criptate cu algoritmii BFV și CKKS deși sunt caracterizate de unele modele de similaritate, prezintă o serie de diferențe vizibile cu ochiul liber ceea ce indică faptul că aceștia oferă un nivel mai redus de similitudine și implicit un nivel îmbunătățit de securitate, fiind imposibil de descifrat imaginea originală prin intermediul histogramei sale pentru vectorii de atac.

Continuând cu analiza algoritmilor criptografici, după cum se poate observa în figura 3.7, valorile entropiei aferente imaginilor biometrice criptate înregistrează valori distincte pentru fiecare algoritm în parte, singurii algoritmi care se apropie de valoarea maximă 8 fiind algoritmii BFV și CKKS care au o valoare medie de 7.99, ceea ce indică faptul că aceaste scheme propuse sunt mult mai eficiente comparativ cu algoritmii Paillier și BGV, prezintă un nivel de securitate ridicat și pot rezista atacurilor de entropie.

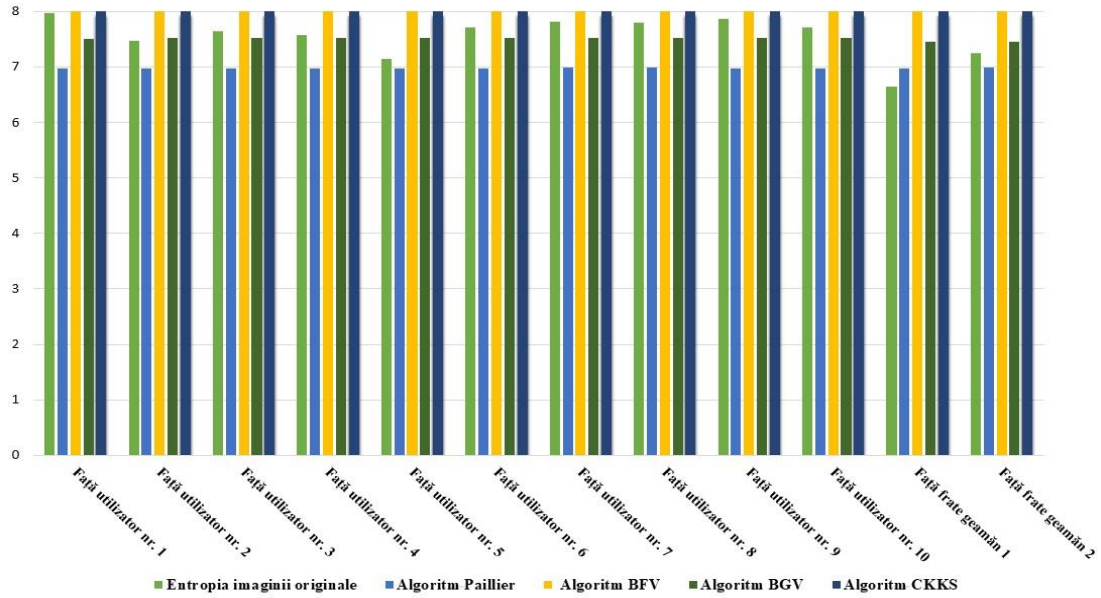


Fig. 3.7 Reprezentarea grafică a rezultatelor entropiei fețelor utilizatorilor autorizați

Valorile MSE și PSNR calculate cu algoritmii de criptare homomorfă propuși sunt foarte strânse și nu există diferențe remarcabile în rezultatele obținute, pentru parametrul MSE înregistrându-se o valoare medie de 0.06, iar pentru PSNR 27.8. Valorile mai mici ale PSNR indică faptul că există un nivel ridicat de zgomot și o corelație slabă între cele două tipuri de imagini, evidențiind performanța de criptare a algoritmilor criptografici. Cu toate acestea, valorile similare mai mici pentru MSE și PSNR obținute la aplicarea algoritmilor Paillier, BFV, BGV și CKKS asupra imaginilor biometrice indică faptul că prin implementarea acestor scheme se poate atinge un nivel adecvat de securitate și eficiență.

Un comportament similar cu parametrii calculați anterior, poate fi observat pentru valorile indicelui SSIM, astfel încât valorile calculate pentru algoritmii criptografici sunt ușor diferite pentru fiecare imagine în parte. Rezultatele obținute pentru indicele SSIM se apropie de 1, ceea ce indică un nivel ridicat de similitudine pe baza

caracteristicilor structurale implicate în prezenta cercetare și o relație strânsă între imaginile analizate și, de asemenea, subliniază eficiența tuturor algoritmilor de criptare homomorfă analizați. Cu toate acestea, valorile cele mai mari se înregistrează pentru algoritmul BFV, de unde reiese superioritatea acestuia în cazul parametrului analizat.

Mergând mai departe în cadrul analizei, scorurile pentru parametrul UACI indică diferențe elocvente și rezultate mult mai bune pentru algoritmii de criptare BFV și CKKS, valorile acestora fiind relativ asemănătoare și concentrate în jurul valorii aproximative 33.3, comparativ cu algoritmii Paillier și BGV, care înregistrează valori mult mai scăzute cu o valoare medie de 13.5, respectiv 11.9. În contrast cu UACI, parametrul NPCR este definit prin valori asemănătoare, prezentând o diferență nesemnificativă, astfel încât toți algoritmii se apropie de procentul maxim. Cu toate acestea, este clar că o îmbunătățire semnificativă a rezultatelor pentru atacul diferenţial şi analiza sensibilităţii imaginii criptate se înregistrează prin aplicarea algoritmului Paillier, de această dată acesta dovedindu-și superioritatea în procesul de criptare față de imaginile biometrice.

Analiza efectuată la nivelul factorului temporal redată grafic în figurile 3.8, 3.9, 3.10 și 3.11 denotă o distincție majoră între algoritmii de criptare homomorfă, algoritmul BFV fiind net superior algoritmilor Paillier, BGV și CKKS în ceea ce privește timpul de criptare aferent imaginilor biometrice evaluate cu dimensiuni diferite provenite de la diverși utilizatori autorizați în sistem. Având în vedere graficele prezentate mai jos, se poate sublinia un fapt cert, că cele mai mici valori pentru timpul de criptare sunt obținute prin intermediul algoritmului BFV care consumă până la 0.31s pentru criptarea unei imagini biometrice cu dimensiunea de 512x512 pixeli pe care o folosim pentru experimentare.

