European Research Studies Journal
Volume XXVIII, Issue 2, 2025

pp. 1127-1143

Identity Management to Reduce the Costs of Cybercrime

Submitted 25/04/25, 1st revision 19/05/25, 2nd revision 13/06/25, accepted 30/06/25

Janusz Jablonski[1]

Abstract:

Purpose: *This article to assess the role of digital identity management in increasing supply chain resilience to cyber incidents and to identify good practices and recommendations by eliminating potential vectors of cybercriminal attacks.*
Design/Methodology/Approach: *The study is based on a literature review and analysis of legal regulations and standards regarding cryptographic security and trust levels in electronic identification. Current secure authentication standards and recommendations for Password-less authentication, as well as recommendations for transitioning to post-quantum cryptography, were considered. The research question was formulated: What impact does decentralized digital identity management and the adaptation of authentication systems to the requirements of the definitional "dynamic authentication" have on risk and cost minimization? In accordance with the research question, a research hypothesis was formulated, which assumes that adapting authentication systems to the requirements of post-quantum cryptography and decentralized digital identity management combined with password-less authentication significantly eliminate the risks and costs of Cybersecurity incidents related to the human factor in authentication. Compliance with the "dynamic authentication" requirements by suppliers, including suppliers, eliminates numerous supply chain risks related to cybecrime.*
Findings: *The results of the analysis indicate that eliminating cybercrime risks requires a change in the approach to digital identity management to a decentralized one and increasing the levels of cryptographic security. It turns out that implementing regulations regarding "dynamic authentication" in relation to OTK can eliminate most of the threats known today and significantly reduce the scale of losses caused by cybercrime.*
Practical implications: *The proposed methodology and study results provide valuable recommendations for organizations seeking to eliminate the risk of cybercrime and ensure compliance with applicable European Union regulations. Implementing IAM/IMS systems that implement "dynamic authentication" reduces operational risk, and regulatory compliance also eliminates the risk of significant fines. The article emphasizes the importance of continued research, particularly into solutions focused on machine and device identity management.*
Originality/value: *Previous research has focused on Quantum Resistance, MFA, Biometrics, or PasswordLess. This paper proposes a methodology that takes a comprehensive approach to identity and access management (IAM/IMS) and incorporates a different approach to mitigating human error. Furthermore, perhaps for the first time, criteria for evaluating digital identity management standards and authentication technologies are proposed.*

[1] *University of Szczecin, Poland, ORCID: 0000-0003-3291-4256,*
e-mail: janusz.jablonski@usz.edu.pl;

Keywords: *Identity Management, risk, cost, cybercrime, supple chain, cybersecurity, security level, regulatory compliance.*

JEL codes: *F52, G32, H56, K2, L38.*

Paper type: *Research article*

Acknowledgement: *This research was co-financed by the Minister of Science under the "Regional Excellence Initiative.*

Regionalna
Inicjatywa
Doskonałości

Ministerstwo Nauki
i Szkolnictwa Wyższego

1. Introduction

Cybercrime isn't longer IT just problem are transform into a global economic crisis, affecting corporations, governments, and individuals alike. The economic risks are not hypothetical: global estimates for 2025 place the annual cost of cybercrime at between $1.2 and $1.5 trillion, including direct losses, lost productivity, downtime and supply-chain disruptions (Miliefsky, 2025).

The European Union Agency for Cybersecurity (ENISA) report inform that in 2024 the costs of cyber incidents in Germany alone amounted to €266 billion (ENISA ETL 2024). In supply chains especially warehouse, logistics attacks can disrupt downstream and upstream operations, increasing the cost of downtime and losses for the entire supplier ecosystem. Furthermore, many companies in these chains don't prioritize security, exacerbating the risk of cascading damage.

The Verizon report highlights that a human element was involved in approximately 60% of breaches meaning user or human error, social engineering manipulation, and abuse are a consistent risk factor (Verizon DBIR, 2025).

The Verizon report indicates that the initial attack vector in 22% of cases began with credential abuse and 16% with phishing. Additionally, 88% of attacks on core web applications, the most common type of attack, involved credential theft. Similar data were given in the FBI 2023 report indicates that approximately 34% of crimes were caused by phishing attacks aimed at obtaining personal, financial and/or login and password information (FBI ICR, 2023).

The Verizon report noted that the human factor is difficult to eliminate, for example, through training, adding that digital identity management systems using traditional authentication methods are already outdated and multi-factor authentication (MFA) has numerous loopholes and weaknesses (Verizon DBIR, 2025).

