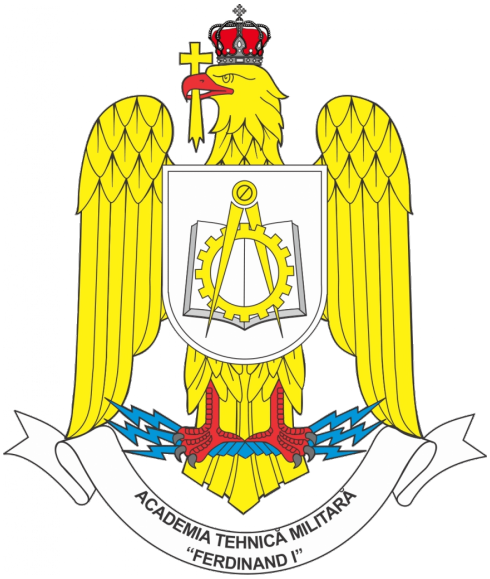
România
Ministerul Apărării Naționale
Academia Tehnică Militară "*Ferdinand I*"

Facultatea de Sisteme Informatice și Securitate Cibernetică
Specializarea Absolvită



Titlul Lucrării

Coordonator Științific
Grad Prenume NUME

Absolvent
Grad Prenume NUME

Conține _____ file
Inventariat sub numărul _____
Cu poziția din indicator _____
Cu termen de păstrare _____

București
An

Abstract

Rezumatul în limba română trebuie să reflecte fidel conținutul lucrării, subliniind contextul, obiectivele, metodologia, rezultatele și concluziile principale. Păstrează o dimensiune similară cu versiunea în limba engleză și evită introducerea de informații care nu apar în capitole.

Cuvinte cheie: inteligență artificială; criptografie; securitate cibernetică; evaluare

Cuprins

List of Tables

Listă de Abrevieri

AI ..... artificial intelligence

ML ..... machine learning

PKI ..... public key infrastructure

RAG ..... retrieval-augmented generation

TLS ..... transport layer security

Capitolul 1: Introducere

1.1 Context general

Prezintă pe scurt evoluția criptografiei moderne și modul în care tehnologiile de inteligență artificială influențează securitatea cibernetică.

1.2 Problema abordată

Descrie problema principală a lucrării, pornind de la nevoile identificate în domeniul securității cibernetice asistate de AI.

1.3 Scopul lucrării

Formulează clar scopul general al proiectului și rezultatul urmărit prin dezvoltarea utilitarului criptografic asistat de AI.

1.4 Obiective specifice

Prezintă obiectivele concrete ce trebuie îndeplinite pentru atingerea scopului.

- O1 – Definirea cadrului teoretic și a cerințelor specifice aplicației.
- O2 – Proiectarea arhitecturii soluției propuse.
- O3 – Implementarea componentelor software și integrarea acestora.
- O4 – Validarea soluției prin scenarii de testare reprezentative.

1.5 Structura lucrării

Include o prezentare succintă a fiecărui capitol pentru a ghida cititorul prin document.

Capitolul 2:
Fundamente Teoretice

2.1 Elemente de bază ale criptografiei

Prezintă noțiunile fundamentale legate de criptografie, clasificările principale și conceptele de bază necesare pentru înțelegerea soluției propuse.

2.1.1 Definiții și clasificare

Include definițiile pentru criptografie simetrică, criptografie asimetrică, funcții hash și alte primitive relevante. Discută diferențele între acestea și cazurile tipice de utilizare.

2.1.2 Standardizare

Enumeră standardele și organismele relevante (NIST, IEEE, RFC, GDPR, standarde militare) și menționează rolul lor în conformarea soluției propuse.

2.2 Elemente fundamentale de inteligență artificială

Descrie conceptele cheie din domeniul inteligenței artificiale care vor fi folosite în lucrare.

2.2.1 Paradigme de învățare

Discută despre învățarea supravegheată, nesupravegheată și prin întărire, raportându-te la scenariul lucrării.

2.2.2 Modele generative și transformere

Introduce arhitecturile Transformer, modelele generative moderne și implicațiile lor în securitatea cibernetică.

2.2.3 GAN și LLM în securitate

Prezintă modul în care GAN și LLM sunt utilizate în detecția și generarea de conținut relevant pentru securitate, incluzând exemple recente.

2.3 Conexiunea AI–Criptografie

Leagă componentele AI și criptografie pentru a fundamenta soluția propusă.

2.3.1 Domenii de aplicare

Analizează scenarii precum cryptoanalysis asistată de AI, generarea de parole, detecția anomaliilor sau automatizarea proceselor de securitate.

2.3.2 Limitări curente

Identifică limitările actuale ale abordărilor combinate AI–criptografie și explică modul în care soluția propusă răspunde acestor provocări.

Capitolul 3:
Stadiul Actual al Soluțiilor

3.1 Analiza soluțiilor existente

Descrie principalele soluții comerciale și open-source care abordează probleme similare, subliniind caracteristicile esențiale.

3.2 Cercetare academică și proiecte conexe

Prezintă studii academice relevante, rezultate publicate și inițiative recente din domeniu.

3.3 Analiză comparativă și limitări

Evaluează critic soluțiile existente, evidențiază lipsurile și construiește argumentul pentru necesitatea abordării propuse în lucrare.

Capitolul 4:
Definirea Problemei și Specificații

4.1 Problema abordată

Precizează limitele sistemelor curente și explică problema concretă pe care o adresează lucrarea.

