Universitatea *POLITEHNICA* București
Facultatea de Automatică și Calculatoare, Departamentul de Calculatoare

Rezumat

Privacy Enhancements for Scalable Storage Systems in Public Cloud Environments

Îmbunătățirea confidențialității sistemelor de stocare scalabile în medii Cloud publice

presented by

Drd.ing. Gabriel Apostol

supervised by

Prof.dr.ing. Florin POP

2023
București, România

Contents

Rezumat

Serviciile de stocare a datelor în Cloud prezintă o serie de probleme și neajunsuri complexe, cauzate în general de lipsa controlului asupra elementelor fizice ce stau la baza infrastructurii. Aceste probleme au un impact substanțial asupra securității și performanței sistemelor Cloud. Când adăugăm la aceste provocări constrângeri de securitate, cum ar fi confidențialitatea, integritatea și disponibilitatea datelor, apar întrebări de cercetare complexe și valoroase. Aceste întrebări au un impact semnificativ în domeniul securității informațiilor și al sistemelor de stocare bazate pe sisteme Cloud. Protecția datelor cu caracter personal este o preocupare generală în societatea contemporană datorată creșterii popularității platformelor bazate pe sisteme Cloud. Indivizii și organizațiile își încredințează o cantitate semnificativă de informații unor entități terțe, precum furnizorii de servicii Cloud. Prin urmare, este important să acordăm prioritate securității acestor date, deoarece pot conține informații confidențile. Abordarea acestei problematici de cercetare cu scopul de a îmbunătăți securitatea sistemelor scalabile de stocare în medii publice Cloud necesită o abordare integrată, care să includă scalabilitatea sistemelor, confidențialitatea datelor, detectarea amenințărilor, conformitatea datelor și interconectarea serviciilor.

Obiectivul principal al acestei teze este cercetarea, proiectarea, implementarea și evaluarea unui cadru multi-strat pentru îmbunătățirea securității sistemelor de stocare scalabile în medii Cloud publice, care include: (i) un mecanism de nivel de transport securizat, care utilizează atât mecanisme criptografice cât și protocoale complexe de comunicație care utilizează date provenite de la dispozitive mobile, (ii) o soluție se securitate pentru datele stocate, care sporește confidențialitatea în sisteme Cloud publice folosind o abordare inovativă pe baza steganografiei și (iii) o soluție de tip plug-and-play pentru îmbunătățirea securității datelor în tranzit, case se bazează pe Overlay-uri care implementează protocolul SOCKS5.

Contribuțiile originale ale acestei teze includ cercetarea, proiectarea, implementarea și evaluarea de mecanisme pentru îmbunătățirea securității sistemelor de stocare bazate pe Cloud, cu un impact semnificativ asupra evoluției și inovației în domeniul securității informațiilor. Rezultatele cercetării noastre sunt valoroase pentru a crește gradul de conștientizare cu privire la riscurile de securitate asociate cu stocarea în Cloud și pentru a educa utilizatorii cu privire la cele mai eficiente practici pentru a reduce aceste riscuri.

1 | Context și Obiective

Colectarea datelor cu caracter personal a devenit o practică de afaceri larg răspândită în lumea online. Actorii principali din acest domeniu sunt Furnizorii de Servicii Internet, companii private care închiriază sau dețin infrastructura și au acces la toate informațiile referitoare la natura activităților online desfășurate de clienții lor.

Chiar dacă o persoană începe o sesiune de navigare criptată, aceasta este susceptibilă profilării bazate pe tipare de acces. Un atacator ar putea exploata faptul că un site este parțial criptat, pentru a obține mai multe informații despre interesele utilizatorilor. O altă metodă de profilare este analiza interogărilor DNS necriptate utilizate de fiecare aplicație conectată la internet. Aceste interogări ar putea disemina date potențial sensibile, cum ar fi informații medicale, interese politice și comerciale și chiar date cu privire la software-ul instalat pe diferite dispozitive.

Chiar dacă utilizarea rețelelor de tip overlay pentru îmbunătățirea confidențialității ridică unele probleme etice, ele sunt cu siguranță centrate în jurul principiilor libertății. Prin urmare, îmbunătățirea constantă a acestora [10] ar trebui considerată o prioritate, deoarece confidențialitatea este un drept uman fundamental.

1.1 Definirea problemelor de cercetare

Scopul acestei secțiuni este de a investiga diverse întrebări de cercetare referitoare la îmbunătățirea confidențialității și securității datelor.

RQ 1: Care sunt riscurile de securitate și confidențialitate asociate stocării datelor personale prin intermediul serviciilor de stocare în medii cloud publice și cum pot consumatorii să le minimizeze? Am analizat cei mai populari furnizori de servicii de stocare în cloud și am evaluat metodele lor de transfer, stocare și prelucrare a datelor utilizatorilor.

RQ 2: Având în vedere că numeroase smartphone-uri își îmbunătățesc capacitățile prin utilizarea serviciilor în cloud, cum ar putea o gama diversă de caracteristici hardware ale acestor terminale mobile să îmbunătățească securitatea? Am analizat cum smartphone-urile pot îmbunătăți securitatea și construi încredere prin implementarea unor mecanisme solide pentru autentificarea utilizatorului, stocarea securizată și criptarea datelor prin intermediul interfețelor biometrice.

RQ 3: Cum ar putea furnizorii de servicii cloud și clienții lor să-și reducă consumul de energie și resurse computaționale, fără a face compromisuri în ceea ce privește securitatea? Am efectuat un studiu privind starea actuală a primitivelor criptografice cu consum de energie redusă, oferind o imagine de ansamblu cuprinzătoare a progreselor recente în domeniu. În plus, am studiat principiile care stau la baza funcționalității dispozitivelor de tip smart-card, deoarece acestea necesită o cantitate relativ redusa de energie pentru a executa operațiuni criptografice într-un mod sigur.

RQ 4: Ce informații pot fi obținute din analiza tiparelor de de acces la rețea în cazul accesării serviciilor de stocare în cloud și cum ar putea schimbarea

acestor tipare să atenueze riscurile asociate? Pentru a atenua amenințările la nivel de rețea, cum ar fi profilarea, recunoașterea și atacurile direcționate, am analizat mai multe sisteme de tip network overlay. Obiectivul nostru principal a fost Rețeaua Tor, deoarece aceasta permite utilizatorilor să utilizeze metode alternative de transportare a datelor.

RQ 5: De ce ar putea fi necesară suplimentarea criptografiei cu steganografie și ce avantaje oferă această combinație în ceea ce privește securitatea și confidențialitatea în medii de tip cloud? Am proiectat și implementat un mecanism pentru îmbunătățirea confidențialității prin combinarea steganografiei video cu metodele de criptare. Obiectivul nostru principal a fost să creăm un instrument capabil să modifice fișierele MKV pentru a le transforma în containere steganografice, într-o manieră care să nu afecteze calitatea video sau entropia fișierului modificat.

1.2 Obiective de cercetare

Luând în considerare obiectivul principal al acestei teze și întrebările de cercetare prezentate în Section 1.1, am identificat următoarele obiective ale acestei cercetări:

1. Cercetarea și definirea riscurilor asociate stocării datelor în medii de tip cloud publice și studiul metodelor prin care se pot atenua riscurile de securitate și confidențialitate;
2. Cercetarea, implementarea și evaluarea unui mecanism robust pentru autentificarea utilizatorilor, prin utilizarea de interfețe biometrice dedicate, corelate cu date generate de senzori hardware specifici terminalelor de tip smart phone;
3. Cercetarea, implementarea și evaluarea unui protocol de comunicare care primește confidențialitatea care utilizează identificatorii diferitelor subsisteme hardware pentru a genera un identificator unic pentru fiecare dispozitiv mobil;
4. Cercetarea, proiectarea, implementarea și evaluarea unei arhitecturi software care presupune interacțiunea cu dispozitive de tip smart card contactless care pot stoca chei criptografice private non-exportabile, oferind securitate sporită;
5. Cercetarea, proiectarea, implementarea și evaluarea unui sistem de tip overlay la nivel de rețea care utilizează o interfață SOCKS5 multiplatformă ce are ca scop conversia datelor specifice protocoalelor suportate în mesaje XMPP;
6. Cercetarea, proiectarea, implementarea și evaluarea unei metode noi de îmbunătățirea a securității și confidențialității în medii cloud, bazata pe tehnici ce presupun agregarea criptografiei și steganografiei pe fișiere multimedia.

1.3 Cuprinsul tezei

Această teză se concentrează pe îmbunătățirea confidențialității datelor în cadrul sistemelor publice de stocare în cloud..

Am evaluat tehnologia mai multor furnizori publici de servicii de stocare în cloud pentru a le identifica caracteristicile cheie, punctele forte și punctele slabe, așa cum este subliniat în capitolul 2, Îmbunătățirea confidențialității în medii de tip Cloud-Edge.

Am analizat potențialul de îmbunătățire a securității sesiunilor utilizatorilor de telefonie mobilă prin colectarea de date atât de la senzori hardware, cât și de la senzori virtuali, așa cum se poate observa în capitolul 3, Algoritmi de îmbunătățire a nivelului de încredere în comunicarea de tip oportunistic.

În capitolul 4, Primitive criptografice cu consum redus de energie,am analizat impactul consumului de energie pentru diverși algoritmi criptografici.

În capitolul 5, Overlay-uri scalabile am analizat componentele fundamentale aferente rețelelor de tip overlay, cum ar fi Tor și I2P. Acest lucru a fost făcut pentru a introduce conceptele, principiile și tehnologiile esențiale necesare pentru a obține confidențialitatea, securitatea și anonimatul online.

În capitolul 6, Îmbunătățirea confidențialității prin intermediul steganografiei, am discutat despre implementarea diferitelor tehnici de steganografie pentru fișierele multimedia digitale. Obiectivul nostru este de a oferi o imagine de ansamblu asupra progreselor care au apărut de-a lungul timpului și de a crește gradul de conștientizare cu privire la metodele și motivele pentru a ascunde și transmite în secret informațiile. În plus, am implementat o nouă metodă steganografică care valorifică flexibilitatea formatului video MATROSKA pentru a încapsula containere criptate dm-crypt.

