Journal of Computer Science and Information Technology
ISSN: 3080-3586
DOI: https://doi.org/10.61424/jcsit.v3i2.1016
Date Published Online: August 27, 2026
Journal Homepage: https://bluemarkpublishers.com/index.php/JCSIT

JCSIT
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Design and Validation Framework for Multi-Level Cybersecurity and Privacy Protection in Modern Digital Infrastructures

Kennedy Owino Jaramba[1] ✉ and Samwel Oonge[2]
[1]Masters in Information Technology, Maseno University, Kenya
[2]Supervisor, Maseno University, Kenya
Corresponding Author: Kennedy Owino Jaramba, **E-mail**: jarambaken@gmail.com

| ABSTRACT

The increasing complexity of cyber threats, interconnected technologies, and data-intensive digital services has exposed limitations in security strategies that depend on isolated controls. This study develops a multi-level cybersecurity and privacy framework that integrates complementary controls across physical, network, endpoint, application, data, identity and access management, monitoring and incident response, and human and policy domains. The framework was developed through structured synthesis of the ten cybersecurity and privacy studies reviewed in the source manuscript and alignment with established cybersecurity guidance. The revised model treats monitoring and incident response as a cross-cutting capability and privacy and governance as cross-cutting concerns. It further introduces a measurable evaluation structure based on layer-specific security indicators and an overall Multi-Level Cybersecurity Resilience Index. The framework is mapped to NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, and Zero Trust principles. The resulting architecture provides a practical basis for coordinating preventive, detective, responsive, recovery, governance, and privacy controls. Because the source studies did not include primary empirical testing, the present manuscript does not claim empirical effectiveness; instead, it specifies a validation protocol using expert assessment and/or controlled simulation. This study contributes an integrated architectural model and a measurable evaluation approach for organizations seeking adaptive and resilient cybersecurity.

| KEYWORDS

Cybersecurity; privacy; defense in depth; multi-level security; zero trust; NIST CSF 2.0; ISO/IEC 27001; incident response; security resilience; information security.

| ARTICLE INFORMATION

ACCEPTED: July 16, 2026 **PUBLISHED:** August 27, 2026 **DOI:** https://doi.org/10.61424/jcsit.v3i2.1016

1. Introduction

Cybersecurity and privacy are closely related because protection of information requires both security controls and appropriate governance over the collection, use, disclosure, retention, and access to information. The original manuscript correctly identifies that confidentiality, integrity, and availability are inseparable from meaningful protection of information and individual privacy.

Modern organizations operate interconnected infrastructures comprising networks, endpoints, applications, cloud services, databases, mobile devices, Internet of Things technologies, and human users. Consequently, compromise

of one component can propagate across other components. A defense strategy based on one control or one perimeter is therefore insufficient for many contemporary environments.

The reviewed literature in the source manuscripts spans cybersecurity education, open-source intelligence and critical infrastructure, CI/CD security, big-data security, cybersecurity ethics, digital fingerprinting, privacy and cybersecurity, generative-AI privacy and security, federated IoT security, and low-power IoT security. The synthesis indicates a recurring need for coordinated controls rather than isolated security mechanisms.

The original manuscript's principal contribution is an eight-layer architecture comprising physical security, network security, endpoint security, application security, data security, identity and access management, monitoring and incident response, and human and policy controls. This revision strengthens that contribution by clarifying the research design, separating established controls from the proposed integration, adding cross-cutting privacy and governance, aligning the architecture with current NIST CSF 2.0 terminology, and specifying measurable validation criteria.

1.1 Problem Statement

Existing cybersecurity guidance provides valuable principles, controls, and outcomes, but organizations still face the practical problem of coordinating controls across technical, physical, organizational, and human domains. The source manuscripts identify a gap in integrating data protection, application protection, device-level security, network defenses, monitoring, and human or policy controls into a coherent architecture. The present study addresses this integration problem by proposing a layered architecture and a corresponding evaluation structure.

1.2 Research Objective

The objective is to develop an integrated multi-level cybersecurity and privacy framework that coordinates preventive, detective, responsive, recovery, governance, and privacy controls across modern digital infrastructures.