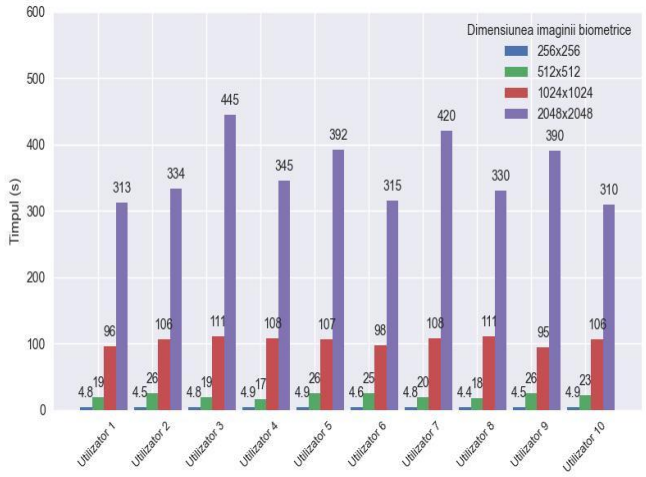


Fig. 3.8 Analiza factorului de timp utilizând algoritmul Paillier

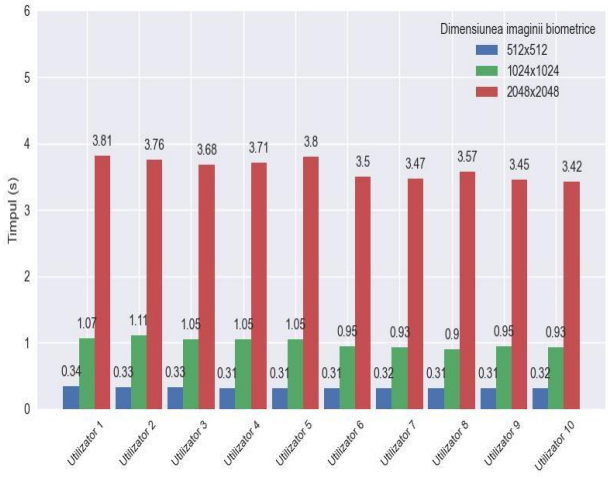


Fig. 3.9 Analiza factorului de timp utilizând algoritmul BFV

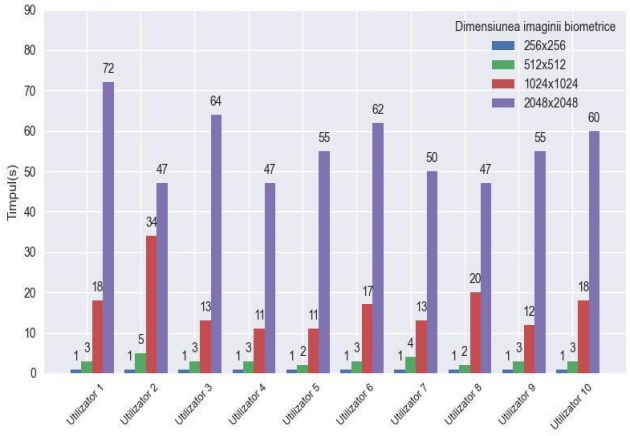


Fig. 3.10 Analiza factorului de timp utilizând algoritmul BGV

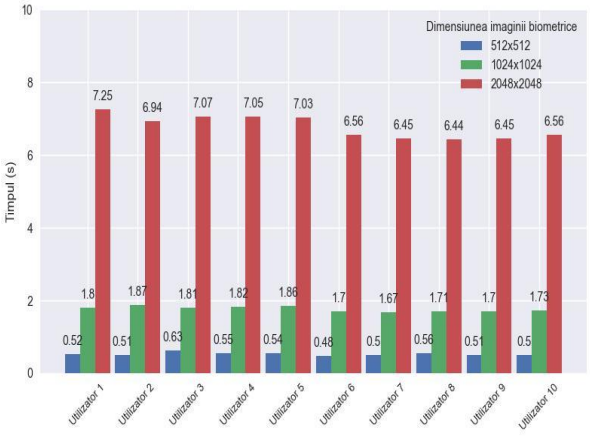


Fig. 3.11 Analiza factorului de timp utilizând algoritmul CKKS

Pentru a realiza o departajare clară între valorile celor doi algoritmi criptografici homomorfi BFV și CKKS, am realizat o analiză a influenței gradului modulului polinomial asupra timpului de criptare a imaginilor biometrice faciale, cu scopul de a identifica cea mai adecvată variantă de implementare. Acest criteriu de departajare justifică, și în acest caz, relația de proporționalitate între variația gradului modulului polinomial, care ia pe rând valorile 4096, 8192 și 16384 și timpul de criptare, respectiv dimensiunea imaginii criptate simulată pentru valorile 512x512, 1024x1024, 2048x2048 pixeli. Astfel că, dacă în cazul algoritmului BFV timpul cel mai bun de criptare aferent gradului modulului polinomial 4096 și a dimensiunii imaginii de 512x512 pixeli atinge valoarea aproximativă de 0.31s, în cazul algoritmului CKKS acesta se încadrează în 0.5s, acesta fiind un criteriu de departajare elocvent care confirmă încă o dată superioritatea algoritmului BFV. Un aspect interesant, constă în faptul că pe măsură ce dimensiunea imaginii crește, diferența între timpul de criptare prin aplicarea celor doi algoritmi devine din ce în ce mai evidentă, chiar ajungându-se la dublarea acesteia, așa cum se poate observa în cazul dimensiunii unei imagini de 2048x2048 pixeli care pentru algoritmul BFV atinge o medie de 3.5s, în timp ce pentru algoritmul CKKS se dublează, înregistrând valoarea de 7s.

În ansamblu, rezultatele obținute în urma acestei analize experimentale subliniază că cea mai adecvată opțiune pentru asigurarea unui nivel mai ridicat de securitate în procesul de autentificare, constă în aplicarea algoritmului de criptare complet homomorf BFV deoarece aduce un avantaj major în ceea ce privește îmbunătățirea performanței și eficienței capabilităților mecanismului propus, care este conceput și proiectat pentru sisteme IT cu cerințe de securitate ridicată.

3.5 Rezultate finale și discuții

Rezultatele obținute în urma acestei analize experimentale subliniază că varianta optimă pentru asigurarea unui nivel mai ridicat de securitate în procesul de autentificare, atât în cazul mecanismului bazat pe autentificarea pe amprentă și RFID, cât și în cazul mecanismului care utilizează autentificarea facială, constă în aplicarea algoritmului de criptare complet homomorf BFV deoarece aduce un avantaj major în

ceea ce privește optimizarea performanțelor și eficienței capabilităților sistemelor propuse. Nu este de neglijat și performanța algoritmului criptografic parțial homomorf CKKS în contextul tuturor parametrilor analizați, care poate constitui o soluție secundară de implementare, a cărui valori sunt apropiate de algoritmul precedent, singurul dezavantaj fiind reprezentat de timpul de criptare care este mai mare și reprezintă un element definitoriu în alegerea soluției potrivite. De departe, varianta utilizării algoritmilor homomorfi Paillier și BGV asupra datelor biometrice nu reprezintă o opțiune favorabilă în contextul cerințelor operaționale actuale, datorită variabilității și lipsei de predictibilitate. Drept urmare, acești algoritmi homomorfi în ciuda diverselor avantaje și dezavantaje oferă un cadru sigur pentru aplicarea practică, comparativ cu algoritmii clasici și asigură protecția datelor cu caracter personal în conformitate cu regulile de securitate ale reglementărilor europene GDPR, care trasează linii directoare clare în ceea ce privește protecția și diseminarea informațiilor personale.

CAPITOLUL IV ANALIZA VULNERABILITĂȚILOR ȘI POTENȚIALELOR ATACURI ASUPRA MECANISMELOR HIBRIDE DE AUTENTIFICARE PROPUSE

4.1 Vulnerabilități și potențiale atacuri asupra componentei biometrice bazate pe amprentă

Analizând primul factor de autentificare bazat pe amprentele biometrice, putem evidenția avantajul major al acestuia față de metodele clasice de autentificare care constă în faptul că acestea sunt mult mai dificil de copiat, partajat și distribuit. Amprentele digitale nu pot fi pierdute sau furate, iar recunoașterea bazată pe amprentă este strâns corelată cu prezența fizică a persoanei în procesul de autentificare, astfel încât este singura tehnologie de securitate care oferă o legătură atât de puternică între o persoană fizică și o acțiune întreprinsă de aceasta. Cu toate acestea, deși datele biometrice în general sunt personale, dar nu private sau secrete s-a demonstrat că acestea prezintă o serie de vulnerabilități și sunt susceptibile unor atacuri emergente, iar din acest considerent este necesară suplimentarea performanței de recunoaștere a acestor sisteme prin combinarea cu alți factori de autentificare. Pornind de la această premisă, vulnerabilitățile senzorului biometric de amprentă, utilizat în cadrul cercetării de față, pot fi regăsite în cadrul tuturor etapelor procesului de autentificare, pornind de la procesul de înrolare, verificare, autorizare, și inclusiv la stocarea informațiilor în baza de date și canalul de transmitere a datelor.

O vulnerabilitate semnificativă valorificată de atacatorii care vor să pătrundă în sistem, prezentă încă din faza incipientă a procesului de autentificarea o constituie amprenta falsă sau artificială, realizată din silicon, latex sau alte materiale maleabile, care simulează caracteristicile unei amprente originale, prin care se urmărește inducerea în eroare a senzorului astfel încât acesta să fie incapabil să facă distincția între trăsăturile false și cele autentice ale amprentei utilizatorului. De asemenea, extragerea amprentei dintr-o fotografie de înaltă rezoluție sau preluarea unei amprente lăsate de utilizator pe suprafețele fizice cu care acesta a intrat în contact sunt modalități probabile, care pot periclita siguranța unui sistem biometric bazat pe recunoașterea amprentei. Alte elemente care pot denatura acuratețea autentificării biometrice pot fi reprezentate de cantitatea de umiditate, transpirație sau murdărie de pe degete care afectează capacitatea senzorului de a capta datele cu succes, schimbările nenaturale ale câtorva caracteristici biometrice, precum tăieturi, cicatrici, eczeme, răni, boli de piele. În funcție de vulnerabilitățile prezentate anterior, putem realiza o clasificare a principalelor tipuri de atacuri informatice asupra componentei biometrice a sistemului de autentificare proiectat, corelate cu componentele din lanțul de autentificare, conform datelor prezentate în figura 4.1.

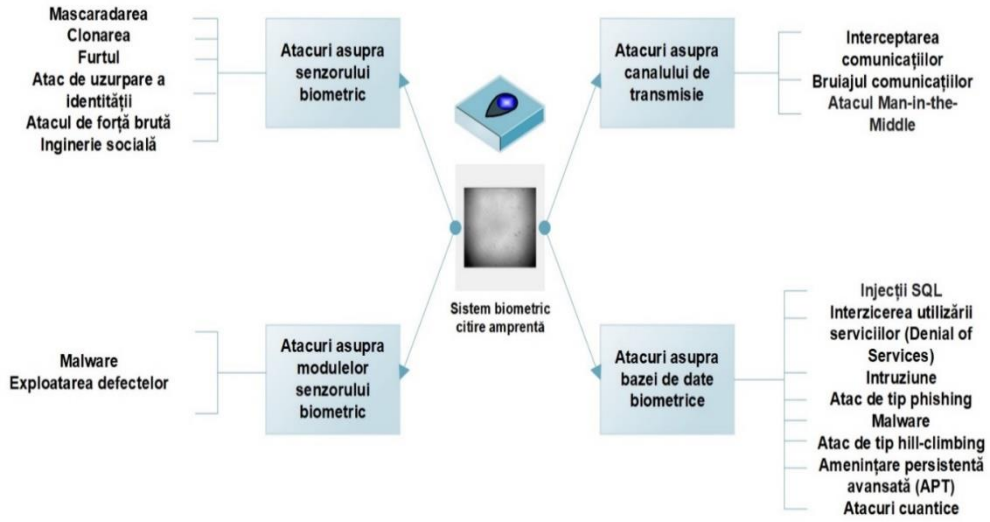


Fig. 4.1 Atacuri emergente asupra componentei biometrice bazată pe amprentă

În concluzie, vulnerabilitățile variază ca severitate și pot fi protejate prin adoptarea diverselor contramăsuri, cum ar fi supravegherea procesului de înrolare a utilizatorilor, implementarea unor senzori de detectare a vitalității, anonimizarea șabloanelor, stocarea și transportul criptografic și suplimentarea măsurilor de securizare a rețelei. Contramăsurile se diferențiază în ceea ce privește maturitatea, costul și rentabilitatea, iar adoptarea acestora izvorăște din necesitatea protejării și asigurării unei reziliențe ridicate a infrastructurilor de rețea în contextul noilor amenințări cibernetice.