În Chapter Concluzii și direcții de cercetare ulterioare încheiem această teză cu o serie de idei generate de cercetarea noastră și schițăm contribuțiile originale ale acestei teze de doctorat.

2 | Îmbunătățirea confidențialității în medii de tip Cloud-Edge

Cererea tot mai crescută pentru rețele de mare viteză și resurse de stocare a condus la adoptarea pe scară largă a serviciilor bazate pe Cloud în diverse industrii. În timp ce beneficiile acestei tehnologii sunt evidente, aceasta a generat probleme semnificative legate de confidențialitatea și integritatea datelor. Pentru a adresa aceste probleme, furnizorii de aplicații software au început să ofere soluții de criptare a datelor.

2.1 Protejarea proprietății intelectuale

Pentru a reduce costurile tradiționale de stocare, unele companii au început să externalizeze stocarea datelor către terți.Procedurile de stocare , dar și gestiunea a datelor sensibile impun asigurarea confidențialității, pentru a asigura protecția proprietății intelectuale.

Deși exista mai multe moduri de protecție a proprietății intelectuale, fiecare cu avantajele și dezavantajele sale, conform Tabelului 2.1, putem observa că secretele comerciale pot fi protejate utilizând sisteme de asigurare a confidențialității în Cloud.

2.2 Furnizori de servicii publice de stocare în medii Cloud

Sincronizarea și backup-ul fișierelor pe platforme Cloud au devenit din ce în ce mai răspândite în ultimii ani. Pentru a observa avantajele platformelor de stocare în Cloud public, am realizat o analiză comparativă, pe baza unor documente de referință și surse online [3], referitoare la Dropbox, Google Drive și Amazon Cloud Drive (Tabelul 2.2).

2.3 Riscuri asociate tehnologiei de stocare a datelor în medii tip Cloud

Serviciile de stocare în Cloud au devenit tot mai populare de-a lungul timpului datorită numeroaselor lor avantaje, cum ar fi scalabilitatea, eficiența și ușurința de utilizare. Cu toate acestea, în ciuda avantajelor lor, există și potențiale riscuri asociate utilizării lor, în special în ceea ce privește securitatea.

Pierderea datelor este un risc semnificativ în ceea ce privește securitatea. Defecțiunile hardware, erorile umane și dezastrele naturale pot duce la pierderea datelor atunci când se utilizează stocarea în Cloud. Deși furnizorii de servicii Cloud implementează în mod obișnuit redundanță și proceduri de backup pentru a minimiza riscul de pierdere a datelor, este încă scenarii nefavorabile.

În cazul în care datele sunt stocate în Cloud, utilizatorii pot să nu aibă control complet asupra lor. În anumite condiții, furnizorii de servicii Cloud pot obține anumite drepturi

Table 2.1. Avantaje și dezavantaje ale metodelor de protecție a proprietății intelectuale.

	Secrete comerciale	**Alte metode**
Avantaje	Perioadă nelimitată de protecție. Publicarea nu este necesară. Potrivit pentru lucrări care nu pot fi protejate.	Proceduri simplificate de licențiere. Conferă drepturi exclusive opozabile oricui, inclusiv inventatorilor independenți.
Dezavantaje	Pierderea are efecte imediate. Nu oferă protecție împotriva inventatorilor independenți. Unele produse pot fi supuse dezasamblării.	Perioadă limitată de protecție. Odată publicată, poate fi supusă cercetării și dezvoltării de către competitori. Reproductibile de către competitori după expirare.

Table 2.2. Analiza comparativa a serviciilor de stocare în Cloud.

	Dropbox	**Google Drive**	**Amazon Cloud Drive**
Limita dimensiunii fișierului	10 Gb	5 Tb	2 Gb
Securitatea transportului pentru datele în tranzit	SSL\TLS [chei de 2048 de biți]	SSL\TLS [chei de 2048 de biți]	SSL\TLS [chei de 2048 de biți]
Stocare gratuită	2 Gb	15 Gb	Niciuna
Criptarea datelor stocate	AES [chei de 256 de biți]	AES [chei de 128 de biți]	Niciuna

de acces, utilizare sau chiar de ștergere a datelor. Aceasta fapt poate genera neîncredere cu privire la confidențialitatea datelor.

Atât pentru persoanele fizice, cât și pentru întreprinderi, stocarea în Cloud este o resursă crucială, și de aceea este important să identificam riscurile asociate. Securitatea informațiilor stocate în Cloud poate fi îmbunătățită prin implementarea unor sisteme fiabile de protejare a confidențialității datelor, dar și prin implementarea autentificării de tip multi-factor.

2.4 Implementări software pentru criptarea datelor

Pe măsură ce tot mai multe persoane au adoptat deja stocarea în Cloud, încep să apară noi probleme în materie de securitate în urma unor atacuri cibernetice ce au vizat marii furnizori din domeniu [4].

Cele mai frecvent utilizate aplicații create de terți pentru asigurarea confidențialității în Cloud sunt Boxcryptor, Cloudfogger, AES Crypt, SpiderOak și Viivo. Aceste aplicații ajută utilizatorii să-și protejeze confidențialitatea datelor înainte ca acestea să ajungă in Cloud, adăugând astfel un nivel suplimentar de securitate.

2.4.1 Viivo

Viivo este o implementare software validată conform standardului FIPS-140-2. Aceasta este gratuită pentru utilizare personală. A fost creată de compania PKWARE și se integrează cu Dropbox, Box, OneDrive, Google Drive și Copy.

Primitivele criptografice utilizate de Viivo sunt RSA-4096 și AES-256, utilizate împreuna într-o schema de tip hibrid, pentru a obține un grad mai mare de confidențialitate.

Viivo poate fi utilizat pe mai multe sisteme de operare, cum ar fi Apple Mac OS X, Windows și Android, asigurând interoperabilitatea și integrarea între dispozitive.

2.4.2 AES Crypt

AES Crypt este o implementare software disponibilă pentru iOs, Android, Linux, Php și Java, care utilizează standardul AES și HMAC-SHA-256 pentru a asigura confidențialitatea și integritatea datelor.

Chiar dacă nu implementează niciun fel de integrare cu medii de tip Cloud, această aplicație este foarte simplu de utilizat pe mai multe dispozitive și are o implementare open-source.

Procesul de criptare poate fi inițiat de către utilizator după ce a fost selectat un fișier și o parolă. Indiferent de complexitatea parolei, algoritmul PBKDF2 este utilizat pentru a deriva cheia și vectorul de inițializare aferent algoritmului AES și cheii HMAC-SHA-256.

2.5 Concluzii

Chiar dacă criptarea este o măsură de securitate esențială pentru protejarea datelor sensibile, există încă probleme legate de aplicarea sa. Cele mai sensibile aspecte asociate criptării sunt:

- Gestionarea cheilor: Gestionarea cheilor de criptare poate fi dificilă, în special atunci când se lucrează cu volum mare de date și mulți utilizatori. Pierderea sau compromiterea cheilor poate duce la accesarea neautorizată a datelor;
- Compromiterea cheilor: Aceasta apare atunci când un atacator obține abilitatea de a decripta datele utilizând o cheie de criptare. Acest lucru poate avea loc dacă algoritmul de criptare este slab sau dacă cheia de criptare are o entropie scăzută;
- Defecte de implementare: Atunci când algoritmii de criptare sunt utilizați în mod incorect sau sunt depășiți, apar o serie vulnerabilități ce pot fi exploatate de către un atacator.
- Probleme de compatibilitate: În funcție de suita de algoritmi criptografici oferita de un protocol de comunicare securizată, faza de negociere poate avea ca rezultat alegerea unui algoritm slab, fapt care duce la vulnerabilizarea protocolului;
- Costurile suplimentare de performanță:Deoarece criptarea și decriptarea pot fi operații intensive din punct de vedere al resurselor computaționale, acestea pot afecta performanța generală a sistemului și pot adăuga costuri de procesare suplimentare.

Pentru a îmbunătăți securitatea datelor cu caracter personal, utilizatorii pot opta să utilizeze sisteme de criptare a datelor de tip overlay înainte de a transmiterea acestora în Cloud. Implementarea overlay-uri-lor de criptare poate servi ca măsură de protecție împotriva atacurilor cibernetice și poate asigura respectarea cerințelor legale prin cifrarea informațiilor anterior transferului acestora în Cloud.

3 | Algoritmi de îmbunătățire a nivelului de încredere în comunicarea de tip oportunistic

În ultima decadă, un număr crescut de atacuri cibernetice a demonstrat că libertăți fundamentale, precum confidențialitatea datelor în spațiul digital, pot fi încălcate. Ca urmare, un numar crescut de cercetători independenți si experți în securitate au început să caute soluții, fapt care a condus la crearea de noi modele de rețelele descentralizate.

3.1 Constrângeri și obstacole în utilizarea biometriei pe dispozitivele mobile

În ultimii ani, numărul terminalelor mobile capabile să citească amprentele utilizatorului în scopul autorizării și autentificării a crescut considerabil.

Studiile anterioare au evidențiat faptul că această implementare poate permite anumitor materiale conductive electric, modelate după o anumita amprenta, să fie acceptate de senzorii biometrici și să permită accesul. Pe lângă acest aspect, s-au demonstrat și alte atacuri, cum ar fi: (i) **Atacul de autorizare confuză**. Acest tip de atac este o tehnică utilizată de aplicațiile malware pentru a declanșa o cerere de autentificare biometrică pe ecranul dispozitivului; (ii) **Atacul de spionaj asupra senzorului de amprentă**. În unele implementări, senzorul de amprentă nu este complet securizat și este gestionat prin intermediul nucleului Linux, permițând astfel atacatorilor să intercepteze datele care trec prin interfața Serial Parallel Interface (SPI).

