

Security-Centric Privacy Architecture for Digital Access Control Systems with AI-Assisted Enforcement

Grigol Mikadze
Ivane Javakhishvili Tbilisi State University
grigol.mikadze976@ens.tsu.edu.ge

Abstract — Digital access control systems form a critical security layer for protecting physical and digital assets by regulating identity-based access. As these systems increasingly rely on centralized credential repositories and detailed event logging, they become attractive targets for misuse, data leakage, and insider abuse. Ensuring strong security guarantees is therefore a prerequisite for effective privacy protection.

This paper presents a security-centric architectural model that embeds privacy safeguards directly into the core of digital access control systems. The proposed architecture prioritizes secure credential management, controlled data flows, and resilient logging mechanisms, while employing artificial intelligence as an auxiliary layer to enhance security monitoring and policy enforcement. AI techniques are applied to support anomaly detection, contextual risk assessment, and adaptive enforcement of privacy-aware security policies.

The study outlines key architectural principles, integration paths for privacy-enhancing technologies (PETs), and evaluation metrics that jointly address security robustness, regulatory compliance, and operational efficiency. By positioning AI as a supporting security mechanism rather than a primary decision authority, the proposed framework enables scalable, adaptive, and auditable protection of both access integrity and personal data.

Keywords — Access Control Systems, Secure Architecture, Data Privacy, Artificial Intelligence, Privacy-by-Design, Adaptive Security, Privacy-Enhancing Technologies, Anomaly Detection