

Zero trust architecture for cyber resilience: Mathematical modelling and human factor minimisation

Roman Topala^{1,†}, Bronislav Chramcov^{2,†} and Viktor Gnatyuk^{3,*,†}

¹RMRF, Verkhovynna Str., 37, Kyiv, 03115, Ukraine

³Tomas Bata University in Zlin, T. G. Masaryk Sq., 5555, Zlin, 76001, Czech Republic

³State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zaliznyak Str., 3, Kyiv, 03142, Ukraine

Abstract

Critical shortcomings of perimeter-based cybersecurity models have been revealed by the increasing complexity of corporate IT infrastructures and the emergence of AI-assisted insider attacks. Formal procedures for quantifying the risk contribution of unauthorised AI tool usage – a vector identified in 62% of breaches in the Verizon DBIR 2026 – are absent from current Zero Trust Architecture (ZTA) frameworks. This paper proposes a modified Integrated Cyber Risk Management equation (ICRM*) that extends the original model by introducing two new parameters: the Shadow AI Index (SAI), which formally quantifies the risk of unauthorised AI tool usage, and the Compliance Factor (CF), which weights resilience according to an organisation's ZTA maturity level per CISA ZTMM 2.0. An independent experiment on the CERT Insider Threat Dataset r4.2 (1,000 users, 70 insiders) demonstrates that AdaBoost achieves AUC = 0.988 in insider threat classification, while ICRM* produces a $2.11 \times$ higher risk differential between insider and normal users compared to the original ICRM baseline. The findings confirm that combining behavioural analytics, algebraic trust modelling, and AI-usage telemetry creates a quantifiably more resilient Zero Trust environment.

Keywords

zero trust architecture, human factor, cyber resilience, trust score, machine learning, behavioural analytics, UEBA, NIST SP 800-207, CISA ZTMM, insider threats

1. Introduction

In the context of exponential growth in corporate information infrastructure complexity, rapid migration to cloud environments, and the dissolution of traditional network perimeters, the classical cybersecurity paradigm has demonstrated its fundamental inability to withstand modern attack vectors [1, 2]. The adoption of hybrid work formats, Bring Your Own Device (BYOD) policies, and distributed microservice architectures have completely dismantled the security illusion of the implicit-trust perimeter model.

In response to these challenges, Zero Trust Architecture (ZTA) was formulated—a strategic concept grounded in the maxim “Never Trust, Always Verify.” This approach eliminates implicit trust, requiring continuous cryptographic authentication and algorithmic authorisation of every user, device, and process before granting access to resources, regardless of network origin.

Despite significant technological progress, the human factor remains the key vulnerability of any information system [3, 4]. Automation can minimise the attack surface, yet it cannot fully neutralise risks arising from cognitive biases, user fatigue, insufficient cyber hygiene, successful social engineering campaigns, or deliberate insider actions [2]. This article offers a comprehensive analysis of ZTA architectural patterns with a focus on neutralising human-factor threats, presenting a mathematical apparatus including Trust Score formulae, probabilistic transaction risk models, and a modified cognitive risk management framework.

CMiGIN'26: Fifth International Workshop on Conflict Management in Global Information Networks, June 26–27, 2026, Krakow, Poland

*Corresponding author.

† These authors contributed equally.

✉ roman.topala@rmrf.tech (R. Topala); vicedean-research@fai.utb.cz (B. Chramcov); gnatyukvo@gmail.com (V. Gnatyuk)

id 0009-0008-3321-2276 (R. Topala); 000-0002-3252-1578 (B. Chramcov); 0000-0002-4916-7149 (V. Gnatyuk)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

1.1. Research novelty

Three distinct contributions to the field of Zero Trust security modelling are presented in this study. First, we propose a modified Integrated Cyber Risk Management equation (ICRM*) that extends the original framework by Eze [5] through the introduction of two new parameters: the Shadow AI Index (SAI), which formally quantifies the risk contribution of unauthorised AI tool usage in corporate environments, and the Compliance Factor (CF), which weights resilience according to an organisation's ZTA maturity level per CISA ZTMM 2.0. Second, we conduct an independent empirical evaluation on the CERT Insider Threat Dataset r4.2, comparing three machine learning classifiers under controlled and reproducible experimental conditions. Third, we demonstrate that ICRM* produces a statistically meaningful separation between insider and normal user risk profiles, yielding a $2.11\times$ higher risk differential compared to the original ICRM formulation.

