Universitatea Transilvania din Brașov

ȘCOALĂ DOCTORALĂ INTERDISCIPLINARĂ

Facultatea de Inginerie Electrică și Știința Calculatoarelor

Rebecca Acheampong

Addressing Cybersecurity Concerns in Virtual Reality Applications

Abordarea Preocupărilor de Securitate Cibernetică în Aplicații de Realitate Virtuală

REZUMATUL tezei de doctorat

Coordonator științific

Prof. Dr. Dorin-Mircea Popovici

BRAȘOV, 2025

Mulțumiri

Îmi exprim cu umilință cea mai profundă recunoștință față de Dumnezeu Atotputernic, a cărui prezență a fost forța călăuzitoare din spatele fiecărei etape a călătoriei mele academice. Intervenția Sa divină și harul Său neclintit m-au susținut și mi-au pavat calea spre finalizarea cu succes a acestei lucrări.

Îi sunt profund recunoscătoare îndrumătorului meu academic, Prof. Dr. Dorin-Mircea Popovici, pentru îndrumarea sa excepțională, încurajarea constantă și sprijinul constant pe toată durata acestei cercetări. Angajamentul său față de excelența academică și atenția deosebită la detalii au modelat în mod semnificativ direcția și calitatea acestei disertații.

Aprecierea mea sinceră se îndreaptă, de asemenea, către cel de-al doilea consilier al meu, Prof. Dr. Ing. Titus Bălan, a cărui expertiză profundă în domeniul securității cibernetice, sfaturile atente și interesul real pentru dezvoltarea mea academică au fost esențiale pentru succesul meu. Îi sunt recunoscătoare pentru mentorat și pentru eforturile depuse în vederea asigurării sprijinului academic în timpul studiilor mele de doctorat.

Mulțumesc din suflet membrilor comisiei mele de doctorat, fiecare dintre aceștia având un rol distinct în modelarea parcursului meu academic. Prof. Dr. Ing. Florin Gîrbacia mi-a oferit o bază solidă în Realitatea Virtuală, ajutându-mă să înțeleg elementele fundamentale ale acestui domeniu în continuă evoluție. Prof. Dr. Ing. Sorin Moraru m-a încurajat constant să îmi consolidez descoperirile și să merg mai departe cu teza mea. Conf. Dr. Elena Băutu a oferit perspective valoroase care m-au propulsat prin diferite faze ale acestei călătorii. Le rămân profund îndatorat tuturor.

Doresc să adresez mulțumiri speciale familiei și prietenilor mei apropiați: Louis Acheampong, Mercy Vicentia Nazzar, Benjamin Anim, Sheila Adjei, Louisa Oppong Afriyie, Gifty Nyarko, Alice Dawson, Francisca Anim și Daniela Mignea, a căror dragoste neclintită, sprijin emoțional și asistență financiară în timp util m-au ajutat să perseverez prin provocări personale și academice neprevăzute. Sacrificiile și încrederea lor în potențialul meu au fost fundamentul rezistenței mele.

De asemenea, le sunt recunoscător colegilor și colaboratorilor din domeniul securității cibernetice ale căror eforturi comune de cercetare și parteneriate intelectuale au îmbogățit profunzimea și rigoarea acestei disertații. În special, doresc să îi mulțumesc lui Alexandre Rekeraho, pentru numeroasele ore petrecute explorând soluții la probleme complexe; lui Ionuț-Alexandru Oprea, pentru contribuțiile și eforturile sale de colaborare; lui Emmanuel Tuyishime, pentru implicarea sa într-o lucrare de cercetare și în activitatea de proiect; și lui Manuel Soto, pentru angajamentele noastre comune de cercetare.

În plus, aș dori să îmi exprim recunoștința sinceră față de finanțatorii proiectului SPIRIT Horizon open call 1, în cadrul căruia am avut privilegiul de a participa în calitate de asistent de cercetare responsabil cu sarcinile de securitate cibernetică. Îi sunt recunoscătoare în mod special coordonatorului meu, Gabriel Danciu, a cărui îndrumare și sprijin mi-au îmbogățit considerabil experiența. Lucrul cu el și cu întreaga echipă GENSAVR a fost atât recompensant din punct de vedere intelectual, cât și inspirator din punct de vedere profesional

În cele din urmă, aș dori să îmi exprim aprecierea sinceră față de studenții cursului de *medii virtuale multimodale* de la Universitatea Ovidius, Constanța, care au contribuit cu generozitate la această cercetare prin participarea la studiul utilizatorilor. Implicarea lor a fost vitală pentru atingerea obiectivelor acestei disertații.

Tuturor celor care au parcurs această călătorie alături de mine prin mentorat, colaborare sau sprijin necondiționat le mulțumesc.

Rebecca Acheampong

CUPRINS

Capitolul 1. Introducere

Evoluția rapidă a tehnologiei a inaugurat o eră a transformării digitale fără precedent, modificând fundamental modul în care trăim, muncim și ne implicăm în lumea din jurul nostru[1]. De la asistență medicală și educație la divertisment și întreprinderi, digitalizarea a creat oportunități vaste pentru inovare, eficiență și conectivitate[2]. Printre cele mai transformative progrese ale acestei revoluții digitale se numără apariția realității virtuale (RV). Această tehnologie a redefinit granițele dintre lumea fizică și cea virtuală, permițând experiențe imersive care altădată erau de domeniul science fiction-ului [3].

VR scufundă complet utilizatorii într-un mediu simulat pe calculator, izolându-i de lumea reală. Cu ajutorul ecranelor montate pe cap (HMD), cum ar fi Oculus Rift și HTC Vive, cuplate cu controlere sau cu urmărirea mâinii și a corpului, RV permite utilizatorilor să se scufunde și să interacționeze cu mediul virtual [4].

În plus, RV permite utilizatorilor să depășească limitele realității, oferind medii imersive în care pot interacționa, colabora și împărtăși experiențe în timp real. Aceste capacități sunt alimentate de progrese semnificative în ceea ce privește puterea de calcul, procesarea grafică și tehnologiile HMD, care au făcut ca RV să fie mai accesibilă și să aibă un impact mai mare decât oricând [5]. În prezent, RV nu doar că revoluționează industriile, ci și reformează interacțiunile sociale, educația și divertismentul, oferind utilizatorilor un sentiment profund de "prezență" și angajament.

1.1. Problema și motivația cercetării

În ciuda adoptării în creștere a tehnologiilor RV, natura lor imersivă și interconectată prezintă provocări semnificative în materie de securitate cibernetică[6]. Integrarea hardware-ului (de exemplu, HMD-uri, controlere de mișcare), a software-ului, a protocoalelor de rețea și a datelor biometrice sensibile creează o suprafață de atac mare și complexă[3]. Aceste caracteristici unice fac ca sistemele RV să fie deosebit de vulnerabile la amenințări precum accesul neautorizat, încălcarea securității datelor, injectarea de malware, ingineria socială și manipularea psihologică

Actorii amenințători pot exploata vulnerabilitățile hardware-ului RV, cum ar fi HMD-urile și controlerele de mișcare, pentru a accesa ilegal informații sensibile. În mod similar, punctele slabe din software-ul RV și protocoalele de comunicare în rețea pot fi exploatate pentru a manipula mediile virtuale, a injecta coduri malițioase sau a lansa atacuri de phishing[7]. În plus, caracterul imersiv al RV estompează granițele dintre lumea fizică și cea virtuală, făcând utilizatorii mai susceptibili la manipularea psihologică și la atacurile de inginerie socială.[8]

Cadrele și protocoalele actuale de securitate cibernetică au fost concepute pentru mediile de calcul convenționale și sunt insuficiente pentru a aborda riscurile spațiale, comportamentale și de confidențialitate specifice RV. Multe platforme RV se concentrează foarte mult pe experiența utilizatorului și pe inovare, adesea în detrimentul unei securități solide. [9]

1.2. Scopul și obiectivele cercetării

Scopul principal al cercetării este de a explora lacunele de securitate cibernetică inerente RV și de a dezvolta o strategie aplicabilă pentru a le aborda.

Obiective specifice:

O1. Identificarea și analiza vulnerabilităților de securitate cibernetică ale sistemelor de RV.

Examinați vectorii comuni de atac, cum ar fi exploatările hardware, vulnerabilitățile software, insecuritățile rețelei și riscurile legate de factorul uman în mediile de RV.

O2. Evaluarea cadrelor de securitate cibernetică existente și a limitelor acestora.

Analizați măsurile și protocoalele actuale de securitate cibernetică aplicate sistemelor de RV și evaluați lacunele și deficiențele cadrelor existente în abordarea amenințărilor specifice RV.

O3. Efectuarea de studii de caz reale și evaluarea riscurilor.

Efectuați simulări ale amenințărilor și studii empirice pentru a evalua impactul atacurilor cibernetice asupra utilizatorilor RV, asupra vieții private și asupra integrității sistemului.

O4. Evaluarea echilibrului dintre utilizabilitate, securitate și confidențialitate în RV

Efectuați evaluări centrate pe utilizator pentru a analiza interacțiunea dintre utilizabilitate, securitate și confidențialitate în mediile RV, asigurându-vă că implementările de securitate sunt perfect integrate fără a compromite imersiunea și calitatea experienței.

O5. Implementați și validați măsurile de securitate în mediile de RV.

Dezvoltarea și integrarea măsurilor de securitate în aplicațiile de RV și evaluarea eficienței și caracterului practic al acestor soluții de securitate prin experimente, teste de utilizare și evaluări ale conformității.

1.3. Structura și tezei

Această teză de doctorat este organizată în șapte capitole. Intitulată "Abordarea preocupărilor legate de securitatea cibernetică în aplicații de realitate virtuală", cercetarea oferă o bază pentru lucrările viitoare privind cadrele de securitate menite să abordeze provocările în materie de securitate și confidențialitate în evoluție în mediile RV.

Studiul include simulări ale amenințărilor pentru a evalua vulnerabilitățile sistemelor de RV și explorează modul în care măsurile de securitate pot fi integrate fără a perturba utilitatea sau experiența utilizatorului. Cercetarea implementează, de asemenea, trei măsuri majore de atenuare a securității în cadrul platformelor de RV pentru a spori protecția, păstrând în același timp imersiunea și interactivitatea. Implementarea a trei măsuri-cheie de atenuare a securității:

1. Semnături digitale criptografice pentru a asigura integritatea și autenticitatea activelor virtuale.

2. Soluții de securitate adaptive pentru protejarea datelor utilizatorilor și asigurarea conformității în mod dinamic.
3. Mecanisme de autentificare multistrat pentru controlul accesului și gestionarea sesiunilor.

Capitolul 1: Introducere

Acest capitol prezintă raționamentul și motivația cercetării, subliniind riscurile de securitate inerente tehnologiilor de RV și importanța abordării acestora. Acesta oferă o imagine de ansamblu asupra sistemelor de RV, discutând componentele lor de bază, semnificația și diversele domenii de aplicare. În continuare, capitolul identifică principalele lacune ale cercetării și articulează scopurile și obiectivele care ghidează acest studiu pentru a rezolva aceste lacune.

Capitolul 2: Preocupări legate de securitatea cibernetică și strategii de atenuare

Acest capitol analizează amenințările la adresa securității cibernetice în RV, clasificându-le folosind Triada CIA și vectorii de atac. Acesta analizează strategiile actuale de atenuare pentru securizarea mediilor imersive și include un studiu de caz din lumea reală cu o evaluare a riscurilor pentru a valida și consolida constatările.

Capitolul 3: Echilibrarea utilizabilității, experienței utilizatorului, securității și confidențialității în sistemele de RV

Acest capitol examinează compromisurile dintre utilizabilitate, experiența utilizatorului, securitate și confidențialitate în RV. Acesta prezintă un model centrat pe utilizator și un studiu de caz cu treisprezece participanți, arătând că modelele de securitate incluzive și intuitive pot spori încrederea și utilitatea fără a reduce securitatea.

Capitolul 4: Îmbunătățirea securității și a autenticității în mediile imersive

Acest capitol prezintă utilizarea semnăturilor digitale RSA-2048 și SHA-256 pentru securizarea artefactelor virtuale în RV. O implementare practică permite utilizatorilor să semneze și să verifice în mod intuitiv bunurile, consolidând încrederea și autenticitatea fără a compromite ușurința în utilizare.

Capitolul 5: Integrarea și îmbunătățirea securității în cadrul platformei GENSAVR

Acest capitol prezintă integrarea unui cadru de securitate pe mai multe niveluri pentru protejarea mecanismelor de autentificare, a gestionării sesiunilor și a sistemelor backend în timp real pe platforma GENSAVR. Îmbunătățirile de securitate includ:

1. Nakama pentru autentificarea securizată a utilizatorilor,
2. Kubescape pentru scanarea securității Kubernetes,
3. ARMO pentru monitorizarea securității în timp real.

Evaluările de risc și scanările de conformitate NSA au identificat și abordat probleme legate de implementarea volumelor de lucru, politicile RBAC, escaladarea privilegiilor și securitatea rețelei.

Accentul a fost pus pe menținerea unor sesiuni de utilizator sigure și neîntrerupte în cadrul experiențelor imersive.

Capitolul 6: Securitate adaptivă în timp real pentru confidențialitate și conformitate în aplicații imersive

Acest capitol abordează provocările legate de confidențialitate generate de colectarea de date multimodale în medii imersive. Acesta prezintă un model de securitate adaptiv în timp real care pune în aplicare legile regionale privind protecția datelor prin ajustarea dinamică a politicilor de colectare a datelor pe baza locației utilizatorului. Folosind detectarea geolocalizării prin IPInfo API și GPS, sistemul asigură conformitatea cu reglementările privind confidențialitatea, cum ar fi GDPR și CCPA. Această abordare protejează datele utilizatorilor în spațiile virtuale, promovând încrederea și diminuând riscurile în peisajul Metaverse în continuă evoluție

Capitolul 7: Concluzii finale, contribuții originale și direcții viitoare

Acest capitol de încheiere rezumă rezultatele cercetării, subliniind contribuțiile originale ale autorului. De asemenea, prezintă metodele de diseminare a cercetării, discutând potențialele aplicații în lumea reală și direcțiile viitoare de cercetare pentru a avansa în continuare cadrele de securitate cibernetică în RV.

Capitolul 2. Preocupări privind securitatea cibernetică de ultimă oră și măsuri de atenuare în sistemele de realitate virtuală

Pe măsură ce dependența societății de tehnologie crește, crește și expunerea acesteia la amenințările cibernetice[10]. Chiar și cele mai sigure infrastructuri de rețea pot fi compromise din cauza erorilor umane[11]. Aceste vulnerabilități pun în pericol sistemele informatice esențiale, sporind necesitatea unor măsuri solide de securitate cibernetică în toate sectoarele.

Acest capitol abordează obiectivele 1-3, concentrându-se asupra riscurilor unice de securitate cibernetică din cadrul sistemelor RV și examinând modul în care atacatorii exploatează lacunele hardware și software. Acesta prezintă principalele preocupări legate de confidențialitate și securitate, clasifică tipurile de amenințări și prezintă studii de caz din lumea reală pentru a demonstra implicațiile practice ale acestor vulnerabilități.

Capitolul contribuie la teză prin:

- Identificarea vulnerabilităților în RV, analizarea amenințărilor și validarea riscurilor prin studii de caz.
- Acesta oferă o explorare cuprinzătoare a amenințărilor la adresa securității cibernetice în mediile RV, oferind o înțelegere detaliată a riscurilor care rezultă din natura imersivă și interactivă a RV
- Aceasta introduce o taxonomie structurată care clasifică amenințările atât în funcție de principiile de bază ale securității cibernetice CIA, cât și de vectorii de atac, cum ar fi vulnerabilitățile rețelei, accesul neautorizat și ingineria socială.

2.1. Amenințări la adresa securității cibernetice și riscuri la adresa vieții private în realitatea virtuală

Fundația securității cibernetice este construită pe triada CIA: Confidențialitate, Integritate și Disponibilitate. Triada CIA servește drept cadru de bază pentru menținerea unei securități puternice a informațiilor[12]. Fiecare pilon joacă un rol esențial în protejarea activelor digitale, iar în contextul RV, aceste principii trebuie menținute cu atenție pentru a proteja utilizatorii și sistemele de amenințările cibernetice. În cazul RV, amenințările pot afecta simultan confidențialitatea, integritatea și disponibilitatea, ducând la consecințe grave [13].

Sistemele RV prezintă o suprafață de atac mai largă datorită dependenței lor de medii bogate în senzori, de procesarea în timp real a datelor și de componentele hardware și software interconectate [3].

Confidențialitatea datelor este una dintre cele mai importante preocupări în mediile de RV [14]. RV colectează date sensibile, cum ar fi mișcările corpului, privirea și datele biometrice, care pot fi exploatate pentru supraveghere sau profilarea identității [15].

Accesul neautorizat rămâne un risc major de securitate cibernetică în mediile RV, unde actorii rău intenționați se pot infiltra în conturile utilizatorilor, manipula identitățile virtuale și exploata vulnerabilitățile sistemului [16].

În ceea ce privește riscurile legate de manipularea obiectelor virtuale și riscurile de siguranță, atacatorii pot manipula elemente virtuale, pot modifica configurațiile spațiale sau pot injecta conținut rău intenționat pentru a perturba experiența utilizatorului [17]. În timp ce atacurile de manipulare sunt reale în RV, amenințările la adresa securității rețelelor afectează conectivitatea rețelelor și expun utilizatorii la interceptarea datelor, atacuri MITM și ascultarea vocii [4], expunând discuțiile confidențiale în cadrul întâlnirilor RV corporative, jocurilor online și claselor virtuale.

Cercetările au arătat că imersiunea reduce gradul de conștientizare al utilizatorului, făcându-l mai vulnerabil la ingineria socială și la înșelăciune [18]. Identitățile RV legate de datele comportamentale și biometrice sunt greu de recuperat în caz de furt, ceea ce duce la forme avansate de uzurpare a identității. Frauda prin RV încorporează limbajul corpului, trăsături comportamentale, tonul vocii și alți identificatori biometrici, făcând înșelăciunea mult mai dificil de detectat [19].

2.2. Vectorii comuni de atac

Adoptarea pe scară largă a RV prezintă, de asemenea, o suprafață de atac în creștere pentru infractorii cibernetici. Aceste amenințări provin din vulnerabilitățile hardware, software, comunicațiile de rețea și interacțiunile utilizatorilor, permițând atacatorilor să intercepteze date, să manipuleze medii virtuale, să implementeze programe malware și să perturbe infrastructura RV. Această secțiune explorează cei mai răspândiți vectori de atac în mediile RV, detaliind modul în care adversarii exploatează punctele slabe din hardware, software, comunicațiile de rețea și comportamentul utilizatorilor.

Malware-ul se manifestă sub diverse forme, inclusiv viruși, viermi, spyware, troieni, ransomware și rootkit-uri [20]. Atacatorii exploatează vulnerabilitățile sistemului RV și plugin-urile terților pentru a injecta malware (de exemplu, troieni, spyware).

Ingineria socială este un atac bazat pe înșelăciune care exploatează psihologia umană pentru a păcăli persoanele să dezvăluie date confidențiale, să efectueze tranzacții frauduloase sau să adopte comportamente nesigure [21]. Ingineria socială rămâne o preocupare majoră în materie de securitate cibernetică, 85% din încălcările securității datelor implicând interacțiunea umană în 2022. Interacțiunile imersive și bazate pe avatar din RV îi fac pe utilizatori mai susceptibili la înșelăciune [22]. Preluarea identității prin intermediul avatarurilor permite phishing-ul și frauda de identitate, după cum se observă în incidente reale precum încălcarea securității datelor Roblox 2022 [23].

Atacurile MITM exploatează de mult timp canalele de comunicare, permițând atacatorilor să intercepteze, să manipuleze sau să falsifice traficul de rețea între două părți care comunică [24]. Adversarii interceptează și manipulează comunicațiile RV în timp real, exploatând protocoalele slabe și autentificarea [25].

Atacatorii MITM se introduc între două părți într-o sesiune RV, făcându-i să pară participanți de încredere, dar interceptând sau modificând în secret comunicațiile. Acest lucru le permite să se dea drept utilizatori legitimi, obținând acces neautorizat la conversații private, tranzacții financiare sau întâlniri corporative [26].

Platformele RV depind foarte mult de conectivitatea neîntreruptă [27]. Atacurile DoS și DDoS pot supraîncărca serverele, întrerupe sesiunile și bloca infrastructura RV, în special în cadrul jocurilor și al educației [3]. Un incident notabil a avut loc în 2019, când un atac DDoS a perturbat rețeaua VRChat, subliniind susceptibilitatea serviciilor RV sociale și orientate spre jocuri [28].

2.3. Clasificarea taxonomică a amenințărilor RV

Natura imersivă și interactivă a RV creează noi suprafețe de atac, ceea ce face esențială stabilirea unei taxonomii cuprinzătoare și structurate a amenințărilor la adresa securității.

Această secțiune identifică 24 de amenințări și le clasifică în Tabelul 2.1. Pentru a clasifica eficient amenințările în RV, se utilizează un model dublu de clasificare, axat pe:

1. Triada CIA - Această categorisire examinează modul în care amenințările afectează CIA a sistemelor RV.
2. Vectorii de atac (cum au loc atacurile?) - Această clasificare se bazează pe metodele utilizate de atacatori pentru a exploata vulnerabilitățile din hardware, software, infrastructura de rețea și interacțiunile utilizatorilor.