The European Union Agency for Cybersecurity (ENISA) report inform, that authorisation management human errors and misconfigurations are at the basis of many data breaches. A proper identity and authorisation management is key to reduce possible threat attacks (ENISA, ETL 2024, ss 118). Identity Management Systems (IMS), or more commonly known as Identity and Access Management (IAM), implement identity management processes in the digital world. This system is a key tool that allows businesses and organizations to manage users' digital identities and control their access to digital resources.

Digital identity management primarily encompasses oversight of the identities and credentials that authenticate process participants and users of services and resources in the digital world. IMS/IAM systems consist of tools and technologies that implement this access management, defining who has access to what and what activities they can perform in digital systems. IMS/IAM system functions include creating, modifying, and deleting user accounts, granting and revoking user privileges, authentication, authorization, and monitoring user activity.

A modern approach to Cybersecurity plays a key role not only as a tool for monitoring the risk of a incident but also as a proactive element of the organization's resistance to current and future threats (Ciekanowski, 2024a). Ensuring supply chain security is one of the key challenges facing contemporary business and national economies. Security encompasses various aspects, from information, data, and image protection, through fraud prevention, crisis management, and operational stability (ENISA, ETL, 2024).

2. Methodology

This study applies a qualitative and analytical research approach combining literature review, regulatory analysis, and comparative evaluation. The first stage included a review of scientific publications, ENISA and Verizon reports, and cybersecurity standards such as NIST SP 800-63-3, FIPS 203–205, and ISO/IEC 29115 to identify key IAM/IMS mechanisms.

The second stage analysed legal frameworks including NIS2, eIDAS, and Regulation (EU) 2015/1502 defining *dynamic authentication*.

The final stage developed a comparative scoring model assessing six parameters: Security Level, Regulatory Compliance, Incident History, Decentralized and Passwordless Implementability, and Cost Resource efficiency.

The research aims to determine how adaptation to post-quantum and dynamic authentication standards reduces cybercrime costs. The hypothesis assumes that decentralized and passwordless IAM/IMS significantly improve security and cost efficiency while ensuring compliance with NIS2 and eIDAS.

Such compliance also reduces the risk of personal data exposure regulated by GDPR, thereby eliminating the risk of severe financial penalties for non-compliance. *Identity Management to reduce the costs of Cybercrime.*

3. The Standards and Technology of Identity Management Systems

The growing importance of the internet in global commerce, communications, infrastructure, and supply chains requires secure and effective identity management. Electronic identification services and authentication mechanisms form the foundation of digital security in both the public and private sectors. International regulations and standards set security benchmarks aimed at protecting digital identities, ensuring transaction integrity, and minimizing the risk of attacks such as replay or phishing attacks.

As digital services including e-commerce, online banking, and cloud applications have expanded, Basic Methods of authentication based on a login and shared secrets as passwords have become increasingly inadequate. Their ubiquity, combined with a low resistance to attacks such as phishing, brute-force, and credential stuffing, has generated an urgent need for more secure, scalable, and user-friendly solutions in the domain of identity and access management.

Basic authentication still dominate the digital identification and authentication landscape. However, the need for privacy, scalability, and convenience have exposed the limitations of this method. Modern identity management (IMS) and access management (IAM) systems recommend different security level methods presented in tab.1 using as multi-factor authentication (MFA) firstly propose (Schneier, 1966) and (O'Gorman, 2003). Extended this metods propos: what you do and where you are (Almgren, 2018). All this method is recommended by CNSSI 4009-2015 and NIST SP 800-53 Rev.5.

The Cybersecurity&Infrastructure Security Agency (CISA) recommends using MFA as an effective way to prevent unauthorized access to your data and applications. It points out that even strong, complex, and powerful passwords can be cracked or bypassed by cybercriminals. It points to MFA as an effective way to protect yourself and your organization.

Table 1. *Methods and security level in Mult-Factor Authentications.*

Factor	Methods	Use Case	Security Level	MFA/2FA
what you know	Password, PIN, …	login-password	Low	No
what you have	Smart Cart, mobile OTP	2FA, MFA	Medium	Yes

who you are	Finger/Face recognition	Biometric	High	Yes
what you do	Patterns: Keystroke, …	Behavioral	Medium	A-MFA
where you are	GPS, Wi-Fi, IP-address	Context/location	Medium	A-MFA

Source: *Own study.*

As if in response to the growing requirements in the field of security, scalability and convenience, new solutions are being proposed.

The new standards for identity management systems (IMS) and access management systems (IAM) have evolved toward passwordless and federated systems using MFA and biometrics implemented in to hardware such as chip cart, hardware tokens or smartphones. As the most important of these include PBKDF2, OAuth 2.0, and WebAuthn, each addressing different cybersecurity challenges.