1.3 Research Questions

RQ1: What cybersecurity and privacy capabilities recur across the reviewed literature?
RQ2: How can these capabilities be integrated into a coherent multi-level security architecture?
RQ3: How can the proposed architecture be mapped to established cybersecurity guidance?
RQ4: Which measurable indicators can be used to evaluate the effectiveness and resilience of the proposed layers?

1.4 Contributions

The study synthesizes ten cybersecurity and privacy publications into an integrated architectural model.
The study proposes an eight-layer defense-in-depth architecture.

Monitoring and incident response are positioned as a cross-cutting operational capability.

Privacy and governance are explicitly treated as cross-cutting concerns rather than merely as a subset of technical security.

The study provides a layer-specific measurement framework and a Multi-Level Cybersecurity Resilience Index for future empirical validation.

The study maps the proposed architecture to current NIST CSF 2.0, ISO/IEC 27001:2022, and Zero Trust principles.

2. Related Literature

2.1 Cybersecurity Education and Human Factors

Ahmad et al. emphasize the need for cybersecurity education across individuals, schools, and higher education and identify increasing privacy risks associated with cloud storage, facial recognition, drones, and connected

technologies. This supports the inclusion of human and policy controls as an integral layer rather than treating users solely as endpoints.

2.2 Open-Source Information and Critical Infrastructure

Zhang et al. examine publicly available information that may support reconnaissance and attacks against critical infrastructure. Their findings reinforce the importance of threat awareness, information governance, and organizational policies in addition to technical defenses.

2.3 CI/CD and Application Security

Asha et al. describe a multi-layered security approach for CI/CD pipelines using security checks, behavioral analysis, anomaly detection, and tools such as Jenkins, Docker, Snort, and Nagios. This literature supports treating application security as an active lifecycle concern (Aniwa, 2021)

2.4 Big Data Security

Rawat et al. examine security using big data and securing big data, including analytics, machine learning, access control, encryption, and alternative security approaches. This supports the proposed data-security layer and the use of analytics within monitoring.

2.5 Cybersecurity Ethics and Governance

Ababneh et al. emphasize accountability, transparency, fairness, proportionality, consent, and regulatory considerations. These themes support the cross-cutting human, governance, and privacy dimension of the proposed framework.

2.6 Digital Traces and Privacy

Musa et al. examine digital fingerprints and the tension between security benefits and privacy risks. This supports explicit privacy-by-design considerations across identity, application, data, and monitoring functions.

2.7 Privacy and Cybersecurity

Landwehr et al. frame privacy and cybersecurity as interconnected domains involving technical, policy, economic, and theoretical dimensions. This provides conceptual support for treating privacy and security as mutually reinforcing rather than independent subjects.

2.8 Generative AI Privacy and Security

Golda et al. examine user, ethical, regulatory, technological, and institutional dimensions of privacy and security in generative AI. The findings reinforce the need for governance and adaptive controls as emerging technologies change the threat environment.

2.9 Federated IoT Security

Kamal et al. analyze IoT security and privacy requirements and propose a federated privacy and security reference architecture. Their work supports the need for interoperability and privacy controls across distributed devices and communication environments.

2.10 Low-Power IoT and 5G Security

Cook et al. identify privacy, physical-layer security, human-centric issues, and gaps in security standards for low-power IoT devices on 5G and beyond. These findings reinforce the need to connect device, network, privacy, and human controls.

2.11 Literature Synthesis and Gap

Domain	Evidence from reviewed literature	Remaining integration need
Human and education	Cybersecurity awareness and education are repeatedly identified as necessary.	Integrate human behavior with technical controls.
Infrastructure and network	Critical infrastructure and IoT environments face reconnaissance and communication risks.	Coordinate network, physical, and device controls.
Application and DevSecOps	Security needs to be embedded throughout development and deployment.	Connect application controls with identity, endpoint, and monitoring.
Data and analytics	Big data requires protection and can also support detection.	Connect data protection with analytics and incident response.
Privacy and ethics	Privacy, accountability, consent, and fairness are recurring concerns.	Make privacy and governance cross-cutting.
Emerging technologies	AI, IoT, and 5G introduce changing attack surfaces.	Provide an adaptive feedback mechanism.

The gap addressed by this study is therefore not the absence of individual security controls. Rather, it is the lack of a single operational architecture in the source literature that explicitly coordinates the identified domains, provides cross-layer monitoring and response, embeds privacy and governance, and defines measurable indicators for evaluating the integrated model.