Combinarea acestor două modele asigură o înțelegere holistică a amenințărilor RV, permițând o mai bună evaluare a riscurilor, strategii de apărare și elaborarea de politici pentru securizarea spațiilor digitale imersive.

Tabelul 2.1. Clasificarea taxonomică a amenințărilor în mediile RV

Amenințări în RV	Vectorul de atac/componenta exploatată	Tip atac	C	I	A
Exploatarea giroscopului și a senzorului de mișcare pentru supraveghere [15]	Hardware și exploatarea senzorilor	Urmărirea și supravegherea utilizatorilor	√		
Scurgeri de date biometrice [3]	Software	Furtul de date și profilarea neautorizată	√		

Exploatarea datelor de urmărire a ochilor pentru analiza comportamentală	Software și rețea	Profilarea comportamentală	√		
Explozii de tip cal troian în aplicații și pluginuri de RV	Software și aplicații	Malware	√	√	
Ransomware care criptează fișierele de RV și datele critice ale utilizatorului [17]				√	√
Rootkit-uri care permit accesul persistent prin backdoor la dispozitivele de RV			√	√	
Spyware care înregistrează interacțiunile și conversațiile utilizatorilor de RV			√		
Atacurile de epuizare a lățimii de bandă perturbă conectivitatea RV	Rețea	DoS & DDoS			√
Atacuri de manipulare a latenței în jocurile de RV competitive					√
Tragerea cu urechea la conversațiile VR Voice & Spatial Audio [24][29]		Deturnarea sesiunii și interceptarea datelor	√		
Atacuri MITM			√	√	
Deturnarea sesiunilor de RV [30]			√		√
Redirecționarea traficului și portaluri de rețea RV false			√		√
Atacuri de dezorientare [17]	Exploatarea hardware și a senzorilor	Atacuri de navigare, mișcare și manipulare spațială		√	
Atacul însoțitorului [17]				√	√
Atac cu suprapunere de camere [17]				√	
Atacul joystick-ului uman [17]				√	√
Atac MITR [24]	Rețea și inginerie socială	Acces neautorizat și control	√	√	
Atacul Inception [31]	Software și manipulare umană	Înșelăciunea și manipularea realității		√	
Avatare înșelătoare și interacțiuni Deepfake bazate pe inteligența artificială	Factorul uman (inginerie socială)	Falsificarea și manipularea identității	√	√	
Bunuri virtuale false și escrocherii de piață în piețele RV		Frauda financiară și furtul de identitate	√	√	
Falsificarea identității în tranzacțiile financiare bazate pe RV		Preluarea contului și furtul financiar	√		
Atacuri de phishing în spațiile de RV [32]		Acces neautorizat și încălcarea confidențialității	√		

Imitarea avatarului și falsificarea identității Deepfake [16]		Furtul de identitate digitală	√		

Prin structurarea amenințărilor în RV prin triada CIA și vectorii de atac, a fost creat un cadru cuprinzător care identifică principalele riscuri cu care se confruntă utilizatorii și organizațiile RV. În plus, acesta explică modul în care aceste amenințări se materializează și ce metode folosesc atacatorii și oferă o bază structurată pentru apărarea, reglementările și strategiile de atenuare a securității cibernetice,

2.4. Măsuri de atenuare pentru securitatea realității virtuale

Această secțiune explorează cele mai recente cadre de securitate, tehnologii și bune practici utilizate pentru a aborda vulnerabilitățile hardware, riscurile de securitate software, amenințările de rețea și atacurile centrate pe om, cum ar fi ingineria socială și falsificarea identității.

2.4.1 Securitatea rețelelor și criptarea comunicațiilor

- **Criptare de la un capăt la altul:** Tehnici precum TLS, SSL și VPN securizează datele RV în tranzit [33].
- **Criptare homomorfă:** Permite efectuarea de operațiuni asupra datelor criptate, utilă în special pentru datele biometrice sau financiare sensibile [34].
- **Detectarea intruziunilor bazată pe IA:** IDS/IPS bazate pe AI detectează anomalii și amenințări precum atacurile MITM în timp real, asigurând o apărare proactivă [35].

2.4.2 Metode de autentificare

Pe măsură ce aplicațiile de realitate virtuală devin adoptate pe scară largă, cererea de mecanisme de autentificare robuste continuă să crească. Au fost propuse diverse strategii de autentificare, de la autentificarea bazată pe cunoștințe și autentificarea biometrică până la autentificarea cu factori multipli (MFA) și gestionarea identității bazată pe blockchain.

- **Autentificare pe bază de cunoștințe (KBA):** Parole tradiționale îmbunătățite cu modele specifice RV, cum ar fi RubikAuth și RubikBiom, pentru a rezista atacurilor prin observare și forță brută [36, 34].
- **Autentificare biometrică:** Folosește trăsături fizice unice, cum ar fi mișcarea ochilor (OcuLock) sau urmărirea privirii pentru verificarea identității în mod transparent și sigur.
- **Managementul identității bazat pe Blockchain:** Managementul identității descentralizat și inviolabil asigură autentificarea sigură fără o autoritate centrală [25, 27].
- **Autentificare adaptivă:** Protocoalele de autentificare se adaptează în funcție de comportament, locație și context pentru a spori securitatea în mod dinamic [37].

2.4.3 Securitatea hardware și stocarea datelor

- **Mediile de execuție de încredere (TEE):** Zonele hardware izolate protejează datele sensibile de atacurile la nivel de sistem [38]. Integrarea TEE-urilor în căștile RV protejează împotriva atacurilor bazate pe memorie, a accesului neautorizat și a vulnerabilităților sistemului
- **Criptare avansată:** Dovezile de cunoaștere zero și criptarea bazată pe atribute impun controlul accesului, păstrând în același timp confidențialitatea utilizatorului [39].

2.4.4 Arhitectura Zero Trust

În consecință, măsurile de securitate trebuie să fie aplicate în fiecare etapă a oricărei operațiuni critice. Acest lucru înseamnă că utilizatorii nu ar trebui să presupună niciodată că altora li se pot încredința datele lor personale în timpul unei sesiune de RV. Nakajima subliniază că o strategie-cheie pentru prevenirea atacurilor de inginerie socială este perfecționarea continuă a criteriilor de luare a deciziilor de către utilizatori prin învățarea din exemple din lumea reală [32].

2.4.5 Învățare federată pentru confidențialitate

Google a introdus învățarea federată (FL) pentru a face față provocărilor legate de confidențialitatea datelor, facilitând formarea colaborativă a modelelor pe diverse dispozitive IoT. Dispozitivele RV pregătesc modele la nivel local fără a partaja datele utilizatorului. Aceasta sprijină colaborarea securizată în cadrul sistemelor distribuite, sporind confidențialitatea datelor. Această abordare permite învățarea colaborativă, păstrând în același timp confidențialitatea datelor individuale [17].

2.4.6 Cadre existente

Atât NIST SP 800-53[40] , cât și ISO/IEC 27001 definesc controale generale de securitate, precum controlul accesului, criptarea și monitorizarea sistemului. Cu toate acestea, ele nu conțin orientări explicite pentru mediile imersive, semnalând o lacună în standardizare pentru amenințările specifice RV.

2.4.7 Constatări și limitări ale măsurilor existente de atenuare a efectelor asupra securității RV

Constatările din acest capitol servesc drept bază pentru elaborarea unor cadre de securitate în RV cuprinzătoare. Cu toate acestea, măsurile de atenuare existente prezintă limitări notabile, subliniind nevoia de cercetare și inovare continue.

O provocare cheie rămâne echilibrarea securității cu experiența utilizatorului. Multe mecanisme de securitate introduc fricțiuni în interacțiunile cu utilizatorii, ceea ce poate avea un impact negativ asupra imersiunii și experienței utilizatorilor. De exemplu, pașii de autentificare excesivi pot întrerupe fluxul experienței și pot duce la frustrarea utilizatorului dacă acesta introduce date.

În plus, mecanismele de monitorizare a securității RV și de răspuns la incidente rămân subdezvoltate. Sistemele actuale IDS și de răspuns la amenințări pentru mediile de RV sunt limitate, ceea ce face dificilă detectarea atacurilor în timp real.

În plus, complexitățile juridice și de reglementare împiedică aplicarea eficientă a măsurilor de protecție a datelor în RV. Natura transfrontalieră a aplicațiilor imersive îngreunează aplicarea legislației privind confidențialitatea, deoarece utilizatorii trec fără probleme de la o jurisdicție la alta, cu politici diferite de protecție a datelor. Aceste limitări subliniază necesitatea unor soluții de securitate centrate pe utilizator, adaptabile și conforme cu legislația.

2.5. Studiu de caz 1: Evaluarea vulnerabilității expunerii la informații personale identificabile

Acest studiu de caz investighează o vulnerabilitate de expunere a informațiilor de identificare personală (PII) detectată pe o platformă de distribuție a jocurilor RV. Ca parte a abordării obiectivului 3, a fost efectuată o evaluare a vulnerabilității din lumea reală pe o platformă RV utilizată pe scară largă, care deservește zilnic mii de utilizatori.

Această secțiune contribuie atât la capitol, cât și la teza generală prin:

1. Oferirea unui studiu de caz real cu privire la modul în care apar scurgeri de informații personale confidențiale în platformele de jocuri RV, extinderea CWE-359 cu constatări practice.
2. Demonstrarea aplicării OWASP ZAP ca instrument pentru testarea neintruzivă a securității în mediile de jocuri online.
3. Evidențierea riscurilor de conformitate legate de configurațiile greșite ale API, în special în contextul standardului PCI-DSS (Payment Card Industry Data Security Standard).
4. Furnizarea unui cadru pentru evaluarea deficiențelor de protecție a datelor în serviciile online, oferind recomandări de securitate aplicabile.

2.5.1 Metodologia cercetării

Această cercetare urmează practici etice de testare a securității, asigurându-se că nu au fost utilizate metode intruzive. Evaluarea a utilizat OWASP ZAP, un scaner de aplicații web open-source standard în industrie.

Ținta selectată este o platformă populară de jocuri RV care acceptă accesul multiplatformă, permițând utilizatorilor să interacționeze pe mai multe dispozitive.

- Procedura de configurare și testare
  - ✓ **Configurare**

Configurarea OWASP ZAP Proxy - Setările OWASP ZAP Proxy au fost ajustate pentru a corespunde IP-ului și portului local al mașinii gazdă.

Configurarea clientului țintă - Setările platformei RV au fost modificate pentru a direcționa traficul de rețea prin proxy-ul OWASP ZAP prin ajustarea setărilor browserului său web pentru a utiliza IP-ul și portul desemnate.

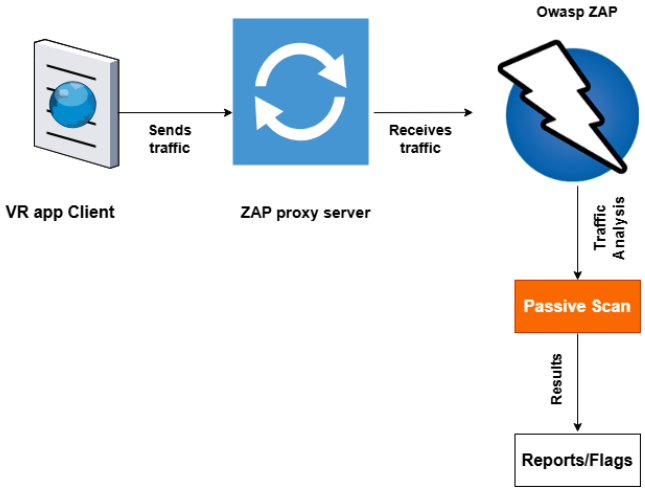

Figura 2.1. Configurarea evaluării vulnerabilității și fluxul de testare

- ✓ Testare

Platforma a fost lansată și au fost efectuate activități normale, cum ar fi navigarea în magazinul de aplicații și interacțiunea cu funcțiile din joc.

Scanare pasivă cu OWASP ZAP - ZAP a interceptat traficul de rețea dintre platformă și serverele externe, analizând răspunsurile API, așa cum se arată în Figura 2.1. Apoi, ZAP a marcat automat vulnerabilitățile, clasificându-le în funcție de gravitate, așa cum se arată în Figura 2.2.

Figura 2.2. Vulnerabilități detectate identificate în timpul interceptării traficului cu OWASP ZAP

2.5.2 Constatări și analiză

În timpul scanării vulnerabilităților cu OWASP ZAP, au fost detectate 18 vulnerabilități, după cum se arată în Figura 2.2. Dezvăluirea PII a apărut ca un risc ridicat și a constituit punctul central al evaluării în cadrul studiului.

Dezvăluirea PII identificată a expus date care conțin tipul cardului de credit, numărul de identificare al băncii (BIN). Figura 2.3 și Figura 2.4 ilustrează răspunsul API expus în timpul răspunsului traficului de rețea al OWASP ZAP.

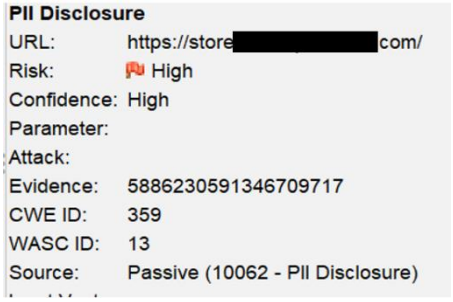

Figura 2.3. Informații detaliate suplimentare privind vulnerabilitatea PII Disclosure. Arată URL-ul, ID-ul CWE și tipul de scanare efectuată

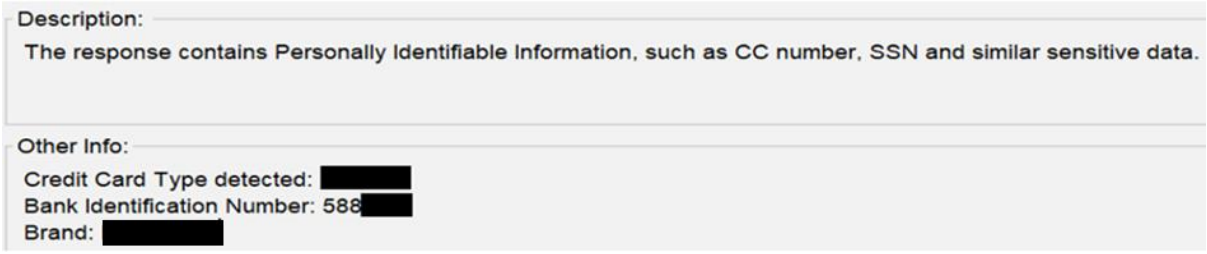

Figura 2.4. Detalii ale informațiilor financiare expuse în timpul interceptării API de către OWASP ZAP

- Riscuri potențiale de securitate

Vulnerabilitatea conține un impact cu risc ridicat și, de asemenea, încalcă confidențialitatea. O astfel de scurgere de informații poate fi asociată cu o serie de riscuri care sunt discutate mai jos.

1. Frauda financiară și abuzul de carduri de credit

Atacatorii ar putea exploata BIN-ul expus și tipul de card pentru a facilita tranzacții frauduloase, ducând la pierderi financiare pentru utilizatorii afectați [41].

2. Riscuri de phishing și inginerie socială

Escrocii ar putea crea mesaje de phishing foarte bine direcționate, folosind datele expuse ale cardurilor de credit. De exemplu: "cardul dvs. [Marca] care se termină cu [numărul BIN] a detectat o activitate neautorizată. Faceți clic aici pentru a vă securiza contul". Utilizatorii care nu bănuiesc nimic pot dezvălui toate detaliile cardului de credit, devenind astfel victime ale unor escrocherii financiare.

3. Umplerea acreditărilor și preluarea conturilor

Atacatorii ar putea utiliza datele expuse pentru a ghici parolele, a reseta conturile sau a lansa atacuri de tip credential stuffing. Dacă utilizatorii refolosesc parolele pe mai multe platforme, acest lucru ar putea escalada în deturnarea generalizată a conturilor.

2.5.3 Strategii de atenuare recomandate

Datele financiare sensibile nu ar trebui să fie niciodată expuse în text clar. Implementarea criptării care păstrează formatul maschează informațiile privind cardurile de credit [42]. Mai mult, răspunsurile API trebuie filtrate pentru a elimina datele sensibile înainte de transmitere. Asigurarea că toate datele financiare aderă la reglementările PCI-GDPR și CCPA este o bună practică pentru a garanta siguranța datelor financiare ale utilizatorilor. În plus, efectuarea de audituri de securitate de rutină este relevantă pentru detectarea și rezolvarea potențialelor vulnerabilități din cadrul API-urilor.

2.5.4 Concluzie

Acest studiu evidențiază pericolele de expunere a datelor financiare din cauza răspunsurilor API configurate greșit într-o platformă de jocuri RV utilizată pe scară largă. Folosind OWASP ZAP, această evaluare a identificat o vulnerabilitate critică care ar putea duce la fraudă, furt de identitate și nerespectarea reglementărilor privind securitatea financiară.

Studiul consolidează importanța stabilirii unor controale de securitate proactive pentru protejarea informațiilor financiare ale utilizatorilor în medii digitale imersive și demonstrează, de asemenea, eficacitatea evaluărilor de securitate neintruzive care utilizează metodologii de hacking etic.

2.6. Studiu de caz 2 - Modelul amenințării

Ca o contribuție cheie la această teză, acest studiu de caz abordează, de asemenea, obiectivul 3 prin realizarea și analizarea scenariilor de amenințare pentru a identifica vulnerabilitățile inerente sistemelor de realitate extinsă (XR).

Secțiunea contribuie la capitol prin:

1. Proiectarea și implementarea unei metodologii de evaluare a riscurilor bazate pe scenarii pentru a evalua riscurile de securitate în mediile XR.
2. Simularea scenariilor de atac din lumea reală pentru a identifica vulnerabilitățile și a analiza impactul acestora în mediile XR.
3. Introducerea unui model de evaluare a riscurilor structurat, bazat pe probabilitate, adaptat mediilor XR, care integrează factori umani, tehnici și de popularitate a atacurilor.
4. Cuantificarea riscurilor de securitate utilizând o abordare hibridă care combină sistemul CVSS (Common Vulnerability Scoring System) cu un model de probabilitate personalizat.

Figura 2.5 și Figura 2.6 ilustrează fluxurile de atac ale scenariilor examinate, oferind o reprezentare vizuală a modului în care aceste amenințări la adresa securității se desfășoară în ecosistemele RV. Procesul detaliat și evaluarea impactului amenințărilor sunt discutate în secțiunile următoare.

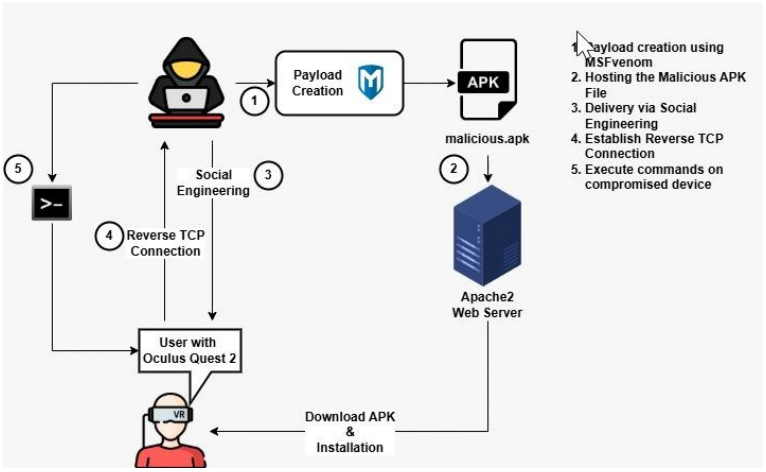

Figura 2.5. Diagrama fluxului de lucru al atacului de executare a codului de la distanță pentru scenariul 1

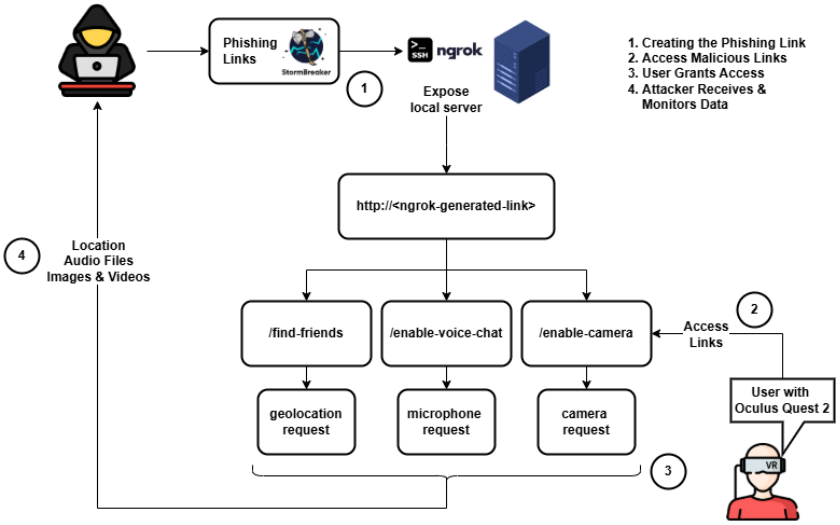

Figura 2.6. Diagrama fluxului de lucru a atacului de ascultare și supraveghere pentru scenariul 2

2.6.1 Metodologie

Această secțiune prezintă etapele tehnice, instrumentele și configurațiile experimentale utilizate pentru a executa și evalua aceste scenarii de atac.