3.2 Identificarea amprentelor digitale aferente dispozitivelor mobile

Identificarea amprentelor digitale aferente dispozitivelor mobile se bazează pe proceduri standard sau non-standard, și are ca scop identificarea în mod unic a unui dispozitiv fizic conectat la rețea. Procedura de identificare a amprentei digitale a dispozitivului poate fi [5] [1]: (i) **Bazată pe client**. Această abordare implică calculul local al amprentei digitale utilizând diverse surse de date, cum ar fi numărul de serie al hard-disk-ului, adresa MAC a plăcii de rețea sau alți identificatori obținuți de către o aplicație. Valoarea rezultată ar trebui să fie unică, persistentă și sigură împotriva modificărilor; (ii) **Bazată pe server**. Valoarea amprentei digitale este calculată pe un server de profilare utilizând detaliile de conectivitate, fără a fi necesară instalarea de software suplimentar la nivel de client pe stația de lucru sau pe computerul personal. Această abordare este utilizată în principal în domeniul bancar online și al comerțului electronic; (iii) **Bazată pe browser**. Această abordare se bazează pe date colectate din browserul utilizatorului, cum ar fi

cookie-urile, valoarea campului user-agent, setările generale și de confidențialitate, modulele suplimentare instalate, etc.; (iv) **Bazată pe HTTP**. Această metodă utilizează o tehnică de identificare a amprentei digitale și constă în extragerea unor metadate specifice unei conexiuni HTTP. Unii dintre parametrii utilizați includ numele metodei de comprimare, suportul pentru proxy-uri, setul de algoritmi de criptare acceptați, etc.; (v) **Bazată pe sistemul de operare**. Această abordare implică calculul unei valorii unice utilizând informații despre sistemul de operare obținute dintr-o conexiune de rețea cu dispozitivul fizic; (vi) **Bazată pe TCP**. Asemănătoare abordării bazate pe HTTP, această metodă se bazează pe informațiile colectate în momentul stabilirii unei conexiuni.

3.3 Proiectarea unui protocol de consolidare a încrederii destinat dispozitivelor mobile

Amprentarea digitală a dispozitivelor mobile este o procedură care cuprinde metode pentru a identifica în mod unic o mașină specifică, în scopul asigurării autorizării și comunicării între nodurile participante dintr-o rețea descentralizată.

Nivelul de confidențialitate al mesajelor transmise reprezintă o problemă deschisă, ce ar putea fi soluționată prin intermediul metodei propuse în cadrul acestei cercetări Figure 3.1.

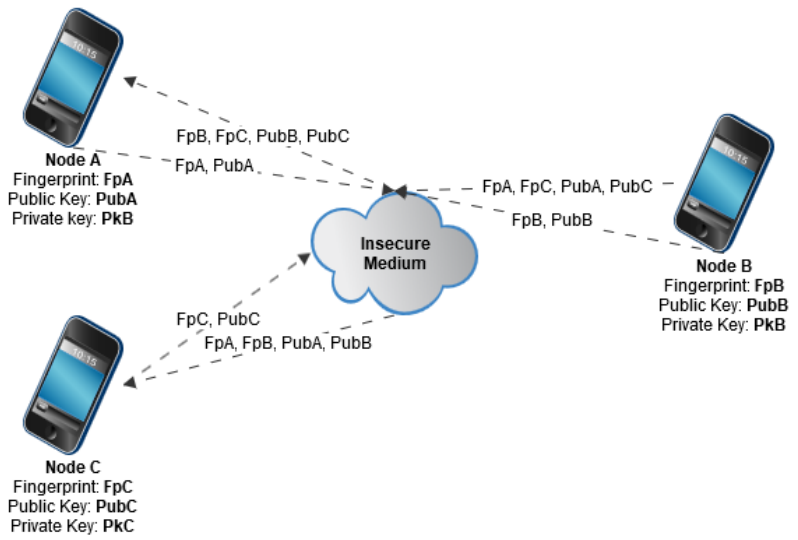

Figure 3.1. Faza de autentificare a protocolului de comunicare propus.

Într-un mod simplificat, așa cum este prezentat în Figura 3.1, fazele protocolului de comunicare propus sunt sunt:

- Fiecare nod din rețeaua spontană are propria pereche de chei asimetrice și o amprentă verificabilă și unic identificabilă.
- Când un nod își anunță prezența, distribuie amprenta și cheia sa publică pentru ca celelalte noduri să le afle.
- Nodurile receptor corelează cheia publică cu amprenta pentru a verifica identitatea nodului care transmite.
- Dacă un alt nod difuzează o pereche identică de chei sau amprente, este respins de nodurile înconjurătoare.

- După ce un nod își transmite detaliile, nodurile înconjurătoare încep un consens pentru a alege cele două noduri cele mai vechi pentru a verifica identitatea nodului participant.
- Dacă entitatea verificată nu reușește să-și dovedească identitatea, verificatorii vor răspândi această informație pentru a preveni alte încercări de conexiune.
- Dacă nodul este validat, nodurile cenzor anunță rezultatul pentru a permite interacțiuni ulterioare.
- Nodurile ar trebui să difuzeze mesaje de tip "heartbeat" la intervale regulate pentru a detecta nodurile care părăsesc rețeaua.
- Numărul maxim de noduri cunoscute pentru un nod este restricționat la 1000.
- Procedura de verificare a noilor noduri începe cu un mesaj de tip "hello" difuzat în rețea pentru a anunța prezența și a descoperi nodurile disponibile.
- Noul participant trimite un mesaj de tip "discover" pentru a anunța prezența sa către cel mai apropiat nod disponibil.

3.4 Identificarea utilizatorului pe baza amprentelor digitale specifice unui terminal mobil

Pentru a genera un identificator unic asociat unui dispozitiv, este necesară identificarea unui set de atribute hardware și software verificabile și rezistente la falsificare. În ceea ce privește dispozitivele mobile, există informații care sunt greu de modificat, cum ar fi rezoluția ecranului, lista de senzori hardware, producătorul dispozitivului și numele sistemului de operare.

Soluția noastră combină informațiile obținute din două categorii de identificatori pseudo-unici: datele NVRAM și caracteristicile hardware specifice. Din NVRAM, pe platforma Android, se poate extrage valoarea IMEI prin metode prestabilite ce nu presupun permsiuni speciale.

La nivel software, sistemul de operare Android nu furnizează valori care ar putea fi utilizate în procesul de amprentare digitala a dispozitivului, deoarece Android ID și Android Advertising ID sunt modificate atunci când utilizatorul efectuează resetarea dispozitivului. Metoda utilizată pentru generarea identificatorului unic se bazează pe algoritmul SHA-256, pentru a obține o valoare a amprentei cu lungimea de 256 de biți, conform Figurii 3.2.

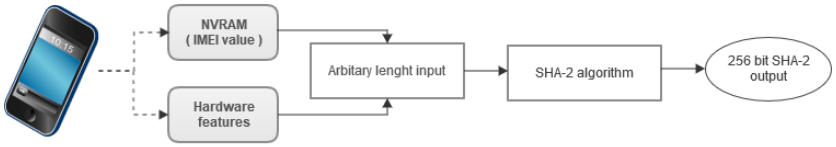

Figure 3.2. Procedura de generare a amprentei digitale.

Modulul de amprentare digitala calculează o valoare unic identificabilă asociată cu un nod și o cheie publică. Primul obstacol întâlnit a fost că dispozitivele emulate nu pot furniza un IMEI valid, așa că din acest motiv am trebuit să implementăm un modul software pentru a genera această valoare o singură dată per dispozitiv.

Chiar dacă soluția propusă este fezabilă pe sistemul de operare Android sau Windows, privilegiile limitate ale sistemului de operare iOS interzic accesul la informații potențial sensibile, precum IMEI-ul.

3.5 Generarea contextuala a amprentelor digitale aferente dispozitivelor mobile

Soluția noastră are ca scop colectarea tuturor datelor brute furnizate de senzorii specifici ai dispozitivului, fără a solicita acces privilegiat la resursele acestuia, deoarece root-area telefonului mobil sau a tabletei va diminua nivelul de securitate și confidențialitate garantat de producătorul dispozitivului. Datele senzorilor pot fi utilizate pentru a furniza informații despre mediul contextual al utilizatorului și starea de mișcare a acestuia.

În primul rând, am ales să identificăm modul în care datele senzorilor sunt influențate de starea de mișcare a utilizatorului, deoarece colectarea datelor despre mediul contextual este legată de starea de mișcare a dispozitivului. Prin urmare, implementarea a fost testată folosind trei scenarii diferite, după cum urmează: (i) Când utilizatorul se află într-o stare de repaus (**Stare de repaus** - SS); (ii) Când utilizatorul se deplasează (**Stare de mișcare** - MS); (iii) Când utilizatorul conduce sau se află într-o mașină (**Stare de conducere** - DS).

Scopul principal al cercetării noastre a fost identificarea cât mai multor informații posibile referitoare la modelele comportamentale ale utilizatorului, influențate de interacțiunea cu mediul înconjurător și cu interfața om-mașină, așa cum sunt percepute de o stivă de senzori gestionată de către sistemul de operare Android. Rezultatele noastre au arătat că smartphone-urile moderne pot detecta prezența unei persoane care interacționează cu ele și pot furniza anumite informații despre contextul de utilizare.

Această abordare ar putea oferi indicii semnificative cu privire la modelele comportamentale ale utilizatorului fără a solicita permisiuni speciale și fără a dezvălui identitatea reală a proprietarului sau datele biometrice ale acestuia.

3.6 Fiabilitatea dispozitivelor mobile în contextul confidențialității

Dispozitivele mobile sunt susceptibile la o gamă largă de amenințări de securitate, inclusiv, dar fără a se limita la malware, atacuri de phishing și încălcări ale datelor. Compromiterea informațiilor personale reprezintă un risc semnificativ pentru indivizi, inclusiv, dar fără a se limita la fraudă financiară, furt de identitate și hărțuire cibernetică.

Dispozitivele mobile au capacitatea de a colecta o cantitate semnificativă de informații personale despre utilizatorii lor, cum ar fi locația geografică, istoricul de căutare și utilizarea aplicațiilor. Pentru a minimiza cantitatea de date personale colectate, este recomandată achiziția unor dispozitive care oferă setări extinse de confidențialitate. De asemenea, se recomanda o analiza atenta atunci când vine vorba despre instalarea de aplicații mobile. Cu toate că oferă funcționalități similare, unele aplicații pot colecta o cantitate mai mare de date decât altele.