2. Empirical analysis of the cyber threat landscape

Empirical data from global research convincingly demonstrates that technological vulnerabilities represent only part of the problem, while cognitive and operational deficiencies of personnel form the primary vector of compromise [6, 7]. Analysis of the Verizon Data Breach Investigations Report (DBIR) 2026 – encompassing over 31,000 security incidents and 22,000 confirmed data breaches – demonstrates that the “human element” was present in 62% of all confirmed cyber incidents [8, 9].

2.1. Evolution of social engineering and the cognitive load problem

Social engineering caused 16% of all successful breaches, with attack vectors shifting from email to mobile devices [8]. The median mobile phishing success rate proved 40% higher than that of traditional email phishing. Mobile devices generate higher cognitive load due to smaller screens, limited contextual information, and constant distraction, reducing the brain's capacity for critical analysis [10, 11]. Formal mental models for human-centred cybersecurity underscore the need for cognitive ergonomics in security interface design [12, 13].

2.2. Impact of Generative AI and the shadow AI phenomenon

AI tools compress the time between vulnerability disclosure and exploitation, reducing the defenders' response window from months to hours. Data shows that 67% of users access AI services from corporate devices using personal, uncontrolled accounts, and the share of employees regularly using AI rose from 15% to 45% [8, 14]. Employees upload confidential corporate data, source code, or financial reports to public ML models, thereby consciously or unconsciously violating privacy policies – a classic example of security policy conflicting with business needs.

2.3. Specifics of the human factor in critical sectors

In healthcare, the human element was involved in an unprecedented 54% of incidents [15, 16]. In manufacturing and critical infrastructure, exploitation of software vulnerabilities overtook stolen credentials as the primary vector, reaching 31% of all incidents [17, 18]. Research confirms that over 40% of all compromises are caused by employees or contractors through negligence or error [19, 4].

3. Architectural models and standardisation of zero trust

The most influential standardised frameworks are published by the US National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) [20, 21, 22].

3.1. Principles and directives of NIST SP 800-207

Special Publication NIST SP 800-207 defines ZTA key building blocks [20]. Two tenets directly relate to minimising human-factor influence:

- **Sessional Access (Tenet 3):** Access to individual enterprise resources is granted at the level of an individual session with least-privilege rights.
- **Dynamic Policy (Tenet 4):** Access is determined by a dynamic policy that continuously incorporates behavioural and environmental attributes including device posture, privilege level, and behavioural history.

The transition to Just-In-Time (JIT) access and continuous monitoring significantly narrows the opportunity window for attacks caused by stolen passwords [23, 24].

3.2. CISA ZTMM version 2.0 and cross-cutting capabilities

CISA released the Zero Trust Maturity Model (ZTMM 2.0), offering a phased transition plan through four stages: Traditional, Initial, Advanced, and Optimal [25, 26, 27]. The model decomposes into five foundational pillars: Identity, Devices, Networks, Applications and Workloads, and Data. Three cross-cutting capabilities complement these pillars: Visibility & Analytics, Automation & Orchestration, and Governance [25].

4. Mathematical modelling in zero trust architecture

ZTA demands continuous, stochastic, and deterministic algorithms capable of processing heterogeneous attribute arrays in real time [28]. The user identification process is described by:

$$U = f(DA, AP, NP, SP) \quad (1)$$

where DA (Device Attributes) = $g(T, OS)$, AP (Application Dependencies) = $h(DA)$, NP (Network Policies) = $k(AP)$, and SP (Security Posture) = $m(T, OS)$. The network is visualised as a directed graph $G = (V, E)$, where V represents microsegments and E represents permitted communication routes [28]. Mathematical approaches to calculating network accessibility in management systems provide a complementary foundation for ZTA network segmentation design [29].