Instrumente utilizate în configurația experimentală

Cadrul Metasploit a fost utilizat pentru testarea penetrării , în timp ce MSFvenom [43] a fost utilizat pentru crearea sarcinilor utile. Serverul web Apache2 a fost utilizat pentru livrarea încărcăturii utile și Storm Breaker pentru ascultare, urmărirea locației și extragerea informațiilor despre dispozitiv [44].

2.6.2 Scenarii de amenințare

Au fost realizate două scenarii practice de atac vizând dispozitive XR. Aceste scenarii demonstrează modul în care atacatorii pot exploata mediile XR prin inginerie socială, instrumente de acces de la distanță și exploatări bazate pe permisiuni.

- ✓ Scenariul 1: RCE (Remote Command Execution) pe Oculus Quest 2 prin APK rău intenționat

Acest scenariu care face trimitere la Figura 2.5 descrie modul în care un fișier APK rău intenționat, creat cu ajutorul MSFvenom (Figura 2.7 ilustrează configurația sarcinii utile) și transmis prin inginerie socială, poate fi utilizat pentru a compromite un Oculus Quest 2. Odată descărcat prin intermediul browserului Oculus și instalat, sarcina utilă se conectează la sistemul atacatorului cu ajutorul Metasploit, acordând acces complet de la distanță (Figura 2.8). Atacatorul poate apoi să execute comenzi, să extragă informații despre sistem și să controleze dispozitivul, evidențiind o metodă reală de executare a codului de la distanță (RCE) pe hardware RV.

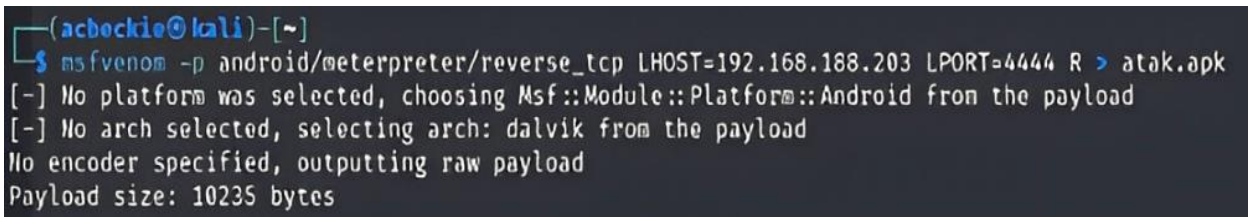

Figura 2.7. Generarea sarcinii utile utilizând MSFvenom

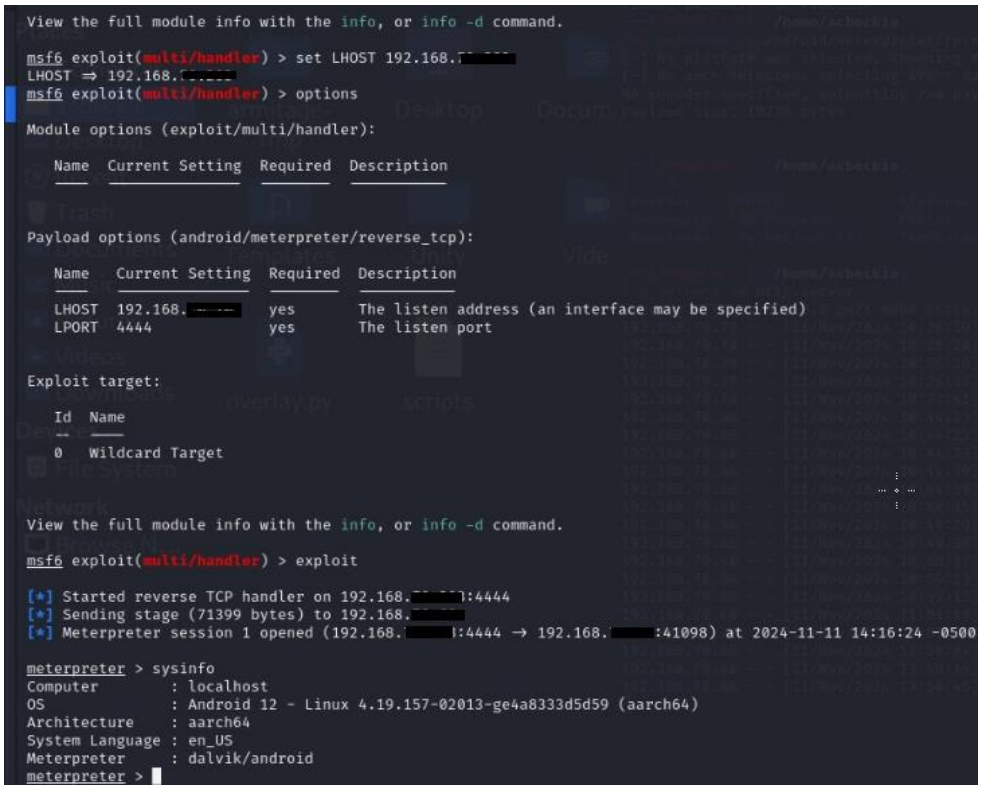

Figura 2.8. Un modul de exploatare multi-handler pentru gestionarea conexiunii reverse shell la țintă pentru a executa comenzi pe țintă. Și o ieșire de comandă sysinfo care afișează informațiile despre dispozitiv

```
meterpreter > app_list
Application List

Name                                Package                                                 Running  IsSystem
----                                -------                                                 -------  --------
Accounts Center                     com.meta.AccountsCenter.pwa                             false    true
AccountsCenter                      com.oculus.accountscenter                               false    false
Activity Stub                       com.meta.frameworkpackagestubs                          false    true
Android Services Library            android.ext.services                                    false    true
Android Shared Library              android.ext.shared                                      false    true
Android System                      android                                                 false    true
Android System WebView              com.android.webview                                     false    true
AppSafety                           com.oculus.appsafety                                    false    true
AvatarEditor                        com.oculus.avatareditor                                 false    true
Blocked Numbers Storage             com.android.providers.blockednumber                     false    true
Bluetooth                           com.android.bluetooth                                   false    true
Bookmark Provider                   com.android.bookmarkprovider                            false    true
Browser                             com.oculus.browser                                      false    true
BugReportService                    com.oculus.bugreportservice                             false    true
BugReportUploaderService            com.oculus.bugreportuploader                            false    true
Calendar Storage                    com.android.providers.calendar                          false    true
CaptionService                      com.oculus.captionservice                               false    true
CaptivePortalLogin                  com.android.captiveportallogin                          false    true
Casting                             com.oculus.magicislandcastingservice                    false    true
Certificate Installer               com.android.certinstaller                               false    true
Charge Control                      com.oculus.os.chargecontrol                             false    true
Companion Device Manager            com.android.companiondevicemanager                      false    true
Companion Server                    com.oculus.companion.server                             false    true
Contacts Storage                    com.android.providers.contacts                          false    true
Creed                               com.survios.CreedDemo                                   false    false
Download Manager                    com.android.providers.downloads                         false    true
Explore                             com.oculus.explore                                      false    true
External Storage                    com.android.externalstorage                             false    true
ExternalStorage                     com.oculus.externalstorage                              false    true
ExtraPermissions                    com.oculus.extrapermissions                             false    true
Federated Computing Services        com.meta.federatedcomputing.oculus                      false    true
Files                               com.android.documentsui                                 false    true
Final Soccer                        com.ivanovichgames.finalkickVR                          false    false
FireZoneVR                          com.SoaringRocStudio.FireZoneVR                         false    false
First Hand                          com.oculus.samples.firsthand                            false    false
```

Figura 2.9. Ieșirea comenzii App List care afișează lista serviciilor de sistem din mediul software instalat pe dispozitiv. Acest lucru poate permite unui actor rău intenționat să găsească vulnerabilități în serviciile care rulează și să le compromită.

✓ Scenariul 2: Ascultări și supraveghere prin Oculus Quest 2

Al doilea scenariu descrie un atac care implică ascultarea și supravegherea neautorizată a aplicațiilor Oculus Quest 2 și AR pe Android, exploatând permisiuni de utilizator configurate greșit prin inginerie socială. Atacul a utilizat Storm Breaker, combinat cu redirecționarea porturilor Ngrok, pentru a configura un link de phishing malițios, după cum se arată în Figura 2.10. Atunci când victima a făcut clic pe link, aceasta a permis atacatorilor, în necunoștință de cauză, accesul la componente sensibile ale dispozitivului, cum ar fi microfonul, camera foto și datele de localizare, evidențiind riscurile prezentate de setările incorecte ale permisiunilor și de tacticile înșelătoare.

Figura 2.10. Interfața serverului Storm Breaker cu portul 2525 deschis care redirecționează traficul prin Ngrok

- **Componentele atacului și detaliile de execuție**

Componentele implicate în scenariul 2, împreună cu executarea pas cu pas a fiecărui atac, sunt prezentate mai jos.

1. **Atac de urmărire a locației**

În acest scenariu, este transmis un link malițios care solicită utilizatorilor să localizeze prietenii din apropiere pe dispozitivele lor XR. La apăsarea linkului malițios prin intermediul browserului Oculus, informațiile despre dispozitivul utilizatorului și coordonatele precise de geolocalizare și informațiile despre dispozitiv au fost capturate și transmise atacatorului, oferindu-i acestuia capacități de localizare în timp real (Figura 2.11).

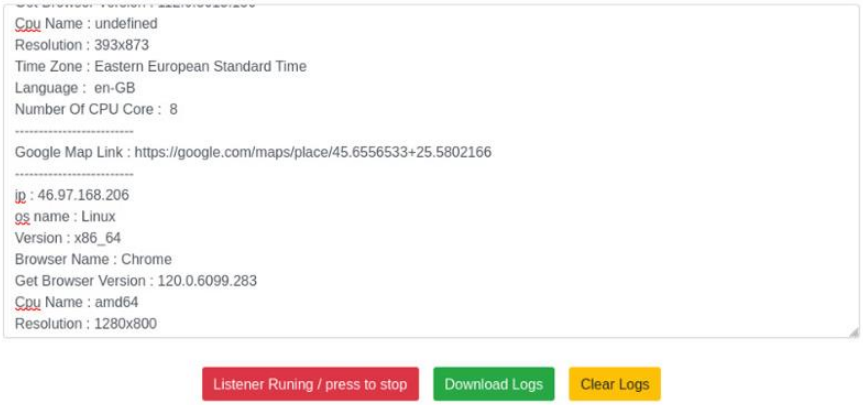

Figura 2.11. Livrarea cu succes a informațiilor de urmărire a locației prin intermediul panoului de administrare al întrerupătorului de furtună

2. Atac de deturnare a microfonului

În atacul de deturnare a microfonului, un link malițios solicita în mod înșelător permisiuni pentru microfon, prezentându-se ca o funcție vocală XR legitimă. La acordarea permisiunii, utilizatorii permiteau atacatorilor, fără să știe, să înregistreze și să transmită în mod continuu conversațiile lor către un server de la distanță. Această supraveghere secretă a persistat până când utilizatorul a închis manual browserul, de obicei fără să știe că este înregistrat (ilustrat în Figura 2.12).

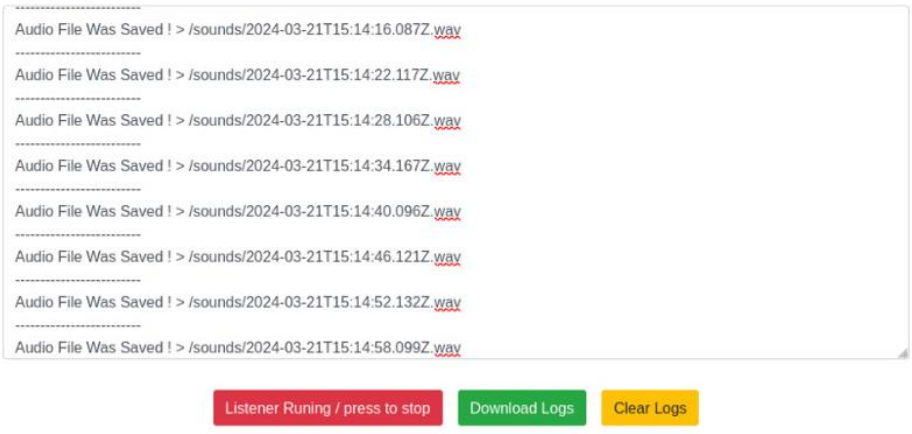

Figura 2.12. Conversații audio înregistrate livrate serverului de ascultare ca urmare a atacului microfonului

3. Deturnarea camerei prin intermediul unui dispozitiv AR

Un link malițios a păcălit utilizatorii să acorde, în necunoștință de cauză, acces la camera foto de pe un dispozitiv AR, permițând atacatorilor să capteze în secret imagini și clipuri video fără știrea victimei. Media capturată a fost colectată de atacator prin intermediul panoului de administrare Storm Breaker din Figura 2.13.

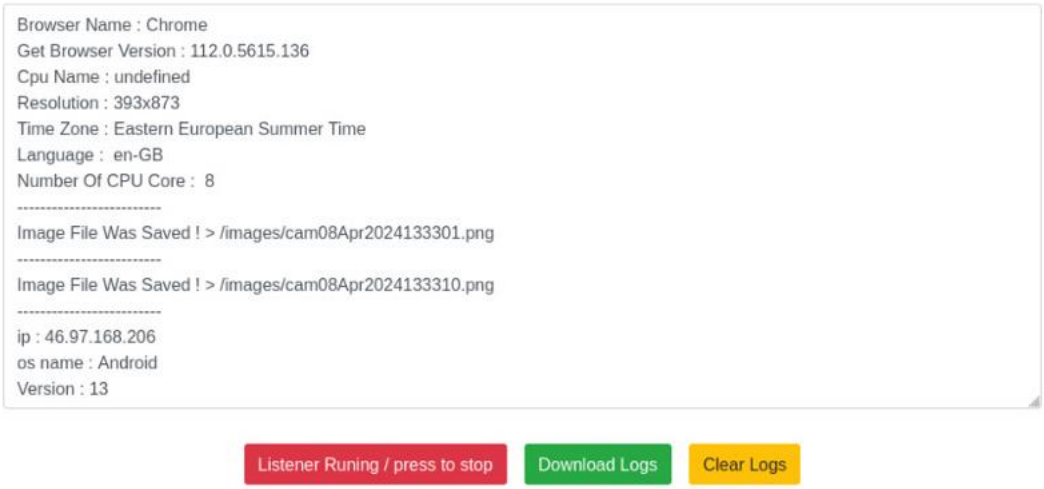

Figura 2.13. Panoul de administrare afișează fișierul imagine primit ca urmare a atacului asupra camerei

2.6.3 Amenințările identificate și vulnerabilitățile acestora

Scenariul 1 evidențiază următoarele amenințări:

- ✓ Remote Code Execution - Vulnerabilitatea exploatată este "Malicious APK execution enables arbitrary code execution"
- ✓ Inginerie socială prin phishing - Vulnerabilitatea exploatată este "lipsa de conștientizare a utilizatorului".
- ✓ Instalarea nesigură a aplicației - Vulnerabilitatea exploatată este "abuzul excesiv de permisiuni".
- ✓ Acces neautorizat și exfiltrare de date - Vulnerabilitatea exploatată este "Expunerea de informații sensibile (fișiere, mesaje, contacte)".

Scenariul 2 evidențiază următoarele amenințări:

- ✓ Ascultări prin microfon - Vulnerabilitatea exploatată este "controlul slab al permisiunilor microfonului".
- ✓ Inginerie socială prin phishing - Vulnerabilitatea exploatată este "*lipsa de conștientizare*".
- ✓ Supraveghere prin intermediul camerei - Vulnerabilitatea exploatată este "niciun indicator persistent al camerei".
- ✓ Urmărirea locației în timp real - Vulnerabilitatea exploatată este "lipsa unor reguli stricte de acces la locație".

2.6.4 Evaluarea riscurilor de securitate cibernetică

Această secțiune completează cazul de utilizare prin efectuarea unei evaluări a riscurilor de securitate cibernetică, cuantificând amenințările, vulnerabilitățile și impactul identificate în conformitate cu triada CIA. Modelele consacrate, cum ar fi calculatorul CVSS NVD și standardele NIST, au fost combinate cu un model personalizat pentru a calcula probabilitatea și scorurile de risc global pentru cele două scenarii descrise.

1. **Analiza riscurilor**

Riscul este definit ca pierderea potențială care rezultă din combinația dintre probabilitatea atacului, vulnerabilitatea exploatată și impactul potențial [45]. Principalul obiectiv al analizei riscurilor este de a evalua impactul amenințărilor și de a evalua cât de eficiente ar putea fi diferitele căi de atac [13].

Riscul este calculat pe baza următoarei formule: Risc = Amenințare * Vulnerabilitate * Impact.

Evaluarea riscurilor integrează CVSS pentru a măsura gravitatea și impactul potențial al fiecărei vulnerabilități. Pentru a determina valorile probabilității, a fost utilizat un model personalizat dezvoltat special pentru scenariile de atac legate de RV. Pe baza factorilor definiți pentru model, probabilitatea este acalculată astfel

$$Likelihood = \frac{(3 * \text{UBS}) + (2 * \text{VEE}) + (3 * \text{APA})}{100}$$

2. **Rezultatele analizei riscurilor**

Scorul de risc pentru fiecare amenințare identificată a fost calculat folosind formula:

$$Risk = Likelihood * Vulnerability * impact$$

Tabelul 2.2. Scorul final de risc calculat care detaliază impactul asupra CIA și gravitatea acestuia

Amenințări	C	I	A	Probabilitate	Vulnerabilitate	Impact	Scorul de risc (2)	Severitate
Instalarea nesigură a aplicațiilor	√	√		0.75	7.3	5.5	30	Înaltă
Inginerie socială	√	√		0.79	8.8	5.3	37	Înaltă
Execuție de cod la distanță (RCE)	√	√	√	0.79	8.8	5.9	41	Înaltă
Acces neautorizat și exfiltrare de date	√	√		0.73	8.2	4.2	25	Mediu
Ascultări	√			0.70	6.5	3.6	16	Scăzut
Supraveghere	√			0.64	6.5	3.6	15	Scăzut

Urmărirea locației	√			0.62	6.5	3.6	15	Scăzut

Rezultatele evidențiază faptul că execuția de cod la distanță (RCE), ingineria socială și instalarea nesigură a aplicațiilor reprezintă cele mai grave riscuri în mediile XR, afectând în principal integritatea și disponibilitatea sistemului. Amenințările legate de confidențialitate, cum ar fi ascultarea, supravegherea și urmărirea locației sunt încă semnificative, dar mai puțin critice (Figura 2.14).

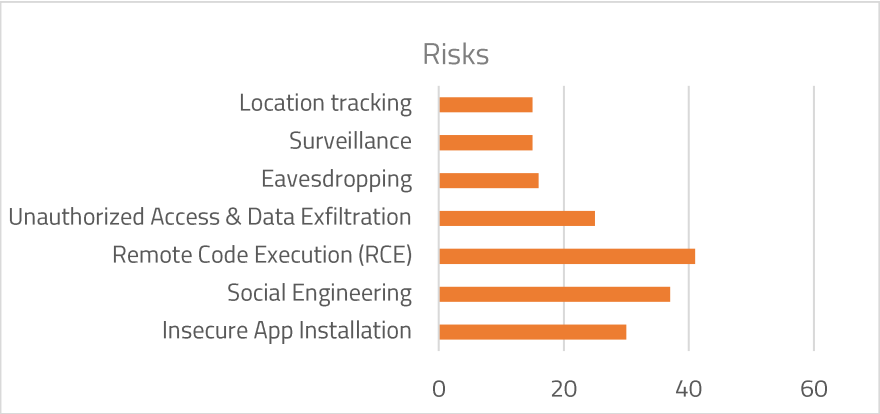

Figura 2.14. O prezentare vizuală a riscurilor pentru o mai bună comparare

2.7. Concluzie

Capitolul îndeplinește obiectivele 1-3 prin identificarea vulnerabilităților RV, analizarea amenințărilor și validarea riscurilor prin studii de caz. Acesta oferă o explorare cuprinzătoare a amenințărilor la adresa securității cibernetice în mediile de realitate virtuală, oferind o înțelegere detaliată a riscurilor care rezultă din natura imersivă și interactivă a RV. Ea introduce o taxonomie structurată care clasifică amenințările atât în funcție de principiile de bază ale securității cibernetice CIA, cât și de vectorii de atac, cum ar fi vulnerabilitățile rețelei, accesul neautorizat și ingineria socială. Acest cadru dual umple un gol critic în literatura existentă și pune bazele viitoarelor cercetări și elaborări de politici în domeniul securității RV.

De asemenea, acesta analizează strategiile actuale de atenuare, inclusiv criptarea, detectarea intruziunilor, autentificarea și modelele de încredere zero. Prin contextualizarea amenințărilor noi și existente într-o taxonomie structurată, capitolul pregătește terenul pentru construirea unor cadre de securitate RV cuprinzătoare în cercetările ulterioare, subliniind urgența securizării platformelor RV pe măsură ce utilizarea lor se extinde.