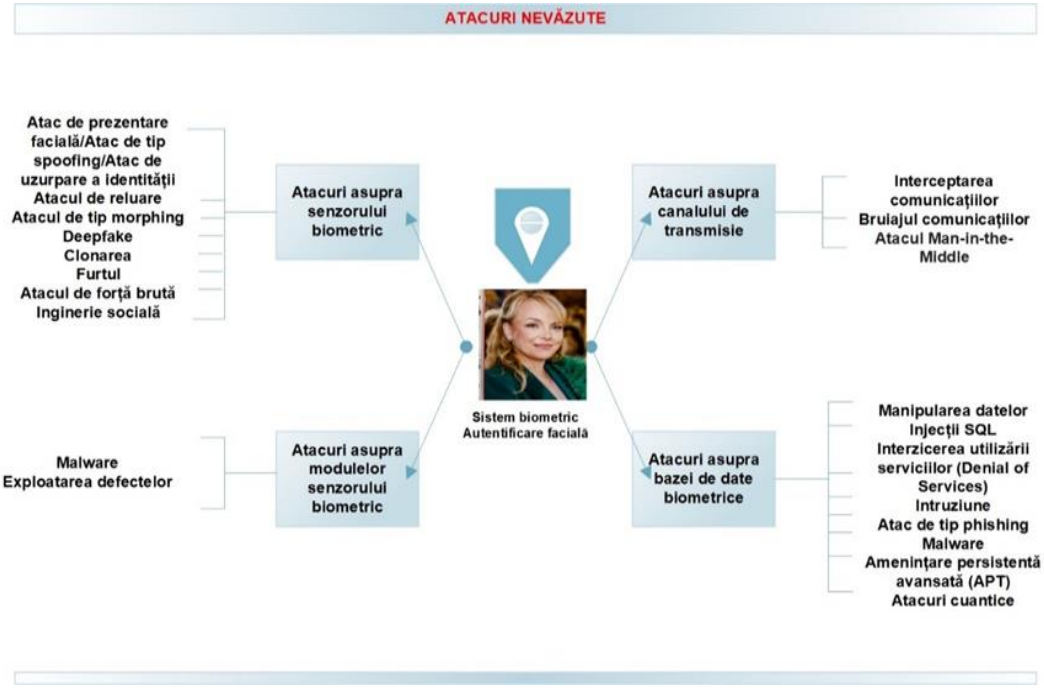
4.2 Vulnerabilități și potențiale atacuri asupra componentei RFID

Analizând cel de-al doilea factor de autentificare din structura primului mecanism proiectat, și anume componenta de autentificare bazată pe tehnologia RFID care utilizează carduri ID, se poate evidenția faptul că acesta prezintă o serie de potențiale vulnerabilități la adresa elementelor componente, precum cititorul de card, canalul de transmisie radio, antena, baza de date serială și etichetele RFID aferente, determinate de distanța de citire dintre cititor și cardul RFID, puterea de emisie și sensibilitatea de emisie a cititorului, numărul unic de identificare al cardului de acces, software-ul de management al cardurilor ID, elemente care îl pot vulnerabiliza în fața diverselor atacuri pasive sau active.

Cu toate acestea, implementarea tehnologiei RFID pasive prezintă o serie de avantaje, care constau în faptul că aceasta are capabilități de calcul limitate, putere de consum redusă, iar informațiile utilizate pentru identificarea și autentificarea unui utilizator sunt minime, reprezentate în general de un număr de serie unic, prin care nu este afectată confidențialitatea informațiilor personale ale utilizatorului, astfel respectându-se prevederile legislației GDPR privind protecția datelor.

4.3 Vulnerabilități și potențiale atacuri asupra componentei biometrice faciale

Sistemele de recunoaștere facială prezintă o serie de vulnerabilități fiind ținte preferate pentru atacatori, deoarece instrumentele de atac sunt relativ ușor de creat și greu de detectat. Popularitatea rețelelor sociale determină informațiile faciale de înaltă calitate purtătoare de identitate să fie ușor disponibile, iar informațiile biometrice să fie partajate cu ușurință. Punctele vulnerabile ale mecanismului facial, utilizat în cadrul cercetării de față, pot fi regăsite atât la nivelul elementelor componente din structura acestuia, cât și la nivelul etapelor procesului de autentificare, pornind de la procesul de înrolare, verificare, autorizare și inclusiv la stocarea informațiilor în baza de date și canalul de transmitere a datelor, în cazul în care această metodă de autentificare este implementată în arhitectura unei rețele informatice, cum se poate observa în reprezentarea grafică din figura 4.2.



. **Fig. 4.2** Atacuri emergente asupra componentei biometrice faciale

Chiar dacă sistemele de autentificare biometrică reprezintă una din cele mai sigure și robuste modalități de autentificare, acuratețea acestora poate fi influențată în mod negativ de o serie de factori precum poziția, iluminarea, expresia feței, procesul de îmbătrânire și eterogenitate, care pot afecta capacitatea senzorului de a capta datele cu succes, existând riscul de respingere a unui utilizator înrolat în sistem. Un atacator poate escalada toate vulnerabilitățile prezentate și poate efectua diverse atacuri pentru a periclita securitatea sistemului de autentificare, cum ar fi accesarea informațiilor private, obținerea de permisiuni de autorizare ridicate, manipularea sistemelor de control acces sau accesarea unor facilități neautorizate. [103]

4.4 Metode de contracarare a vulnerabilităților și atacurilor existenta asupra mecanismelor de autentificare proiectate

Caracteristici definitorii precum robustețea, reziliența și securitatea sistemelor biometrice în fața atacurilor iminente poate fi îmbunătățită prin implementarea diverselor tehnici defensive, care pot fi defalcate pe structura hardware, structura software sau concatenarea mai multor modele. Tehnicile structurate pe mai multe modele îmbunătățesc robustețea, reziliența și securitatea sistemului, dar pot crește costurile logistice și pot avea un impact nefavorabil asupra gradului de utilizare. Dintr-o perspectivă generală, aceste tehnici defensive pot fi valorificate la îmbunătățirea performanței sistemelor de autentificare, printre cele mai eficiente tehnici numărându-se implementarea caracteristicilor bazate pe mișcare, implementarea caracteristicilor bazate pe calitatea imaginii, autentificarea adaptivă, valorificarea algoritmilor de învățare profundă și învățare automată, precum și dezvoltarea sistemelor multimodale.

Pe lângă aceste metode inovatoare propuse spre implementare pentru contracararea vulnerabilităților și atacurilor existente la adresa mecanismelor de autentificare dezvoltate, soluția noastră se axează pe adoptarea unui algoritm criptografic homomorf pentru criptarea informațiilor biometrice care sunt stocate și procesate pe un dispozitiv extern independent, proiectat ca un sistem închis cu acces restricționat, o soluție tehnică hardware care are la bază arhitectura system-on-device.

4.5 Direcții viitoare de îmbunătățire a mecanismelor de autentificare contra atacurilor emergente

Direcțiile viitoare de dezvoltare vor fi concentrate asupra îmbunătățirii capabilităților mecanismelor actuale de autentificare prin implementarea unor factori inovatori precum meta-learning, învățarea prin consolidare, învățarea federată, inteligența artificială explicabilă (XAI), precum și utilizarea tehnologiei blockchain.

4.6 Concluzii

Concluzionând, îmbunătățirea capabilităților de securizare a unui sistem informatic se poate obține prin diverse tehnici de hibridizare a protocoalelor, metodelor și mecanismelor de autentificare existente sau în curs de dezvoltare, dar și prin identificarea sistematică a potențialelor vulnerabilități și printr-un management cât mai eficient al acestora, care poate fi cheia apărării împotriva atacurilor iminente. Dacă esența acestui capitol s-a concretizat pe identificarea posibilelor limitări și constrângeri funcționale determinate de factori externi și interni la adresa elementelor structurale din componența mecanismelor de autentificare propuse, în capitolul următor ne-am propus să evidențiem posibilitatea interconectării și integrării lor la diferite sisteme de comunicații și informatică și aplicabilitatea în trei scenarii reale de implementare cu scopul de a oferi o perspectivă cât mai amplă asupra gradului de flexibilitate și adaptabilitate al acestora.