5. Dynamic trust assessment: calculations and formulae

The core of ZTA is the continuous calculation of the Trust Score (TS) throughout the session lifecycle [30].

5.1. Trust score calculation equation

The Trust Score is computed as the weighted sum of normalised factors [5]:

$$TS = \sum_i (w_i \times f_i) \quad (2)$$

where $TS \in [0, 1]$, w_i is the weight of the i -th factor ($\sum w_i = 1$), and f_i is the normalised value of the trust factor. Four primary vectors are identified: user behaviour (B), network environment (N), device state (D), and threat history (T) [31].

5.2. Extended algebraic transaction risk assessment model

Risk assessment is performed through inverse proportionality to trust: $RA = TS^{-1}$. The extended transaction risk model is [5]:

$$R = f(H_i, C_i, T_i, A_i, P_i) \quad (3)$$

where H_i is transaction history, C_i is context (geolocation, IP), T_i is temporal characteristics, A_i is volume anomaly, and P_i is policy compliance. To transform this into a probabilistic metric $[0, 1]$, a sigmoid function is applied [5]:

$$P(\text{risk}) = \frac{1}{1 + e^{-R}} \quad (4)$$

5.3. Simulation: step-by-step risk calculation

For a corporate employee attempting to copy confidential data at 03:00 from an atypical IP address, UEBA system scores (0–10, where 10 = maximum risk) are: $H_i = 2$, $C_i = 8$, $T_i = 9$, $A_i = 10$, $P_i = 3$. With SOC-configured weights $w_1=0.10$, $w_2=0.20$, $w_3=0.25$, $w_4=0.35$, $w_5=0.10$:

$$R = 0.10 \cdot 2 + 0.20 \cdot 8 + 0.25 \cdot 9 + 0.35 \cdot 10 + 0.10 \cdot 3 = 7.85 \quad (5)$$

The risk score of 7.85/10 triggers immediate device isolation and incident notification, completely neutralising the human factor.

6. Cognitive zero-trust resilience framework and ICRM

The Cognitive Zero-Trust Resilience Framework (CZTRF) integrates cognitive computing and AI technologies to create a self-evolving system [5, 32, 33]. Its Cognitive Engine continuously recalculates the global Integrated Cyber Risk Management (ICRM) equation [5, 34, 35]:

$$\text{ICRM} = \frac{\text{Threat} \times \text{Vulnerability}}{\text{Resilience}} \quad (6)$$

Each component is dynamically scaled in $[0.25, 1.0]$. Based on this foundation, the present paper proposes the following modification:

$$\text{ICRM}^* = \frac{\text{Threat} \times \text{Vulnerability} \times (1 + \alpha \cdot \text{SAI})}{\text{Resilience} \times \text{CF}} \quad (7)$$

where SAI (Shadow AI Index, $\in [0, 1]$) formally quantifies the risk contribution of unauthorised AI tool usage; $\alpha = 0.20$ is the SAI weighting coefficient derived from the 20% elevated risk attributed to Shadow AI behaviour in Verizon DBIR 2026 [8]; and CF (Compliance Factor, $\in [0.25, 1.0]$) weights resilience according to the organisation's CISA ZTMM 2.0 maturity level. When $\text{SAI} = 0$, Eq. (7) reduces to Eq. (6), ensuring backward compatibility.

7. Experimental evaluation on CERT insider threat dataset r4.2

7.1. Experimental setup

An independent experiment was conducted using the CERT Insider Threat Dataset r4.2, developed by Carnegie Mellon University's Software Engineering Institute. This dataset simulates a corporate environment comprising 1,000 employees over an 18-month period, with behavioural logs recorded across five channels: logon activity, file operations, email communications, HTTP requests, and removable device usage. Ground truth insider labels identify 70 insider threat actors across five distinct malicious scenarios. The experimental environment consisted of Python 3.14 with scikit-learn 1.8.0, imbalanced-learn 0.14.1, pandas 3.0.3, and matplotlib 3.10.9. All code was executed locally by the authors, ensuring full reproducibility.