În plus, capitolul atrage atenția și asupra amenințărilor emergente, specifice RV, inclusiv manipularea chaperonilor, atacurile de inițiere și deturnarea identității. Prin contextualizarea acestora în cadrul sistemelor imersive, capitolul îmbunătățește înțelegerea modului în care astfel de atacuri afectează siguranța, încrederea și confidențialitatea utilizatorilor. Se extinde această analiză printr-un studiu de

caz real care implică o platformă de jocuri RV, demonstrând modul în care pot apărea vulnerabilități precum expunerea PII și oferind perspective practice pentru evaluarea securității.

Dincolo de identificarea amenințărilor, capitolul analizează strategiile actuale de atenuare, inclusiv tehnicile de criptare, detectarea intruziunilor bazate pe inteligență artificială, autentificarea biometrică și cu factori multipli, protecțiile bazate pe hardware și învățarea federată pentru păstrarea confidențialității. Aceste metode reprezintă stadiul actual al tehnologiei în materie de securizare a tehnologiilor imersive.

În general, acest capitol pune bazele dezvoltării unor cadre de securitate eficiente adaptate la RV. Acesta îndeplinește obiectivele inițiale ale tezei prin identificarea riscurilor cheie, validarea acestora prin analize empirice și explorarea strategiilor de atenuare atât tehnice, cât și comportamentale.

Capitolul 3. Echilibrarea utilizabilității, experienței utilizatorului, securității și confidențialității în sistemele de RV

Pornind de la rezultatele capitolului 2, acest capitol abordează obiectivul 4 prin examinarea relației complexe dintre utilizabilitate, experiența utilizatorului, securitate și confidențialitate în sistemele de RV.

Capitolul adoptă o abordare multifațetată, integrând analiza teoretică cu perspective practice derivate din studii de caz din lumea reală și un studiu empiric al utilizatorului pentru a determina compromisurile dintre factorii studiați în vederea atingerii unui echilibru delicat. Acesta contribuie la teză prin:

- Furnizarea unui cadru holistic pentru integrarea usabilității, UX, securității și confidențialității în mediile RV.
- Elaborarea unui model conceptual pentru a identifica punctele de intersecție dintre utilizabilitate, UX, securitate și confidențialitate.
- Folosind analiza de date bazată pe Python, capitolul evaluează cantitativ relația dintre acești patru factori.

3.1. Definirea termenilor

1. **Utilizabilitatea**

Utilizabilitatea este un aspect fundamental pentru orice produs conceput pentru interacțiunea umană. Unul dintre cele mai adoptate instrumente de măsurare a utilizabilității este Scala de utilizabilitate a sistemului, un chestionar conceput pentru a evalua percepțiile utilizatorilor cu privire la utilizabilitate [46]. Cu alte cuvinte, utilizabilitatea este capacitatea unui anumit utilizator de a utiliza un anumit sistem pentru a atinge anumite obiective cu succes, în mod eficient și satisfăcător într-un context de utilizare clar definit [47].

2. **Experiența utilizatorului**

Experiența utilizatorului (UX) descrie modul în care o persoană se simte sau răspunde la un produs, sistem sau serviciu după ce îl utilizează sau anticipează utilizarea acestuia [48]. În plus, într-un anumit context de utilizare, UX reală este realizată atunci când utilizatorii pot obține utilizabilitate, siguranță și satisfacție [49].

3. Securitate

Elaborarea de măsuri de contracarare a atacurilor cibernetice trebuie să respecte principiile de confidențialitate, integritate și disponibilitate (CIA). Securitatea este un set de măsuri care protejează CIA de securitatea informațiilor [12].

4. Confidențialitate

Multe persoane nu sunt conștiente și nu înțeleg clar drepturile lor în materie de confidențialitate și, adesea, au așteptări reduse sau inexistente cu privire la confidențialitate. Acest lucru duce la alegeri greșite atunci când se confruntă cu decizii privind confidențialitatea. Măsurile de protecție a vieții private oferă utilizatorilor controlul asupra datelor colectate, a modului în care acestea sunt prelucrate și stocate.

3.2. Atingerea unui echilibru între utilizabilitate, experiența utilizatorului, securitate și confidențialitate în RV

Echilibrul dintre utilizabilitate și UX, pe de o parte, și securitate și confidențialitate, pe de altă parte, este esențial în proiectarea și punerea în aplicare a sistemelor RV. Sistemele RV nu ar trebui să ofere pur și simplu măsuri de securitate și confidențialitate ca caracteristici izolate, ci să le integreze perfect în însăși structura UX [50]. Utilizatorii, în timp ce sunt absorbiți de scenele imersive ale RV, ar trebui, de asemenea, să fie protejați de potențiale amenințări și încălcări ale securității datelor pentru a crea încredere [51]. Realizarea acestei armonii necesită luarea în considerare atentă a fiecărui element de design, securitate, interacțiune cu utilizatorul și protecție a vieții private.

3.2.1 Conceptul de experiență a utilizatorului și utilizabilitate în sistemele RV

Sistemele RV promit în mod normal o experiență imersivă și un sentiment de prezență. Prin urmare, după ce o persoană interacționează cu un sistem RV, experiența ar trebui să fie memorabilă, astfel încât utilizatorul să fie mulțumit de imersiune și să povestească senzația de a fi acolo. În plus, sistemul RV trebuie să fie ușor de utilizat de către utilizator și să fie capabil să creeze o adevărată imersiune participativă pentru a produce experiențe inovatoare [52].

Utilizarea simplă a sistemului de RV este principalul obiectiv al garantării unei UX satisfăcătoare. Proiectarea unei interfețe RV utilizabile care să acorde prioritate ușurinței de utilizare trebuie să ia în considerare interacțiunea, navigarea și feedback-ul. Utilizabilitatea este un aspect crucial al UX. În RV, o utilizare deficitară poate întrerupe imersiunea, diminuând experiența generală. Deși utilizabilitatea și UX sunt strâns legate și ambele sunt legate de factorii umani, utilizabilitatea este un subset cheie al UX. Figura 3.1 prezintă elementele care alcătuiesc UX în sistemele RV. Având în vedere elementele de utilizabilitate, acestea au o influență directă asupra UX în RV.

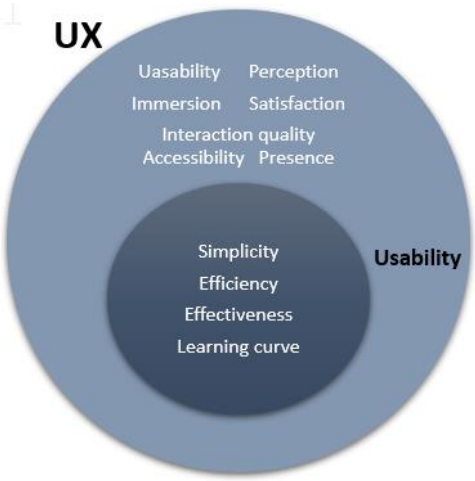

Figura 3.1. Relația dintre UX și utilizabilitate

3.2.2 Relația dintre utilizabilitate, UX, securitate și confidențialitate

În timp ce asigurarea protecției datelor și prevenirea riscurilor potențiale sunt esențiale [51], conceperea unor sisteme RV pe care utilizatorii să le găsească intuitive, captivante și captivante este la fel de esențială. Figura 3.2 prezintă un model care relevă relația dintre utilizabilitate, UX, securitate și confidențialitate în RV.

În timp ce securitatea se concentrează pe autentificare, criptare și măsuri de protecție împotriva accesului neautorizat [53], confidențialitatea cuprinde gestionarea etică a informațiilor personale, asigurând conformitatea cu standardele legale și de reglementare [54]. Cu toate acestea, ele se pot suprapune în anumite situații. Securizarea datelor sensibile într-un mediu RV este esențială pentru realizarea securității și a confidențialității. Pe de altă parte, securitatea și UX se suprapun în ceea ce privește integritatea și confidențialitatea. Interacțiunea și percepția de securitate nu ar trebui să fie manipulate sau accesate de utilizatori neautorizați. Manipularea malițioasă a intrărilor senzoriale sau gestionarea ilegală a interacțiunilor pot fi utilizate pentru a înșela utilizatorii, a provoca dezorientare și chiar răni fizice[17].

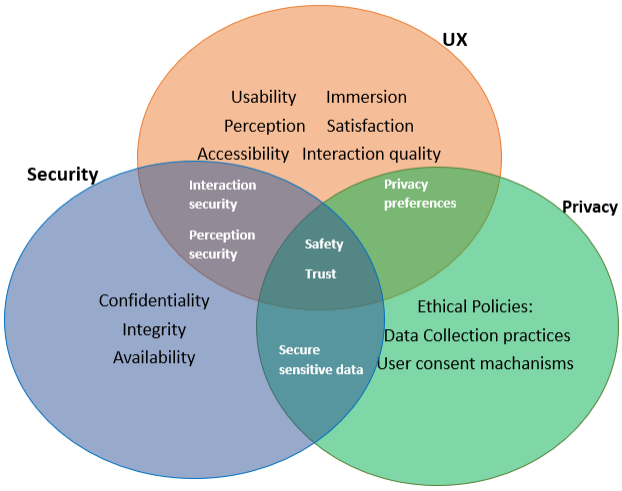

Figura 3.2. Un model care descrie relația dintre UX, utilizabilitate, securitate și confidențialitate în sistemele RV

Între timp, UX și confidențialitatea se întâlnesc cu preferințele utilizatorilor, care ar trebui să aibă control asupra datelor lor, să le șteargă, să permită permisiuni sau să le refuze.

3.2.3 Metodologia și rezultatele studiului de caz

A fost efectuat un studiu de utilizare folosind setul cu cască Oculus Quest 2 și aplicația vTime VR. Treisprezece participanți au testat scenarii predefinite legate de autentificare, personalizarea avatarului, mesagerie și controlul confidențialității. Rezultatele au indicat mai multe provocări: lipsa navigării intuitive, organizarea deficitară a mesajelor și explicații insuficiente privind confidențialitatea. Participanții și-au exprimat îngrijorarea cu privire la accesul neautorizat și utilizarea abuzivă a datelor din cauza absenței opțiunilor de deconectare și a protecției slabe a contului. În ciuda acestor probleme, mulți au apreciat experiența vizuală imersivă și bazată pe gesturi. Opiniile utilizatorilor sunt raportate cu privire la confidențialitatea căștilor (Figura 3.3). Opiniile participanților cu privire la platforma RV sunt ilustrate în Figura 3.4 pentru utilizabilitate, Figura 3.5 pentru UX, Figura 3.6 pentru securitate și Figura 3.7 pentru confidențialitate.

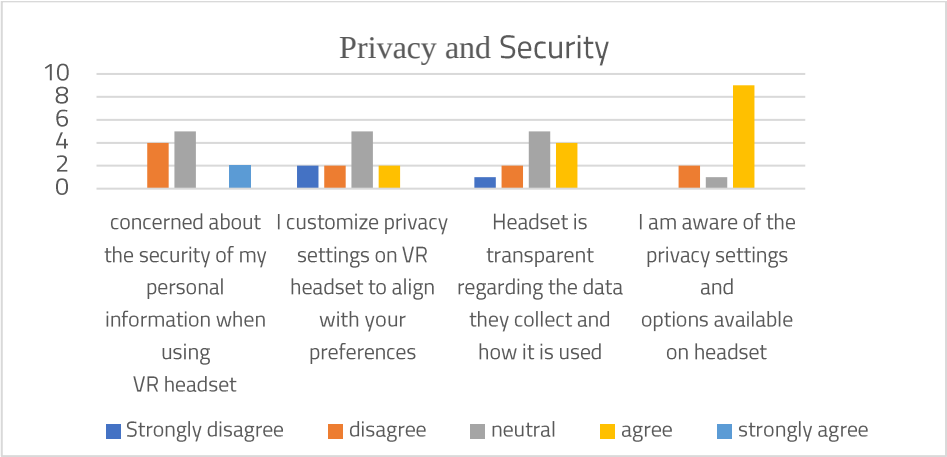

Figura 3.3. Prezentarea statistică a opiniilor participanților cu privire la confidențialitate atunci când folosesc căștile de RV

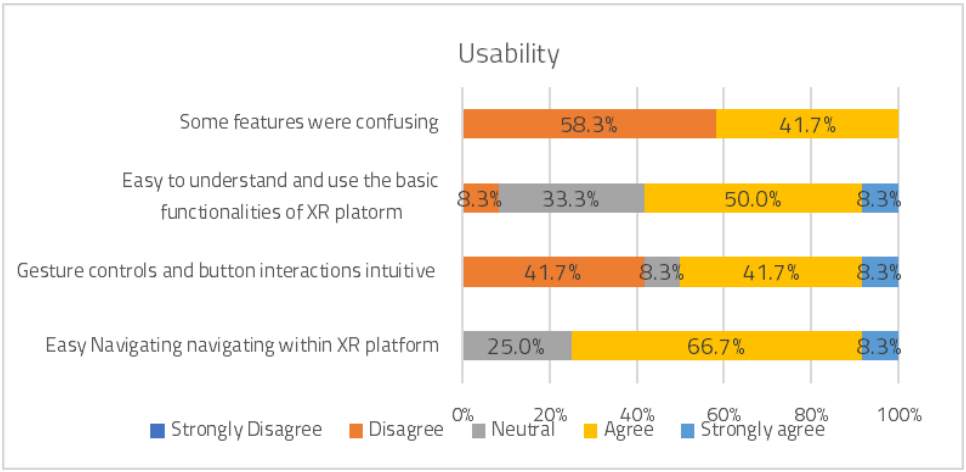

Figura 3.4. Prezentarea statistică a opiniilor participanților cu privire la utilitatea în cadrul platformei de RV

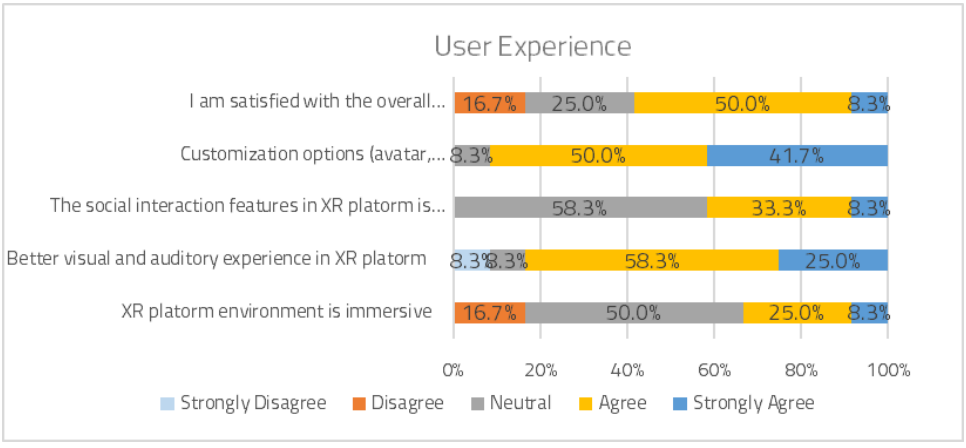

Figura 3.5. Prezentarea statistică a opiniilor participanților cu privire la UX în cadrul platformei de RV

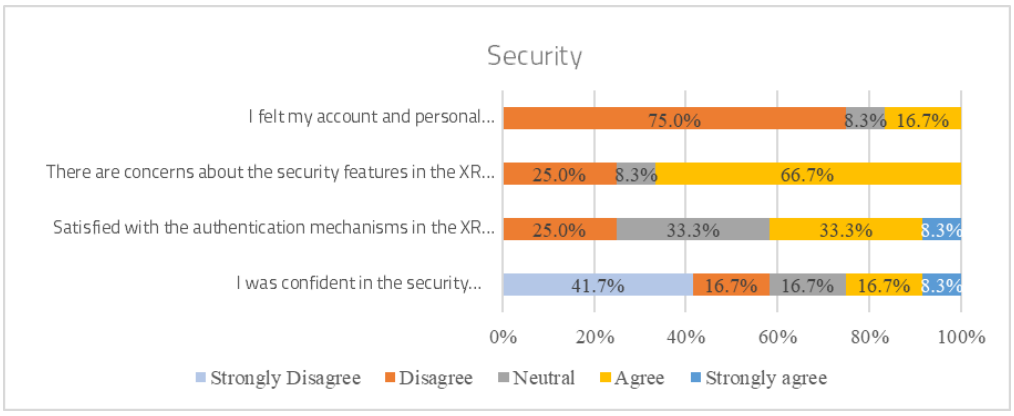

Figura 3.6. Prezentarea statistică a opiniilor participanților privind securitatea în cadrul platformei de RV

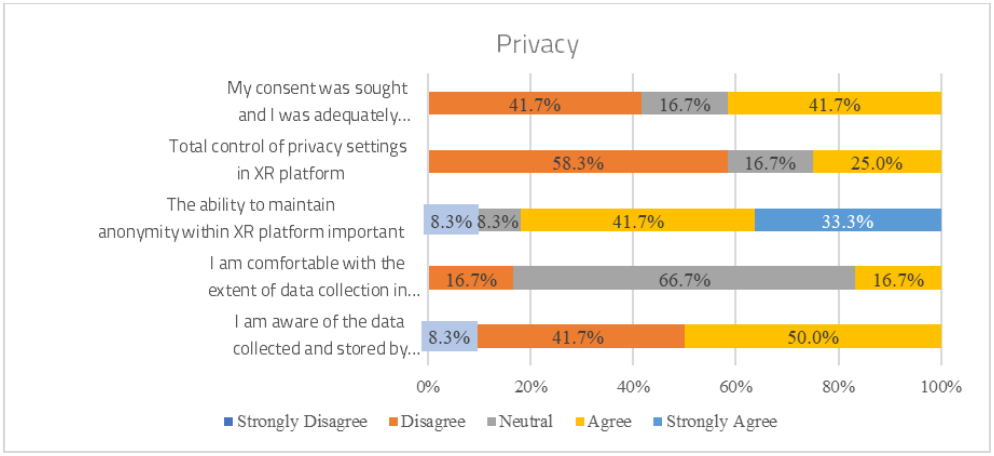

Figura 3.7. Prezentarea statistică a opiniilor participanților cu privire la confidențialitate în cadrul platformei de RV

3.2.4 Corelația dintre variabilele utilizate pentru studiu

Folosind analiza datelor bazată pe Python, corelațiile dintre variabile au arătat o relație moderată între confidențialitate și UX (0,32), indicând faptul că utilizatorii apreciază confidențialitatea ca fiind o componentă a experienței lor generale. În același timp, corelațiile mai slabe dintre securitate și utilitate (0,14) au evidențiat importanța proiectării unor caracteristici de securitate care să nu deranjeze.

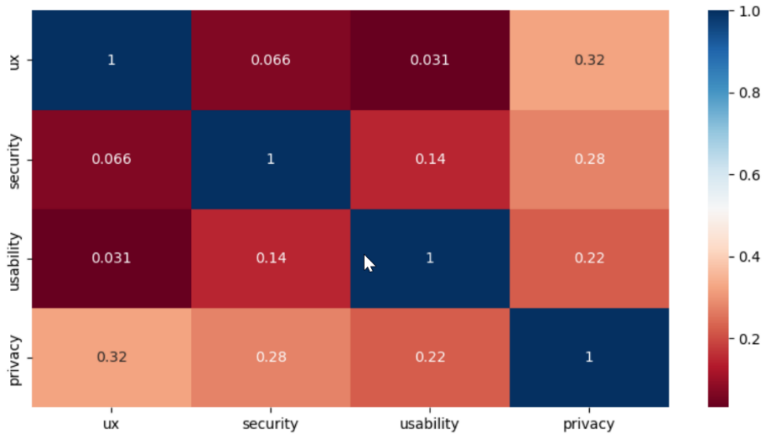

Figura 3.8. Harta termică a corelațiilor pentru aplicația de RV

3.3. Concluzie

Capitolul propune un model conceptual care cartografiază zonele de suprapunere ale acestor patru elemente, oferind recomandări practice de proiectare, cum ar fi autentificarea biometrică, permisiunile adaptive, notificările de confidențialitate în timp real și educația utilizatorilor prin gamificare.

În concluzie, capitolul demonstrează că, deși utilizabilitatea, UX, securitatea și confidențialitatea sunt distincte, acestea trebuie abordate holistic. O integrare echilibrată a tuturor celor patru conduce la experiențe RV mai demne de încredere, mai sigure și mai imersive. Aceste constatări oferă un cadru strategic pentru proiectanții, dezvoltatorii și cercetătorii care lucrează pentru a crea sisteme imersive sigure, dar fără cusur.

Studiul a adus următoarele

- **Cadru de integrare holistică**: A propus un cadru multidimensional care armonizează utilizabilitatea, experiența utilizatorului (UX), securitatea și confidențialitatea în mediile de RV, asigurându-se că experiențele imersive nu sunt compromise de măsurile de securitate.
- **Studiu de caz empiric**: Am efectuat un studiu real cu 13 participanți care au folosit vTime VR pe Oculus Quest 2, oferind informații practice despre modul în care utilizatorii interacționează cu sistemele de RV în ceea ce privește securitatea, utilitatea și confidențialitatea.
- **Dezvoltarea modelului conceptual**: A introdus un model conceptual care cartografiază suprapunerile și compromisurile dintre utilizabilitate, UX, securitate și confidențialitate pentru a ghida proiectarea echilibrată a sistemului.
- **Identificarea conflictelor**: Au fost identificate și analizate conflictele cheie de utilizare-securitate, cum ar fi autentificarea intruzivă sau controalele neclare privind confidențialitatea, care pot împiedica imersiunea și încrederea în sistemele de RV.
- **Analiza cantitativă a corelației**: Am efectuat o analiză de corelație bazată pe Python care a arătat că confidențialitatea și UX sunt corelate moderat, subliniind faptul că funcțiile de

îmbunătățire a confidențialității pot îmbunătăți experiența utilizatorului fără a compromite utilitatea.