PBKDF2 - The Password-Based Key Derivation Function 2 was introduced in 2000 as part of the PKCS #5 v2.0 specification by RSA Laboratories and later standardized in RFC 2898 and RFC 8018. It was designed to address systemic weaknesses in earlier password storage methods (Kaliski, 2000), which often relied on single-round hashes (e.g., MD5 or SHA-1) without salting. PBKDF2 strengthens derive password-keys by repeatedly applying a pseudorandom function (typically HMAC-SHA-1 or HMAC-SHA-256) combined with a unique *salt* and *pepper* a configurable iteration count, thereby increasing computational cost the ataks and eliminate simple brute-force and dictionary attacks.

PBKDF2 is one of the IAM/IMS standards for authenticating access to digital assets in operating systems and web applications, as well as numerous cryptographic libraries. However, credential repositories are not immune to leaks of hashed data, which are susceptible to off-line exploitation of GPUs or dedicated ASICs to recover credentials such as passwords.

Vulnerability CVE-2017-5638 (Apache Struts / Equifax Breach, 2017) — Although the root cause was a web-application vulnerability, compromised credentials were later exploited offline. The case illustrates how weak password-storage configurations amplify the impact of unrelated software flaws.

Vulnerability CVE-2020-10148 (SolarWinds Orion Authentication Bypass, 2020) shows how supply-chain compromise allowed unauthorized remote code execution and credential exposure. Even when PBKDF2 or other key derivation methods were used internally, failure to secure the authentication perimeter rendered them ineffective.

Numerous media as example blog “huntress.com” or (BreachSense, 2023) outlets and industry portals are reporting on leaks of credentials with hashed passwords, with one of the latest reports concerning the EuroCert 2025 incident (MC, 2025), but without any hard evidence that it involves leaks of data protected by PBKDF2.

OAuth 2.0 — Open Authorization Framework, defined in RFC 6749 (2012) by IETF, is a protocol for delegated authentication that enables applications to access user resources without directly processing user credentials (Hardt, 2012). This standard was developed in response to fundamental weaknesses Basic Authentication models and the risks associated with sharing login data with third-party applications.

4. Identity Management to reduce the costs of Cybercrime

OAuth 2.0 use the concepts of access tokens and refresh tokens within the delegated trust mechanism. These tokens are typically represented as JWT (RFC 7519–JSON Web Tokens) containing so-called *claims* (e.g., issuer, subject, expiration time) be generated using SHA-256 (HS256) with a shared secret or digitally signed using cryptography RSA-2048 (RS256) or ECC-256 (ES256) and may also employ TLS and X.509 certificates to secure token exchanges without being directly dependent on a global PKI hierarchy.

Despite numerous improvements such as PKCE (RFC 7636) and OpenID Connect (OIDC) which mitigate risks related to code interception, token theft, and identity spoofing the RFC 9700 (January 2025) report identifies multiple security weaknesses and provides recommendations for addressing them. Therefore, even after many revisions, OAuth 2.0 does not guarantee full protection of authentication data.

Today, OAuth 2.0 serves as a cornerstone of Identity and Access Management (IAM) and Identity Management Systems (IMS) across cloud environments (Google, Microsoft, Amazon Web Services), supporting federated identities and cross-domain authorization. However, challenges remain regarding token storage, validation, and revocation, which can expose systems to security risks.

- Vulnerability CVE-2020-26878 (Microsoft OAuth 2.0 Implementation Bypass, 2020) — caused by improper validation of redirect URIs — allowed attackers to obtain valid access tokens from legitimate endpoints, demonstrating the risks associated with weak validation of redirect and scope parameters.
- Vulnerability CVE-2021-31992 (OAuth 2.0 Access Token Leakage in Azure AD, 2021) exploited misconfigured application scopes and user consent grants to exfiltrate valid JWT tokens, showing how poor token lifecycle management can compromise IAM systems.

Additionally, numerous security reports (e.g., Cisco Talos, 2023; MITRE ATT&CK T1550.001 “Use of Web Tokens”) document cases of phishing and token replay attacks, where adversaries captured valid JWTs or refresh tokens to impersonate authenticated users.

These incidents reveal a fundamental limitation of bearer-token models: once a token is compromised, access remains valid until expiration — unless mitigated through short-lived One-Time Keys (OTK), continuous revalidation, or other dynamic authentication mechanisms.
Although OAuth 2.0 has significantly improved security and interoperability compared to earlier protocols, numerous unresolved issues highlight the need for adaptive, compromise-resilient identity systems, particularly in zero-trust environments leveraging asymmetric cryptography.