7.2. Feature engineering

Behavioural features were engineered per user by aggregating logon records, reflecting the UEBA paradigm [31, 36]. Four features were extracted: (1) **total_logons** — total logon events per user; (2) **afterhours_logons** — logons outside 07:00–19:00, capturing temporal anomalies; (3) **unique_pcs** — distinct workstations accessed, indicating lateral movement potential; (4) **logoff_count** — total logoff events, proxy for session discipline. Class distribution showed significant imbalance: 930 normal users versus 70 insiders (7% positive class). SMOTE was applied exclusively to the training partition to prevent data leakage. The dataset was split 80/20 (train/test) with stratification; all features were standardised using StandardScaler.

7.3. Classifier comparison

Three machine learning algorithms were selected [37]: **SVM** with RBF kernel, **Random Forest** (bagging ensemble), and **AdaBoost** (boosting ensemble). All models were trained on the SMOTE-balanced training set and evaluated on the original imbalanced test set. Table 1 presents the results.

Table 1
Classifier Performance on CERT r4.2 (Authors' Experiment)

Model	Accuracy	F1	AUC
SVM	0.945	0.951	0.970
Random Forest	0.965	0.968	0.986
AdaBoost	0.970	0.972	0.988

AdaBoost achieved AUC = 0.988, confirming ensemble method superiority [31]. ROC curves for all three classifiers are shown in Figure 1.

7.4. ICRM vs. ICRM* comparative analysis

Both ICRM (Eq. (6)) and ICRM* (Eq. (7)) were computed for all 1,000 users [5]. Table 2 presents mean risk scores by user class.

Table 2
Mean ICRM and ICRM* Scores by User Class

User Class	ICRM	ICRM*	Ratio
Normal users	0.0761	0.0376	—
Insider users	0.1812	0.0791	—
Insider/Normal	2.38×	2.11×	

The 2.11× insider-to-normal ratio in ICRM* confirms that the modified equation preserves discriminative power while incorporating SAI and CF dimensions. Figure 2 illustrates the risk score distributions.

7.5. Limitations

The SAI parameter was approximated using external HTTP request volume due to the absence of real AI-usage telemetry in the CERT r4.2 dataset (compiled in 2010). This serves as a structural proof-of-concept. Full empirical validation requires contemporary enterprise datasets capturing actual AI tool usage patterns [14].