Capitolul 4. Autenticitatea și integritatea artefactelor virtuale în mediile imersive

Acest capitol abordează obiectivul 5 prin examinarea utilizării semnăturilor digitale pentru a asigura autenticitatea și integritatea datelor, cu accent pe aplicarea lor în securizarea artefactelor virtuale în mediile de RV.

Capitolul contribuie la teză prin:

- A implementat o soluție criptografică într-un spațiu de RV care permite utilizatorilor să semneze bunuri virtuale și să verifice autenticitatea acestora în timp real.
- Oferirea unei abordări centrate pe utilizator în ceea ce privește securitatea, prin oferirea de metode de securitate utilizatorilor finali în medii imersive pentru a-și proteja bunurile.

4.1. Conceptul de semnătură digitală

Semnăturile digitale sunt un domeniu al criptografiei, dedicat securizării informațiilor prin asigurarea confidențialității, integrității, autenticității și nerepudierii datelor [55]. Criptografia realizează acest lucru prin criptare, pentru a converti textul într-un format codificat, și prin decriptare, pentru restabilirea datelor originale, împiedicând accesul neautorizat.

Tehnicile criptografice sunt clasificate de obicei în două categorii principale: criptografia simetrică și asimetrică [56]. Criptografia asimetrică, cunoscută și sub denumirea de criptografie cu cheie publică, utilizează o pereche de chei - o cheie publică și o cheie privată. Acest mecanism cu două chei sporește securitatea, în special în cazul semnăturilor digitale și al comunicațiilor securizate.

Semnăturile digitale, bazate pe criptografia cu cheie publică, asigură autenticitatea, integritatea și nerepudierea datelor [57]. Acestea utilizează o pereche de chei private-publice și un algoritm de hashing precum SHA-256. Din mesajul original și criptat cu cheia privată a expeditorului se creează un hash (digest al mesajului) [58]. Destinatarul utilizează cheia publică a expeditorului pentru a verifica semnătura prin compararea valorilor hash. Dacă hash-urile corespund, mesajul este confirmat ca fiind autentic și neschimbat [56]. Figura 4.1. ilustrează procesul de generare și verificare a unei semnături digitale, de la expeditor la destinatar.

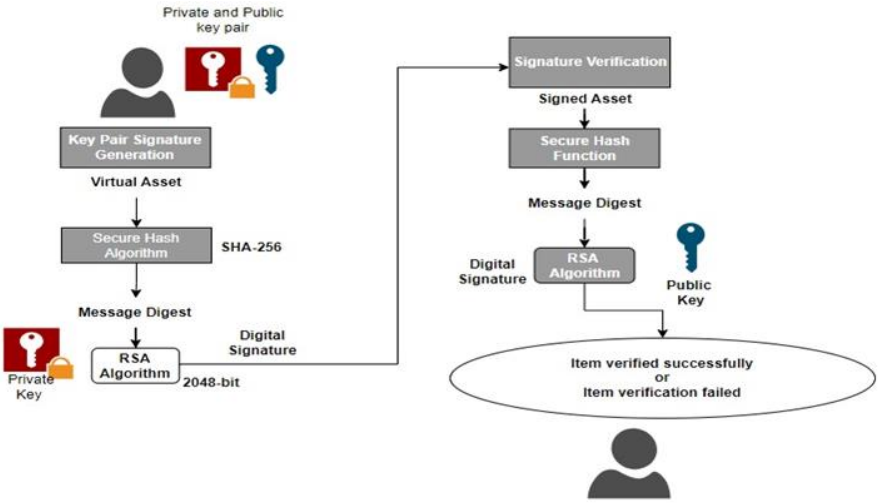

Figura 4.1. Procesul semnăturii criptografice

4.2. Rolul autenticității și integrității în securizarea bunurilor virtuale în spațiile de RV

Un element central al mediilor de RV este activul virtual, care îmbunătățește atât imersiunea, cât și UX [59]. În acest studiu, definim activele virtuale ca avatare personalizate, proprietăți imobiliare virtuale, opere de artă digitale, elemente de joc și alte obiecte interactive [60]. Deși sunt esențiale pentru experiențele RV imersive, activele virtuale se confruntă cu amenințări precum falsificarea și modificarea neautorizată [61]. Soluțiile existente, precum blockchain și asigurarea bunurilor digitale, sunt adesea complexe sau costisitoare, în special pentru utilizatorii individuali [62].

Această secțiune subliniază necesitatea unor metode accesibile și ușor de utilizat pentru a asigura autenticitatea și integritatea activelor virtuale. Dovedirea autenticității ar putea fi mai simplă în lumea fizică decât în lumea virtuală. În modelele de afaceri tradiționale, tranzacțiile sunt validate cu ajutorul semnăturilor sau sigiliilor fizice, care certifică și ratifică acordurile din punct de vedere juridic. Cu toate acestea, în ecosistemele digitale, autenticitatea și integritatea sunt de obicei asigurate prin semnături criptografice [63]. Construită pe hashing criptografic și criptografie cu cheie publică, semnătura digitală este o soluție ușoară și eficientă. Prin integrarea semnăturilor digitale în interacțiunile RV, utilizatorii pot verifica proprietatea și detecta manipulările în timp real, sporind încrederea și securitatea fără a compromite imersiunea.

4.3. Soluție propusă centrată pe utilizator pentru semnarea și verificarea activelor în timp real în spațiile RV

Această secțiune prezintă un sistem practic, ușor de utilizat, care integrează semnăturile digitale criptografice în mediile RV pentru a asigura autenticitatea și integritatea bunurilor virtuale. Construită folosind Unity 3D și RSA-2048 cu hashing SHA-256, soluția permite utilizatorilor să semneze și să verifice elemente digitale în timp real folosind simple intrări ale controlerului: butonul A pentru

semnare, butonul B pentru verificare, fără a necesita cunoștințe tehnice. Principala arhitectură a sistemului este ilustrată în Figura 4.3.

Fluxul de lucru stratificat al sistemului include patru straturi: interacțiunea cu utilizatorul, logica aplicației (semnare/verificare), comunicarea în rețea (Unity Netcode) și un strat criptografic pentru operațiunile de securitate, după cum se arată în Figura 4.2. Feedback-ul în timp real sporește încrederea prin avertizarea utilizatorilor cu privire la validitatea sau falsificarea semnăturii. Demonstrată în Figura 4.4 afișează răspunsul privind validitatea în interiorul camerei virtuale în timpul verificării, în timp ce Figura 4.6 și Figura 4.5 demonstrează detectarea falsificării atunci când sistemul detectează o nepotrivire în compararea valorilor hash.

Evaluările de performanță arată o eficiență ridicată, cu timpi de semnare în medie de 17.3 ms și timpi de verificare sub 1 ms. Utilizarea memoriei este minimă (4 KB per semnătură), asigurând scalabilitatea. Sistemul detectează în mod eficient falsificarea și alterarea și rămâne cripto-agil pentru viitoare integrări cu siguranță cuantică.

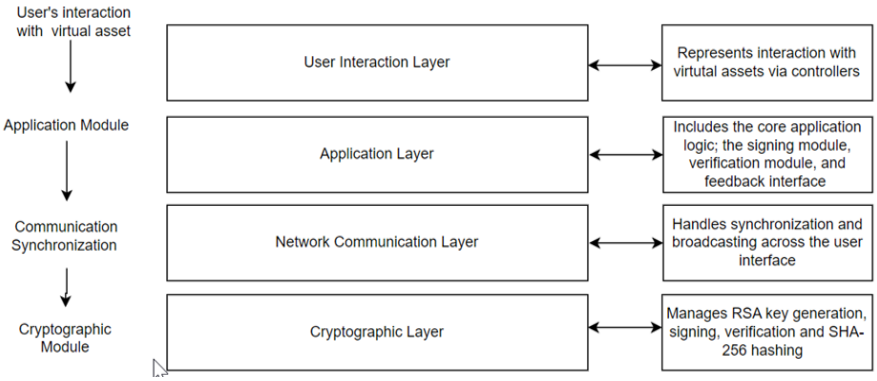

Figura 4.2. Arhitectura stratificată a sistemului de RV propus

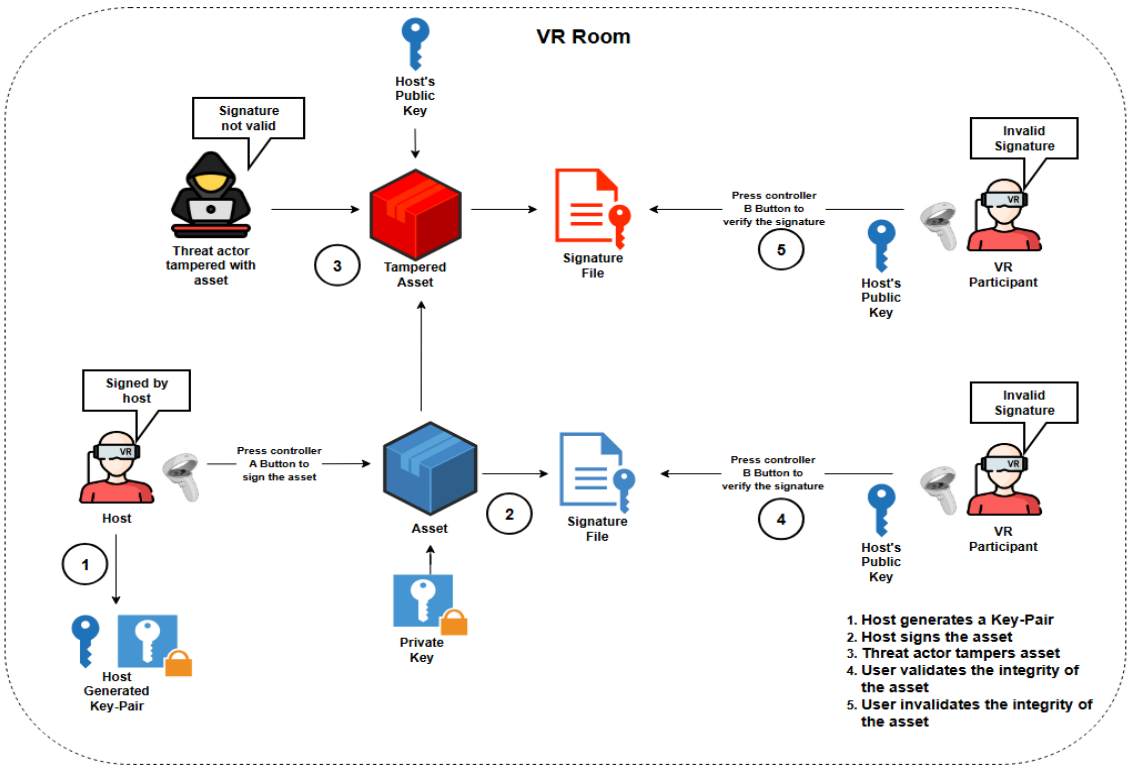

Figura 4.3. Arhitectura principală a sistemului propus

Figura 4.4. Interfața de feedback pentru utilizator afișată la detectarea manipulării

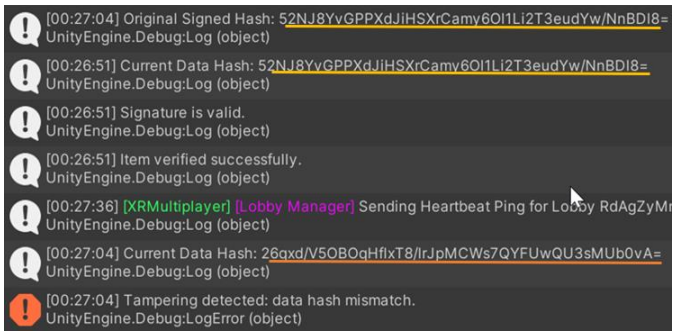

Figura 4.5. Jurnalele consolei prezintă comparația hash între datele originale și cele modificate, oferind trasabilitate pentru detectarea manipulării

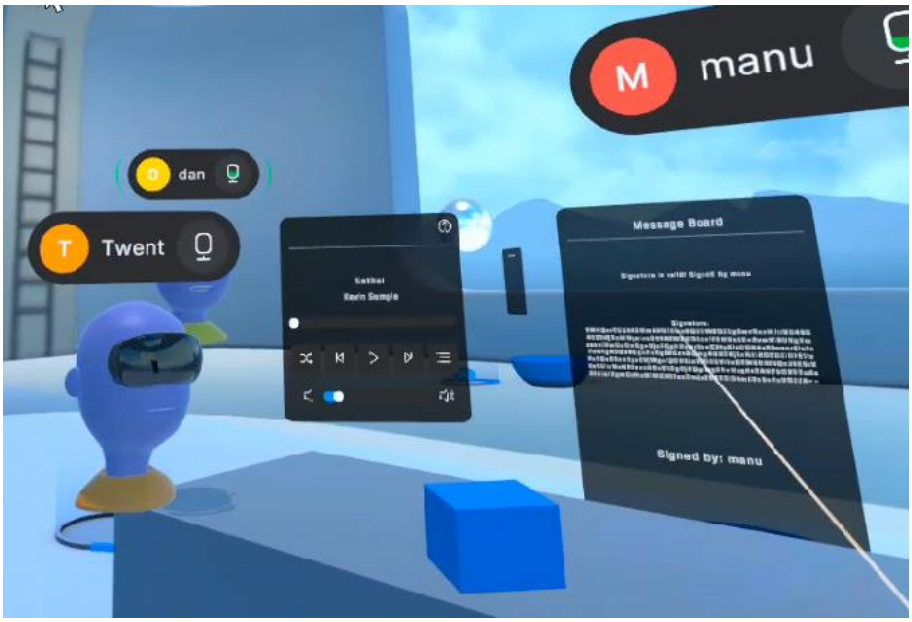

Figura 4.6. În camera virtuală, verificarea feedback-ului activelor este afișată pe tablă, cu numele semnatarului și mesajul de validitate. Semnătura este vizibilă doar în scopuri de cercetare

4.4. Concluzie

Acest capitol prezintă o soluție criptografică centrată pe utilizator pentru securizarea activelor virtuale în medii RV prin utilizarea semnăturilor digitale RSA-2048 și a hashing-ului SHA-256. Sistemul permite utilizatorilor să semneze și să verifice bunurile în mod intuitiv folosind intrările standard ale controlerului de RV, menținând atât ușurința în utilizare, cât și experiența imersivă. Acest lucru oferă un model de securitate centrat pe utilizator, care este transparent și împuternicește utilizatorii în spațiile de RV, după cum este ilustrat în Figura 4.7.

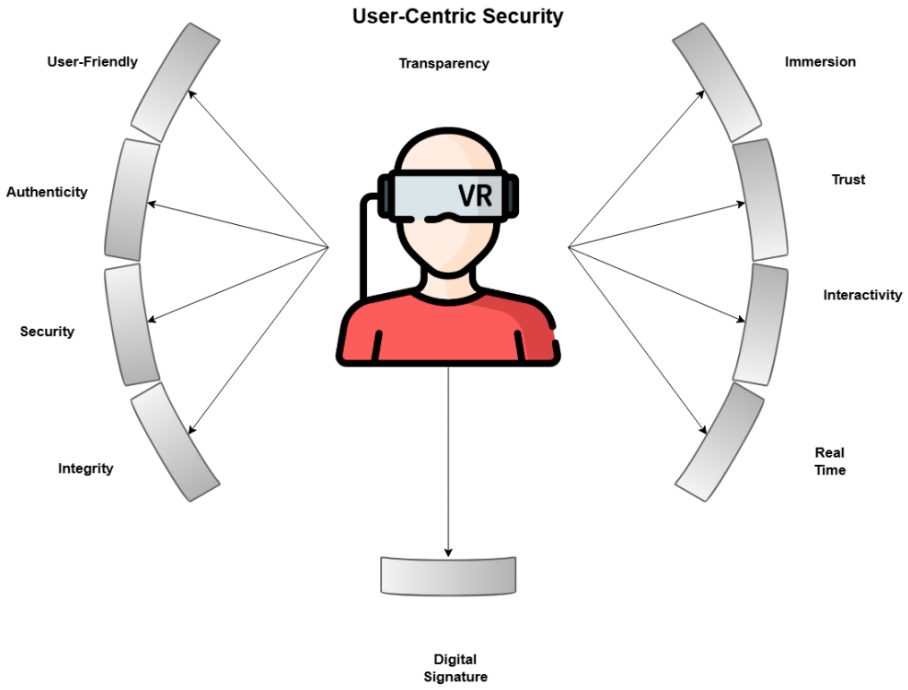

Figura 4.7. Un model centrat pe utilizator care împuternicește utilizatorii de RV prin semnături digitale

Principalele contribuții includ:

- Proiectarea și punerea în aplicare a semnăturilor digitale în timp real în RV pentru a asigura autenticitatea și integritatea.
- O concepție de securitate utilizabilă care face ca operațiunile criptografice să fie accesibile utilizatorilor non-tehnici.
- Integrare interdisciplinară care combină securitatea cibernetică, dezvoltarea RV și interacțiunea om-computer.
- O abordare centrată pe utilizator, care permite persoanelor fizice să își protejeze direct activele virtuale.
- Propunerea unor aplicații mai largi pentru semnăturile digitale în contexte RV, de la protecția identității la proprietăți imobiliare virtuale sigure.

Sistemul a demonstrat o performanță puternică, cu o latență de semnare scăzută (17,3ms), o utilizare minimă a memoriei (4KB) și o detectare eficientă a manipulării și a falsificării. Acesta oferă o bază scalabilă și rezistentă pentru interacțiunile virtuale de încredere. Privind în perspectivă, arhitectura suportă actualizări viitoare cu criptografie rezistentă la cuantică, consolidând viabilitatea sa pe termen lung în ecosistemele digitale imersive.

Această contribuție demonstrează că securitatea robustă și utilizabilă poate fi integrată în mediile imersive, oferind o bază pentru viitoarele sisteme de RV sigure, atât în contexte de active financiare, cât și nefinanciare.

Capitolul 5. Integrarea și îmbunătățirea securității în platforma GENSAVR

Platforma GENSaVR este un sistem de RV de înaltă fidelitate pentru formarea imersivă în laborator, oferind simulări sigure și interactive pentru dezvoltarea competențelor. Având în vedere natura sa multi-utilizator, aceasta necesită măsuri de securitate puternice, cum ar fi autentificarea, controlul sesiunii și monitorizarea infrastructurii pentru a proteja datele utilizatorilor și a asigura interacțiuni sigure, în timp real. Acest capitol tratează componentele și integrarea componentelor de securitate în GENSAVR pentru a spori securitatea acestuia

Capitolul contribuie la teză prin:

- Dezvoltarea unui cadru de securitate multistrat pentru platforma GENSAVR
- Asigurarea monitorizării securității infrastructurii și reducerea riscurilor.

5.1. Componente ale platformei GENSAVR

Platforma GENSAVR utilizează o arhitectură modulară de microservicii pentru a susține aplicații imersive scalabile, în timp real. Componentele cheie includ:

- **Docker**: Permite containerizarea pentru portabilitate, implementare rapidă și utilizarea eficientă a resurselor.
- **Kubernetes (K8s)**: Gestionează și scalează containerele pentru disponibilitate ridicată și toleranță la erori.
- **Nakama**: Powers: interacțiuni în timp real între mai mulți utilizatori și gestionarea utilizatorilor.
- **MageAI**: Procesează și optimizează datele în timp real pentru răspunsuri adaptive ale sistemului.
- **WebSockets și WebRTC**: Asigurați o comunicare în timp real, cu latență redusă, pentru o experiență imersivă fără întreruperi.

5.2. Integrarea securității în platforma GENSAVR

Dezvoltat inițial fără caracteristici de securitate, GENSAVR a fost îmbunătățit prin această cercetare cu un cadru de securitate robust, modular și scalabil. Principalele îmbunătățiri includ:

- Autentificare multistratificată pentru a controla accesul și a preveni utilizarea neautorizată.
- Gestionarea sesiunii care susține o experiență de utilizare fără întreruperi, prevenind în același timp deturnarea.

- Instrumente de monitorizare și conformitate în timp real pentru detectarea amenințărilor și îmbunătățirea rezilienței.

Integrarea soluțiilor de securitate a îmbunătățit semnificativ poziția de securitate a GENSAVR, făcându-l mai rezistent la amenințări, menținând în același timp performanța și utilitatea. Arhitectura GENSAVR îmbunătățită este ilustrată în Figura 5.1.

1. **Nakama: Secure Multiplayer Backend pentru GENSAVR**

Nakama este un backend multiplayer cu sursă deschisă [64] integrat în GENSAVR pentru a sprijini instruirea RV în timp real, cu mai mulți utilizatori. Acesta îmbunătățește securitatea prin autentificarea încorporată, verificarea sigură a identității, gestionarea sesiunii și controlul accesului. În plus, Nakama asigură criptarea datelor și protecția acreditărilor utilizatorilor, consolidând securitatea generală a GENSAVR și oferind un mediu de instruire sigur, scalabil și captivant.

