SESIUNEA DE COMUNICĂRI ȘTIINȚIFICE STUDENȚEȘTI
9 MAI 2025
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
UNIVERSITATEA TEHNICĂ "GHEORGHE ASACHI" DIN IAȘI

Creșterea rezilienței și securității datelor stocate în sisteme distribuite împotriva atacurilor ransomware

Domeniu: Criptografie si Blockchain

Program de studii: Tehnologia Informației

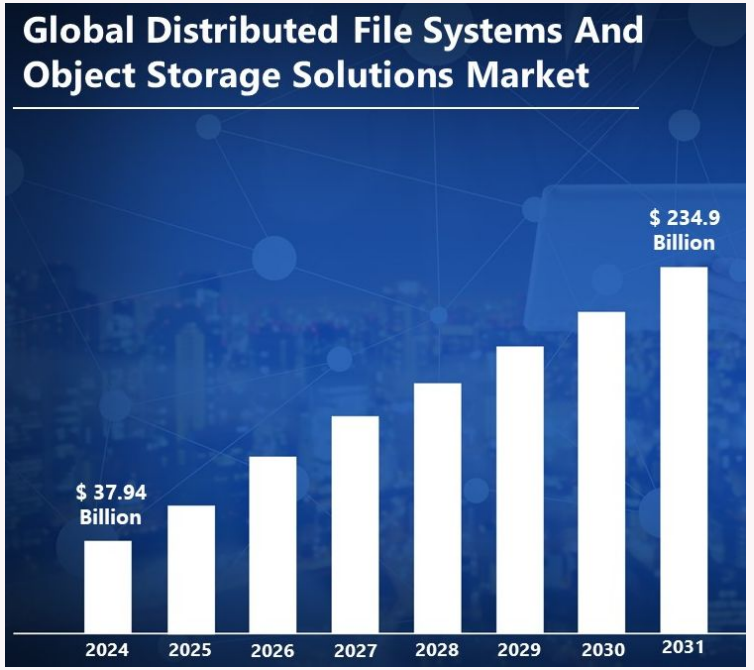
An de studiu: IV licenta

Autor (Voineag Diana-Ioana)

Îndrumător: *Mironeanu Catalin*

Context

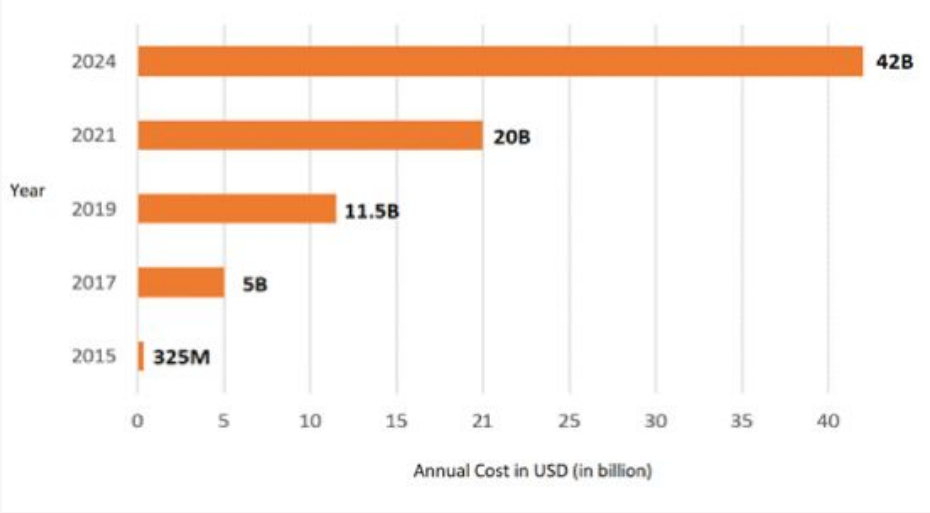
➔ Creșterea utilizării stocării distribuite a datelor



