Social Sciences & Humanities Conference

INTERNATIONAL ACADEMIC CONFERENCE ON
SOCIAL SCIENCES AND HUMANITIES

27 - 29 March 2026 Singapore , Singapore

Comparative Analysis of Privacy Authentication Methods Concerning IOT And Industry 4.0 Scenarios

Rachel John Robinson , Rohaan Behira

IU University of Applied Sciences, Germany

Abstract

Authentication is a foundational component of cybersecurity, ensuring that only legitimate users, devices, and processes gain access to digital resources. As modern technological ecosystems expand across highly diverse environments—ranging from resource constrained Internet of Things (IoT) devices to complex Industry 4.0 manufacturing systems and traditional office infrastructures—the choice of authentication methods becomes increasingly critical. This paper analyzes the advantages and disadvantages of the three primary authentication factor categories defined by NIST: knowledge factors (passwords and PINs), possession factors (tokens and digital certificates), and inherence factors (biometrics and behavioral traits). The study systematically assesses how each factor performs in terms of security, cost, scalability, resource consumption, and operational feasibility across IoT, Industry 4.0 manufacturing, and office environments. Knowledge factors are lightweight and inexpensive but prone to weak credential management and phishing vulnerabilities. Possession factors offer stronger security, particularly through SIM based IoT provisioning and certificate-driven machine authentication, yet introduce hardware and administrative overhead. Inherence factors provide the strongest non transferable identity assurance but face practical barriers such as high cost, environmental sensitivity, and irreversibility in case of compromise. The paper further evaluates multi factor authentication (MFA) as a layered approach that mitigates the weaknesses of individual factor types. Comparative analysis and cost benefit deploy ability assessments lead to domain specific strategic recommendations: selective MFA adoption in IoT, certificate biometric combinations in Industry 4.0, and phishing resistant MFA (e.g., WebAuthn/FIDO2) in office settings. The study concludes that a context aware, risk based selection of authentication methods is essential for building resilient and scalable security architectures.

Keywords: Authentication Factors; Iot Security; Industry 4.0; Multi Factor Authentication; Biometrics