Fiabilitatea garantata de un producător este un criteriu esențial în selectarea unui dispozitiv. Este crucial ca un produs sa provină de la o companie de încredere care prioritizează protecția informațiilor personale. Se recomandă alegerea unor companii care au o reputație dovedită în protejarea informațiilor utilizatorilor și care pot gestiona în mod eficient vulnerabilitățile de securitate.

3.7 Concluzii

Datorită variațiilor intrinseci ale procesului de fabricație și altor factori, este posibil ca două dispozitive identice să afișeze valori ale senzorilor care diferă ușor în aceleași

circumstanțe. Pot exista diferențe între componentele utilizate în construcția dispozitivului sau în mediul de funcționare, chiar și atunci când dispozitivele sunt fabricate conform acelorași specificații.

În plus, senzorii pot fi afectați de mai multe variabile, cum ar fi temperatura, umiditatea și interferența electromagnetică. Acești factori pot determina senzorii să producă valori diferite chiar și atunci când funcționează în condiții identice. Pentru a furniza valori precise și consistente pe diferite dispozitive, terminalele de tip smartphone includ în mod obișnuit date de calibrare.

Dacă datele senzorilor sunt utilizate pentru a îmbunătăți procesul de autentificare a utilizatorului, acestea trebuie să treacă printr-un proces suplimentar de filtrare și prelucrare pentru a ajusta variațiile de citire. Aceste variații sunt cauzate de factori de mediu și fluctuații naturale. Chiar dacă dispozitivele nu sunt identice, filtrarea și normalizarea datelor achiziționate de la senzori pot contribui la îmbunătățirea procesului de autentificare al utilizatorilor.

4 | Primitive criptografice cu consum redus de energie

4.1 Analizarea eficienței primitivelor criptografice

Pentru a obține un raport mai bun între cost și securitate, este necesar să se analizeze consumul de timp și resurse computaționale aferent primitivelor criptografice clasice, dar și emergente.

4.1.1 Primitive de confidențialitate

Pentru a determina care dintre algoritmii criptografici moderni sunt potriviți în cazul nostru de utilizare, este necesar să evaluăm echilibrul între consumul de putere de calcul, viteză și securitate. În analiza noastră critică, am utilizat doar date referitoare la Numărul de Runde, Ciclurile CPU pe byte și Ciclurile CPU pentru stabilirea cheii și a IV-ului.

Table 4.1. Utilizarea resurselor computaționale pentru diferiți algoritmi criptografici.

Algorithm	Number of rounds	Block size (bits)	Cycles per byte	CPU Cycles to set up key and iv
DES	16	64	54.7	1532
IDEA	8	64	49.9	1277
AES	10/12/14	128	12.6	1277
RC5	12/16	32/128	23.4	4665
RC6	20	128	17.3	5128
MARS	2 x 16	128	37.2	6435
XTEA	32	32	67.4	1165
Serpent	32	128	54.7	2191
Twofish	16	128	29.4	14121

4.1.2 Primitive de integritate

în medii cu restricții de consum al energiei, costul resurselor computaționale este o metrică la fel de importantă precum nivelul de încredere furnizat de metoda hash selectată. Tabelul 4.2 prezintă aceste informații.

Table 4.2. Utilizarea CPU pentru algoritmi de sumarizare (hashing).

Algorithm	Number of rounds	Input size (bits)	Hash size (bits)	CPU Cycles per byte
MD5	4	512	128	6.8
SHA-1	4	512	160	11.9
SHA-256	64	512	256	15.8
SHA-512	80	512	512	17.7
WH	10	64	64	30.5

4.2 Primitive criptografice cu consum redus de energie

Termenul ***primitivă criptografică cu consum redus de energie*** denotă o operațiune sau funcție criptografică care poate fi executată pe dispozitive cu nivel redus de energie, inclusiv, dar fără a se limita la telefoane mobile, dispozitive din categoria Internet of Things (IoT) și alte dispozitive cu baterii. Utilizarea acestui tip particular de primitive este crucială în asigurarea securității transmisiilor în medii cu resurse limitate.

Conceptul de criptare cu consum redus ar putea fi redefinit de evoluția constanta a procesoarelor. Algoritmii criptografici mai complecși și mai intensivi din punct de vedere computațional, care anterior erau imposibil de implementat în medii cu nivel redus de energie, pot fi acum susținuți de noile generații de procesoare, pe măsură ce acestea devin mai puternice și mai eficiente din punct de vedere energetic.

4.3 Tehnologia si securitatea dispozitivelor de tip smart card

Smart-cardurile au apărut ca o soluție fiabilă și eficientă pentru stocarea sigură a cheilor criptografice și pentru procesarea datelor critice [7]. Smart-cardurile sunt dispozitive de dimensiuni reduse care conțin memorie încorporată și microprocesoare.

Smart-cardurile sunt utilizate în diferite aplicații și industrii [2], inclusiv: (i) Instituțiile bancare oferă clienților smart-carduri pentru a facilita plățile electronice, inclusiv carduri de debit și de credit; (ii) Companiile de transport implementează diverse smart-carduri ca metodă convenabilă de plată pentru utilizatorii transportului public; (iii) Guvernele emit documente de identificare, precum pașapoarte, cărți de identitate naționale și permise de conducere, care se bazează pe smart-carduri; (iv) Sistemele de sănătate utilizează smart-carduri pentru a stoca informații despre pacienți și pentru a oferi acces securizat la înregistrările medicale; (v) Controlul accesului impune utilizarea unui smart-card pentru identificarea angajaților și pentru a permite accesul acestora în diferite zone.

Alegerea limbajului de programare și a platformei depinde de cerințele specifice ale aplicației, deoarece fiecare platformă are propriile puncte forte și slabe. Pentru Java Card, există o comunitate mare de dezvoltatori și o gamă largă de instrumente și biblioteci disponibile. În cazul DotNET Card, o platformă relativ nouă, se oferă integrare cu framework-ul .NET și un mediu de dezvoltare de ultimă generație.

4.4 Proiectarea unui overlay de stocare pentru dispozitive mobile

În această secțiune, propunem un overlay nou de criptare a datelor stocate în cloud. Această soluție poate fi implementată pe dispozitive de tip smartphone, si prezintă caracteristici ce o fac rezistentă la furtul de chei private și malware. Utilizarea acestui overlay este foarte utila în minimizarea impactului unui atac cibernetic ce a avut ca rezultat compromiterea credentialelor de acces în cloud. Mai întâi, vom descrie arhitectura sistemului și apoi alte aspecte relevante legate de funcționalitate.

4.4.1 Architectură

Unul dintre cele mai sensibile aspecte în ceea ce privește sistemele criptografice este gestionarea cheilor, deoarece stocarea acestora pe un computer conectat la internet este indezirabila. Pentru a depăși această problemă, propunem migrarea datelor sensibile către un alt domeniu de încredere. Acest domeniu de încredere este un smart-card programabil, îmbunătățit cu un co-procesor criptografic și alimentat prin inducție electromagnetică. Deși un smart card necesită configurare și reprezinta un cost financiar suplimentar, acesta garantează un nivel mai înalt de securitate în vederea protejării datelor sensibile.

4.4.2 Applet-ul Java Card

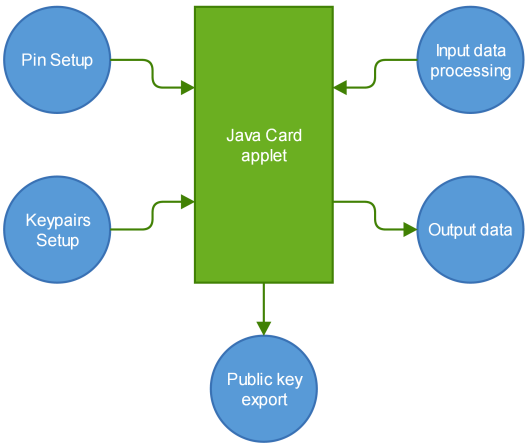

Figure 4.1. Prezentare generală a arhitecturii applet-ului Java Card

Java Card este o tehnologie destinată dispozitivelor embedded cu consum redus de energie, pentru a le permite să ruleze în mod securizat diverse aplicații, cunoscute sub numele de applet-uri. Ecosistemul smart-cardurilor este foarte prohibitiv, nepermițând exportarea sau manipularea applet-urilor, în conformitate cu diverse politici impuse de bănci și guverne. Propunerea noastră, ilustrată în Figura 4.1, referitoare la applet implică o implementare software protejată printr-un cod PIN și stochează în siguranță un set de chei pentru a efectua criptarea datelor pentru fișierele care vor fi transferate catre medii de stocarea cloud publice sau private. Comunicarea cu cardul se va realiza prin intermediul tehnologiei NFC (Near Field Communication) pentru instalarea applet-ului, autentificarea cu PIN, criptarea simetrică, decriptarea simetrică, calculul integrității, verificarea integrității, criptarea asimetrică și decriptarea asimetrică.

4.4.3 Stocarea datelor

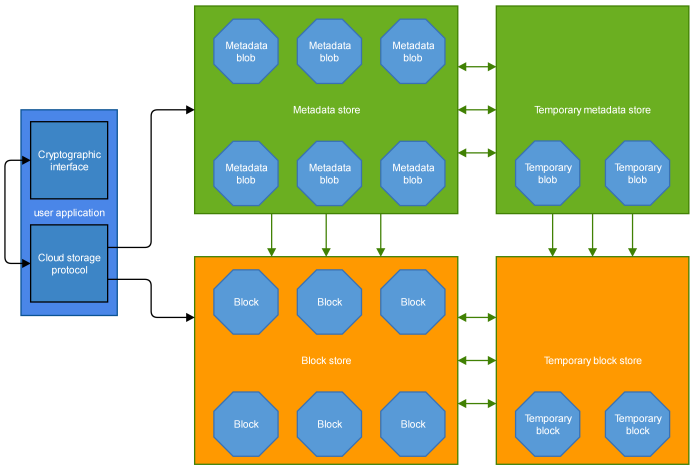

Figure 4.2. Prezentare generală a arhitecturii.