3. Research Methodology

3.1 Research Design

This study adopts a design-oriented conceptual framework approach supported by structured synthesis of the ten publications analyzed in the sourced manuscripts. The literature is used to identify recurring cybersecurity and privacy capabilities, while the framework is the study's design output. The present manuscript does not claim that the framework has already been empirically validated.

3.2 Literature Synthesis Procedure

The sourced manuscripts reviewed ten publications selected for their relevance to cybersecurity education, critical infrastructure, CI/CD, big data, ethics, digital traces, privacy, generative AI, IoT, and next-generation networks.

3.3 Framework Development

Framework development followed four stages: (1) extraction of security and privacy capabilities from the reviewed literature; (2) thematic grouping of capabilities into architectural domains; (3) organization of domains into defense-in-depth layers; and (4) definition of cross-cutting monitoring, response, privacy, governance, and evaluation mechanisms.

3.4 Validation Protocol

Because the sourced manuscripts contain no primary empirical validation, the framework should be evaluated in a subsequent empirical phase. A recommended protocol is expert assessment followed by controlled simulation or organizational case study. Experts should rate completeness, relevance, feasibility, clarity, scalability, privacy coverage, and adaptability using a five-point Likert scale. A simulation should measure detection rate, false-positive rate, mean time to detect, mean time to respond, patch compliance, MFA coverage, vulnerability reduction, backup recovery success, and policy compliance.

3.5 Measurement Model

Each security layer can be scored using normalized indicators. Let S_i denote the score of layer i and w_i its weight, with the weights summing to one. The proposed Multi-Level Cybersecurity Resilience Index (MLCRI) is:

$$MLCRI = \sum_{i=1}^{8} w_i S_i, \quad \text{where } \sum_{i=1}^{8} w_i = 1.$$

Equal weights may be used for an initial assessment; empirically derived weights should be preferred after expert validation.

4. Proposed Multi-Level Cybersecurity and Privacy Framework

4.1 Design Principles

Defense in depth: compromise of one control should not expose the entire environment.
Least privilege: users, devices, applications, and services receive only necessary access.
Continuous monitoring: security events are collected and correlated across layers.
Adaptive response: detected threats feed risk assessment and control adjustment.
Privacy by design: privacy requirements are incorporated into collection, processing, access, sharing, and retention. Governance and accountability: technical controls are supported by policies, responsibilities, training, and compliance mechanisms.

4.2 Physical Security Layer

The physical layer protects hardware, infrastructure, facilities, and environmental conditions. Controls include biometric authentication, surveillance cameras, secure server rooms, environmental monitoring, smart locks, and access cards. Physical compromise can bypass logical controls; therefore, physical security is the foundation of the architecture.

4.3 Network Security Layer

The network layer protects communication paths and regulates traffic between internal and external systems. Controls include firewalls, IDS/IPS, VPNs, network segmentation, secure configurations, and Zero Trust principles. Network events should feed the monitoring and incident-response capability.

4.4 Endpoint Security Layer

The endpoint layer protects laptops, servers, mobile devices, and other computing endpoints. Controls include anti-malware, endpoint detection and response, patch management, configuration management, device encryption, and asset inventory.

4.5 Application Security Layer

The application layer protects software and web services through secure software development practices, code review, vulnerability assessment, API security, web application firewalls, dependency management, and secure deployment practices. The layer addresses common application weaknesses including injection and cross-site scripting.

4.6 Data Security Layer

The data layer protects information at rest, in transit, and during processing. Controls include encryption, access control, data loss prevention, backup and recovery, retention controls, integrity mechanisms, and data classification. The layer supports confidentiality, integrity, and availability while incorporating privacy requirements.

4.7 Identity and Access Management Layer

IAM controls who can access resources, what they can access, and under which conditions. Core controls include multi-factor authentication, role-based access control, privileged access management, single sign-on, account lifecycle management, and periodic access review.

4.8 Monitoring and Incident Response Layer

Monitoring and incident response is a cross-cutting capability spanning all layers. SIEM, threat intelligence, security operations, log management, detection analytics, alert triage, containment, eradication, recovery, and post-incident learning provide continuous feedback. This layer converts the architecture from a collection of preventive controls into an adaptive defense system.