CAPITOLUL V PROPUNERI DE SCENARII REALE DE IMPLEMENTARE

În contextul în care evenimentele globale recente continuă să remodeleze peisajul amenințărilor cibernetice, care se extind pe toate palierele și mediile de transmisie a informațiilor, dezvoltarea și implementarea mecanismelor sigure de autentificare în sistemele informatice reprezintă o cerință stringentă de securitate și o condiție sine qua non. Obiectivul principal al acestora este de a restricționa accesul utilizatorilor la resursele informaționale și de a contracara eventualele breșe de securitate, care pot avea efecte negative de la nivel tactic, operațional, până la nivel strategic. Plecând de la aceste premise, în cele ce urmează vor fi exemplificate trei scenarii reale diferite, în care pot fi integrate mecanismele de autentificare create cu scopul de a sprijini procesul decizional în suplimentarea măsurilor de securitate.

5.1 Securizarea accesului în sistemele informatice din rețelele radio militare HF de date

Un prim scenariu de implementare a mecanismelor de autentificare propuse, cuprinde integrarea acestor instrumente de protecție a accesului într-o rețea radio militară, monocanal de transmitere date în gama HF pentru a diminua potențialele riscuri și amenințări la adresa comunicațiilor radio conform figurii 5.1.

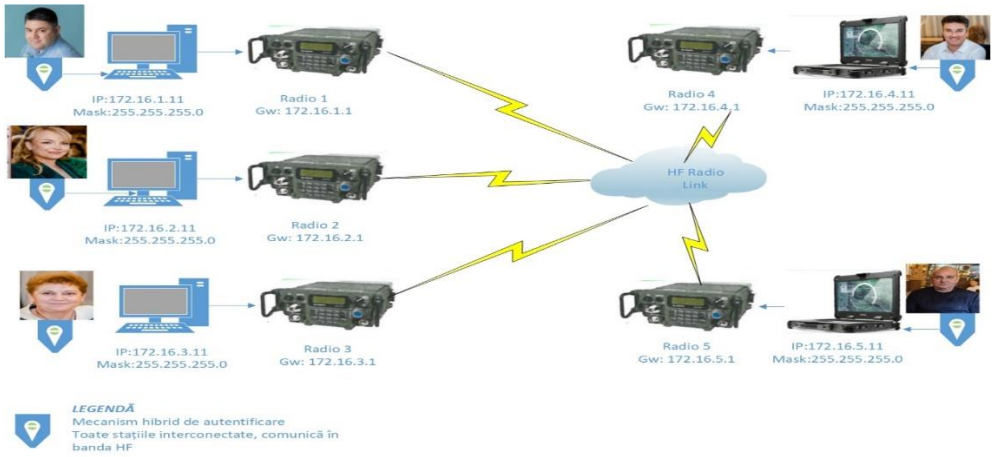


Fig. 5.1 Securizarea accesului în cadrul unei rețelele radio HF de date

5.2 Securizarea accesului în sistemele de supraveghere video

Un alt scenariu de implementare a mecanismelor de autentificare proiectate, reprezentat grafic în figura 5.2, constă în încorporarea acestora în arhitectura unui sistem de supraveghere video modern prin care se realizează monitorizarea în timp real, sistem care reprezintă un element cheie în diminuarea riscurilor existente la nivel

organizațional și optimizarea nivelului de securitate și siguranță și asigurarea protecției generale a bunurilor, serviciilor și persoanelor.

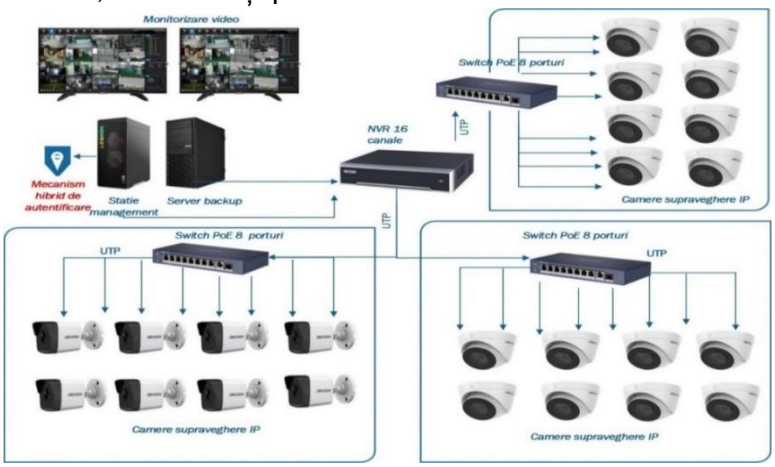


Fig. 5.2 Securizarea accesului în cadrul unui sistem de supraveghere video

5.3 Securizarea accesului în rețelele de supraveghere cu drone

Rețelele de supraveghere cu drone prezintă o serie de caracteristici unice care le particularizează față de rețelele prezentate anterior, și anume, mobilitatea foarte ridicată, dar și capabilitățile relativ limitate în ceea ce privește puterea de calcul, capacitatea de stocare, puterea de consum și autonomia. Dacă în cazurile anterioare se preta implementarea ambelor mecanisme de autentificare proiectate, în situația de față este recomandată utilizarea mecanismului bazat pe amprentă, RFID și algoritmul criptografic homomorf, datorită formei mai compacte, aceasta fiind mai ușor de integrat în structura unei drone. Descrierea arhitecturii unei rețele de drone cu acces securizat este prezentată în figura 5.3.

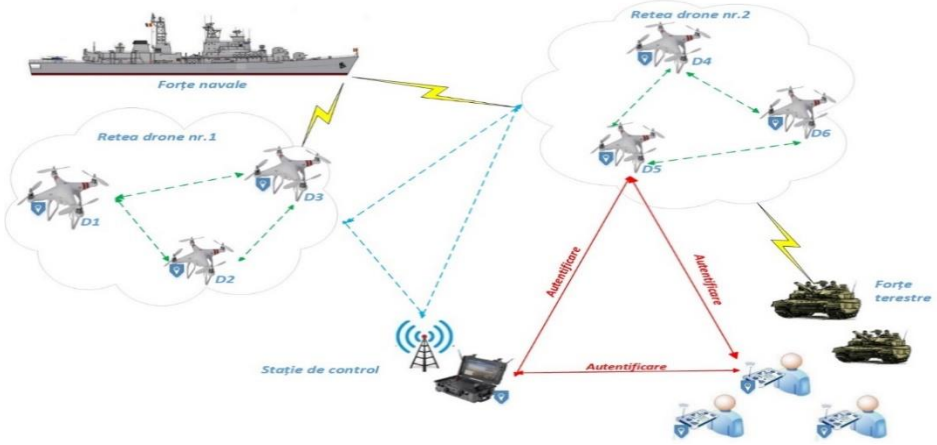


Fig. 5.3 Securizarea accesului în cadrul unei rețelele de supraveghere cu drone

Scenariile prezentate ilustrează versatilitatea și adaptabilitatea mecanismelor de autentificare propuse deoarece pot fi valorificate într-un spectru larg de activități și domenii, care necesită un nivel înalt de protecție a informațiilor și cerințe stricte pentru păstrarea confidențialității utilizatorilor, reprezentând o alternativă viabilă față de protocoalele, metodele și mecanismele de autentificare clasice.

CONCLUZII FINALE, CONTRIBUŢII, DIRECŢII DE CERCETARE VIITOARE, DISEMINAREA REZULTATELOR

Concluzii finale

Dezvoltarea de noi tehnologii în biometrie și criptografie aduce în prim plan noi oportunități pentru îmbunătățirea securității informațiilor într-un număr cât mai mare de aplicații. Abordarea actuală din cadrul acestei cercetări constă în integrarea și valorificarea potențialului acestor două tehnici puternice, componente importante ale sistemelor moderne de control al accesului, cu scopul de a îmbunătăți nivelul de securizare a procesului de autentificare în cadrul sistemelor informatice și, de asemenea, de a proteja și supraveghea de la distanță resursele informaționale utilizate în autentificarea utilizatorilor pentru a contracara eventualele intruziuni în sistem.

Prin urmare, în cadrul tezei de doctorat, am îndeplinit toate cele șase obiective principale care au fost stabilite inițial, prin proiectarea, implementarea și dezvoltarea a două mecanisme de autentificare fiabile, destinate pentru utilizare atât în sisteme independente, cât și în arhitectura diferitelor topologii de rețea, având la bază componenta biometrică combinată cu componenta criptografică, sisteme relativ complexe și compacte bazate pe module Raspberry Pi și Arduino. Aceste module oferă mai multe avantaje, inclusiv costuri rezonabile de achiziție, interfață ușor de utilizat, flexibilitate și versatilitate pentru dezvoltarea de soluții personalizate. Mai mult decât atât, mecanismele de autentificare pot fi personalizate cu ușurință pentru diferite nevoi organizaționale și adaptate în diferite scenarii în care se vehiculează informații sensibile care trebuie să respecte reguli de securitate stricte defalcate pe mai multe niveluri de clasificare și cerințe puternice de autentificare.

Prin urmare, printre principalele beneficii ale acestor mecanisme de autentificare dezvoltate pe baza fuziunii complementare a celor doi factori de autentificare, se numără:

- Îmbunătățirea nivelului de securitate împotriva accesului neautorizat.
- Simplificarea procesului de autentificare și reducerea sarcinii de autentificare a utilizatorului.
- Furnizarea unei metode eficiente de identificare bazată pe caracteristicile fiziologice ale utilizatorului.
- Generarea unei soluții tehnice accesibile în ecuația cost versus performanță versus securitate.