Modul de stocare al datelor gestionate de aplicația noastră, ilustrat în Figura 4.2, va fi implementat într-un mod care nu va permite unui atacator să afle informații despre numele fișierelor, dimensiunile și conținutul acestora. Pentru a obține caracteristicile menționate anterior, este necesara implementarea unui modul software ce are ca scop integrarea cu mai mulți furnizori de servicii de stocare Cloud. Configurația de stocare presupune împărțirea în patru zone distincte: metadate, metadate temporare, blocuri și blocuri temporare. Această separare va asigura divizarea fișierelor, criptarea numelui fișierelor, consistența și criptarea datelor. Zona de metadate va conține descriptori criptați care conțin informații despre numele real al fișierului, dimensiunea fișierului și identificatorii de blocuri. Zona de metadate temporare este o locație intermediară folosită pentru a stoca în siguranță metadate tranziente generate în timpul procesului de criptare.

Scopul zonei de blocuri este acela de a stoca fișiere individuale care conțin informații securizate rezultate din operațiuni de criptare și divizare a fișierelor. Blocurile se vor stoca în fișiere cu nume aleatorii, pentru a preveni divulgarea numelui real al fișierului. Pentru a asigura consistența, până când operația de criptare a fișierului a fost finalizată, datele intermediare vor fi încărcate în zona de blocuri temporare. După ce o operație de criptare a fost finalizată cu succes, datele sunt mutate din zonele de date temporare în zonele implicite. Orice fișier temporar va avea numele generat în mod aleatoriu.

4.5 Concluzii

Nivelul de consum energetic asociat unui algoritm de criptare nu corespunde neapărat gradului de securitate al acestuia. Puterea unui algoritm de criptare depinde de complexitatea matematică a acestuia și de dimensiunea cheii de criptare utilizată pentru securizarea datelor.

Pentru a îmbunătăți securitatea și a proteja datele extrem de sensibile, telefoanele și smart-cardurile pot fi utilizate în mod complementar. Smart-cardurile pot fi utilizate și prin interfața Near Field Communication (NFC). În cazul în care un smartphone este compromis, cheile private stocate pe smart-card nu pot fi accesate de către un atacator. Această abordare are potențialul de a minimiza impactul unui incident, atâta timp cât adversarul nu are acces fizic la smart-card.

5 | Overlay-uri scalabile

În prezent, majoritatea site-urilor web sunt criptate prin intermediul protocolului HTTPS. Cu toate acestea, există încă anumite riscuri legate de sistemul DNS. Într-un astfel de scenariu, înainte de a încărca orice site web criptat, browserul transmite o cerere de rezolvare a numelui DNS pentru a determina adresa de internet asociată domeniului solicitat de utilizator.

5.1 Cenzura și instrumentele de protecție a confidențialitate în era digitală

Activitățile online sunt omniprezente în viața de zi cu zi, dar mulți oameni nu sunt conștienți cât de multă informație dezvăluie prin accesarea diferitelor servicii. Chiar și cu traficul criptat, furnizorii de servicii de internet pot deduce date private despre software-ul clienților lor, interesele și obiceiurile acestora.

Pentru a minimiza impactul profilării, utilizatorii de servicii de internet pot recurge la utilizarea rețelelor de tip overlay. Utilizarea acestor overlay-uri facilitează transferul datelor utilizând adrese virtuale.

În funcție de strategia de monitorizare a unui furnizor de servicii de internet, tiparele de acces la rețea generate de aceste instrumente pot atrage în mod efectiv atenția autorităților, chiar dacă utilizatorii acestor sisteme nu desfășoară activități ilegale.

5.2 Ascunderea tiparelor de acces la rețeale de tip Cloud-Edge

Instrumentele de confidențialitate în internet, precum fi Tor, Freenet, I2P, GnuNet și Loki Network, oferă o multitudine de cazuri legitime de utilizare pentru persoanele care acordă prioritate confidențialității și securității online. Aceste instrumente pot fi utilizate de către jurnaliști pentru a proteja sursele și a asigura transmiterea securizată a informațiilor sensibile.

Pentru a îmbunătăți confidențialitatea și pentru a împiedica firewall-urile avansate să blocheze conectivitatea, Proiectul Tor a introdus conceptul de Pluggable Transports (PTs), o colecție de module software care sunt utilizate pentru a masca traficul Tor, făcându-l mai dificil de detectat și obstrucționat de către cenzori.

Sistemele de tip Pluggable Transports reprezintă un instrument crucial pentru utilizatorii care doresc să evite cenzura pe internet și să-și protejeze confidențialitatea online. Datorita faptului ca traficul generat de acestea este dificil de detectat și blocat de către cenzori, acestea contribuie la asigurarea rezilienței rețelei Tor pentru utilizatorii din întreaga lume.

5.3 Proiectarea unui sistem de tip Ovelay multi-platformă pentru asigurarea confidențialității rețelei

Evitarea cenzurii și supravegherii din partea diverselor furnizori de servicii de internet (ISP) poate fi realizată utilizând soluția propusă de noi, care constă într-un set de instrumente de anonimizare ce au ca scop mascarea utilizării diferitelor protocoale într-un mod scalabil. Pentru a asigura compatibilitatea cu aplicațiile existente, soluția noastră implementează o interfață de proxy SOCKS5. Principala funcție a acestui proxy este divizarea și transmiterea mesajelor de ieșire către diferite canale de comunicare, precum AllJoyn, Irc Chat și XMPP chat. Implementarea noastră a fost proiectată pentru obfuscarea tiparelor de acces la rețeaua de stocare Cloud și transferul de date cu latență redusă. Pentru a împiedica detectarea traficului generat de implementarea noastră la nivel de rețea, punctele terminale trebuie să fie implementate atât pe mașina utilizatorului, cât și pe o mașina dintr-o infrastructura a unui furnizor de servicii Cloud. Utilizând această abordare, tiparele de trafic devin mai complexe și, prin urmare, mai greu de identificat.

5.3.1 Reutilizarea XMPP pentru obfuscarea traficului

Soluția noastră poate fi configurată cu una sau mai multe opțiuni dintr-o listă de canale de transport predefinite. Deoarece un canal de transport este stabilit între roboți folosind un serviciu de chat (conform Figurii 1), este necesară crearea unui cont pentru a asigura comunicarea.

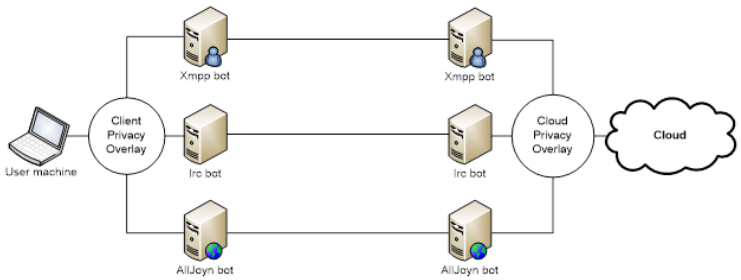

Figure 5.1. Arhitectura propusă.

Soluția noastră se bazează pe protocoale care operează la nivelul transport al modelului OSI (conform Figurii 5.2). Am ales protocoale de mesagerie deoarece pot fi ușor adaptate pentru transferul oricărui tip de date în mod full-duplex. Pentru a depăși eventualele probleme de viteză cauzate de limitarea lățimii de bandă, am utilizat simultan diferite servicii de chat.

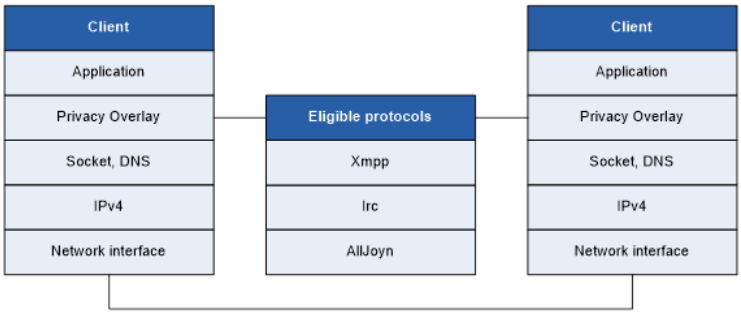

Figure 5.2. Integrarea overlay-ului de securitate la nivel de rețea.

Arhitectura noastră se bazează pe două componente high-level: un obfuscator de trafic de rețea și un deobfuscator de trafic de rețea.

Interfața compatibilă cu SOCKS5 este o componentă creată special pentru a asigura integrarea cu software-ul existent. Astfel, aplicațiile care pot utiliza un proxy SOCKS5 pot beneficia de acest overlay de confidențialitate fără a avea nevoie de alte modificări.

5.3.2 Interfața overlay-ului SOCKS5

Implementarea noastră își propune să ofere o integrare facilă cu aplicațiile existente, prin combinarea unui proxy local SOCKS5 cu diverse protocoale legitime care permit manipularea și încapsularea unui volum mare de date. Astfel de protocoale sunt utilizate în principal de serviciile de chat text.

Am implementat și analizat performanta un server proxy SOCKS5 multiplatformă Figure 5.3, care va fi folosit pentru a captura date generate de aplicație. Serverul nostru proxy folosește un set limitat de instrucțiuni SOCKS5. În prezent, acceptă doar metoda TCP CONNECT și nu oferă nicio metodă de autentificare.

Managerul de conexiuni rulează într-un fir separat. Dacă o cerere a fost transmisă către un server, acesta folosește un handler de protocol specific sesiunii pentru a evalua cererile și, în funcție de rezultatul obținut, acesta își comunica rezoluția.

Orchestratorul TCP este responsabil pentru crearea și gestionarea conexiunilor multiple. De asemenea, direcționează datele generate de solicitări reale către client.