WebAuthn 2.0 (FIDO2) Web Authentication Framework, defined by the World Wide Web Consortium (W3C) and the FIDO Alliance in 2019 (Fido, 2019) (and extended during 2021–2024), offers a user-friendly IAM/IMS platform whose security is based on a cryptographically secured digital signature as proof of user identity. This authentication standard uses public and private keys to eliminate the weaknesses of basic methods based on sharing secrets of other IAM/IMS.

The FIDO2 architecture consists of the WebAuthn API, a W3C browser API that allows web applications to register and authenticate users using cryptographic data, and the Client-to-Authenticator Protocol (CTAP2), developed by the FIDO Alliance for communication between browsers, operating systems and external authenticators such as security keys, TPM modules or smartphones or smartphones held by the user.

During credential registration, the relying party generates a challenge, which is signed by the authenticator using a unique private key stored in a secure enclave. The corresponding public key is then registered with the service, typically associated with a credential ID and an attestation certificate *Public Key Infrastructure* or X.509 to verify device provenance.

The authentication process follows a similar challenge–response pattern. This model introduces partial decentralization of identity management because the user stores the private key on their device instead of in centralized credential repositories, but the public key, which is susceptible to cryptanalysis, is exposed.

The WebAuthn as IAM/IMS standard has been increasingly adopted by major technology providers — Google, Microsoft, and Apple as a secure cross-device and federated identity mechanism.

In practice, vulnerabilities continue to arise not from cryptographic design flaws but from implementation and integration weaknesses, such as:

- CVE-2020-0601 (CurveBall / Windows CryptoAPI, 2020) — allowed forged X.509 certificates and ECDSA signatures, exposing indirect risks to WebAuthn attestation chains;
- CVE-2022-22706 (FIDO2 USB Token Memory Exposure, 2022) — revealed insecure firmware that enabled extraction of credential material, compromising hardware-backed authentication.

Additional reports, including MITRE ATT&CK T1556.007 (*Modify Authentication Process*) and the ENISA Threat Landscape 2024 (supply chain pp 3, pp 12, pp48, pp. 15, phishing credentials pp 23, ZERO DAYS pp26, czynnik ludzki pp 62 This also exceeds the previous record of 223.5 billion euros from 2021. Pp 72, błąd użytkownika 31% I miejsce pp 74), highlight supply-chain and firmware-level threats targeting trusted authenticators rather than the WebAuthn protocol itself.

Despite such incidents, WebAuthn 2.0 remains a highly mature and user-friendly authentication framework, offering phishing resistance through cryptographic proof of user identity instead of reusable secrets. Combined with JWT-based session encapsulation and ephemeral trust via One-Time Keys (OTK), WebAuthn forms the foundation for the next generation of IAM/IMS architectures — designed for dynamic authentication and resilience against post-quantum threats (QuantumResists).

5. Proposed Methodology for Scoring IAM/IMS

The first attempts to introduce an authentication system evaluation methodology that takes into account the need to replace passwords in authentication proposed in 2001 (Ratha *et al.*, 2001).

The first attempt to include the parameters of usability, deployability, and security in the authentication assessment was made in 2012 (Bonneau *et al.,* 2012). However, this attempt focused primarily on technical considerations indicating that omitting passwords in authentication would be unlikely, while completely ignoring legal regulations and shifting the burden of OTK authentication to the relying party

Despite various proposals for IMA/IMS systems, the continuing increase in the number of incidents and the increasing costs of cybercrime prompt consideration of their future development Specifically, which features are crucial for containing or mitigating risks and costs.

For further analysis, evaluation criteria were proposed to combine aspects concerning theoretical analyses of cryptographic security levels, practical characteristics of implementation feasibility, as well as the human factor.

Eliminating cybercrime risks must take into account not only raising user awareness and new IAM/IMS technologies, but must also take into account the risk of penalties imposed for non-compliance with the legal regulations of individual regions and countries (Okari *et al.*, 2025).

Incident analysis shows that threats can be prevented by raising awareness and complying with established regulations. However, management must be aware of cybercrime risks and consciously and thoughtfully implement new methods and technologies (Bartczak *et al.*, 2021),(Ciekanowski *et al.,* 2024b, p. 145).

Eliminating cybercrime risks must take into account not only raising user awareness and new IAM/IMS technologies, but must also take into account the risk of penalties imposed for non-compliance with the legal regulations of individual regions and countries (Okari *et al*., 2025).

By shifting the burden of user authentication and access control, and positioning devices, Google has significantly reduced the number of incidents related to internal threats, demonstrating the true effectiveness of adaptive IAM methods in eliminating vulnerabilities and cybercrime risks (Yeoh *et al.,* 2023).