Concluzionând, noutatea cercetării constă în proiectarea mecanismelor hibride de autentificare care realizează autentificarea utilizatorilor în timp real și oferă o interfață web ușor de utilizat pentru administrarea de la distanță.

Contribuții

Întregul demers științific aduce în prim plan contribuții semnificative, prin îndeplinirea în integralitate a obiectivelor stabilite inițial, concretizate prin rezultate dezvoltate la nivel conceptual prin realizarea unei analize a stadiului actual a metodelor de autentificare contempoane utilizate în sistemele și rețelele informaționale, accentul fiind pus asupra metodelor biometrice, fiind evidențiate, de asemenea, vulnerabilitățile, potențialele atacuri și metode de contracarare a acestora. Rezultatele dezvoltate la nivel practic-aplicativ se materializează prin proiectarea unor mecanisme de autentificare scalabile și ușor de integrat în sistemele informaționale actuale pentru a îmbunătăți securitatea generală și acuratețea autentificării utilizatorilor, dar și pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor personale.

Proiectarea, dezvoltarea și implementarea din punct de vedere hardware și software a unui mecanism hibrid de autentificare, realizat prin complementaritatea a trei factori de autentificare amprenta biometrică, componenta RFID și componenta criptografică, având la bază microcontrolerul Arduino, dar și a unui mecanism de autentificare versatil și non-invaziv, care combină componenta biometrică facială și componenta criptografică, având în componență microcontrolerul Arduino și microprocesorul Raspberry Pi, reprezintă contribuții substanțiale în ceea ce privește protejarea datelor de acces ale utilizatorilor și realizarea unui management eficient a datelor biometrice.

Pentru a demonstra eficacitatea algoritmilor criptografici homomorfi selectați pentru experimentare în vederea criptării datelor biometrice, a fost efectuată o analiză comparativă în software-ul Python, versiunea 3.10, între algoritmul de criptare parțial homomorf Paillier, respectiv algoritmii de criptare complet homomorfă BFV, BGV, CKKS utilizând o serie de parametri statistici, cu scopul de a identifica și evalua cel mai optim algoritm care să îmbunătățească capabilitățile de securizare a mecanismelor proiectate. Modalitatea de selecție a acestor algoritmi criptografici, aplicabilitatea acestora asupra informațiilor biometrice, prelucrarea informațiilor obținute, precum și interpretarea rezultatelor acestor experimente constituie o contribuție relevantă. Toate datele utilizate în analiza algoritmilor criptografici homomorfi reprezintă contribuție proprie și au fost obținute în timp real de la utilizatorii sistemelor informatice.

Rezultatele experimentale indică algoritmul de criptare complet homomorf BFV, ca fiind cea mai bună soluție pentru un proces rapid și sigur de criptare, valorile ideale recomandate fiind pentru o imagine biometrică cu dimensiunea 512x512 pixeli și selectarea valorii 4096 pentru gradul modulului polinomial, dar bineînteles că pe măsură ce gradul de complexitate al imaginii și al parametrilor utilizați crește cu atât nivelul de protecție al imaginii criptate se îmbunătățește semnificativ.

Evaluarea principalelor vulnerabilități și a potențialelor atacuri emergente, la nivel conceptual asupra mecanismelor hibride de autentificare și propunerea unor măsuri adiacente inovatoare de protecție pentru reducerea efectelor negative și maximizarea securității în mediul digital actual, reprezintă, de asemenea, o contribuție considerabilă.

Nu în ultimul rând, demonstrarea aplicabilității soluțiilor tehnice se realizează prin propunerea unor scenarii reale și originale de implementare în arhitectura diferitelor

topologii de rețea, valabile pentru diverse entități organizaționale, prin care se poate evidenția versatilitatea și adaptabilitatea acestora la mediile operaționale în care sunt vehiculate informații în format electronic ce implică cerințe sporite de securitate.

Direcții viitoare de cercetare

Direcțiile viitoare de dezvoltare vor fi concentrate asupra îmbunătățirii capabilităților mecanismului actual de autentificare facială prin implementarea unui factor adițional de autentificare, bazat pe caracteristicile irisului, cu scopul de a dezvolta un sistem multimodal, complex și non-intruziv, prin care să se diminueze substanțial posibilitatea compromiterii informațiilor personale în contextul abstractizării din ce în ce mai mult a vectorilor de atac.

O altă direcție viitoare de cercetare necesară și obligatorie constă în optimizarea algoritmilor criptografici homomorfi utilizați pentru criptarea șabloanelor biometrice în vederea minimizării nivelului de zgomot și menținerii acestuia sub o anumită limită favorabilă pentru a realiza o criptare eficientă și pentru a îmbunătăți timpul de execuție care este considerat un criteriu esențial în orice domeniu ce are în prim plan securitatea sistemelor informaționale.

Nu în ultimul rând, o altă direcție de dezvoltare vizează îmbunătățirea algoritmilor de autentificare dezvoltați la nivel software prin integrarea unor algoritmi mai avansați care utilizează tehnici de inteligență artificială, algoritmi de tip învățare profundă, învățare automată sau învățare federată, dar și algoritmi informatici care pot cuantifica emoțiile, starea de spirit, precum și posibilele intenții ale utilizatorului. Astfel, prin integrarea acestor tehnici procesul de autentificare poate dobândi un nivel de eficiență, performanță, fiabilitate, dar mai ales calitate a imaginii net superioare atât în rețelele fizice, cât și cele virtuale.

Diseminarea rezultatelor

Rezultatele activității de cercetare științifică, care fundamentează prezenta teză de doctorat au fost diseminate și validate atât în reviste științifice naționale și internaționale, cât și prin lucrări susținute în cadrul unor conferințe naționale și internaționale, astfel:

a) Articole științifice publicate în jurnale cotate ISI WoS:
   1. Crihan, G.; Dumitriu, L.; Crăciun, M.; 2024, Preliminary experiments of a real-world authentication mechanism based on facial recognition and fully homomorphic encryption, Applied Sciences, vol.14, no. 2, pp.718, **ISSN: 2076-3417**.
   2. Crihan, G.; Crăciun, M.; Dumitriu, L., 2023, A comparative assessment of homomorphic encryption algorithms applied to biometric information, Inventions, Special Issue Perspectives and Challenges in Doctoral Research - Selected Papers from the 11th Edition of the Scientific Conference of the Doctoral Schools of „Dunărea de Jos" University of Galati (SCDS-UDJG), vol.8, no. 4, pp.102, **ISSN: 2411-5134**.

b) Articole științifice publicate în jurnale BDI/B+:
    1. Crihan, G.; Crăciun, M.; Dumitriu, L., 2024, An efficient hybrid authentication mechanism based on biometric fingerprint recognition and homomorphic encryption, International Journal of Modeling and Optimization, vol.14, no. 2, pp.69-75, **ISSN: 2010-3697**, indexat INSPEC.

c) Articole științifice în volume de specialitate
    1. Crihan, G.; Crăciun, M.; Dumitriu, L., 2023, Hybrid methods of authentication in network security, The Annals of „Dunarea De Jos" University of Galati, Fascicle III Electrotechnics, Electronics, Automatic Control, Informatics, vol.41, no. 1, pp. 11-17, **ISSN: 2344-4738, ISSN-L: 1221-454X**.

d) Conferințe științifice
    1. Crihan, G.; Crăciun, M.; Dumitriu, L., *Hybrid methods of authentication in network security*, Conferința Școlilor Doctorale SCDS-UDJG, 09-10.06.2022, ediția 10, Galați, România.
    2. Crihan, G.; Crăciun, M.; Dumitriu, L., *A comparative assessment of homomorphic encryption algorithms applied to biometric information*, Conferința Școlilor Doctorale SCDS-UDJG, 08-09.06.2023, ediția 11, Galați, România.
    3. Crihan, G.; Crăciun, M.; Dumitriu, L., *An efficient hybrid authentication mechanism based on biometric fingerprint recognition and homomorphic encryption*, Conferința internațională SLS OPTIROB, 29.06-03.07.2023, ediția 18, Jupiter, Constanța, România.

e) Premii obținute
    1. Mențiune Conferința Școlilor Doctorale SCDS-UDJG, 08-09.06.2023, ediția 11, Galați, România pentru lucrarea *A comparative assessment of homomorphic encryption algorithms applied to biometric information*, Conferința Școlilor Doctorale SCDS-UDJG, 08-09.06.2023, ediția 11, Galați, România.
    2. Diplomă de excelență (Mențiune) - Gala CEREX UDJG 2023 pentru rezultatele în activitatea de cercetare în cadrul IOSUD-UDGJ în anul 2023.

BIBLIOGRAFIE

[1] Chang, C.C., *Privacy-preserving information hiding and its applications,* Teză de doctorat susținută la Univesitatea Warwick, Coventry, UK, 2019.

[2] *Review of CBP's major cybersecurity incident during a 2019 biometric pilot*, Department of Homeland Security, Washington DC, 2020, https://www.oig.dhs.gov/reports/2020/review-cbps-major-cybersecurity-incident-during-2019-biometric-pilot/oig-20-71-sep20.

[3] Boonkrong, S., *Authentication and access control: practical cryptography methods and tools*, Berkeley, CA, Apress, pp. 48-49, 2021, ISBN 978-1-4842-6569-7.