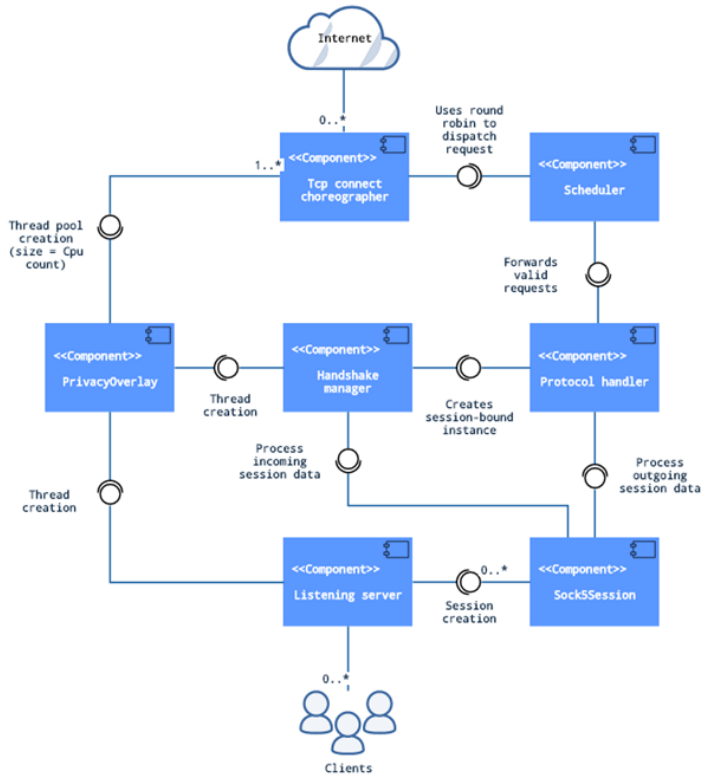

Figure 5.3. SOCKS5 local server high-level architecture.

Am efectuat mai multe testele, modificând timpul implicit de solicitare pentru a reduce rata de eroare. Execuție s-a realizat fără erori când am configurat valoarea implicită de expirare a cererii la 10 secunde.

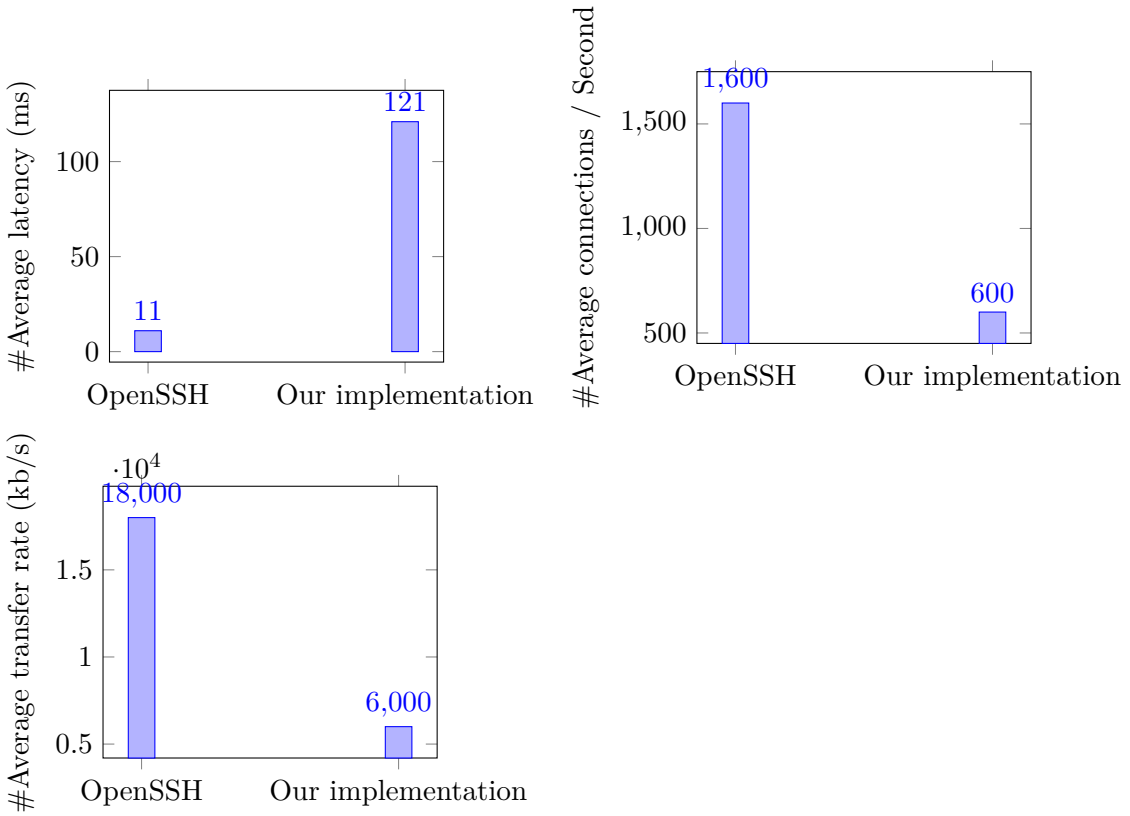

Figure 5.4. Evaluare de performanță.

5.4 Concluzii

Ca răspuns la practicile non-etice de supraveghere, noi proceduri de îmbunătățire a confidențialității sunt cercetate în mod constant pentru a evita cenzura și utilizarea abuzivă a datelor cu caracter personal. Soluția noastră este centrată pe ideea că fiecare persoană are dreptul de a fi anonimă și are control complet asupra datelor sale.

Soluția noastră își propune să ofere o noua metodă de integrare cu rețelele definite software, utilizând protocolul SOCKS5. Chiar dacă ideea nu este nouă, aveam nevoie de o soluție software care să nu aibă dependințe externe și o bază de cod de dimensiuni relativ reduse, ușor de întreținut.

Cu toate acestea, mai sunt încă probleme deschise în specificarea unui protocol de tip overlay fiabil și în alegerea unei metodologii pentru a spori încrederea între entitățile care comunică. Soluția noastră nu are scopul de a înlocui un overlay de confidențialitate existent, ci de a interopera cu alte servicii, pentru a ocoli cenzura și supravegherea. Chiar dacă această soluție ar putea fi folosită în scopuri discutabile, recunoaștem faptul că fiecare persoană are libertatea de a decide cum să folosească internetul.

6 | Îmbunătățirea confidențialității prin intermediul steganografiei

Încă din cele mai vechi timpuri, steganografia a fost folosită pentru a ascunde mesaje secrete. Metodele steganografice au fost rafinate și transformate de multe descoperiri științifice de-a lungul timpului. În informatică, steganografia poate fi folosită pentru a ascunde informații private prin diferite metode și tehnici.

Acest capitol explorează utilizarea steganografiei în fișiere multimedia pentru a ascunde datele confidențiale. Acest studiu examinează caracteristicile fișierelor MKV in vederea aplicării de tehnici steganografice.

Implementarea propusă de noi utilizează elemente specifice Matroska [6] pentru a stoca date suplimentare într-un astfel de fișier multimedia, fără a afecta caracteristicile cadrelor video.

6.1 Formatul Matroska

Matroska Video (MKV) este un format de container multimedia binecunoscut ce poate stoca o mare varietate de tipuri de media, inclusiv video, audio, subtitrări și imagini statice. A fost creat în 2002 ca un format de container open-source, iar acum este întreținut de grupul nonprofit Matroska.org.

Extensible Binary Meta Language (EBML) este folosit pentru a specifica structura fișierului în formatul Matroska Video (MKV). Fiecare element din fișier primește o etichetă specifică, cunoscuta sub numele de ID EBML. Aceste ID-uri sunt folosite pentru a specifica poziționarea fiecărui element în cadrul unui fișier, precum și formatul acestuia.

ID-urile EBML care sunt utilizate frecvent în fișierele MKV includ:

- EBMLHeader (ID: 0x1A45DFA3): Acest ID marchează începutul fișierului și oferă informații despre versiunea de EBML utilizată și dimensiunea fișierului.
- Segment (ID: 0x18538067): Acesta este elementul principal dintr-un fișier MKV și conține toate celelalte elemente care urmează acestuia.
  Informații
- (ID: 0x1549A966): Acest element conține informații generale despre fișierul MKV, cum ar fi durata, data creării și titlul.
- Atașamente (ID: 0x1941A469): Acest element conține fișiere suplimentare care sunt legate de fișierul MKV, cum ar fi coperta, subtitrări sau piese audio suplimentare.
- Void (ID: 0xEC): Acest element este de tip rezervat și este utilizat în principal pentru alinieri specifice impuse de structura EBML.

Specificația Matroska, care este disponibilă pe site-ul https://matroska.org/technical/basics.html, conține lista completă a ID-urilor EBML.

Analizând în continuare specificațiile, am ajuns la concluzia că elementele de tip Void sau Attachment ar fi un purtător ideal pentru informații ascunse, deoarece modificarea acestora nu afectează calitatea video.

Având în vedere faptul că datele ascunse steganografic pot fi detectate, este foarte recomandabil ca utilizatorii să le protejeze confidențialitatea cu metode de criptare fiabile.

6.2 Criptarea volumelor folosind dm-crypt

Dm-crypt [9] este un subsistem pentru criptarea discurilor în Linux, care oferă criptarea transparentă a dispozitivelor de tip bloc. Este un modul criptografic la nivelul kernelului care facilitează crearea de partiții sau volume criptate, permițând astfel stocarea securizată a datelor pe dispozitive de stocare precum unitățile cu stare solidă (SSD-uri), hard disk-uri sau stick-uri USB.

Dm-crypt este folosit pe scară largă în sistemele de operare bazate pe Linux pentru a oferi criptarea datelor stocate. Chiar și în cazul în care dispozitivul este compromis fizic sau furat, datele rămân protejate. Această capacitate a fost evidențiată și în literatură, după cum menționează Richter et al. în introducerea lor despre criptarea datelor [8].

În scenariile de utilizare tipice care implică dm-crypt, criptarea este aplicată unei partiții sau unui volum începând de la poziția 0. În scenariul nostru specific, care implică steganografia, este dezirabila încapsularea unui volum criptat într-un fișier purtător.

6.3 Soluția propusă : Hidden in the Void

De fiecare dată când un utilizator creează un volum criptat pentru a fi utilizat cu dm-crypt, acesta poate folosi încapsularea "plain dm-crypt with offset". Fișierul rezultat va conține date aleatoare și un volum criptat la o poziție prestabilita.