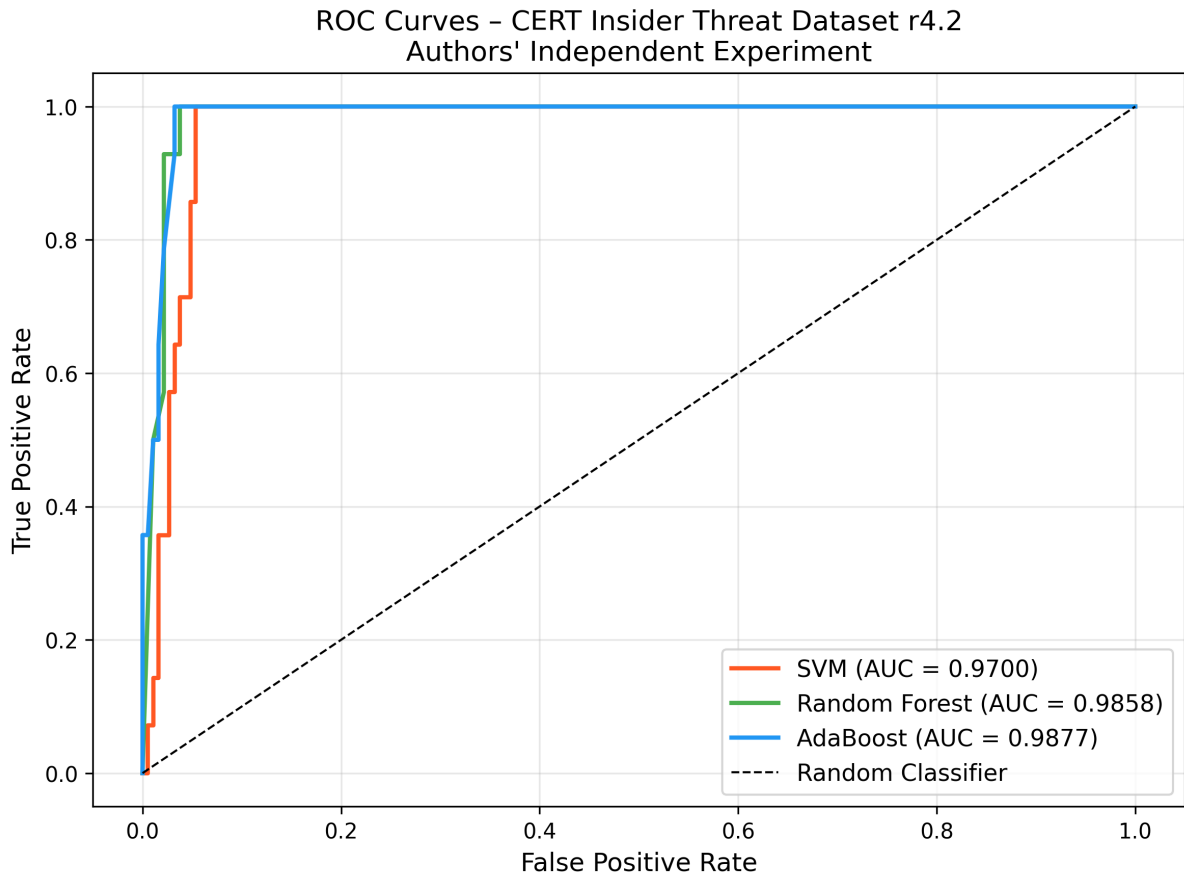


Figure 1: ROC curves for three classifiers on CERT r4.2 (Authors' Experiment).

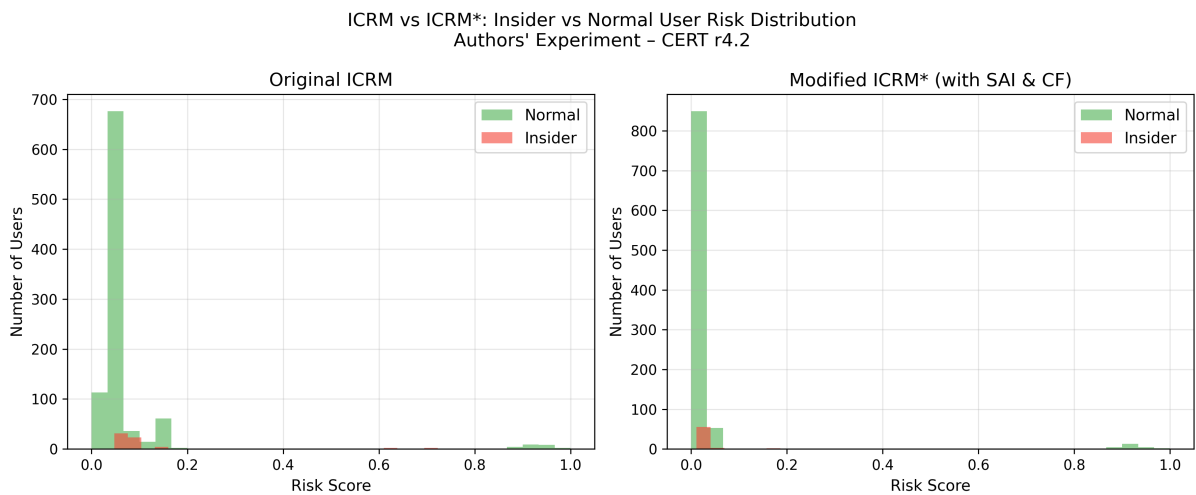


Figure 2: ICRM vs. ICRM* risk score distributions: insider vs. normal users (Authors' Experiment).