[4] Temoshok, D., *NIST SP 800-063-4 ipd: Digital identity guidelines online,* Gaithersburg, National Institute of Standards and Technology, MD, USA, 2022, doi: 10.6028/NIST.SP.800-63-4.ipd.

[5] Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., *Quality measures in biometric systems*, IEEE Security & Privacy, vol. 10, no. 6, pp. 52-62, 2022.

[6] Yang, J., *New trends and developments in biometrics*, InTech, Rijeka, Croatia, pp. 31, 2012, ISBN 978-953-51-0859-7.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L119/1, 2016.

[8] Rao, U.H., Nayak, U., *The InfoSec Handbook. An introduction to information security,* New York*,* Apress, pp.51-53, 2014, ISBN 978-1-4302-6383-8.

[9] Otta, S. P., Panda, S., Gupta, M., Hota, C., *A systematic survey of multi-factor authentication for cloud infrastructure*, Future Internet, vol. 15, no. 4, pp. 146, 2023, ISSN 1999-5903.

[10] Boonkrong, S., *Authentication and access control: practical cryptography methods and tools*, Berkeley, CA, Apress, pp. 49-69, 2021, ISBN 978-1-4842-6569-7.

[11] Nirmal, J. R., Kiran, R. B., Hemamalini, V., *Improvised multi-factor user authentication mechanism using defense in depth strategy with integration of passphrase and keystroke dynamics*, Materials Today: Proceedings, vol. 62, pp. 4837–4843, 2022, ISSN 2214-7853.

[12] Agrawal, V., Paliwal, R. K., Sharma, P., Shrivastava, A., *Web security using user authentication methodologies: CAPTCHA, OTP and User Behaviour Authentication*, SSRN Journal, pp. 1578-1589, 2019, ISSN 1556-5068.

[13] Vatra, N., *A PKI architecture using open source software for e-government services in Romania,* Indian Journal of Computer Science and Engineering (IJCSE), vol. 2, no. 4, pp. 532-538, 2011, ISSN 0976-5166.

[14] Kim, H.J., Lee, I.Y., *A study on a secure single sign-on for user authentication information privacy in distributed computing environment*, *I*nternational Journal of Communication Networks and Distributed Systems, vol. 19, no. 1, pp. 28-45, 2017, ISSN 1754-3916.

[15] Jain, A.K., Flynn, P., Ross, A.A*., Handbook of Biometrics,* New York, Springer, pp. 3-5, 2008, ISBN 978-0-387-71040-2.

[16] Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., Malli, M., *Cyber-physical systems security: Limitations, issues and future trends*, Microprocessors and Microsystems, vol. 77, pp. 103201, 2020, ISSN 0141-9331.

[17] Crihan, G., Craciun, M., Dumitriu, L., *Hybrid methods of authentication in network security*, The Annals of „Dunarea de Jos“ University of Galati, Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics, vol. 45, no. 1, pp. 7, 2023, ISSN 2344-4738, 1221-454X.

[18] Zhang, S., Du, X., Liu, X., *An efficient and provable multifactor mutual authentication protocol for Multigateway Wireless Sensor Networks*, Security and Communication Networks, vol. 2021, pp. 1–17, 2021, ISSN 1939-0122, 1939-0114.

[19] Khan, A. S., Javed, Y., Saqib, R.M., Ahmad, Z., Abdullah, J., Zen, K., Abbasi, I.A., Khan, N.A., *Lightweight multifactor authentication scheme for NextGen Cellular Networks*, IEEE Access, vol. 10, pp. 31273–31288, 2022, ISSN 2169-3536.

[20] Chiadighikaobi, I. R., Katuk, N., Osman, B., *DMUAS-IoT: A descentralised multi-factor user authentication scheme for IoT systems*, International Journal of Computing, pp. 424–434, 2022, ISSN 1727-6209, 2312-5381.

[21] Vijay, M., Indumathi, G., *A highly secure multi-factor authentication system using biometrics to enhance privacy in Internet of Things (IoT)*, International Research Journal of Multidisciplinary Technovation, vol.1, no. 6, pp. 26–34, 2019, ISSN 2582-1040

[22] Mostafa, A. M, Ezz, M., Elbashir, M., Alruily, M., Hamouda, E., Alsarhani, M., Said, W., *Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication*, Applied Sciences, vol. 13, no. 19, pp. 10871, 2023, ISSN 2076-3417.

[23] Song, J., Li, G., Xu, B., Ma, C., *A novel multiserver authentication protocol with multifactors for cloud service*, Security and Communication Networks, vol. 2018, pp. 1–13, 2018, ISSN 1939-0122, 1939-0114.

[24] Duan, Z., Mahmood, J., Yang, Y., Berwo, M.A., Yassin, A.K.A., Mumtaz Bhutta, M., Chaudhry, S.A., Fu, A., *TFPPASV: A three-factor privacy preserving authentication scheme for VANETs*, Security and Communication Networks, vol. 2022, pp.1–15, 2022, ISSN 1939-0122, 1939-0114.

[25] Kim, M., Oh, J., Son, S., Park, Y., Kim, J., Park, Y., *Secure and privacy-preserving authentication scheme using decentralized identifier in Metaverse environment*, Electronics, vol. 12, no. 19, pp. 4073, 2023, ISSN 2079-9292.

[26] Nasir Abdulhussien, I., Abdulridha Abduljaleel, S., *Fuzzy logic based authentication in cognitive radio networks*, International Journal of Electrical and Computer Engineering *(IJECE)*, vol. 12, no. 4, pp. 4327, 2022, ISSN 2088-8708, e-ISSN 2722-2578.

[27] Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R. A. Regenscheid, A. R., Burr, W. E., Richer, J.P., *Digital identity guidelines: authentication and lifecycle management*, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63b, 2017, doi: 10.6028/NIST.SP.800-63b.

[28] Rivera Sánchez, Y. K., Demurjian, S. A., Baihan, M. S., *A service-based RBAC & MAC approach incorporated into the FHIR standard*, Digital Communications and Networks, vol. 5, no. 4, pp. 214–225, 2019, Online ISSN 2352-8648, Print ISSN 2468-5925.

[29] Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., *A robust embedded biometric authentication system based on fingerprint and chaotic encryption*, Expert Systems with Applications, vol. 42, no. 21, pp. 8198–8211, 2015, Online ISSN 1873-6793, Print ISSN 0957-4174.

[30] Yang, W., Wang, S., Yu, K., Kang, J. J., Johnstone, M. N., *Secure fingerprint authentication with homomorphic encryption*, 2020 Digital Image Computing: Techniques and Applications (DICTA), Melbourne, Australia IEEE, 2020, pp. 1–6, ISBN 978-1-72819-108-9.

[31] Zulfiqar, M., Syed, F., Khan, M.J., Khurshid, K., *Deep face recognition for biometric authentication*, Proceedings of the 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, 2019, pp. 1–6, ISBN 978-1-72813-825-1.

[32] Ali, M.A.S., Meselhy Eltoukhy, M., Rajeena, F.P.P., Gaber, T., *Efficient thermal face recognition method using optimized curvelet features for biometric authentication,* PLoS ONE, vol. 18, no. 6, pp. e0287349, 2023, ISSN 1932-6203.

[33] Yang, Y., Zhang, Q., Gao, W., Fan, C., Shu, Q., Yun, H., *Design on face recognition system with privacy preservation based on homomorphic encryption*, Wireless Personal Communications, pp. 3737–3754, 2022, Online ISSN 1572-834X, Print ISSN 0929-6212.

[34] Morampudi, M.K., Prasad, M.V.N.K., Verma, M., Raju, U.S.N., *Secure and verifiable iris authentication system using fully homomorphic encryption*, Computers and Electrical Engineering, vol.89, pp. 106924, 2021, Online ISSN 1879-0755, Print ISSN 0045-7906.

[35] Khoury, F.E., *Iris biometric model for secured network access*, CRC Boca Raton, FL, USA, 2013, ISBN 978-1-4665-0214-7.

[36] Chowdhury, R., Ghosh, D., Agarwal, P., Kumar, S, *Ear based biometric authentication system*, World Journal of Engineering Research and Technology WJERT, vol. 2, no.5, pp. 224–233, 2016, ISSN 2454-695X.

[37] Annapurani, K., Sadiq, M.A.K., Malathy, C., *Ear authentication and template protection using bio-key*, Research Journal of Applied Sciences, Engineering and Technology, vol.8, no.12, pp.1450–1455, 2014, ISSN 2040-7459, 2040-7467.

[38] Madhusudhan, M.V., Udayarani, V., Hegde, C., *Finger vein recognition model for biometric authentication using intelligent deep learning*, International Journal of Image and Graphics, vol.23, no.03, pp. 5403–5408, 2020, Online ISSN 1793-6756, Print ISSN 0219-4678.

[39] Gupta, P., Srivastava, S., Gupta, P., A*n accurate infrared hand geometry and vein pattern based authentication system*, Knowledge-Based Systems, vol. 103, pp. 143–155, 2016, ISSN 0950-7051.

[40] Islam, M.S., *Heartbeat biometrics for remote authentication using sensor embedded computing devices*, International Journal of Distributed Sensor Networks, vol. 11, no. 6, pp. 549134, 2015, ISSN 1550-1477, 1550-1477.