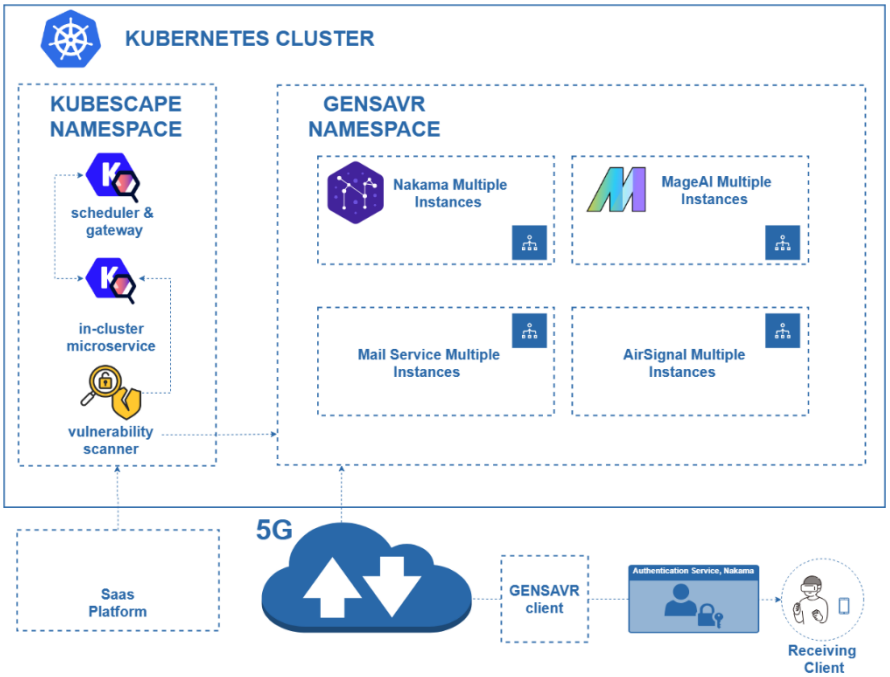

Figura 5.1. Arhitectura GENSAVR cu integrarea securității

2. **Kubescape și ARMO: Monitorizarea și conformitatea securității Kubernetes**

Kubescape este un instrument de securitate open-source integrat în GENSAVR pentru a monitoriza și proteja infrastructura Kubernetes. Acesta asigură securitatea în timpul dezvoltării, implementării și rulării prin detectarea vulnerabilităților, aplicarea conformității și sprijinirea practicilor DevSecOps [65]. Principalele caracteristici includ:

- Detectarea amenințărilor în timpul rulării.
- Scanarea vulnerabilităților clusterului.
- Integrare CI/CD.

- Aplicarea politicii.

Împreună cu ARMO, un tablou de bord vizual pentru monitorizare în timp real, această integrare consolidează postura generală de securitate a GENSAVR, permițând detectarea proactivă a amenințărilor și conformitatea pe tot parcursul ciclului său de viață.

5.2.1 Implementare și desfășurare

Această secțiune prezintă punerea în aplicare practică și implementarea mecanismului de autentificare împreună cu instrumentele de monitorizare a infrastructurii utilizate în platforma GENSAVR.

1. Îmbunătățirea autentificării cu Nakama

GENSAVR integrează un sistem de autentificare sigur, pe mai multe niveluri, folosind Nakama și Unity. Platforma acceptă autentificarea tradițională prin e-mail/parolă (Figura 5.2), autentificarea pe bază de dispozitiv pentru sesiuni persistente și gestionarea sesiunilor pe bază de jetoane cu reactualizare automată (Figura 5.3). Unity 3D asigură interfața cu utilizatorul (Figura 5.4), în timp ce Nakama gestionează operațiunile backend, cum ar fi autentificarea securizată, urmărirea sesiunii și stocarea datelor utilizatorului (Figura 5.5). Sistemul utilizează un model Singleton (Figura 5.3) pentru a gestiona sesiunile pe mai multe scene și asigură gestionarea securizată a acreditărilor. Împreună, aceste implementări oferă o experiență de conectare fără întreruperi, sigură și ușor de utilizat în mediile de formare RV imersive.

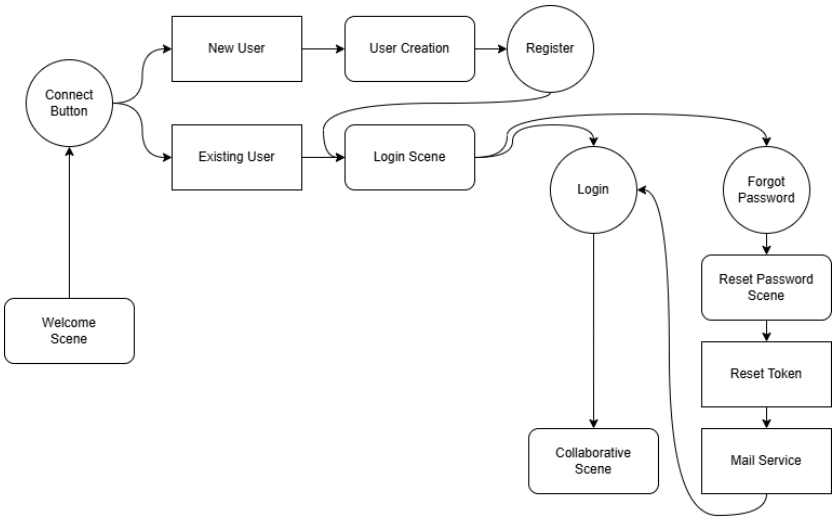

Figura 5.2. Prezentare generală a fluxului de autentificare

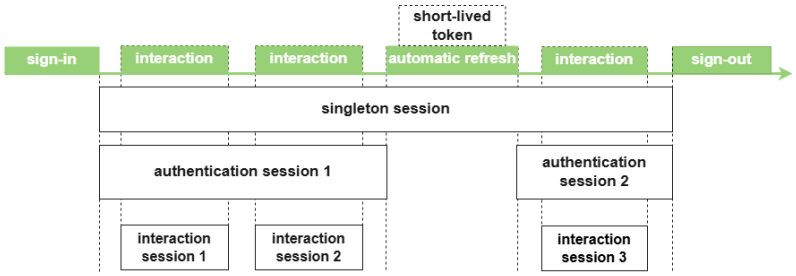

Figura 5.3. Sesiune persistentă utilizând Singleton

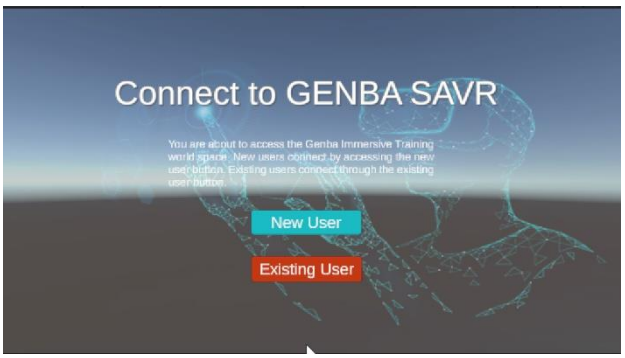

Figura 5.4. Scena AboutScene în care un utilizator este redirecționat către Scena de conectare sau către Scena de înregistrare în funcție de selecția utilizatorului dezvoltată cu Unity 3D

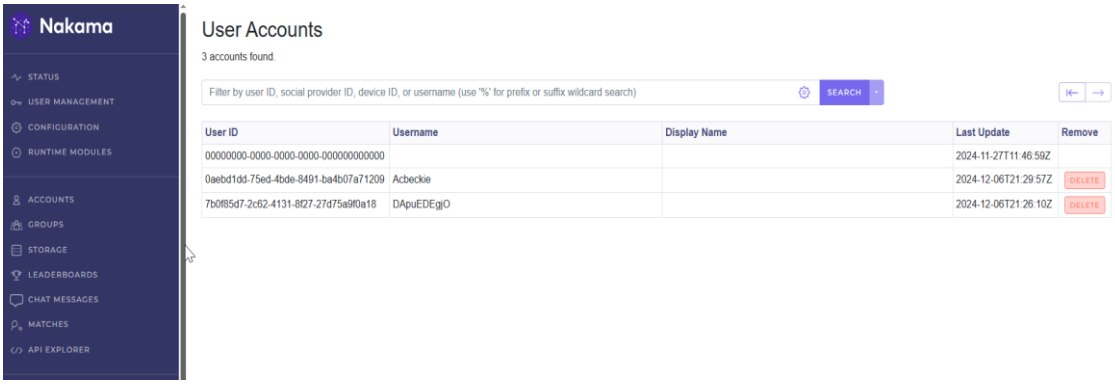

Figura 5.5. Contul utilizatorului stocat în baza de date Nakama.

2. Implementarea Kubescape pentru securitatea și monitorizarea infrastructurii

Kubescape a fost integrat în platforma GENSAVR pentru a spori securitatea infrastructurii prin detectarea vulnerabilităților, a configurațiilor greșite și a problemelor de conformitate în cadrul mediului Kubernetes. Instrumentele-cheie utilizate includ Kubescape CLI, Helm, kubectl și ARMO Dashboard. Procesul de implementare a implicat instalarea Kubescape la nivel local, implementarea operatorului Kubescape utilizând Helm și conectarea acestuia la ARMO pentru monitorizarea securității în timp real. Odată configurat, fluxul de lucru al Kubescape în GENSAVR este ilustrat în Figura 5.6. Această configurare permite scanarea continuă, aplicarea politicilor și detectarea amenințărilor, asigurându-se că GENSAVR rămâne sigur și conform pe tot parcursul ciclului său de viață.

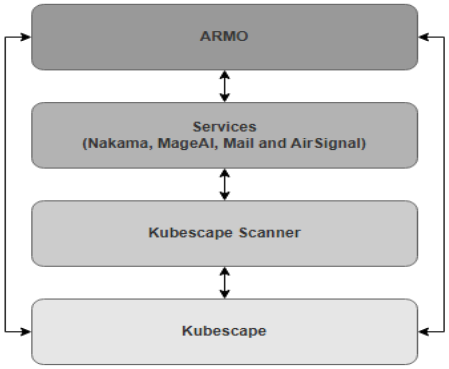

Figura 5.6. Fluxul de lucru Kubescape în GENSAVR, scanarea infrastructurii și comunicarea cu ARMO

5.2.2 Rezultatele testelor de securitate

O scanare de securitate cuprinzătoare a platformei GENSAVR utilizând Kubescape CLI și tabloul de bord ARMO a evidențiat 39 de vulnerabilități (Figura 5.7): 2 probleme critice, 6 probleme cu risc ridicat, 26 probleme cu risc mediu și 5 probleme cu risc scăzut. Majoritatea problemelor au fost de risc mediu, indicând necesitatea unei monitorizări continue. Principalele componente vulnerabile au inclus Nakama, ws-airsignal-default și serverul de e-mail.

Figura 5.7. Gradul de risc al vulnerabilităților identificate în infrastructura GENSAVR

Scorurile de conformitate au fost mari - 86,34% (MITRE) și 78,56% (NSA), după cum se arată înFigura 5.8. Preocupările majore au inclus lipsa limitelor CPU/memorie, escaladarea privilegiilor și reguli de rețea configurate greșit. Abordarea acestor constatări este esențială pentru îmbunătățirea securității și rezilienței sistemului.

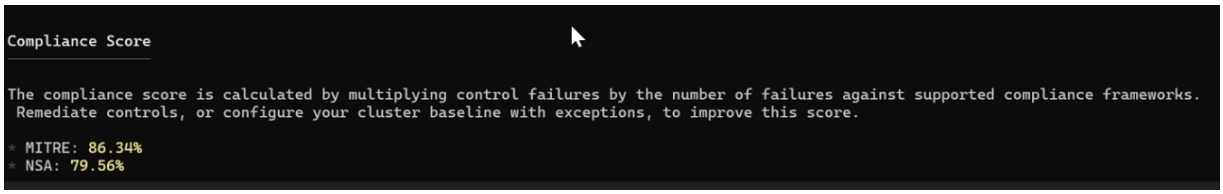

Figura 5.8. Rezultatul statisticilor pentru respectarea cadrului standard

Analiza a descoperit un potențial atac DOS prin nakama fără limite, după cum se indică în Figura 5.9 , și a sugerat remedierea ilustrată în Figura 5.10.

Figura 5.9. O ilustrare a unui atac DOS

SEVERITY	CONTROL ID	CONTROL NAME	REMEDIATION
High	C-0271	Ensure memory limits are set	Set the memory limits or use exception mechanism to avoid unnecessary notifications.
High	C-0270	Ensure CPU limits are set	Set the CPU limits or use exception mechanism to avoid unnecessary notifications.

Figura 5.10. Riscuri potențiale și remediere referitoare la Nakama

5.3. Concluzie

Studiul a introdus principiile DevSecOps în medii de RV imersive, prezentând o abordare proactivă, centrată pe utilizator, a securității platformei. Acesta creează o punte între infrastructura containerizată și cele mai bune practici moderne de securitate cibernetică, oferind un model de securitate scalabil și rezilient.

Acest capitol a contribuit la un cadru de securitate cuprinzător pentru platforma GENSAVR, îmbunătățind securitatea realității virtuale imersive prin autentificare multistratificată, gestionarea sesiunilor și monitorizarea continuă a infrastructurii. Prin integrarea Nakama pentru accesul securizat al utilizatorilor și a Kubescape cu ARMO pentru evaluarea vulnerabilității Kubernetes, platforma oferă acum o detectare îmbunătățită a amenințărilor, atenuarea riscurilor și conformitatea cu NSA.

Aceste progrese nu numai că securizează GENSAVR, dar servesc și ca referință pentru viitoarele implementări ale securității în RV. Cercetările viitoare ar trebui să exploreze simulări de atacuri reale pentru a consolida și mai mult apărarea sistemului împotriva amenințărilor din lumea reală.

Capitolul 6. Securitate adaptabilă în timp pentru confidențialitate și conformitate în aplicațiile imersive

Acest capitol abordează nevoia urgentă de confidențialitate și conformitate în Metaverse, unde utilizatorii se deplasează frecvent prin spații virtuale legate de diferite jurisdicții din lumea reală. Pe măsură ce platformele imersive se dezvoltă, protecția datelor devine complexă din cauza extinderii globale și a lipsei unei reglementări centralizate.

Studiul propune un cadru de securitate adaptiv în timp real care se aliniază dinamic la legile regionale privind confidențialitatea datelor, precum GDPR, CCPA, PIPL și altele. Acest model asigură că, pe măsură ce utilizatorii fac tranziția între mediile virtuale, datele lor rămân protejate în conformitate cu reglementările locale relevante.

Capitolul contribuie la teză prin:

- Dezvoltarea unui model de securitate adaptiv bazat pe locație care aplică în mod dinamic legile regionale privind confidențialitatea pe măsură ce utilizatorii interacționează între jurisdicții.
- Introducerea unei arhitecturi de sistem pe mai multe niveluri care integrează detectarea locației în timp real, aplicarea conformității și controlul accesului la date.

6.1. Dilema confidențialității în interacțiunile multimodale în medii imersive

Deși integrarea datelor multimodale sporește realismul și imersiunea, aceasta introduce, de asemenea, riscuri unice în materie de confidențialitate. Riscurile la adresa confidențialității sunt reprezentate de sistemele imersive care colectează date multimodale bogate, continue și adesea inconștiente, precum gesturi, expresii faciale și modele comportamentale [66]. Astfel de date pot identifica în mod unic utilizatorii și pot dezvălui detalii intime, ridicând serioase probleme etice și de securitate [67]. Spre deosebire de platformele online tradiționale, unde guvernanța datelor este de obicei legată de o anumită jurisdicție, Metaverse funcționează ca un ecosistem digital global, ceea ce face ca aplicarea reglementărilor și protecția utilizatorilor să devină din ce în ce mai complexe [68]. Printre principalele probleme legate de confidențialitate se numără:

- Colectarea netransparentă a datelor și transferurile transfrontaliere.
- Urmărirea și profilarea comportamentală, permițând manipularea și inducerea identității.
- Exploatarea datelor biometrice pentru falsuri profunde, supraveghere și impostură.
- Recreerea infracțiunilor din lumea reală în spații virtuale, cum ar fi urmărirea și hărțuirea.

Pe măsură ce mediile imersive se dezvoltă la nivel global, este nevoie urgentă de mecanisme de confidențialitate adaptive, în timp real, care să respecte legile regionale (de exemplu, GDPR) pentru a proteja datele utilizatorilor și a menține încrederea în interacțiunile virtuale.

6.2. Rolul securității adaptive în aplicarea conformității

Experiențele imersive în RV se bazează pe date în timp real, cum ar fi urmărirea privirii și a mișcării, dar aceleași fluxuri de date prezintă riscuri serioase de confidențialitate. Pentru a echilibra imersiunea cu confidențialitatea utilizatorului și conformitatea juridică, această secțiune propune un model de securitate adaptiv care ajustează gestionarea datelor în timp real pe baza reglementărilor regionale.

Sistemele biologice și ecologice prezintă o capacitate inerentă de a se adapta la mediul lor, răspunzând dinamic la amenințări prin mecanisme de autoreglare [37]. Pornind de la aceste principii, acest principiu al adaptabilității autosustenabile poate fi reprodus în Metaverse ca securitate adaptivă, pentru a crea mecanisme de securitate inteligente, în timp real, care se adaptează în mod dinamic la evoluția vieții private, a securității și a cadrului de reglementare. Această securitate adaptivă în Metaverse ar fi realizată prin:

- Monitorizarea continuă a activității utilizatorilor.
- Ajustarea în mod dinamic a colectării datelor pentru a respecta legislația locală.
- Restricționarea accesului neautorizat și a transferurilor transfrontaliere de date.

Modelul funcționează în patru faze:

1. Predicție - Anticipează amenințările cu ajutorul analizei.
2. Prevenire - Blochează proactiv acțiunile neautorizate.
3. Detectare - Identifică în timp real riscurile și anomaliile.
4. Respond - Reduce amenințările în mod automat.

Acest sistem proactiv și autoreglabil asigură faptul că mediile imersive rămân atât conștiente de confidențialitate, cât și conforme din punct de vedere legal, sprijinind adoptarea globală în siguranță a tehnologiilor Metaverse.

6.2.1 Asigurarea respectării confidențialității datelor specifice fiecărei regiuni în Metaverse

Pe măsură ce utilizatorii se deplasează prin spații virtuale legate de diferite regiuni ale lumii reale, Metaverse trebuie să se adapteze la diverse reglementări privind confidențialitatea, precum GDPR, CCPA și PIPL. Este nevoie de un cadru de conformitate dinamic care să echilibreze experiențele imersive cu protecția datelor utilizatorilor.

Soluția constă în sistemele de securitate adaptive în timp real care pot ajusta automat colectarea și prelucrarea datelor în funcție de locația utilizatorului. Aceasta include asigurarea transparenței,

asigurarea consimțământului utilizatorului, aplicarea minimizării datelor și respectarea legilor privind suveranitatea datelor. Pentru a permite acest lucru, platformele trebuie să:

- Implementeze securitatea adaptivă în timp real pentru a aplica legile locale privind confidențialitatea.
- Asigure suveranitatea asupra datelor (de exemplu, păstrarea datelor chinezești în China).
- Adopte securitatea Zero-Trust, prin verificarea continuă a entităților în RV.
- Extindă reglementările pentru a acoperi datele comportamentale și emoționale.

Prin integrarea respectării confidențialității în proiectarea platformelor imersive, Metaverse poate evolua într-un mediu legal și de încredere pentru utilizatori, protejând datele sensibile fără a compromite experiența utilizatorului.

6.3. Implementarea securității adaptive în timp real pentru confidențialitate și conformitate

Pe măsură ce Metaverse continuă să evolueze într-un ecosistem virtual interconectat la nivel global, asigurarea respectării confidențialității datelor specifice fiecărei regiuni devine o provocare majoră. Această secțiune prezintă dezvoltarea unui sistem de securitate adaptiv în timp real conceput pentru a asigura respectarea confidențialității în medii imersive, echilibrând progresul tehnologic cu drepturile și securitatea utilizatorului.

6.3.1 Metodologie

Folosind Unity 3D și IPinfo, sistemul detectează locația utilizatorului și ajustează automat practicile de colectare a datelor pe baza legilor regionale precum GDPR, CCPA și PIPL. Arhitectura generală a sistemului este ilustrată în Figura 6.1. Aceste instrumente au fost integrate pentru a construi un model de securitate dinamic, bazat pe locație, care asigură respectarea confidențialității în Metaverse.

Implementarea include urmărirea geolocalizării în timp real, un motor de conformitate care aplică politici de date specifice fiecărei regiuni, un tablou de bord de confidențialitate destinat utilizatorilor pentru gestionarea preferințelor și măsuri de protecție împotriva transferurilor neautorizate de date. Această abordare modulară asigură că experiențele imersive rămân conforme și sigure în toate jurisdicțiile globale.