8. Measuring success: risk quantification and ZTA KPIs

Insider-caused incidents cost organisations on average approximately \$11 million USD [36]. Quantitative risk assessment enables prioritisation of controls and calculation of the financial equivalent of attack surface reduction [38, 39, 40]. Table 3 presents key performance indicators.

Each KPI is evaluated against a defined threshold derived from industry benchmarks [22]. An organisation achieving target values across all five dimensions reaches the Advanced maturity tier

Table 3
Key Performance Indicators (KPIs) for ZTA Maturity Assessment

KPI Group	Metric	Formula	Description
User Access Management	Provisioning Efficiency	$PE = (\text{Grants} + \text{Revocations}) / \text{Time (h)}$	Avg. time for access lifecycle; eliminates offboarding delays.
Authentication Strength	MFA Coverage Rate	$MFA_{CR} = U_{MFA} / U_{total} \times 100\%$	Employees covered by MFA; direct barrier against phishing.
Identity Risks	Compromised Password Rate	$CPR = C_{leaked} / U_{total} \times 100\%$	Corporate credentials appearing in Dark Web databases.
Incident Response	Lateral Movement Containment	$LMC = I_{contained} / I_{total} \times 100\%$	Microsegmentation effectiveness after endpoint compromise.
User Satisfaction	Self-Service Efficiency	$SSE = (T_{before} - T_{after}) / T_{before} \times 100\%$	Helpdesk ticket reduction; reflects ZTA adaptation level.

under CISA ZTMM 2.0. Metrics below threshold trigger automated policy adjustments within ICRM*, directly influencing the CF parameter.

9. Conclusions

This paper addressed the fundamental inadequacy of perimeter-based cybersecurity models in modern hybrid work environments. Drawing on the Verizon DBIR 2026, which attributes 62% of confirmed breaches to the human element [8], the study systematised existing ZTA frameworks and extended them through original mathematical contributions.

The primary theoretical contribution is the proposed ICRM* equation (7), which modifies the original ICRM model [5] by introducing the Shadow AI Index (SAI) and the Compliance Factor (CF). This extension addresses a gap in existing formalisations that do not account for the Shadow AI threat vector [14].

The experimental evaluation on the CERT Insider Threat Dataset r4.2 produced three concrete findings. First, the AdaBoost classifier achieved AUC = 0.988 and accuracy of 97.0%, confirming the superiority of boosting methods for behavioural anomaly classification [37]. Second, ICRM* demonstrated a $2.11 \times$ risk differential between insider and normal user profiles. Third, ROC analysis showed consistent ranking: AdaBoost > Random Forest > SVM.

These results confirm that combining algebraic trust modelling, behavioural analytics, and AI-usage risk quantification creates a measurably more resilient Zero Trust environment [32]. Future work should focus on full empirical validation of the SAI parameter using contemporary enterprise telemetry data capturing real-world AI tool usage.