În linii mari, scopul software-ului nostru este de a citi toate metadatele MKV dintr-un fișier și de a le combina cu un container dm-crypt, pentru a obține un nou fișier MKV care poate fi deschis în orice player media, dar și montat ca un volum pentru a accesa datele criptate.

```
 private static void bindFiles() throws IOException {
   final List<Element> elementList =
    Reader.getAllElementsFromFile(INPUT_MKV);
   final Writer writer = Writer.aBuilder()
         .setElementList(elementList)
         .setInputFile(INPUT_MKV)
         .setOutputFile(OUTPUT_MKV)
         .setEmbeddableFile(CONTAINER)
         .build();
   writer.assemble();
}
```

Listing 6.1. Top level code snippet

Modificarea elementelor EBML ce alcătuiesc un fișier MKV poate afecta compatibilitatea cu diverse codec-uri, și prin urmare, generăm un fișier de ieșire nou ori de câte ori dorim să adăugăm date suplimentare. Aceasta abordare face ca implementarea noastră sa nu altereze fișierele de intrare, în eventualitatea întreruperii neplanificate a procesului.

6.4 Rezultate

Utilizarea soluției noastre poate avea implicații complexe și specifice contextului. Poate fi un instrument util pentru securitate și confidențialitate, dar poate fi folosit și în

scopuri non-etice. Din perspectiva securității, poate fi aplicat ca metodă de protejare a informațiilor sensibile sau private.

Pentru a demonstra avantajele soluției noastre propuse, am realizat un experiment pentru a măsura variația entropiei indusă de instrumentul nostru. Am obținut entropia inițială a fișierului MKV și entropia fișierului purtător utilizând implementarea software "ent". Rezultatele studiului nostru demonstrează că metodologia utilizată a dus la o reducere a entropiei, chiar și atunci când a fost folosit un container criptat. Scaderea entropiei se datorează introducerii voluntare de date adiționale nesemnificative cu entropie redusă în elementul Void.

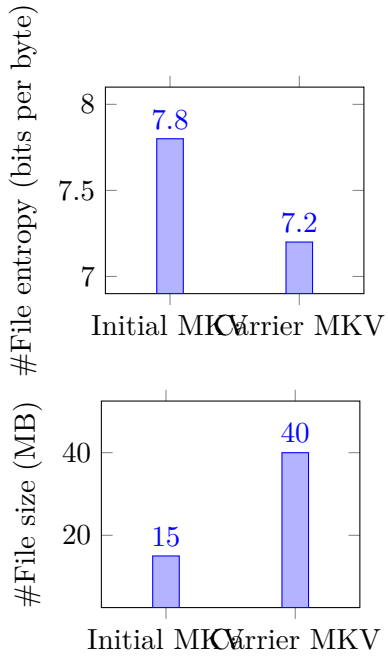

Figure 6.1. File entropy and size comparison using the Linux ent tool.

Un alt scenariu de utilizare pentru implementarea noastră este detectarea automată a steganografiei. Software-ul nostru poate analiza fișierele MKV cu precizie, identificând rapid elementele necunoscute. Încercarea de a vizualiza un fișier MKV malformat va rezulta întotdeauna într-o eroare. Soluția noastră poate detecta elemente MKV invalide de trei ori mai rapid (Figura 6.2) decât instrumentul open-source MKVInfo. Pentru a demonstra acest fapt, am dezvoltat un script shell și am comparat viteza la care ambele metode rezolvă problema.

```
#!/bin/bash
var=$(mkvinfo -v $@ | grep -c Unknown)
if [ $var > 0 ]; then echo "suspect for steganography"
else echo "valid"
fi
```

Listing 6.2. MKV anomaly detection script (mkvhunt.sh) .

Am comparat, de asemenea, viteza pentru diferite dimensiuni ale fișierelor de intrare, pentru a observa că metoda noastră se adaptează linear. În acest context, scalabilitatea se referă la capacitatea unui sistem de a gestiona sarcini de lucru în creștere fără a experimenta o scădere semnificativă a performanței. Prin evaluarea diferitelor dimensiuni ale

datelor de intrare prin benchmarking, am evaluat scalabilitatea sistemului nostru și am determinat că poate gestiona eficient seturi de date mari.

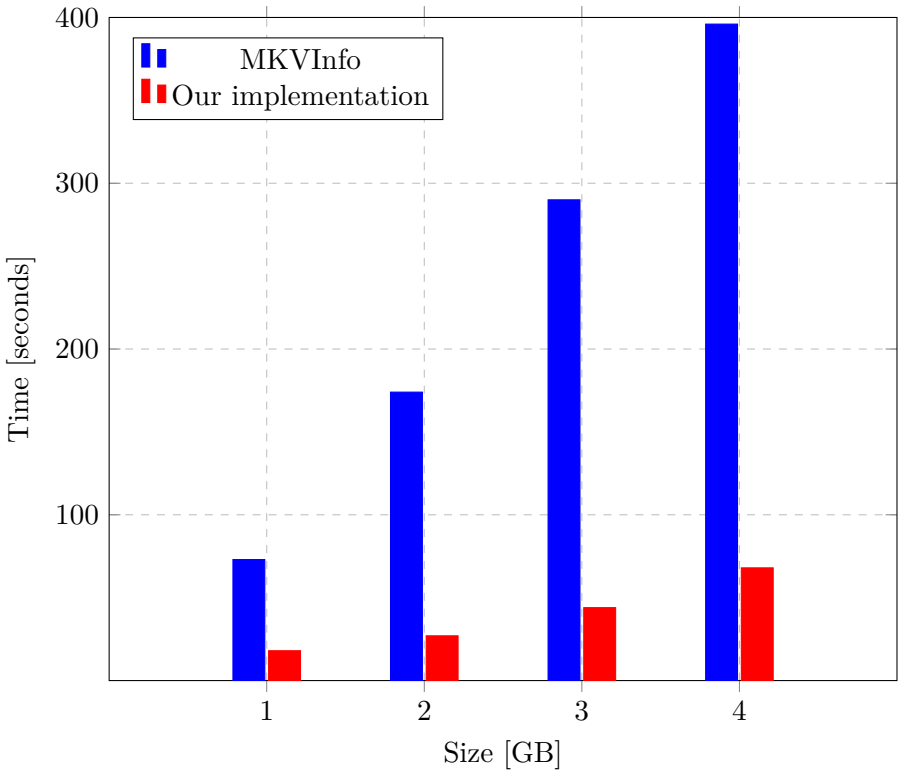

Figure 6.2. Speed comparisons using different file sizes.

Ca o posibilă direcție viitoare, instrumentul nostru ar putea fi integrat cu software-ul de investigații open-source, Autopsy, pentru a identifica date ascunse în fișiere MKV. Suplimentar, software-ul nostru are potențialul de a fi extins pentru a identifica anomalii și a calcula entropia elementelor individuale EBML dintr-un fișier MKV.

Utilizarea non-etică a instrumentului nostru de steganografie este dificil de detectat, în principal pentru că încapsulează date în structuri valide din interiorul unui fișier video MKV. Cercetarile viitoare ar putea fi concentrată asupra dezvoltării unor instrumente de digital forensics capabile să detecteze metodele noastre. Deoarece implementarea software-ului nostru a fost dezvoltată utilizând Java, aceasta poate fi ușor transformată într-un plugin pentru aplicația Autopsy.

7 | Concluzii și direcții de cercetare ulterioare

7.1 Concluziile tezei

CCriptarea este un principiu fundamental în domeniul securității informațiilor și este de importanță primordială în protejarea datelor sensibile. Aceasta implică transformarea datelor clare și comprehensibile într-un format codificat care poate fi accesat sau înțeles doar de către persoanele autorizate. Principalele concluzii ale acestei teze sunt:

- Criptarea este importantă pentru protejarea datelor sensibile, dar există probleme legate de aplicarea sa, inclusiv, dar fără a se limita la managementul cheilor, compromiterea cheilor, erori de implementare, probleme de compatibilitate și costurile suplimentare de performanță, toate acestea fiind riscuri potențiale asociate cu criptarea;
- Algoritmi de criptare robusti, gestionarea atentă a cheilor și respectarea celor mai bune practici din industrie pot ajuta la reducerea acestor riscuri;
- Suprapuneri de criptare, cum ar fi criptarea la nivel de client sau criptarea de la un capăt la celălalt, pot oferi un nivel suplimentar de protecție pentru stocarea în cloud.

Relația dintre procesarea în Cloud și smartphone-uri este puternic interdependentă, rezultând o asociație reciproc benefică care amplifică capacitățile și funcționalitățile dispozitivelor mobile. Utilizarea tehnologiei de calcul în Cloud permite smartphone-urilor să acceseze o gamă vastă de resurse de calcul, aplicații și servicii de stocare prin intermediul internetului, fără a se baza exclusiv pe puterea de procesare și capacitatea de stocare limitate ale dispozitivului în sine.

În capitolul Algoritmi de îmbunătățire a nivelului de încredere în comunicarea de tip oportunistic am analizat modul în care smartphone-urile pot îmbunătăți autentificarea serviciilor în cloud prin utilizarea datelor de la senzori în scenarii dependente de context.

- Dispozitive identice pot afișa valori de senzori ușor diferite din cauza variațiilor de fabricație și a factorilor de mediu;
- Calibrarea în timpul fabricației contribuie la asigurarea datelor precise și fiabile ale senzorilor;
- Filtrarea și normalizarea citirilor senzorilor pot îmbunătăți precizia și consistența proceselor de autentificare a utilizatorilor;
- Stabilirea unei limite pentru citirile senzorilor poate elimina datele neesențiale și evidenția modelele sau comportamentele relevante pentru crearea profilului utilizatorului;
- Includerea unei limite poate îmbunătăți precizia și relevanța creării profilului utilizatorului prin datele senzorilor mobili.

Pentru a stabili comunicarea cu sistemele bazate pe cloud, precum și cu dispozitive cu resurse limitate, cum ar fi smartphone-urile, utilizarea criptografiei este imperativă. În

capitolul Primitive criptografice cu consum redus de energie am analizat impactul criptării asupra dispozitivelor cu restricții de resurse.