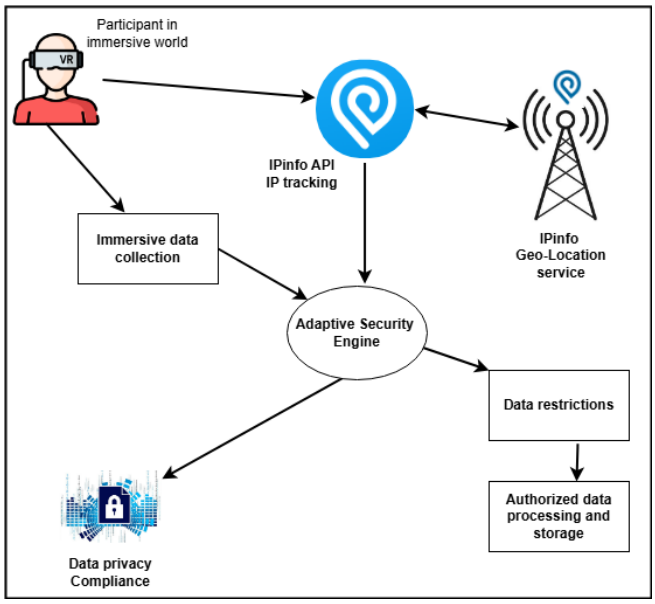

Figura 6.1. Arhitectura propunerii de securitate adaptivă în timp real pentru confidențialitate și conformitate

- **Componente ale arhitecturii de securitate adaptivă în timp real**

Sistemul de securitate adaptiv cuprinde șase componente-cheie:

1. **Stratul de interacțiune cu utilizatorul** - captează intrările utilizatorului (mișcare, privire, voce, biometrie) prin intermediul dispozitivelor imersive.
2. **Detectarea locației** - Utilizează IPInfo API și GPS pentru a determina locația utilizatorului și a asigura cartografierea exactă a jurisdicției.
3. **Motor de securitate adaptiv** - Potrivește locația cu legile regionale privind confidențialitatea și aplică politici adecvate privind datele în timp real.
4. **Baza de date de conformitate** - Stochează diverse reglementări globale privind protecția datelor pentru a ghida deciziile de aplicare a legii.
5. **Privacy Dashboard** - Permite utilizatorilor să gestioneze preferințele de urmărire și să vizualizeze starea de conformitate, aplicând consimțământul acolo unde este necesar
6. **Controlul accesului și stocării datelor** - Oferă opțiuni de păstrare a datelor controlate de utilizator și previne transferurile transfrontaliere ilegale de date.

- **Pași de implementare pentru conformitatea adaptivă în timp real în Unity 3D**

Am luat în considerare GDPR (UE), CCPA (California), PIPL (China) și actele de protecție a datelor DPA 2012 pentru a construi sistemul nostru.

În cele ce urmează sunt prezentate în detaliu etapele parcurse pentru a implementa sistemul de conformitate adaptivă în timp real în Unity 3D.

1. **Detectarea geolocalizării**: API IPinfo integrat în Unity pentru a identifica țara utilizatorului prin adresa IP, validată cu GPS. Sistemul corelează codurile de țară cu legile regionale privind confidențialitatea (de exemplu, GDPR, CCPA, PIPL, DPA 2012).
2. **Motor de securitate adaptiv**: Pe baza locației detectate, sistemul aplică normele de confidențialitate corespunzătoare, de exemplu, GDPR dezactivează urmărirea în mod implicit și necesită opțiunea de participare, în timp ce CCPA permite excluderea. Punerea în aplicare este dinamică și specifică fiecărei regiuni.
3. **Tablou de bord privind confidențialitatea**: Oferă utilizatorilor o stare de conformitate în timp real și control asupra preferințelor de urmărire și păstrare a datelor, adaptând opțiunile în funcție de reglementările aplicabile.

6.3.2 Testarea și validarea sistemului

Sistemul adaptiv de conformitate a fost testat în două jurisdicții:

Cazul de testare 1: Europa (GDPR) - În România și Germania, urmărirea a fost dezactivată implicit. Utilizatorii au trebuit să ofere opțiunea explicită de acceptare pentru a permite colectarea datelor. Sistemul a afișat starea de conformitate corespunzătoare și a permis controlul asupra păstrării datelor. Rezultatele Figura 6.2 ilustrează comportamentul dezactivat și urmărirea mișcărilor în mod implicit pentru a satisface regula acceptării explicite, în timp ce Figura 6.3 demonstrează regulile de păstrare a datelor aplicate. Jurnalele generate sunt ilustrate în Figura 6.4.

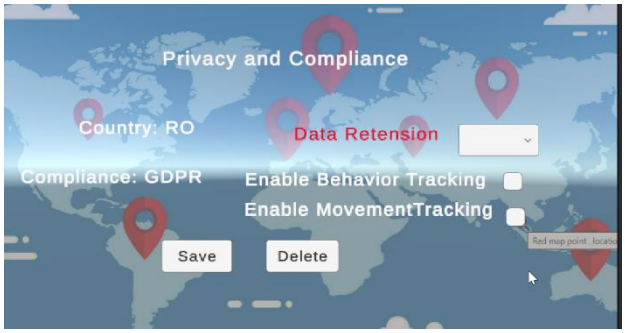

Figura 6.2. Teste efectuate în România, în conformitate cu GDPR. Detectarea GDPR dezactivează datele de urmărire ale utilizatorului, chiar dacă acestea au fost deja salvate. Permite utilizatorului să opteze în mod explicit.

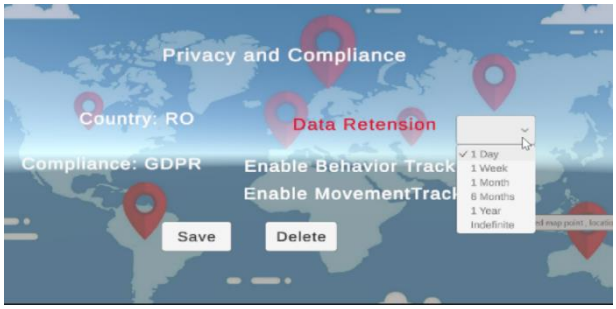

Figura 6.3. Păstrarea datelor poate fi modificată de către utilizator. Valoarea implicită este de o zi. Acest lucru arată cum utilizatorii au control asupra datelor lor atunci când respectă legislația privind protecția datelor

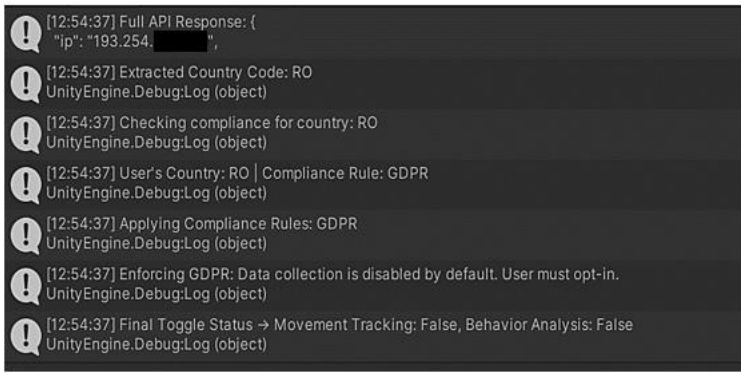

Figura 6.4. Jurnale capturate atunci când locația a fost detectată

Cazul de testare 2: Ghana (DPA 2012) - Similar GDPR, urmărirea a fost dezactivată implicit (Figura 6.5). Transferurile de date în afara Ghanei necesitau consimțământul explicit. Sistemul a impus conformitatea locală prin solicitarea confirmării utilizatorului înainte de prelucrarea datelor în exterior, iar jurnalele sunt prezentate în Figura 6.6.

În general, sistemul s-a adaptat dinamic în funcție de locația utilizatorului, aplicând reguli de confidențialitate specifice regiunii.

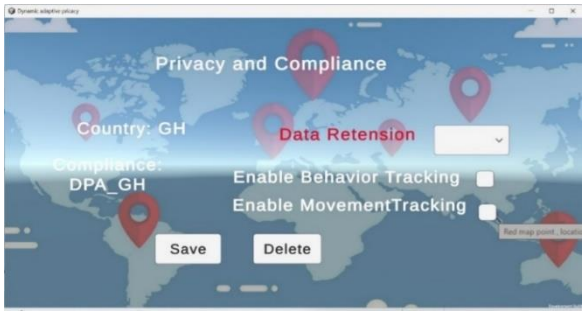

Figura 6.5. Rezultatul testului pentru zona de jurisdicție Ghana

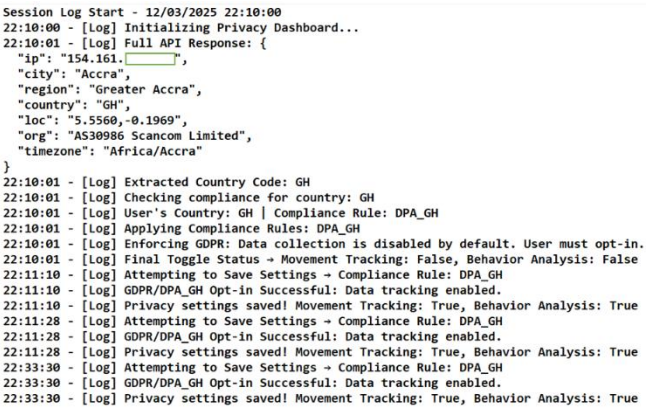

Figura 6.6. Jurnalele capturate la testarea în Ghana. Un fișier jurnal a fost adăugat la aplicația construită pentru a salva jurnalele

6.3.3 Discutarea rezultatelor

Sistemul Real-Time Adaptive Security a fost testat în diferite regiuni pentru a evalua capacitatea sa de a pune în aplicare legile privind confidențialitatea datelor specifice locației. Parametrii cheie au inclus acuratețea detectării locației, aplicarea conformității, controlul utilizatorului, protecția vieții private și capacitatea de reacție a sistemului.

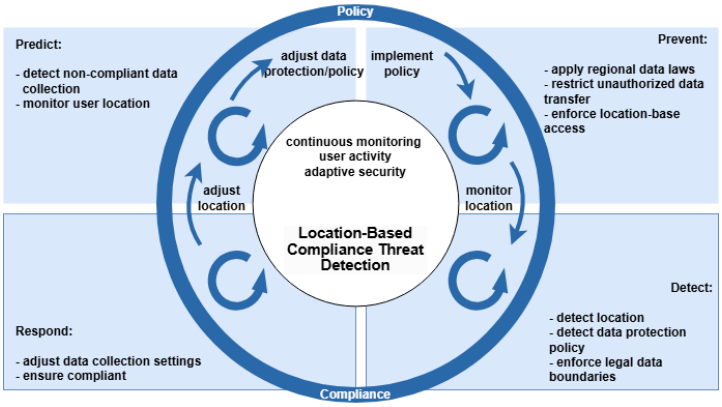

Figura 6.7. Ciclul de viață al sistemului adaptiv în timp real propus de noi pentru confidențialitate și conformitate

Figura 6.7 ilustrează ciclul de viață al sistemului. Rezultatele au arătat:

- Detectarea exactă a locației utilizând IPInfo și GPS.
- Aplicarea cu succes a GDPR în țările UE (de exemplu, România și Germania), cu urmărirea dezactivată implicit și activată numai prin consimțământ explicit.
- Privacy Dashboard a oferit controale clare și transparență.
- Sistemul a prevenit în mod eficient urmărirea neautorizată și a actualizat în mod dinamic setările de conformitate pe măsură ce utilizatorii se deplasau între regiuni.

Studiul confirmă faptul că conformitatea adaptivă, bazată pe locație, este atât practică, cât și eficientă pentru mediile imersive. Îmbunătățirile viitoare pot include detectarea amenințărilor pe bază de inteligență artificială și aplicarea automată pentru o protecție și mai puternică a datelor.

6.4. Concluzie

Sistemul a fost implementat și testat cu succes, dovedind capacitatea sa de a proteja datele utilizatorilor în medii imersive. Pe măsură ce platformele imersive se dezvoltă, astfel de cadre adaptive sunt esențiale pentru protejarea vieții private, asigurarea conformității cu reglementările și construirea încrederii utilizatorilor.

Acest capitol contribuie la sistemele imersive conștiente de confidențialitate prin introducerea unui model de securitate adaptiv în timp real, bazat pe locație, care pune în aplicare legile regionale privind confidențialitatea datelor pe măsură ce utilizatorii se deplasează între jurisdicții. Acesta combină geolocalizarea (IPInfo și GPS), aplicarea conformității și un tablou de bord de confidențialitate ușor de utilizat pentru a asigura gestionarea legală a datelor fără a perturba experiența utilizatorului.

Principalele realizări includ:

- O arhitectură multistratificată pentru automatizarea conformității.
- Controlul dinamic al confidențialității bazat pe locația utilizatorului.
- O interfață utilizator pentru transparență și gestionarea preferințelor privind datele.

Lucrările viitoare pot explora detectarea anomaliilor pe baza inteligenței artificiale și prevenirea automată a amenințărilor pentru a spori reziliența sistemului.

Capitolul 7. Concluzii finale, contribuții originale și noi direcții de cercetare

7.1. Concluzii

Această cercetare doctorală a explorat sistematic provocările de securitate cibernetică în realitatea virtuală, identificând principalele vulnerabilități și implementând soluții practice pentru a spori securitatea în mediile imersive. Lucrarea se aliniază la fiecare dintre obiectivele de cercetare descrise, după cum se detaliază mai jos:

O1. Identificarea și analizarea vulnerabilităților de securitate cibernetică în sistemele de RV

- Studiul clasifică amenințările folosind triada CIA și modelele vectorului de atac.
- Acesta evidențiază riscuri precum manipularea obiectelor virtuale, furtul de identitate, încălcarea confidențialității datelor și ingineria socială.
- Este furnizată o bază structurată pentru viitoarele strategii de atenuare a amenințărilor și de reglementare

O2. Evaluarea cadrelor de securitate cibernetică existente și a limitelor acestora

- Analiza a arătat că modelele actuale de securitate nu sunt adaptabile pentru sistemele imersive.
- Acesta subliniază nevoia de soluții de securitate în timp real, care să protejeze confidențialitatea și să țină cont de identitate, specifice RV.

O3. Efectuarea de studii de caz în lumea reală și evaluarea riscurilor

- Studiile empirice, inclusiv testele etice de penetrare, au scos la iveală vulnerabilități reale precum CWE-359 (expunerea PII), executarea malițioasă a APK pe Oculus Quest 2, abuzul excesiv de permisiuni, controalele audio/video slabe, conștientizarea inadecvată a utilizatorului
- Aceste constatări validează existența unor lacune critice de securitate în platformele RV populare.

O4. Evaluați echilibrul dintre utilizabilitate, securitate și confidențialitate în RV

- O evaluare centrată pe utilizator a demonstrat că măsurile de securitate implementate necorespunzător pot reduce implicarea utilizatorilor.
- Studiul pledează pentru soluții de securitate intuitive și neintruzive care mențin imersiunea.

O5. Implementarea și validarea atenuărilor de securitate în mediile de RV

Implementările cheie au inclus:

- **Securitate criptografică pentru active virtuale**

RSA cu SHA-256 a fost utilizat pentru semnarea și verificarea elementelor virtuale, asigurând autenticitatea și integritatea în timp real.

- **Soluții de securitate adaptive**

A fost creat un cadru dinamic pentru a se adapta la amenințările emergente și la reglementările privind protecția datelor.

- **Mecanisme de autentificare pe mai multe niveluri**

Metodele biometrice, comportamentale și bazate pe jetoane au fost combinate pentru a îmbunătăți controlul accesului.

- **Securitatea și reziliența infrastructurii**

Instrumente precum Kubescape și ARMO au asigurat monitorizarea continuă a infrastructurii și aplicarea conformității în mediile bazate pe Kubernetes.

Aceste eforturi reduc decalajul dintre o securitate cibernetică puternică și o experiență de utilizare fără cusur în RV.

Această teză nu numai că identifică amenințările specifice RV, dar oferă și soluții practice, testate. Ea sprijină crearea de aplicații sigure, scalabile și imersive și servește drept bază pentru viitoarele standarde de securitate, cadre de politică și cercetare în domeniul securității tehnologiei imersive.

7.2. Contribuții originale ale cercetării

Această cercetare aduce mai multe contribuții originale în domeniul securității cibernetice a RV, abordând clasificarea amenințărilor, evaluarea riscurilor, implementarea securității, cadrele de conformitate și considerațiile privind utilizabilitatea în medii imersive.

A. **Categorizarea cuprinzătoare a amenințărilor la adresa securității cibernetice a RV**

1. A dezvoltat un model de clasificare dublă, clasificând amenințările pe baza Triadei CIA și a vectorilor de atac.
2. A furnizat o analiză sistematică a amenințărilor emergente, inclusiv a atacurilor chaperone, a atacurilor cu joystick uman, a atacurilor inception și a atacurilor MITR, contextualizând impactul acestora în cadrul mediilor de RV.

B. **Studii de caz empirice și evaluarea riscurilor amenințărilor în RV**

1. A efectuat simulări ale amenințărilor din lumea reală pentru a evalua vulnerabilitățile practice în aplicațiile imersive.

2. A dezvoltat un cadru de evaluare a riscurilor pentru a cuantifica impactul potențial al atacurilor asupra utilizatorilor XR, confidențialității datelor și securității sistemului.
3. A efectuat o evaluare a vulnerabilității expunerii PII utilizând OWASP ZAP, analizând răspunsurile API configurate greșit pe o platformă de jocuri de RV care a expus date financiare sensibile (CWE-359: Expunerea de informații sensibile).

C. Implementarea semnăturilor digitale criptografice pentru integritatea activelor virtuale

1. Conceput și implementat un mecanism de semnătură criptografică folosind RSA-2048 și SHA-256 pentru a asigura autenticitatea și integritatea activelor digitale în medii de RV.
2. A dezvoltat un proces intuitiv de semnare și verificare care sporește securitatea, păstrând în același timp ușurința în utilizare.
3. Au fost efectuate evaluări ale performanței, demonstrându-se semnarea cu latență redusă (17,3 ms) și verificarea instantanee, făcând soluția scalabilă pentru aplicațiile de RV în timp real.

D. Dezvoltarea unui cadru de securitate adaptiv pentru confidențialitate și conformitate

1. A propus și a integrat un model de securitate adaptiv în timp real care ajustează în mod dinamic colectarea datelor, politicile de confidențialitate și protocoalele de securitate pe baza locației utilizatorului și a cerințelor de conformitate.
2. Am valorificat detectarea geolocalizării (IPInfo API, urmărire GPS) pentru a aplica reglementările transfrontaliere privind protecția datelor, abordând preocupările legate de confidențialitate în Metaverse și aplicațiile de RV globale.

E. Consolidarea securității platformei GENSAVR

1. Nakama integrat pentru autentificare, Kubescape pentru scanarea securității Kubernetes și ARMO pentru monitorizarea securității pentru a securiza platforma de realitate virtuală GENSAVR.
2. A efectuat scanări de conformitate NSA și evaluări ale vulnerabilităților pentru a identifica și atenua riscurile de securitate în implementările de sarcini de lucru, configurațiile RBAC și lacunele de securitate ale rețelei.
3. A implementat protocoale sigure de gestionare a sesiunilor, asigurând autentificarea continuă și persistentă și prevenind în același timp deturnarea sesiunii și accesul neautorizat.

F. **Reducerea decalajului dintre securitate, utilitate și experiența utilizatorului în RV**

1. A dezvoltat un model de securitate centrat pe utilizator care echilibrează utilizabilitatea, UX, securitatea și confidențialitatea, asigurându-se că măsurile de securitate nu perturbă imersiunea.
2. Și a efectuat studii empirice UX pentru a evalua modul în care mecanismele de securitate pot fi integrate fără probleme în aplicațiile imersive.

7.3. Diseminarea și valorificarea rezultatelor cercetării

Rezultatele lucrărilor de doctorat au fost publicate în reviste de specialitate și în lucrările conferințelor internaționale din domeniu.