4.2 Cerințe funcționale

Listează funcționalitățile pe care soluția trebuie să le îndeplinească pentru a răspunde problemei definită anterior.

4.3 Cerințe nefuncționale

Documentează cerințele de performanță, scalabilitate, securitate, disponibilitate și mentenanță.

4.4 Model de atac și scenarii de amenințări

Identifică actorii rău intenționați, capabilitățile lor și scenariile de atac ce trebuie contracarate.

4.5 Obiective aplicate soluției

Reformulează obiectivele generale într-un set de livrabile verificabile pentru soluția implementată.

Capitolul 5:
Soluția Propusă

5.1 Arhitectura generală

Descrie arhitectura macro a sistemului și include o diagramă care evidențiază principalele componente și fluxuri de date.

5.2 Metodologie și justificarea alegerilor

Explică abordarea metodologică, pașii parcurși și motivele pentru alegerea tehnologiilor și a modelelor AI.

5.2.1 Selecția tehnologiilor

Detaliază limbajele, cadrele și infrastructura utilizate și argumentează selecția lor.

5.2.2 Modele AI utilizate

Prezintă modelele AI integrate, modul în care sunt antrenate, configurate și orchestrate.

5.2.3 Principii de securitate

Descrie măsurile de securitate și mecanismele de protecție integrate încă din etapa de proiectare.

5.3 Descrierea componentelor

Analizează fiecare componentă a soluției folosind paragrafe dedicate ce includ rolul, funcționarea, diagrama și justificarea tehnologică.

5.3.1 Modul AI

Detaliază agentul AI, capabilitățile, datele utilizate și modul de interacțiune cu celelalte componente.

5.3.2 Modul criptografic

Descrie serviciile criptografice, protocoalele implementate și modul de integrare cu orchestrarea AI.

5.3.3 Orchestrator și interfețe

Prezintă modul de coordonare între componente, fluxurile de lucru și interfețele expuse (CLI, API, UI).

Capitolul 6: Implementare

6.1 Mediu de dezvoltare

Descrie mediul hardware și software utilizat, precum și instrumentele de dezvoltare.

6.2 Framework-uri, librării și modele

Detaliază componentele software externe și modul în care sunt configurate pentru a susține soluția.

6.3 Containerizare și orchestrare

Prezintă modul în care sunt utilizate containerele, imaginile Docker și soluțiile de orchestrare.

6.4 Măsuri de securitate implementate

Enumeră măsurile de securitate aplicate în faza de implementare (hardening, audit, monitorizare).

6.5 Automatizare și DevOps

Descrie pipeline-urile CI/CD, scripturile de automatizare și infrastructura (IaC) folosită.

Capitolul 7:
Testare și Evaluare

7.1 Metodologia de testare

Descrie strategia generală de testare și criteriile utilizate pentru a valida soluția.

7.1.1 Teste unitare

Prezintă acoperirea testelor unitare, instrumentele folosite și exemple relevante.

7.1.2 Teste de integrare

Detaliază scenariile de integrare și modul în care componentele sunt validate împreună.

7.1.3 Teste de performanță

Specifică metodologiile și instrumentele folosite pentru măsurarea performanței și scalabilității.

7.2 Metrici și criterii de evaluare

Definește indicatorii cantitativi și calitativi utilizați în analizarea rezultatelor testelor.

7.3 Validarea rezultatelor

Analizează rezultatele obținute în raport cu obiectivele propuse și discută implicațiile.

Capitolul 8:
Rezultate și Discuții

8.1 Rezultate experimentale

Prezintă datele și graficele rezultate în urma testării soluției și compară-le cu cerințele inițiale.

8.2 Analiza performanței

Analizează performanța sistemului din perspectiva latenței, preciziei, consumului de resurse și scalabilității.

8.3 Beneficii și limitări

Evaluează beneficiile soluției propuse, dar și limitările identificate pe parcursul implementării și testării.

8.4 Direcții de îmbunătățire

Propune îmbunătățiri viitoare și potențiale extensii ale proiectului.

Capitolul 9:
Concluzii

9.1 Gradul de atingere a obiectivelor

Evaluează modul în care obiectivele stabilite în introducere au fost îndeplinite.

9.2 Contribuții și impact

Enumeră contribuțiile teoretice și practice ale lucrării și discută impactul acestora în mediul militar, academic sau industrial.

9.3 Dezvoltări viitoare

Propune direcții de continuare a proiectului și idei pentru cercetări ulterioare.

Bibliografie

Utilizează mediul LaTeX standard de citare (`\cite`, `\parencite`, `\textcite`) pe parcursul capitolelor. Toate sursele vor fi colectate automat aici cu ajutorul `biblatex`. Se pot defini secțiuni tematice suplimentare folosind opțiuni precum `keyword` sau `type` în fișierul `bibliography.bib`.

Capitolul 10:
Anexe

10.1 Listă de diagrame suplimentare

Include diagrame detaliate (de exemplu, PlantUML, diagrame de secvență sau arhitecturi alternative) care completează prezentarea din capitolele principale.

10.2 Configurații tehnice

Prezintă fișiere de configurare relevante (de exemplu, ‘docker-compose.yml‘, fișiere de mediu, politici de securitate) și explică modul în care acestea sunt utilizate.

10.3 Scripturi și manual de utilizare

Include scripturile auxiliare și un ghid succint de utilizare a aplicației pentru diferitele roluri implicate.