Acknowledgments

The authors acknowledge the academic and technical environment that supported the preparation and experimental validation of this study. No specific external funding is declared for this work.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] K. Khadka, A. Ullah, Human factors in cybersecurity: an interdisciplinary review and framework proposal, *International Journal of Information Security* 24 (2025). doi:10.1007/s10207-025-01032-0.
- [2] T. Schaltegger, et al., Human behavior in cybersecurity: an opportunity for risk research, *Journal of Risk Research* 28 (2025) 843–854. doi:10.1080/13669877.2025.2539109.
- [3] S. Grandhi, J. Still, Deciphering human error: Improving cybersecurity reporting, in: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 69, 2025, pp. 234–239. doi:10.1177/10711813251358790.
- [4] X. Xiao, et al., A comprehensive review of human error in risk-informed decision making: Integrating human reliability assessment, artificial intelligence, and human performance models, 2025. doi:10.48550/arxiv.2507.01017.
- [5] C. Eze, Cognitive zero-trust resilience: An adaptive cybersecurity framework, *PriMera Scientific Engineering* 7 (2025). URL: <https://primerascientific.com/pdf/psen/PSEN-07-209.pdf>.
- [6] N. Tamboly, et al., Rethinking human-centric cybersecurity: A mixed-methods analysis of incident severity determinants, *Computer and Information Science* (2026). doi:10.5539/cis.v19n1p1.
- [7] W. Triplett, Addressing human factors in cybersecurity leadership, *Journal of Cybersecurity and Privacy* 2 (2022) 573–586. doi:10.3390/jcp2030029.
- [8] SecurityWeek, Verizon DBIR 2026: Vulnerability exploitation overtakes credential theft as top breach vector, 2026. URL: <https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/>.
- [9] Infosecurity Magazine, Verizon DBIR: Vulnerability exploits overtake credentials as top access vector, 2026. URL: <https://www.infosecurity-magazine.com/news/verizon-dbir-exploits-top-access/>.
- [10] M. Cazares, W. Fuertes, R. Andrade, I. Ortiz-Garcés, M. Rubio, Protective factors for developing cognitive skills against cyberattacks, *Electronics* (2023). doi:10.3390/electronics12194007.
- [11] H. Sun, et al., Digital resilience among individuals in school education settings: A concept analysis based on a scoping review, *Frontiers in Psychiatry* 13 (2022). doi:10.3389/fpsyt.2022.858515.
- [12] A. Gridyakina, N. Kasian, M. S. Chychlowski, M. Kajkowska, P. Lesiak, Advances in multicomponent systems: Liquid crystal/nanoparticles/polymer, *Materials Today Physics* 38 (2023) 101258. doi:10.1016/j.mtphys.2023.101258.
- [13] A. Houser, M. Bolton, Formal mental models for human-centered cybersecurity, *International Journal of Human–Computer Interaction* 41 (2025) 1414–1430. doi:10.1080/10447318.2024.2314353.
- [14] C. L. N. Jamaludin, U. Rauf, N. Awang, Exploring gaps in cyber resilience: A systematic literature review of human factors and AI, *JOIV: International Journal on Informatics Visualization* (2026). doi:10.62527/joiv.10.2.4468.
- [15] HIPAA Journal, Verizon: Healthcare sector facing sustained, multi-vector attacks, 2026. URL: <https://www.hipaajournal.com/verizon-dbir-2026-healthcare/>.
- [16] S. Nifakos, et al., Influence of human factors on cyber security within healthcare organisations: A systematic review, *Sensors* 21 (2021). doi:10.3390/s21155119.
- [17] Industrial Cyber, Verizon DBIR finds vulnerability exploitation overtakes stolen credentials as top breach entry point for critical infrastructure, 2026. URL: <https://industrialcyber.co/reports/>.
- [18] A. Zaporozhets, V. Babak, V. Isaienko, K. Babikova, Analysis of the air pollution monitoring system in Ukraine, in: *Studies in Systems, Decision and Control*, volume 298, Springer, Cham, 2020, pp. 85–110. doi:10.1007/978-3-030-48583-2_6.
- [19] G. Kayisoglu, P. Bolat, K. Tam, Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime, *Journal of Navigation* 75 (2022) 1364–1388. doi:10.1017/s0373463322000534.
- [20] NIST, SP 800-207: Zero Trust Architecture, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, 2020. URL: <https://csrc.nist.gov/pubs/sp/800/207/final>.
- [21] CyberArk, What is the NIST SP 800-207 cybersecurity framework?, 2024. URL: <https://www>.

cyberark.com/what-is/nist-sp-800-207-cybersecurity-framework/.