The European Union has strict regulations on personal data protection and cybersecurity, such as GDPR or NIS2, which provide for high fines of up to 10 million euros or up to 4% of revenues for non-compliance.

Regulatory Complance in the European Union's NIS2 – Directive of the European Parliament and of the Council (EU)2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union in the field of IAM/IMS is based on Regulation (EU)2014/910 eIDAS, requiring that essential and important services meet a medium or higher security level in accordance with the definition of Regulation (EU)2015/1502 define: *"dynamic authentication" means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity.*

Dynamic authentication in cryptography means that each transaction is authenticated with a new key controlled by the user One-Time Keys (OTK) or One-Time-Password (OTP), which are managed by the user. Therefore, each user controls their own identity in a decentralized architecture that is less susceptible to mass leaks of authentication data.

The cryptographic key is linked to the user's identity, so there is no need to use passwords — that is, it assumes a PasswordLess approach. In such an IAM/IMS, security is partially dependent on the cryptographic security level and the security of the OTK exchange protocol.

Regions outside the European Union follow regulations in accordance with ISO/IEC 29115, FIPS 201, and currently being introduced are FIPS 203, FIPS204, FIPS205 standards, which do not impose the obligation to use OTP/OTK.

Currently deployed IAM/IMS solutions aiming to enhance security may optionally employ Time-based One-Time Passwords (TOTP, RFC 6238) or HMAC-based One-Time Passwords (HOTP, RFC 4226). However, these mechanisms do not constitute true cryptographic authentication factors, as their entropy and validity are centrally managed and only partially under the user's control.

Similarly, SMS-based verification codes, often generated by pseudo-random number generators (PRNG) and used as a second factor in MFA schemes, typically consist of short numeric sequences (e.g., 6–8 digits). Such codes are not user-controlled, lack cryptographic binding to the authentication session, and therefore cannot ensure integrity or resistance to interception.

According to NIST SP 800-63-3, these TOTP/HOTP methods are classified as possession-based factors rather than cryptographic authenticators. While they may contribute to achieving Assurance Level AAL2, they do not provide the cryptographic proof-of-possession required for AAL3. Consequently, their security is constrained by transmission vulnerabilities (e.g., SIM swap, SMS hijacking) and by the absence of user-managed key material, which limits their suitability for high-assurance or decentralized identity systems.

Therefore, it is difficult to consider them secure solutions. Table 1 summarizes the obligations and properties for IAM/IMS resulting from applicable standards and regulations. It should be noted that both NIST (SP 800-63-3) and ENISA (NIS2, eIDAS) recommend using at least two-factor authentication (2FA).

Security Level or Internet security, as well as IAM/IMS, largely relies on cryptography, it is worth recalling that the highest is **Perfect Secrecy**, offered by One-Time Key cryptography, which was proven by C. Shannon in 1949 (Shannon, 1949). However, for the purpose of ensuring Quantum Resistance, cryptography offering

Semantic Security has been proposed, which is relevant in the context of NIST regulations for standards FIPS203, FIPS204, FIPS205. Semantic security is determined based on the IND-CCA2 security game outlined (NIST IR.8545), according to the theory of modern cryptography proposed (Rackoff, 1991; Bellare, 2005).

Computational security can be assumed to be the next lower level of cryptographic security, which describes the amount of work needed to break the cryptosystem and is expressed as an exponent of 2. The security level is assumed to be equivalent to the key size k for AES encryption, if k = 128 then the adversary's workload needed to break the cryptosystem is 2^k basic operations, assuming that once the key is known, one decryption operation is performed.

Table. 1 *Properties IAM/IMS resulting from regulations.*

Regulation	OTK	MFA	Biometry	Security level	Comments
ISO/IEC 29115	Option	Option	Option	Computational	MFA,X.509
NIST FIPS201	Option	Option	Option	Computational	PKI, PRNG
NIST FIPS203	Option	Option	Must	Semantic	IND-CCA2
ENISA/NIS2	Must	Must	Must	Semantic	IND-CCA2
(UE)1502/2015	Must	Must	Must	Perfect secrecy	OTK

Source: *Own study.*

PasswordLess authentication implementability. The root cause of numerous incidents is weak and reused passwords, as well as the exploitation of credentials in various forms of phishing. The human factor is often identified as the weakest link in cybersecurity, and mitigating risks through training is ineffective.

A natural path to improving IAM/IMS security seems to be adopting NIS and ENISA recommendations and implementing **PasswordLess** authentication. Eliminating passwords from the secure authentication process is desirable to improve security without sacrificing simplicity and user convenience, but it's not always possible.