Descrierea problemei

➔ Necesitatea unui sistem de securizare robust și eficient

➔ Atacurile crypto-ransomware



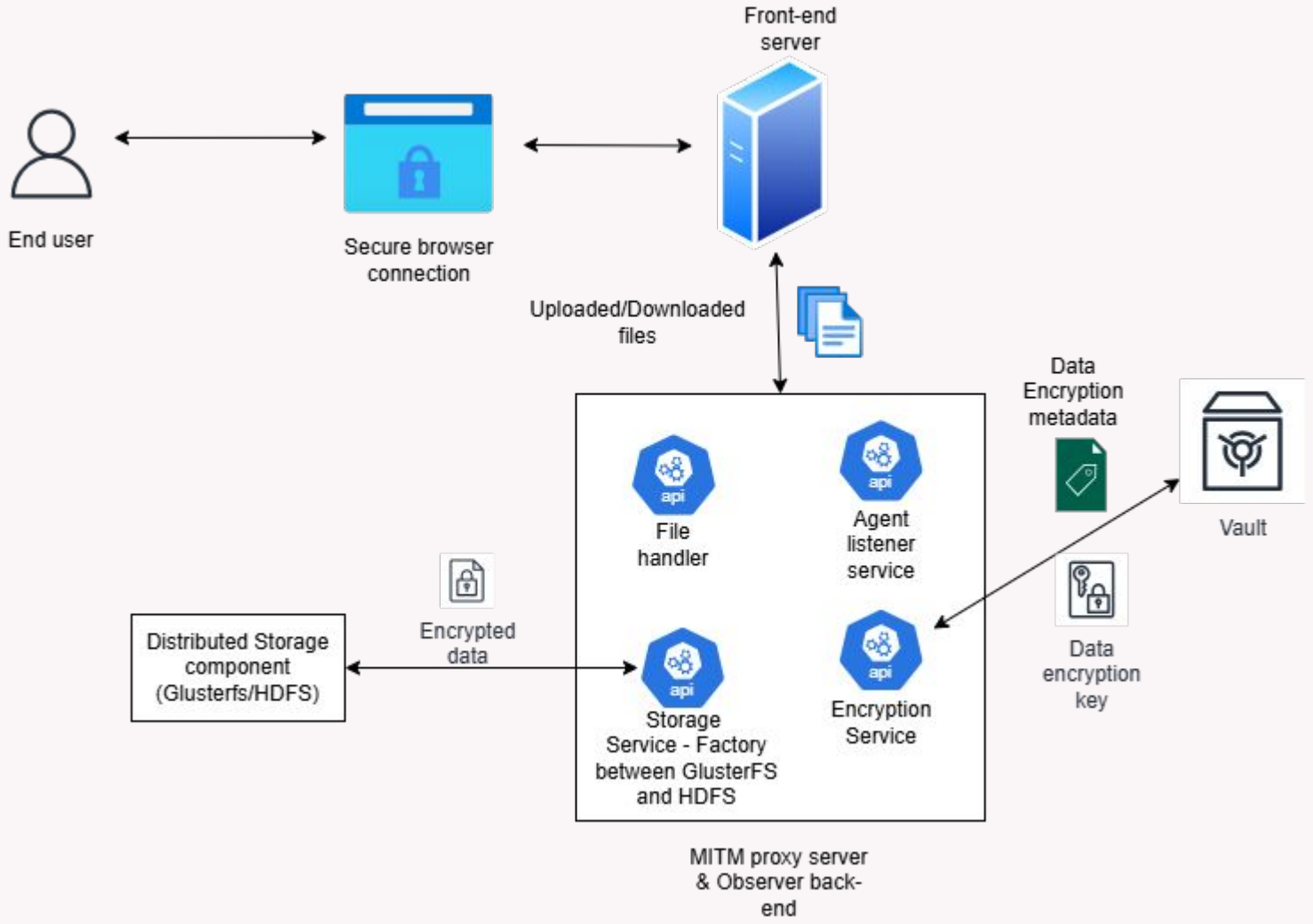
Soluții prezente de stocare distribuită

Feature	GlusterFS	HDFS	Ceph	MooseFS	Proposed System
Transparent Data Encryption (TDE)	✗	✓	✓	✗	✓
File-level Ransomware Detection	✗	✗	✗	✗	✓
Key Rotation Support	✗	✓	✓	✗	✓ (via Vault)
Agent-based Behavioral Monitoring	✗	✗	✗	✗	✓
Vault Integration (KMS)	✗	Partial*	✓	✗	✓
Performance-Aware Encryption	✗	✗	✗	✗	✓