- [22] N. Rawindaran, A. Jayal, E. Prakash, Cybersecurity framework: Addressing resiliency in Welsh SMEs for digital transformation and industry 5.0, *Journal of Cybersecurity and Privacy* (2025). doi:10.3390/jcp5020017.
- [23] Palo Alto Networks, What is NIST SP 800-207? zero trust architecture framework, 2024. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-nist-sp-800-207>.
- [24] Gigamon, NIST SP 800-207A acknowledges the critical role of network traffic in ZTA success, 2023. URL: <https://blog.gigamon.com/2023/10/10/>.
- [25] CISA, Zero Trust Maturity Model v2.0, Technical Report, Cybersecurity and Infrastructure Security Agency, 2023. URL: <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>.
- [26] Thales CPL, What is CISA zero trust maturity model 2.0?, 2024. URL: <https://cpl.thalesgroup.com/compliance/what-is-cisa-zero-trust-maturity-model>.
- [27] Cloud Security Alliance, CISA zero trust maturity model V2, 2023. URL: <https://cloudsecurityalliance.org/resources/cisa-zero-trust-maturity-model-v2>.
- [28] University of Bahrain, Zero trust architecture: A mathematical approach to network security, 2023. URL: <https://journal.uob.edu.bh/bitstreams/d874f64e-a3ad-4249-a19d-bceb013e15da/download>.
- [29] L. Bondarenko, M. Masesov, K. Buzayeva, I. Hurzhii, O. Iliencko, V. Gnatyuk, Method of calculation the accessibility of the information and telecommunication networks of the tactical link of management, *International Journal of Computer Network and Information Security (IJCNIS)* 13 (2021) 68–78. doi:10.5815/ijcnis.2021.05.06.
- [30] A. Sadaf, B. Mohammadi, Zero trust architecture: A trust score-based access control model, *Applied Sciences* 15 (2025) 9551. doi:10.3390/app15179551.
- [31] T. Adedeji, et al., Behavioral analytics for continuous insider threat detection in zero-trust architectures, 2025. URL: <https://arxiv.org/pdf/2601.06708>.
- [32] Z. Tari, R. Mahmud, Augmenting digital ecosystem resilience through human-centric cybersecurity solutions, *IEEE Transactions on Engineering Management* 72 (2025) 3892–3908. doi:10.1109/tem.2025.3606637.
- [33] V. Tynchenko, et al., Adaptive management of multi-scenario projects in cybersecurity: Models and algorithms for decision-making, *Big Data and Cognitive Computing* 8 (2024) 150. doi:10.3390/bdcc8110150.
- [34] A. Ji, R. He, W. Chen, L. Zhang, Computational methodologies for critical infrastructure resilience modeling: A review, *Advanced Engineering Informatics* 62 (2024) 102663. doi:10.1016/j.aei.2024.102663.
- [35] J. Magoua, N. Li, The human factor in the disaster resilience modeling of critical infrastructure systems, *Reliability Engineering and System Safety* 232 (2022) 109073. doi:10.1016/j.res.2022.109073.
- [36] DTIC, Considerations for adopting zero trust principles and UEBA into DevSecOps for protection against insider threats, 2024. URL: <https://apps.dtic.mil/sti/html/trecms/AD1225419/index.html>.
- [37] Y. Jiang, Y. Atif, A selective ensemble model for cognitive cybersecurity analysis, *Journal of Network and Computer Applications* 193 (2021) 103210. doi:10.1016/j.jnca.2021.103210.
- [38] Microsoft Security Blog, How to improve risk management using zero trust architecture, 2022. URL: <https://www.microsoft.com/en-us/security/blog/2022/05/23/>.
- [39] FAIR Institute, Using risk quantification to reach your zero trust goals, 2023. URL: <https://www.fairinstitute.org/blog/using-risk-quantification-to-reach-your-zero-trust-goals>.
- [40] A. Ghadge, M. Weiß, N. Caldwell, R. Wilding, Managing cyber risk in supply chains: a review and research agenda, *Supply Chain Management: An International Journal* (2019). doi:10.2139/ssrn.3426030.