Decentralized Identity describe of digital identity management represents a significant security enhancement in modern IAM/IMS architectures. By shifting credential and token storage from centralized or federated repositories to user-controlled devices. This systems inherently reduce the volume of exposed data and mitigate large-scale breach risks.

In contrast, Federated Identity Management (FIM) introduces central points of failure, where a single compromise can expose millions of records and enable privilege escalation across multiple domains. Moreover, PKI-based models dependent on global certificate authorities (e.g., X.509) remain vulnerable to certificate misuse and systemic trust failures.

Decentralized model align with privacy-by-design and zero-trust principles, ensuring that private keys and identifiers remain under user control and are never shared with third parties. This model effectively contains the impact of attacks, as a single compromised identity affects only its holder rather than an entire federation. While FIM combined with multi-factor authentication (MFA) meets higher assurance levels such as NIST SP 800-63-3, it still relies on shared secrets that are vulnerable to phishing, replay, and credential-stuffing attacks.

Consequently, fully decentralized systems as promoted by the W3C and ENISA guidelines on Self-Sovereign Identity, offer a security-justified evolution of IAM/IMS consistent with the forthcoming eIDAS 2.0 and the European Digital Identity Wallet model.

Incident History coefficient is an empirical resilience metric ranging, designed to reflect the real-world exposure and historical security performance of an authentication mechanism or standard.

The rating is derived from the number, severity, and impact of disclosed vulnerabilities as well as the volume of compromised credentials and data that have enabled subsequent attack escalation, including supply-chain breaches.

High score denotes mechanisms with no significant public vulnerabilities reported in CVE/NVD databases, minimal exposure of user data or credentials, and no verified large-scale compromises. I-H low score corresponds to mechanisms with numerous CVSS-classified vulnerabilities, multiple documented breaches, and broad data disclosures enabling attack propagation across dependent services exemplified by incidents such as the EuroCart data breach in Poland (MC, 2025), which demonstrated how credential leaks can escalate through interconnected systems.

This metric aggregates verified data from MITRE CVE, NVD, and CVSS, supplemented by incident reports (Verizon DBIR, CERT-EU, EuroCERT) and peer-reviewed publications.

Unlike theoretical cryptographic analysis, I-H reflects empirical evidence and operational risk, providing a practical indicator of how authentication mechanisms perform under real attack conditions within the 2020–2025 observation window.

Cost Resource metric represents the relative computational, infrastructural, and operational expenses required to implement and maintain a given authentication mechanism. It reflects not only processing and storage overheads but also administrative effort, energy consumption, and cost of cryptographic operations.

From a cyber-risk management perspective, this parameter score indicates the feasibility and economic efficiency of deploying secure mechanisms that mitigate cybercrime-related losses. A high score corresponds to low resource requirements and high efficiency, typical of lightweight and decentralized mechanisms, such as Dynamic Authentication with OTK/OTP.

In this case, the keys are generated locally on the user side, reducing dependence on centralized infrastructure and eliminating the need for complex key-lifecycle generation or validation in too RSA, ECC and Lattice Cryptography for FIPS203 based at NIST IR.8545.

Consequently, this approach offers a level of computational efficiency comparable to Basic Authentication while maintaining a significantly higher level of cryptographic assurance. Conversely, a low score indicates high operational costs and lower cost-effectiveness. Such mechanisms often require frequent synchronization, centralized certificate management, or high-entropy key generation and validation (as in PBKDF2, OAuth2.0, or WebAuthn).

These higher costs translate into reduced scalability and slower adoption across large infrastructures, indirectly increasing exposure to cyber threats due to inconsistent or delayed updates.

This parameter directly correlates with the system's ability to economically sustain risk mitigation against cybercrime - low-cost, decentralized, and dynamically generated key mechanisms achieve the best balance between security assurance and financial efficiency.

6. Quantitative Cost Model and Expected Savings

Evaluation Framework in order to assess the security, regulatory, and operational efficiency of modern Identity and Access Management (IAM) and Identity Management Systems (IMS), six key parameters were defined for comparative evaluation. These six parameters were scored from 1 to 5, where base at description IAM/IMS the 5 represents optimal performance (high security, low risk, minimal cost) and 1 represents poor resilience or high exposure and possibility:

Parameter	Description
C-R (Cost Resource)	Computational and operational cost of implementation, maintenance, and key management FIA.
S-L (Security Level)	Strength of cryptographic and protocol-level resilience against modern attacks.
R-C (Regulatory Compliance)	Conformity with major cybersecurity and data protection frameworks (e.g., NIS2, eIDAS,FIPS203).
I-H (Incident History)	Empirical record of known vulnerabilities, exploits (MITRE CVE, CERT-EU, and peer-reviewed data).
D-I (Decentralized Implementability)	Ability to operate in decentralized or user-managed key and credentials architectures.
P-L (PasswordLess Implementability)	Ease of integration with passwordless or biometric schemes.

