Ghulam Ishaq Khan Institute of Engineering Sciences and Technology

Secure Software Development and Engineering – CY-321

By

Ayesha Kashif – 2022132

Mohammad Abdur Rehman – 2022299

Noor ul Ain – 2022485

Submitted to:

Dr. Zubair Ahmad, Assistant Professor, FCSE

Title: AI-Driven Identity Verification & Document Validation

1. **Introduction**

As our system deals with sensitive identity documents and AI-based verification, it is vulnerable to various security risks, such as forgery attempts, unauthorized access, and data breaches. This document presents a structured Threat Modelling & Risk Assessment, identifying potential threats, their risk levels, and mitigation strategies.

2. **Attack Vectors & Potential Threats**

The following attack vectors are identified based on the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) threat modelling approach:

Threat Category	**Possible Attack**	**Risk Level (High/Medium/Low)**	**Mitigation Strategy**
Spoofing	Impersonation using fake identity documents	High	AI-based forgery detection, multi-factor authentication (MFA)
Tampering	Modifying identity documents to bypass verification	High	Cryptographic integrity checks, AI-powered forgery detection
Repudiation	Users denying submission of identity documents	Medium	Audit logs with digital signatures
Information Disclosure	Data breaches exposing sensitive personal data	High	End-to-end encryption, secure API communication (HTTPS, TLS 1.3)
Denial of Service (DoS)	Attackers flooding system with fake document uploads	High	Rate limiting, CAPTCHA verification
Elevation of Privilege	Unauthorized admin access to sensitive data	High	Role-based access control (RBAC), least privilege principle

3. **Security Mitigation Strategies**

To address the identified risks, we will implement the following security measures:

3.1 Secure Authentication & Access Control

- Multi-factor authentication (MFA) for all users.
- Role-Based Access Control (RBAC) to limit privileges.
- Strong password policies and OAuth-based authentication.

3.2 Secure Data Storage & Transmission

- AES-256 encryption for stored identity documents.
- TLS 1.3 for secure API communication.
- Database security measures such as hashing (bcrypt) for user credentials.

3.3 Anti-Tampering & Document Validation

- AI-based deep learning model for document forgery detection.
- Digital signatures to verify document authenticity.
- Watermark verification for official documents.

3.4 Protection Against Denial of Service (DoS) Attacks

- Rate limiting on document uploads.
- CAPTCHA verification to prevent bot-based attacks.
- Cloud-based scalable infrastructure to handle high loads.

3.5 Logging & Monitoring

- Audit logs for all user actions.
- Real-time monitoring for suspicious activities.
- Alerts and notifications for security breaches.

4. **Conclusion**

By implementing these threat mitigation strategies, our AI-driven identity verification system will be secure against common cyber threats while ensuring user data protection, document authenticity, and system resilience.