Contribuțiile principale ale lucrării

1. Proxy Man-in-the-middle (MITM) care implementează un strat de criptare prin Transparent Data Encryption (TDE)
2. Implementarea unui model de tip Zero Knowledge folosind HashiCorp Vault
3. Mecanism de detecție timpurie Ransomware prin un model de tip Observer-Agent
4. Experimente de interoperabilitate cu sistemele GlusterFS si HDFS

1. Arhitectura proxy MITM

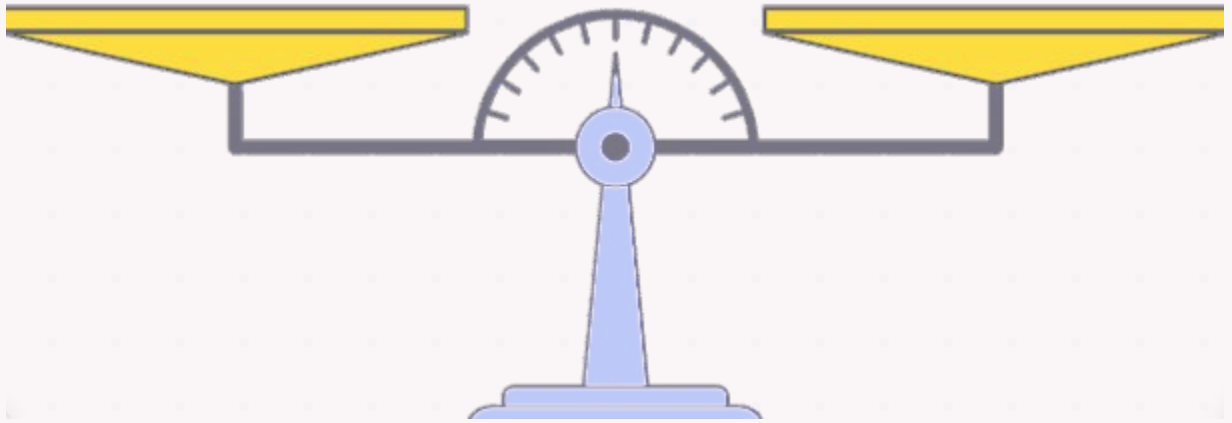


1. TDE cu criptare file-aware

➔ Mecanism de encriptie dinamica:

- are în vedere anumite caracteristici ale fișierului (marime, indicatori - importanta, senzitivitate)
- Chacha20–Poly135 vs AES-GCM
- chunking & streaming

1. File-aware encryption



1. File-aware encryption

$$S(A) = 0.4 \cdot f_{size}(A) + 0.3 \cdot f_{sens}(A) + 0.3 \cdot f_{value}(A)$$

- $f_{size}(A)$ favors AES-GCM for small files and ChaCha20 for large ones:
  - $f_{size}(\text{AES-GCM}) = 0.9$ for files ≤ 5 MB
  - $f_{size}(\text{ChaCha20}) = 0.9$ for files > 5 MB
- $f_{sens}(A)$ = 1.0 for highly sensitive files, 0.5 otherwise
- $f_{value}(A)$ = 1.0 for high-value files, 0.5 otherwise

$$P(A) = \frac{e^{S(A)}}{\sum_{j=1}^{m} e^{S(A_j)}}$$

Contribuțiile principale ale lucrării

1. Proxy Man-in-the-middle (MITM) care implementează un strat de criptare prin Transparent Data Encryption (TDE)
2. Implementarea unui model de tip Zero Knowledge folosind HashiCorp Vault
3. Mecanism de detecție timpurie Ransomware prin un model de tip Observer-Agent
4. Experimente de interoperabilitate cu sistemele GlusterFS si HDFS