4.9 Human and Policy Layer

The human and policy layer provides organizational governance and behavioral safeguards. Controls include awareness training, phishing-resistance programs, password policies, incident-response plans, role definitions, acceptable-use policies, risk governance, compliance monitoring, and management accountability.

4.10 Cross-Cutting Privacy and Governance

Privacy is treated as a cross-cutting requirement across all layers. Relevant controls include data minimization, purpose limitation, lawful and documented processing, consent where applicable, access and correction processes, pseudonymization or anonymization where appropriate, retention controls, secure sharing, privacy impact assessment, and accountability. Governance links these controls to organizational risk management and regulatory obligations.

5. Framework Architecture and Operational Flow

The architecture operates as a feedback system. Assets and users are protected through the eight layers; events from those layers are collected by monitoring and incident response; threat intelligence and risk assessment inform response and control adjustment; and lessons learned feed policy, configuration, training, and future risk assessments.

Layer	Core controls	Indicative measures
Physical	Biometrics, CCTV, secure rooms, environmental controls	Unauthorized access events; physical-control compliance
Network	Firewall, IDS/IPS, VPN, segmentation, Zero Trust	Blocked attacks; segmentation coverage; intrusion detection rate
Endpoint	EDR, anti-malware, patching, encryption	Patch compliance; malware incidents; EDR detection
Application	SSDLC, code review, WAF, API security, scanning	Critical vulnerabilities; remediation time; secure-release compliance
Data	Encryption, DLP, backup, access control	Encryption coverage; DLP incidents; recovery success
IAM	MFA, RBAC, PAM, SSO	MFA coverage; privileged violations; access-review compliance
Monitoring/IR	SIEM, SOC, threat intelligence, response	MTTD; MTTR; false-positive rate; containment time
Human/Policy	Training, policies, governance, response plans	Training completion; phishing failure; policy compliance

6. Alignment with Established Frameworks

The proposed architecture is complementary to, rather than a replacement for, established frameworks. NIST CSF 2.0 provides a taxonomy of high-level cybersecurity outcomes and does not prescribe a single way to achieve those outcomes. This creates space for an organization-specific operational architecture such as the one proposed here. ISO/IEC 27001:2022 provides requirements for an information security management system and continual improvement. Zero Trust contributes principles for continuous verification and least-privilege access.

Proposed component	NIST CSF 2.0 alignment	ISO/IEC 27001:2022 / governance alignment	Operational role
Physical	Protect	Physical and asset protection	Prevent physical compromise
Network	Protect; Detect	Network and communications protection	Control traffic and segmentation
Endpoint	Protect; Detect	Asset/configuration management	Reduce endpoint exposure
Application	Protect	Secure development and technical controls	Reduce software vulnerabilities
Data	Protect; Govern	Information protection and risk treatment	Protect sensitive information
IAM	Govern; Protect	Access control and identity governance	Reduce credential and privilege abuse
Monitoring/IR	Detect; Respond; Recover	Monitoring and incident management	Detect, contain and recover
Human/Policy	Govern	Organizational and people controls	Govern behavior and accountability
Privacy/Governance	Govern	Privacy, risk, compliance and continual improvement	Protect rights and manage obligations

7. Evaluation Framework

7.1 Expert Evaluation

A panel of cybersecurity, information-security, privacy, networking, and governance practitioners can evaluate the framework using a five-point scale. Suggested criteria are completeness, relevance, clarity, feasibility, interoperability, scalability, privacy coverage, adaptability, and perceived usefulness.

7.2 Technical Simulation

A controlled test environment can implement representative controls for the eight layers. Attack scenarios should be selected ethically and executed only in an isolated environment. Outcomes should include detection rate, false-positive rate, mean time to detect, mean time to respond, vulnerability reduction, access-control violations, patch compliance, and recovery success.

7.3 Statistical Analysis

Descriptive statistics should summarize expert ratings and technical measurements. Reliability of multi-item scales may be examined using Cronbach's alpha where assumptions are satisfied. Differences between baseline and framework-enabled conditions can be evaluated using appropriate paired or independent tests depending on the experimental design. Effect sizes and confidence intervals should accompany significance tests.