These six parameters were scored from 1 to 5, where base at description IAM/IMS the 5 represents optimal performance (high security, low risk, minimal cost) and 1 represents poor resilience or high exposure and possibility. The total maximum score per method is 30. The scores assessing individual attributes for individual methods are presented in Table 2.

Table 2. *Attribute evaluation scores for individual methods*

Standard	P-L	S-L	I-H	D-I	C-R	R-C	Total	Saving vs basic
Basic Method	0	0	1	1	5	0	7	0%
PBKDF2	1	2	2	2	2	3	12	40%
OAuth2.0	2	3	3	3	3	3	17	57%
WebAuth2.0	3	4	3	3	2	3	18	60%
Dynamic-Auth	5	5	5	5	4	5	29	97%

Source: *Own study.*

The scoring framework and radar chart on fig. 1 illustrates progressive improvement from traditional, static methods (Basic Method, PBKDF2) to Dynamic Authentication, which achieves the highest balance between cost efficiency and resilience.

Quantitative Cost Model and Expected Savings - based on reports from Cybersecurity Ventures (Ventures, 2025) and Verizon DBIR (Verizon, 2025), the global cost of cybercrime in 2025 is estimated at **USD 10.5 trillion**, with approximately **30%** attributed to *phishing, credential theft, and authentication-related breaches*.

Let:

$\boldsymbol{T} = 10{,}5 * 10^{12}$ USD – total cybercrime cost,
$\boldsymbol{p} = 0{,}3$ – proportion related to phishing and credentials,
$\boldsymbol{P} = \boldsymbol{T} * \boldsymbol{p}$ – potenitial recoverable losses/eliminate cost,

Assuming the economic efficiency of each IAM/IMS method is linearly proportional to its normalized score (s_m/30), the savings potential is defined as:

$$Saving\ s_m = \begin{cases} 0, & for\ Basic\ Authentication \\ \frac{s_m}{30} \times P, & for\ other\ metodhs \end{cases}$$

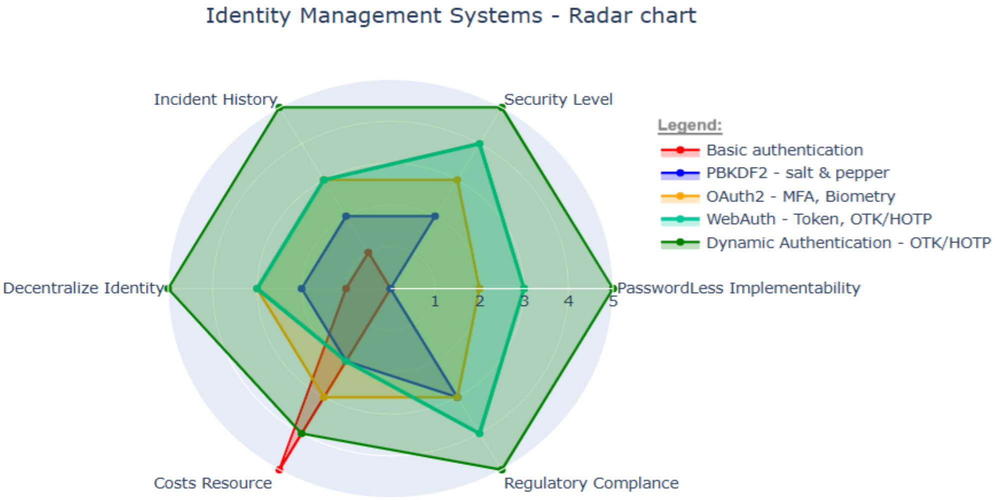
and estimated reduction cost presented in Table 3.

Table 3. *Estimated Cybercrime Cost Reduction by IAM/IMS*

Standard	Score	Saving vs basic	Estimated Saving USD (bn/year)
Basic Method	7	0%	0,00
PBKDF2	12	40%	1,26
OAuth2.0	17	57%	1,79
WebAuth2.0	18	60%	1,89
Dynamic-Auth	29	97%	3,05

Source: *Own study.*

Figure 1. *Radar diagram of parameter coverage by IAM/IMS standards.*



Source: *Own study.*

7. Conclusion

IAM/IMS systems are confirmed to play a key role in mitigating the financial and operational impact of cybercrime. Comparative studies show that dynamic authentication, decentralizing identity and implementing OTK, ensures security, regulatory compliance, and resistance to known vulnerabilities, including phishing and replay attacks.