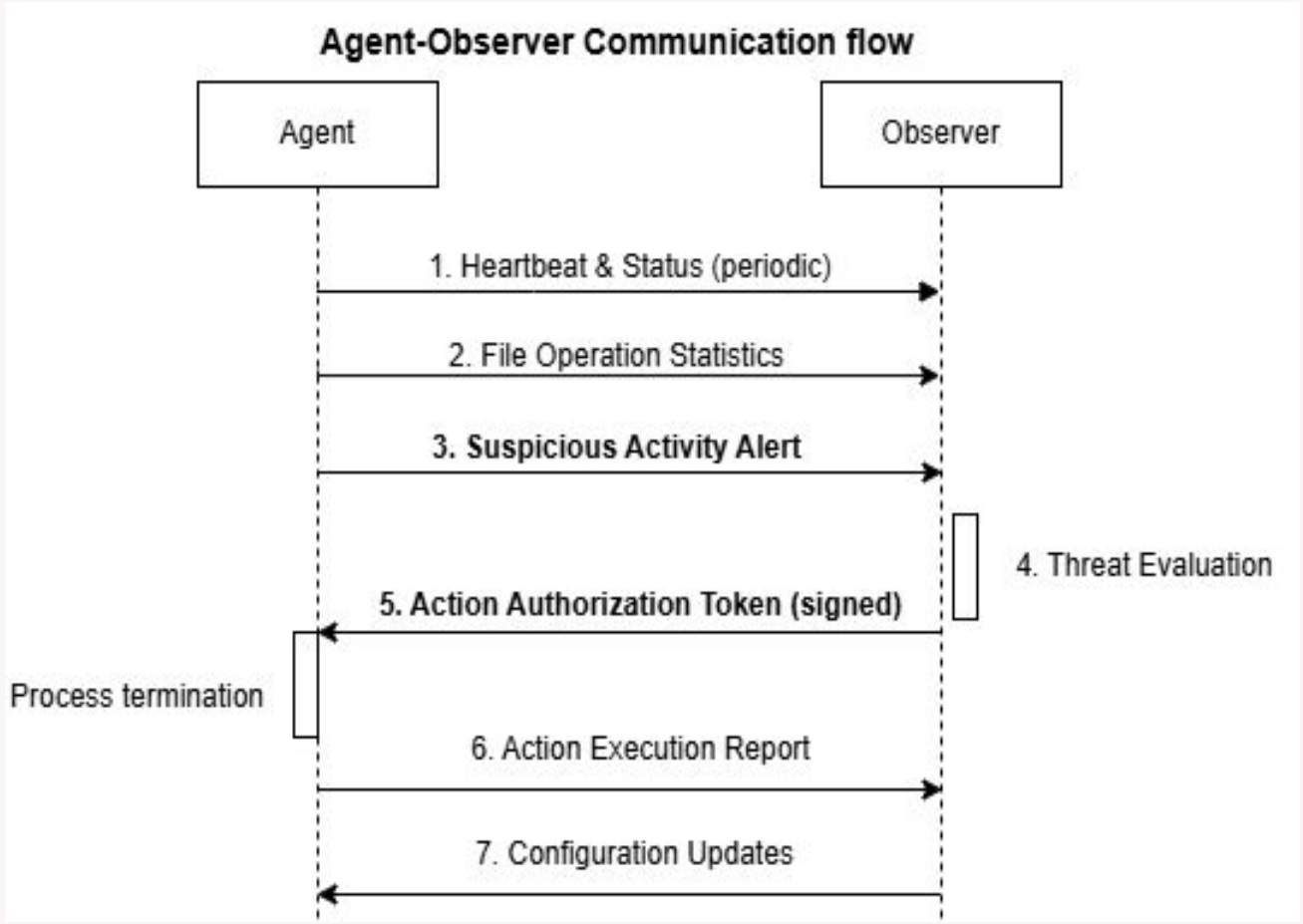
2. Zero knowledge architecture

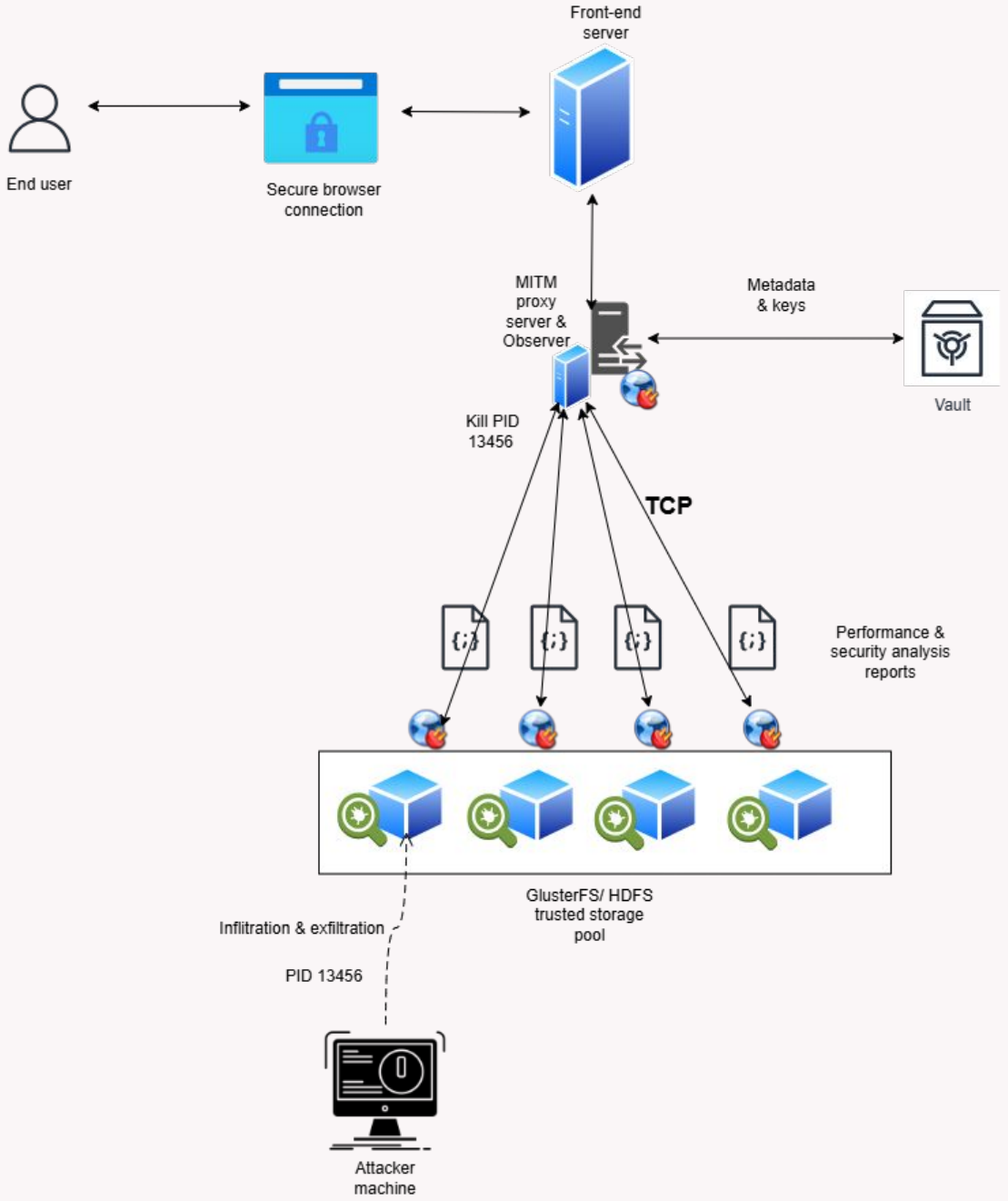
- principii - cu check datorita vault

Contribuțiile principale ale lucrării

1. Proxy Man-in-the-middle (MITM) care implementează un strat de criptare prin Transparent Data Encryption (TDE)
2. Implementarea unui model de tip Zero Knowledge folosind HashiCorp Vault
3. Mecanism de detecție timpurie Ransomware prin un model de tip Observer-Agent
4. Experimente de interoperabilitate cu sistemele GlusterFS si HDFS

3.5 chema detectie





Contribuțiile principale ale lucrării

1. Proxy Man-in-the-middle (MITM) care implementează un strat de criptare prin Transparent Data Encryption (TDE)
2. Implementarea unui model de tip Zero Knowledge folosind HashiCorp Vault
3. Mecanism de detecție timpurie Ransomware prin un model de tip Observer-Agent
4. Experimente de interoperabilitate cu sistemele GlusterFS si HDFS

Concluzii

- Figuri ilustrative
- Tabele

Referințe (dacă este cazul)

- Text
- Text
- Text