[41] Jeswani, D., Govarthan, P.K., Selvaraj, A., Thomas, C.B., Thomas, J., Ronickom, J.F.A. *A feasibility study on using EEG for biometric trait authentication system*, Current Directions in Biomedical Engineering, vol. 9, no.1, pp. 690–693, 2023, ISSN 2364-5504.

[42] Sharma, S., Dubey, S.R., Singh, S.K., Saxena, R., Singh, R.K., *Identity verification using shape and geometry of human hands*, Expert Systems with Applications, vol. 42, no. 2, pp. 821–832, 2015, ISSN 0957-4174.

[43] Rashed, A., Santos, H., *Odour user interface for authentication: Possibility and acceptance: Case study*, Proceedings of the International Multi Conference of Engineers and Computer Scientists, Hong Kong, vol. I, 2010, Online ISSN 2078-0966, Print ISSN 2078-0958.

[44] Yevetskyi, V., Horniichuk, I., *Selection of handwritten signature dynamic indicators for user authentication,* Information Technology and Security, vol.8, no.1, pp. 19-30, 2020, ISSN 2411-1031.

[45] Isaac, E. R. H. P., Elias, S., Rajagopalan, S., Easwarakumar, K. S., *Template-based gait authentication through Bayesian thresholding*, IEEE/CAA Journal of Automatica Sinica, vol. 6, no. 1, pp. 209–219, 2019, ISSN 2329-9266.

[46] Meng, Z., Altaf, M. U. B., Juang, B.-H. (Fred), *Active voice authentication*, Digital Signal Processing, vol. 101, pp. 102672, 2020, Online ISSN 1095-4333, Print ISSN 1051-2004.

[47] Kang, Y., Kim, W., Lim, S., Kim, H., Seo, H., *Deep Detection: Privacy-enhanced deep voice detection and user authentication for preventing voice phishing,* Applied Sciences, vol. 12, no. 21, pp.11109, 2022, ISSN 2076-3417.

[48] Neacsu, T., Poncu, T., Ruseti, S., Dascalu, M., *DoubleStrokeNet: Bigram-Level keystroke authentication*, Electronics, vol. 12, no. 20, pp. 4309, 2023, ISSN 2079-9292.

[49] Velmurugan, S., Selvarajan, S., *A multimodal authentication for biometric recognition system using hybrid fusion techniques*, Cluster Computing, vol. 22, no. S6, pp. 13429-13436, 2019, ISSN 1386-7857.

[50] Elmir, Y., Al-Maadeed, S., Amira, A., Hassaine, A., *Multi-modal biometric authentication system using face and online signature fusion*, Proceedings of the Qatar Foundation Annual Research Forum, vol. 2012, no.1, Doha, Qatar, 2012.

[51] Abozaid, A., Haggag, A., Kasban, H., Eltokhy, M., *Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion*, Multimedia Tools Application, vol. 78, no. 12, pp. 16345–16361, 2019, ISSN 1380-7501.

[52] Sujatha, E., Chilambuchelvan, A., *Multimodal biometric authentication algorithm using iris, palm print, face and signature with encoded DWT*, Wireless Personal Communications, vol. 99, no.1, pp.23–34, 2018, ISSN 0929-6212.

[53] Singh, K.K., Barde, S., *A feasible adaptive fuzzy genetic technique for face, fingerprint, and palmprint based multimodal biometrics systems*, Journal of Current Science and Technology, vol. 14, no. 1, 2024, ISSN 2630-0656.

[54] Sharma, R., Mishra, N., Yadav, S. K., *Fingerprint recognition system and tehniques: a survey*, International Journal of Scientific & Engineering Research, vol. 4, no. 6, pp. 1670-1674, 2013, ISSN 2229-5518.

[55] Nath, D., Ray, S., Ghosh, S. K., *Fingerprint recognition system : design and analysis*, International Conference on Scientific Paradigm Shift In Information Technology & Management, SPSITM'11, 2011, https://www.academia.edu/436093/ Fingerprint_Recognition_System_ Design_and_Analysis.

[56] Menon, A., *Overview of face recognition methodologies: a literature review*, preprint, 2023. doi: 10.14293/PR2199.000346.v1.

[57] Waqar, A., Wenhong, T., Salah, U. D., Desire, I., Abdullah, A. K., *Classical and modern face recognition* approaches: a complete review, Multimedia Tools and Applications, vol. 80, pp. 4825–4880, 2021, ISSN 1573-7721.

[58] Adjabi, I., Ouahabi, A., Benzaoui, A., Taleb-Ahmed, A., *Past, present, and future of face recognition: a review*, Electronics, vol. 9, no. 8, pp. 1188, 2020, ISSN 2079-9292.

[59] Maltoni, D., Maio, D., Jain, A. K., Feng, J., *Handbook of fingerprint recognition*, Springer International Publishing, Cham, 2022, ISBN 978-3-030-83623-8.

[60] Crihan, G., Crăciun, M., Dumitriu, L., *An efficient hybrid authentication mechanism based on fingerprint recognition, RFID and homomorphic encryption*, International Journal of Modeling and Optimization, vol.14, no. 2, pp.69-75, 2024, ISSN 2010-3697.

[61] Jain, A.K., Flynn, P., Ross, A.A., *Handbook of Biometrics,* New York, Springer, 2008, ISBN 978-0-387-71040-2.

[62] Morampudi, M. K., Sandhya, M., Dileep, M., *Privacy-preserving and verifiable multi-instance iris remote authentication using public auditor*, Optik, vol. 274, pp. 170515, 2023, Online ISSN 1618-1336, Print ISSN 0030-4026.

[63] Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., Fierrez, J. *Multi-biometric template protection based on homomorphic encryption*, Pattern Recognition, vol. 67, pp. 149–163, 2017, Online ISSN 1873-5142, Print ISSN 0031-3203.

[64] Blanton, M., Gasti, P., *Secure and efficient protocols for iris and fingerprint identification*, Computer Security – ESORICS 2011, Berlin, Heidelberg, vol. 6879, pp. 190–209, 2011, ISBN 978-3-642-23821-5 978-3-642-23822-2.

[65] Kim, T., Oh, Y., Kim, H., *Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption,* Security and Communication Networks, vol. 2020, pp. 1–11, 2020, ISSN 1939-0114.

[66] Barni, M., Bianchi, T., Catalano, D., Di Raimondo, M., Labati, R.D., Failla, P., Fiore, D., Piuri, V., Piva, A., Scotti, F., *A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates*, Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, pp. 1–7, 2010, ISBN 978-1-4244-7581-0.

[67] Crihan, G., Dumitriu, L., Crăciun, M., *Preliminary experiments of a real-world authentication mechanism based on facial recognition and fully homomorphic encryption*, Applied Sciences, vol. 14, no. 2, pp. 718, 2024, ISSN 2076-3417.

[68] Huang, H., Wang, L., *Efficient privacy-preserving face verification scheme*, Journal of Information Security and Applications, vol. 63, pp. 103055, 2021, Online ISSN 2214-2134, Print ISSN 2214-2126.

[69] Boddeti, V. N., *Secure face matching using fully homomorphic encryption,* 2018, http://arxiv.org/abs/1805.00577.

[70] Drozdowski, P., Buchmann, N., Rathgeb, C., Margraf, M., Busch, C., *On the application of homomorphic encryption to face identification*, Proceedings of the 2019 International Conference of the Biometrics Special Interest Group (BIOSIG 2019) - Lecture notes in Informatics (LNI), Darmstadt, Germany, 2019, ISSN 1617-5468.

[71] Tamiya, H., Isshiki, T., Mori, K., Obana, S., Ohki, T., *Improved post-quantum-secure face template protection system based on packed homomorphic encryption*, 2021 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, pp. 1-5, 2021, ISBN 978-1-66542-693-0.

[72] Mfungo, D.E., Fu, X., *Fractal-based hybrid cryptosystem: Enhancing image encryption with RSA, homomorphic encryption, and chaotic maps*, Entropy, vol. 25, no. 11, pp. 1478, 2023, ISSN 1099-4300.

[73] Pradel, G., Mitchell, C., *Privacy-preserving biometric matching using homomorphic encryption*, 2021, http://arxiv.org/abs/2111.12372.

[74] Jindal, A.K., Shaik, I., Vasudha, V., Chalamala, S.R., Rajan, M., Lodha, S., *Secure and privacy preserving method for biometric template protection using fully homomorphic encryption*, Proceedings of the IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, ISBN 978-1-6654-0392-4.

[75] MacMillan, J., *Infosec strategies and best practices: gain proficiency in information security using expert-level strategies and best practices*, Packt Publishing, Birmingham, UK, 2021, ISBN 978-1-80056-364-3.

[76] Vallabhadas, D. K., Sandhya, M., *Securing multimodal biometric template using local random projection and homomorphic encryption*, Journal of Information Security and Applications, vol. 70, pp. 103339, 2022, ISSN 2214-2126.

[77] Radley-Gardner, O., Beale, H., Zimmermann, R., *Fundamental texts on european private law*, Hart Publishing, 2016.

[78] Chirileanu, T., *Criptografia homomorfică în practică*, Lucrare de licență susținută la Universitatea „Alexandru Ioan Cuza”, Iași, 2017.