7.4 Success Criteria

Outcome	Example success criterion
Detection	Higher proportion of simulated incidents detected
Response	Lower mean time to detect and respond
Endpoint hygiene	Higher patch and EDR coverage
Identity	Higher MFA and access-review compliance
Application security	Lower number/severity of unresolved vulnerabilities
Data protection	Higher encryption and backup-recovery coverage
Human controls	Higher training/policy compliance
Overall resilience	Higher MLCRI without unacceptable operational overhead

8. Discussion

The framework's primary contribution is architectural integration. The reviewed literature demonstrates that cybersecurity challenges arise across education, infrastructure, software delivery, data, ethics, privacy, IoT, AI, and next-generation networks. The proposed model brings these concerns into a common defense-in-depth structure. Its distinction from a simple list of controls lies in the explicit relationships among layers, cross-cutting monitoring and response, cross-cutting privacy and governance, and a proposed measurement model.

The framework should not be interpreted as a substitute for NIST CSF 2.0 or ISO/IEC 27001:2022. Instead, it can serve as an operational architecture through which organizations organize controls and map them to established risk-management outcomes. NIST CSF 2.0 emphasizes outcomes and organizational profiles, while ISO/IEC 27001 provides ISMS requirements; the proposed architecture supplies a layer-oriented view for implementation and assessment.

The adaptive component is especially important. Cybersecurity controls cannot be assumed to remain optimal as threats, technologies, and organizational processes change. Continuous monitoring, risk assessment, response, lessons learned, and control adjustment therefore form a feedback loop. The proposed validation model is intended to test whether this integrated arrangement produces measurable improvement rather than assuming that layering automatically produces effectiveness.

9. Limitations

- The framework is derived from the ten publications analyzed in the source manuscript and therefore does not constitute a systematic review of the entire cybersecurity literature.
- The source study did not include primary empirical data or a controlled implementation; consequently, effectiveness, scalability, and cost claims remain to be validated.
- The proposed MLCRI weighting scheme is conceptual until expert or empirical evidence supports specific weights.
- Implementation feasibility may vary according to organizational size, budget, skills, technology, regulatory environment, and risk profile.
- Cross-border cybercrime and privacy enforcement involve legal and jurisdictional issues beyond the technical architecture.

10. Conclusion and Future Research

This study proposes an integrated multi-level cybersecurity and privacy framework that combines physical, network, endpoint, application, data, identity and access management, monitoring and incident response, and human and policy controls. The framework responds to the integration gap identified in the reviewed literature by organizing complementary controls into a defense-in-depth architecture and by introducing cross-cutting privacy, governance, monitoring, and adaptive feedback.

The manuscript deliberately distinguishes conceptual contribution from empirical evidence. The architecture is sufficiently specified to support subsequent validation through expert assessment, controlled simulation, organizational case studies, or longitudinal implementation. Future research should validate the layer indicators, estimate evidence-based weights for the MLCRI, assess implementation cost and scalability, compare the framework against alternative architectures, and examine its performance in cloud, IoT, AI, healthcare, financial, and public-sector environments.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

[1] Ababneh, J., et al. (2025). Cybersecurity Ethical Aspects (CEA).
[2] Ahmad, N., et al. (2022). A cybersecurity educated community.
[3] Asha, P., et al. (2025). Multi-layered Security Approach for CI/CD Pipeline with Web Application Development.
[4] Aniwa S.C. (2021). Impact of Supply Chain Integration on Operational Performance: Insights from Manufacturing Firms in Emerging Economies. Iconic Research And Engineering Journals, 5(4).
[5] Cook, J., et al. (2023). Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions.
[6] Golda, A., et al. (2024). Privacy and Security Concerns in Generative AI: A Comprehensive Survey.
[7] International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
[8] Kamal, M., et al. (2023). Privacy and Security Federated Reference Architecture for Internet of Things.
[9] Landwehr, C., et al. (2012). Privacy and Cybersecurity: The Next 100 Years.
[10] Musa, A., et al. (2025). Our Digital Traces in Cybersecurity: Bridging the Gap Between Anonymity and Identification.
[11] National Institute of Standards and Technology. (2020). Zero Trust Architecture. NIST Special Publication 800-207.
[12] National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource and Overview Guide. NIST SP 1299. https://doi.org/10.6028/NIST.SP.1299
[13] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. https://doi.org/10.6028/NIST.CSWP.29
[14] Rawat, D. B., et al. (2021). Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security.
[15] Zhang, et al. (2022). Accessible from the open web: A qualitative analysis of the available open-source information involving cyber security and critical infrastructure.