- Criptarea cu consum redus de energie este importantă pentru dispozitivele cu capacități de procesare și durată de viață a bateriei limitate, cum ar fi dispozitivele IoT și mobile. Prin urmare, criptarea cu consum redus de energie poate îmbunătăți performanța dispozitivelor și durata de viață a bateriei;
- Puterea unui algoritm de criptare depinde de complexitatea sa matematică și de dimensiunea cheii de criptare, nu doar de consumul de energie;
- Smartphone-urile sunt vulnerabile la malware și furt fizic, iar utilizarea cardurilor inteligente în combinație cu telefoanele poate îmbunătăți securitatea.

Cu toate acestea, metadatele protocolului pot furniza singure informații valoroase. Când sunt integrate cu alte surse de date, acestea pot îmbunătăți profilul comportamentului utilizatorului și prezența digitală. Prin urmare, în capitolul Overlay-uri scalabile am analizat instrumentele de anonimizare existente care furnizează rețele de suprapunere pentru a aborda scurgerile de metadate, în contextul supravegherii digitale și a cenzurii.

- Metodele de îmbunătățire a confidențialității rețelei sunt cercetate în mod continuu pentru a evita cenzura și a preveni utilizarea greșită a datelor personale;
- Suprapunerea rețelelor, cunoscută și sub numele de rețele definite prin software, este o tehnică de îmbunătățire a rețelei care poate fi definită utilizând software, deschizând noi oportunități în domeniul cercetării în securitate;
- Rețelele de suprapunere rezolvă problemele de confidențialitate generate de profilarea protocolului de rețea și supraveghere prin mascarea traficului utilizând diferite protocoale de transport, precum servicii de chat sau jocuri;
- Pentru a proiecta și opera astfel de instrumente de anonimizare a rețelei, este important să se ia în considerare aspecte precum dimensiunile mesajelor, modelele de comunicare și limitele de lățime de bandă.

În capitolul Îmbunătățirea confidențialității prin intermediul steganografiei am analizat tehnici cunoscute de steganografie aplicate fișierelor multimedia.

- Steganografia a fost utilizată încă din antichitate pentru a ascunde mesaje secrete. În informatică, steganografia poate fi folosită pentru a ascunde informații private prin diverse metode și tehnici;
- Fișierele multimedia reprezintă o opțiune viabilă pentru steganografie datorită dimensiunii lor relativ mari. În plus, acestea sunt frecvent schimbate prin diverse canale de comunicare, făcându-le un mijloc ideal pentru transportul mesajelor sau datelor ascunse.

7.2 Contribuții originale

Contribuțiile principale prezentate în aceste capitole oferă perspective valoroase pentru discutarea securității în contextul stocării în cloud.

Putem concluziona că principalele contribuții ale cercetării la această teză sunt:

- Evaluarea tehnologică a mai multor furnizori de stocare în cloud public pentru identificarea caracteristicilor lor cheie, punctelor forte și punctelor slabe, așa cum este detaliat în Capitolul 2, Îmbunătățirea confidențialității în medii de tip Cloud-Edge;
- Analiza potențialului îmbunătățirii securității sesiunilor utilizatorilor mobili prin colectarea datelor de la senzorii hardware și virtuali, pe măsură ce smartphone-urile se bazează tot mai mult pe medii cloud pentru a efectua mai multe sarcini, așa cum

se poate observa în Capitolul 3, Algoritmi de îmbunătățire a nivelului de încredere în comunicarea de tip oportunistic;
- Analiza impactului consumului energetic al diferitelor algoritmi de criptare cu consum redus de energie în comunicarea cu dispozitive cu resurse limitate, cum ar fi bateria și resursele computaționale, așa cum este prezentat în Capitolul 4, Primitive criptografice cu consum redus de energie;
- Analiza componentelor fundamentale ale rețelelor de suprapunere definite prin software, cum ar fi Tor și I2P, pentru a introduce conceptele, principiile și tehnologiile esențiale necesare pentru a obține confidențialitate, securitate și anonimat online, așa cum este detaliat în Capitolul 5, Overlay-uri scalabile;
- Discuția despre implementarea diverselor tehnici de steganografie pentru fișierele multimedia digitale în Capitolul 6, Îmbunătățirea confidențialității prin intermediul steganografiei, cu scopul de a oferi o imagine de ansamblu a progreselor care au apărut de-a lungul timpului și pentru a crește gradul de conștientizare cu privire la metodele și motivele de ascundere și transmitere în mod secret a informațiilor.

7.3 Lista de publicații

Pentru a valida descoperirile noastre, am publicat mai multe articole în prestigioase conferințe și reviste internaționale, după cum urmează: International Journals as follows:

1. **Apostol, G. C.**, Mocanu, A.-E., Mocanu, B. C., Radulescu, D., Negru, C., Petre, I. & Pop, F., In Studies in Informatics and Control, 1220-1766, 2023, https://doi.org/10.24846/v32i2y202310;

2. Mocanu, A.-E., Mocanu, B.-C., **Apostol, G. C.**, Negru, C., Petre, I. & Pop, F., In 24th International Conference on Control Systems and Computer Science (CSCS24) 2023. IEEE. Accepted;

3. **Apostol, G. C.**, Mocanu, A. E., Mocanu, B. C., Radulescu, D. M., & Pop, F. (2023, February). CPSOCKS: Cross-Platform Privacy Overlay Adapter Based on SOCKSv5 Protocol. In Green, Pervasive, and Cloud Computing: 17th International Conference, GPC 2022, Chengdu, China, December 2–4, 2022, Proceedings (pp. 149-161). Cham: Springer International Publishing;

4. **Apostol, G. C.**, Mocanu, B. C., Radulescu, D. M., Petre, I., & Pop, F. (2022, September). Hiding Cloud network access patterns for enhanced privacy. In 2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet) (pp. 1-5). IEEE;

5. Mocanu, B. C., **Apostol, G. C.**, Radulescu, D. M., & Serbanescu, C. (2022, July). TrustS: Probability-based trust management system in smart cities. In 2022 21st International Symposium on Parallel and Distributed Computing (ISPDC) (pp. 65-69). IEEE.

6. **Apostol, G. C.**, Borcea, L., Dobre, C., Mavromoustakis, C. X., & Mastorakis, G. (2021). A Survey on Privacy Enhancements for Massively Scalable Storage Systems in Public Cloud Environments. Big Data Platforms and Applications: Case Studies, Methods, Techniques, and Performance Evaluation, 207-223;

7. **Apostol, G. C.**, & Pop, F. (2016, May). MICE: Monitoring high-level events in Cloud environments. In 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 377-380). IEEE.

7.4 Direcții viitoare de cercetare

Domeniul de cercetare privind îmbunătățirea confidențialității pentru serviciile publice de stocare în cloud prezintă numeroase probleme nerezolvate care necesită investigații suplimentare. În timp ce cercetarea noastră a oferit perspective valoroase, există încă mai multe probleme urgente care necesită investigații suplimentare. Aceste probleme pot fi prezentate în următoarele moduri:

- Îmbunătățirea conștientizării și educației utilizatorilor reprezintă un aspect crucial în contextul calculului în cloud, deoarece contribuie la creșterea înțelegerii riscurilor de confidențialitate și a celor mai bune practici printre utilizatori.
- Viitoarea cercetare ar trebui să vizeze abordarea preocupărilor de confidențialitate care rezultă din colectarea și modelarea datelor de la senzori de pe smartphone-uri, cu accent deosebit asupra măsurilor care pot fi luate pentru a asigura securitatea acestor date.
- Dezvoltarea viitoare ar trebui să se concentreze pe integrarea și compatibilitatea algoritmilor de criptare post-cuantici cu infrastructurile, protocoalele și standardele actuale de carduri inteligente. Scopul este de a asigura o integrare fără probleme a acestor algoritmi cu sistemele existente.
- Accentul cercetării viitoare ar putea fi pus pe îmbunătățirea rezistenței transporturilor pluggable TOR în fața eforturilor de detectare și blocare de către cenzori. Obiectivul este de a dezvolta strategii care pot reduce în mod eficient impactul acestor eforturi asupra funcționalității transporturilor pluggable.
- Viitoarea cercetare ar trebui să abordeze provocările puse de steganaliză, care este procesul de detectare a prezenței datelor ascunse în media. Dezvoltarea tehnicilor de steganografie care pot rezista diverselor metode de steganaliză, menținând totodată o probabilitate redusă de detectare, reprezintă o sarcină dificilă.

Bibliography

[1] Norihiro Fukumoto, Shigehiro Ano, and Shigeki Goto. Passive smart phone identification and tracking with application set fingerprints. *Proceedings of the Asia-Pacific Advanced Network*, 36:41–48, 2013.

[2] Mike Hendry. *Multi-application smart cards: technology and applications*. Cambridge university press, 2007.

[3] Dropbox Inc. Dropbox business security (white paper). https://www.dropbox.com/static/business/resources/Security_Whitepaper.pdf, 2015. Accessed: 2016-06-12.

[4] Umer Khalid, Abdul Ghafoor, Misbah Irum, and Muhammad Awais Shibli. Cloud based secure and privacy enhanced authentication & authorization protocol. *Procedia Computer Science*, 22:680–688, 2013.

[5] Threat Metrix. Device fingerprinting and fraud protection whitepaper.

[6] Nikolaos Pitropakis, Costas Lambrinoudakis, Dimitris Geneiatakis, and Dimitris Gritzalis. A practical steganographic approach for matroska based high quality video files. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pages 684–688. IEEE, 2013.

[7] Wolfgang Rankl and Wolfgang Effing. *Smart card handbook*. Wiley, 2010.

[8] Jan Richter. An introduction to luks disk encryption. In *Annual Digital Forensic Research Workshop*. Citeseer, 2010.

[9] Herbert Robertson. dm-crypt: Transparent disk encryption subsystem for linux. In *Linux Symposium*, 2007.

[10] Irvin Zhan. Dnscatproxy: A pluggable transport based on dns tunneling, 2015.