[79] Țiplea, F.L., *Fundamentele algebrice ale informaticii*, Universitatea „Alexandru Ioan Cuza”, Iași, 2006.

[80] Falmari, V. R., Brindha, M., *Privacy preserving biometric authentication using Chaos on remote untrusted server*, Measurement, vol. 177, pp. 109257, 2021, Online ISSN 1873-412X, Print ISSN 0263-2241.

[81] Kim, A., Polyakov, Y., Zucca, V., *Revisiting homomorphic encryption schemes for finite fields*, Advances in Cryptology – ASIACRYPT 2021, Springer International Publishing, Berlin, Germany, vol. 13092, pp. 608–639, 2021, ISBN 978-3-030-92077-7 978-3-030-92078-4.

[82] Pulido-Gaytan, B., Tchernykh, A., Babenko, M., Radchenko, G., Drozdov, A.Y., *Privacy-preserving neural networks with homomorphic encryption: Challenges and opportunities*, Peer-to-Peer Networking and Applications, vol. 14, no. 3, pp. 1666–1691, 2021, ISSN 1936-6442, 1936-6450.

[83] Biasioli, B., Marcolla, C., Calderini, M., Mono, J., *Improving and automating BFV parameters selection: an average-case approach*, Cryptology ePrint Archive, Paper 2023/600, https://eprint.iacr.org/2023/600.

[84] Rana, S., Jadhav, O., Rajput, S., Bhansali, P., Jyotinagar, V., *Homomorphic image encryption*, International Research Journal of Engineering and Technology (IRJET), vol. 06, no. 04, 2019, pp. 3934-3940, ISSN 2395-0056.

[85] Huang, J., Wu, D., *Cloud storage model based on the BGV fully homomorphic encryption in the blockchain environment*, Security and Communication Networks, vol. 2022, pp. 1–9, 2022, ISSN 1939-0122, 1939-0114.

[86] Weir, B., *Homomorphic Encryption,* Disertație susținută la Universitatea Waterloo, Ontario, Canada, 2013.

[87] Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A., Vaikuntanathan, V., *Homomorphic Encryption Standard,* Springer International Publishing, pp. 31–62, 2021, ISBN 978-3-030-77286-4 978-3-030-77287-1.

[88] Jiang, L., Ju, L., *FHEBench: benchmarking fully homomorphic encryption schemes*, 2022, http://arxiv.org/abs/2203.00728.

[89] Panda, S., *Principal Component Analysis using CKKS homomorphic scheme*, Cyber Security Cryptography and Machine Learning, Springer International Publishing, Cham, vol. 12716, pp. 52–70, 2021, ISBN 978-3-030-78085-2 978-3-030-78086-9.

[90] *Introduction to the CKKS/HEAAN FHE Scheme*, Inferati Inc. Washington, USA, 2022, https://inferati.azureedge.net/docs/inferati-fhe-ckks.pdf

[91] Deng, W., Liu, L., Chen, H., Bai, X., *Infrared image contrast enhancement using adaptive histogram correction framework*, Optik, vol. 271, pp. 170114, 2022, Online ISSN 1618-1336, Print ISSN 0030-4026.

[92] Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J. P., Natarajan, P., *Local Shannon entropy measure with statistical tests for image randomness*, Information Sciences, vol. 222, pp. 323–342, 2013, ISSN 0020-0255.

[93] Kumar, A., Rani, R., Singh, S., *Encoder-Decoder architecture for image steganography using Skip Connections*, Procedia Computer Science, vol. 218, pp.1122–1131, 2023, ISSN 1877-0509.

[94] Bakurov, I., Buzzelli, M., Schettini, R., Castelli, M., Vanneschi, L., *Structural similarity index (SSIM) revisited: A data-driven approach*, Expert Systems with Applications, vol. 189, pp. 116087, 2022, ISSN 0957-4174.

[95] Firdous, A., *Symmetric image encryption using chaos and hash*, Teză de doctorat susținută la Universitatea Islamia, Bahawalpur, Punjab, Pakistan, 2019.

[96] Noor, S., Hammood, D. A., Al-Naji, A., Chahl, J., *A fast text-to-image encryption-decryption algorithm for secure network communication*, Computers, vol. 11, no. 3, pp. 39, 2022, ISSN 2073-431X.

[97] Crihan, G., Crăciun, M., Dumitriu, L., *A comparative assessment of homomorphic encryption algorithms applied to biometric information*, Inventions, Special Issue Perspectives and Challenges in Doctoral Research - Selected Papers from the 11th Edition of the Scientific Conference of the Doctoral Schools of “Dunărea de Jos” University of Galati (SCDS-UDJG), vol. 8, no. 4, pp. 102, ISSN 2411-5134.

[98] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S., *Impact of artificial „gummy” fingers on fingerprint systems*, Electronic Imaging, San Jose, CA, pp. 275–289, 2002.

[99] Roddy, A. R., Stosz, J. D., *Fingerprint features-statistical analysis and system performance estimates*, Proceedings of the IEEE, vol. 85, no. 9, pp. 1390–1421, 1997, ISSN 0018-9219.

[100] Khairnar, S., Gite, S., Kotecha, K., Thepade, S. D., *Face liveness detection using artificial intelligence techniques: a systematic literature review and future directions*, Big Data and Cognitive Computing, vol. 7, no. 1, pp. 37, 2023, ISSN 2504-2289.

[101] Wang, X., Yan, Z., Zhang, R., Zhang, P., *Attacks and defenses in user authentication systems: A survey*, Journal of Network and Computer Applications, vol. 188, pp. 103080, 2021, ISSN 1084-8045.

[102] Hamza, M., Tehsin, S., Humayun, M., Almufareh, M. F., Alfayad, M., *A comprehensive review of face morph generation and detection of fraudulent identities,* Applied Sciences, vol.12, no.24, pp.12545, 2022, ISSN 2076-3417.

[103] Alshareef, N., Yuan, X., Roy, K., Atay, M., *A study of gender bias in face presentation attack and its mitigation*, Future Internet, vol. 13, no. 9, pp. 234, 2021, ISSN 1999-5903.

[104] Ryu, R., Yeom, S., Herbert, D., Dermoudy, J., *The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction*, ICT Express, 2023, ISSN 2405-9595.

[105] Kokal, S., Vanamala, M., Dave, R., *Deep learning and machine learning, better together than apart: a review on biometrics mobile authentication,* Cybersecurity and privacy, vol. 3, pp. 227–258, 2023, ISSN 2624-800X.

[106] Ammour, N., Bazi, Y., Alajlan, N., *Multimodal approach for enhancing biometric authentication*, Journal of imaging, vol. 9, no. 9, pp. 168, 2023, ISSN 2313-433X.

[107] Wang, Y., Shi, D., Zhou, W., *Convolutional Neural Network approach based on multimodal biometric system with fusion of face and finger vein features*, Sensors, vol. 22, no. 16, pp. 6039, 2022, ISSN 1424-8220.

[108] Alay, N., Al-Baity, H. H., *Deep Learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits*, Sensors, vol. 20, no. 19, pp. 5523, 2020, ISSN 1424-8220.

[109] Srivastava, R., Bhardwaj, P.K., Othman, O.T., Pushkarna, M., Bajaj, M., Shafiq, M., Hamam, H., *Match-level fusion of finger-knuckle print and iris for human identity validation using neuro-fuzzy classifier*, Sensors, vol. 22, no. 10, pp. 3620, 2022, ISSN 1424-8220.

[110] Pooyandeh, M., Han, K.-J., Sohn, I., *Cybersecurity in the AI-Based Metaverse: A Survey*, Applied Sciences, vol. 12, no. 24, pp. 12993, 2022, ISSN 2076-3417.

[111] Aggarwal, D., Zhou, J., Jain, A. K., *FedFace: Collaborative learning of face recognition model*, 2021 IEEE International Joint Conference on Biometrics (IJCB), Shenzhen, China, pp. 1–8, 2021, ISBN 978-1-66543-780-6.

[112] Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J.M., Confalonieri, R., Riccardo Guidotti, R., Ser, J., Díaz-Rodríguez, N., Herrera, F., *Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence*, Information Fusion, vol. 99, pp. 101805, 2023, Online ISSN 1872-6305, Print ISSN 1566-2535.

[113] Ghafourian, M., Sumer, B., Vera-Rodriguez, R., Fierrez, J., Tolosana, R., Moralez, A., Kindt, E.*, Combining blockchain and biometrics: a survey on technical aspects and a first legal analysis*, 2023, http://arxiv.org/abs/2302.10883.

[114] Karygiannis, A. T., Eydt, B., Barber, G., Bunn, L., Phillips, T., *Guidelines for securing Radio Frequency Identification (RFID) systems*, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-98, 2007.

[115] Roy, K. S., Sujith, M., Bhanu, B., Preethi, P., Hazarika, R. A., *ECC and AES based secure authentication scheme for the Internet of Drones using FPGA*, In Review, 2023, doi: https://doi.org/10.21203/rs.3.rs-3285523/v1.

[116] Zhang, S., Liu, Y, Han, Z., Yang, Z., *A lightweight authentication protocol for UAVs based on ECC scheme,* Drones, vol. 7, no. 5, pp. 315, 2023, ISSN 2504-446X.