Adapting IAM/IMS systems to NIS2, eIDAS, and GDPR requirements increases operational resilience, reduces the risk of personal data breaches and financial penalties, and narrows the area of attack escalation on supply chains. The research and findings underscore the growing importance of decentralized and quantum-resistant security architectures in next-generation digital ecosystems.

Research is limited by its reliance on secondary data sources and aggregated cybersecurity incident records (CVE, NVD, CERT-EU), which omit undisclosed or classified incidents, which can compromise the comprehensiveness of the comparative assessment.

The assessment model primarily reflects IT-centric environments, while the rapidly growing operational technology (OT) space, with a device-to-user ratio exceeding 80:1, remains underrepresented in the analysis.

The research and model could be expanded to include OT assessments requiring device identification and real-time access control. Expanded analysis, encompassing a holistic understanding of cybersecurity economics, could contribute to the unification of IT-OT security models.

Further research on dynamic, decentralized, and post-quantum IAM solutions could provide standardization knowledge and strategic management focused on implementing cyber resilience in sectors critical to national and economic security.

References:

Bartczak, K. 2021. Cybersecurity as the Main Challenge to the Effective Use of Digital Technology Platforms in E-Commerce. European Research Studies Journal, Volume XXIV, Issue 2B, 240-256. DOI:10.35808/ersj/2230.

Bellare, M., Rogaway, P. 2005. Introduction to Modern Cryptography, https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf

Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: 2012 IEEE Symposium on Security and Privacy, pp. 553-567. IEEE. https://doi.org/10.1109/SP.2012.44.

BreachSense, 2023. Examples of data breaches using PBKDF2 hashes. https://www.breachsense.com/blog/data-breach-examples/.

Ciekanowski, M., Żurawski, M., Pauliuchuk, Y., Ciekanowski, Z., Marciniak, S. 2024a. Strategies for Effective Cybersecurity Management in Organizations. European Research Studies Journal, Volume XXVII, Issue 1. DOI: 10.35808/ersj/3364.

Ciekanowski, Z., Elak, L., Chrzaszcz, A., Załoga, W., Marciniak, S. 2024b. Digitalisation as an Essential Area of Security and Management in Modern Organisations. European Research Studies Journal, Volume XXVII, Issue 2, pp. 827-837. DOI:10.35808/ersj/3820.

ENISA (European Union Agency for Cybersecurity). 2024. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, September.

FIDO Alliance. 2019. FIDO2: Moving the World Beyond Passwords. https://fidoalliance.org/fido2/.

Miliefsky G. 2025. The True Cost of Cybercrime: Why Global Damages Could Reach $1.2 – $1.5 Trillion by End of Year 2025. https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/.

Hardt, D. 2012. The OAuth 2.0 Authorization Framework, (IETF). https://datatracker.ietf.org/doc/html/rfc6749.

Internet Crime Report. 2023. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.

Kaliski, B. 2000. Password-Based Cryptography Specification, RSA Laboratories. https://datatracker.ietf.org/doc/html/rfc2898.

Ministry of Digital Affairs, Republic of Poland 2025. Announcement of the Government Plenipotentiary for Cybersecurity regarding data leakage as a result of a cyberattack against EUROCERT Sp. z o.o. https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-ws-wycieku-danych-w-wyniku-cyberataku-wobec-firmy-eurocert-sp-z-oo.

NIST. 2024. IR 8545 – A Cybersecurity Posture for Transitioning to Post-Quantum Cryptography.

O'Gorman, L. 2003. Comparing passwords, tokens, and biometrics for user authentication. IEEE Proceedings. DOI: 10.1109/JPROC.2003.819611.

Okari Orucho, D., Katila C., Mandela N.A. 2025. Descriptive Analysis of Security Threats and Attacks in Public Cloud Computing: Safeguarding Data from Cyber Attacks. International Journal of Computer Science and Information Security (IJCSIS), Vol. 23, No. 4, July-August. https://zenodo.org/records/16925069.

Ratha, N.K., Connell, J.H., Bolle, R.M. 2001. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal. DOI: 10.1147/sj.403.0614.

Schneier, B. 1996, Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). Wiley. DOI: 10.1002/9781119183471.

Shannon, C. E. 1949. Communication Theory of Secrecy Systems, Bell System Technical Journal, 28(4), 656-715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

Verizon Data Breach Investigations Report - 2025 (DBIR, 2025). https://www.verizon.com/business/resources/reports/dbir/.

Yeoh, W., Liu, M., Shore, M., Jiang, F. 2023, Zero trust cybersecurity: Critical success factors and A maturity assessment framework. Computers and Security, 133, Article 103412. https://doi.org/10.1016/j.cose.2023.103412.