A. **Lucrări publicate în reviste cotate ISI**

1. **Rebecca Acheampong**, Dorin-Mircea Popovici, Titus Balan, Alexandre Rekeraho, and Manuel Soto Ramos. "*Enhancing Security and Authenticity in Immersive Environments.*" Information 16, no. 3 (2025): 191. https://doi.org/10.3390/info16030191, eISSN 2078-2489, WOS:001452699400001, Journal Impact factor: 5-Year Impact Factor: 2.6 (2023), Q3

2. **Rebecca Acheampong,** Dorin-Mircea Popovici, Titus Balan, Emmanuel Tuyishemi, Alexandre Rekeraho, Gheorghe Daniel Voinea. "*Balancing Usability, User Experience, Security and Privacy: Multidimensional Approach*". *Int. J. Inf. Secur.* 24, 112 (2025). https://doi.org/10.1007/s10207-025-01025-z, Impact factor: 2.4 (2023)

3. Rekeraho, Alexandre, Daniel Tudor Cotfas, Titus C. Balan, Petru Adrian Cotfas, **Rebecca Acheampong**, and Emmanuel Tuyishime. "*Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability.*" Sustainability 17, no. 6 (2025): 2386. https://doi.org/10.3390/su17062386, Journal Impact Factor: 2.4 (2023), Q2

4. Rekeraho, Alexandre, Daniel Tudor Cotfas, Petru Adrian Cotfas, Emmanuel Tuyishime, Titus Constantin Balan, and **Rebecca Acheampong**. "*Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems.*" Electronics 13, no. 4 (2024): 756. https://doi.org/10.3390/electronics13040756. eISSN: 2079-9292, WOS:0011682446000015, 5-Year Impact Factor: 2.6 (2023), Q2

5. Rekeraho, Alexandre, Daniel Tudor Cotfas, Petru Adrian Cotfas, Titus Constantin Bălan, Emmanuel Tuyishime, and **Rebecca Acheampong**. "*Cybersecurity challenges in IoT-based smart renewable energy.*" International Journal of Information Security 23, no. 1 (2024): 101-117. http://doi.org/10.1007/s10207-023-00732-9. ISSN: 1615-5262, WOS:001093252200001, 5-Year Impact Factor: 2.5(2023), Q2

6. **Rebecca Acheampong**, Dorin-Mircea Popovici, Titus Balan, Alexandre Rekeraho, Ionut-Alexandre Oprea. "A cybersecurity Risk Assessment for Enhanced Security in Virtual Reality", Information (2025). – **Under review** - Journal Impact factor: 5-Year Impact Factor: 2.6 (2023), Q2

B. Lucrări publicate în ISI Rated Proceedings of International Conferences

7. **Rebecca Acheampong**, Titus Constantin Balan, Dorin-Mircea Popovici, and Alexandre Rekeraho. "Embracing XR system without compromising on security and privacy." In International Conference on Extended Reality , pp. 104-120. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-43401-3_7, ISI Indexed conference paper: WOS:001156975100007

8. **Rebecca Acheampong**, Bogdan Valentin Floricescu, Ionut Alexandru Oprea, Alexandre Rekeraho, Vladut Gabriel Anghel, Gabriel Danciu, Ioana Corina Bogdan, George Stefan Ionesc. "Scalable Secure Platform for XR", EEITE 2025 Conference, 4-6 June, Chania - **Accepted**

C. Lucrări publicate/prezentate în conferințe BDI

9. **Rebecca Acheampong**, Titus Constantin Bălan, Dorin-Mircea Popovici, and Alexandre Rekeraho. "Security scenarios automation and deployment in virtual environment using ansible." In 2022 14th International Conference on Communications (COMM), pp. 1-7. IEEE, 2022. http://doi.org/10.1109/COMM54429.2022.9817150.

10. Rekeraho, T. Balan, D. T. Cotfas, P. A. Cotfas, **R. Acheampong** and C. Musuroi, "Sandbox Integrated Gateway for the Discovery of Cybersecurity Vulnerabilities," 2022 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 2022, pp. 1-4, http://doi.org/10.1109/ISETC56213.2022.10010327.

11. RAMOS, Manuel SOTO, **Rebecca ACHEAMPONG**, and Dorin-Mircea POPOVICI. "A multimodal interaction solutions."The Way" for educational resources" , *International*

Conference on Virtual Learning, ISSN 2971-9291, ISSN-L 1844-8933, vol. 18, pp. 79-90, 2023. https://doi.org/10.58503/icvl-v18y202306.

7.4. Direcții viitoare de cercetare

Deși această cercetare a oferit informații valoroase cu privire la securitatea cibernetică a RV, mai multe domenii necesită investigații suplimentare:

- Scalabilitatea cadrelor de securitate adaptive: Cercetările viitoare pot explora modul în care soluțiile de securitate adaptive se pot adapta în ecosisteme XR la scară largă, cu milioane de utilizatori simultani.
- Securitate comportamentală bazată pe IA: Investigarea modului în care modelele de învățare automată și de învățare profundă pot prezice și preveni amenințările cibernetice în timp real pe baza modelelor de comportament ale utilizatorilor în RV.
- Protocoale criptografice rezistente la cuantică: Pe măsură ce informatica cuantică evoluează, securitatea tehnicilor criptografice actuale în RV trebuie evaluată în continuare. Lucrările viitoare ar trebui să exploreze criptarea cu siguranță cuantică pentru aplicații imersive.
- Standardizarea securității între platforme: Stabilirea standardelor globale de securitate pentru aplicațiile de RV și XR pentru a asigura conformitatea cu reglementările internaționale privind confidențialitatea și securitatea cibernetică.

Această cercetare a pus bazele progreselor viitoare în domeniul securității cibernetice imersive, oferind o bază solidă pentru dezvoltarea cadrelor de securitate pentru RV de generație viitoare. Pe măsură ce adoptarea RV se extinde în jocuri, asistență medicală, educație și aplicații pentru întreprinderi, nevoia de soluții de securitate robuste, scalabile și care să protejeze confidențialitatea va deveni din ce în ce mai critică.

Bibliografie

[1] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas și N. Roig-Tierno, "Digital Transformation: An Overview of the Current State of the Art of Research", *Sage Open*, vol. 11, nr. 3, p. 21582440211047576, iul. 2021, doi: 10.1177/21582440211047576.

[2] G. Vial, "Understanding digital transformation: A review and a research agenda," *J. Strateg. Inf. Syst.*, vol. 28, nr. 2, pp. 118-144, iun. 2019, doi: 10.1016/j.jsis.2019.01.003.

[3] M. El-Hajj, "Cybersecurity and Privacy Challenges in Extended Reality: Threats, Solutions, and Risk Mitigation Strategies", *Virtual Worlds*, vol. 4, nr. 1, p. 1, dec. 2024, doi: 10.3390/virtualworlds4010001.

[4] H. Guo, H.-N. Dai, X. Luo, Z. Zheng, G. Xu și F. He, "An Empirical Study on Oculus Virtual Reality Applications: Security and Privacy Perspectives", 21 februarie 2024, *arXiv*: arXiv:2402.13815. doi: 10.48550/arXiv.2402.13815.

[5] Y. Wang *et al.*, "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Commun. Surv. Tutor.*, vol. 25, nr. 1, pp. 319-352, 2023, doi: 10.1109/COMST.2022.3202047.

[6] S. Dastgerdy, "Virtual Reality and Augmented Reality Security: A Reconnaissance and Vulnerability Assessment Approach", 22 iulie 2024, *arXiv*: arXiv:2407.15984. doi: 10.48550/arXiv.2407.15984.

[7] B. Falchuk, S. Loeb și R. Neff, "The Social Metaverse: Battle for Privacy", *IEEE Technol. Soc. Mag.*, vol. 37, nr. 2, pp. 52-61, iun. 2018, doi: 10.1109/MTS.2018.2826060.

[8] R. Acheampong, D.-M. Popovici, T. Balan, A. Rekeraho și M. S. Ramos, "Enhancing Security and Authenticity in Immersive Environments", *Information*, vol. 16, nr. 3, p. 191, mar. 2025, doi: 10.3390/info16030191.

[9] R. Di Pietro și S. Cresci, "Metaverse: Security and Privacy Issues," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, GA, USA: IEEE, Dec. 2021, pp. 281-288. doi: 10.1109/TPSISA52974.2021.00032.

[10] E. Kadena și M. Gupi, "Human Factors in Cybersecurity: Risks and Impacts," *Secur. Sci. J.*, vol. 2, nr. 2, pp. 51-64, dec. 2021, doi: 10.37458/ssj.2.2.3.

[11] Mazhar Hamayun, "The Importance of the Human Factor in Cyber Security - Check Point Blog," The Human Factor of Cyber Security. Accesat: Aug. 27, 2024. [Online]. Disponibil: https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/

[12] S. Mohanty, M. Ganguly și P. K. Pattnaik, "CIA Triad for Achieving Accountability in Cloud Computing Environment", nr. 3, 2018.

[13] CSA, *GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE*, feb. 2021. Accesat: Jun. 13, 2023. [Online]. Disponibil: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf?sfvrsn=a63bf6d8_0

[14] Y. Chen, J. Yu, L. Kong, H. Kong, Y. Zhu și Y.-C. Chen, "RF-Mic: Live Voice Eavesdropping via Capturing Subtle Facial Speech Dynamics Leveraging RFID," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 7, nr. 2, pp. 1-25, Jun. 2023, doi: 10.1145/3596259.

[15] Z. Ling, Z. Li, C. Chen, J. Luo, W. Yu și X. Fu, "I Know What You Enter on Gear VR", în *2019 IEEE Conference on Communications and Network Security (CNS)*, Washington DC, DC, SUA: IEEE, iunie 2019, pp. 241-249. doi: 10.1109/CNS.2019.8802674.

[16] R. Acheampong, T. C. Balan, D.-M. Popovici și A. Rekeraho, "Embracing XR System Without Compromising on Security and Privacy", în *Extended Reality*, vol. 14218, L. T. De Paolis, P. Arpaia și M. Sacco, ed., în Lecture Notes in Computer Science, vol. 14218. , Cham: Springer Nature Switzerland, 2023, pp. 104-120. doi: 10.1007/978-3-031-43401-3_7.

[17] P. Casey, I. Baggili și A. Yarramreddy, "Immersive Virtual Reality Attacks and the Human Joystick", *IEEE Trans. Dependable Secure Comput.*, vol. 18, nr. 2, pp. 550-562, mar. 2021, doi: 10.1109/TDSC.2019.2907942.

[18] S. R. K. Gopal, J. D. Wheelock, N. Saxena și D. Shukla, "Hidden Reality: Atenție, intrările gesturilor mâinii în lumea virtuală imersivă sunt vizibile pentru toți!".

[19] N. Huq, R. Reyes, P. Lin și M. Swimmer, "Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences", *Trend Micro Res. TX USA*, p. 24, 2022.

[20] Ö. A. Aslan și R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249-6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[21] J. Lake, "Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection," *EMORY LAW J.*, vol. 69.

[22] "2024 Data Breach Investigations Report | Verizon." Accesat: Mar. 04, 2025. [Online]. Disponibil: https://www.verizon.com/business/resources/reports/dbir/

[23] "Creșterea atacurilor cibernetice care vizează industria jocurilor de noroc în 2022 - SOCRadar® Cyber Intelligence Inc." Accesat: Mar. 05, 2025. [Online]. Disponibil: https://socradar.io/increasing-cyberattacks-targeting-the-gaming-industry-in-2022/

[24] M. Vondráček, I. Baggili, P. Casey și M. Mekni, "Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses," *Comput. Secur.*, vol. 127, p. 102923, apr. 2023, doi: 10.1016/j.cose.2022.102923.

[25] S. Ali, Q. Li și A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Netw.*, vol. 152, p. 103320, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.

[26] M. Vondráček, J. Pluskal și O. Ryšavý, "Automated Man-in-the-Middle Attack Against Wi-Fi Networks," *J. Digit. Forensics Secur. Law*, 2018, doi: 10.15394/jdfsl.2018.1495.

[27] M. Hatami, Q. Qu, Y. Chen, H. Kholidy, E. Blasch și E. Ardiles-Cruz, "A Survey of the Real-Time Metaverse: Challenges and Opportunities", *Future Internet*, vol. 16, nr. 10, p. 379, oct. 2024, doi: 10.3390/fi16100379.

[28] "VRChat este victima atacurilor DDoS - Ryan Schultz". Accesat: Mar. 05, 2025. [Online]. Disponibil: https://ryanschultz.com/2019/04/18/vrchat-is-the-victim-of-ddos-attacks/

[29] C. Shi *et al.*, "Face-Mic: inferarea discursului live și a identității vorbitorului prin dinamica facială subtilă capturată de senzorii de mișcare AR/VR", în *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, New Orleans Louisiana: ACM, oct. 2021, pp. 478-490. doi: 10.1145/3447993.3483272.

[30] A. N. Ramaseri-Chandra și P. Pothana, "Cybersecurity threats in Virtual Reality Environments: A Literature Review", în *2024 Cyber Awareness and Research Symposium (CARS)*, octombrie 2024, pp. 1-7. doi: 10.1109/CARS61786.2024.10778838.

[31] Z. Yang, C. Y. Li, A. Bhalla, B. Y. Zhao și H. Zheng, "Inception Attacks: Immersive Hijacking in Virtual Reality Systems," Mar. 08, 2024, *arXiv*: arXiv:2403.05721. Accesat: Mar. 18, 2024. [Online]. Disponibil: http://arxiv.org/abs/2403.05721

[32] A. Jafar, A. Yeboah-Ofori, T. Abisogun, I. Hilton, O. Oguntoyinbo și O. Oyetunji, "The Impact of Social Engineering Attacks on the Metaverse Platform", în *2024 11th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2024, pp. 201-208. doi: 10.1109/FiCloud62933.2024.00038.

[33] F. Mathis, J. Williamson, K. Vaniea și M. Khamis, "RubikAuth: Fast and Secure Authentication in Virtual Reality", în *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, aprilie 2020, pp. 1-9. doi: 10.1145/3334480.3382827.

[34] F. Mathis, H. I. Fawaz și M. Khamis, "Knowledge-driven Biometric Authentication in Virtual Reality", în *rezumatele extinse ale Conferinței CHI 2020 privind factorii umani în sistemele informatice*, Honolulu HI SUA: ACM, aprilie 2020, pp. 1-10. doi: 10.1145/3334480.3382799.

[35] Z. Lv, D. Chen, R. Lou și H. Song, "Industrial Security Solution for Virtual Reality," *IEEE Internet Things J.*, vol. 8, nr. 8, pp. 6273-6281, apr. 2021, doi: 10.1109/JIOT.2020.3004469.

[36] N. Noah, S. Shearer și S. Das, "Security and Privacy Evaluation of Popular Augmented and Virtual Reality Technologies," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4173372.

[37] "Securitate adaptivă, beneficii, bune practici și multe altele | Digital Guardian," Digita Guardian - protecția datelor. Accesat: Mar. 09, 2025. [Online]. Disponibil: https://www.digitalguardian.com/blog/what-adaptive-security-definition-adaptive-security-benefits-best-practices-and-more

[38] M. Anwar *et al.*, "Immersive Learning and AR/ VR-Based Education," 2023, pp. 1-22. doi: 10.1201/9781003369042-1.

[39] R. Kumar Yekollu, T. Bhimraj Ghuge, S. S. Biradar, S. V. Haldikar și O. F. Mohideen Abdul Kader, "Securing the Virtual Realm: Strategies for Cybersecurity in Augmented Reality (AR) and Virtual Reality (VR) Applications," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2024, pp. 520-526. doi: 10.1109/I-SMAC61858.2024.10714591.

[40] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[41] "Ce este un atac BIN și cum să îl prevenim | SEON." Accesat: Mar. 14, 2025. [Online]. Disponibil: https://seon.io/resources/dictionary/bin-attack/

[42] "Format Preserving Encryption (FPE) | Encryption Consulting". Accesat: Mar. 14, 2025. [Online]. Disponibil: https://www.encryptionconsulting.com/education-center/what-is-fpe/

[43] G. S. Arunanshu și K. Srinivasan, "Evaluating the Efficacy of Antivirus Software Against Malware and Rats Using Metasploit and Asyncrat," in *2023 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Dec. 2023, pp. 1-8. doi: 10.1109/i-PACT58649.2023.10434431.

[44] E. Blancaflor, H. K. S. Billo, B. Y. P. Saunar, J. M. P. Dignadice și P. T. Domondon, "Penetration assessment and ways to combat attack on Android devices through StormBreaker - a social engineering tool," in *2023 6th International Conference on Information and Computer Technologies (ICICT)*, Mar. 2023, pp. 220-225. doi: 10.1109/ICICT58900.2023.00043.

[45] "An Enhanced Risk Formula for Software Security Vulnerabilities." Accesat: Mar. 22, 2024. [Online]. Disponibil: https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities

[46] Y. Lee, "Efectul timpului neîntrerupt de lucru asupra succesului studenților în cursurile online deschise masive (MOOC)", *Comput. Hum. Behav.*, vol. 86, pp. 174-180, sept. 2018, doi: 10.1016/j.chb.2018.04.043.

[47] E. Pedroli *et al.*, "Caracteristici, utilizabilitate și experiența utilizatorilor unui sistem care combină terapia cognitivă și terapia fizică într-un mediu virtual: Positive Bike", *Sensors*, vol. 18, nr. 7, p. 2343, Jul. 2018, doi: 10.3390/s18072343.

[48] Y. Arifin, T. G. Sastria și E. Barlian, "User Experience Metric for Augmented Reality Application: A Review," *Procedia Comput. Sci.*, vol. 135, pp. 648-656, 2018, doi: 10.1016/j.procs.2018.08.221.

[49] A. Altaf, S. Faily, H. Dogan, A. Mylonas și E. Thron, "Use-Case Informed Task Analysis for Secure and Usable Design Solutions in Rail", în *Critical Information Infrastructures Security*, vol. 13139, D. Percia David, A. Mermoud și T. Maillart, ed., în Lecture Notes in Computer Science, vol. 13139. , Cham: Springer International Publishing, 2021, pp. 168-185. doi: 10.1007/978-3-030-93200-8_10.

[50] D. Jones, S. Ghasemi, D. Gračanin și M. Azab, "Privacy, Safety, and Security in Extended Reality: User Experience Challenges for Neurodiverse Users," în *HCI for Cybersecurity, Privacy and Trust*, vol. 14045, A. Moallem, Ed., în Lecture Notes in Computer Science, vol. 14045. , Cham: Springer Nature Switzerland, 2023, pp. 511-528. doi: 10.1007/978-3-031-35822-7_33.

[51] Y. K. Dwivedi *et al.*, "Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse," *Inf. Syst. Front*, Jun. 2023, doi: 10.1007/s10796-023-10400-x.

[52] D. A. Norman, "THE WAY I SEE ITThe transmedia design challenge: technology that is pleasurable and satisfying," *Interactions*, vol. 17, nr. 1, pp. 12-15, Jan. 2010, doi: 10.1145/1649475.1649478.

[53] G. A. Spanos și T. B. Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video," in *Proceedings of Fourth International Conference on*

Computer Communications and Networks - IC3N'95, Sep. 1995, pp. 2-10. doi: 10.1109/ICCCN.1995.540095.

[54] IEEE Std 610.12, *IEEE Standard Glossary of Software Engineering Terminology*, Standard, 28 septembrie 1990.

[55] W. Yang, S. Wang, J. Hu și N. M. Karie, "Multimedia security and privacy protection in the internet of things: research developments and challenges", *Publ. Inderscience Publ. Ltd*, vol. 4, 2022, [Online]. Disponibil: http://creativecommons.org/licenses/by/4.0/

[56] Alfred J. Menezes, Paul C. van Oorschot și Scott A. Vanstone, *Manual de criptografie aplicată*. 1996. Accesat: Sep. 20, 2024. [Online]. Disponibil: https://labit501.upct.es/~fburrull/docencia/SeguridadEnRedes/old/teoria/bibliography/HandbookOfAppliedCryptography_AMenezes.pdf

[57] R. Dhagat și P. Joshi, "New approach of user authentication using digital signature," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, Mar. 2016, pp. 1-3. doi: 10.1109/CDAN.2016.7570947.

[58] R. Kasodhan și N. Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm", în *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India: IEEE, Mar. 2019, pp. 10-15. doi: 10.1109/ICCMC.2019.8819710.

[59] S. Sukaridhoto, A. Haz, E. Fajrianti și R. Putri Nourma Budiarti, "Comparative Study of 3D Assets Optimization of Virtual Reality Application on VR Standalone Device," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 13, p. 999, iun. 2023, doi: 10.18517/ijaseit.13.3.18375.

[60] "Metaverse Security Considerations - Identity Management Institute®." Accesat: Jan. 26, 2025. [Online]. Disponibil: https://identitymanagementinstitute.org/metaverse-security-considerations/

[61] Eamon Javers, Scott Zamost și Paige Tortorelli, "Cybercriminals target metaverse investors with phishing scams", CNBC. Accesat: Sep. 19, 2024. [Online]. Disponibil: https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html

[62] "Modalități de protejare a proprietății digitale și a bunurilor imobiliare virtuale - FortySeven." Accesat: Feb. 20, 2025. [Online]. Disponibil: https://fortyseven47.com/blog/ways-to-protect-your-digital-property-and-virtual-real-estate/

[63] C. Tianhuang și X. Xiaoguang, "Digital signature in the application of e-commerce security," prezentat la 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies, p. 4.

[64] Heroic Labs, "Nakama: Cel mai important server de jocuri open-source pentru studiouri și editori - Heroic Labs", Serverul popular de jocuri open-source. Accesat: Apr. 12, 2025. [Online]. Disponibil: https://heroiclabs.com/nakama/

[65] A. Amrendra Tripathi, "Attacking and Defending Kubernetes," 2024. Accesat: Mar. 06, 2025. [Online]. Disponibil: https://esource.dbs.ie/server/api/core/bitstreams/62cbffaa-d0b8-4a95-8030-ef0b9093d1d2/content

[66] K. Lake *et al.*, "Cybersecurity and Privacy Issues in Extended Reality Health Care Applications: Scoping Review", *JMIR XR Spat. Comput.*, vol. 1, pp. e59409-e59409, oct. 2024, doi: 10.2196/59409.

[67] G. M. Garrido, V. Nair și D. Song, "SoK: Data Privacy in Virtual Reality," *Proc. Priv. Enhancing Technol.*, vol. 2024, nr. 1, pp. 21-40, Jan. 2024, doi: 10.56553/popets-2024-0003.

[68] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky și B. Gordijn, "The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy," *Sci. Eng. Ethics*, vol. 22, nr. 1, pp. 1-29, feb. 2016, doi: 10.1007/s11948-014-9621-1.